2016
PRAGUE
PRAHA

17th International Conference

17. ročník mezinárodní konference

SECURITY – WELCOME BACK

May 25th – 26th 2016
25. – 26. května 2016

Under the Auspices of / Záštita

Mgr. Bohuslav Sobotka
předseda vlády České republiky
Prime Minister

Milan Chovanec
ministr vnitra České republiky
Minister of Interior

Ministerstvo školství, mládeže a tělovýchovy
Ministry of Education, Youth and Sports

Ing. Zdeněk Adamec
náměstek ministra zemědělství pro řízení sekce ekonomiky a informačních technologií
Deputy Minister of Agriculture

Ing. Jaroslav Šmíd
náměstek ředitele Národního bezpečnostního úřadu
Deputy Director of National Security Authority

Ing. Vladimír Dlouhý, CSc.
prezident Hospodářské komory České republiky
President of the Czech Chamber of Commerce

Dear madam, Dear sir,

The last week of May is for the 17th time devoted to the information security conference IS2, this time with a title Security – Welcome Back. This year's conference will be held in the beautiful baroque space of the Mirror Hall of Klementinum in Prague on 25th-26th May, 2016. As each year, top experts on information security from both the Czech Republic and foreign countries will present their views on the topic.

This regular conference presents an opportunity to get to know the latest news and developments in the world of information security. We believe that these two days spent in the beautiful premises of Klementinum with interesting people will present for you an opportunity for both formal and informal exchange of information with both the presenters and participants of the conference.

We look forward to seeing you at the conference.

Programme Committee

Lukáš Klášterský, Erste Group
Radim Kolář, Medtronic
Vashek Matyáš, MU Brno
Richard Michálek
Eva Racková, RVDA
Zdeněk Říha, MU Brno (chairman)
Pavel Východský
Václav Žid, Ministerstvo obrany

In co-operation / Ve spolupráci

AFCEA

Cacio

ISACA
Trust in, and value from, information systems
Czech Republic Chapter

Platinum partner / Platinový partner

IBM

Vážená paní, vážený pane,

Již po sedmnácté patří poslední květnový týden konferenci o informační bezpečnosti IS2, tentokrát s tématem Security – Welcome Back. Letošní ročník proběhne v krásných prostorách barokní Zrcadlové kaple Klementina ve dnech 25. – 26. května 2016 a jako každý rok na konferenci vystoupí špičkoví odborníci na informační technologie a řízení rizik z České republiky i ze zahraničí.

Tato pravidelná akce je příležitostí seznámit se s novinkami a vývojem ve světě informační bezpečnosti. Věříme, že dva dny strávené v krásných prostorách Klementina se zajímavými lidmi pro Vás budou příležitostí k formální i neformální výměně zkušeností s přednášejícími i účastníky konference.

Na setkání s Vámi se těší

Programový výbor

Lukáš Klášterský, Erste Group
Radim Kolář, Medtronic
Vashek Matyáš, MU Brno
Richard Michálek
Eva Racková, RVDA
Zdeněk Říha, MU Brno (předseda)
Pavel Východský
Václav Žid, Ministerstvo obrany

Gold partner / Zlatý partner

Special Partners / Speciální partneři

SECURITY – WELCOME BACK

May 25th – 26th 2016
25. – 26. května 2016

National Library of the Czech Republic, Prague
Zrcadlová kaple – Národní knihovna ČR, Praha

PROGRAMME

Wednesday, May 25th 2016

12:30 – 12:50	Registration
12:50 – 13:30	**Artifical Intuition Tool for Extraction of Meaning from Texts** Shmuel Bar
13:30 – 14:10	**The future of financial services online access** Simona Buchovecká
14:10 – 14:30	Coffee break
14:30 – 15:10	**Measuring and Studying Cybercrime** Richard Clayton
15:10 – 15:50	**The biggest threat for citizen´s privacy** Pavol Lupták
15:50 – 16:10	Coffee break
16:10 – 18:00	**Panel Discussion: Path to eHealth in the Czech Republic** Jiří Borej, Vlastimil Černý, Leoš Heger, Soňa Měrtlová, Petr Pavlinec

Thursday, May 26th 2016

8:45 – 9:00	Registration
9:00 – 9:30	**The processes of response on computer security incidents** Ivan Makatura
9:30 – 10:15	**The Cyber Security Act – one year later** Adam Kučínský
10:15 – 10:35	Coffee break
10:35 – 11:20	**What is Information?** John Rogers Searle
11:20 – 12:05	**Modern Security Operations in Bank Sector** Roland Supper
12:05 – 13:00	Lunch
13:00 – 13:40	***Section A:* From hackers´s diary…** Pavol Lupták ***Section B:* Detecting malware with machine learning, from C&C to exfiltration** Michal Svoboda
13:40 – 14:20	***Section A:* SCADA security – good news or nightmare?** Pavel Hejduk ***Section B:* Changes in attack strategies over the last five years and further outlook** Jiří Slabý
14:20 – 14:50	***Section A:* Improving security management with SIEM** Martin Dvořák, Zora Říhová, Libor Dostálek ***Section B:* Your genome and insurance: opportunity or threat?** Ondřej Antoš
14:50 – 15:10	Coffee break
15:10 – 15:50	**GPS Radio Hacking – What the Hell Time Is It?** Tomáš Rosa
15:50 – 16:30	**eIDAS and GDPR regulations** Martin Maisner
16:30 – 16:50	Lottery Draw, Closing Ceremony

PROGRAM

Středa, 25. května 2016

12:30 – 12:50	Zahájení
12:50 – 13:30	**Umělá intuice ve službách bezpečnosti** Shmuel Bar
13:30 – 14:10	**Budoucnost online přístupu k finančním službám** Simona Buchovecká
14:10 – 14:30	Přestávka
14:30 – 15:10	**Měření a studium kyberzločinu** Richard Clayton
15:10 – 15:50	**Najväčšia hrozba pre digitálne súkromie občanov** Pavol Lupták
15:50 – 16:10	Přestávka
16:10 – 18:00	**Panelová diskuse: Cesta k eHealth v ČR** Jiří Borej, Vlastimil Černý, Leoš Heger, Soňa Měrtlová, Petr Pavlinec

Čtvrtek, 26. května 2016

8:45 – 9:00	Zahájení
9:00 – 9:30	**Procesy riešenia bezpečnostných počítačových incidentov** Ivan Makatura
9:30 – 10:15	**Zákon o kybernetické bezpečnosti – rok poté** Adam Kučínský
10:15 – 10:35	Přestávka
10:35 – 11:20	**Informace ~ Informace?** John Rogers Searle
11:20 – 12:05	**Moderní provoz bezpečnosti v bankovním sektoru** Roland Supper
12:05 – 13:00	Oběd
13:00 – 13:40	***Sekce A:* Z deníčku hackera…** Pavol Lupták ***Sekce B:* Detekce malware pomocí strojového učení, od C&C po exfiltraci** Michal Svoboda
13:40 – 14:20	***Sekce A:* Bezpečnost SCADA – dobrá zpráva nebo noční můra?** Pavel Hejduk ***Sekce B:* Změny v přístupu útočníků za posledních pět let a další výhled** Jiří Slabý
14:20 – 14:50	***Sekce A:* Možnosti zlepšení provozu systémů SIEM** Martin Dvořák, Zora Říhová, Libor Dostálek ***Sekce B:* Váš genom a pojištění: příležitost nebo hrozba?** Ondřej Antoš
14:50 – 15:10	Přestávka
15:10 – 15:50	**Radiohacking GPS – víme, která bije?** Tomáš Rosa
15:50 – 16:30	**Nařízení eIDAS a GDPR** Martin Maisner
16:30 – 16:50	Tombola, závěr

TABLE OF CONTENTS / OBSAH

ARTIFICIAL INTUITION TOOL FOR EXTRACTION OF MEANING FROM TEXTS / UMĚLÁ INTUICE VE SLUŽBÁCH BEZPEČNOSTI
SHMUEL BAR 1

THE FUTURE OF FINANCIAL SERVICES ONLINE ACCESS / BUDOUCNOST ONLINE PŘÍSTUPU K FINANČNÍM SLUŽBÁM
SIMONA BUCHOVECKÁ 9

MEASURING AND STUDYING CYBERCRIME / MĚŘENÍ A STUDIUM KYBERZLOČINU
RICHARD CLAYTON 21

THE BIGGEST THREAT FOR CITIZEN´S PRIVACY / NAJVÄČŠIA HROZBA PRE DIGITÁLNE SÚKROMIE OBČANOV
PAVOL LUPTÁK 29

THE PROCESSES OF RESPONSE ON COMPUTER SECURITY INCIDENTS / PROCESY RIEŠENIA BEZPEČNOSTNÝCH POČÍTAČOVÝCH INCIDENTOV
IVAN MAKATURA 41

THE CYBER SECURITY ACT – ONE YEAR LATER / ZÁKON O KYBERNETICKÉ BEZPEČNOSTI – ROK POTÉ
ADAM KUČÍNSKÝ 51

WHAT IS INFORMATION? / INFORMACE ~ INFORMACE?
JOHN ROGERS SEARLE 59

MODERN SECURITY OPERATIONS IN BANK SECTOR / MODERNÍ PROVOZ BEZPEČNOSTI V BANKOVNÍM SEKTORU
ROLAND SUPPER 61

FROM HACKER'S DIARY... / Z DENÍČKU HACKERA...
PAVOL LUPTÁK 71

SCADA SECURITY – GOOD NEWS OR NIGHTMARE? / BEZPEČNOST SCADA – DOBRÁ ZPRÁVA ANEBO NOČNÍ MŮRA?
PAVEL HEJDUK 85

IMPROVING SECURITY MANAGEMENT WITH SIEM / MOŽNOSTI ZLEPŠENÍ PROVOZU SYSTÉMŮ SIEM
MARTIN DVOŘÁK, ZORA ŘÍHOVÁ, LIBOR DOSTÁLEK 91

DETECTING MALWARE WITH MACHINE LEARNING, FROM C&C TO EXFILTRATION /
DETEKCE MALWARE POMOCÍ STROJOVÉHO UČENÍ, OD C&C PO EXFILTRACI
MICHAL SVOBODA 111

CHANGES IN ATTACK STRATEGIES OVER THE LAST FIVE YEARS AND FURTHER OUTLOOK /
ZMĚNY V PŘÍSTUPU ÚTOČNÍKŮ ZA POSLEDNÍCH PĚT LET A DALŠÍ VÝHLED
JIŘÍ SLABÝ 119

YOUR GENOME AND INSURANCE: OPPORTUNITY OR THREAT? / VÁŠ GENOM A POJIŠTĚNÍ: PŘÍLEŽITOST NEBO HROZBA?
ONDŘEJ ANTOŠ 133

GPS RADIO HACKING – WHAT THE HELL TIME IS IT? / RADIOHACKING GPS – VÍME, KTERÁ BIJE?
TOMÁŠ ROSA 143

EIDAS AND GDPR REGULATIONS / NAŘÍZENÍ EIDAS A GDPR
MARTIN MAISNER 159

PANEL DISCUSSION – PATH TO EHEALTH IN THE CZECH REPUBLIC / PANELOVÁ DISKUSE – CESTA K EHEALTH V ČR
JIŘÍ BOREJ, VLASTIMIL ČERNÝ, LEOŠ HEGER, SOŇA MĚRTLOVÁ, PETR PAVLINEC 165

O2 IT Services

Security Expert Center od O2 IT Services

Kybernetické hrozby bývají až do okamžiku vlastního napadení neviditelné, a proto jsou často podceňovány. Zhmotní-li se však taková hrozba, dokáže udeřit velmi tvrdě a zákeřně.

Security Expert Center (SEC) je profesionální služba, která efektivně eliminuje rizika spojená s kybernetickými hrozbami a se ztrátou, zneužitím nebo zcizením informací. Kybernetickou bezpečnost řeší jako komplexní problematiku. Spojuje v sobě řešení bezpečnostního monitoringu, reportingu a dalších modulárních bezpečnostních služeb a chrání tak IT prostředí jako celek. Pomáhá identifikovat klíčová aktiva společnosti, jako jsou kritické a důležité informace, procesy nebo systémy, a nastavuje optimální model jejich ochrany. Naplňuje požadavky zákona o kybernetické bezpečnosti a vytváří rovněž podmínky pro úspěšnou certifikaci ISO 27001 a ISO 22301. Ochranou aktiv se současně posílí účinnost ochrany zájmů a klíčových procesů klienta.

Vědět, co chránit

Každá informace má svoji cenu a útočníci si většinou vybírají cíle, aktiva, která jsou pro ně zajímavá, přinášejí přímý či nepřímý finanční zisk nebo poskytují něco, co se dá na peníze transformovat. Ne vždy ale organizace a podniky svá klíčová aktiva skutečně znají a jen málokdy vědí, jaká je jejich skutečná hodnota, jak ji měřit a jak aktiva doopravdy chránit.

Prevence, detekce a odpovědnost

Security Expert Center stojí na třech základních pilířích: prevence, detekce, odpovědnost. Efektivně eliminuje rizika spojená s kybernetickými hrozbami, případně se ztrátou, zneužitím a zcizením informací. Bezpečnostní produkty integruje do funkčních a srozumitelných řešení, která poskytují celkové zabezpečení IT prostředí. Identifikace klíčových aktiv ve spojení s optimalizací ještě není na českém trhu standardem.

Komplexní bezpečnost

Potenciální kybernetické hrozby se identifikují proaktivně na základě průběžného vyhodnocování anomálií v chování jednotlivých infrastrukturních prvků. SEC zajišťuje komplexní nasazení bezpečnostních nástrojů, dohledových zařízení a ochrany. Nastaví průběžný reporting, analýzy a připraví návrhy nápravných opatření. Služba může být jednorázová nebo dlouhodobá formou tzv. učící se organizace. Implementovat lze na základě požadavků zákazníka různé varianty řešení.

Varianty řešení

Přizpůsobení

Přizpůsobení spočívá v úpravě bezpečnostního monitoringu u zákazníka. Na základě detailní analýzy se navrhne optimální řešení: nákladový model, architekturu, postup implementace atd. Výhodou je maximalizace využití vlastního HW a SW a interních lidských zdrojů.

Vybudování

Implementace nového řešení na klíč. SEC se pro zákazníka staví bez nutnosti hledat volné lidské zdroje na trhu práce. Správu a provoz centra lze postupně převést do rukou O2 IT Services.

Komplexní služba

Komplexní služba je vhodné řešení i pro střední a malé společnosti a organizace. Poskytuje bezpečnostní monitoring a dohled jako komplexní službu, včetně potřebného zaškolení zaměstnanců zákazníka. Investiční náklady na straně zákazníka jsou přitom minimální.

O2 IT Services

O2 IT Services je stoprocentní dceřinou společností a členem koncernu O2 Czech Republic a.s. Její portfolio tvoří především IT a business consulting, systémová integrace, aplikační vývoj a vývoj tzv. Managed Services, služby provozu a optimalizace IT a řešení IT bezpečnosti. IT služby poskytuje komerčně, ale i vnitřně v rámci skupiny O2.

Podrobněji na stránkách www.o2its.cz.

Ing. Jiří Sedlák, ředitel Security Expert Center O2 IT Services s.r.o.

Artificial Intuition Tool for Extraction of Meaning from Texts
Nástroj umělé intuice pro extrakci významu z textů

Shmuel Bar

Shmuel Bar
sbar@intuview.com

Dr. Shmuel Bar is Senior Research Fellow at the Samuel Neaman Institute for National Policy Studies at the Technion – Israel Institute for Technology and founder and CEO of IntuView Ltd – a start-up dealing in “artificial intuition” technology. Shmuel served for thirty years in the Israeli intelligence community including in senior positions in the Office of the Prime Minister, where he dealt, inter alia, with Jihadist movements and WMD proliferation issues and in diplomatic posting in Europe where he liaised with European Intelligence agencies on these and other issues. He holds a Ph.D. in History of the Middle East from Tel-Aviv University.

Dr. Shmuel Bar je výzkumný pracovník na Institutu Samuela Neamana pro studia národních politik v Technionu – Israelském technologickém institutu a zakladatel a CEO společnosti IntuView Ltd – start-upu zabývajícím se technologií „umělé intuice“. Shmuel sloužil třicet let v izraelské zpravodajské komunitě, včetně vedoucích pozicích v úřadu předsedy vlády, kde se zabýval mimo jiné džihádistickými hnutími a otázkami šíření zbraní hromadného ničení a dále působil v diplomacii na postech v Evropě, kde spolupracoval s evropskými zpravodajskými službami na těchto a dalších otázkách. Je držitelem titulu Ph.D. v oboru historie Blízkého východu, který získal na Univerzitě v Tel-Avivu.

Artificial Intuition Tool for Extraction of Meaning from Texts

In a global environment challenged with enormous amounts of information, there is a need to identify affinities and disaffinities between semantic units in different languages in order to normalize streams of information and mine the “meaning” within them regardless of their original language. In the absence of a “silver bullet” of one technology that can be applied to all domains, the solution is based on emulation of the “intuitive” links that domain experts find between concatenations of lexical occurrences and appearances of a document and conclusions regarding the authorship, inner meaning and intent of the document.

Nástroj umělé intuice pro extrakci významu z textů

V dnešním globálním světě charakteristickým obrovským množstvím informací palčivě vzrůstá potřeba identifikovat příbuznost sémantických pojmů v různých jazycích tak, aby bylo možné tyto informace normalizovat a vytěžit z nich skutečný význam bez ohledu na jejich mateřský jazyk. Protože neexistuje produkt nebo technologie, které by daný problém pokryl ve všech oblastech, je jeho řešení založeno na emulaci intuitivních vztahů, které odborníci v dané oblasti naleznou mezi zřetězením slovních výskytů, povahou dokumentu, autorstvím dokumentu a skutečným smyslem a účelem dokumentu.

1 The Problem

Ever since the Tower of Babel, the human race has taken recourse to translation to bridge the gap between languages, cultures, societies and nations. Translation serves many purposes: it enables us to broaden the scope of our cultural perspective, to see the world in a way that others – friends and foes – do, to retrieve ancient knowledge that, otherwise, would be lost to mankind and to communicate between people on a day to day basis.

However, in a global environment challenged with enormous amounts of information, a challenge has arisen that cannot be solved by translation. This is the need to identify affinities and disaffinities between semantic units in different languages in order to normalize streams of information and mine the "meaning" within them regardless of their original language. When we look for information or wish to generate alerts – particularly in domains that are global – we do not want to be restricted to streams of information in one language; when we are interested in information – be it alerts on terrorism, fraud, cyber attacks or financial developments – we do not care if the origin is in English, French or Chinese.

The problem facing automated extraction of meaning from language is not restricted to translation between languages but within languages. That which we call a "language" is frequently a political definition and not one based on the linguistic reality. Some cases of a "language" are, actually a group of "dialects" that in other cases are defined as separate languages. The decision to call Swedish, Danish and Norwegian separate languages on one hand, and Moroccan, Libyan, Saudi Arabia and Egyptian all "Arabic" is political and not linguistic. Even within a language, the litmus test of inter-intelligibility is not always passed. For example: the correlation between the linguistic register of Shakespeare (or even a 19th Century writer) and the New York Times may be no more than 60-70%. A modern English speaker would find it difficult to understand an "English speaker" from the Elizabethan era. This is also true regarding the register of a fatwa by al-Qaeda and a modern Kuwaiti newspaper.

Even within the same language register, words, quotations, idioms or historic references can be „polysemic"; they have different meanings according to the domain and the context of the surrounding text. Waterloo can be a place in Belgium, an allusion to a final defeat or surrender, a London railway station, or a song by ABBA. It all depends in what context and who referred to it. A verse in the Quran may mean one thing to a moderate or mainstream Muslim and the exact opposite to a radical. The word "court" may mean: a royal court, a sports court, a school courtyard, a courthouse, or to court a person. The limited span of N-grams (three-four or even five tokens around the word) will not suffice to disambiguate the meaning: "What happened in/at the court yesterday amazed everyone who saw it" can refer to a ball game (that „happened in the court"), an exchange between lawyers, a fight between schoolboys or an event at the Royal Palace.

2 Existing Solutions

Methods to deal with this problem have generally been based on multi-lingual dictionaries that enable key words spotting (by input of a key word in one language, the search engine can add the nominal corresponding terms in other languages) or by automated translation of texts and application of the search criteria in the target language. The limitations of such methods are obvious: a word in one language has many "translations" and not all of them may even be remotely related to the meaning that the user is interested in. This limitation is partially mitigated by clustering techniques. However, these too leave us with low precision at the expense of high recall. This may be tolerable when the total quantity of data is within the realm of human capability to absorb. However, in a world of big data, the high precision-low recall paradigm is impractical.

In 1949, Warren Weaver who was director of the Natural Sciences Division of the Rockefeller Foundation and was involved during World War II in the American cryptology effort wrote a memorandum on automated translation using computer technology. In his memorandum, he likened translation to cryptology, and using the principles of information theory that he had worked on with Claude Shannon, he claimed: “It is very tempting to say that a book written in Chinese is simply a book written in English which was coded into the ‘Chinese code’.” If we have useful methods for solving almost any cryptographic problem, may it not be that with proper interpretation we already have useful methods for translation?” However, Weaver believed that there were very few words in a language that were ambiguous to the point that limited N-grams surrounding the words and he could not effectively “decrypt” them. This theory remains the basis for most automated translation efforts.

However, Weaver also raised in his memorandum another point. He suggested the analogy, of individuals living in a series of tall closed towers, all erected over a common foundation. When they try to communicate with one another, they shout back and forth, but cannot make the sound penetrate even the nearest towers. But, when an individual goes down his tower, he finds himself in a great open basement, common to all the towers. Here he establishes easy and useful communication with the persons who have also descended from their towers. Thus, he suggested, “it may be true that the way to translate from Chinese to Arabic, or from Russian to Portuguese, is not to attempt the direct route, shouting from tower to tower. Perhaps the way is to descend, from each language, down to the common base of human communication – the real but as yet undiscovered universal language – and then re-emerge by whatever particular route is convenient.”[i] In this description, Weaver touched – without calling it by name – on the approach that we are suggesting: semantic normalization of statements in different languages according to domain-specific ontologies.

Current technology for automated translation leaves much to be desired. Existing automated translation technology and tools for document categorization can provide guidelines for translators or rough categorization of texts in different languages; none however can provide the user with real-time operable intelligence and a detailed understanding of the meaning of the document. The more esoteric the text is, the less automated translation and categorization can extract the sentiment or the “hermeneutics” of the text. Therefore current cross-language information extraction relies, in the end, on human translation and analysis of the content of each document before any operational decision. This process suffers from several major deficiencies: long processing times, high percentage of false negatives and false positives, loss of insights due to ignorance of central cultural nuances. Named entity recognition has also not achieved the holy grail of automated entity creation and relationary mapping of all entities, which may relate to the user’s requirement.

3 The Proposed Solution

The need, therefore, is for technology that scans the entire gamut of information, identify the language and the language register of the texts, perform domain and topic categorization and match the information conveyed in different languages in order to create normalized data for assessment of the scope and nature of a problem.

In the absence of a “silver bullet” of one technology that can be applied to all domains, the solution is based on emulation of the “intuitive” links that domain experts find between concatenations of lexical occurrences and appearances of a document and conclusions regarding the authorship, inner meaning and intent of the document. In essence, this approach looks at a document as a holistic entity and deduces from combinations of statements meanings, which may not be apparent from any one statement. These meanings constitute the „hermeneutics” of the text, which is manifest to the initiated (domain specialist or follower of the political stream that the document represents) but is a closed book to the outsider. The crux of this concept is to extract not only the prima facie identification of a word or string of words in a text, but to expand the identification to include implicit context-dependent and culture-dependent information or “hermeneutics“ of the text. Thus, a word or quote in a text may “mean“ something that even contradicts the ostensible definition of that text.

The meanings that are represented in one language by one word (“court”) may be represented in other languages by completely different lexemes (words). When a human being reads the ambiguous word in a document, he may already know what sort of document he is reading – a sports newspaper, the school gazette, a legal document or a story about a royal court. Hence, he or she quickly disambiguates the word as holding the meaning typical of that type of document and the other meanings fade into the background.

“Idea Analysis” or “Meaning Mining” is the ability to extract from a text the hermeneutics (interpretation) that is not obvious to the non-initiated reader. Platform DOCEX (Document Exploitation) will make use of “Artificial Intuition“ technology for this purpose. Artificial Intuition is based on algorithms that apply to input of unstructured texts the aggregated comprehension by seasoned subject matter experts regarding texts of the same domain used in training. Humans reach “intuitive” conclusions – even by perfunctory reading – regarding the authorship and intent of a given text, subconsciously inferring them from previous experience with similar texts or from extra-linguistic knowledge relevant to the text. After accumulating more information through other features (statements, spelling and references) in the text, they either strengthen their confidence in the initial interpretation or change it.

These intuitive conclusions are part of what the Nobel Laureate Prof. Daniel Kahneman called “fast thinking” – a judgment process that operates automatically and quickly, with little or no effort and no sense of voluntary control[1]. “Fast thinking” is employed when a person reading a text or receiving new information identifies in it patterns and features from texts that he or she has encountered in the past in other texts, and links them to conclusions that he or she made then.

For example, viewing reprints from “The Telegraph” and “The Guardian” may lead to identification of the newspaper by the fonts and alignment. “Wicked” in America means “evil” and in colloquial British English – “great”, leading to language recognition from the context in which the word appeared

Words may also have different meanings (these are called *polysemes*) according to the domain and the context of the surrounding text. For example, Waterloo can be a place in Belgium (if mentioned in the context of other places nearby), a reference to a final defeat, a London railway station, or a song by ABBA. It all depends on in what context and who referred to it.

Quotations, idioms or historic references mean different things for different people. For example, in the Quran verse: “*And slay them wherever ye find them, ... but if they desist … Allah is forgiving and merciful. And fight them until persecution is no more, and religion is for Allah*” the last words would mean, to a moderate Muslim, “Do not wage war except in defense” whereas for radicals this is one of the most important verses mandating Jihad against non-Muslims.

Extra-linguistic knowledge also provides us implicit information on a name’s bearer: gender, ethnicity, tribal and family relations, nicknames, status, religious affiliation and even age. We expect a person by the name of Nigel or Alistair, to be British and not American. We would also expect an American woman by the name of “Ethyl”, “Lois” “Doris” or “Dorothy” to be an elderly woman. Indeed, the first two names are far more common in the UK than in the US and the female names were given to approximately 7% of the girls born in the United States in the 1930’s and to less than 0.05% in the 1970’s on.

IntuView has approached this problem through combining language-specific and language-register specific NLP (Natural Language Processing) with domain-specific ontologies. The IntuView

[1] Kahneman, D. (2011) *Thinking, Fast and Slow*, ISBN 978-0374275631.

technology[2] extracts such implicit meaning from a text or the hermeneutics of the text. It employs the relationship between lexical instances in the text and ontology - graph of unique language-independent concepts and entities that defines the precise meaning and features of each element and maps the semantic relationship between them. As a result of these insights, the process of disambiguation of meaning in texts is based on a number of stages:

1. Identification of the "register" of the language. The register of the language may represent a certain period of the language), dialects, social strata etc. In the global world today, however, it is not enough to identify languages; the world is replete with "hybrid languages" (e.g. "Spanglish" written and spoken by Hispanics in the US; "Frarabe" written and spoken by people of Lebanese and North African origin in France and Belgium) that are created when a person inserts secondary language into a primary (host) language, transliterates according to his own literacy, accent etc. It is necessary, therefore, to take the non-host language tokens, discover their original language, back transliterate them and then find the ontological representation of that word and insert it back into the semantic map of the document.
2. Identification through statistical analysis (based on prior training of tagged documents) of the ontological instances in the text in order to determine the probability that the author represents a certain background and ideological leaning. Statistical categorization of a document as belonging to a certain domain, topic, or cultural or religious context can reduce the number of possible interpretations of a given lexical occurrence, hence reducing ambiguity.
3. Disambiguation using the immediate neighborhood of the lexical instances. Such neighborhood consists of the lexical tokens directly preceding or following the lexical instance. After reading a number of texts of a given genre, the algorithm infers that X percent accord to statement A the meaning B. When statement C is encountered in a text that is categorized as belonging to the same genre, the algorithm derives from this a high level of confidence that C also means B. This confidence can be enhanced by additional information in the text.
4. Statistical categorization of a document as belonging to a certain domain, topic, or cultural or religious context in order to reduce ambiguity.
5. Chunking and Part of Speech Analysis of the text in order to use the relationship between different words (not necessarily arbitrarily choosing a certain level of N-grams) in order to provide additional disambiguating information.
6. Based on the identification of the domain of the text, the lexical units (words, phrases etc.) are linked to ontological instances with a unique meaning (as opposed to words which may have different meanings in different contexts) that can be "ideas", "actions", "persons", "groups" etc. An idea may be composed of statements in different parts of the document, which come together to signify an ontological instance of that idea.[3]
7. The ontological digest of the document then is matched with pre-processed statistical models to perform categorization.

[2] See US patent – Decision-support expert system and methods for real-time exploitation of documents in non-english languages, US 8078551 B2, PCT/IL2006/001017.

[3] Ontology is a graph of unique language-independent concepts and entities built by experienced subject matter experts that defines the precise meaning and features of each element in the graph and maps the semantic relationship between them. Hence, the features that are encountered in the surroundings of a lexical instance are factored in the system's decision to what unambiguous meaning (ontological instance) to refer the lexical instance. "Ontology", Tom Gruber, Encyclopedia of Database Systems, Ling Liu and M. Tamer Özsu (Eds.), Springer-Verlag, 2009.

This approach, therefore, is not merely "data mining" but "meaning mining". The purpose is to extract meaning from the text and to create a normalized data set that allows us to compare the "meaning" extracted from a text in one language with that, which is extracted from another language.

This methodology applies also to entity extraction. Here, the answer to Juliette's queclarative, "what's in a name" is – quite a lot a not – as Juliette suggested almost nothing. A name can tell us gender, ethnicity, religion, social status, family relationships and even age or generation.

In order to extract the information, however, we must first be able to resolve entities that do not look alike but may be the same entity (e.g. names of entities written in different scripts English, Arabic, Devanagari, Cyrillic) and to disambiguate entities that look the same but may not be (different transliterations of the same name in a non-Latin source language or culturally acceptable permutations of the same name). This entails:

1. Identification of entities within a structured to unstructured text, using both statistical and rule-base algorithms to categorize them as possible persons, groups, locations, addresses (URLs, dates, bank accounts), ideas, actions, and basically every type which is defined in the ontology. The data base entity or unstructured text is analyzed, using NLP tools or data mining in the DB to determine if it contains relevant entities and what type of entities they represent.
2. Statistical modeling of the names in order to identify possible ethnicity (much the same way that humans intuitively understand that a name is Irish, Hispanic or Indian).
3. The identified named entity, written in any given script (Latin, Cyrillic, Hindi or Arabic, etc.) is analyzed to determine its possible linguistic origin and then processed to extract possible spelling variants in the language of origin of the name. Thus, the name of the entity is restored to the original name in the source language or possible source languages. Information from the transliteration, which provides further identification, is retained for later analysis.
4. Validating the re-constructed names to identify if they correspond to possible names (as given or family names according to their place in the full name).
5. Parsing each name for identification of constituent parts (given name, patronymics etc.). The analysis of these components provides further validation or reassessment of the categorization of the type of the entity (an entity which may initially be considered a person-entity may actually be a place entity named after that person). This engine fills the attribute slots of the virtual entity (gender, location, size, object, predicate, ethnicity etc.) to provide further qualities for identification and matching. The name is vetted to determine its validity (a possible name or corrupt one).
6. Finding all the name alternatives by application of cultural naming convention in order to apply the appropriate naming conventions for disambiguation and matching.
7. Extracting implicit and contextual information from each entity, creating a virtual "identity card" of an entity with all the aggregated information that is collected in the inputs about it.
8. Aggregation of all the variants and aliases referring to an entity within the different inputs, while maintaining their source identity for possible regression.
9. Matching the names based on culture-specific naming conventions and matching the information implicit in it or in its context in order to discover links between the entities. Matching of entities by finding relations between identified entities (family relations in person entities, person-location relationships etc.).

4 Applications

The applications of the above technology are numerous and include:

- Real time field DOCEX and content forensics for users (fighting forces, law enforcement, etc).
- Scanning of Websites, social media and blogs to identify high-risk information.
- Matching of names in watch lists with new input intelligence and in border control.
- Emergency Response through characterizing feeds of social media, relating to their geographical area/ areas of responsibility in terms of locations, populations etc.
- Support of legal teams expeditiously and with minimal expenses identify all the relevant information, including the proverbial "unknown unknown".
- Support of financial researchers, providing them with the capability to extract relevant information from a large quantity of financial data (research reports, and public filing), to generate a structured representation of the information in the documents and to apply the data extracted to discover trends in references, co-references, sentiment and other correlations between financial entities.
- Comprehensive and in-depth analysis of social networks to identify subgroups based on linguistic and interest.

References

[1] Reproduction of Weaver's memorandum in http://www.mt-archive.info/Weaver-1949.pdf.

The future of financial services online access
Budoucnost online přístupu k finančním službám

Simona Buchovecká

Simona Buchovecká
buchovecka@sefira.cz

Simona Buchovecká works as IT Security Consultant in SEFIRA, where she participates on the design, preparation and realization of the projects in the field of information security and deployment of security technologies. Her main focus is on authentication and mobile identity, security of mobile devices and advanced persistent threat protection. Prior joining SEFIRA, she worked as Security and Privacy analyst in Deloitte. She graduated from the Czech Technical University in Prague, in the field of Computer Security. During her studies she also stayed at Ruhr-Universtity Bochum, where she focused on security of embedded systems.

Simona Buchovecká působí jako ICT Security Consultant ve společnosti SEFIRA, kde se dlouhodobě zaměřuje na informační bezpečnost a bezpečnostní technologie. Aktivně se podílí se na návrhu, přípravě a realizaci projektů zaměřených zejména na autentizaci a mobilní identitu, bezpečnost mobilních zařízení a ochranu před moderními pokročilými hrozbami. Dříve pracovala jako analytik pro oblast Security a Privacy ve společnosti Deloitte. Vystudovala Počítačovou bezpečnost na Fakultě informačních technologií ČVUT. Během studia absolvovala studijní stáž na Ruhr Universität v Bochumi, kde se věnovala bezpečnosti embedded zařízení.

The future of financial services online access

Online financial services represents very attractive target for the hackers. Attacks on e-banking users are wide spreading all over the world including Czech Republic. Providing simple, comfortable, and at the same time secure access to online services is nowadays a challenge for all financial institutions. In our paper we discuss weaknesses of traditional authentication methods, an efficient solution in form of multi-layered authentication concept is introduced and finally possible benefits of eIDAS directive utilization for fully paperless “virtual” banking enablement is demonstrated.

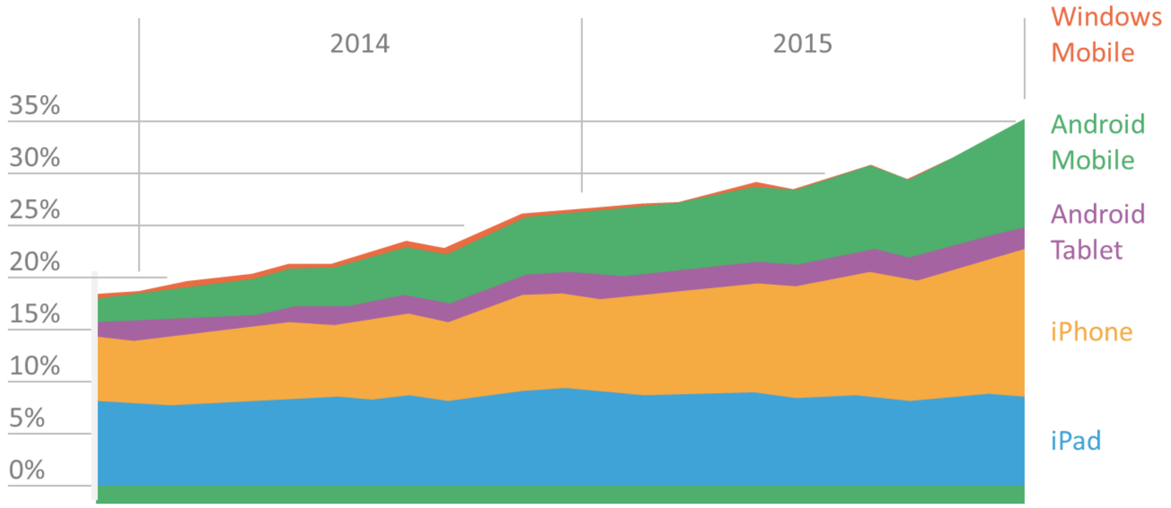
Budoucnost online přístupu k finančním službám

Online finanční služby představují pro hackery velmi atraktivní cíl a s útoky na elektronické bankovnictví se čím dál tím častěji setkáváme i v České republice. Poskytování komfortního a jednoduchého přístupu ke svým službám při současném zachování maximální úrovně bezpečnosti je tak velkou výzvou pro všechny finanční instituce. V příspěvku jsou popsány slabiny tradičních autentizačních metod, představeny efektivní řešení v podobě konceptu vícevrstvé adaptivní autentizace a demonstrovány příležitosti pro vytvoření plně bezpapírového „virtuálního“ bankovnictví, které přináší nařízení eIDAS.

1 Úvod

Přístup zákazníků ke službám, finanční služby nevyjímaje, je silně ovlivněn obecnými trendy v IT, jako jsou cloudové služby, mobilita či sociální sítě. Díky nim jsme zvyklí čerpat většinu služeb online, odkudkoliv a kdykoliv. Rychlý a pohodlný přístup k finančním službám očekáváme i od svojí banky, elektronické bankovnictví chceme mít stále nadosah a jednoduše přístupné. Online finanční služby jsou ale velmi atraktivním cílem pro hackery a útoky na elektronické bankovnictví jsou stále častější. Zavádění nových bezpečnostních opatření tak často komplikuje přístup k čerpání či zřizování nových služeb.

Poskytovat uživatelům komfortní a jednoduchý přístup ke službám při zachování maximální úrovně bezpečnosti se proto stává aktuální výzvou pro všechny finanční instituce.



Obrázek 1: Podíl plateb iniciovaných z mobilních zařízení roste – graf zobrazuje procento plateb iniciovaných z mobilních zařízení z celkového objemu plateb dle Adyen Mobile Payment Index[1] – index zahrnuje webové mobilní platby, a nebere v potaz tzv. in-app mobilní platby.

2 Hrozby a rizika

Útoky cílené na samotnou banku jsou dnes již málo pravděpodobné a vyskytují se velmi zřídka, neboť bankovní infrastruktura je dobře zabezpečená a takový útok vyžaduje detailní technické znalosti a pečlivou přípravu útočníka.

Mnohem jednodušší jsou útoky na koncové uživatele a jejich zařízení, která jsou už zcela mimo bezpečnostní perimetr a kontrolu banky. Nejjednodušší z pohledu provedení, ale zároveň velmi efektivní, jsou útoky využívající sociální inženýrství, které nevyžadují žádné hluboké znalosti útočníka. Sociální inženýr jednoduše uživatele více či méně sofistikovaným způsobem požádá o sdělení přístupových údajů.

Technicky propracovanější jsou útoky typu *Man in the Browser* (MitB), jejichž koncept prezentoval poprvé Augusto Paes de Barros v roce 2005 ve své prezentaci na téma budoucnosti backdoorů [2]. Dnes tohoto principu často využívají trojské koně zaměřené na elektronické bankovnictví. Příkladem mohou být Zeus či Hesperbot, které se masivně šířily i v České republice.

Útok typu MitB využívá techniky „process hooking“, který umožní kontrolovat a modifikovat data zobrazovaná uživateli ve webovém prohlížeči. Celý útok se odehrává na prezentační vrstvě a nemusí být na první pohled zřejmý. Webová doména, ke které se uživatel připojuje, je správná a její certifikát není podvržen. Ve chvíli, kdy trojský kůň odchytí požadavek na autentizaci, vloží do zobrazované stránky falešný přihlašovací formulář a uživatel tak nechtěně odešle data útočníkovi.

Odchycení samotných přihlašovacích údajů by ale útočníkovi nestačilo, protože ani po přihlášení by nemohl autorizovat transakce, pro které jsou např. využity OTP hodnoty zasílané prostřednictvím SMS. Tady útočníci mohou využít sociálního inženýrství, nebo zkombinovat MitB s technikou *Man in the Mobile* (MitMo). Takový útok pak probíhá následovně: Ve chvíli, kdy uživatel navštíví stránky internetového bankovnictví, je mu zobrazena výzva na instalaci dodatečné mobilní aplikace, obvykle se zdůvodněním zvýšení jeho bezpečnosti. Uživatel poté vyplní telefonní číslo, kam je mu zaslaný odkaz pro stažení aplikace a zároveň dojde ke spárování autentizačních údajů s telefonním číslem, kam jsou zasílané autorizační SMS. Po nainstalování mobilní aplikace získá útočník přístup k SMS autorizačním kódům a má vše co potřeboval k provedení transakce. Tímto scénářem jsou ohroženi zejména uživatelé, kteří pro ověřování plateb využívají zařízení na platformě Android, neboť Android obsahuje uživateli dostupné API, které umožňuje aplikacím přistupovat k SMS. U iOS takový útok prakticky není možný, kromě případů zařízení u kterého byl provedený jailbreak, neboť v iOS aplikace k SMS přistupovat nemohou.

I takto sofistikované nástroje jsou dnes běžně dostupné – na černém trhu je dnes možné zakoupit generátory malware (včetně technické podpory a s definovaným SLA), kde si útočník jednoduše navolí požadované vlastnosti malware a dle toho je mu vygenerovaný finální škodlivý soubor (spustitelný, či ve formě PDF nebo MS Office dokumentu), který stačí rozeslat mezi uživatele.

I když se koncový uživatel nachází mimo kontrolu a bezpečnostní perimetr banky, jedno z opatření stále zůstává pod její kontrolou – autentizace k portálu či poskytované službě. Vhodným výběrem autentizačních metod a zahrnutím bezpečnostních opatření do procesu ověřování identity uživatele je tak možné riziko zneužití přihlašovacích údajů minimalizovat.

3 Zranitelnosti aktuálně využívaných autentizačních metod

Dnes využívané autentizační metody zvyšují náklady a snižují uživatelský komfort, často však neposkytují požadovanou míru bezpečnosti. Jak plyne z předchozích odstavců, nejčastější hrozby, které v současné době cílí na uživatele internetového bankovnictví, jsou:

- Sociální inženýrství (krádež přístupových údajů).
- Man in the Mobile (zachytávaní autorizačních SMS).
- Man in the Browser (modifikace legitimních webových stránek elektronického bankovnictví).

Autentizační metody, které dnes běžně využíváme, jsou vůči těmto útokům zranitelné, jak shrnuje následující tabulka.

Autentizační metoda	**Zranitelnost**
Jméno, heslo	Sociální inženýrství, MitB
Knowledge based authentication (personifikované otázky)	Sociální inženýrství, MitB
Virtuální klávesnice	MitB
OTP tokeny	Sociální inženýrství
Autorizační SMS	MitMo, Sociální inženýrství

Tabulka 1: Zranitelnosti využívaných autentizačních metod.

4 A co na to uživatel?

Komfortní a jednoduchý přístup ke službám představuje důležitý aspekt při návrhu a výběru autentizačních a autorizačních mechanismů. Banky totiž kromě uložení a správy finančních prostředků nabízí klientům celou škálu služeb od investičních a spořících produktů, kreditních karet a krátko či dlouhodobých úvěrů a jednoduché zřizování a přístup k těmto službám je pro ně prioritou.

Analýza využití více faktorové autentizace v prostředí online bankovnictví [3] ukazuje, že autentizační metody často ovlivňují způsob, jakým, kdy a kde uživatelé využívají online bankovnictví – zejména když si musí pamatovat velké množství různých autentizačních metod, či mít u sebe hardwarový token. Spokojenost uživatelů klesá s rostoucím počtem kroků autentizačního procesu a s nutností využívaní hardwarových tokenů. Naopak, využití mobilních zařízení jako autentizačních prostředků (ať již pro zasílání autorizačních SMS či využití mobilní aplikace) je uživateli obecně vnímáno pozitivně.

Situace se komplikuje u úkonů, které vyžadují podpis papírového dokumentu a osobní návštěvu banky, čímž se ještě více zpomaluje vyřizování uživatelských požadavků. Zřizování nových služeb je administrativně náročné a odrazuje nemálo uživatelů.

5 Regulace

Proces autentizace k bankovním službám je navíc silně ovlivňován regulatorními požadavky, jako jsou např. Obecné pokyny k bezpečnosti internetových plateb[5] vydané Evropským orgánem pro bankovnictví, či nová směrnice o platebních službách na vnitřním trhu (PSD2), která vstoupila v platnost v lednu 2016 s účinností od ledna 2018. Související technické normy, včetně normy definující požadavky na silné ověření klienta, jsou teprve v přípravě, nicméně již dnes víme, že PSD2 vyžaduje *„při iniciaci elektronické platební transakce silné ověření klienta, jež zahrnuje prvky dynamicky propojující transakci s konkrétní částkou a konkrétním příjemcem.“* [6]

6 Jak by to mohlo fungovat?

Jak plyne z předchozích kapitol, při návrhu a výběru autentizačního řešení je nutné zohlednit nejen bezpečnost a robustnost celého řešení a soulad s regulatorními požadavky, ale i uživatelskou přívětivost a následnou jednoduchou dostupnost služeb, kterým proces autentizace předchází.

Zcela novou příležitostí pro finanční instituce pak bude využití možností, které skýtá již platné nařízení Evropského parlamentu a rady č. 910/2014 – eIDAS [4]. To definuje pravidla pro vznik elektronických identit subjektů, které lze následně využít s definovanou mírou záruky jako spolehlivou elektronickou identifikaci napříč EU a to i pro online bankovnictví a další finanční služby. eIDAS dále zrovnoprávňuje elektronické dokumenty podepsané kvalifikovaným elektronickým podpisem s vlastnoručně podepsanými listinnými dokumenty. Nařízení je závazné pouze pro státní správu, nicméně mohou z něj těžit i subjekty z komerční sféry – eIDAS umožní poskytování všech služeb zákazníkům bez nutnosti návštěvy klasické kamenné pobočky, veškeré potřebné dokumenty totiž zákazník bude moci vyřídit elektronicky.

7 Koncept vícevrstvé autentizace

Koncept vícevrstvé autentizace vychází z potřeby silné autentizace, která odpovídá regulatorním požadavkům kladeným na poskytovatele finančních služeb, a zároveň reaguje na hrozby, které jsou zaměřeny na koncové uživatele těchto služeb. Základní myšlenkou je autentizovat nejenom uživatele, ale ověřit i způsob jakým k službám přistupuje včetně aplikace, a to v následujících 4 krocích.

7.1 Autentizace uživatele

Autentizace uživatele může probíhat klasicky jménem a heslem vůči internímu autentizačnímu serveru. Online služby dnes ale přináší federované identity, kdy se uživatel autentizuje jednou u tzv. Identity providera, a ten pak předává už ověřenou identitu tzv. Service providerům. Dnes se v roli Identity providerů často objevují i sociální sítě. Tento přístup může mít pozitivní přínosy i v oblasti finančních služeb, zejména pro nabídku produktů na míru konkrétnímu uživateli.

Další příležitosti v oblasti federovaných identit přinese eIDAS a chystané národní elektronické identity. S nimi bude možné pracovat technicky stejně, jako pracujeme s federovanými identitami již dnes, avšak navíc bude garantována úroveň důvěry v takovou identitu. Uživatele tak bude možné důvěryhodně ověřit bez nutnosti fyzické návštěvy banky i při sjednávání nových produktů a podepisování smluv, a vše tak vyřídit online.

Pro snížení rizika podvodného přístupu můžeme v tomto kroku zahrnout i analýzu chování uživatele zachycující např. v jaké denní době obvykle přistupuje k službám a jak často.

7.2 Autentizace zařízení

V dalším kroku je nutné ověřit, zda zařízení, z kterého uživatel přistupuje, je důvěryhodné a jestli z něj již uživatel v minulosti přistupoval. Pozornost věnujeme např. softwarovému vybavení a jeho konzistenci – zda odpovídají jazykové mutace OS a aplikací, nebo zda odpovídají desktopové/mobilní verze OS a prohlížeče apod. Dále můžeme zkoumat, zda se nejedná o jedno zařízení, které je využívané pro přístup z mnoha různých účtů v krátké době apod.

7.3 Autentizace přístupového kanálu

Neméně důležitá je znalost místa, odkud uživatel přistupuje, zda se jedná o stále stejnou lokalitu, či mezi přístupy z různých lokalit měl uživatel dostatečný čas na přesun. Dnes je technologicky možné ověřit informaci o lokalitě např. využitím informací jako je ISP, IP adresy či Wi-Fi sítí, u mobilních zařízení dále můžeme využít polohu z GPS. Dále je možné měřit dobu od zaslání požadavku na klientské zařízení po vrácení odpovědi (a zda tato doba odpovídá deklarované lokalitě uživatele), a zjišťovat Proxy či VPN tunely po cestě, za kterými by se případný útočník mohl maskovat.

7.4 Autentizace bankovní aplikace

Na závěr autentizačního procesu musíme ověřit, že uživatel přistupuje k originální, legitimní a nemodifikované bankovní aplikaci – webovému portálu. Dnes již existují technologie, které umožňují na základě otisků originálního webového portálu, porovnat originální aplikaci s tou, která je zobrazena uživateli a odhalit tak útoky typu MitB. Technologie by měla fungovat na bázi whitelistu – originální podoba webového portálu je známá, čímž umožní detekovat i tzv. zero-day hrozby a malware, pro který ještě nebyly vytvořeny signatury.

Celý proces vícevrstvé autentizace je technicky možné realizovat již dnes, kombinací technologií jako jsou autentizační servery a systémy threat detekce/prevence a to jak pro webový přístup z pracovní stanice či mobilního zařízení, tak pro přístup z mobilní e-bankingové aplikace.

Vícevrstvý přístup k autentizaci navíc umožňuje zavést tzv. adaptivní autentizaci, kdy při malém riziku (přístup ze známého zařízení a známé lokality) bude stačit, když se uživatel autentizuje jménem a heslem, při středním riziku (neznámé zařízení či neznámá lokalita) bude vyžadována dodatečná autentizace (např. ve formě mobilního tokenu) a při vysokém riziku (detekován malware) může být transakce zamítnuta.

8 Autorizace bankovní transakce…

Po úspěšné autentizaci uživatele můžeme pokračovat autorizací samotné transakce. Vhodným prostředkem pro autorizaci pak může být mobilní zařízení – potažmo speciální mobilní aplikace. Mobilní zařízení jsou uživateli jako autentizační/autorizační prostředek vnímaná obecně pozitivně, protože uživatelé jsou na mobilní telefony zvyklí, mají neustále u sebe, a nejsou tak limitováni odkud a kdy mohou transakce provádět.

Řešení, které splňuje jak požadavky na jednoduchost a uživatelskou přívětivost, tak i požadavky na bezpečnost, kombinuje speciální mobilní aplikaci, sloužící jako token, s technologií PUSH notifikací, která umožní uživatele automaticky notifikovat o transakci (transakcích) čekajících na jeho schválení.

Obrázek 2: Princip autorizace transakcí s využitím technologie PUSH notifikací.

Proces autorizace transakce pak probíhá v následujících krocích:

- Uživatel v online bankovnictví iniciuje transakci.
- Na mobilním zařízení je automaticky vyvolaná aplikace sloužící jako token, která zobrazí informace o transakci čekající na schválení.
- Uživatel v mobilní aplikaci transakci potvrdí nebo zamítne. Pro potvrzení transakce může být ještě vyžadovaná na mobilním zařízení dodatečná autentizace uživatele (např. otiskem prstu, či zadáním PINu).

Technicky pak může být samotná autorizace zajištěna různými způsoby na bázi symetrické (HMAC) či asymetrické (PKI a elektronický podpis) kryptografie.

Tento přístup minimalizuje rizika v procesu autentizace a snižuje pravděpodobnost typických útoků na internetové bankovnictví:

- Minimalizujeme riziko sociálního inženýrství, protože požadavek na autorizaci dokumentu/transakce je na mobilní zařízení zasílán ve formě push notifikace, s využitím cloudové infrastruktury výrobce zařízení či operačního systému, a po potvrzení uživatelem obstarává veškerou komunikaci s backendem mobilní aplikace. Uživatel přímo nikam nezadává jednorázové kódy, či kódy na bázi challenge-response, které by se mohl útočník snažit zjistit.
- Riziko útoku MitB je primárně minimalizováno opatřením vícevrstvé autentizace, zejména krokem autentizace aplikace, kdy je ověřeno, že uživateli je zobrazována původní a originální podoba stránky bez neautorizovaných zásahů z vnějšku.

- Pokud by se útočníkovi přesto povedlo útok MitB provést, minimalizujeme i riziko útoku MitMo. Pro útočníka je snadné odchytávat autorizační SMS (jak již bylo zmíněno, např. u Androidu existuje veřejné API pro přístup k SMS), avšak u mobilních operačních systémů, které jsou dnes běžně využívané je uplatňován princip sandboxingu – tudíž aplikace standardně nemohou přistupovat k datům jiné aplikace. Útočník by musel najít další zranitelnost systému, aby získal systémový či root přístup, který by mu dovolil přistupovat k datům aplikací, čímž se útok komplikuje. Aplikace dále může obsahovat seznam důvěryhodných serverů, se kterými má komunikovat. Server rovněž může vyžadovat autentizaci mobilní aplikace.
- Uživateli jsou v aplikaci zobrazeny veškeré detaily o autorizované transakci, snižujeme tak riziko různých útoků typu Man in the Middle – uživatel přesně ví, co schvaluje.

9 … a podpis elektronických dokumentů

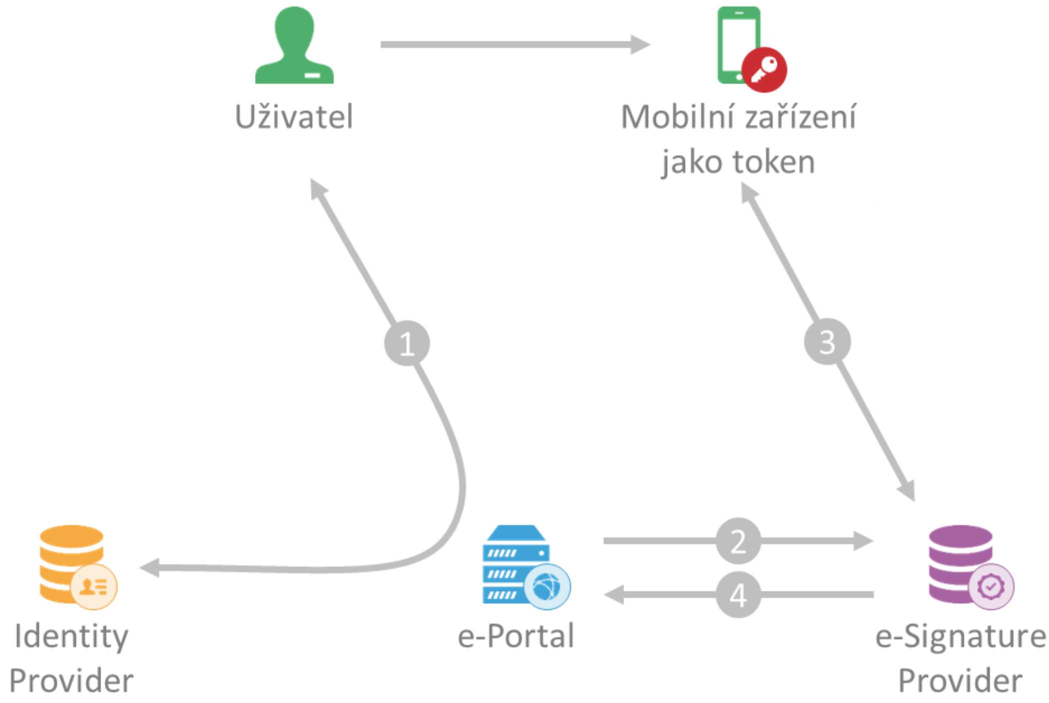
Pokud jako autorizační metodu využijeme elektronický podpis založený na certifikátech, můžeme kromě autorizací transakcí stejným způsobem umožnit i podpis dokumentů, a zjednodušit stávajícím zákazníkům přístup k novým bankovním produktům či rozšíření stávajících služeb. Tento přístup má podporu i v nařízení eIDAS[4], které ve svém článku 25 říká, že *„elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy,“* navíc se dá s vysokou mírou pravděpodobnosti předpokládat, že takový postup bude i v souladu s PSD2 a odpovídajícími připravovanými technickými normami.

9.1 Podpis v mobilním zařízení

Při registraci je přímo v mobilní aplikaci vygenerovaná dvojice klíčů (soukromý a veřejný) a interní certifikační autoritou vydán odpovídající certifikát, který je uložen do registrovaného zařízení. Soukromý klíč je pak neexportovatelný z mobilního zařízení – což je technicky zajištěno prostředky konkrétního mobilního operačního systému.

Samotný proces autorizace je zobrazený na obrázku níže a probíhá následujícím způsobem:

1. Uživatel je autentizován (vůči externímu či internímu Identity Provideru) na portálu e-bankovnictví.
2. Po zadání požadavku na podpis dokumentu portál iniciuje požadavek na podpis, který zajišťuje e-Signature provider.
3. e-Signature provider odešle požadavek na podpis (ve formě otisku dokumentu a odkazu na dokument, příp. dalších metadat) na registrované zařízení (pomocí tzv. push notifikace), uživatel dokument autorizuje, a povolí použití soukromého klíče uloženého v mobilním zařízení pro vytvoření podpisu (zadáním PINu, či otisku prstu).
4. e-Signature provider zkompletuje dokument a vrátí výsledek bankovnímu portálu.



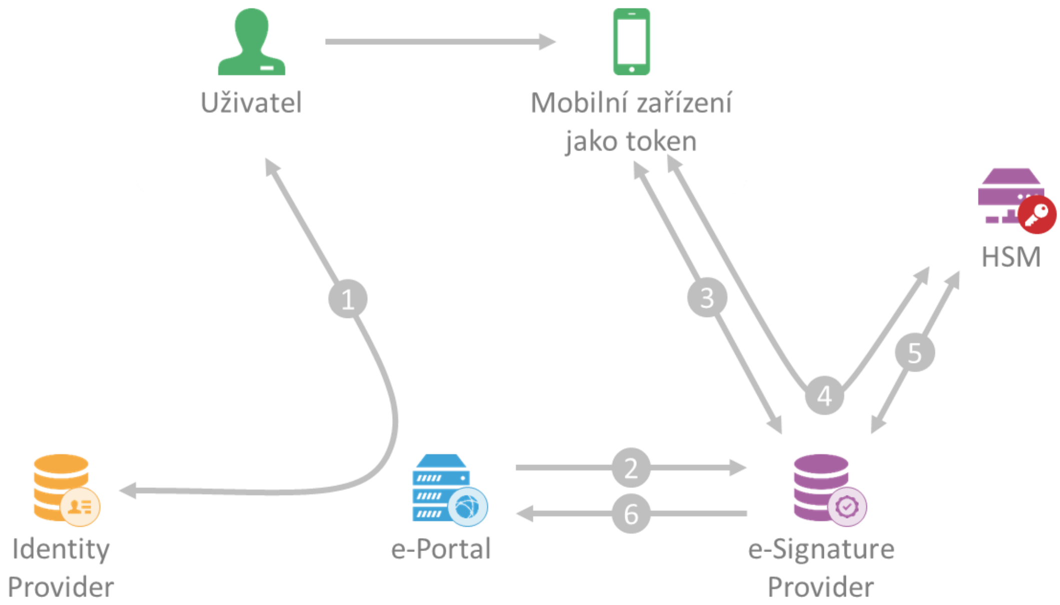
Obrázek 3: Podpis dokumentu – klíče uložené v mobilním zařízení.

9.2 Koncept vzdáleného podepisování

Nařízení eIDAS přináší koncept vzdáleného podpisu, který umožňuje ponechat správu a bezpečné uložení klíčů na poskytovateli služeb. V tomto případě nejsou klíče uloženy přímo v mobilním zařízení, ale v HSM modulu v zabezpečené infrastruktuře banky, a mobilní zařízení (potažmo mobilní aplikace) plní pouze funkci silné autentizace klienta – klient prostřednictvím aplikace svolí k užití PKI klíčů pro podpis konkrétního dokumentu či transakce.

Celý proces je ilustrován na obrázku níže a probíhá následovně:

1. Uživatel je autentizován (vůči externímu či internímu Identity Provideru) na portálu e-bankovnictví.
2. Po zadání požadavku na podpis dokumentu portál iniciuje požadavek na podpis, který zajišťuje e-Signature provider.
3. Následně e-Signature provider odešle požadavek na podpis dokumentu na registrované zařízení (využije se push notifikace).
4. Uživatel na mobilním zařízení autorizuje transakci, čímž povolí e-Signature provideru použití soukromého klíče uloženého v HSM pro podpis.
5. Samotný podpis je bezpečně vygenerován v HSM modulu.
6. e-Signature provider zkompletuje dokument a vrátí výsledek portálu.



Obrázek 4: Podpis dokumentu – klíče uloženy v HSM v infrastruktuře banky,
mobilní zařízení jako autentizační prostředek.

10 eIDAS v praxi? – projekt STORK

Jednou z deseti priorit Evropské komise je vytvoření jednotného digitálního trhu napříč Evropou a překonání existujících bariér v oblasti online služeb [7]. To se dotýká i finančních služeb, které mohou využít nařízení eIDAS pro zkvalitnění a zefektivnění finančních služeb a vytvoření plně bezpapírového „virtuálního“ bankovnictví bez hranic. Jak by to mohlo fungovat v praxi, ukázal jeden z pilotů v rámci projektu STORK 2.0, zaměřený na elektronické bankovnictví, který proběhl v roce 2015 [8]. V rámci pilotního provozu byly předvedeny tři scénáře užití, které mohou zjednodušit proces oslovování a získávání nových zákazníků:

- Založení bankovního účtu – občané zemí zapojených do projektu, kterým bylo vydáno eID a odpovídající certifikát, mohli zažádat o otevření zahraničního bankovního účtu bez nutnosti osobní návštěvy banky či nutnosti vyplňovaní papírových formulářů. Uživatel jednoduše vyplnil online formulář a podepsal jej svým kvalifikovaným certifikátem.
- Přihlášení k e-bankingu – při využití eID může banka důvěryhodně ověřit jakoukoliv fyzickou či právnickou osobu z jakékoliv země EU přistupující k službám elektronického bankovnictví.
- E-invoicing demonstroval ukázku elektronického doporučeného doručování, které umožní ověřit autenticitu dokumentů předávaných mezi společnostmi, s cílem zvýšit důvěryhodnost procesu elektronické fakturace.

Ukazuje se, že eID a kvalifikované certifikáty se mohou uplatnit zejména v případech, kdy byla dříve nutná osobní návštěva klasické kamenné pobočky – při sjednávání nových produktů a smluv, čímž zjednoduší a zefektivní proces oslovování nových zákazníků. Autentizace stávajících klientů a autorizace běžných transakcí stávajících zákazníků zůstane nejspíš i nadále plně v režii banky.

11 Závěr

Způsob poskytování služeb, finanční služby nevyjímaje, se v poslední době mění a elektronizuje. Uživatelé vyžadují komfortní a jednoduchý přístup s maximální mírou mobility. Situaci ale komplikuje nárůst sofistikovaných útoků a pokročilého malware, cíleného na koncové uživatele a jejich zařízení, která se nacházejí mimo bezpečnostní perimetr a kontrolu banky.

Zajištění požadované úrovně bezpečnosti v této situaci nabízí koncept vícevrstvé adaptivní autentizace, kdy je postupně autentizován uživatel, jeho zařízení, kanál, kterým přistupuje, vlastní aplikace a nakonec i zadávaná transakce. Řešení vyžaduje dodatečné uživatelské akce (tzv. „step-up“ autentizace) pouze v případě, kdy jsou zjištěny odchylky od běžného chování jako je např. pokus o přihlášení z nového zařízení, v neobvyklou dobu, z jiné země apod. Pro samotnou autorizaci transakce je pak využito mobilního zařízení jako tokenu, tak aby bylo možné minimalizovat rizika nejběžnějších útoků cílených na klienty elektronického bankovnictví – sociální inženýrství, a malware využívající technik Man in the Browser a Man in the Mobile, zároveň ale zachovává uživatelský komfort. Řešení umožňuje nejenom autorizaci transakcí, ale i autorizaci/podpis dokumentů, čímž umožní jednoduché online sjednávání nových služeb.

Koncept respektuje aktuálně platné regulatorní předpisy ovlivňující finanční sektor a využívá nových příležitostí, které přináší eIDAS – poskytování služeb zákazníkům moderně, bezpapírově a bez hranic napříč celým evropským digitálním trhem.

Reference

[1] ADYEN MOBILE PAYMENT INDEX, dostupné online: https://www.adyen.com/home/business-intelligence/mobile-payments-index.

[2] Augusto Paes de Barros: *O futuro dos Backdoors – O pior dos mundos,* CONGRESSO DE SEGURANÇA DA INFORMAÇÃO 2005, dostupné online: https://web.archive.org/web/20110706153819/http://www.paesdebarros.com.br/backdoors.pdf.

[3] Kat Krol, Eleni Phillipou, Emiliano De Cristofaro, M. Angela Sasse: *"They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking,* NDSS Workshop on Usable Security (USEC 2015), dostupné online: http://arxiv.org/pdf/1501.04434v1.pdf.

[4] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, dostupné online: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014R0910&from=EN.

[5] Obecné pokyny k bezpečnosti internetových plateb, dostupné online: https://www.eba.europa.eu/documents/10180/1004450/EBA_2015_CS%20Guidelines%20on%20Internet%20Payments.pdf/a2305991-71b2-4411-9f1c-ebd31129ad8f.

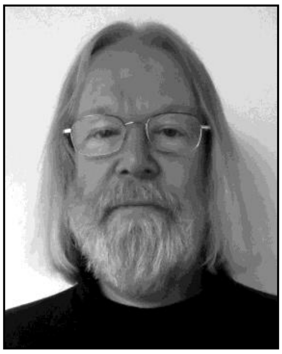
[6] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Text s významem pro EHP), dostupné online: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32015L2366&from=EN.

[7] European Commission Priorities: Digital Single Market, Bringing down barriers to unlock online opportunities, dostupné online: http://ec.europa.eu/priorities/digital-single-market_en.

[8] STORK 2.0 – Secure Identity across borders linked 2.0, eBanking Pilot, dostupné online: https://www.eid-stork2.eu/pilots/ebanking/index.php/en/.

Measuring and Studying Cybercrime
Měření a studium kyberzločinu

Richard Clayton



Richard Clayton
richard.clayton@cl.cam.ac.uk

Richard Clayton is the Director of the Cambridge Cloud Cybercrime Centre. The Centre intends to build one of the largest and most diverse data sets about cybercrime that any organisation holds and more importantly aims to make this data available to other academics for them to apply their own skills to address cybercrime issues. Academics currently face considerable difficulties in researching cybercrime and the centre intends to drive a step change in the amount of cybercrime research by making datasets available, not just of URLs but content as well, so that other academics can concentrate on their particular areas of expertise and start being productive immediately.

Richard Clayton je ředitelem Cambridge Cloud Cybercrime Centre. Toto centrum cílí na vybudování jednoho z největších a nejrozmanitějších souborů dat o kyberzločinu, jaký kdy nějaká organizace měla a především na to, aby tato data byla dostupná dalším akademikům pro aplikaci dovedností při řešení problému kyberzločinu. Nyní mají akademici při zkoumání kyberzločinu obtížnou situaci a centrum v Cambridge chce udělat zásadní krok ke změně v tom, aby rozsáhlá data o kyberzločinu byla přístupná jako plnohodnotné soubory dat, nikoliv jen jako URL, ale s plným obsahem tak, aby se další akademici mohli soustředit na své znalostní domény a jejich výzkumná produktivita se rozběhla rychleji.

Measuring and Studying Cybercrime

Lord Kelvin famously suggested that if you were unable to measure something then your knowledge would be “meagre and unsatisfactory” and studying it would not be “science”. That’s clearly where cybercrime research is today. I’ll explore what we currently know, the challenges in getting any plausible measurements, and how a new initiative at Cambridge may get more researchers into the field.

Měření a studium kyberzločinu

Lord Kelvin byl názoru, že pokud nejste schopni něco změřit, pak vaše znalost tohoto fenoménu je „mizerná a nedostačující“ a jeho studium by nebylo „vědou“. A toto je přesně bod, kde jsme dnes s výzkumem kyberzločinu. Budu se věnovat ve své přednášce tomu, abych popsal dnešní stav věci, výzvy vize získávání nějakých smysluplných měření a také naši novou iniciativu v Cambridge, která by mohla k této oblasti přilákat další výzkumníky.

1 Introduction

I have been studying cybercrime for several decades, initially looking at email spam, then with my long-term collaborator Tyler Moore, writing a series of papers on phishing (email enticements to visit fake websites and disclose credentials). Most recently I have been looking at IP prefix hijacking by email spammers and DDoS (Distributed Denial of Service), particularly the use of UDP reflection.

In this paper I discuss the difficulties faced by those who wish to study cybercrime by collecting data and making measurements. There are other approaches to the study of cybercrime and you will find my name on qualitative work [1] as well as on the many quantitative studies I discuss below. However, if one wants to view what we are doing as a science that is on a par with Physics or Chemistry then we need to consider how we are going to measure what is going on.

> In physical science a first essential step in the direction of learning any subject is to find principles of numerical reckoning and methods for practicably measuring some quality connected with it. I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of *science*, whatever the matter may be.
>
> *William Thompson (Lord Kelvin)* [9]

I start by discussing some phishing research that Tyler Moore and I did in 2007/8 and discuss the difficulties this illustrates about performing research into cybercrime with accurate reproducible measurements. I then discuss a new data sharing initiative at the University of Cambridge which is intended to address these issues and drive a step change in the level of cybercrime measurement research.

2 Phishing Research

In 2007 Tyler Moore and I started our research into phishing. In the first paper we published [2], our main innovation was to measure phishing website lifetimes, so we built an infrastructure to visit dubious URLs every 30 minutes in order to determine if they were still hosting a phishing website or whether the fraudulent pages had been "taken down".

We were lucky, in that just as we started our measurements, some of the criminals (the "rock-phish gang") started to use an innovative "fast flux" technique. The hostnames within their URLs resolved to the IP addresses of compromised end-user machines which were operating HTTP relay software. The relays connected to a hidden "mother ship" which actually hosted the phishing websites. Every few minutes the DNS would be changed so that a different group of relays were used. The only viable defence was to take-down the domain name rather than the relays or the (hard to locate) mother ship.

Our measurements of take-down times showed the impact of the rock-phish gang's innovations, which were causing websites to remain available for significantly longer periods. This led to considerable interest in our work by the companies in the front-line of taking-down phishing websites.

After seeing a presentation of our results we were approached by a number of practitioners who told us that our average measurements for take-down times were too high. They told us that, in their experience, removal was complete within hours rather than days. We explained about the impact on the statistical mean of the “long tails” we were seeing – and they suggested that we repeat our measurements with more complete datasets and arranged to provide us with the datasets that they were processing.

So we carried on with our research, using feeds of phishing URLs from a number of companies until one day Tyler Moore came to me and explained that he had worked out why there was a disparity between our measurements and the experience of the take-down companies.

Each of the companies collated data about every possible phishing website, no matter which brand was being targeted, but would only take-down the websites for the brands that were employing them. However, they would pass the complete list of the URLs they had found to us, as neutral academics, whilst failing to pass the information to their competitors. Hence, if a company found a website for a brand that would not pay them to do a “take-down” they would do nothing – but we would start to measure the website lifetime from that point. Only when a company that was acting for the brand-owner became aware of the website would take-down activity commence.

This lack of information sharing was why our observations had been different from those of the industry professionals. We were able to publish another paper [5] that showed that when brands were aware of phishing websites they were taken down, on average, within four hours. If the brand was unaware it took around four days!

3 The Problems Facing Cybercrime Researchers

The research I’ve just described on phishing serves to illustrate many of the difficulties facing cybercrime researchers:

- Datasets are bigger than you think: we initially found it somewhat of a struggle to handle just a few thousand phishing URLs;
- Datasets contain many errors: many sites that were said to be phish were false positives and had to be weeded out to avoid distorting our results;
- Datasets are biased: as has just been explained, combining feeds gave us more information than anyone else, but what we were measuring was the effectiveness of others acting on what they knew;
- Datasets are often proprietary: I am not permitted to pass on copies of the data (from any of our phishing studies) for others to combine with their data, for them to repeat the work – or even to check if we added it up right!

I’ll now discuss these issues in more detail.

3.1 Real datasets are bigger than you expect!

At present a phishing URL feed contains at least 750,000 unique URLs every year. This figure can be easily exceeded as some feeds are considerably inflated – a great many URLs in the feed can be, fairly readily, seen to be going to lead to exactly the same webpage.

To avoid being caught in email spam filters criminals sometimes construct victim specific URLs (usually by varying the parameters, occasional by using wildcard DNS and varying the hostname). Others exploit URL shortening systems, with huge numbers of different URLs leading to a single webpage. Additionally, the companies that compile the feeds check if a website will serve the phishing page independently of the hostname with the URL and then mine passive DNS data to identify every hostname that resolves to the same web server.

With experience irrelevant duplicates can be ignored, but it is still a major undertaking to promptly visit every individual phishing website and record its contents.

Phishing is not unique in providing challenges in coping with data volumes. I track reflective DDoS attacks, seeing up to 75 million events a month and 5000 to 10000 unique victims/day [8]; I tracked a "worm" that spread over Instant Message systems, recording 55 million downloads of the malware and over 3 million victims [7]; and the Conficker dataset now exceeds 40TB.[1]

If you start working with cybercrime datasets without understanding what sort of scale you are dealing with, you'll most likely be swamped and end up with a data processing project rather than a cybercrime project – or you will just process a subset of the data and hope that it is representative of the rest.

3.2 Datasets are biased

One of the early phishing datasets that Tyler Moore and I worked with was a a mixture of public data and data from just one particular take-down company [3]. In our paper we presented a graphic that showed the different take-down times we had measured for various different banks. We later realised that many of these differences arose from the lack of data sharing: where the company acted for a particular bank and was also the sole source of the URL we'd expect to measure a faster take-down for that URL than the general case. Therefore, the shorter average take-down times on our graph were generally for banks that were clients of the company who had given us their data. The company was unconcerned about the bias – and used our graphic in their promotional material for several years, since it apparently showed that their clients could expect better take-down times than average.

Many phishing papers only use data from PhishTank[2] because it is the largest public source of phishing URLs. However, Tyler Moore and I measured its coverage on several occasions and found that for various periods (and compared to various other sources) it contained 73% ([4]), 35% ([5]) and 48% ([6]) of all phishing URLs. Nevertheless, because of the data sharing policies of PayPal and eBay, it invariably holds almost 100% of URLs for phishing sites that attack these two brands. Unless you know this bias is present you might reach erroneous conclusions when measuring who is most likely to be phished.

There is a similar bias in the analysis of reports made to the FBI's Internet Crime Complaint Center (IC3)[3] – if you encounter fraud on the eBay auction website then you are very likely to be encouraged, especially if eBay cannot solve the problem, to make a report to IC3. This is capable of skewing their data to overemphasise auction fraud.

Bias can be dealt with if it can be modelled and thereby allowed for, but this is not always possible. I've looked at datasets of many thousands of compromised websites that were being used for relays by a spammer who was promoting work-from-home schemes. Potentially such a dataset tells us something about how websites are compromised – but if they were all compromised by a single spammer (or they bought a list of compromised sites from a small number of vendors who themselves did the compromise) then I would be studying a very small number of actors and my results could well be completely unrepresentative.

3.3 Datasets are proprietary

In order to obtain datasets it is usual to sign an NDA (non-disclosure agreement). This precludes sharing datasets with other academics so that they can reproduce or extend our work. We did our

---

[1] http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
[2] http://www.phishtank.org/
[3] http://www.ic3.gov/default.aspx

best in all of our papers to describe the nature of our datasets, so a savvy reviewer could have rejected our first paper by pointing out the biases, but at that time no-one knew any better.

In theory other academics could approach the people I signed NDAs with and sign their own so that I could share the data – but in one case I'm not even allowed to say who I signed an NDA with!

What this means in practice is that it is perfectly possible to work with cybercrime datasets provided you put in the time and effort to build the relationships and trust so that data holders will be persuaded to share. But these are individual efforts and without these relationships whole areas of cybercrime research are closed to you.

4 Encouraging Research to Measure Cybercrime

My research is not unique in that almost no academic work on cybercrime can be reproduced by other people, so can we really call this a "science"? My colleagues who work on operating systems and computer architecture say that they have similar experiences and there are now initiatives to address these issues: keeping copies of virtual machine images, carefully recording exact details of system components, preserving all aspects of a development toolchain and of course making everything "open data".

There are very few undergraduate projects or MSc theses that tackle cybercrime. If the data is not to hand (and it might take years to build the relationships to collect it) then cybercrime topics look too much like "research", and even PhD candidates should be thinking twice about the difficulties before tackling topics in the measurement of cybercrime.

To summarise the problems you face if you want to improve upon my cybercrime research:

- I am not allowed to give you my data;
- It may take you years to source your own data;
- The data may be at such a scale as to swamp you;
- The data may have biases that you (and I) fail to understand;
- Obtaining the raw data may be only the beginning of your problems because you may have to build a web scrapers, learn how to fetch whois information (running into access limits), avoid refetching the same thing under another name, deal with retaliation from the criminals etc. etc.

Perhaps the easiest research question to tackle is "Why are so few cybercrime measurement papers published"? However, I am working on a new initiative to tackle this issue.

4.1 The Cambridge Cloud Cybercrime Centre

I have five years funding from the EPSRC[4] to develop and run what we are calling the Cambridge Cloud Cybercrime Centre.[5]

We aim to leverage our neutral academic status to obtain significant feeds of cybercrime data and build one of the largest and most diverse datasets that any organisation holds. We will mine and correlate this data to extract information about criminal activity. We will learn more about crime "in the cloud", detect it better and faster and determine what forensics looks like in this space (and

---

[4] The Engineering and Physical Sciences Research Council (EPSRC) is the UK's main agency for funding research in engineering and the physical sciences.
[5] http://www.cambridgecybercrime.uk/

where appropriate work with law enforcement). In short we aim to create a sustainable and internationally competitive centre for academic research into cybercrime.

However, we are going to do something brand new as well.

We are working on renegotiating our existing Non-Disclosure Agreements into "Distribution Agreements". We aim to collect cybercrime data, add value to it, and then make it available to other academics under one (we hope) simple NDA that they will sign with us – in principle you will discover we hold an interesting dataset, sign the paperwork, and be able to start your research, utilising our data, the following morning.

We aim to have a "catalogue" describing cybercrime datasets that can be used by others in their own specialist areas of research without the need to learn all about the web scraping, the whois limits, the duplicated data and so on. We aim to make it easy to set MSc work in this area knowing that it will not take two years to get the data together. We aim to see more *science* by letting people run different techniques on the same data and compare results.

We're going to have a LOT of data – but it will not be "open data": you will need to sign an NDA. The reason for this is that the companies who supply it to us are concerned that it not be available to their competitors and it must not be available to their customers (who have to pay for it). Furthermore, the companies may have specific obligations under privacy policies and may be concerned about the public relations aspects of being linked, even loosely, to ecrime. There are also data protection concerns, albeit very little of the data contains what the Americans call PII (personally identifying information). Finally, and by no means least, if the data were to be "open" the criminals might reverse engineer the sensor architectures that pick out their wickedness and adapt their behaviour accordingly.

5 Conclusions

I have presented an example from my own cybercrime measurement research (phishing website take-down) and explained how the first paper we wrote on this topic failed to appreciate that our data was biased, and showed how we eventually understood that bias.

I then explained how this research topic illustrates some common issues faced by all researchers in this space: Scale, Errors, Bias and Proprietary data. I went on to discuss how a new initiative, the Cambridge Cloud Cybercrime Centre aims to tackle these problems by collating and packaging cybercrime datasets to make it much, much easier for academics to bring their specialist skills to cybercrime research without having to address many of the current difficulties in obtaining data.

We will be working on the datasets that we create at Cambridge as well – we will have world class researchers doing world class research. But I want to enable other people to use our data to do world class research as well. At the end of the first five years I want to be judged not on how many papers we wrote in Cambridge but how many academic papers were written world-wide because our datasets helped to make that research possible.

I also want to see MSc and undergraduate students tackling cybercrime projects and confirming or refuting classic results. Besides improving the science – this is a fascinating area and I want others to experience that too and come and join us. Together I believe that we will find new ways to prevent crime, to detect and deter criminals – and that is a major reason why society funds our work.

Acknowledgements

The author is supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHSS&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific via contract number N66001-13-C-

0131. This paper represents the position of the author and not that of the aforementioned agencies. The Cambridge Cloud Cybercrime Centre is supported by the EPSRC [grant number EP/M020320/1].

References

[1] Hutchings, A., and Clayton, R., and Anderson, R.: Taking down websites to prevent crime. *Eleventh APWG eCrime Researchers Summit (eCrime)*, Toronto, Canada, June 1–3 2016.

[2] Moore, T., and Clayton, R.: An Empirical Analysis of the Current State of Phishing Attack and Defence. *Sixth Annual Workshop on Economics and Information Security (WEIS07)*, Pittsburgh PA, USA, June 7–8 2007.

[3] Moore, T., and Clayton, R.: Examining the Impact of Website Take-Down on Phishing. *Second APWG eCrime Researchers Summit (eCrime)*, Pittsburgh PA, USA, October 4 – 5 2007.

[4] Moore, T., and Clayton, R.: Evaluating the Wisdom of Crowds in Assessing Phishing Websites. In: Gene Tsudik (editor): *Financial Cryptography and Data Security, 12th International Financial Cryptography and Data Security Conference (FC08)*, Cozumel, Mexico, January 28–31 2008, LNCS 5143, pages 16–30, Springer Berlin/Heidelberg.

[5] Moore, T., and Clayton, R.: The Consequence of Non-Cooperation in the Fight Against Phishing. *Third APWG eCrime Researchers Summit (eCrime)*, Atlanta GA, USA, October 15–16 2008.

[6] Moore, T., and Clayton, R.: Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing. In: Roger Dingledine and Philippe Golle (editors*): Financial Cryptography and Data Security, 13th International Financial Cryptography and Data Security Conference (FC09)*, Barbados, February 23–26 2009, LNCS 5628, pp. 256–272, Springer Berlin/Heidelberg.

[7] Moore, T., and Clayton, R.: Which Malware Lures Work Best? Measurements from a Large Instant Messaging Worm. *Tenth APWG eCrime Researchers Summit (eCrime)*, Barcelona, Spain, May 25–29 2015.

[8] Thomas, D.R., and Clayton, R., and Beresford, A.R.: *Analysing UDP Reflection DDoS Attacks*, in preparation.

[9] Thomson, W.: *Popular Lectures and Addresses*, Vol. 1, Constitution of Matter, 1889, page 72, McMillan & Co, London and New York.

The biggest threat for citizen´s privacy
Najväčšia hrozba pre digitálne súkromie občanov

Pavol Lupták

Pavol Lupták
pavol.luptak@nethemba.com

Pavol Lupták is CEO, Certified IT Security Professional. He gained his BSc. at the FEI-STU in Bratislava and MSc in Computer Science at the Czech Technical University with master thesis focused on ultra-secure systems. He holds many prestigious security certifications including CISSP and CEH, he is Slovak OWASP chapter leader, co-founder of Progressbar and SOIT organizations where he is responsible for IT security. Pavol uses to have regular presentations at various worldwide security conferences (in Netherlands, Luxembourg, Berlin, Warsaw, Krakow, Prague). In the past, he demonstrated vulnerabilities in the public transport SMS tickets in all major cities in Europe, together with his colleague Norbert Szetei he practically demonstrated vulnerabilities in Mifare Classic RFID cards. He has 14 years experience in IT security, penetration testing and security auditing including social engineering and digital forensic analysis. He is co-author of the OWASP Testing Guide v3, has a deep knowledge of the OSSTMM, ISO17799/27001 and many years experience in seeking vulnerabilities. He has a knowledge of many programming languages (ASM, C, C++, XSLT, Perl, Java, PLSQL, Lisp, Prolog, scripting languages) and operating systems. He is also focused on VoIP and interesting IT security research.

Pavol Lupták je výkonný ředitel, certifikovaný bezpečnostní specialista. Vystudoval FEI-STU v Bratislavě a FEL-ČVUT v Praze obor informatika s diplomovou prací zaměřenou na ultra-bezpečné systémy. Je držitelem prestižních bezpečnostních certifikací CISSP a CEH, vede slovenskou OWASP pobočku. Je také spoluzakladatelem organizací Progressbar a SOIT, kde vede sekci pro IT bezpečnost. Pavel má pravidelné prezentace na různých světových bezpečnostních konferencích (Nizozemsku, Lucembursku, Berlíně, Varšavě, Krakově, Praze). V minulosti demonstroval možnost zneužití SMS jízdenek ve všech velkých městech Evropy, spolu s kolegou Norbertem Szeteiom demonstroval masivní prolomení čipových karet Mifare Classic. Má čtrnáctileté zkušenosti v oblasti IT bezpečnosti a penetračního testování a tvorby nejrůznějších bezpečnostních auditů včetně sociálního inženýrství či forenzní analýzy. Je spoluautor testovací příručky OWASP Testing Guide v3, detailně ovládá OSSTMM, ISO17799/27001, má dlouholeté zkušenosti s manuálním vyhledáváním zranitelností a různými bezpečnostními nástroji. Ovládá množství programovacích jazyků (ASM, C, C++, XSLT, Perl, Java, PLSQL, Lisp, Prolog, skriptovací jazyky) a operačních systémů, věnuje se také VoIP a zajímavému výzkumu v oblasti IT bezpečnosti.

The biggest threat for citizen’s privacy

Celine’s first law: National Security is the chief cause of national insecurity. Slovak Information Service (SIS) repeatedly has proposed the draft for interception of an encrypted communication – the duty to give off the encryption keys for the given non-specified devices. Leaked information from Wikileaks has shown Slovak and Czech’s government considered to buy or bought the spying malware from Gamma group and Hacking Team – both companies with the bad reputation because of selling the same spying malware to the dictatorship countries for spying of innocent people. The Slovak government has rejected this information, Czech Secret Police has confirmed this fact and see no problem in doing the business with dictatorship supporting company because they use this software for “legal reasons”. The new Slovak legislation legitimizes the use of spying software for the particular government agencies and strongly criminalized use by others that may lead to the criminalization of legal business activities of IT security companies. The goal of this presentation is to show why it is immoral to buy and use spying malware from dictatorship supporting companies. Why whistleblowing remains the only way to find out the unethical behavior of secret government agencies and why all government´s tries to regulate cryptographic systems drastically degrade our digital privacy. And therefore, why the government is the biggest privacy threat for their citizens.

Najväčšia hrozba pre digitálne súkromie občanov

Slovenská Informačná Služba (SIS) opakovane podala návrh na odpočúvanie šifrovanej komunikácie – povinnost odovzdávať šifrovacie kľúče pre nešpecifikovaný okruh zariadení. Uniknuté informácie z Wikileaks poukazujú na to, že Slovenská a Česká vláda uvažovala nakúpiť alebo nakúpila špehovací malware od Gamma group a Hacking Team – obe spoločností so zlou reputáciou, ktorú získali vďaka predaju tohoto malwareu diktátorským vládam na špehovanie nevinných ľudí. Slovenská vláda poprela túto informáciu, Česká tajná polícia ju potvrdila a nevidí žiadný problém v spolupráci so spoločnosťou, ktorá podporuje diktátorské režimy, kedže tento softwér používa na „legálne účely“. Nová slovenská legislatíva legitimizuje používanie špehovacieho softwaru pár vyvolenými vládnymi agentúrami a kriminalizuje toto použitie inými osobami a spoločnosťami, čo môže viesť ku kriminalizácii legálnych biznis aktivit IT bezpečnostných firiem. Cieľom prezentácie je ukázať prečo je nemorálne kupovať a používať špehovací malware od spoločností, ktoré podporujú diktátorské režimy. Prečo je whistleblowing jediný spôsob na odhalenie neetického správania tajných vládných agentúr a prečo akékoľvek pokusy vlád regulovať kryptografiu, drasticky degradujú naše digitálne súkromie. A teda, prečo vlády predstavujú najväčšiu hrozbu pre digitálne súkromie ich občanov.

1 Celine's First Law: National Security is the chief cause of national insecurity

V roku 1995 bolo identifikovaných 174 000 neoficiálnych Stasi informátorov, čo bolo takmer 2,5 % populácie z celého Východného Nemecka vo veku 18 až 60 rokov. Podľa materiálu, ktorý bol zničený počas posledných dní socialistického režimu vo Východnom Nemecku, úrad na správu Stasi záznamov (Bstu) odhadoval, že počas režimu mohlo aktívne pôsobiť až 500 000 Stasi informátorov, pričom ich celkové množstvo (vrátane takých, ktorí informovali len príležitostne) bolo až 2 milióny (!)

Paranoia zo všade nainfiltrovaných agentov tajných služieb Stasi, ktorých pôvodným zámerom bolo „zabezpečovať ochranu štátu“ mala na bezpečnosť štátu úplne opačný efekt – nikto nikomu v štáte neveril a každý sa cítil ohrozený.

Zámer zabezpečovať ochranu štátu je úloha každej štátnej informačnej služby – v našich krajinách Slovenská informačná Služba (ďalej SIS) a česká Bezpečnostní Informační Služba (ďaľej BIS).

Pozrime sa ako štátne informačné agentúry a tajná polícia na Slovensku a v Čechách zasahuje a ovplyvňuje individuálne súkromie obyvateľov.

2 SIS ako najväčšia hrozba pre súkromie občanov na Slovensku

Predtým ako sa pustíme do kauzy leaknutej emailovovej komunikácie slovenskej SIS a talianskej hackerskej spoločnosti Hacking Team[11] na Wikileaks, ktorá bola pred pár mesiacmi kompletne vyhackovaná (Citizenlab o ich nemorálnych aktivitách dlhodobo informuje)[12], analyzujme historické škandály SIS týkajúce sa obmedzovania digitálneho súkromia.

1. SIS opakovane podala kontroverzný návrh na odpočúvanie akejkoľvek šifrovanej komunikácie všetkých občanov. Viac informácií SIS chce špehovať všetko, nás internet banking aj e-maily[13].

Na základe veľkého občianskeho odporu a viacerých kampaní proti tomuto návrhu (Tajná služba chce viac moci. 11 zmien, aby ju nezneužívala[14], hromadná pripomienka mimovládnych organizácií k návrhu zákona o Úrade civilného spravodajstva a Vojenskom spravodajstve[15]) a rozporovom konaní na Ministerstvu vnútra, ktorého som sa osobne zúčastnil, SIS uvedený návrh odpočúvania nakoniec stiahla.

Návrh SIS o nekontrolovateľný zber metadát občanov SR a povinnosť odovzdávať šifrovacie kľúče bez akejkoľvek súdnej kontroly predstavuje mimoriadny zásah do súkromia občanov, navyše bez akejkoľvek protiváhy. Návrh prikazuje pod hrozbou vysokej pokuty povinnosť odovzdávať šifrovacie kľúče z nejednoznačne definovaného okruhu zariadení – preemptívne a všeobecne.

2. Dňa 15.9.2014 Wikileaks zverejnili informáciu o tom[16], že Slovenská Republika nakúpila 39 licencií softvéru FinFisher v sume viac ako 5 miliónov EUR. FinFisher vyvíjaný spoločnosťou Gamma je využívaný totalitnými vládami rôznych krajín na špehovanie a monitorovanie disidentov. Ide o extrémne účinný softvér, lebo využíva tzv. 0-day zraniteľnosti na ktoré ešte neexistujú účinné bezpečnostné záplaty. Úrad vlády SR uvedenú informáciu dementoval – „Vo všeobecnosti nekomentujeme informácie Wikileaks, lebo majú kvalitu na úrovni „jedna pani povedala“. Problematiku, na ktorú sa pýtate, zastrešujú príslušné inštitúcie; obráťte sa prosím na nich,“ reagoval tlačový a informačný odbor Úradu vlády SR.

Wikileaks odhaľuje ale ďalšie informácie[17], ktoré Úrad vlády SR ani SIS verejnosti nepovedali a sú dosť šokujúce. Pán Jozef Mozolík zo SIS spriaznenej firmy GISS s.r.o. a pán Jan Fiala z ALLSAT s.r.o. pozvali do Bratislavy nielen zástupcov pofidérnej talianskej spoločnosti Hacking Team, ale aj zástupcov podobnej spoločnosti Gamma s cieľom odprezentovať ich špehovacie riešenie (FinFisher). A samozrejme čakali na ponuky od oboch týchto firiem.

Nezávisle zverejnené záznamy na Wikileaks svedčia o tom, že SIS reálne vyberali špehovacie riešenie medzi spoločnosťami Hacking Team a Gamma a je veľmi pravdepodobné, že nakoniec aj nejaké vybrali (o tomto svedčí minuloročné zverejnenie na Wikileaks, že Slovenská republika je klientom Gamma, ktoré slovenské úrady popreli).

Bohužiaľ všetko toto podliehalo utajeniu, takže SIS si mohla dovoliť závažny fakt, že komunikuje, dohaduje sa na stretnutiach a chce zakúpiť špehovacie riešenie od dvoch pofidérnych firiem (ktoré obe pracujú pre diktátorské krajiny) **zamlčať** (a to aj spravili).

O celej kauze FinFisher vs. Slovenská republika som mal pred takmer rokom prezentáciu – FinFisher – top government spying[18], video z prezentácie k dispozícii napríklad tu[19].

3. SIS má u všetkých mobilných operátoroch priamy prístup k Vašej mobilnej komunikácii a možnosť odpočúvať akúkoľvek Váš hovor alebo SMS správy. Potrebuje k dispozícií síce súdny príkaz, ktorý je ale len málokedy zamietnutý. Akýmkoľvek mobilným hovorom na Slovensku a v Čechách sa preto nedá vôbec veriť a preto jeden z mála spôsobov, ako sa reálne voči odpočúvaniu štátom brániť je realizovať „end-to-end“ šifrované hovory využitím aplikácie Signal Private Messenger pre Android[20] alebo pre iOS [21], prípadne využiť iný spôsob hlasového šifrovania použítim VoIP ZRTP protokolu.

4. Talianska spoločnosť Hacking Team, s ktorou obchodne rokovala SIS[11] bola kompletne vyhackovaná a boli zverejnené všetky kompromitujúce informácie súvisiace s jej biznisom. Viac informácií nájdete v článku: Hackli firmu, ktorá pomáha štátom špehovať občanov[22].

Uvedený softvér od spoločnosti Hacking Team nakúpila Česká polícia – Česká policie údajně platí miliony za nelegální hackerské nástroje[23]. Tu by som podotkol, že predaj Českej polícii bol realizovaný cez spoločnosť Bull s.r.o., k dispozícii faktúra[24]. Podľa komunikácie zverejnenej na Wikileaks[11] SIS plánovala na tento účel využiť súkromnú spoločnosť GISS s.r.o.[25]

Využívanie špehovacieho softvéru od Hacking Team riešili členovia Českej snemovne (Sledovací software policie použila v desítkách případů, zaznělo ve Sněmovně[26]). Vyzerá, že českí politici obhajujúci konanie českej polície sú mierne nechápaví a nerozumejú tomu, že nakupovanie špehovacieho software (na „legálne účely“) od Hacking Teamu je analogicky to isté ako nakupovanie munície (tiež na „legálne účely“) od ISIS, ktorý okrem toho, že ju predáva svojím klientom na obranu, tak ňou zabíja nevinných ľudí.

Česká polícia odmieta zverejniť akékoľvek ďalšie informácie o samotnom softvéri Galileo, ktorý nakúpil od spoločnosti Hacking Team – Policie ČR: Šmírovací software jsme koupili, ale vše je tajné, nic neřekneme[27], Hacking Team hacked: prodával spyware mnoha státům včetně Česka[28].

Konanie (a obchodovanie s diktátorskými krajinami) v prípade Hacking Team navrhujú vyšetriť priamo členovia Európskeho parlamentu[29].

Podľa zverejnenej Wikileaks komunikácie[11] vyzerá, že slovenská SIS nestihla od spoločnosti Hacking Team do doby zverejnenia nič zakúpiť (kedže spoločnosť Hacking Team bola kompletne vyhackovaná a prakticky zmetená z IT bezpečnostného trhu).

3 Prečo Česká polícia a SIS úplne morálne zlyhali?

Pofidérne nemorálne aktivity talianskej hackerskej spoločnosti Hacking Team sú **verejne známe** už niekoľko rokov, pravidelne sa o tom publikuje (v minulosti publikoval napríklad Citizenlab[12]).

Je neuveriteľné, že štátne inštitúcie ako Česká polícia, ktorá od nich uvedený nástroj za desaťtisíce eur reálne zakúpila, podobne slovenská SIS, ktorá uvedený nástroj plánovala zákupiť, neboli schopné pri tak veľkej čiastke si spraviť jednoduchý „background check" (overenie biznis partnera) samotnej spoločnosti Hacking Team a zistiť, že v IT bezpečnostnej komunite majú skutočne veľmi zlú reputáciu.

Ak to náhodou omylom nespravili, tak nezostáva nič iné, len konštatovať, že sú neschopní a mrhajú desaťtisíce eur od svojich daňových poplatníkov na nákup špehovacieho softvéru od firiem, ktorých reputáciu si nevedia alebo nechcú overiť.

4 Prečo je nemorálne používať špehovacie hackerské nástroje firiem od Hacking Team alebo Gamma?

Existuje viacero navzájom podporujúcich sa dôkazov, že uvedený softvér používajú vlády diktátorských krajín na špehovanie disidentov a politických aktivistov, ktorí sú následne kriminalizovaní, často aj mučení a zabití.

SIS nemá morálny problém cez spostredkovateľské firmy dohadovať si stretnutie s firmami, ktoré tieto režimy reálne podporujú.

Najnemorálnejšie na celom incidente okolo hackerských firiem „pracujúcich pre vlády" ako Hacking Team alebo Gamma nie je to, že vytvárajú a predávajú sofistikovaný špehovací softvér. Ale to, že vlády, ktoré si hovoria, že sú „demokratické" (a tam patrí aj slovenská a česká) od týchto firiem (ktorých kľúčový biznis je postavený na obchodovaní s diktátorskými vládami/režimami) za peniaze daňových obetí nakupujú špehovacie služby a nástroje.

Zo strany bežného občana smerom k tajným štátnym službám neexistuje prakticky žiadna transparentnosť (možnosť napríklad využívať infozákon). Bez Wikileaks a pomoci whistleblowerov by sa občania o týchto škandáloch zrejme nikdy nedozvedeli.

Taktiež to, že sa ako bežný občan nemáte fakt šancu akokoľvek voči tomuto brániť – na 0-day exploity neexistujú bezpečnostné záplaty (viac informácii ako funguje zvrhlý 0-day biznis s vládami vysvetľujem v mojej prezentácii Government's fight against cyber terrorism vs. FinFisher 0-day economy[30]). Súčasne nedokážete ani legálne zistiť či vaša vláda uvedené špehovanie reálne zakúpila a používa, kedže tento softvér nakupujú štátne inštitúcie, ktoré podliehajú kompletnému utajeniu (viď vyššie uvedené prehlásenie Českej polície).

Je to ukážka toho, ako sa „demokracia" reálne zmršťuje do Orwellovskej špehovacej diktatúry bez možnosti občana sa voči tomu akokoľvek brániť.

Kedže nemorálny biznis „government-friendly" firiem ako Hacking Team alebo Gamma vlády nikdy nezakážu a nebudú kriminalizovať (nakoľko sú sami klientami tohto biznisu), hackerské útoky voči týmto firmám je bohužiaľ jedna z mála možností ako sa dozvedieť zákulisné informácie o štátnej špehovacej diktatúre.

Ak sa skutočne bojíte o Vaše digitálne súkromie, štátne informačné služby sú to, z čoho by ste mali mať ten najväčší strach.

5 Whistleblowing ako jediný spôsob ako sa dozvedieť nemorálne zákulisné informácie o štátnych agentúrach podliehajúcich utajeniu

Jeden z najväčších škandálov, ktoré postihol slovenskú spoločnosť, bola kauza Gorila (únik hlasového prepisu odpočúvania komunikácie predstaviteľov najväčších finančných skupín a slovenských politikov). Kauza Gorila bola tak závažná, že ležala niekoľko týždnov v poštových schránkach všetkých veľkých slovenských médii a nikto nemal odvahu začať so zverejnením a hlbším analyzovaním. To nastalo až vtedy, keď samotný prepis Gorily bol anonymne zverejnený. Napriek závažným veciam, ktoré boli v kauze Gorila zverejnené, doteraz celá kauza nebola poriadne vyšetrená a je veľmi otázne či niekedy bude. Zvýšena frekvencia únikov informácií od whistleblowerov svedčí len o netransparentnosti a narastajúcom zneužívaní právomocí štátu, podobne o absencii interných vyšetrovacích mechanizmov. Toto sa bezprostredne dotýka napríklad aj našej súkromnej spoločnosti – časti jej portfólia boli ukradnuté a následne použité na vytvorenie ponuky a projektu pre štátnu zákazku podliehajúcu utajeniu pre štátny podnik JAVYS. Napriek tomu, že sme tento prípad medializovali – doteraz sa nezačalo interné vyšetrovanie.

6 Legalizácia používania špehovacieho softvéru (Informačno-technický prostriedok, ďalej ITP) pre vyvolené štátne úrady, kriminalizácia používania ITP inými osobami

Na Slovensku od 1.1.2016 platí nový zákon, ktorý legalizuje používanie špehovacieho softvéru (ďalej ITP) pre vyvolené štátne úrady (konkrétne Policajný zbor, SIS, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa). Konkrétne to znamená, že uvedené štátne inštitúcie môžu legálne používať kontroverzné špehovacie nástroje Galileo a FinFisher, a iné.

Znenie zákona „*Orgány územnej samosprávy, súkromné bezpečnostné služby ani fyzická osoba alebo právnicka osoba NESMIE použiť informačno-technický prostriedo*k“ vytvára legálne ohrozenie pre všetky firmy, ktoré takéto nástroje používajú pri svojej bežnej práci. Napríklad naša (ako aj iné) firmy využívajú množstvo nástrojov (Wireshark, Burp Suite Pro, Metasploit, testovací malware a iné) na obojstranne dohodnuté etické penetračné testovanie, ktoré svojou podstatou a časťami funkcionality sú dosť podobné ITP. V tomto prípade všetkým týmto firmám hrozí potenciálna kriminalizácia ich normálnej podnikateľskej činnosti. Zákon bohužiaľ ITP definuje veľmi vágne, takže táto možnosť tam stále existuje a je ľahko zneužiteľná.

7 „Rejdište zločinců a semeniště zla“ – Chovanec vyhlásil válku anonymite na Internetu.

Minister vnútra Milan Chovanec (ČSSD) ako aj množstvo západných európskych politikov (napríklad David Cameron) podliehajú v dôsledku svojej technickej nevedomosti ilúzii, že je možné vybudovať neanonymný Internet a zabezpečiť, aby všetci jeho používatelia boli „štátom overení“ vďaka čomu bude možné nadobro vyplieniť „semenište hnutí propagujúcich zlo“[30].

Stať sa vládcom nad Internetom a jeho obsahom je cieľom nejedného svetového diktátora. Každý z nich má na to podobný, ak nie rovnaký dôvod ako pán Minister — “bezpečnejší Internet bez hnutí propagujúcich zlo“.

Je pravdepodobné, že pán Chovanec pred svojim populistickým prehlásením[31] nekonzultoval technickú realizovateľnosť svojich politických vízií s odbornou verejnosťou, v nasledujúcich odstavcom by som poukázal na nebezpečnosť tohto aj iných podobných politických prehlásení týkajucích sa proklamovanej nevyhnutnosti štátnej kontroly nad Internetom.

8 Je vôbec technické možné kontrolovať Internet a znemožňovať anonymitu?

Bez drastických zásahov do súkromia ľudí, zákazu šifrovania a monitorovania akejkoľvek komunikácie **určite nie**.

Najsofistikovanejšie spôsoby štátnej kontroly nad Internetom existujú v Číne, Severnej Kórey či v rôznych arabských štátoch. Napriek tomu:

1. Vo všetkých týchto krajinách funguje anonymizačná sieť Tor[32] (aktivistami obľúbena distribúcia je Tails[33]).
2. V niektorých sú blokované prístupy na tzv. adresárové uzly („directory nodes“). Toto obmedzenie je možné obísť používaním neverejných Tor premostení (tzv. „Bridge relay nodes“[34]).
3. V niektorých krajinách je blokovaná Tor komunikácia (ktorá sa normálne tvári ako „https“) pomocou DPI alebo aplikačných firewallov. Toto je možné obísť steganografiou — vkladaním citlivého obsahu do bežnej verejnej komunikácie) pomocou obfsproxy3[35]. Vývojari Toru aktívne pracujú tiež na sofistikovanejšom spôsobe obfuskácie obfs4[36].

Nutne podotknúť, že na trh prichádzajú stále nové a nové zariadenia využívajúce rôzne anonymizačné technológie (alebo VPN) umožňujúce ich používať okamžite bez technických znalostí (napríklad SafePlug[37], ktorý stoji len $49).

Momentálne v každej diktátorske krajine na svete je možné obísť štátne centrálne vynucované kontroly Internetu a to aj napriek tomu, že by si ich diktátori želali opak.

Kedže prakticky nezakázateľné anonymizačné siete v súčasnej dobe používajú nielen aktivisti a novinári v diktátorských krajinách, ale aj kriminálnici a teroristi, stojí za zamyslenie, či dá sa zaviesť efektívna kontrola prístupu k Internetu?

9 Dá sa zaviesť efektívna kontrola prístupu k Internetu?

Technicky nie. Obeťou štátneho špehovania a kontroly sa stanú najbežnejší ľudia, ktorí anonymizačné siete používať nebudú. Akékoľvek informácie o nich zbierané sa stanú predmetom zneužitia a korupcie. Položme si otázku: “existuje politik, ktorému dôverujete dostatočne na to, aby ste sa dobrovoľne zbavili práva na svoje anonymné príspevky?“.

Ak ste odpovedali áno, tak vedzte, že obrovské množstvo skúsených používateľov Internetu a ľudí preferujúcich slobodu má úplne opačný názor.

Akékoľvek pokusy štátu zákazovať Internetovú anonymitu a vynucovať štátom pridelený identifikátor vždy pri prístupe do Internetu, nielenže je technicky ťažko realizovateľné, ale malo by to drastický dopad na Internetové súkromie všetkých obyvateľov štátu. Ocitlo by sa totiž v rukách nedôveryhodných skorumpovaných politikov a ich štátneho aparátu.

Uvažovanie „keď nerobím nič zlé, nemám čo skrývať“ je chybné a veľmi krátkozraké, kedže štátom zbierané informácie môžu byť o vás zneužité ďalšou politickou garnitúrou, s ktorou už vôbec sympatizovať nemusíte.

Internetová anonymita tiež umožňuje dosiahnúť a demonštrovať existenciu alternatívnej decentralizovanej spoločnosti ku štátu, v ktorej neexistuje možnosť centrálne riadiť a vynucovať pravidlá, kde obojstranné dohody sú zabezpečované formou vzájomnych kontraktov.

10 Akú politickú legitimitu majú predkladatelia "diktátorských" zákonov?

Celoplošné špehovanie občanov, regulácia a kontrola sú bohužiaľ v súčasnej dobe stále otvorené a obľúbené politické témy v Čechách aj na Slovensku.

Ak niektorá zo súčasných štátnych inštitúcií alebo jej predstaviteľov predloží zákon o povinnom označovaní Židov žltou hviezdou, budeme ho brať vážne?

Ak nie, prečo potom berieme vážne návrhy diktátorských zákonov a fašizujúce názory štátnych inštitúcií ako SIS, MV SR, MV ČR?

Podľa štúdie Inštitútu pre verejné otázky Internet Freedom Report 2014: Slovakia, v roku 2012 slovenská polícia zadala 1551 žiadostí o odpočúvanie, z ktorých boli schválené prakticky všetky (1489), ale len 59 sa reálne použilo v nejakom súdnom procese (to je menej ako 4 %). Vyplýva z toho, že riziko nelegitímneho odpočúvania (kedy nebol spáchany žiadny trestný čin) je relatívne vysoké a preto je dobré sa voči nemu brániť.

11 Dopady štátnych zásahov na naše súkromie

Ak štátne inštitúcie budú mať prístup k dešifrovanej komunikácii alebo kľúčovému materiálu svojich občanov, tak je zjavné, že tieto zákony určite spôsobia cielené oslabenie používaných krypto systémov. Akýkoľvek štátny pokus o reguláciu šifrovania degraduje ochranu digitálneho súkromia všetkých ľudí a spôsobuje zvýšenie rizika odpočúvania tretími stranami. História bohužiaľ ukazuje, že „legálne odpočúvacie systémy" štátnej moci boli opakovane nabúrané hackermi a zneužité na odpočúvanie a špehovanie nevinných ľudí [5][6].

Ak štát bude vyžadovať od výrobcov krypto riešení poskytovanie akéhokoľvek prístupu k prenášaným údajom či kľúčovému materiálu (tzv."zadné vrátka"), tak reálne hrozí, že akékoľvek silné krypto riešenia sa v Čechách a na Slovensku prestanú ponúkať a komerčne distribuovať. Podobná situácia nastala pred pár rokmi v Saudskej Arábii a Spojených štátoch Emirátskych, ktorí od spoločnosti Blackberry pred vstupom na ich trhu explicitne vyžadovali implementáciu „backdoorov" („zadných vrátok") do akejkoľvek šifrovanej komunikácie hovorov vykonaných na území týchto krajín a teda možnosť poskytnúť samotným vládam prístup ku všetkým hovorom[7]. Kedže Blackberry odmietlo oslabiť bezpečnosť a súkromie svojich klientov, vlády týchto krajín znemožnili vstup Blackberry na ich trh. Podobná kauza momentálne prebieha v USA, kedy federálna služba FBI chcela donútiť spoločnosť Apple vytvoriť a nasadiť špeciálnu verziu iOS firmwareu so „zadnými vrátkami", ktorá by im umožnila odpočúvanie komunikácie používateľov iPhone telefónov. Apple to verejne odmietol a New Yorský súd pred pár dňami rozhodol, že nútiť Apple do cieleného oslabenia krypto systémov svojich klientov zo strany FBI je protiústavné.

Je potrebné si uvedomiť, že podobnou navrhovanou legislatívou sa českí a slovenskí občania úplne pripravia o možnosť mať dostatočné silné riešenia na trhu na ochranu svojho digitálneho súkromia a paradoxne vďaka štátu, ktorý intenzívne bojuje voči cyberzločinu sa stanú jeho ľahšími obeťami.

Súčasna legislatíva na Slovensku, ktorá umožňuje použitie ITP výhradne pár vyvoleným štátnym úradom tiež vytvára obrovskú informačnú nerovnováhu (špehovací software so 0-day exploitami môže použiť len štát – samotní občania sa nemajú ako brániť). Podobne vágna definícia ITP v zákone vytvára priestor pre zneužitie (bude naša spoločnosť kriminalizovaná za to, že používa pre účel svojej práce špehovacie nástroje a exploity?)

12 Tri dôvody prečo vaše štátne úrady predstavujú najväčšiu hrozbu pre Vaše digitálne súkromie

12.1 Netransparentnosť

V prípade štatnych agentúr podliehajúcich utajeniu prakticky žiadna. Nemáte takmer žiadnu možnosť zistiť, aké sofistikované nástroje a zbrane uvedené štátne agentúry nakupujú a v akom rozsahu (koľko občanov je obeťou špehovania).

12.2 Monopol

Opakované zneužitie právomoci štátnych agentúr (čo je určite aplikovateľné aj na SIS) nevedie k strate reputácie a jej prípadnemu krachu. Štátne agentúry na danom území nemajú prirodzenú konkurenciu, trhovú potrebu udržiavať si spokojných zákaznikov a teda udržiavať si trhovú reputáciu. To automaticky vedie k opakovanému zneužívaniu ich právomocí a osobne som presvedčený o tom, že bez decentralizácie a demonopolizácie týchto služieb nie je možné tento problém vyriešiť.

12.3 Špehovací malware softvér so 0-day exploitami

Jedna z najzákernejších vecí, ktorá sa dotýka všetkých ľudí, je silná informačná nerovnováha, ktorú softvér so 0-day exploitami (Galilelo, Gamma) vlastnený a používaný štátnymi agentúrami a štátnou políciou vytvára. Ako bežní občania prakticky nemáte žiadnu možnosť sa voči týmto odpočúvacím a špehovacím nástrojom brániť. A bohužiaľ vo väčšine prípadov ani zistiť, že ste obeťou odpočúvania.

13 Chráňte sa!

Súčasne technológie umožňujú do veľmi slušnej miery chrániť akúkoľvek hlasovú, textovú, či inú komunikáciu. Medzi najpopulárnejšie nástroje s dobrou a overenou reputáciou na šifrovanie hlasu je nástroj Signal private messenger [8] dostupný pre platformy Android a iOS. Alternatívne nástroje sú napríklad Telegram[9] alebo Threema[10].

Pri šifrovanej instantnej komunikácii sa neodporúčajú používať nešifrované protokoly, resp. protokoly, ktoré priamo neumožňujú end-to-end šifrovanú komunikáciu (Skype, MSN, ICQ, Google Talk, Facebook messenger a iné). Naopak odporúča sa používať XMPP protokol (napríklad Jabber) s podporou end-to-end šifrovania prostredníctvom OTR.

Aj napriek tomu, že veľa bezpečnostných expertov pokladá šifrovanie využitím PGP alebo S/MIME už za historicky prekonané (napríklad kvôli absencii PFS – „Perfect Forward Secrecy“), použitie uvedených technológií na šifrovanie emailovej komunikácie môže výrazne navýšiť ochranu vašej komunikácie (obzvlášť ak používate verejné poštové servery ako GMAIL, kde je možnosť nainštalovať si Mailvelope Plugin, ktorý vám PGP šifrovanie umožní).

Prakticky nevyhnutná vec je kompletné zašifrovanie vášho disku (v prípade Microsoft Windows použitím Microsoft Bitlocker prípadne použitím iných otvorených nástrojov, v prípade Mac OS FileVault, v prípade Linuxu dm-crypt/LUKS). A to sa netýka len osobného počítača či laptopu, ale aj vašich mobilných zariadení (Android podporuje kompletné šifrovanie od verzie 3.0). V krajinách, ktoré vynucujú poskytovanie kľúčového materiálu štátnym agentúram ako napríklad UK (majú tzv. „key disclosure law“) je vhodné používať aj tzv.“hidden volumes“, teda skryté časti diskov, ktorých existenciu nie je možné dokázať digitálnou forenznou analýzou a umožňujú vám dobre reagovať aj v situáciach, kedy ste donútení zo strany štátu alebo teroristov prezradiť svoje heslo alebo heslovú frázu k vaším zašifrovaným dátam.

Tiež je dôležité dbať o používanie a inštaláciou softvéru z dôveryhodných overených zdrojov a jeho neustálu aktualizáciu. To sa týka aj aktualizácie operačných systémov a ich jadier (podľa uniknutných informacií, špehovacie softvéry Gamma a Galileo nedisponovali funkčnými 0-day exploitami na posledné verzie iOS).

Referencie

[1] Hacking Team Breach Shows a Global Spying Firm Run Amok

[2] Hacking Team Asks Customers to Stop Using Its Software After Hack

[3] Online mirror hacknutého archívu http://ht.musalbas.com/

[4] Nepracujeme pre štát

[5] http://spectrum.ieee.org/telecom/security/the-athens-affair

[6] https://en.wikipedia.org/wiki/SISMI-Telecom_scandal

[7] http://www.bbc.com/news/world-middle-east-10888954

[8] https://whispersystems.org/

[9] https://telegram.org/

[10] https://threema.ch/en

[11] https://wikileaks.org/hackingteam/emails/?q=sis.gov.sk&mfrom&mto&title&notitle&date&nofrom&noto&count=50&sort=0#searchresult

[12] https://citizenlab.org/?s=hacking+team

[13] http://ekonomika.sme.sk/c/7171055/sis-chce-spehovat-vsetko-nas-internet-banking-aj-e-maily.html

[14] http://www.changenet.sk/?section=kampane&x=796541

[15] http://www.ekoforum.sk/peticia/sifrovanie

[16] https://wikileaks.org/spyfiles4/customers.html#customer_15

[17] https://wikileaks.org/hackingteam/emails/?q=mozolik+gamma&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult

[18] https://prezi.com/iodh3l4ej2l9/finfisher-top-government-spying/

[19] https://www.youtube.com/watch?v=lqIe68KDrcY

[20] https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone&hl=de

[21] https://itunes.apple.com/de/app/signal-private-messenger/id874139669?mt=8

[22] http://tech.sme.sk/c/7899235/hackli-firmu-ktora-pomaha-statom-spehovat-obcanov.html?ref=trz

[23] http://tech.ihned.cz/geekosfera/c1-64277360-kdo-hackuje-hackery-policie-hackovaci-nastroje

[24] http://i.iinfo.cz/images/144/hacking-team-bull-prev.png

[25] http://orsr.sk/vypis.asp?ID=14790&SID=2&P=0

[26] http://www.novinky.cz/internet-a-pc/bezpecnost/374517-sledovaci-software-policie-pouzila-v-desitkach-pripadu-zaznelo-ve-snemovne.html

[27] http://www.lupa.cz/clanky/policie-cr-smirovaci-software-jsme-koupili-ale-vse-je-tajne-nic-nerekneme/?forceSwitch

[28] http://www.root.cz/clanky/hacking-team-hacked-prodaval-spyware-mnoha-statum-vcetne-ceska/?forceSwitch

[29] http://motherboard.vice.com/read/italy-should-investigate-hacking-team-european-parliament-member-says

[30] https://prezi.com/hgiy1j955pdj/governments-fight-against-cyber-terrorism-vs-finfisher-0-day-economy/

[31] http://www.parlamentnilisty.cz/arena/monitor/Semeniste-zla-promluvil-ministr-Chovanec-o-internetu-Nazrala-pry-doba-abychom-s-nim-neco-delali-416218

[32] https://www.torproject.org/

[33] https://tails.boum.org/

[34] https://www.torproject.org/docs/bridges.html.en

[35] https://www.torproject.org/projects/obfsproxy.html.en

[36] https://github.com/Yawning/obfs4

[37] https://pogoplug.com/safeplug

The processes of response on computer security incidents
Procesy riešenia bezpečnostných počítačových incidentov

Ivan Makatura

Ivan Makatura
ivan.makatura@sk.ibm.com

Ivan Makatura is the member of IBM Security Services team in the role of Senior security consultant, focused on Information & Cyber Security, Regulatory, Personal Data Protection Risk & Compliance management. Ivan is skilled security manager with more than thirteen years of experience as Chief Security Officer in banks, with broad knowledge in IT, specialized to Information Security Management Systems, IT Service Management Systems as well as on IT Risk Management processes.
Ivan is judicial expert in field Security and protection of information systems licensed by Slovak Ministry of justice. He acts also as certified information security auditor and vice-chairman of Slovak Information Security Association.
He graduated at Technical University of Košice, Faculty of Electrical Engineering and Informatics, studied Computer science and graduated from the same school in Applied Informatics. Later he completed a postgraduate degree in Judicial Expertise and Forensic engineering at Slovak University of Technology in Bratislava. Currently he is working on his doctoral study, with Network Intrusion Detection Systems dissertation thesis.
He holds a few professional certifications: Certified in Risk and Information Systems Control (CRISC, ISACA), Management of Risk (M_o_R, APMG), ITIL v3 and Cisco Certified Network Associate (CCNA).

Ivan Makatura je členom tímu IBM Security Services v pozícii staršieho bezpečnostného konzultanta, so zameraním na oblasť informačnej a kybernetickej bezpečnosti, ochranu osobných údajov, manažment rizika a riadenie súladu. Ivan je skúsený bezpečnostný manažér s viac, než 13 ročnou praxou riaditeľa odboru bezpečnosti (CSO) v bankách, s rozsiahlymi znalosťami v oblasti IT, so špecializáciou na systémy riadenia informačnej bezpečnosti (ISMS), manažment IT služieb (ITSM) a na procesy riadenia IT rizík.
Ivan je súdnym znalcom v odvetví Bezpečnosť a ochrana informačných systémov zapísaný v Zozname znalcov, tlmočníkov a prekladateľov Ministerstva spravodlivosti Slovenskej Republiky. Pôsobí tiež ako certifikovaný audítor informačnej bezpečnosti a výkonný podpredseda Slovenskej asociácie pre informačnú bezpečnosť.
Vyštudoval odbor výpočtová technika a neskôr odbor aplikovaná informatika na Fakulte elektrotechniky a informatiky Technickej univerzity v Košiciach. Absolvoval postgraduálne štúdium na Znaleckom ústave elektrotechniky a informatiky Fakulty elektrotechniky a informatiky Slovenskej Technickej univerzity v Bratislave. V súčasnosti je externým doktorandom s dizertáciou v oblasti systémov detekcie prieniku v počítačových sieťach. Je držiteľom niekoľkých profesných certifikácií: Certified in Risk and Information Systems Control (CRISC, ISACA), Management of Risk (M_o_R, APMG), ITIL v3 a Cisco Certified Network Associate (CCNA).

The processes of response on computer security incidents

One of the key responsibilities of company management in mitigation of risks is the deployment of process of response on the computer security incidents. The organization's ability to respond effectively to the incident depends on the quality of preparation for all possible events that could adversely affect the information assets of the enterprise.

In case of incidents related to critical information assets, handling must be based on comprehensive, accurate analysis and prudent response. Preparation of incident response must therefore be necessarily based on a thorough resource planning and especially on the early deployed and tested response procedures. Implementation of incident handling process would be derived from the correct understanding of the entire incident life cycle - from its inception to the closing and subsequently lesson learnt.

In organizations with greater complexity of systems, it is highly recommended to pre-establish and to continuously educate the dedicated team, whose task will be to properly respond to identified incidents. That team will be able to take timely countermeasures to ensure the proper collection of evidences for further investigation of the incident and any criminal implications.

The presentation describes the life cycle of the incident, activities of which is composed the incident resolution process and also briefly summarizes the essential prerequisites for the founding of a computer emergency response team, which could be potentially provided as an outsourced service.

Procesy riešenia bezpečnostných počítačových incidentov

Jednou z kľúčových zodpovedností vedenia podniku v ošetrovaní rizík je zavedenie procesu riešenia bezpečnostných incidentov. Schopnosť organizácie efektívne reagovať na identifikovaný incident je závislá od kvalitnej prípravy na všetky potenciálne udalosti, ktoré by mohli nepriaznivo pôsobiť na informačné aktíva podniku.

Ak sa incident týka kritických informačných aktív, jeho zvládnutie si vyžaduje komplexné podchytenie, presnú analýzu a uvážlivú reakciu. Príprava riešenia incidentov preto musí byť nevyhnutne založená na dôkladnom plánovaní zdrojov ale najmä na včasnom vybudovaní a otestovaní reakčných procedúr. Implementácia procesov reakcie na bezpečnostné incidenty by mala byť odvodená od správneho pochopenia celého životného cyklu incidentu od jeho vzniku až po uzatvorenie a ponaučenie.

V organizáciách s vyššou komplexitou informačných systémov je nanajvýš vhodné, aby bol vopred ustanovený a priebežne školený špecializovaný tím, ktorého úlohou bude správne reagovať na identifikované incidenty.

ktorý bude schopný včas prijať protiopatrenia, zabezpečiť zber dôkazov pre ďalšie vyšetrovanie incidentu a prípadné vyvodenie pracovnoprávnych alebo trestnoprávnych dôsledkov.

Prezentácia opisuje životný cyklus incidentu, aktivity, z ktorých je zložený proces riešenia incidentu a zároveň stručne zhŕňa základné predpoklady pre založenie tímu reakcie na bezpečnostné počítačové incidenty, potenciálne poskytovaného aj formou outsourcingu.

Jednou z kľúčových zodpovedností vedenia podniku pri podpore systému riadenia informačnej bezpečnosti je zavedenie procesu riešenia bezpečnostných incidentov. Schopnosť organizácie efektívne reagovať na identifikovaný incident je závislá od kvalitnej prípravy na všetky potenciálne udalosti, ktoré by mohli nepriaznivo pôsobiť na informačné aktíva podniku.

Ak sa incident týka kritických informačných aktív, jeho zvládnutie si vyžaduje komplexné podchytenie, presnú analýzu a uvážlivú reakciu. Príprava riešenia incidentov preto musí byť nevyhnutne založená na dôkladnom plánovaní zdrojov, ale najmä na včasnom vybudovaní a otestovaní reakčných procedúr. Implementácia procesov reakcie na bezpečnostné incidenty je podmienená správnym pochopením celého životného cyklu incidentu, od jeho vzniku, až po uzatvorenie a ponaučenie.

Povedzme si niečo ku životnému cyklu incidentu a stručne aj k aktivitám, z ktorých sa skladá proces riešenia bezpečnostného incidentu.

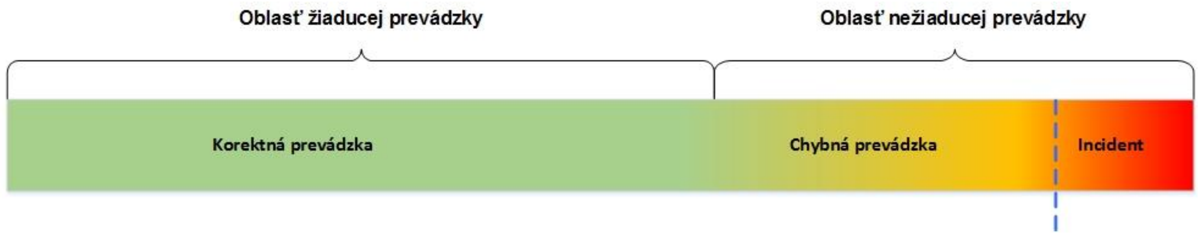
1 Udalosť vs. incident

Bez vetra sa ani lístok nepohne, ako hovorí známe slovenské príslovie. Platí to aj pre bezpečnostné počítačové incidenty. Podľa lexikálneho slovníka je incident nepríjemná príhoda, nemilá udalosť a podobne je potrebné nahliadať aj na celý proces vzniku bezpečnostného incidentu. **Bez predchádzajúcej UDALOSTI nemôže jestvovať INCIDENT**.

V informačných technológiách je udalosťou (ang. „event“) akýkoľvek pozorovateľný jav v systémoch a v sieťach. Udalosťou je prihlásenie používateľa, spustenie aplikácie, aktivita sieťovej vrstvy a akýkoľvek iný proces, ktorý môže byť potenciálne negatívny, nechcený a nepríjemný, napríklad aj preto, že je zlomyseľný. **Udalosť, nemusí nevyhnutne znamenať incident, môže však poskytnúť indície, ktoré po vyhodnotení môžu odhaliť nezvyklú, alebo neočakávanú škodlivú aktivitu**.

Udalosť, podľa ITIL-u, je taká zmena stavu, ktorá má význam pre manažment konfiguračných položiek, alebo pre IT službu. Termín „udalosť“ je používaný aj v zmysle výstrahy, alebo upozornenia vytvoreného IT službou, alebo monitorovacím nástrojom. Udalosť si spravidla vyžaduje zásah prevádzkového personálu a často má za následok vytvorenie záznamu o incidente.

Na incident je možné nazerať napríklad aj prostredníctvom kvality prevádzky IT služby. Je prirodzené, že za žiaducu sa považuje len taká prevádzka služby, ktorá nejaví žiadnu kvalitatívnu odchýlku od pôvodnej špecifikácie. Oproti tomu, prevádzka IT služby, ktorá má známky nekvality, už môže byť považovaná za nežiaducu. Samotná **chyba, alebo služba so zníženou kvalitou však ešte nie je bezpečnostným incidentom**.



2 Definícia incidentu

Bezpečnostný počítačový incident je taká škodlivá udalosť, v rámci ktorej došlo ku strate dôvernosti dát, zničeniu dát, prelomeniu integrity systému, alebo obmedzeniu, či odmietnutiu dostupnosti služby. Môže to byť akékoľvek nezvyklá, alebo neočakávaná aktivita, priestupok, alebo riziko priestupku proti bezpečnostnej politike, prípadne proti akceptovateľnému použitiu bezpečnostných politík, nesplnenie štandardných postupov, ktoré viedlo ku takej zmene kvality služby, ktorá je pre organizáciu zásadne neprijateľná.

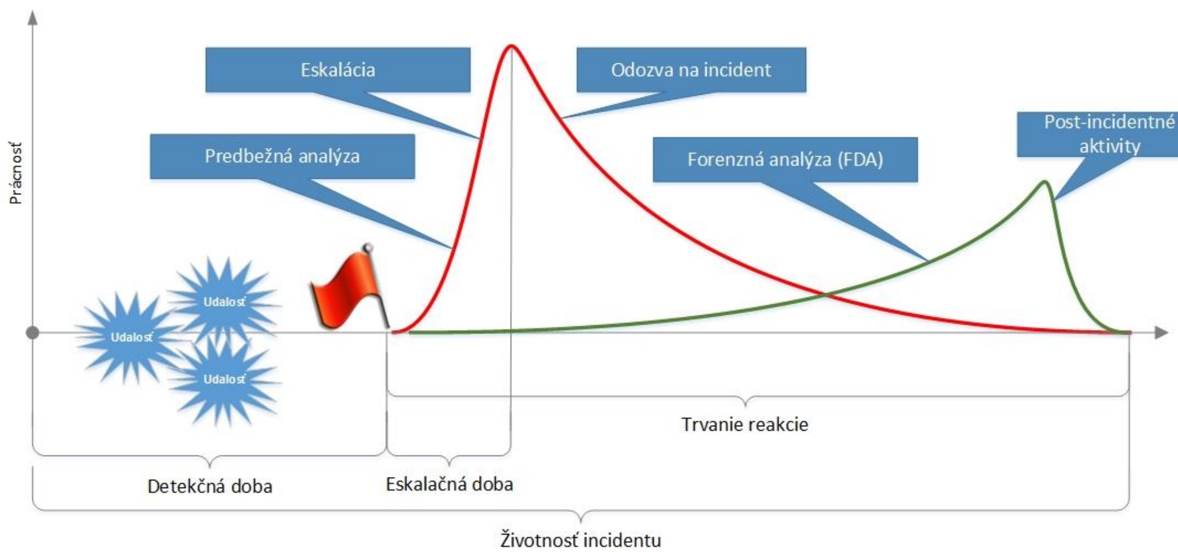
Podľa ISO 27001 je bezpečnostný incident jedna, alebo viac nežiaducich, alebo neočakávaných bezpečnostných udalostí, u ktorých existuje vysoká pravdepodobnosť kompromitácie činností organizácie a ohrozenie bezpečnosti informácií.

Medzinárodná norma ISO/IEC 27013, ktorá pojednáva o zjednotenej implementácii systému riadenia informačnej bezpečnosti (ISO/IEC 27001) a manažmentu služieb IT (ISO/IEC 20000-1), odporúča ošetrovať incidenty v informačnej bezpečnosti ako špecifický typ závažného incidentu (ang. „major incident“). Taký postup zabezpečí, že:

- vedenie organizácie bude o incidente informované,
- procesy ošetrovania bezpečnostných incidentov budú vopred stanovené,
- pre tieto procesy bude vopred určený a vyškolený okruh zodpovedných zamestnancov.

3 Životný cyklus incidentu

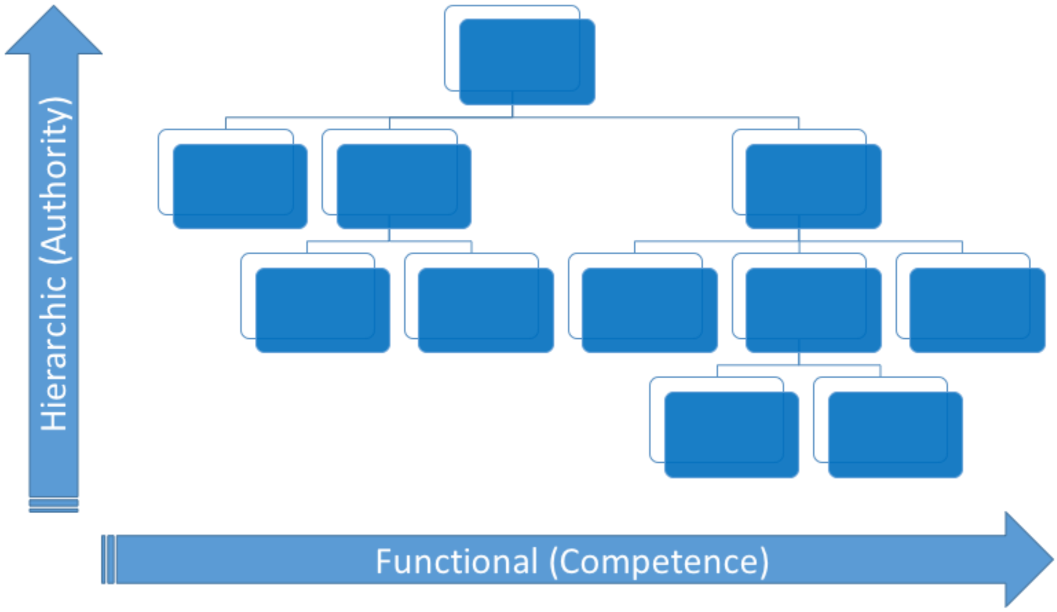
Pre pochopenie jednotlivých fáz bezpečnostného počítačového incidentu je potrebné pozrieť sa najskôr na incident z pohľadu časového rozlíšenia. Incident počas svojej životnosti (ang. „time to live”) prechádza niekoľkými fázami, ktoré sa vzájomne prelínajú a ktoré majú rôznu, v čase sa meniacu prácnosť i zložitosť.



Od chvíle, keď sa vyskytne škodlivá udalosť, vždy uplynie istý čas, kým túto udalosť zodpovedné osoby detegujú. Pravda je taká, že niekedy ju nedokážu detegovať vôbec. Ale táto téma by bola na samostatnú úvahu. ☺

Po úspešnom zistení incidentu, je potrebný určitý čas na to, aby zodpovedné osoby získali výsledky hrubej analýzy a aby na základe zistených informácií zhodnotili udalosť, ktorá determinuje incident. Tento časový interval sa nazýva detekcia (ang. „detection time“). Keďže najmä pri vážnych incidentoch nie je v možnostiach jedného človeka aby reagoval na incident, je bezprostredne nutné zabezpečiť eskaláciu iným útvarom a vyhľadanie kontaktných osôb zúčastnených na vopred definovaných procesoch reakcie na incident (ang. „escalation time“).

Eskalačná procedúra je dvojakého charakteru. Jednak je skôr či neskôr potrebné informovať o incidente príslušné autority v rámci organizácie – táto vertikálna eskalácia nazýva „hierarchická“, alebo „autoritatívna“. Treba však mať na pamäti, že cieľom by malo byť skrátenie celkovej doby eskalácie s cieľom čo najskôr začať reálne práce na odstránení následkov incidentu. Vyššie postavení manažéri však ku úspešnému zvládnutiu incidentu zvyčajne nedokážu prispieť viac, než profesionálni informatici a odborníci z oblasti informačnej bezpečnosti. Pre vyššiu efektivitu odozvy na incident možno iba odporúčať, aby prednosť vždy dostala horizontálna, teda „funkčná“, alebo tiež „kompetenčná“ eskalácia.



Trvanie reakcie, alebo tiež odozva na incident (ang. „response time“), je čas ktorý uplynie od detekcie až po nápravu dôsledkov incidentu a ukončenie vyšetrovania. Hlavným cieľom aktivít odozvy na incident by malo byť obnovenie funkčnosti poškodených informačných aktív, ich návrat do pôvodného stavu, zaručenie kontinuity činnosti, zákonná náprava incidentu a zhromaždenie dôkazov na podporu postupu proti vinníkom. Z toho dôvodu má odozva na incident dve samostatné časti, ktorých cieľ by sa dal zjednodušene heslovite pomenovať:

1. „oprav a pokračuj“
2. „vyšetri a stíhaj“

V organizáciách, pre ktoré sú ich informačné aktíva kriticky dôležité pre pokračovanie činnosti, je logicky prvou časťou vymedzenie a izoláciu incidentu a následná koordinácia snahy o obnovenie funkčnosti poškodených informácií a systémov, odstránenie následkov incidentu, náprava škôd a pokračovanie v činnosti.

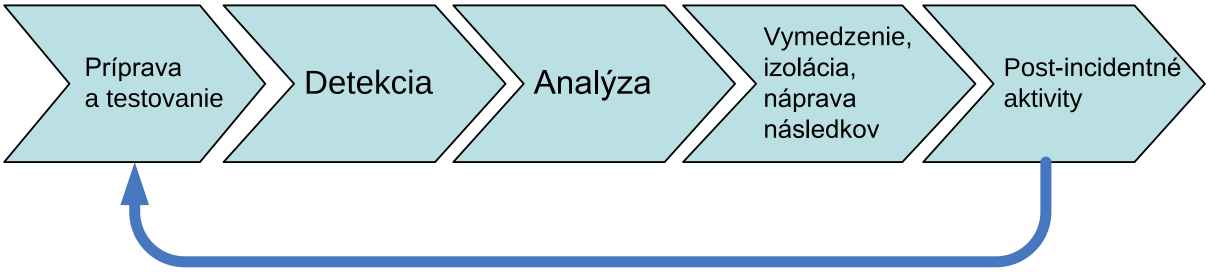
Popritom musí zároveň začať racionálny a premyslený rozbor incidentu, rozklad indikácie od abstraktného, všeobecného zistenia, ku konkrétnemu popisu podstaty a podrobností incidentu, stanovenie otázok pre identifikáciu typu incidentu, overenie nastavenia bezpečnostných politík, rozpoznanie typu bezpečnostného incidentu, stanovenie pátracích postupov podľa príslušnej kategórie incidentu, klasifikácia napadnutých systémov a kompromitovaných informácií, zhodnotenie možných vyvolaných vplyvov na spolupracujúce systémy a forenzná analýza incidentu.

Podrobný opis postupov nie je vzhľadom na rôznorodosť systémov a procesov v možnostiach jedinej prednášky. Čo však je nutné zdôrazniť - unáhlené reakcie sú v procese riešenia incidentov extrémne kontraproduktívne. **Bezpečnostný incident je neštandardná udalosť, ktorá vyvoláva tendenciu chaotického konania, čo následne zvyšuje riziko strát**. Je preto veľmi účelné, ak organizácia má vopred pripravený plán reakcie a popis procesov, súvisiacich so spôsobom riešenia bezpečnostného počítačového incidentu, napríklad diagnostickú maticu pre urýchlenie rozhodovania, najmä pre menej skúsený personál.

4 Niet nad skúsenosti...

Kedysi dávno vyhlásil generál A. V. Suvorov známu vetu: „Ťažko na cvičisku, ľahko na bojisku“. Nedá sa, než s týmto tvrdením súhlasiť. Prezieravé vedenie podniku v ideálnom prípade zabezpečí, že plán reakcie na incident bude vopred otestovaný v realistických cvičeniach s modelovými situáciami.

Poučenie z incidentu (ang. „incident learning“, alebo „lessons learnt“) je súčasťou tzv. post-incidentných aktivít. Tým sa vlastne zabezpečí previazanosť nadobudnutých skúseností s prípravou na budúci podobný incident.



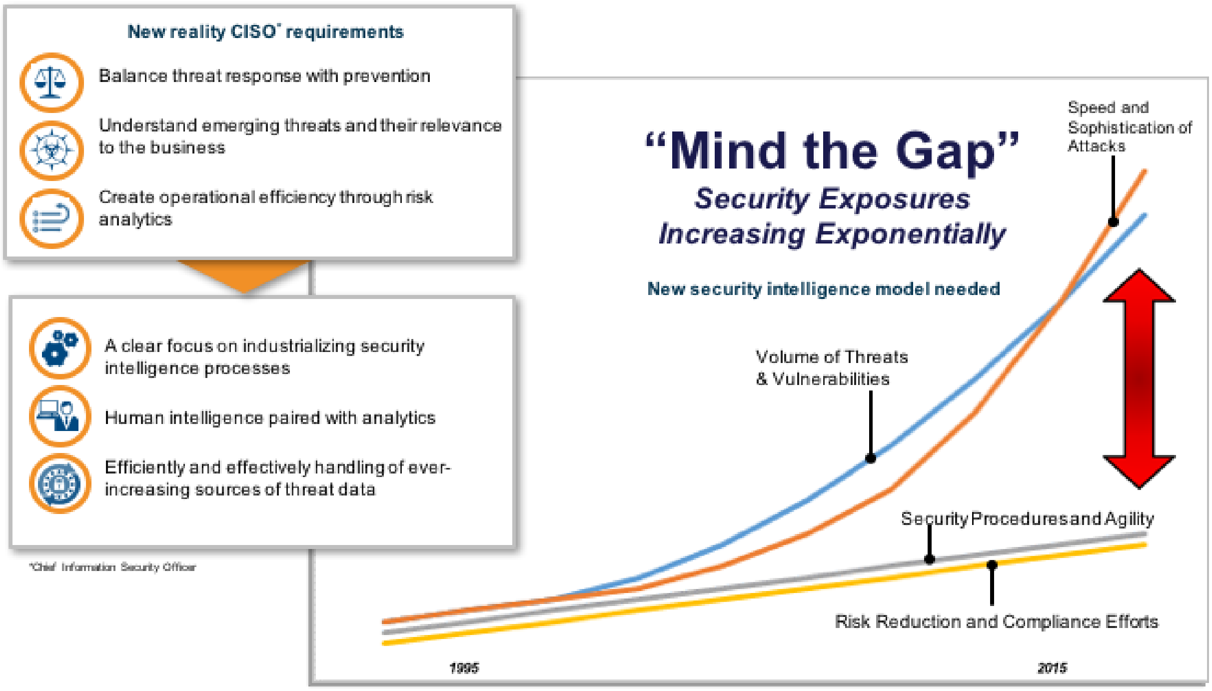
Pokiaľ má organizácia úprimný záujem vyhnúť sa v budúcnosti incidentu, ktorý bol práve predmetom riešenia, potom je potrebné v čase, keď sú ešte všetky poznatky a skúsenosti čerstvé, tieto prediskutovať so všetkými zainteresovanými stranami, ktoré boli súčasťou procesu riešenia incidentu. Ako výstup z tejto diskusie je vhodné navrhnúť také protiopatrenia (alebo zmenu existujúcich protiopatrení), ktoré pomôžu organizácii zlepšiť:

1. úroveň technického zabezpečenia voči zraniteľnosti, ktorá bola v incidente zneužitá,
2. schopnosť reagovať na podobný incident v budúcnosti s kratšími časmi odozvy

5 SOC – CERT – MSS

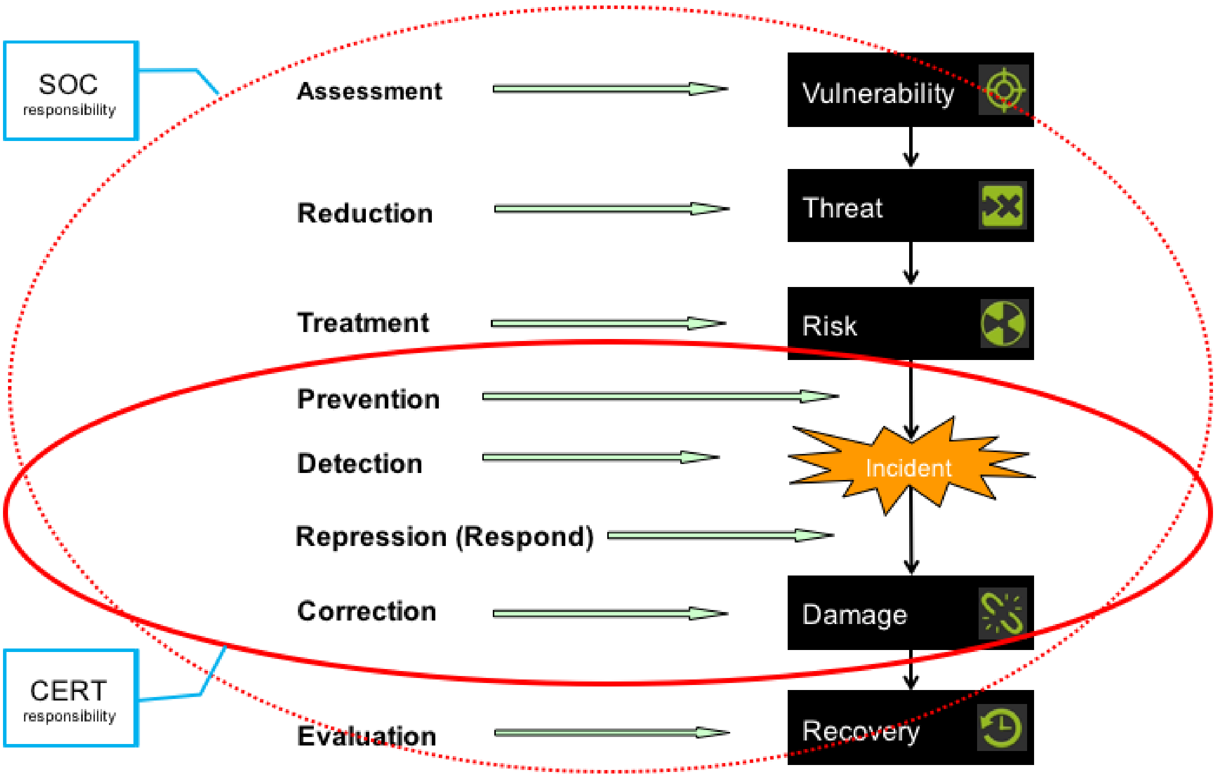
Nezávisle od snahy všetkých zúčastnených strán znižovať bezpečnostné riziká, vrátane postupne narastajúceho počtu regulačných požiadaviek a vrátane sprísňujúcej sa legislatívy, hlavnou výzvou pre bezpečnostné tímy je fakt, že IT infraštruktúra je dnes zraniteľná oveľa viac, než bola v minulosti. Útoky spôsobujú rôzne negatívne dopady na biznis. Poskytnúť ucelenú štatistiku incidentov nie je v možnostiach tejto prednášky, napriek tomu, že IBM disponuje výsledkami vlastného výskumu v tejto oblasti. Posledný report skupiny IBM X-Force® „Cyber Security Intelligence Index 2016“ bol vydaný len nedávno. Materiál je k dispozícii na stiahnutie napríklad na adrese https://securityintelligence.com

Od bezpečnostných profesionálov sa vyžaduje adekvátna ochrana pred hrozbami ktoré pôsobia na informačné aktíva podnikov. Udržanie kontroly nad zvyšujúcim sa počtom zraniteľností a následne aj pokusov o kompromitáciu informačných aktív je úloha s vysokým nárokom na prácnosť. Navyše tu jestvuje potreba udržiavať úroveň znalostí bezpečnostného tímu na vysokej úrovni, čo vytvára tlak na na zvyšovanie ceny práce.



Riešením tohto nepríjemného stavu je zdieľanie zdrojov. Organizácia môže zdieľať svoje bezpečnostné zdroje a využiť zdieľané cudzie zdroje napríklad tým spôsobom, že si bude vzájomne „požičiavať“ odborné pracovné kapacity s inými podnikmi vo svojom odvetví. Tomuto postupu však relatívne bránia rôzne regulácie v oblasti zamestnanosti a daní. Preto oveľa efektívnejším spôsobom je využiť ponuku odborných spoločností, ktoré sa na trhu špecializujú práve na ochranu informačných aktív, t.j. použiť na vybrané procesy bezpečnosti obchodný model zvaný **outsourcing**.

Rozhodnutie o tom, ktorý proces je možné a vhodné outsourcovať, musí byť založené na pochopení hrozieb a životného cyklu incidentu od vzniku zraniteľnosti až po zotavenie sa z následkov prípadného incidentu.



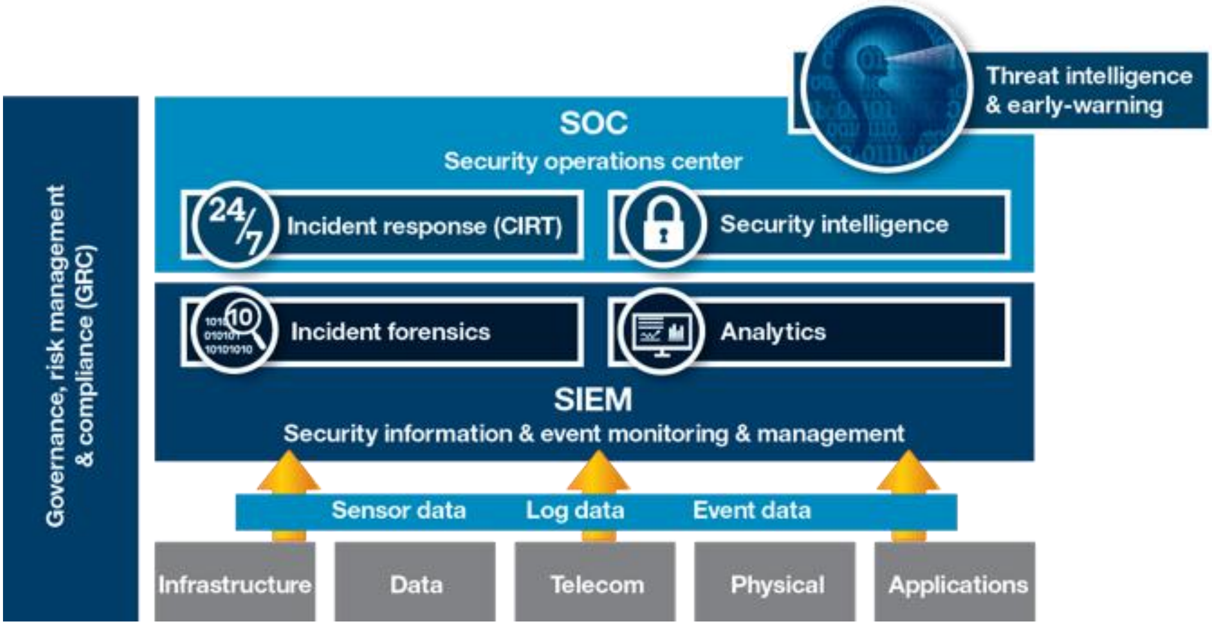
Životný cyklus incidentu začína jestvujúcou zraniteľnosťou, ktorá nezávisle od existencie zdroja hrozby a nezávisle od toho, či bola hrozba identifikovaná, prechádza do rizika s určitým dopadom a pravdepodobnosťou, že sa hrozba uplatní a z rizika sa stane reálny incident. Náprava následkov nechcenej udalosti a vyhodnotenie použitých postupov sú už len logickým ukončením životného cyklu incidentu.

A teda – ktoré časti tohto životného cyklu je možné v bezpečnostných procesoch outsourcovať? Odpoveď je triviálna: všetky...

Jediný proces, ktorý je nanajvýš vhodné ponechať si v podniku pod vlastnou kontrolou je riadenie informačnej bezpečnosti („information security governance“). V niektorých odvetviach, napríklad v bankovníctve, je outsourcing riadiacich procesov priamo zamedzený legislatívne, alebo nariadením regulátora trhu.

Stručne ku skratkám uvedeným v nadpise:

- Pokiaľ sú predmetom outsourcingu procesy, ktoré priamo súvisia s reakciou na bezpečnostný počítačový incident, tím, ktorý tieto procesy zabezpečuje sa nazýva **CERT** („Computer Emergency Response Team“). CERT je síce predovšetkým názov tímu, ale rovnaká skratka sa zvyčajne používa aj pre samotnú službu.
- Ak sú outsourcované aj procesy, ktoré majú súvis s hodnotením zraniteľností, znižovaním úrovne hrozieb a ošetrovaním rizík, potom sa jedná o proces zvaný **SOC** („Security Operations Centre“).
- A ak sú tieto služby poskytované zo strany tým spôsobom, že outsourcer sa „na kľúč“ postará o nejakú ucelenú časť IKT infraštruktúry podniku, používa sa názov Riadené bezpečnostné služby, so skratkou **MSS** („Managed Security Services“)



6 Záver

V organizáciách s vyššou komplexitou informačných systémov je nanajvýš vhodné, aby bol vopred ustanovený a priebežne školený špecializovaný tím, ktorého úlohou bude správne reagovať na identifikované incidenty, ktorý bude schopný včas prijať protiopatrenia, zabezpečiť zber dôkazov pre ďalšie vyšetrovanie incidentu a prípadné vyvodenie pracovnoprávnych, alebo trestnoprávnych dôsledkov. Formálna definícia typov udalostí, ktoré pre organizáciu znamenajú incident, je dôležitou vstupnou podmienkou pre zavedenie procesov riešenia počítačových incidentov. Avšak je to len prvým krokom zo série následných zmien procesov, ktoré by podniku mali zaručiť schopnosť efektívneho vysporiadania sa s rizikami, ktoré sa stali bežnou súčasťou modernej doby.

Schopnosť podniku efektívne pokryť bezpečnostné procesy, najmä procesy riešenia bezpečnostných incidentov môže byť podporená aj zo strany externých spoločností, zameraných na túto oblasť. Outsourcing bezpečnosti nie je nemožný. Je len potrebné citlivo zvážiť kvalitu a kvalifikáciu potenciálneho outsourcera a externú podporu bezpečnosti založiť na dobrých vzťahoch, optimálne aj zazmluvnených prostredníctvom Zmluvy o úrovni poskytovaných služieb (SLA) a Zmluvy o mlčanlivosti (NDA).

The Cyber Security Act – one year later
Zákon o kybernetické bezpečnosti – rok poté

Adam Kučínský

Adam Kučínský
a.kucinsky@nbu.cz

Adam Kučínský is a graduate of the Faculty of Law and Faculty of Economics and Administration Masaryk University. He deals with, among other things, crisis management and critical infrastructure. Before ending Master's degree at the Faculty of Economics and Administration, he started working for the National Security Authority, where he works at the National Cyber Security Centre. His main activity is the identification of critical information infrastructure, implementation of the Cyber Security Act and compliance audits.

Adam Kučínský je absolvent Právnické a Ekonomicko-správní fakulty Masarykovy university v Brně. Zabývá se, mimo jiné krizovým řízením a kritickou infrastrukturou. Před dokončením magisterského studia na Ekonomicko-správní fakultě nastoupil na Národní bezpečnostní úřad, kde působí v Národním centru kybernetické bezpečnosti. Jeho hlavní činností je určování kritické informační infrastruktury, implementace zákona o kybernetické bezpečnosti a kontrola plnění povinností z něj vyplývajících.

The Cyber Security Act – one year later

With the society's growing dependence on information technology, the criticality of failure and the growing number of cyber attacks there is a need to comprehensively address this issue. The Czech Republic recognizes these challenges and as the result, the National Cyber Security Centre (NCSC) was established. Accordingly the Cyber Security Act was adopted and is in force from 1st January 2015. Based on the fact that for some entities the transitional period has passed, the compliance audits for cyber security commenced. How is the Act implemented? What problems are the compulsory subjects facing and what are the experiences from the first audit? What can we expect from newly created European directive on network and information security (NIS) and what are the main differences compared to the current national regulations? All this will be addressed in the presentation.

Zákon o kybernetické bezpečnosti – rok poté

S rostoucí závislostí společnosti na informačních technologiích, kritičností jejich selhání a vzrůstajícímu počtu kybernetických útoků roste potřeba tuto problematiku komplexně řešit. Česká republika si je výše uvedeného vědoma a ve světle aktuálního vývoje se na tento fenomén připravuje. Z těchto důvodů bylo zřízeno Národní centrum kybernetické bezpečnosti (NCKB) a přijat zákon o kybernetické bezpečnosti, který je účinný od 1. ledna 2015. Některým subjektům spadajícím pod zákon již také uplynuly přechodné lhůty pro plnění povinností a v závislosti na tom byly spuštěny kontroly. Jak se zákon daří implementovat, jakým problémům po roce účinnosti povinné subjekty čelí a jaké jsou zkušenosti z prvních auditů? Co přinese nově vytvořená evropská směrnice o bezpečnosti sítí a informací (NIS) a jaké jsou hlavní rozdíly oproti současné národní úpravě? Na tyto i další otázky se příspěvek pokusí odpovědět.

1 Zákon o kybernetické bezpečnosti

Od 1. 1. 2015 je účinný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a jeho prováděcí právní předpisy – vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) a vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Současně s tím bylo novelizováno nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Těmito kroky byl položen právní základ pro ochranu životně důležitých informačních a komunikačních systémů. Česká republika se tak stala jednou z prvních evropských zemí, která zavedla takto komplexní legislativu věnující se oblasti kybernetické bezpečnosti.

Hlavním důvodem této regulace byla na straně jedné rostoucí závislost společnosti na informačních a komunikačních technologiích (ICT), jejich vzájemná integrace a rostoucí potenciál dopadů v případě jejich selhání např. kvůli vzrůstajícímu počtu kybernetických útoků. Na straně druhé pak absence povinných bezpečnostních standardů kybernetické bezpečnosti a potřeba zajištění koordinovaného postupu zajištění kybernetické bezpečnosti zejména u systémů důležitých pro stát. Cílem zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů je tak především stanovení základní úrovně bezpečnostních opatření a zlepšení detekce kybernetických bezpečnostních incidentů. Zákon proto zavádí pro určité subjekty povinnost hlášení kybernetických bezpečnostních incidentů, zavedení bezpečnostních standardů a upravuje činnost dohledových pracovišť, takzvaných CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team). Zákon vedle toho také zavádí systém opatření k reakci na kybernetické bezpečnostní incidenty.

2 Na koho zákon dopadá

Zákon o kybernetické bezpečnosti dopadá zejména na orgány a osoby (subjekty), uvedené v jeho § 3. Těchto skupin je pět a jedná se o:

a) poskytovatele služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací,

b) orgány nebo osoby zajišťující významnou síť,

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury,

e) správce významného informačního systému.

Pro přesné stanovení, kdo je povinným subjektem, je nutné jednotlivá ustanovení § 3 zákona o kybernetické bezpečnosti blíže rozebrat.

V případě poskytovatelů služby elektronických komunikací a subjektů zajišťující síť elektronických komunikací je potřeba vycházet ze zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Tyto subjekty určovány nejsou a při jejich identifikaci je nutno vycházet z definic uvedených v § 2 písm. f) a n) zmíněného zákona o elektronických komunikacích.

Orgánem nebo osobou zajišťující významnou síť je subjekt, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře. Podobně jako u předchozí skupiny povinných osob určování jako takové neprobíhá a subjekty se identifikují samy na základě definice. S jejich identifikací je spojen problém ohledně toho, že tyto subjekty často nevědí, že připojují prvek kritické informační infrastruktury, což je jedna z určujících podmínek.

Prvky kritické informační infrastruktury (dále také KII) podle § 3 písm. c) a d) určuje Národní bezpečnostní úřad (NBÚ) podle kritérií stanovených nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Proces určování probíhá podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Obecně se jedná o takové informační a komunikační systémy, jejichž narušení by mohlo mít závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku. Pro představu jsou to například systémy, na kterých jsou zcela nebo významně závislé další prvky kritické infrastruktury, např. elektrárny, přenosové soustavy elektrické energie, některé banky apod. Jde tedy o nejdůležitější systémy ve vztahu k základním funkcím státu, vyjma systémů souvisejících s obranou České republiky, na které se krizový zákon nevztahuje. Určování provádí NBÚ na základě oboustranných jednání se správci a na základě analýz takových systémů. Nemůže tedy dojít k tomu, že by byl prvek určen, aniž by o tom předem jeho správce věděl. Určování je rozdílné podle povahy subjektů. Kritická informační infrastruktura ve správě organizačních složek státu je určována usnesením vlády, kdy jeho neveřejná příloha uvádí seznam těchto prvků. Prvky KII ve správě ostatních subjektů pak určuje NBÚ opatřením obecné povahy.

Poslední skupinou povinných subjektů jsou správci významných informačních systémů (dále také VIS). Správcem VIS může být pouze orgán veřejné moci, přičemž podle § 3 odst. 2 vyhlášky 317/2014 Sb. významným informačním systémem není informační systém, jehož správcem je obec. Významné informační systémy (VIS) musejí mimo výše uvedené naplnit kritéria stanovená vyhláškou č. 317/2014 Sb. Zjednodušeně to jsou takové informační systémy, které jsou svou funkcí důležité, nicméně dopady jejich narušení nedosahují závažnosti určené krizovým zákonem pro kritickou informační infrastrukturu. Narušení bezpečnosti informací v těchto informačních systémech by pak mohlo omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci. V souladu s tím, nejsou jako VIS určeny systémy v soukromé sféře. Posouzení naplnění kritérií pro VIS provádí sám správce systému, který v případě naplnění těchto kritérií nahlásí kontaktní údaje NBÚ pomocí formuláře z přílohy č. 7 k vyhlášce č. 316/2014 Sb.

Aby tedy byl určitý systém určen jako KII nebo VIS musí splňovat určitá kritéria stanovená legislativou. Jednak to jsou kritéria určující míru závažnosti důsledků narušení těchto systémů (u KII se nazývají průřezová, u VIS dopadová) a dále odvětvová kritéria (u VIS oblastní), která vymezují pouze některé klíčové oblasti, které jsou pro stát resp. pro zajištění jeho společenských a hospodářských funkcí důležitá. Pro určení musí daný systém splnit z každé skupiny kritérií alespoň jedno.

3 Požadavky vyplývající ze zákona

Na povinné osoby klade zákon množství požadavků. Největší míra regulace se týká správců kritické informační infrastruktury a významných informačních systémů. Tyto povinnosti jsou blíže upřesněny prováděcí vyhláškou č. 316/2014 Sb. označovanou jako vyhláška o kybernetické bezpečnosti. Jedná se o opatření vycházející zejména z norem řady 27 000 o systému řízení bezpečnosti informací (ISMS) a metodik COBIT, CRAMM, RAMSES apod. Řada těchto opatření a zásad je využitelná pro všechny subjekty, které chtějí řídit bezpečnost informací a minimalizovat dopady rizik v oblasti kybernetické bezpečnosti, i když nejsou povinným subjektem ze zákona. Povinnosti, které subjektům zákon o kybernetické bezpečnosti ukládá lze rozdělit do čtyř skupin.

3.1 Hlášení kontaktních údajů

Základní povinnost, kterou musejí splnit všechny povinné subjekty. KII a VIS hlásí kontaktní údaje vládnímu CERT, který provozuje NBÚ. Vedle správců KII a VIS tuto povinnost musejí splnit i další dvě povinné osoby ze zákona o kybernetické bezpečnosti, tedy poskytovatelé služby elektronických komunikací a subjekty zajišťující síť elektronických komunikací a orgány nebo osoby zajišťující tzv. významnou síť. Tyto subjekty hlásí kontaktní údaje národnímu CERT, který v současné době provozuje sdružení CZ.NIC na základě veřejnoprávní smlouvy s NBÚ.

3.2 Hlášení kybernetických bezpečnostních incidentů

Zákon v § 8 zavádí povinnost hlásit kybernetické bezpečnostní incidenty pro orgány a osoby zajišťující významnou síť, správce kritické informační infrastruktury a správce významného informačního systému. Správci KII a VIS hlásí vládnímu CERT, zatímco významné sítě hlásí incidenty národnímu CERT. Vyhláška č. 316/2014 Sb. pak stanoví typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob jejich hlášení.

3.3 Zavedení bezpečnostních opatření

Správci KII a VIS jsou povinni v souladu s § 4 zákona zavést bezpečnostní opatření. Bezpečnostní opatření lze rozdělit na organizační a technická. Do organizačních opatření lze zahrnout zavedení systému řízení bezpečnosti informací, řízení rizik, zavedení bezpečnostní politiky, stanovení požadavků na dodavatele apod.

3.4 Podřízení se opatřením vydaným NBÚ

Vedle výše uvedených povinností zákon zavádí systém opatření, tedy úkonů, kterých je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou, incidentem, anebo pokud již incident nastane a je třeba jej řešit. Tato opatření zákon rozděluje na varování, reaktivní opatření a ochranná opatření. K vydávání těchto opatření je pověřen NBÚ. Zatímco varování jsou vydávána jako informace a povinné osoby se jimi řídit nemusí, u reaktivních a ochranných opatření je již vynutitelnost připuštěna. Ochranná i reaktivní opatření musejí provádět správci KII a VIS vždy, když jsou vydána. Zbývající dvě povinné osoby pak musejí provádět opatření reaktivní a to pouze za stavu kybernetického nebezpečí nebo za nouzového stavu.

4 Současný stav implementace zákona

Bezprostředně po vstupu zákona o kybernetické bezpečnosti v účinnost zahájil Národní bezpečnostní úřad určování kritické informační infrastruktury. Proces určování byl zahájen u organizačních složek státu, konkrétně u ministerstev a jiných ústředních správních úřadů. Výsledkem bylo určení prvních 45 prvků KII v květnu 2015. Následovala zbývající část státní správy a soukromý sektor. Tento proces stále probíhá a lze říci, že vzhledem k velmi dynamickému prostředí bude probíhat i v budoucnu.

V rámci určování KII proběhlo více než 170 jednání se státními i soukromými subjekty, na kterých byly posuzovány dopady v případě narušení bezpečnosti informací v těchto systémech a naplnění stanovených kritérií. Výsledkem těchto jednání bylo 19 opatření obecné povahy určující 50 prvků KII ve správě soukromých subjektů či státních podniků a dvě usnesení vlády určující 48 prvku KII v rukou 17 organizačních složek státu. Jde o kontinuální proces, který stále pokračuje.

Významné informační systémy jsou uvedeny výčtem v příloze č. 1 vyhlášky č. 317/2014 Sb. Současná příloha uvádí výčet 92 VIS ve správě 36 orgánů veřejné moci. Vedle toho zákon připouští možnost tzv. samoučení. Správce má povinnost posoudit, zda systémy, které spravuje, splňují stanovená kritéria pro VIS. V případě, že některé jeho systémy tato kritéria splní, má povinnost takový systém nahlásit. Na základě poměrně podstatných změn ohledně určených VIS od účinnosti vyhlášky č. 317/2014 Sb. je příloha č. 1 nyní novelizována a nachází se v Legislativní radě vlády. V současné době je evidováno cca 153 VIS ve správě cca 55 orgánů veřejné moci.

5 Kontrola plnění povinností u správců kritické informační infrastruktury a významných informačních systémů

Kontrolu v oblasti kybernetické bezpečnosti vykonává NBÚ. Úřad podle § 23 zákona kontroluje, jak orgány a povinné osoby plní zákonem stanovené povinnosti, případně povinnosti uložené v rámci reaktivních a ochranných opatření. Výkon kontroly se řídí zákonem č. 255/2012 Sb., o kontrole a probíhá podobně jako audit ISMS (Information Security Management System). Kontroly jsou prováděny na základě plánu auditu a jsou kontrolovanému oznámeny cca 14 – 30 dní před kontrolou. Před kontrolou jsou také poskytnuty informace o tom, jak se na audit připravit a kontrolovanému je zaslán předběžný program auditu. Program auditu obsahuje časový harmonogram auditních činností a na konci kontroly je upraven podle skutečného průběhu. Audit se zaměřuje na cca 100 – 150 kontrolních bodů z vyhlášky č. 316/2014 Sb. a je prováděn metodou vzorkování. Výsledkem kontroly je protokol obsahující případné nálezy. Jako první byly kontroly zahájeny u správců VIS, kterým již vypršelo přechodné období pro zavedení zákona. V jejich případě trvala kontrola cca 2 – 3 dny. U správců KII prozatím kontrola zahájena nebyla, neboť roční přechodné lhůty pro zavedení opatření ještě neuplynuly, ale podle předběžných odhadů by měla kontrola trvat zhruba 2 – 8 dní. Vždy však záleží na rozsahu kontrolovaného systému.

V prvním kvartále 2016 proběhlo 5 kontrol a bylo zkontrolováno na 382 kontrolních bodů. V průměru byly identifikovány 4 neshody na jeden subjekt. Mezi nejčastějšími auditními zjištěními převládají nedostatky formálního charakteru, jako je například neplatná či neřízená dokumentace, nedodržování interně stanovených postupů, nedostatečné řízení aktiv a rizik nebo nedostatky plánu zvládání rizik. Obecně lze říci, že spolupráce s kontrolovanými subjekty je na dobré úrovni. Kontroly dále pokračují i v druhém kvartále 2016.

6 Směrnice NIS

Stále rostoucího významu kyberprostoru i dopadů v případě narušení některých služeb, které poskytuje si je vědoma i Evropská unie. Již v roce 2013 byl předložen Návrh směrnice Evropského parlamentu a rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, tzv. směrnice NIS (dále jen směrnice). Cesta k vytvoření konečného znění této směrnice byla nicméně dlouhá a skončila až v letošním roce. Směrnice je vypracována a bude předložena ke schválení pravděpodobně v průběhu května tohoto roku. Směrnice vstoupí v účinnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie. Účinnost tedy lze předpokládat v srpnu tohoto roku, termíny se však mohou změnit. Lhůta na transpozici do národního práva činí 21 měsíců od účinnosti směrnice. NBÚ již začal s přípravou transpozice, probíhají analýzy shody s národní legislativou a analýzy dopadu. V tomto ohledu byla oslovena odborná veřejnost a partneři z řad státní správy.

Směrnice zavádí požadavky na bezpečnost a oznamování incidentů pro určitě vybrané informační systémy, které rozlišuje na dvě skupiny. Jsou jimi tzv. provozovatelé základních služeb a poskytovatelé digitálních služeb.

Provozovatelem základních služeb je podle směrnice subjekt poskytující službu, která je z hlediska zachování klíčových činností pro společnost nebo hospodářství základní a poskytování této služby je závislé na sítích a informačních systémech. Při hodnocení závažnosti dopadů incidentu v těchto službách mají členské státy zohlednit minimálně počty uživatelů závislých na dané službě, dopad na hospodářství, společenské funkce nebo bezpečnost, velikost obsluhovaného území, dostupnost alternativ a podíl na trhu. Odvětví, ve kterých podle směrnice provozovatelé základních služeb operují, pak uvádí příloha II. směrnice. Tato odvětví se částečně překrývají s odvětvími stanovenými nařízením vlády č. 432/2010 Sb. pro kritickou infrastrukturu, resp. kritickou informační infrastrukturu. Pro provozovatele základních služeb platí zásada minimální harmonizace, kdy si členské státy mohou stanovit přísnější povinnosti tykající bezpečnosti, než vyžaduje směrnice.

Druhou skupinou subjektů, které směrnice reguluje, jsou poskytovatelé digitálních služeb. Těmi jsou ve smyslu směrnice subjekty poskytující služby on-line tržiště, cloud computingu a internetové vyhledávače. Povinnosti vyplývající ze směrnice pro tyto subjekty jsou nižší než u provozovatelů základních služeb a mají být zavedeny přiměřeně s ohledem na míru existujícího rizika. Zároveň zde platí tzv. zásada maximální harmonizace, kdy subjekt nemůže být regulován přísněji, než dovoluje směrnice.

Směrnice dále ukládá členským státům vytvořit strategii pro bezpečnost sítí a informací, stanovit bezpečnostní požadavky pro zajištění bezpečnosti sítí a informačních systémů, ustanovit příslušné orgány v této oblasti a „skupiny pro reakci na incidenty v oblasti počítačové bezpečnosti“ atd. Je možné podotknout, že Česká republika má již množství povinností vyplývajících ze směrnice zavedeno a je nutné národní legislativní rámec upravit tak, aby byl se směrnicí plně v souladu. Směrnice se tak jeví jako vhodná zejména pro ty státy, které s kybernetickou bezpečností teprve začínají.

Zdroje

[1] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

[2] Zákon č. 240/2014 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

[3] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

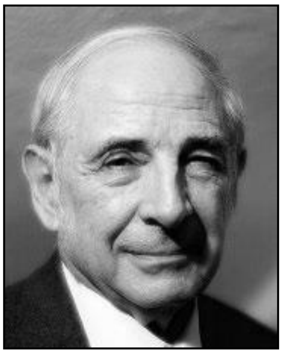
[4] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

[5] Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

[6] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

What is Information?
Informace ~ Informace?

John Rogers Searle



John Rogers Searle
searle@berkeley.edu

John Rogers Searle is an American philosopher and the Professor of Philosophy at the University of California, Berkeley. Widely noted for his contributions to the philosophy of language, philosophy of mind and social philosophy. He began teaching at Berkeley in 1959. He received the Jean Nicod Prize in 2000, the National Humanities Medal in 2004, and the Mind & Brain Prize in 2006. Among his notable concepts is the "Chinese room" argument against "strong" artificial intelligence.

John Rogers Searle je americký filosof a profesor filosofie na University of California v Berkeley. Je široce známý díky svým příspěvkům v oblasti filozofie jazyka, filozofie mysli a sociální filozofie. Na univerzitě v Berkeley začal učit v roce 1959. V roce 2000 získal cenu Jeana Nicoda, v roce 2004 Medaili národních humanitních věd a v roce 2006 cenu Mysl & Mozek. Mezi jeho pozoruhodné koncepty patří argument „čínského pokoje“ vůči tzv. „silné“ umělé inteligenci.

What is Information?

Just about all of the crucial notions in cognitive science are systematically ambiguous between an intrinsic, or observer-independent, sense and a derived, or observer-relative sense. In the intrinsic sense, all information is in conscious beings like us. The information in computers is like the information in books. It is all metaphorical or observer relative. The failure to understand these distinctions is responsible for a lot of horrible mistakes that I will correct in this talk.

Informace ~ Informace?

Všechny klíčové pojmy v kognitivních vědách jsou systematicky dvojznačné mezi přirozeným smyslem nezávislým na pozorovateli a odvozeným smyslem závislým na pozorovateli. V přirozeném smyslu jsou veškeré informace vědomé bytosti jako jsme my. Informace v počítačích je jako informace v knihách. Jsou zcela metaforické nebo závislé na pozorovateli. Nepochopení těchto rozdílů vede k mnoha hrozným omylům, které se budu snažit napravit v mé prezentaci.

Modern Security Operations in Bank Sector
Moderní provoz bezpečnosti v bankovním sektoru

Roland Supper

Roland Supper
roland.supper@googlemail.com

Roland Supper graduated from the University of Applied Sciences in Vienna. He then started to work as a network and security specialist in the finance sector. Since 2010, he has been employed with s IT Solutions Spardat GmbH, the IT provider of Erste Group and saving banks in Austria, where he built up the Critical Incident Response Center (CIRC) and currently holds the post of the CISO. As such he is responsible for Security Operations (SecOps), steering people, processes and tools, necessary to secure data for one a systemically important financial institute in Austria. Heading the department Cyber Defense Center, he is also leading the Erste Group competence center Security Operations & Workplace Security. Additionally, he is working as lecturer at the University of Applied Sciences in Vienna, teaching bachelor and master degree students in the field of IT Security.

Roland Supper vystudoval Universitu aplikovaných věd ve Vídni. Poté působil jako síťový a bezpečnostní specialista ve finančním sektoru. Od roku 2010 pracuje ve společnosti IT Solutions Spardat GmbH poskytující IT služby finanční skupině Erste Group. Zde vybudoval CIRC (Centrum kybernetické bezpečnosti) a zároveň zde zastává roli CISO. Je zodpovědný za provoz v oblasti kybernetické bezpečnosti a koordinaci všech nezbytných zdrojů, procesů a nástrojů pro systematické zabezpečení dat významné finanční instituce v Rakousku. Je také zodpovědný za vedení kompetenčního centra „Security Operations“, které zajišťuje expertní služby pro všechny centrální infrastruktury i koncová zařízení v rámci celé skupiny Erste Group. Dále přednáší IT bezpečnost pro studenty bakalářského a inženýrského programu na Universitě aplikovaných věd ve Vídni a je aktivním členem rakouského „Trust Circle“ (Tým spolupráce ve financích při CERT.at a rakouského spolkového kancléře).

Modern Security Operations in Bank Sector

Nowadays the financial sector is facing an intense increase of new regulations from different authorities as the European Central Bank, local finance market authorities, or the EU cyber security agenda, especially in the field of cyber security. To comply with this regulations, it is essential to evolve from traditional defenses to active incident response. Understanding the actual situation at the banking market and the need to uprate their core business into a digital one, SecOps responsibilities must detect and react in time at threats and determine between small security incidents and real data breaches within minutes. To cope with this challenging situation, it is prerequisite to bundle up resources and cooperate close with internal and external entities to share knowledge and experience. This talk focus on aspects and best practice methods for modern security operations at the bank sector, and points out a wide range of changes and the need for a paradigm shift for existing cyber security strategies.

Moderní provoz bezpečnosti v bankovním sektoru

V současné době je finanční sektor pod intenzivním tlakem bezpečnostních hrozeb a také nových regulací v oblasti kybernetické bezpečnosti od různých autorit – od Evropské centrální banky, národních regulátorů nebo i EU Kybernetické agendy. Udržet krok s těmito trendy znamená posun v oblasti kybernetické bezpečnosti od tradičních „obranných“ opatření k „aktivnímu“ způsobu práce... Bankovní sektor se navíc stává více digitálním a týmy, které se starají o provoz bezpečnosti (SecOps), musejí včas rozpoznávat a reagovat na nové hrozby, rozlišovat mezi malými incidenty a skutečným útoky či závažnými úniky dat, a to vše během několika minut. Nezbytným předpokladem pro zvládnutí této náročné situace je sdružit všechny dostupné zdroje, úzce spolupracovat s interními a externími subjekty a využít všechny dostupné znalosti i zkušenosti. To však významně mění paradigmata tradičně užívaná v oblasti kybernetické bezpečnosti do nového a moderního stylu provozu kybernetické bezpečnosti v bankovním sektoru.

1 Challenges for Security Operations in Finance

Over the last decade, the security landscape for the finance industry has changed dramatically. Having branches in every bigger village, close physical presents to customers in the region and dealing with physical assets (cash, gold, credits, properties…) have been the typical business activities of banks in the past.

In the back office of course, the finance industry has ever been a driver of automatization, continually expanding their computer capacities (#mainframe) to be able to handle more and more complex finance operations in less time.

Today, the crown jewels of banks have changed in most cases from physical to digital assets. The branch network of banks is constantly down sized, retail customers are urged to use digital media for their business with the bank, including online counseling talks and completion of deals. Protecting these channels in a fully digitized environment with a very fast changing and complex security landscape, can be very challenging for each service provider in the finance industry.

1.1 Cyber Security Challenges

The evolvement from standard malware threats, used by individuals and distributed randomly all over the world, towards highly organized groups of experts executing targeted attacks against individual companies, is for sure one of the trigger for rethinking the own cyber defense strategy. Following a short excerpt of some of those challenges:

1.1.1 Sophisticated Malware

The fact that traditional Anti-Virus (AV) software is not able to detect and block each single malware thrown on it, is well known. But why is it that difficult for AV systems to fight these threats?

One of the reasons is, that most AV's rely on a signature based detection engine. If we analyze the ecosystem of malware code writing, it quickly comes up that the base code can utilize a series of hiding technics, such as cryptors, protectors, packers or binderns. Each iteration leads to a changed code, which makes it even more difficult for signature based AV's to detect this.

In the past, well prepared phishing campaigns have come up with fast changing attack vectors (word, pdf, web-link, dropbox-links). The delivered malware code and the dropzone IP's are typically changed within 24-48 hours. This makes it very hard for traditional AV's at the perimeter (mail, proxy,…) and at endpoints (clients, servers) to fight such kind of malware.

A rising and very aggressive malware family is Ransomware. This type of malware uses similar methods to distribute itself (phishing), but uses additional distribution methods as well (drive by downloads, social media, …). Annoying enough that it is very hard to block this kind of malware, which will encrypt the data at the client and your connected network shares, in most cases there is currently no way to break this strong encryption. Nobody want to pay a high amount of bitcoins to the kidnapper, so hopefully you can draw on good backup mechanisms.

1.1.2 Fraud

As mentioned in the introduction, the bank business is more and more digitized. This change in the finance industry, means also a shift from bank robbery towards online fraud practices. We can distinguish between several different types of fraud.

Customer fraud targets the digital wallets of bank clients, mostly using phishing mails as entry point to drop sophisticated malware, which is able to manipulate transactions. More advanced attacks include social engineering components (#VHISHING) which trick the client into disclose sensitive information or to click on suspicious links. To compete with two-way authentication technics, modern malware infects not only the PC/laptop, but moreover the mobile device as well.

Another type of this category are insider threats. With a link to dissatisfied employees with access to transaction systems, or privileged users (administrators) those who can access sensitive systems and data, insider fraud is very challenging to handle for any security department. Often such a fraud case hit the IT out of nowhere if suddenly the internal Audit department knocks on the door, hand in hand with public prosecution and request very detailed information (logs on every layer).

But the fraud category can be extended for one more very interesting category, named CEO fraud. This type of fraud describes a technic to trick the accounting department into authorizing one or more transactions, by simply send mails from (CEO, CFO,…) and to the right persons (accounting department). To be successfully, the attacker need to know a lot of inside information regarding the used wording, processes and names of usually involved people. But in companies with unregulated procedures and with the help of social engineering technics, a lot of such fraud cases have been made public in the past.

1.1.3 Advanced Persistent Threat

The most complex and challenging threats are traded under the name “Advanced Persistent Threats (APT)”.

In that scenario, “Advanced” stand for a well organized group of individuals, which are funded by organizations or even nations. These attackers are able to research and make use of unknown vulnerabilities (0-day exploits) which are nearly undetectable by traditional security measures. Most often, such groups combine multiple attack methodologies, including social engineering, to gain access to the information they are looking for.

“Persistent” indicate a low and slow approach, which generate just as little noise (alerts, logs, etc.) as possible to stay stealth and invisible for a long time. Short after the initial breach, the attackers will try to install backdoors, which grant them easy access to the network at any time. After that they will start with lateral movement, exploit different vulnerabilities at different servers/clients (or obtain a Kerberos golden ticket at worst), until they can access the data they are looking for.

The last word in the APT acronym is “Threat” and points to a high level of coordinated human involvement. In contrast to single attackers, the APT group is composed of several very skilled, highly motivated and well organized (well-paid) individuals.

This combination makes APT attacks very sophisticated and hard to detect. Most breaches led to data compromise within days, but it can take weeks or more to discover the breach.

1.2 Regulatory Challenges

It’s not only a matter of external or internal threats what makes nowadays security operation challenging, but there are a range of conditions all around, which can influence this.

1.2.1 Compliance

To be compliant with regulators is mandatory for IT providers in the finance industry. International Standard on Assurance Engagements (ISAE) No. 3402, assurance reports on controls at a service organization for example. Another common standard if you deal with card holder data is the Payment Card Industry Data Security Standard (PCI DSS). Both standards introduce a series of controls with the need of (long term) evidences, which must be proven to authorities at a certain time.

This means a high amount of effort not only for the responsible department, but also for any security operation entity. For example, one need to proof that signatures are up to date, systems are hardened according to the regulation and evidences must be kept for a certain time.

1.2.2 External Directives

Data Protection

There are different views on the topic data protection, which need to be discussed. On one hand, it is important to ensure that all customer and employee data are protected under valid laws (EU Data Protection Directive 95/46/EC and other local laws). To ensure this protection, security must be enforced at different layers which will increase the effort not only in operations (guidelines, regulations and policies are equally important).

On the other hand, if security operation entities must be able to protect the infrastructure and detect any kind of threats, there will be the need to intercept (SSL) encrypted traffic to do so. In that case, operators are able to read even data, which fall under this kind of laws. Modern security operation must be able to deal with that and provide agreements with the worker's council and data privacy office (DPO) as well as ensure data protection standards on a technical level (e.g. tokenization of sensitive data).

NIS Directive

The Network and Information Security (NIS) directive is an EU initiative with the goal to improve local (member states) national cyber security capabilities. Regardless that the final version is not approved yet, the text indicates lots of additional measures as well as the need to report security incidents in a certain matter of time.

To fulfill this and other directives, it is mandatory that companies in question run a security operation organization, which have the necessary tools, processes and people in place.

2 Traditional Security Practice

During the last years, the security protection in most organizations was subjected to a constantly improvement process. Typically, tools were deployed to protect online services (web, mail, DNS) as well as servers and endpoints. Dividing the network into different segments, segregate clients from server networks, put critical assets into DMZs and split solutions into application-, web- and database layers is common sense today.

If one divides nowadays protection capabilities into perimeter and endpoint security, the following solutions can be assumed as minimum security standard.

2.1 Perimeter Security

At the first line of defense one will often find at first solutions to mitigate Distributed Denial of Service (DDoS) attacks, targeting online (banking) infrastructure. This can be on-premises appliances, cloud based protection solutions or mixed services (depending on the infrastructure). Such solutions must be able to detect a composure of different attack vectors, ranging from simple floods, attacks against the DNS service, to sophisticated application-layer attacks within SSL protected services. High volume attacks can reach bandwidths up to several hundred Gbps, where the help from big backbone ISP providers could be necessary.

Network based Intrusion Prevention and Detection Systems (NIDPS) are meanwhile also counted to a minimal perimeter protection. They are deployed inline (no IP at the protection interfaces) and in "blocking mode", but not only at the boarder to the internet, but also at critical network perimeters within the datacenter. They are usually deployed between client and server networks, card data processing areas (needed for PCI DSS compliance) and other critical network areas.

If it comes to classic firewalling (up to OSI layer 4), these solutions are not seen as a sufficient protection solution any more. Nevertheless, firewalls are indispensable for establishing zone concepts, protection against spoofing attacks and guard services from unauthorized access.

2.2 Endpoint Security

It does not matter how strong your perimeters are protected if you don't protect your endpoint (clients, server, ATM's,) and peripheries (printers, building services, etc.) accordingly. Traditionally an Antivirus is deployed since long time, but an AV can't protect vulnerabilities at the endpoints from being exploited, nor defend the data at endpoints from fraudulent insiders or protect the device when it is operated outside the secured company network.

The minimum standard for endpoint protection comprise beside AV and FW, a well configured Host Intrusion Detection and Prevention (HIDPS), encrypted hard disk, and a Data Loss Prevention (DLP) solution.

The HIDPS can help to protect a system from exploits targeting (known) vulnerabilities. This is very important in use-cases where employees can plug in unknown thumb drives, need to working with public Wi-Fi networks or connect to encrypted cloud services, where your perimeter protection is maybe not able to look inside.

A use-case for DLP can be to protect endpoints from losing data by "accident", where employees send data to their private mail account, favorite collaboration service or simply copy it to a USB thumb drive to be able continue the work from home. A DLP solution can also help to build awareness if it just come up with a warning dialog when a user tries to upload files (e.g. a dump file uploaded in a support case can include very sensitive information).

Today, lot of finance institutions have these minimal security measures in place, commonly operated from different responsible entities, with more or less coordinated effort behind the operation.

If it comes to a more modern security operation, it is not only needed to extend the visibility to get an overall picture, but to strengthen the cooperation and bundle up for a strong team of experts with deep insight knowledge. Right after this organizational change, the security operation unit will be in a condition to understand the whole cyber kill chain of ongoing attacks and response with the right action.

3 Modern Security Operations

To act on the assumption that IT providers invest a good amount of money in protection solutions as described in the previously chapters, if one wants to compete with new threats, it's self-evident to furthermore think about shifting resources.

If we split the resources into the areas "prevention", "monitoring" and "response", the investment focus was up to 80% into prevention technologies, 15% in monitoring capabilities and only 5% in response actions in the past (self-reflecting my own experience). To be able to fulfil modern security operation tasks, there is the need bring the resources more in line with each other (e.g. 33% prevention, 33% monitoring, 33% response capabilities).

In the end, we established a solution framework for Security Operations (SecOps), composed of Technology, People and Processes.

The SecOps solution framework should ensure surrounding conditions to provide services for defense-in-depth, threat intelligence as well as operations and reporting capabilities.

3.1 Technology

Heart of the technology part is a next generation SIEM system, which is able to fulfill the following features.

3.1.1 Deep Network Analysis

The system monitors incoming and outgoing network traffic to answer simple questions like "what entered and what left the company network?". Further must it ensure to detect known as well as unknown threat communication and have the ability for network forensic (full packet capture for a certain period, meta data for long time retention). To fulfil this, external feeds must be subscribed from different sources, which can enrich the network metadata with information, that can help the SecOps unit to follow hints and detect unknown threats.

3.1.2 Advanced Log Monitoring

When security systems are operated in different departments with different responsibilities, it is inevitable to collect all those logs/events and process into one system. Imagine thousands of "low/medium/high" alerts at each single security solution (NIPS, HIPS, AV, DLP, Active Directory, Radius, AAA,…) a day – no operator is able to handle that without having an overall picture of what is going on. To have the continuing ability of correlating network and log data together, complex event processing can be realized.

3.1.3 Enhanced 0-day Malware Analysis

Out of the captured network traffic and enriched with external feeds and indicators of compromise (IOC), the system must be able to extract suspicious files and sandbox it for further analysis (inline or for later analysis) or block it bevor reaching the employees system.

3.1.4 Fraud prevention

Protect customer bank accounts from losses through malware, it is very important to have capabilities for detecting such threats bevor money get lost. This needs the involvement of transaction monitoring or even code injected in the transaction pages to examine if malware is trying to hijack the browser at a customer PC or the APP running at their smartphones.

To be able to prevent the company from insider threats, the SecOps unit must have the capability for user behavior monitoring. With this technique, advanced threats will be comprehensible and hidden behavior visible. Using machine learning algorithms to anonymized metadata is precondition to not violate employee privacy.

3.1.5 External Threat Intelligence

All of above tools and solutions are focusing on preventing the institutions infrastructure from being hit by security threats. But when it comes to learn about the current threat landscape, being able to react in time on upcoming threats, or the need to know which malware family is currently targeting the bank customers, an External Threat Intelligence service is very important. Such a service can monitor underground networks (e.g. darknet websites) for already stolen customer login credentials or credit card numbers currently dealt, hacker groups discussing when to plan the next big DDoS attack against own finance services or which new malware is under development.

On the very top of this set of tools, there is the need for an umbrella framework to handle alerts, trigger processes and security procedures. Such a framework shall include all available asset information (clients, server, router, printer, ATMs, …) from the company (#CMDB) as well as the (business) solution setup the assets belongs to, and the contact details of the administrator who is responsible for. If an alert is triggered by the system, an automatically opened incident can correlate for example the source IP address with the corresponding solution and contact details from business owner and administrator.

3.2 People

A modern security operation center (SOC) is typically staffed with people on different skill set, ranging from network experts to malware reverse engineering. Therefor a layered operation architecture is common. “Tier 1” analysts take alerts, enrich them with additional information and follow predefined procedures to handle the incident. If they are not able to handle it by their own, they can escalate the incident ticket to higher skilled “Tier 2” analysts. In some cases, when it comes to advanced threats or unknown malware, the advanced skills of the “Tier 3” analyst could be needed (e.g. malware reverse engineering). “Tier 1” and “Tier 2” analysts must be onsite and having a very good understanding of the complex application landscape of a finance institute, but because a “Tier 3” analyst shouldn’t be necessary each day, this special service can also be offered through an external partner.

Needless to state, that there is the need for an ongoing educational program, where all analysts are able to extend their skills and go alongside with up to date security trends.

3.3 Processes

To handle tools and alerts, a mature Security Operations Management is mandatory. The management setup includes policies and handling procedures for Tier 1, Tier 2 and Tier3 operators, to help them during analyzing and fast right handling of security incidents.

Having a good understanding about duties and the area of responsibility, ensures efficient operation capabilities. In some cases, it is needed to involve stakeholders (business) to make decisions like shutting down services or segregate network segments to curtail more damage.

4 Level od Ambition

To complete the thoughts of modern security operations, a strategic view at some more areas is advisable.

4.1 Business Awareness

To continue with that high standard of defense technologies and people in SecOps, the business owner must be kept informed about a changing threat landscape at a regular basis. On the other hand, developers, project managers and infrastructure operators shall involve security experts at a very early stage while building new solutions/services.

If new services are secured by design and benefit from existing measures, intruders will have a much harder job to reach their goals.

4.2 IT Risk Management

A side product of modern SecOps is the visibility of existing vulnerabilities in applications or infrastructure. To get the needed attention of stakeholders for closing this findings, a valid IT Risk Management processes can be useful. Introducing such structures can help to build a bridge between security gaps and the budget owners while using a "common language". In the end, the CEO will be responsible for any damage when he/she is not willing to spend money for closing proper documented "high" risks.

4.3 Strong Network

Providing a well-functioning platform for exchanging information with other (finance) institutions at a trusted level, provide a very good opportunity for sharing know-how about new threats seen in other organizations. With that knowledge, the security operations unit can prepare them self for similar threats and will have a big advantage in time.

4.4 Incident response

Another important strategic goal is the ability for incident response and counteract measures. In that case it is not meant to "hack back", but there are technologies on the raise which allows to prepare e.g. documents, that can "call home" if opened by the attacker.

This can be very helpful when intruders gain access to files or intercept communications to instruct fraudulent transactions. If the SOC have the ability to "hand over" such a prepared document to the intruder (e.g. place it nearby sensitive documents, send one more mail during an ongoing CEO fraud communication,..) and the intruder opens this document, the real IP address and more information can be revealed. This information can then be forwarded to official authorities who handle this case.

From hacker's diary...
Z deníčku hackera...

Pavol Lupták

Pavol Lupták
pavol.luptak@nethemba.com

Pavol Lupták is CEO, Certified IT Security Professional. He gained his BSc. at the FEI-STU in Bratislava and MSc in Computer Science at the Czech Technical University with master thesis focused on ultra-secure systems. He holds many prestigious security certifications including CISSP and CEH, he is Slovak OWASP chapter leader, co-founder of Progressbar and SOIT organizations where he is responsible for IT security. Pavol uses to have regular presentations at various worldwide security conferences (in Netherlands, Luxembourg, Berlin, Warsaw, Krakow, Prague). In the past, he demonstrated vulnerabilities in the public transport SMS tickets in all major cities in Europe, together with his colleague Norbert Szetei he practically demonstrated vulnerabilities in Mifare Classic RFID cards. He has 14 years experience in IT security, penetration testing and security auditing including social engineering and digital forensic analysis. He is co-author of the OWASP Testing Guide v3, has a deep knowledge of the OSSTMM, ISO17799/27001 and many years experience in seeking vulnerabilities. He has a knowledge of many programming languages (ASM, C, C++, XSLT, Perl, Java, PLSQL, Lisp, Prolog, scripting languages) and operating systems. He is also focused on VoIP and interesting IT security research.

Pavol Lupták je výkonný ředitel, certifikovaný bezpečnostní specialista. Vystudoval FEI-STU v Bratislavě a FEL-ČVUT v Praze obor informatika s diplomovou prací zaměřenou na ultra-bezpečné systémy. Je držitelem prestižních bezpečnostních certifikací CISSP a CEH, vede slovenskou OWASP pobočku. Je také spoluzakladatelem organizací Progressbar a SOIT, kde vede sekci pro IT bezpečnost. Pavel má pravidelné prezentace na různých světových bezpečnostních konferencích (Nizozemsku, Lucembursku, Berlíně, Varšavě, Krakově, Praze). V minulosti demonstroval možnost zneužití SMS jízdenek ve všech velkých městech Evropy, spolu s kolegou Norbertem Szeteiom demonstroval masivní prolomení čipových karet Mifare Classic. Má čtrnáctileté zkušenosti v oblasti IT bezpečnosti a penetračního testování a tvorby nejrůznějších bezpečnostních auditů včetně sociálního inženýrství či forenzní analýzy. Je spoluautor testovací příručky OWASP Testing Guide v3, detailně ovládá OSSTMM, ISO17799/27001, má dlouholeté zkušenosti s manuálním vyhledáváním zranitelností a různými bezpečnostními nástroji. Ovládá množství programovacích jazyků (ASM, C, C++, XSLT, Perl, Java, PLSQL, Lisp, Prolog, skriptovací jazyky) a operačních systémů, věnuje se také VoIP a zajímavému výzkumu v oblasti IT bezpečnosti.

From hacker's diary...

Since 2007 when Nethemba was started, we have begun to focus on public research projects. One of the reasons was that we were aware of a lack of security in technologies most people use daily, the second one, was a need of being different compared to our IT security competition, especially in Czech and Slovak republic. During the period 2007-2015, we published many security-related articles, blogs, and papers.

The most important ones with the considerable impact were the following four projects:

1. SMS public transport ticket vulnerabilities.
2. Mifare Classic vulnerabilities and implementation of Mifare Classic Offline Cracker.
3. SMS parking ticket vulnerabilities.
4. Security analysis of Slovak and Czech NFC payment cards.

The goal of the presentation is to introduce these projects briefly.

Z deníčku hackera...

Náš tým se již od roku 2007 zabývá veřejnými výzkumnými projekty. Primárním motivačním faktorem byla absence bezpečnosti v technologiích, které většina lidí denně používá, druhým důvodem pak byla potřeba se odlišit od konkurenčních společností na poli IT bezpečnosti, zejména na trhu v České a Slovenské republice.

V období let 2007-2015 jsme publikovali a dali k dispozici množství článků, blogů a dokumentů na bezpečnostní téma. Mezi nejdůležitější a ty s největším dopadem by bylo možné zařadit tyto čtyři projekty:

1. Zranitelnosti systému SMS jízdenek pro veřejnou dopravu.
2. Zranitelnosti Mifare Classic a implementace nástroje Mifare Classic Offline Cracker.
3. Zranitelnosti systému SMS parkovacích karet.
4. Bezpečnostní analýza implementovaných NFC patebních karet na Slovensku a v Česku.

Cílem prezentace je představení výstupů z těchto projektů. Mnohé z uvedených technologií jsou dodnes používány, a to i pro nové projekty. Doufáme, že přednáška bude určitým příspěvkem k zviditelnění problému a následná veřejná diskuse na toto téma pak umožní rizika pro cílové uživatele těchto projektů snížit.

1 Introduction, our reasons & motivation

Since 2007 when Nethemba was started, we have begun to focus on public research projects. One of the reasons was that we were aware of a lack of security in technologies most people use daily, the second one, was a need of being different compared to our IT security competition, especially in Czech and Slovak republic. During the period 2007-2015, we published many security-related articles, blogs, and papers. We would like to discuss the most important ones with the considerable impact.

2 SMS public transport ticket vulnerabilities

SMS tickets are widely used in all large cities in Central Europe (Prague, Bratislava, Košice, Vienna, Warsaw, ..). Using a simple SMS message (e.g. "DPT") sent to a predefined number, you can receive a valid SMS public transport ticket, e.g. "*Price XYZ, Validity: from 28.10.07 13:20 to 28.10.07 14:50, code YrQPtMKs7 /52845*". The critical security issue lays in an absence of the connection between user's identity and his SMS ticket's identity. Therefore, SMS ticket can be shared by a community without any technological problems, despite the fact that legislatively it is prohibited to generate and distribute copies of personal SMS ticket. In our research, we have shown there is almost no way to detect these duplicates or the detection would be very expensive. We've also shown that an arbitrary SMS message can be locally generated on every current smartphone with the predefined sender, recipient, body, and status flag ("Not-Read-Yet"). Therefore, they are visually indistinguishable from the original ones. We have proposed two ways of "valid SMS ticket" distribution. One using SMS channel (it is publicly available, but too expensive with the impossibility to modify SMS headers) and the second one using TCP/IP (very cheap, but requiring a prepaid mobile data service and a smartphone which has to be capable of generating local SMSes). We have designed and described a communication architecture including SMS hack clients and servers. We've also described the following security workarounds implemented by public transport company that can by bypassed by our proposed circumvention methods:

Potential security fix (by public transport company)	**Circumvention method (suggested by us)**
Public transport inspector can look for duplicate SMS tickets (if two or more people use the same ticket, it is cleared that the shared ticket is used and distributed).	Regeneration of already checked tickets (in case the inspector looks for duplicate SMS tickets or uses sophisticated geographic correlation). It can be done fully automatically using passenger's geographical collision detection. SMS hack clients will send the passenger's current location to the central SMS hack server that will evaluate possible collisions and invalidate "collision" SMS tickets and ask for the new valid ones.
Public transport service can use sophisticated geographical correlation systems to reveal that one SMS ticket is used in a short time in multiple places that are too far from each other.	Mandatory regeneration of already checked tickets.
The inspector makes a call to the SMS ticket sender (because he knows his number).	Use GSM card / Asterisk VOIP call center on the central SMS hack server, if any call to this number is detected, Asterisk will make a call to all participants/clients (and only the right one

	will pick up it).
The inspector sends a verification. SMS to the SMS ticket sender (because he knows his number).	If the inspector's verification SMS message is received by the central SMS hack server, this SMS is redistributed to all participants/clients with properly applied caller ID spoofing.
The inspector can ask the user to make a call to his predefined number (and he checks if the same sender number is used that was used for the SMS ticket request).	The black passenger can run his special application that makes VOIP call through the central SMS hack server to the inspector phone – the inspector will see the same number that was used for SMS ticket request.
The inspector can ask the user to send him an SMS verification (to verify if the user number is the same as the sender number that was used for the SMS ticket request).	The black passenger can run his special application that sends this SMS verification message through the central SMS hack server, so the inspector will see the same sender number that was used for the SMS ticket request).
Public transport service can reveal that many SMS ticket requests are sent from the same number. Consequently, it can blacklist this number and reject all SMS tickets requests.	Change of SIM/mobile number periodically (SIM cards/unique numbers can be bought completely anonymously in the Czech Republic or Austria). Use of multiple SIMs/mobile numbers in the central SMS hack server. Use private P2P mobile networks.

There still can be a single point of detection – the central SMS hack server uses the unique and still same phone number – this phone number can be easily detected and blacklisted. In this, each SMS hack client should also have its SMS sending server. Thanks to this the proposed architecture can be fully decentralized with no single point of detection – every client participates in sending of SMS ticket requests – P2P mobile network cannot be easily blacklisted.

We have described two security fixes which are too expensive to implement:

5. **Using IMEI for passenger identification** (we can bind the passenger's IMEI with his SMS ticket (after his proper registration).
6. **Geographical localization of checked passengers** – we need to know the response to a question: “Is a just checked passenger sufficiently closed (in a defined distance) to the inspector?” It requires cooperation with GSM/3G operators (they have to provide the name/position of the BTS the passenger or inspector). It may be a big privacy issue and too expensive.

The only viable and secure solution we have proposed was the registration of all new users with their birthdate or ID number (personal ID or passport). We have described two different ways – the one using public, the second using symmetric cryptography. The final verification should be quite easy to use – the inspector just scans the personal ID document and visually compares the result of his PDA with the given SMS ticket. The inspector's PDAs should support automatic personal ID scanning (e.g. using QR codes).

More information is available in our paper Public transport SMS ticket hacking[1].

Few years after our public release, the iOS and Android version of the application FareBandit[2] was published, allowing anyone to share his or her SMS public transport ticket. It is a quite simple application, and it does not implement most of our described functionality, but despite this fact, it is still widespread used by many black passengers in Central Europe.

Despite the fact that public transport companies have already been informed about this serious vulnerability, they ignore this fact and still use the vulnerable systems. We are not aware of any public transport SMS tickets which are not vulnerable to this kind of attacks.

3 Mifare Classic vulnerabilities and implementation of Mifare Classic Offline Cracker

Mifare Classic represents one of the most used RFID cards (more than a billion smart card chips are used). It is based on ISO/IEC 14443 Type A, 1kB or 4kB and uses 13.56 Mhz contactless smart card standard. It uses a proprietary CRYPTO1 with 48 bits keys. Historically this technology had many security problems in the past. In Czech/Slovak Republic this technology was used by all University/ISIC/Euro26 cards, public transport ID (“električenka”) in Bratislava, Slovak Lines, Slovak railways cards, parking cards, swimming pools or skiing resorts. Mifare Classic security was based on readonly Unique Identifier (UID), mutual authentication between reader and writer and encrypted communication, CRYPTO1 nonpublic algorithm implementation and some other elements. The set of Mifare Classic commands is quite limited – *authenticate, read, write, increment, decrement, transfer,* and *restore*. We have revealed a lot publicly used cards (even in Czech Republic and Slovakia) used at least one block encrypted with the default keys (i.e. 0xffffffffffff, 0xa0a1a2a3a4a5, 0xb0b1b2b3b4b5, 0x4d3a99c351dd, 0x1a982c7e459a, 000000000000, 0xd3f7d3f7d3f7 and 0xaabbccddeeff), so these blocks can be easily read by NFC tag reader.

The fundamental problem of Mifare Classic security was a pseudo-random generator that is defined by the polynomial x^16 + x^14 + x^13 + x^11 + 1, also called LFSR. Despite its length of 32 bits, it has only 16 bits entropy. This random generator was used for generation of “random” nonces that were consequently used for a mutual authentication between the RFID card and RFID reader. Despite the existence of various other attacks to Mifare Classic technology (e.g. “timeout” attack), we have decided to implement “Nested Attack”.

This attack can be described by four following steps:

7. Authenticate to the block with default key and read tag's Nt (determined by LFSR).
8. Authenticate to the same block with default key and read tag's Nt' (determined by LFSR) (this authentication is in an encrypted session).
9. Compute “timing distance” (number of LFSR shifts).
10. Guess the Nt value and authenticate to the different block.

The proposed attack works with Mifare Classic cards with at least one default block. This block encrypted with default keys can be quickly revealed by many NFC Android-based applications or by our released tool – Nethemba Mifare Offline Cracking Tool – MFOC [2].

Revealing all keys from Mifare Classic often makes possible cloning. When all keys are gained, every card can be easily cloned; it is possible to make 99.6% clone (except 0.block in 0.sector that contains readonly UID, in these days it is possible to buy in Chinese shops even Mifare Classic with rewritable UID). All these blocks (including UID!) can be 100% emulated by Proxmark3 or by any other card emulator. Proxmark3 is a general purpose RFID tool designed to snoop, listen and emulate everything from LF (125kHz) to HF (13.56Mhz) tags, it is a universal hacking RFID device.

Our MFOC implementation has been tested using very cheap (30 EUR) TouchTag RFID reader (ISO14443a 13.56 Mhz NFC reader).

For our “nested offline” card attack implementation we have used an open library Crapto1 that can be used for cracking Mifare Classic initial authentication handshake.

Unfortunately, we see a lot of practical applications of Mifare Classic (especially in public transport/transport companies) that use a sensitive information, e.g. “credit” physically stored on the card. Even if there is some complex crypto solution used for encryption/signing the credit, it is possible to make a full dump of the card (after charging the credit) and after spending some credits just restore this made the dump with the original credit (UID remains the same one). We have proposed three countermeasures for this situation:

- Countermeasure #1 – use safer cards (Mifare Plus/DESFire or other).
- Countermeasure #2 – use “decrement counter” protection (it is only “workaround”).
- Countermeasure #3 – use online checking (the most secure one), unfortunately, this is not technically possible in all situations.

Our analysis of Slovak Mifare Classic cards has shown:

- All tested cards use the same keys for the first 1024 bytes (first 16 keys).
- There was always at least one sector encrypted with a default key! (therefore, it was always possible to perform our “nested attacks”.
- The name of passenger/the card owner was always stored in 0xd block – (imagine what can happen with strong antenna).
- There was no protection against cloning or modification.
- All these cards could be easily cloned and modified.

We have also done a binary difference analysis between the newly bought card, after its activation and charging credit. We have revealed the sensitive information that was available on all tested Slovak cards (“passenger/username”, expiration date of public transport document in Bratislava, student's university number, student's name).

Total costs for potential attackers are:

- 30 EUR for tikitag/touchatag RFID reader (sufficient for reading / cracking / writing / cloning Mifare Classic cards).
- $400 for Proxmark 3 (universal RFID emulator, reader, writer, sniffer).
- Less than 1 EUR for a blank 4kB Mifare Classic card.

There is no universally working security fix for Mifare Classic cards. We recommend using a safer technology (Mifare DESFire EV1). If Mifare Classic cards should be still used, we propose a partial workaround only – bind user identity with card's readonly UID, use UID in content card encryption, use UID whitelists, use “decrement counter” solution. Because replacing all Mifare Classic cards to safer ones may be very expensive and time-consuming process, for a short time it is possible to use the “decrement-counter” workaround. Let's have the “decrement counter” – initially set to 0xffffffff. Mifare access keys A and B have permission for decrementing counter only and these keys cannot be changed. The content of the card (with passenger credit) should be re-encrypted/hashed with card UID, this decrement counter, and private key. It is still possible to make a full clone of this card to Mifare Classic card with rewritable 0-block, but the original card cannot be re-used.

In addition to our released Mifare Classic Offline Cracker[2], there is also another tool from Andrei C called Mifare Classic Key Recovery Tool[3]. Compared to MFOC this tool is a bit slower, but it can recover at least one key from the card with non-default keys (e.g. London Oyster cards). This key can be used by MFOC to crack other keys from the card.

4 SMS parking ticket vulnerabilities

In 2010, we revealed critical vulnerabilities in SMS mobile parking. All big cities (including Bratislava and Košice) were affected. We revealed two critical vulnerabilities:

11. We were able to force any registered prepaid Mobile Parking user to pay for parking of an arbitrary car.
12. We were able to dump mobile numbers of all registered users in prepaid Mobile Parking.

Firstly, we would like to explain how prepaid Mobile Parking works. If someone wants to use prepaid Mobile Parking, she should be registered in this system with her mobile number and car plate number. After this registration, she needs to charge her parking credit (and transfer her money to her Mobile Parking account). In this situation billing is performed by the Mobile parking company. If she decide not to register to use prepaid Mobile parking, and she wants to pay immediately for her parking by SMS messages, billing is performed by the mobile operator.

Syntax of SMS parking request looks like:

ParkingTime_CarPlateNumber

Parking Time – in hours (Bratislava) or in minutes (Vienna)

Car Plate number – it is possible to pay for parking of an arbitrary car (not only yours!)

The SMS message is sent to the particular number, e.g., +421902020202

The fundamental security problem is that the subscriber of the prepaid Mobile parking is identified according to the SMS sender of the SMS parking request. Moreover, of course, this number can be easily spoofed. For our experiments, we have used the SMS spoofing service www.armsms.com. Because some SMS spoofing services accept Bitcoin, thanks to Tor and Bitcoin payments, the potential attacker can be completely anonymous.

The question is how it is possible to force the existing registered users to pay for the parking without their notice. Now we can send any SMS parking ticket with an arbitrary spoofed sender number, but if we want to park for free, we need to send it from the originator number that is already registered in the Mobile Parking system. So another question is – How it is possible to reveal existing registered numbers?

We have revealed both Slovak M-parking system www.m-parking.sk and Austrian M-Parking system www.handyparken.at are vulnerable to the trivial enumeration attacks. During the registration process, the Mobile Parking system always informs if the given mobile number exists or not. Therefore, this behavior can be exploited to dump all mobile numbers of all Mobile parking registered users(!)

Using these two vulnerabilities it is possible to cause total Mobile Parking chaos:

The victim receives the SMS notification that he pays for parking of XYZ car plate. The owner of XYZ car does not need to know necessarily anything about the victim and the attacker. The attacker can be still anonymous and cause a maximum chaos because it will be difficult to distinguish between justified and unjustified complaints. This confusion may lead to mobile parking anarchy and shutting down the Mobile Parking service in the worst case.

Despite the fact the registration form at www.m-parking.sk was protected against enumeration attacks by Captcha, we were able to crack 100% of all Captcha images using commercial Captcha cracking services http://decaptcher.com and

http://www.deathbycaptcha.com, solving 1000 Captcha images costs 0.97 €, cracking one mobile subnet (0905XXXXXX) costs 978 €.

The registration form at www.handyparken.at did not use Captcha protection at all. Therefore, mobile numbers of all registered users could be dumped just in few hours or days.

To fix these vulnerabilities, we have proposed three solutions:

4.1 SMS center verification

The Mobile Parking system should always checks if the number of SMS center of the SMS request has the given country prefix (Slovakia +421*, Austria, +43*) if not, the SMS parking request should be throw away

Advantages: probably very efficient solution, because SMS spoofing services are prohibited in Slovakia / Austria

Disadvantages: it is not possible to pay for the parked car in Slovakia from outside of Slovakia

4.2 Shortened numbers

The Mobile Parking company should disallow using the international number (e.g. +421902020202) for the Mobile parking that can be easily reached from the SMS spoofing service. In the case of shortened numbers, spoofing will be much more complicated because the SMS spoofing service has to be functional in the given country where a mobile parking is used.

4.3 Protection against enumeration attacks

If a user put his mobile number on the registration form, a random authentication token should be sent to his number. He should enter this authentication token to the second form and if it is valid, he will be successfully registered to the system.

If anyone with this number is registered to the system – he will receive the SMS message with text "This mobile number has been already used. Please ask for your forgotten credentials". We recommend not to use Captcha images at all.

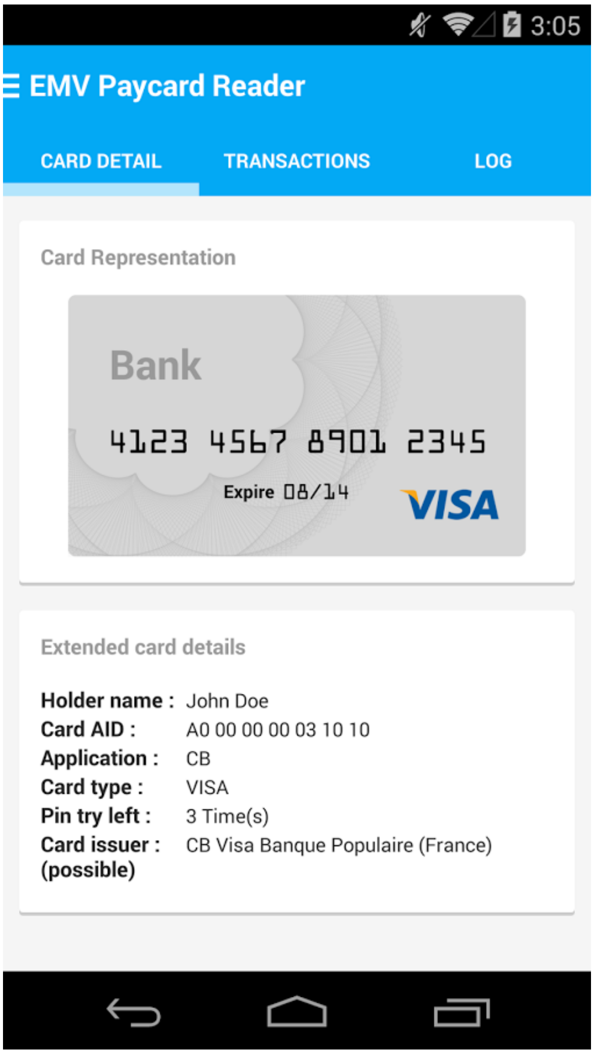
5 Security analysis of Slovak and Czech NFC payment cards

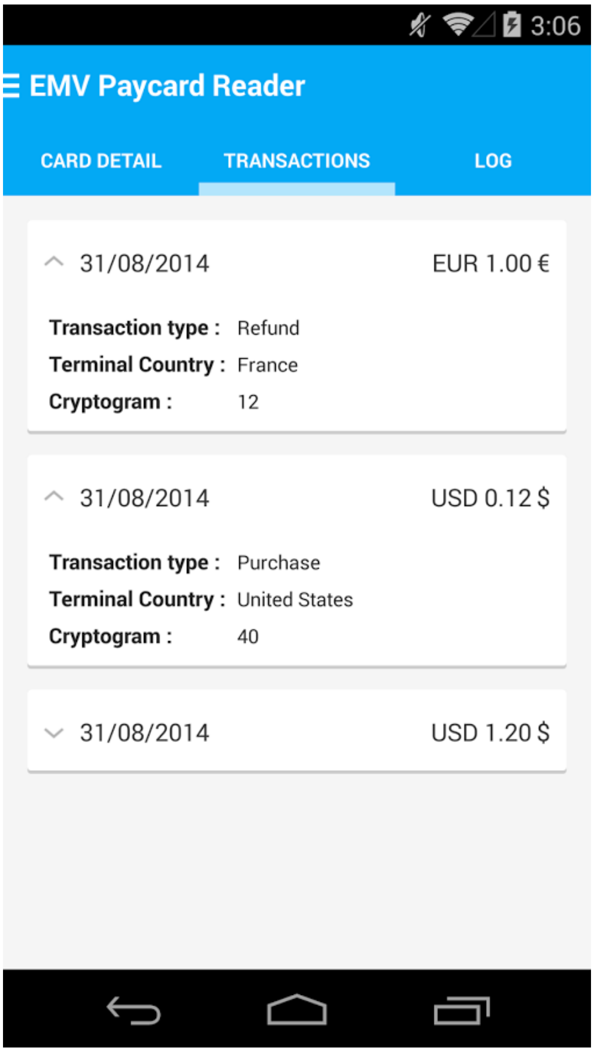
Contactless payment cards VISA (payWave) and Mastercard (PayPass) are probably the most popular in Slovakia – prefers them more than half of people (56% [4]. In April 2012, at the Conference Hackito Ergo Sum in Paris there was published presentation "Hacking the NFC credit cards for fun and profit"[5] firstly describing how it is technically possible fully anonymously and without authentication to gain a significant amount of sensitive information that can be subsequently misused. Such information includes, for example, a list of all executed payment transactions (payments in POS terminals, ATM withdrawals).

Three years after this presentation, we decided to implement a similar security analysis of NFC credit cards used in Slovakia and Czech Republic to find out if card issuers had already fixed these old vulnerabilities and started to issue sufficiently secure NFC payment cards. The result of our analysis was alarming – it is still possible to read much sensitive information from the most NFC cards used in Slovakia and Czech Republic.

The confidential information from NFC cards can be read by any seller with access to POS terminals, ATM owner/provider or anyone with physical access to a vulnerable NFC card payments. Consequently, it is possible to exploit this information to obtain "buying profile" of the card owner, to reveal all countries (based on the currency used) the card owner had visited in the past, to assess the card owner solvency and used this information for better-targeted marketing.

Contactless NFC cards can be read by an arbitrary ISO14443 based NFC reader working at the frequency of 13.56 MHz. In our case we have used standard smartphones and tablets with NFC support a special NFC reader (touchatag) [6]. As an Android application, we have used the Banking Card Reader (EMC) available directly from Google Play. Some information (e.g. card owner's name) could not be read by Banking Card Reader application. To read this information we have used a special Android application NFC millionaire [7] instead. As it was demonstrated in the following video [8], reading the sensitive information from NFC cards can be performed very fast.





We were able to read cards without external NFC antenna from a distance of 4 cm. The NFC standard allows this range to increase up to a distance of 20 cm.

According to a presentation "Hacking the NFC credit cards and debit for fun"[5] (slide 21) you can use an external antenna read range amplifier (for 2000 EUR) and antenna (for 1000 EUR) to increase the distance up to 1.5 meters.

We have revealed that most than half of all tested NFC EMV payment cards contain sensitive information that is not necessary for the correct card functionality – e.g. the transaction history.

During our analysis of more than 60 Slovak NFC cards and 30 Czech NFC cards, we have discovered that it was possible for more than half of all tested cards to read a complete transaction history. Of course without any authentication. For our comprehensive results, see [9]. For all tested cards, we were able to read a card number, expiration date, and PIN tries. For almost half of them, it was possible to read the whole transaction history, for some of them “owner name”.

Using applications NFC millionaire[7] we have also been able to retrieve the owner of the card.

CVC / CVV code is not stored on the card and therefore cannot be read.

In the case it was possible to know the transaction history, then for each transaction the following parameters were available:

- Type of operation (payment cards, ATM withdrawals, etc.).
- Date of the transaction.
- The total amount and the currency that was used.

Based on the used currency where the transaction was executed, it was possible to evaluate a geographical profile of the card owner – it means when and what countries he had visited in the past.

Based on the frequency and volume of the payments it was possible to create a “buying profile” and assess his solvency, which is how much money the card owner had spent for the defined period.

It is necessary to emphasize that this information that can be obtained by any POS terminal owner (seller) or any attacker who is sufficiently close to the card owner. More important, many e-commerce websites still do not require CVC / CVV code for card transaction (only the owner name, card number and expiration date). Therefore, stolen card information from NFC cards can be misused easily.

How to check if someone is vulnerable to the attack mentioned above?

First of all, on any Android device that supports NFC, we recommend to install the application Banking card reader[6] and try to find out what kind of information can be read from the given NFC card. If it is possible to read a very sensitive information (e.g. a transaction history, the name, and surname), we strongly recommend to contact the bank and ask them to issue newer and safer card replacement.

As long as the bank does not support secure NFC credit cards, we recommend choosing the bank that supports secure NFC cards.

If this is not possible, we recommend putting NFC cards to secure RFID shields (Faraday cage that blocks any electromagnetic radiation).

References

[1] Public transport SMS ticket hacking https://nethemba.com/resources/SMS-ticket-hack4.pdf.

[2] Recent version available here http://tools.kali.org/wireless-attacks/mfoc.

[3] MiFare Classic Universal toolKit (MFCUK) https://github.com/nfc-tools/mfc.

[4] http://www.mastercard.sk/osobne-karty/_assets/06_11_mastercard_index.pdf.

[5] http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-rlifchitz-contactless-payments-insecurity.pdf.

[6] https://play.google.com/store/apps/details?id=com.github.devnied.emvnfccard.

[7] https://github.com/laane/nfcmillionaire.

[8] https://www.youtube.com/watch?v=8ptqLROjgsg&feature=youtu.be,

https://nethemba.com/update-bezpecnostna-analyza-platobnych-nfc-kariet/.

SCADA security – good news or nightmare?
Bezpečnost SCADA – dobrá zpráva anebo noční můra?

Pavel Hejduk

Pavel Hejduk
pavel.hejduk@cez.cz

Pavel Hejduk works in area of ICT security in utility sector more than 10 years. Since October 2008 he leads group of ICT security specialists and company CSIRT team. His responsibility is to ensure that the security of main information systems in CEZ Group is on appropriate level and align with company strategic goals. He is member of board of security managers in CEZ Group and last few years he is focused on progressive security awareness, efficient methods of security incidents handling, ICT systems and SCADA systems security testing.Pavel graduated as Ing. in field of Electronics control systems on Faculty of Electricity University of West Bohemia in Pilsen and he holds professional certifications Certified Information Security Manager (CISM, ISACA) and Certified Information Systems Security Professional (CISSP, ISC2).

Pavel Hejduk pracuje v oblasti ICT bezpečnosti v energetickém sektoru více jak 10 let. Od roku 2008 vede tým bezpečnostních ICT specialistů a CSIRT tým společnosti. Jeho odpovědnost je zajistit, že bezpečnost hlavních informačních systémů ve Skupině ČEZ je na odpovídající úrovni a v souladu se strategickými cíli společnosti. Pavel je členem boardu bezpečnostních manažerů ve Skupině ČEZ a v posledních letech se specializuje na progresivní metody bezpečnostního vzdělávání, efektivní metody zvládání bezpečnostních incidentů a bezpečnostní testování ICT a SCADA systémů. Pavel vystudoval inženýrský obor Elektronické řídicí systémy na Elektrotechnické fakultě Západočeské university v Plzni a je držitelem profesních certifikací Certified Information Security Manager (CISM, ISACA) a Certified Information Systems Security Professional (CISSP, ISC2).

SCADA security – good news or nightmare?

Joining of words "security" and "SCADA" is important topic in discussions (not only) for professionals for few last years. SCADA systems are very important for control of technology, distribution and production systems in the utility business sector. These systems were typically built as integral part of whole technology complex years ago. SCADA systems were developed as operationally robust and safe systems, but how they'll manage risks in face of cyber threads in 21th century?
Talk is based on experiences from real projects and solved topics for internal customers in CEZ Group and other external cases.

Bezpečnost SCADA – dobrá zpráva anebo noční můra?

Spojení slov „bezpečnost" a „SCADA" rezonuje zejména v posledních několika letech nejen v uších odborné veřejnosti. V utility sektoru jsou systémy SCADA velmi důležité pro řízení technologických, distribučních a výrobních celků. Tyto systémy jsou budované zpravidla jako součást daného technologického celku před řadou let. Jedná se o provozně robustní a spolehlivé systémy, nicméně obstojí tyto systémy i vůči kybernetickým hrozbám dvacátého prvního století?
Přednáška je založena na zkušenostech z reálných projektů a řešených tématech interních zákazníků ve Skupině ČEZ i mimo ni.

1 Úvod do problematiky

Spojení slov „bezpečnost“ a „SCADA“ rezonuje, zejména v posledních několika letech, nejen v uších odborné veřejnosti. V utility sektoru jsou systémy SCADA velmi důležité pro řízení technologických, distribučních a výrobních celků. Tyto systémy jsou budovány zpravidla jako součást daného technologického celku. Jedná se o provozně robustní a spolehlivé systémy. Obstojí ale tyto systémy i vůči kybernetickým hrozbám dvacátého prvního století?

Tuto otázku si v posledních letech kladou zejména zástupci z řad provozovatelů SCADA systémů. Vedle zcela pozitivních postojů, někteří z nás by použili spíše přívlastek „naivních“, jsou zde řekněme i daleko rezervovanější a pragmatičtější názory.

Hrozby týkající se SCADA systémů jsou někdy bagatelizovány s argumentací poukazující na naprostou oddělenost těchto systémů od okolního světa a na specifické protokoly, případně proprietární řešení hardwarové i softwarové vrstvy. Tyto faktory jsou považovány za významné a údajně posouvají pravděpodobnost rizika „kybernetického útoku“ na SCADA systémy do zanedbatelných hodnot.

V kontrastu s touto rétorikou se na odborných konferencích stále častěji setkáváme s naléhavým tónem prezentací z řad odborníků a dodavatelů bezpečnostních řešení, kteří doslova bijí na poplach a snaží se rozhýbat ony pověstné „klidné vody“ v tak konzervativní oblasti, jako je kybernetická bezpečnost technologických informačních systémů.

Pravdou je, že i ve sdělovacích prostředcích a online informačních kanálech stále častěji slyšíme slovní spojení „bezpečnost SCADA“. Někteří z nás sice mohli na chvíli podlehnout přesvědčení, že kybernetické útoky na SCADA jsou cílené pouze na regiony blízkého východu nebo na působení blackoutů ve Spojených státech amerických. Stále častěji nicméně zaznívají informace o úspěšně provedených útocích se skutečnými dopady kybernetických hrozeb právě na technologické informační systémy, a to i v některých Evropských zemích. Pozvolna se tedy rozplývá iluze nezajímavosti či nedotknutelnosti tohoto regionu.

2 Bezpečnost průmyslových SCADA systémů

„Jak ve skutečnosti SCADA systémy vypadají? Kde jsou jejich hranice a co ovlivňuje jejich bezpečnost? Jsme schopni je účinně zabezpečit, v jakém čase a s jakými náklady? Naše zkušenost z prostředí Skupiny ČEZ je taková, že tzv. „problém zabezpečení SCADA“ zdaleka není problémem pouze průmyslových sběrnic, specifických protokolů a proprietárního hardware, jak je často účelově zjednodušováno výrobci ICT bezpečnostních řešení. Ukazuje se, že významnými faktory v bezpečnosti SCADA systémů je také rozdílný životní cyklus technologií oproti konvenčnímu IT, bezpečnostní povědomí personálu pracující se SCADA systémy a v neposlední řadě i adekvátní návrh ICT architektury a správně navržené integrace s okolními systémy.“

Popisovat „co to jsou SCADA systémy“ může někomu v dnešní době přijít již skutečně jako ztráta času. I tak si pojďme v několika bodech znovu připomenout, co obvykle vnímáme pod pojmem SCADA a proč jsou SCADA systémy vlastně používány. Při úvahách o zabezpečování těchto systémů se totiž, bohužel až příliš často, detailně věnujeme technickému návrhu a nástrojům, přičemž opomíjíme významné souvislosti plynoucí ze způsobu používání těchto systémů.

S ohledem na naši zkušenost ze společnosti, která se primárně zabývá výrobou, distribucí a prodejem energií, zde budeme hovořit zejména o SCADA systémech výrobních a distribučních zařízení.

SCADA systém, „Supervisory control and data acquisition – Dispečerské řízení a sběr dat“, je systém, který primárně představuje tyto základní funkcionality:

- centrální monitoring a ovládání zařízení a technologických procesů,
- přesné měření technologických dat,
- ukládání historie dat,
- přenos dat do dalších zařízení / systémů.

Součástí dispečerského pracoviště je dnes běžně schematicky znázorněná anebo přímo vizualizovaná podoba řízeného technologického procesu, která operátorovi umožňuje komplexní pohled na stav řízeného procesu, dílčí parametry a jejich historii. Samozřejmě poskytuje obsluze efektivní prvky ovládání, ať už mluvíme o možnostech změny více parametrů najednou např. formou předdefinovaných profilů a provozních režimů nebo dálkového ovládání konkrétních prvků v řízeném procesu.

Operátorské pracoviště pak samozřejmě na pozadí aktivně komunikuje s dalšími, běžnému oku často skrytými prvky typu PLC, RTU, MTU a průmyslovými sběrnicemi (typicky je konkrétní označení poplatné danému výrobci anebo rodině, případně generaci, konkrétních řešení), které zajišťují konkrétní funkce v řízené technologii, jako je měření hodnot sledovaných veličin v jednotlivých místech procesu nebo ovládání nejrůznějších stykačů, armatur a pohonů.

SCADA systém je nasazován jako součást daného technologického celku, ať už hovoříme o bloku uhelné elektrárny, distribučním centru, solární farmě nebo malé vodní elektrárně. Tyto systémy jsou zpravidla navrženy a nasazeny jako velmi robustní a provozně spolehlivé. Klíčové komponenty jsou zdvojeny a vždy existuje možnost potenciální chybnou funkci části SCADA systému vyblokovat a danou část technologického celku řídit místně. V tu chvíli samozřejmě obsluha ztrácí možnost komplexního pohledu a poměrně komfortní obsluhy řízeného technologického procesu. V těchto případech však, lety (často desítkami let) prověřené a pravidelně testované postupy místní obsluhy zajistí provozní spolehlivost celého systému.

Až do této chvíle zní popis situace poměrně idylicky a to i z pohledu kybernetické bezpečnosti. V pomyslném kontrolním checklistu si označíme: systém byl navržen jako provozně robustní, byl řízeně nasazen, zdokumentován, byla proškolena obsluha a existují náhradní postupy.

Když to však zhodnotíme znovu, ve větším detailu, první co nás jistě zaujme je fakt, kdy byl systém nasazen (v době instalace daného technologického celku – není tedy výjimkou, že uplynulo 10-20 let od nasazení) a jakou má plánovanou živostnost (10-15-30-? let). V dalším přiblížení zjistíme, že v zadání pro design SCADA nebylo zpravidla nic, co by připomínalo požadavky kybernetické bezpečnosti (snad s výjimkou zabezpečení přístupu do objektů, rozvoden a rozvaděčů). Zde však primární motivací nebyla kybernetická bezpečnost ICT komponent umístěných např. v oněch rozvaděčích, ale zejména ochrana majetku, provozní bezpečnost a bezpečnost při práci. Jak jistě tušíte, ona idylka o bezpečném SCADA systému se nám začíná rychle rozplývat. Při dalším ověřování zjišťujeme, že v rámci nasazení sice byla provedena velká řada testů – kyberneticko-bezpečnostní test však žádný. Obsluha perfektně zvládá řízení technologického celku jak místně, tak prostřednictvím SCADA systému, nicméně zpravidla nic neví o kybernetických rizicích a nezdráhá si z operátorského počítače vyřizovat soukromé e-maily a prohlížet web. Snad jediná dobrá zpráva je existence a funkčnost náhradních postupů.

Teorie je jedna věc, ale co praxe? Jak to ve skutečnosti vypadá v konkrétních řešeních a jaké máme možnosti situaci řešit?

Rozmanitost výrobních zdrojů vlastněných společnostmi Skupiny ČEZ nám v uplynulých letech umožnila ověřit stav kybernetické bezpečnosti a reálně bezpečnost SCADA otestovat v řadě instalací rozdílných velikostí i různého data uvedení do provozu.

V průběhu těchto let téma kybernetické bezpečnosti SCADA systémů postupně rostlo na významu a bylo zajímavé sledovat, jak rychle se objevila řada exkluzivních a zaručených out-of-box řešení údajné komplexní ochrany SCADA systémů. Tato řešení v podobě nejrůznějších bezpečnostních bran, sond a appliances jistě při zabezpečování SCADA systému lze s výhodou využít, neměli bychom však podlehnout iluzi, že komplexně vyřeší celý problém zabezpečení těchto systémů.

Rychlým úsudkem bychom mohli říci, že SCADA systémy uváděné do provozu v posledních letech jsou významně bezpečnější. Bohužel toto pravidlo není zcela pravdivé.

Při zobecnění výstupů testování SCADA systémů, a to prakticky bez ohledu na termín spuštění do provozu lze říci, že mezi obvyklé oblasti s významnými dopady do úrovně bezpečnosti, lze řadit zejména:

- celková ICT architektura, topologie a použité platformy,
- bezpečnost operátorských stanic,
- bezpečnost použitých komunikačních protokolů,
- neprovedený hardening platforem,
- bezpečnost PLC/MTU/RTU jednotek a průmyslových sběrnic.

3 „SCADA svět“ vs. „konvenční IT“

„Často slýcháme, že „SCADA svět“ a „konvenční IT“ nelze porovnávat. Jsou to rozdílné filozofie, architektury, procesy i způsoby užití. Je tomu skutečně tak?
Tradice ICT (kybernetických) bezpečnostních návyků, opatření, technologií a bezpečnostního povědomí se v konvenčním IT v řadě společností počítá na 10 a více let. Ukazuje se, že „SCADA svět“ do jisté míry stál po celou tu dobu stranou a řada dobrých návyků, postupů, architektur a technologií zde nebyla aplikována. Máme šanci to nyní napravit, nebo jsou tyto světy natolik odlišné, že toho nebudeme schopni?“

Řada oblastí ovlivňující bezpečnost SCADA systémů je pro nás důvěrně známá ze světa tzv. „konvenčního IT“. Anebo Vám témata typu: neprovedený hardening platforem, volba správné ICT architektury, bezpečnost pracovní stanice a topologie sítě, přijdou jako ryze SCADA témata?

V diskusích s operátory technologií řízených SCADA systémy (řekněme tedy uživateli SCADA) téměř vždy zaznívá, že jsou si vědomi nepodporované platformy např. daného operačního systému. Zpravidla však jedním dechem dodávají, že oni to nezmění – systém SCADA byl dodán jako součást dané čerpadlové stanice, kotelny atd., která je podporována dodavatelem XY.

Logicky tedy vedeme dialog se servisním dodavatelem daného řešení, který omezení zpravidla potvrzuje: „… vizualizace SCADA využívá knihovnu, která funguje jen s webovým serverem verze …, atd.“ Při dalším dotazování však zpravidla již najdeme společnou řeč a shodneme se, že není žádný důvod používat defaultní hesla, sdílené přístupy, přímý přístup na Internet, servisní kanál přes plain HTTP protokol atd. Ve finále zjišťujeme, že servisní dodavatel zpravidla velmi dobře ví, jak bezpečnost SCADA zlepšit, jen to po něm nikdo nechtěl. Servisní kontrakt se většinou týká jen zajištění provozních parametrů.

Ano, „svět SCADA“ je možná v některých ohledech jiný než svět konvenčního IT, nicméně nevidíme důvod, proč bychom se neměli pokusit aplikovat nejlepší praxi z konvenčního IT, minimálně pokud se jedná o obdobné platformy, detekci malware, segmentaci sítě, bariérovou ochranu, bezpečnostní povědomí nebo bezpečnostní požadavky v dodavatelských smlouvách.

Ukazuje se, že těmi správnými cestami k rychlému zlepšení úrovně kybernetické bezpečnosti jsou aktivity typu průběžného bezpečnostního vzdělávání uživatelů (operátorů SCADA), zavázání dodavatele SCADA pro uplatnění bezpečné administrace a správy systému, aplikace účinné bariérové ochrany SCADA systémů a v neposlední řadě i řízené změny obnovy již nepodporovaných platforem a případné úpravy ICT architektury systémů. Doplnění o nové infrastrukturní prvky cílené na detekci a eliminaci „SCADA*relevant“ hrozeb je jen další oblastí k řešení.

4 Malé SCADA systémy jako (budoucí) součást Internetu věcí (IoT)

Skupina ČEZ kromě velkých (a obecně známých) výrobních zdrojů typu klasické (uhelné), vodní anebo jaderné elektrárny operuje i dílčí, relativně malé, výrobní zdroje typu fotovoltaické, malé-vodní anebo větrné elektrárny. Tyto malé zdroje jsou samozřejmě také vybaveny SCADA systémy, které jsou generačně často velmi mladé. Jsou zde, z bezpečnostního pohledu platné, stejné charakteristiky jako pro SCADA systémy u velkých výrobních zdrojů? Jsou tyto SCADA systémy připraveny stát se součástí IoT, nebo jí už dokonce jsou?

V této části přednášky se společně podívejme na slabá místa relativně mladých instalací SCADA systémů ve větším detailu.

Tyto instalace samozřejmě mají, oproti svým „starším sourozencům“, nespornou výhodu ve využití aktuálně podporovaných operačních systémů a platforem. Stejně tak poslední roky prolomily tabu technologických sítí, což umožnilo aplikovat řadu principů z dobré praxe známé z „konvenčního IT“.

I tak výsledky bezpečnostních testů nejsou nijak omračující. Značnou měrou se na tomto stavu podepisuje, dnes již poměrně běžný, požadavek na přímou konektivitu do sítě Internet. Ať už se jedná o propojení dílčích „malých“ výrobních zdrojů na centrální dispečink (sběr dat, dohled, řízení) anebo vzdálený přístup servisních společností.

Při hledání typických oblastí s bezpečnostními nedostatky prakticky můžeme okopírovat předchozí poznatky – byť situace, např. v otázkách zabezpečených protokolů a zvolené IT architektury, je jistě o dost jiná. Stále však nelze konstatovat, že je situace zcela uspokojivá.

Dozajista tyto SCADA systémy byly v době spuštění daného technologického celku „v pořádku“, několik měsíců poté již instalace velmi pravděpodobně obsahuje řadu platformních zranitelností a často i „uvolněné“ chování obsluhy. Toto velmi dobře známe z „konvenčního IT“ a nezbývá než nasazovat další prvky dobré praxe: patch management, testování změn, periodické bezpečnostní vzdělávání atd.

5 Závěr

Přednáška rozhodně nemá za cíl přesně popsat všechny možnosti a principy zabezpečení SCADA systémů. Mým cílem bylo poskytnout posluchačům pohled na problematiku zabezpečení SCADA systémů očima členů bezpečnostního týmu z prostředí Skupiny ČEZ a jejích zákazníků.

Předkládaný pohled není zcela ve shodě s marketingovými prezentacemi některých výrobců SCADA a společností zabývající se bezpečností SCADA, ani není rešerší tohoto tématu v národním, evropském anebo celosvětovém měřítku. Přednáška vychází zejména z našich reálných zkušeností s konkrétními instalacemi a technologiemi, přičemž svým charakterem odpovídá case-study.

Skupina ČEZ tradičně věnuje provozní bezpečnosti a ochraně svých výrobních zdrojů, a samozřejmě i svých dalších aktiv, vysokou pozornost. Kybernetická bezpečnost SCADA je jednou kapitolou tohoto příběhu. Začali jsme jej pomyslně psát již před lety a rozhodně tento příběh prozatím nekončí. Nové hrozby a nové technologické možnosti nám do cesty staví stále nové výzvy …

Improving security management with SIEM
Možnosti zlepšení provozu systémů SIEM

Martin Dvořák
Zora Říhová
Libor Dostálek

Martin Dvořák
dvorakmar@
seznam.cz

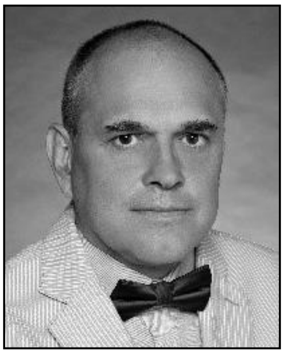
Martin Dvořák is auditor of information security according to ISO 27001. He has worked as an IT consultant at KPMG, where he worked on security projects for major companies in the telecommunications industry and the public sector. Before that he worked at Atos IT Solutions and Services, s.r.o., Where he also participated in security projects, he was responsible for implementation of information security management system according to ISO 27001 and optimizing processes of information security management. Besides his job duties he is dedicated to postgraduate studies at the Faculty of Informatics and Statistics at the University of Economics.

Martin Dvořák je auditorem bezpečnosti informačních systémů dle normy ISO 27001. Pracoval jako IT konzultant ve společnosti KPMG, kde se podílel na bezpečnostních projektech pro významné společnosti z oblasti telekomunikací a veřejného sektoru. Před tím pracoval ve společnosti Atos IT Services and Solutions, s.r.o., kde se taktéž podílel na bezpečnostních projektech, byl odpovědný za implementaci systému řízení informační bezpečnosti dle normy ISO 27001 a za optimalizaci procesů řízení informační bezpečnosti. Vedle svých pracovních povinností se věnuje doktorskému studiu na Fakultě informatiky a statistiky na Vysoké škole ekonomické v Praze.

Zora Říhová
zora.rihova@
prf.jcu.cz

Zora Říhová is dedicated to project management, IT quality management (including information security). She has extensive practical experience in the management of large-scale implementation projects, where in addition to the implementation of application software solved the problems of system integration and security from the companies such as Unipetrol, Siemens IT Solutions and Services or ATOS IT Services and Solutions. She is currently docent in the Department of Applied Informatics at the University of South Bohemia in the Ceske Budejovice and the Faculty of Informatics and Statistics, University of Economics.

Zora Říhová se věnuje řízení projektů a řízení kvality IT (včetně informační bezpečnosti). Má bohaté praktické zkušenosti z Unipetrolu a.s., Siemens IT Solutions and Services či ATOS IT Services and Solutions při řízení rozsáhlých implementačních projektů, kde se kromě implementace aplikačního programového vybavení řešily problémy systémové integrace a bezpečnosti. V současnosti je docentkou Ústavu aplikované informatiky Jihočeské university v Českých Budějovicích a Fakulty informatiky a statistiky Vysoké školy ekonomické v Praze.



Libor Dostálek
dostalek@prf.jcu.cz

Libor Dostálek is head of the Department of Applied Science at the University of South Bohemia in the Ceske Budejovice. He was involved in architecture and safety of several IT projects in banking and telecommunications. He deals mainly with the security of telecommunication systems. He is also the auditor of security of information systems according to ISO 27001. He has written a number of publications in the field of computer network security, digital signature and PKI. Led joint cross-border project between the University of South Bohemia and the University of Passau in Digital Humanities.

Libor Dostálek je vedoucím Ústavu aplikované informatiky na Jihočeské univerzitě v Českých Budějovicích. Podílel se na architektuře a bezpečnosti řady IT projektů v oblasti bankovnictví a telekomunikací. Zabývá se zejména bezpečností telekomunikačních systémů. Je rovněž auditorem bezpečnosti informačních systémů dle normy ISO 27001. Napsal řadu publikací z oblasti bezpečnosti počítačových sítí, elektronického podpisu a PKI. Vedl společný přeshraniční projekt mezi Jihočeskou univerzitou a Univerzitou v Pasově v oblasti Digital Humanities.

Improving security management with SIEM

Organizations within their risk management activities implement a SIEM (Security Information and Event Management) systems to ensure information security. These systems evaluate data from applications within the IT environment of the organization and based on that decide whether there is a security incident or not. The authors of the article are dealing with the possibilities of improving SIEM systems and also propose a method based on filtering of SQL queries to achieve better performance characteristics of these systems.

Možnosti zlepšení provozu systémů SIEM

Organizace v rámci řízení rizik implementují systémy SIEM (Security Information and Event Management) za účelem zajištění informační bezpečnosti. Tyto systémy vyhodnocují data aplikací v rámci IT prostředí organizace a na základě toho rozhodují, zda došlo k bezpečnostnímu incidentu či nikoliv. Autoři se v článku zabývají možnostmi zlepšení systémů SIEM a zároveň navrhují metodu založenou na filtrování SQL dotazů, aby bylo dosaženo lepších provozních charakteristik těchto systémů.

1 Úvod

Organizace provádí stále větší množství aktivit elektronicky, přičemž roste podíl aktivit, které jsou z pohledu informační bezpečnosti rizikové [2]. Zároveň dochází ke stále většímu množství bezpečnostních incidentů s cílem finančního obohacení či odcizení citlivých dat organizace. Útočníci provádějí útoky mnohem sofistikovaněji a důmyslněji nejen s pomocí informačních technologií, ale také s pomocí technik sociálního inženýrství. Tohoto vzrůstajícího trendu jsou si vědomy vládní instituce a přijímají opatření umožňující zvýšit informační bezpečnost obecně. Důkazem toho je i Evropským parlamentem nedávno schválená direktiva „Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union." Z této direktivy vychází zákon č. 181/2014 Sb., o kybernetické bezpečnosti přijatý parlamentem České republiky v létě roku 2014. Zákon dále doplňují následující vyhlášky: vyhláška č. 316/2014 Sb., vyhláška č. 317/2014 Sb. a nařízení vlády č. 315/2014 Sb.

1.1 Definice problému a cíle článku

Předmětem této práce je informační bezpečnost (dále jen IB) organizace, která využívá systém vyhodnocující události informační bezpečnosti (dále jen SIEM). Systémy SIEM vyhodnocují data z aplikací v rámci IT prostředí organizace a na základě toho rozhodují, zda došlo k bezpečnostnímu incidentu či nikoliv. Problém je, že aplikace generují příliš velké množství dat / událostí, které musí systém vyhodnotit. Toto činí provoz systémů SIEM nákladným, a to jak z hlediska přímých, tak nepřímých nákladů: přímé náklady jsou způsobeny vysokými licenčními poplatky, protože většina řešení má licenční model postavený na množství zpracovaných dat / událostí [8]; nepřímé náklady vyplývají z množství dat, které je zpracováváno v systému SIEM. Čím více dat musí systém vyhodnotit, tím větší jsou nároky na výpočetní výkon systému a také nároky na síťovou infrastrukturu organizace[1], která musí transportovat do systému tato data k vyhodnocení.

Cílem prezentovaného výzkumu je posoudit relevanci implementace systémů SIEM pro organizaci z pohledu dnešních trendů v oblasti IB a navrhnout metodu, která umožní snížení množství dat, jež vstupují do systému SIEM k vyhodnocení, aniž by tím byla snížena úroveň IB organizace. Tato metoda zároveň umožňuje organizaci zlepšit provoz systému SIEM.

Autoři touto prací navazují na svůj předešlý výzkum [3], kde byl definován normativní rámec IB organizace včetně představení principů auditu IB a [4], kde byly definovány předpoklady pro správné fungování systémů vyhodnocujících chování uživatelů informačních technologií (IT).

1.2 Definice základních pojmů

Cílem této podkapitoly je definovat v práci nejvíce používané termíny a dosáhnout tak jednotného porozumění zkoumaného tématu.

Informační bezpečnost

Ve vědecké obci platí pro pojem informační bezpečnost následující definice: bezpečnost informací je zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako například: autentičnost, odpovědnost, nepopiratelnost a spolehlivost. Tato definice byla převzata i mezinárodním standardem ČSN ISO/IEC 27001.

Událost

Pod pojmem událost bude pro potřeby tohoto článku rozuměna jakákoliv akce v IT prostředí organizace, která je natolik významná pro informační bezpečnost organizace, že stojí za to ji

[1] Jinými slovy: nároky na šířku komunikačního kanálu.

zaznamenat, je v čase ohraničena a lze k ní jednoznačně přiřadit další atributy, a to zejména: kde a kdy se uskutečnila, předmět události, typ události (čtení, úprava, mazání) a kdo ji inicioval.

Bezpečnostní incident

Za bezpečnostní incident je považována událost, která zahrnuje porušení bezpečnosti (dostupnosti, integrity či důvěrnosti) informací. Bezpečnostní incident může nastat, aniž by byla patrná škoda v momentě jeho výskytu. Vše se může projevit později.

1.3 Základní principy hodnocení událostí

Tato kapitola slouží k definici základních principů fungování systémů SIEM. Z těchto principů fungování vychází níže definovaná metoda redukce dat. Autoři sestavili tyto principy na základě syntézy poznatků učiněných během analýzy současných SIEM řešení. Pro analýzu byly zvoleny 3 nejlépe hodnocené produkty (IBM QRadar, HP ArcSight, Splunk) dle konzultační společnosti Gartner [5].

Systémy hodnotící události fungují tak, že v IT prostředí organizace pomocí sond[2] monitorují data a události a následně z nich sestavují pomocí statistických metod (korelace) řetězce událostí, které mají jeden společný jmenovatel. Tím bývá zpravidla uživatel. Řetězce událostí jsou tedy aktivity jednoho uživatele seřazené v časové souslednosti, jak je uživatel inicioval. K tomu, aby systém mohl posoudit, že daný řetězec události je tzv. kritickým řetězcem událostí bezpečnostního incidentu, musí znát tzv. kontext, ve kterém se události udály. Kontext je sestaven na základě dodatečných dat zevnitř i vně organizace. Jinak řečeno, systém na základě posbíraných dat z datových zdrojů dokáže odpovědět na otázky kdo, co, kdy, kde a proč provádí: jaký uživatel inicioval či z jaké IP adresy byla iniciována událost; co bylo náplní události (editace dat, kopírování, mazání); v kolik hodin; v jaké aplikaci se událost stala, a proč se událost stala.

Systém SIEM vyhodnocuje kybernetické události na základě definovaných pravidel. Systémy disponují vlastností „učit se“, což znamená, že za provozu jsou schopny připravit nová pravidla pro vyhodnocování událostí. Zpravidla však platí, že počáteční pravidla hodnocení musí definovat administrátor systému SIEM na základě bezpečnostní politiky organizace.

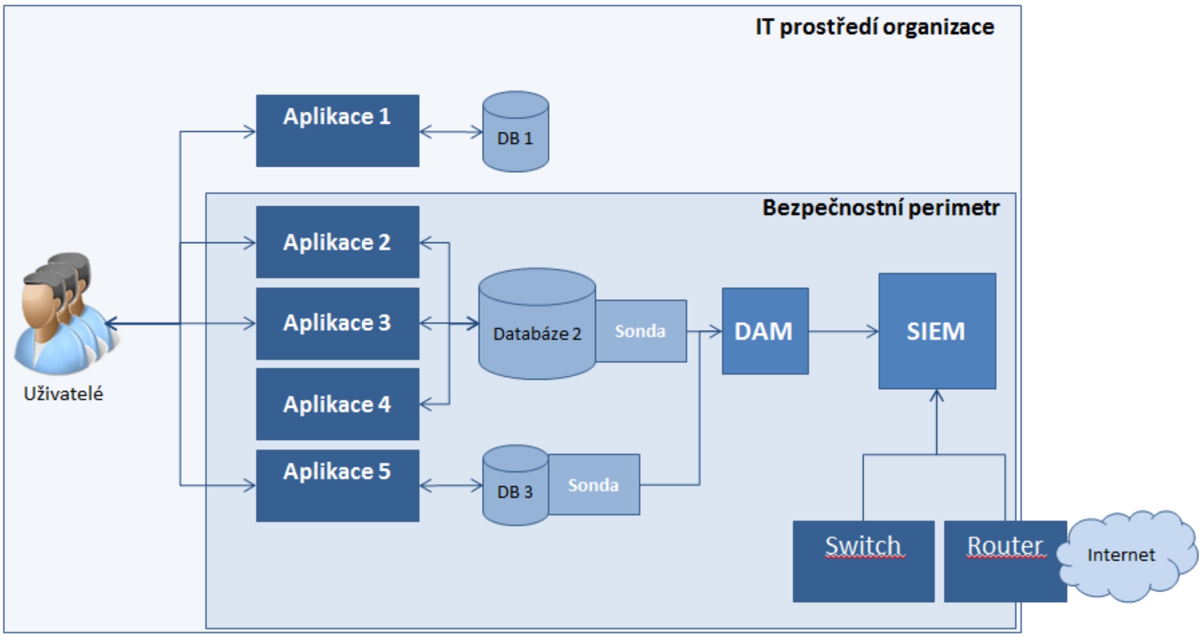
Na základě těchto pravidel je každá událost posouzena a je rozhodnuto o tom, jaká kategorie události nastala: známý bezpečný stav; neznámý stav; známý nebezpečný stav. Pro každou kategorii lze v systému SIEM definovat podkategorie, ke kterým lze přiřadit konkrétní sady operací, které má SIEM provést v případě jejich výskytu. Například při neznámém stavu odesílá SIEM celou událost k další analýze členům týmu SOC[3] – ti potom mohou rozhodnout o vytvoření nového pravidla, jež vymezuje, jak danou událost posoudit; při známém nebezpečném stavu může SIEM generovat výstražné hlášení či danou aktivitu zcela zastavit.

Obrázek 1 zobrazuje velmi zjednodušené schéma architektury IT organizace včetně znázornění umístění sond, které dodávají data do systému SIEM k vyhodnocení. K připojení systému SIEM do databází se využívají nástroje DAM[4], které sbírají data o událostech v databázích. Díky nástroji DAM nastává první úspora v toku dat v komunikaci mezi DAM a SIEM.

[2] Sonda je typicky programová komponenta, která sbírá data o provozu v IT infrastruktuře organizace a následně je odesílá do systému SIEM k vyhodnocení.

[3] Security Operations Centre (tým zajišťující aktivity kolem řízení informační bezpečnosti organizace).

[4] Database Activity Monitoring systém slouží jako konektor, který umožňuje připojit SIEM a sledovat tak aktivity v databázích.



Obrázek 1: Zjednodušené schéma sběru dat do systému SIEM. Zdroj: [autoři].

Zlepšení (optimalizace) provozu systému SIEM téměř vždy znamená omezení dat, které do něj vstupují, proto je vždy nutné volit kompromis mezi dostatečnou úrovní IB organizace a dostatečným množstvím relevantních dat. Pokud dojde k přílišnému omezení dat, jež do systému vstupují, může se stát, že systém nebude schopen vyhodnocovat události. To se v konečném důsledku může projevit neschopností systému identifikovat nastalý bezpečnostní incident nebo může generovat příliš mnoho falešných výstražných hlášení.

2 Relevance systémů SIEM z pohledu dnešních trendů v oblasti informační bezpečnosti

Účelem této kapitoly je odpovědět na otázku, zda je nasazení systémů SIEM pro organizace z dnešního pohledu relevantní.

2.1 Přispívá SIEM k naplnění požadavků zákona č. 181/2014 Sb.?

Sledování a vyhodnocování událostí kybernetické bezpečnosti nařizuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti [15] v §7, odstavec 3. Navazující vyhláška č. 316/2014 Sb. [13] požadavky na vyhodnocování událostí dále konkretizuje. Toto však platí pouze pro organizace spadající do působnosti zákona č. 181/2014 Sb., která je vymezena v navazujících vyhláškách: [12] a [14].

Zákon č. 181/2014 o kybernetické bezpečnosti	Způsob ošetření / implementace
§ 4 odst. 2	Administrativní úkon
§4 odst. 3	Administrativní úkon
§7 odst. 3	SIEM
§8 odst. 1	SIEM a následně administrativní úkon
§16 odst 2	Administrativní úkon

Tabulka 1: Způsoby řešení požadavků v paragrafech zákona č. 181/2014. Zdroj: autoři.

Vyhláška č. 316/2014 Sb.	Způsob implementace
§ 3	Administrativní úkon
§ 4	Administrativní úkon
§ 5	Administrativní úkon
§ 6	Administrativní úkon
§ 7	Administrativní úkon
§ 8	Administrativní úkon
§ 9	Administrativní úkon, SIEM a systém Identity and Access Management
§ 10	Administrativní úkon a SIEM
§ 11	Administrativní úkon a systém Identity and Access Management
§ 12	Administrativní úkon
§ 13	Administrativní úkon
§ 14	Administrativní úkon
§ 15	Administrativní úkon
§ 16	Administrativní úkon
§ 17	Administrativní úkon a Firewall
§ 18	Administrativní úkon a systém Identity and Access Management
§ 19	Systém Identity and Access Management
§ 20	Antivir
§ 21	SIEM
§ 22	SIEM
§ 23	SIEM a administrátorský úkon
§ 24	IDS (Intrusion detection system) a případně SIEM
§ 25	Administrativní úkon
§ 26	Monitoring a redundance
§ 27	Administrativní úkon

Vyhláška č. 316/2014 Sb.	Způsob implementace
§ 28	Administrativní úkon
§ 29	Administrativní úkon
§ 30	Administrativní úkon
§ 31	Administrativní úkon
§ 32	Administrativní úkon
§ 33	Administrativní úkon
§ 34	Administrativní úkon

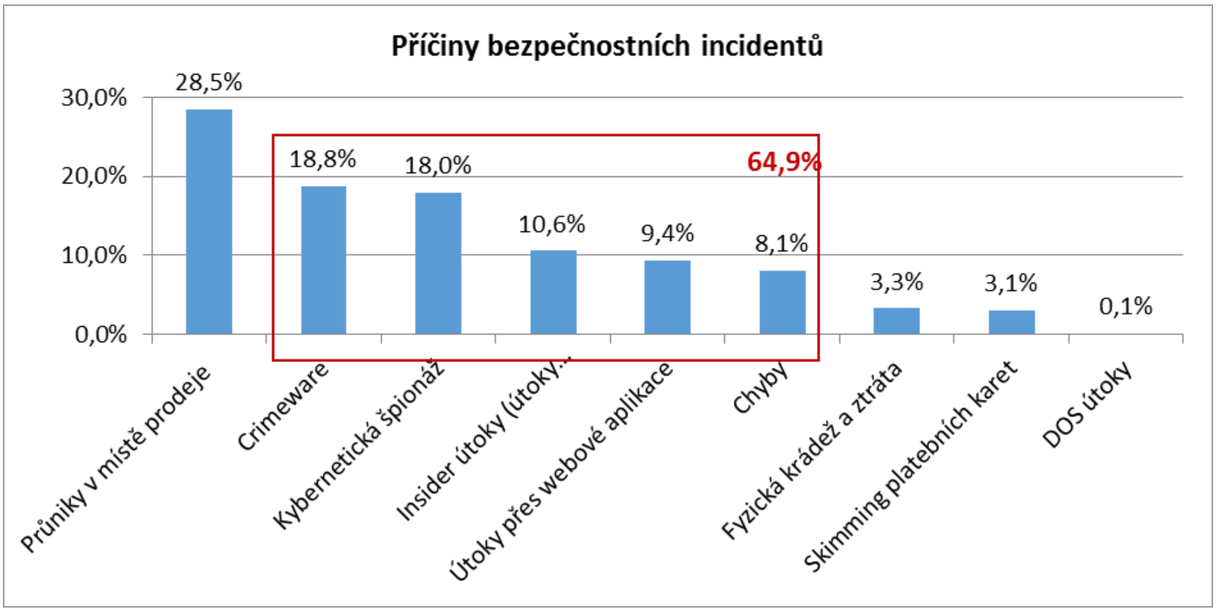
Tabulka 2: Způsoby řešení požadavků v paragrafech vyhlášky č. 316/2014. Zdroj: autoři.

Z autory provedené analýzy požadavků zákona 181/2014 Sb. i vyhlášky 316/2014 Sb. vyplývá, že nasazení systému SIEM napomáhá plnit tyto legislativní požadavky: §7 a §8 odst. 1. zákona 181/2014 Sb., o kybernetické bezpečnosti a §9, §10, §21, §22, §23, §24 specifikované ve vyhlášce 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

2.2 Další zdroje požadavků na sledování a vyhodnocování bezpečnostních událostí

Není to však pouze zákon o kybernetické bezpečnosti, který vyžaduje sledování událostí za účelem dosažení organizací definované úrovně IB. Sledování a vyhodnocování bezpečnostních událostí je v souladu s best–practice a významnými normami, jako je například mezinárodní standard ČSN ISO/IEC 27001 [11], který definuje systém řízení informační bezpečnosti a zákon č. 181/2014 z něj do značné míry vychází.

Implementace systémů, které vyhodnocují události, je pro organizace relevantní nejen z pohledu plnění legislativních a normativních požadavků, ale také z pohledu realizace opatření proti rizikům, kterým organizace čelí. Dle globálního průzkumu [10], který zkoumá příčiny bezpečnostních incidentů za rok 2015, lze implementací systému SIEM pokrýt cca 64,9% bezpečnostních incidentů (viz Graf 1). Konkrétně se jedná o crimeware, kybernetickou špionáž, insider útoky (útoky zevnitř) a zneužití pravomocí, útoky přes webové aplikace a chyby lidského faktoru.

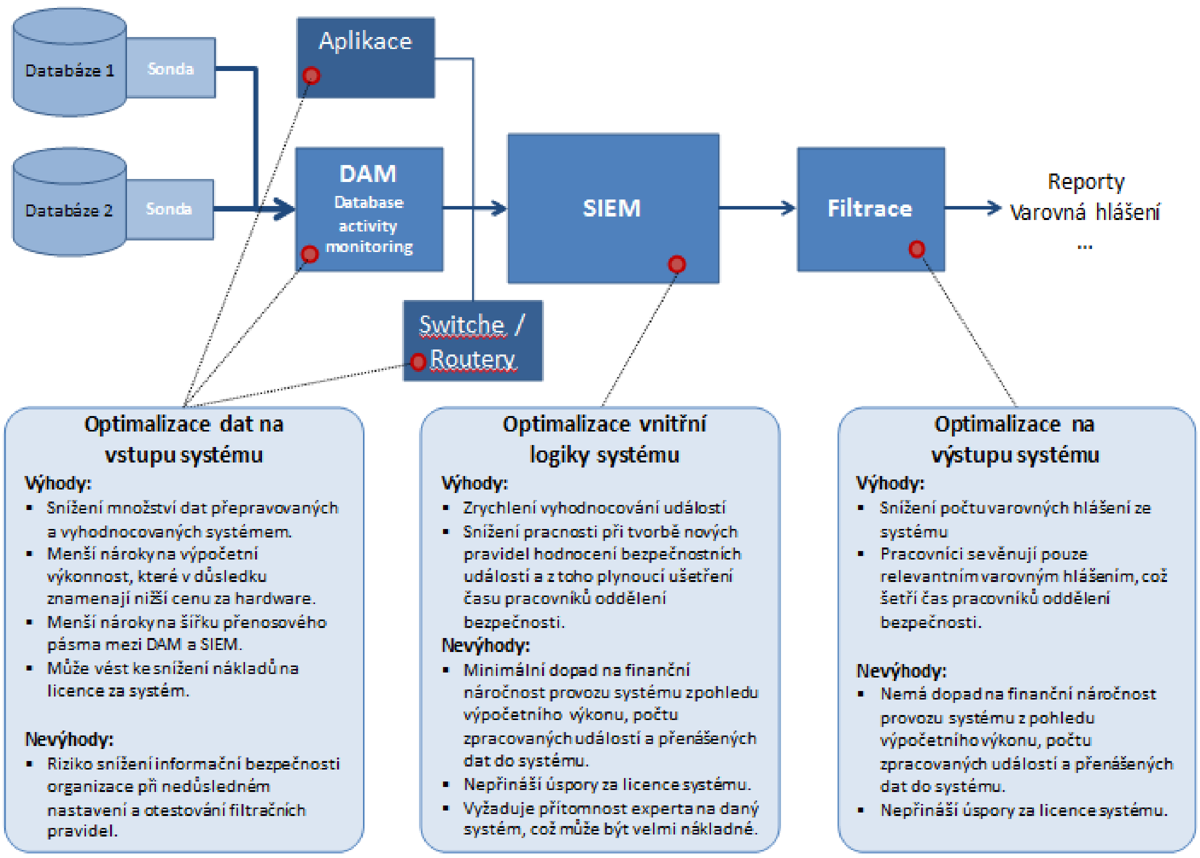


Graf 1: Příčiny bezpečnostních incidentů. Zdroj: [10].

Na základě výše popsaného lze učinit závěr, že nasazení systému SIEM je pro organizace relevantní z pohledu souladu s legislativou, plnění doporučení best–practice a realizace opatření proti rizikům.

3 Možnosti zlepšení provozu systémů SIEM

Ve vědecké obci je zkoumáno několik přístupů k redukci provozních nákladů SIEM či zlepšení jeho výkonnostních charakteristik. Snahy o zlepšení provozu lze pozorovat jak na vstupní straně systému SIEM, tak i na výstupní straně systému SIEM. Zlepšení provozu na vstupní straně systému SIEM má za cíl redukci množství dat, které do něj vstupují; na tomto principu je založena autory navržená metoda. Zlepšení provozu na výstupu cílí na omezení počtu varovných hlášení („alerts“) ze systému SIEM, kterým by se jinak museli věnovat pracovníci SOC či administrátoři systému. Dalším přístupem k zlepšení provozu systému SIEM je zlepšení vnitřní logiky systému, jež vyhodnocuje nastalé události dle definovaných pravidel. Stručné porovnání těchto přístupů uvádějí autoři na obrázku 2.



Obrázek 2: Možnosti zlepšení provozu SIEM. Zdroj: autoři.

Koncept filtrování paketů na vstupu systému SIEM v rámci detekce malware je prezentován v [6]. Princip spočívá v modelování dopravy na síti a její rozlišení na „známou“, která je filtrována, a na neznámou, která je puštěna k dalšímu vyhodnocení do systému SIEM. Nevýhodou tohoto přístupu je, že neumožňuje pokrýt širší spektrum IT rizik vyplývající například z lidského faktoru (chyba, krádež dat, apod.), protože pracuje na příliš nízké vrstvě ISO/OSI modelu. Autoři proto v této práci navrhují metodu založenou na filtraci SQL dotazů, která pracuje na vyšší vrstvě ISO/OSI modelu a umožňuje tato rizika zohlednit.

Příkladem zlepšení vnitřní logiky SIEM je práce [9], jejíž autoři aplikují poznatky z umělé inteligence a prezentují korelační modul[5] založený na genetickém programování a neuronových sítích, který je schopen sám navrhnout a učit se nová korelační pravidla. Tento přístup významně usnadňuje práci SOC operátorům při definici nových pravidel vyhodnocování bezpečnostních událostí. Nevýhodou je, že nesnižuje množství dat, které systém SIEM musí vyhodnotit.

Metoda, která je zaměřena na optimalizaci výstupu ze systému SIEM je prezentována v článku [7]. Tato metoda spočívá ve filtraci hlášení ze systému SIEM. Toto ve výsledku přináší snížené nároky na počet FTE[6] pracovníků SOC, kteří se tak věnují pouze relevantním hlášením.

Další vědecké články věnující se této problematice jsou například [1], kde se autor věnuje představení vývoje IB v posledních letech a jejím základním principům.

[5] „Correlation Engine“
[6] Full-time ekvivalent (FTE) je jednotka sloužící k vyjádření pracovní náročnosti daného úkolu.

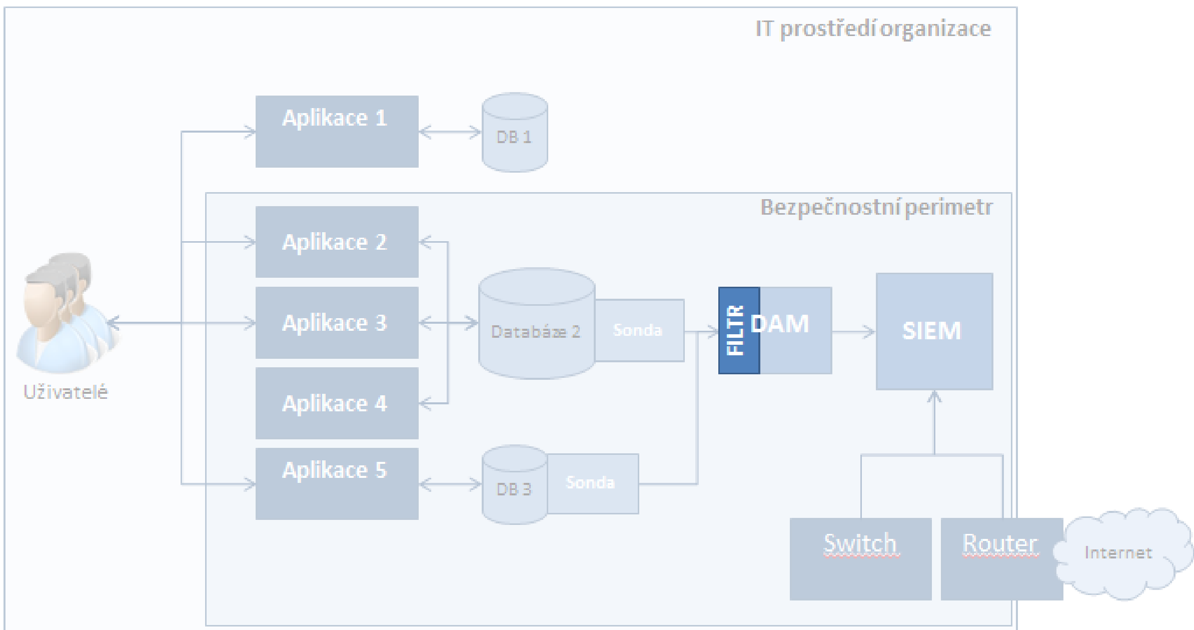
Výše zmíněné přístupy včetně metody prezentované v tomto článku se vzájemně nevylučují, proto organizace mohou za účelem dosažení optimálního provozu systému SIEM zvolit několik přístupů dle svých interních podmínek.

4 Metoda zlepšení provozu SIEM pomocí filtrování SQL dotazů

Pro splnění výše definovaného cíle výzkumu je nutné redukovat množství dat vstupující do systému vyhodnocující události infomační bezpečnosti. Za tímto účelem navrhují autoři článku níže popsanou metodu. Tato metoda má následující předpoklady:

1. Organizace má implementovaný systém řízení informační bezpečnosti například dle ČSN ISO/IEC 27001. Důvodem tohoto předpokladu je, že při jeho splnění má tímto organizace definovaný bezpečnostní perimetr, klasifikována data a má definovánu politiku řízení informační bezpečnosti.
2. Organizace plánuje implementovat nebo již má implementovaný systém SIEM, který je oddělen od vlastního informačního systému; pro připojení k databázím slouží nástroj DAM.
3. Vlastní informační systém využívá databázovou datovou základnu. Tento předpoklad nicméně není pro funkčnost metody zásadní; metodu lze přeformulovat též pro jiné modely architektury IT organizace.

Již samotný předpoklad 2 (využití nástroje DAM) pro připojení databází znamená výrazné snížení dat pro vlastní SIEM, protože SQL dotazy jsou ponechány na úrovni DAM a do SIEM se dostávají pouze varovná hlášení (incidenty) z DAM ohledně dění v databázích. Tímto se však problém ohledně množství dat přesunul na stranu DAM, který musí vyhodnocovat všechny SQL dotazy, jež na databáze směřují (viz obrázek 1). Ústřední myšlenka navrhované metody proto spočívá v implementaci filtrační vrstvy před nástroj DAM, čímž bude zajištěno, že DAM vyhodnocuje pouze z pohledu IB relevantní SQL dotazy (viz obrázek 3).



Obrázek 3: Zjednodušené schéma sběru dat do systému SIEM včetně zobrazení umístění filtru SQL dotazů. Zdroj: autoři.

Pro efektivní funkci filtrační vrstvy je nutné identifikovat citlivá data pro jednotlivé databáze. Samotná implementace filtru následně spočívá v konstrukci parseru SQL dotazů, který o každém dotazu rozhodne, zda se dotazuje na citlivá data či nikoli.

Autory navržená metoda redukce množství dat pro systém vyhodnocující události má následující kroky:

1. Identifikace citlivých dat.
2. Identifikace aplikací zpracovávajících citlivá data.
3. Sestavení pravidel filtrace dat.
4. Implementace filtrace dat.
5. Ověření a případná úprava pravidel filtrace.

Kroky 3 – 5 lze iterativně opakovat, dokud není dosaženo optimálního množství dat, jež vstupují do systému SIEM.

Rizikem navržené metody je možnost odcizení dat přímo prostřednictvím lokálního připojení do databáze prostřednictvím souborového systému. Pokud předpokládáme, že toto činí oprávněný uživatel (administrátor) lze toto riziko redukovat personální politikou organizace – dostatečným prověřením a výběrem kandidátů na pozice administrátorů systémů. Pokud však předpokládáme, že k tomuto bezpečnostnímu incidentu došlo prostřednictvím získání privilegovaného přístupu vzdáleným uživatelem (např. za pomoci škodlivého programového kódu), pak lze předpokládat, že tento vzdálený uživatel, je zkušený útočník a následně umí deaktivovat sondy na databázi a tak nepozorovaně data rovněž prostřednictvím souborového systému odcizí. V takovémto případě však selhal celý systém řízení informační bezpečnosti organizace (již od úrovně antiviru) a SIEM tomuto incidentu nezabrání[7].

Dalším rizikem je možnost vyvolávání systémových funkcí vzdáleným uživatelem prostřednictvím škodlivých SQL dotazů (viz např.: zranitelnost CVE–2007–3280). Tuto zranitelnost však autoři považují za již ošetřenou na straně poskytovatelů databází.

Na základě zkušeností z implementace lze zmínit i riziko opomenutí některých datových položek obsahujících citlivá data. Toto riziko nastává v případě provádění „Identifikace citlivých dat“ pouze na základě dokumentace, která může být v některých případech neaktuální. Autoři proto doporučují raději provádět identifikaci na základě datových položek přímo v databázi.

4.1 Identifikace citlivých dat

Citlivá data jsou identifikována v souladu s vymezením bezpečnostního perimetru. Lze rozlišit dvě skupiny citlivých dat:

1. Identifikátory (sloupce tabulek v databázi), které jsou citlivé samy o sobě. Do této skupiny je zařazen každý identifikátor, jenž je v rámci bezpečnostního perimetru označen jako citlivý údaj. Do skupiny identifikátorů budou patřit i ta datová pole, jejichž sledování je vyžadováno legislativně, např. legislativou chránící osobní údaje apod. Množina všech identifikátorů, které jsou citlivé samy o sobě, bude dále značena I_c.
2. Množiny identifikátorů, které dohromady tvoří citlivá data. Do této skupiny jsou zařazeny takové množiny identifikátorů, které jsou v rámci bezpečnostního perimetru označeny za citlivé, tj. takové množiny identifikátorů, které dohromady umožňují plnit roli citlivého identifikátoru (viz bod 1.). Kolekce všech takových množin identifikátorů se bude značit I_m.

[7] Lze pouze diskutovat nakolik je útočník zkušený a bude po sobě umět „zamést stopy“ či deaktivovat sondy, které sbírají data do SIEM. SIEM pak incident zaznamená nebo nikoliv. Pokud k takovémuto selhání systému řízení IB dojde, jsou možnosti zabránění incidentu velmi omezené.

Příklad:

Rodné číslo je vždy citlivým údajem, neboť jednoznačně identifikuje osobu a umožňuje tak přistupovat k osobním datum konkrétní entity.

Příjmení (v analogické situaci) samo o sobě není citlivým údajem, neboť osobu jednoznačně neidentifikuje. Z hlediska informační bezpečnosti lze v tomto případě příjmení označit za nezajímavý identifikátor. Pokud však příjmení zkombinujeme s dalšími údaji, například s datem narození (které je taktéž zřejmě samo o sobě nezajímavé), získáme množinu identifikátorů, která již může vymezit dostatečně malou skupinu osob, aby bylo možné data získaná pomocí kombinace těchto identifikátorů považovat za citlivá.

Výstupem tohoto kroku jsou tedy množiny I_c identifikátorů citlivých dat (datové položky, které obsahují citlivá data) a I_m množin identifikátorů, které dohromady vedou k citlivým datům. Pro jednoduchost následujícího výkladu dále předpokládejme, že prvky I_c jsou jednoprvkové množiny.

4.2 Identifikace aplikací zpracovávající citlivá data

Cílem tohoto procesního kroku je identifikovat, v jakých aplikacích a jak jsou citlivá data zpracovávána. První část v podstatě znamená identifikovat toky citlivých dat skrz aplikace organizace. Druhá část analýzy se primárně zabývá zjištěním způsobu, podle jakých položek jsou data vyhledávána, jaké datové položky lze v daných aplikacích zobrazit a jaké možnosti mají uživatelé pro čtení, editaci či mazání konkrétních datových položek.

Analyzovány jsou vždy ty aplikace, které spadají do vymezeného bezpečnostního perimetru bezpečnostní politikou organizace. Avšak pro kontrolu lze použít i schéma architektury nebo datový model organizace, pokud jsou dostupné a aktuální.

Ke každé množině citlivých identifikátorů I se pro každou aplikaci v bezpečnostním perimetru eviduje, zda je nutné ve filtrační vrstvě dotazy směřující na I sledovat.

Označíme-li symbolem A množinu aplikací spadajících do bezpečnostního perimetru, je výstupem tohoto kroku funkce $f: I_c \cup I_m \times A \mapsto \{0,1\}$. Význam funkčních hodnot je následující: je li I množina identifikátorů a a aplikace, $f(I,a) = 1$ tehdy, pokud je nutné množinu identifikátorů I v aplikaci a sledovat, v opačném případě je $f(I,a) = 0$.

Je–li z organizačních důvodů žádoucí rozlišovat akce (čtení, editace, mazání), které lze v aplikaci a nad množinou identifikátorů I provádět, lze funkci f zavést jako $f: I_c \cup I_m \times A \mapsto 2^O$, kde $O = \{\text{mazani, cteni, editace}\}$ a 2^O je množina všech podmnožin množiny O.

Funkční hodnoty funkce f lze případně pro přehlednost uchovávat v matici, kde by řádky odpovídaly jednotlivým množinám identifikátorů a sloupce jednotlivým aplikacím.

Identifikátor	**Aplikace**			
	SAP	**Siebel**	**EXK**	**…**
Rodné číslo	X	X	X	…
ID osoby v DB	X	X	X	…
Příjmení + Datum narození		X		…
Příjmení + Trvalá adresa	X	X	X	…
Trvalá adresa + Datum narození		X		…
…	…	…	…	…

Tabulka 3: Příklad matice zpracování citlivých dat. Zdroj: autoři.

4.3 Sestavení pravidel filtrace dat

Pro každou aplikaci (každou sondu) je nutné implementovat ta filtrační pravidla, která budou testovat, zda jsou jednotlivé individuální události v aplikaci iniciované dotazy nad citlivými daty.

Podobně jako při konstrukci množin identifikátorů tvořících citlivá data, i zde může výpočet narazit na limity rozumné časové náročnosti. Snadno se totiž nahlédne, že pro otestování, zda se zadaný dotaz neptá na některou z množin identifikátorů sestavených v kroku 1, je nutné SQL dotaz převést na disjunktivní normální formu (dále jen DNF), případně provést nějakou ekvivalentní operaci. Převod na DNF je obecně NP–obtížný. Je proto namístě hledat rozumné heuristické postupy.

Navržená metoda problém sestavení DNF obchází následovně: je stanoven počet p mintermů (literálů spojených konjunkcí), které je přípustné zkonstruovat. Pokud se v průběhu konstrukce DNF ukáže, že DNF mintermů obsahuje více než p, je dotaz automaticky označen za citlivý.

Počet p je možné optimalizovat v krocích 3–5.

Pokud se DNF podaří zkonstruovat, je dále otestováno, zda některá kombinace identifikátorů z množiny $I_c \cup I_m$ je podmnožinou identifikátorů v některém mintermu. Pokud ano, považujeme dotaz za citlivý, v opačném případě jej můžeme odfiltrovat.

Test popsaný výše lze realizovat ("hrubou silou") v čase $O(np|I_c \cup I_m|)$, kde n je počet identifikátorů a $|I_c \cup I_m|$ značí počet prvků množiny $I_c \cup I_m$.

4.4 Implementace filtrace dat

Cílem tohoto kroku je vytvořit funkční prototyp filtru (filtračních pravidel) v podobě modulu databázové sondy systému SIEM – nástroje DAM nebo prostřednictvím jeho konfigurace.

Funkčnost vytvořeného filtru spočívá v ověření splnění definovaných filtračních pravidel; následně při splnění pravidla bude posílat SQL dotazy k dalšímu vyhodnocení v DAM. V případě nesplnění podmínky filtr nepustí SQL dotaz dále do DAM.

Výstupem tohoto procesního kroku je modul filtrující SQL dotazy či sada nakonfigurovaných filtračních pravidel, tak aby do DAM vstupovaly pouze ty SQL dotazy, které jsou relevantní pro IB organizace.

4.5 Ověření a případná úprava pravidel filtrace

Pro ověření lze využít sestavená pravidla filtrace či již zmíněnou matici citlivých dat z procesního kroku 2 (byla–li sestavena). Oba tyto podklady slouží jako testovací scénáře. Tester zadává SQL dotazy dle této matice a následně ověřuje, že dané SQL dotazy se v případě potřeby promítly či nepromítly do systému SIEM. Pokud se výsledky shodují s definovanými filtračními pravidly, lze aplikaci nasadit do reálného provozu.

Vlastnímu ověření navržené metody se věnují autoři v kapitole níže.

4.6 Klíčové role a odpovědnosti v procesu

Na základě zkušeností z implementace této metody v praxi sestavil tým autorů matici klíčových rolí a jejich odpovědností v procesu – tzv. matici RACI (Responsible, Accountable, Consulted, Informed). Tuto matici uvádí následující tabulka. Pro úplnost je ke každému kroku přidán klíčový výstup a vstup pro to, aby mohl být proveden.

Definice klíčových odpovědností a rolí v procesu							
Krok	Vstup	Výstup	Bezpečnostní vedoucí	Aplikační specialista	Databázový specialista	Programátor / Administrátor	Tester
Analýza citlivých dat	Bezpečnostní politika organizace Klasifikace dat v organizaci Datový model organizace	Matice citlivých dat	A	C	R		
Analýza zpracování citlivých dat v aplikacích	Matice citlivých dat Rozsah systému řízení informační bezpečnosti organizace Schéma aplikační architektury Datový model organizace	Aktualizovaná matice citlivých dat	A	R	C	I	I
Sestavení pravidel filtrace dat	Matice citlivých dat	Pravidla filtrace dat	A	C	R	C	I
Implementace filtrace dat	Pravidla filtrace dat Matice citlivých dat	Modul filtrující SQL dotazy	A	C	C	R	I
Ověření a případná úprava pravidel filtrace	Matice citlivých dat Pravidla filtrace dat	Potvrzení o souladu pravidel filtrace s realitou	A	I	I	C	R

Tabulka 4: Definice klíčových odpovědností a rolí v procesu. Zdroj: autoři.

5 Ověření navržené metody

Autoři ověřili výše navrženou metodu empiricky. Jednalo se o praktické nasazení v organizaci zpracovávající osobní data. Organizace si z bezpečnostních důvodů nepřála být jmenována. Organizace má třívrstvou IT architekturu respektující principy SOA[8] s centrálním datovým úložištěm a má cca 8 000 zaměstnanců. Ověření probíhalo na implementovaném systému IBM QRadar (a IBM Guardium jako nástroj DAM) a mělo dva kroky:

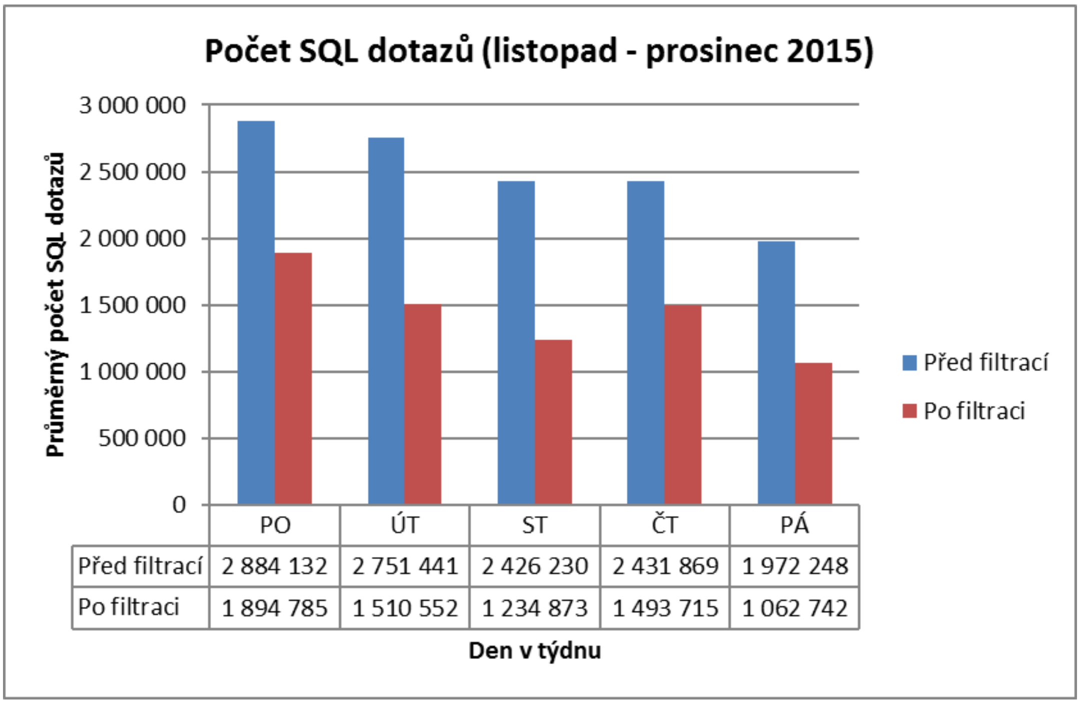
1. Ověření, zda navržená metoda přispívá ke snížení dat, jež vstupují do SIEM pomocí metriky počet SQL dotazů před a po aplikaci filtrace dat.
2. Vyhodnocení, zda metoda nesnižuje úroveň IB organizace tím, že neposkytne systému SIEM všechna data o SQL dotazech.

V prvním kroku ověření byla sledována jedna metrika, a to počet SQL dotazů. Ověření probíhalo v období trvajícím 7 týdnů, a to od 2. listopadu 2015 do 18. prosince 2015. Z nasbíraného vzorku byly vynechány víkendy a svátek (17.11.). Měření se týkalo všech aplikací zpracovávající citlivá data[9]. Měření probíhalo paralelně na vstupu databáze před aplikací filtračních pravidel a na výstupu filtru po aplikaci filtračních pravidel. Výhodou paralelního měření ve dvou bodech zároveň je eliminace sezónních a dalších rušivých vlivů.

Výše navržená metoda filtrace SQL dotazů vedla v dané organizaci k tvorbě celkem 250 filtračních pravidel.

[8] Service Oriented Architecture.
[9] To znamená všechny aplikace zahrnuté v bezpečnostním perimetru organizace.

Před filtrem bylo naměřeno průměrně 2 493 184 SQL dotazů denně, které by vstoupily do DAM k vyhodnocení. Po aplikaci filtračních pravidel došlo k poklesu počtu SQL dotazů na průměrně 1 439 333 za den. Průměrný počet SQL dotazů po aplikaci navržené metody filtrování dat je o 43 % nižší. Detailní průměrné počty dotazů za každý den v týdnu za měřenou periodu zobrazuje graf 2.



Graf 2: Počet SQL dotazů před a po filtraci. Zdroj: autoři.

Lze tedy konstatovat, že navržená metoda významně snížila množství dat, které vstupují do DAM k vyhodnocení.

Odfiltrované dotazy lze rozdělit do několika kategorií. Tyto kategorie jsou seřazeny dle svého podílu ve skupině:

1. Tzv. „Dummy“ dotazy – „dummy selekty“ (34,05 %), například se jedná o tento typ dotazů: *Select "1" from Dual* nebo *Select sysdate() from dual.* Tento typ dotazu může sloužit pro aplikaci k ověření spojení s databází, ale z pohledu ztráty citlivých dat je irelevantní. Jednalo se rovněž o dotazy typu ukládání logových záznamů: *„Insert into log…“*
2. Dotazy na číselníky (23,54 %) – tyto dotazy typicky vrací hodnoty číselníků, proto je lze považovat z bezpečnostního hlediska za irelevantní.
3. Procedury na databázi: *proc vymaz_log(den)* (22,6 %). Některé aplikace mohou volat předdefinované procedury, které má databáze vykonat. Procedury pracující s citlivými daty musí být identifikovány v kroku 2 a následně o ně musí být upravena filtrační pravidla. Procedura uvedená v příkladu vymaže log soubor za daný konkrétní den.
4. Poslední kategorií jsou takové dotazy, které nesměřovaly k získání citlivých dat (19,81 %). To jsou takové dotazy, které po parsování na tzv. SQL konstrukt (ten se skládá z příkazu – command, objektu – object, a pole – field) nepracují s předem definovanými poli tabulky, jež citlivá data obsahují.

Autoři analyzovali také variabilitu v počtu SQL dotazů za dané sledované období. Počet SQL dotazů ze strany aplikací směrem do databáze má několik složek, které jej významně ovlivňují:

1. „Fixní datový přesun" – tato doprava se objevuje každý den a nesouvisí s aktivitou uživatelů v aplikacích. Například: aplikace provádějí denní závěrku, počítají reporty apod.
2. SQL dotazy z okolních systémů – například vstupy z „reálného světa" v podobě každodenních dávkových importů z datových schránek.
3. SQL dotazy způsobené vlastní aktivitou uživatelů, která může být každý den odlišná.

Druhý krok ověření spočívá v posouzení, zda metoda nepřispívá ke snížení IB organizace tím, že snižuje množství dat systému SIEM. Toto autoři provedli porovnáním reportů o průměrném počtu bezpečnostních incidentů za týden před a po aplikaci filtrace dat. Měření probíhalo sekvenčně: měření před filtrací dat probíhalo za měsíce září až říjen 2015; měření po aplikaci filtrace dat probíhalo v období listopad až prosinec 2015. Porovnáním obou reportů bylo zjištěno, že průměrný počet bezpečnostních incidentů za týden zůstal na úrovni jednotek incidentů za týden před i po filtraci, což znamená, že nedošlo k žádným významným odchylkám.

Jako třetí krok ověření chtěli autoři zkoumat i množství výstražných hlášení ze systému SIEM před i po filtraci dat, avšak nedostali povolení od organizace tato data dále publikovat.

Na základě výsledků ověření z obou výše popsaných kroků lze konstatovat, že navržená metoda významně snižuje množství dat, jež vstupují do systému SIEM k vyhodnocení bez snížení IB organizace, čímž byl splněn cíl této práce.

Ekonomické přínosy navržené metody filtrace SQL dotazů jsou: nižší nároky na kapacitu datového úložiště[10] DAM o 30 %, Nižší vytížení serverů o 21 %, na kterých je celé řešení provozováno a tím lepší výkonnostní charakteristiky celého řešení vyhodnocující události kybernetické bezpečnosti. I přes významné snížení množství SQL dotazů, nedošlo k poklesu do nižšího licenčního pásma. Důvodem je široké nastavení licenčních pásem ze strany poskytovatelů SIEM systémů a také fakt, že se navržená metoda zaměřuje pouze na filtraci SQL dotazů a nebere v úvahu další způsoby redukce dat, které organizace může souběžně realizovat. Výhodou připojení databází prostřednictvím DAM však je možnost proaktivního řešení IB ve smyslu okamžitého přerušení aktivity, která směřuje na odcizení citlivých dat. Toto by v případě alternativních způsobů připojení databází nebylo možné.

6 Závěr

Cílem výzkumu prezentovaného v této práci bylo posoudit relevanci SIEM systémů pro organizaci z pohledu dnešních trendů v oblasti informační bezpečnosti a navrhnout a ověřit novou metodu, která vede ke snížení množství dat, jež systém SIEM zpracovává. Na základě provedeného průzkumu lze konstatovat, že systémy SIEM jsou pro organizace relevantní z pohledu plnění legislativních a normativních požadavků a také z pohledu realizace opatření proti rizikům. Autoři dále navrhli metodu, která je založena na filtraci SQL dotazů za účelem zlepšení provozu systému vyhodnocujícího události kybernetické bezpečnosti.

Ověření metody proběhlo empiricky na základě měření počtu SQL dotazů a bezpečnostních incidentů. Měření potvrdilo, že navržená metoda umožňuje významně snížit množství událostí (SQL dotazů), které by bylo nutné do systému zaslat k vyhodnocení, aniž by byla snížena úroveň informační bezpečnosti organizace. V našem případě je snížení významné. To může být zapříčiněno

[10] Organizace, kde ověření probíhalo, je legislativně vázána k ukládání historických záznamů po dobu 3 měsíců. Filtrování SQL dotazů, proto pro ni má velký význam z pohledu kapacity datového úložiště.

mimo jiné nízkou kvalitou aplikačního software zkoumané organizace, který generuje velké množství, z našeho pohledu, balastních SQL příkazů.

Přínosy navržené metody jsou zlepšení výkonnostních parametrů celého řešení vyhodnocujícího události kybernetické bezpečnosti a snížení potřebné kapacity datového úložiště pro nástroj DAM.

Autoři dále během ověřování jimi navržené metody identifikovali možné další vylepšení procesu optimalizace, a to pomocí sledování a filtrování SQL dotazů dle jeho iniciátora. Zejména se jedná o implementaci metrik pro jednotlivé vyhledávací údaje, které by umožňovaly provádět „scoring" jednotlivých SQL dotazů – obdobně, jako se používá při rozhodování, jestli je zpráva elektronické pošty SPAM. Tuto hypotézu chtějí ověřit v dalším výzkumu.

Zdroje

[1] CATES, S. (2015) *The Evolution of Security Intelligence*. Journal Network Security. 2015, Elsevier Science Publishers B. V. Amsterdam, The Netherlands.

[2] ČSÚ. (2015) *Informační technologie v podnikatelském sektoru*. [cit. 20. 12. 2015]. Dostupný online: https://www.czso.cz/csu/czso/podnikatelsky_sektor.

[3] DVOŘÁK, M., ŘÍHOVÁ, Z. (2011) *Problems of ISO 27001 Matrix certification*. Prague 25.05.2011 – 26.05.2011. In: Information Security Summit. Praha : TATE International, 2011.

[4] DVOŘÁK, M. (2013) *The preconditions for the management of IT security based on standard user behaviour.* ECON. 2013.

[5] GARTNER. (2015) Magic Quadrant for SIEM. [cit. 5. 1. 2016]. Dostupný online: https://securityintelligence.com/ibm-is-a-leader-again-in-2015-gartner-magic-quadrant-for-siem/.

[6] HORNE, W. (2015) Collecting, Analyzing and Responding to Enterprise Scale DNS Events.In: CODASPY '15 Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. ACM New York, 2015.

[7] PECCHIA, A., COTRONEO, D., GANESAN, R., SARKAR, S. (2014) *Filtering Security Alerts for the Analysis of a Production SaaS Cloud*. In: UCC '14 Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. IEEE Computer Society Washington, 2014.

[8] SPLUNK. (2015) *Splunk pricing*. [cit. 20.12.2015] Dostupný online: http://www.splunk.com/en_us/products/pricing.html.

[9] SUAREZ-TANGIL, G., PALOMAR, E., RIBAGORDA, A., SANZ, I. (2015) *Providing SIEM systems with self-adaptation*. Information Fusion Journal. 2015, Elsevier Science Publishers B. V. Amsterdam, The Netherlands.

[10] VERIZON. (2015) 2015 *Data breach investigations report*. [cit. 9. 1. 2016]. Dostupný online: http://www.verizonenterprise.com/DBIR/2015/.

Normy, Zákony a vyhlášky:

[11] ČSN. (2014) ČSN ISO/IEC 27001 Informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – Požadavky.

[12] Nařízení vlády č. 315/2014 Sb., nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o *kritériích pro určení prvku kritické infrastruktury.* Praha: MVČR, 2014.

[13] *Vyhláška č. 316/2014 Sb.,* o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Praha: MVČR, 2014.

[14] *Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.* Praha: MVČR, 2014.

[15] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.* Praha: MVČR, 2014.

Detecting malware with machine learning, from c&c to exfiltration
Detekce malware pomocí strojového učení, od C&C po exfiltraci

Michal Svoboda

Michal Svoboda
micsvobo@cisco.com

Michal Svoboda is a data analytics technical leader in the Cognitive Threat Analytics team within Security and Business Group of Cisco Systems. We do internet-scale security analytics of web traffic meta-data. Our mission is to build AI detection engines that reveal active breaches inside the networks of our customers, and that without traffic content inspection and signatures. Michal's role includes analytics, engineering, as well as leadership and continuous improvement of the team's unique methodology, practices, and tools.

Michal Svoboda je technickým expertem v oblasti analýzy dat. Pracuje pro skupinu Cognitive Threat Analytics, která je součástí Security and Business Group v rámci Cisco Systems. Naší misí je pracovat se záznamy o provozu na sítích našich zákazníků, a stavět samoučící se řešení, která odhalují aktivní bezpečnostní průniky. Tato řešení se neopírají o metody rozpoznávání pomocí signatur, ani o metody kontroly obsahu síťového provozu. Michalova role pokrývá datovou analytiku, programování, ale také vedení a zlepšování metodik a nástrojů, se kterými tým pracuje.

Detecting malware with machine learning, from c&c to exfiltration

In this example-driven session, we will cover novel malware detection methods, as used by Cisco Cognitive Threat Analytics (CTA) engine. Participants will learn about:

- Modern malware, its modus operandi and revenue streams.
- Evasion of traditional security defenses (firewall, antivirus).
- How network anomaly detection and machine learning can uncover its presence.
- Methods used to reduce false positives (FP) and false negatives (FN).
- Cohesive and actionable incident assembly.

Detekce malware pomocí strojového učení, od C&C po exfiltraci

V tomto příspěvku se budeme bavit o moderních metodách detekce malwaru, které se současně používají v Cisco Cognitive Threat Analytics (CTA). Na příkladech se účastníci naučí o:

- Moderním malware, jak funguje a jak vydělává.
- Pronikání tradičními bezpečnostními prvky (firewall, antivir).
- Způsobu nalezení malware pomocí detekce anomálií a strojového učení nad síťovým provozem.
- Metodách, které snižují počet nesprávných nálezů (false positive/false negative).
- Sestavování incidentů, které poskytují kompletní přehled o situaci.

Abstract

In this paper, we present an example of modern malware. We discuss how it operates and gains money for its operators and how it evades detection by antivirus and web reputation. Then, we describe how we can reliably detect its main behavioral aspects – command and control (c&c) and data exfiltration – by looking at network traffic meta-data and analyzing them in a working system using a combination of both supervised and unsupervised learning methods.

1 Meet #CMST

The malware with code name #CMST represents one of the more advanced botnets today. This designation covers a number of malware that exhibit similar network behavior, with industry names such as Miuref and Boaxxe. Known samples of this malware infect Windows based systems and are distributed through common channels, including but not limited to:

1. Droppers (small executables that download and install the malware, usually attached to spam e-mails, and similar),
2. Exploit kits (web-based applications that scan, identify, and exploit vulnerabilities in browsers),
3. Other malware that is already present at the endpoint.

The threat evades detection by signature-based antivirus software by using polymorphism, i.e. the executable is always unique when distributed, and also by employing strong encryption of its own parts with symmetric ciphers (RC4 or similar). Since the antivirus cannot see it, traditional cleaning is also impossible. It has also been observed that some samples behave differently or refuse to execute inside sandbox, therefore evading detection by sandboxing technologies. Finally, it employs the usual mix of anti-debug and heavy obfuscation to make reverse-engineering of its binary code as hard as possible.

From network standpoint, #CMST establishes a secure command-and-control (c&c) channel with the aid of strong asymmetric and symmetric ciphers (RSA, RC4, and other). This channel is carried over HTTP or HTTPS connections, as these are usually permitted by common firewall setups. Two transport methods have been observed:

1. Embedding the encrypted data into base-64 encoded string directly in URL of the request, and in the body of the response, which works reliably even with inspecting HTTP proxies in the way.
2. Direct communication to TCP port 443, which is normally used for HTTPS, but the protocol is not actually HTTPS, rather a binary custom protocol [EXFIL1], taking advantage of the fact that port 443 traffic is rarely validated or inspected.

Both of these channels are easy to miss using traditional network traffic inspection, but can be reliably detected with network behavior analysis methods used by Cognitive Threat Analytics (CTA). The c&c nodes are located in various countries and autonomous systems, and have been observed to promptly migrate once they gained negative reputation or got blacklisted.

Once installed on target machine, the malware can load additional modules or perform “software updates” on itself. Indeed, running an older sample warrants an immediate observation of megabyte-long downloads. Its main monetization methods are:

1. Click-jacking: a web browser plugin is installed that forces users to visit a revenue-generating page in addition to their normal browsing.
2. Click-fraud: an autonomous hidden browser is launched on the system that visits pay-per-click destinations.

In addition to click-fraud, the malware was also observed to exfiltrate gigabytes of data from infected computers, and participate in delivery of additional malware, such as ransomware.

2 Behavior analysis based on network meta-data

CTA analysis engine works with web proxy log entries. Such entries include source and target of the request, the URL, status codes, byte amounts (upload and download). For unencrypted HTTP transaction, the log entries include select headers, such as MIME-type and referrer. Web proxy log entries do not include the actual body of the request or response. The engine is therefore agnostic to the actual content of the web traffic and works purely on the principle of analyzing statistical models derived from the web log data. In the case of HTTPS, most of the HTTP-specific fields are missing, but this type of traffic can also be analyzed by CTA engine. The engine processes billions of such web proxy log entries daily.

Let’s examine the engine design from ground up. The proxy log is processed by the system in multiple stages which are, in order: anomaly detection, trust modelling, behavior classification, and incident assembly. The first two layers are based on unsupervised learning, and their purpose is to detect anomalies in the observed traffic. As we shall see in the next section, the malware traffic is highly anomalous when compared to the rest of the traffic. This layer is designed to have high recall, rather than precision. After this layer, we can safely remove 95% of the traffic from processing and focus on the remaining top anomalous 5% with more aggressive precision-biased algorithms.

The result of anomaly detection – the anomalies – can be actual threats as well as uninteresting traffic anomalies. To distinguish those, we employ a number of supervised classifiers that can classify threats with high precision in two ways:

1. Wide-range behaviors, such as various c&c types.
2. Campaign specific behaviors, which track individual campaigns. These are both novel and industry-known.

The final step is incident assembly from the detections. The system maintains a concept of incidents that include multiple behaviors to tell a story. The incidents can evolve over time as the threat escalates. Incidents can be created even retrospectively, if enough supportive evidence is gathered.

These incidents are assigned severity and confidence levels, which then are used to formulate concrete remediation steps. Some classifiers, especially the campaign-specific ones, are capable of producing incidents that have 100% confidence, thus do not require any additional investigation on the customer side.

3 Anomalous traffic

Let’s look at how #CMST traffic is handled by different layers of the CTA detection engine. A typical c&c web request has the form

Bytes up=385, Bytes down=337, HTTP status=200 OK, URL=hxxp://83.222.126.211/m/IbQD[… 112 more characters …]

The anomaly detection layer contains dozens of heterogeneous anomaly detectors that will assign an anomaly score from 0.0 (not anomalous) to 1.0 (extremely anomalous). These small detectors are allowed to err frequently. A snapshot of few example detectors acting on the #CMST behavior would be:

1. Very anomalous from "repetitive requests" detector based on the Fourier transform, since this behavior occurs periodically.
2. Very anomalous from "rarely visited sites" detector, as not many users visit this site.
3. Somewhat normal from "this site is visited with only one path" detector, since the encrypted string varies from request to request.
4. Somewhat normal from "site is visited during out of office hours" detector, since usually it requires active user session to produce c&c requests, although this can vary depending on the user's habits.
5. Absolutely normal from "visited countries" detector, since the IP address is hosted in the U.S.

As we can see, the individual detectors have very different opinions. Plainly averaging these opinions would result in high false positive (FP) and false negative (FN) rate of the anomaly detection layer. We are able to improve the results by applying additional techniques.

First step is to do several interim sub-aggregations on detectors that react to common attributes of the traffic, and then do an orthogonal average between these groups. Such groups are called ensembles and the "common attributes" can be found automatically instead of manual analysis.

The second step is trust modelling. If we can observe these requests for extended time periods, and on multiple users, we can average out random fluctuations in the detector results and form a consistent opinion (trust) of a given behavior. A trust model indexes the behaviors by position inside an N-dimensional cube whose dimensions are features of the behavior, such as number of bytes transferred, destinations, etc. This cube cell is maintained over long term, accumulating overall anomaly score. There are several such trust models, indexed by different features, and again their results are aggregated in multiple stages.

The applied principles of multiple aggregation and long-term trust modelling result in significant reduction of both false positives and false negatives. The typical anomaly score for #CMST behavior turns to be very anomalous, which makes it distinguishable from the normal traffic.

4 Getting it classified

The next step is to find and clearly label #CMST in the anomalies (some of which can still present non-threat behavior). We could obviously lock-on the IP address, but as has been mentioned before this is relocated frequently, and also that would prevent us from autonomously detecting alternate c&c channels. We use a robust classifier, so that if the malware decides to use another c&c node, it will be automatically detected again and again, as long as it represents an anomalous behavior.

To train this classifier, we proceed as follows. The already discovered c&c behavior is presented to a supervised learning algorithm, which then learns its key attributes. In this case, a random forest classifier is used. The learning method first derives over 300 features from the web-flow, such as byte transfer values, timings, URL features, etc. Then a number of random decision trees is generated, and the one with best performance is selected. This is further refined by splitting the classifier into multiple stages of decisions, which are run in sequence.

With this method, we can train a classifier that labels the HTTP requests of #CMST with very high precision. Same learning method can be used to train more classifiers for different campaigns, or to label generic malware techniques such as use of domain generation algorithms (DGAs).

5 Exfiltration in the kill chain

#CMST can also employ a different c&c channel, which connects directly to TCP port 443, normally reserved for HTTPS, but uses a custom binary protocol (which is neither HTTP nor HTTPS). This has been observed with mostly very large data uploads (over gigabyte). The supervised training method described above is not suitable for classifying this kind of behavior.

CTA engine uses a different method to spot the exfiltration traffic. For each combination of user and web server, a histogram of observed values of transferred bytes in both directions and request timings is perpetually created. This histogram is set to have finite number of bins and thus can be used as feature vector, allowing a linear classifier to be trained. The training method used for this classifier is based on optimizing the FP-50 benchmark [STEGO].

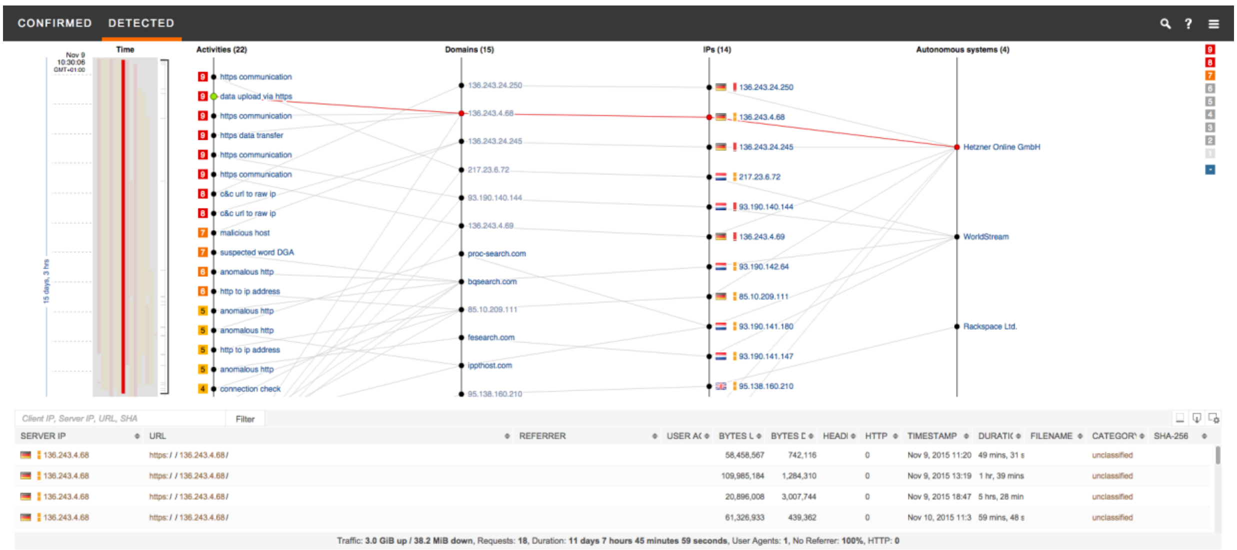
The anomaly detection pre-processing helps to a large extent, because this classifier can be trained and executed only on the more interesting anomalous data. It also allows to reduce computational footprint of the histograms.

Another trick to use here is correlation of the kill-chain. We know that the malware must execute different behaviors

1. It must first establish a working c&c channel
2. It will likely perform click-fraud
3. It will optionally perform data exfiltration

Therefore, we can look for the exfiltration events that occur at the same endpoint as the c&c events. If the c&c does not happen, we can delay the incident, if it happens we create an incident containing multiple behaviors. That in turn allows for increased confidence and severity levels of the incidents.

A visual example of such incident with generous amounts of c&c and exfiltration as shown on the dashboard:



6 Conclusion

We have described how one of the more advanced botnets, designated #CMST, operates on the network, how it gets money for its authors, and how it evades detection by traditional security systems. The network behavior analysis engine outlined in this paper allows for accurate detection of this threat, and is also robust against common changes in the malware c&c infrastructure. We have also presented how several indicators of compromise can be turned to work together if correlated on a kill-chain.

References

[EXFIL1] http://blogs.cisco.com/security/malware-stealing-gigabytes-of-your-data-as-seen-by-cognitive-threat-analytics

[STEGO1] http://www.cs.ox.ac.uk/andrew.ker/docs/ADK65B.pdf

Changes in attack strategies over the last five years and further outlook
Změny v přístupu útočníků za posledních pět let a další výhled

Jiří Slabý

Jiří Slabý
JiSlaby@deloittece.com

Jiří Slabý is a Senior Manager in the Advisory Services of Deloitte Czech Republic. He has more than 11 years of experience in the ICT industry. Jiri held many positions within the life-cycle of IT projects. He established a small IT company and as a lead architect designed and co-developed several information systems. Then joined bigger IT companies to continue his journey with complete pre-sale and sales activities, application/system/enterprise architecture and design of big systems and industry solutions. Currently Jiri acts as a head of Security & Privacy consulting group in Deloitte Czech Republic, which primarily deals with security audits, security monitoring, penetration testing and mobile security topics.

Jiří Slabý je senior manažerem v oddělení poradenských služeb společnosti Deloitte Česká republika. Má 11 let zkušeností v oblasti IT a z toho 8 let zkušeností v oblasti informační bezpečnosti. Má široké technické znalosti a je zkušeným IT a bezpečnostním architektem. Začínal jako zakladatel malé technologické firmy na vývoj systémů a postupně vystřídal několik větších společností, aby si vyzkoušel práci i v těch největších, jakými byly IBM nebo Deloitte. Zároveň se snažil fungováním v různých rolích pochopit, jak jednotlivé části v IT projektech do sebe zapadají, od prodeje HW, SW licencí, přes IT vývoj až po konzultační sféru. Jiří je držitelem doktorátu z ČVUT v Praze v oboru Systémové inženýrství a aplikovaná informatika.

Changes in attack strategies over the last five years and further outlook

The session will sumarize the most important breaches and attacks globally and specifically in the Czech Republic during the last 5 years. Then interesting statistics and patterns derived from past data will be presented. Ent the end the session will outline emerging trends for upcoming year with some hints how to defend against them.

Změny v přístupu útočníků za posledních pět let a další výhled

Již jsme si zvykli na překotný a extrémně rychlý vývoj ve světě IT technologií. To samé ale platí o bezpečnosti, protože každá nově představená technologie s sebou nese i bezpečnostní rizika a jelikož jsou technické vymoženosti využívány širokou veřejností, týká se jejich zabezpečení všech. Dokonce i těch, kteří zatím ještě odolávají IT pokroku a sami technologie moc nevyužívají, avšak mají své osobní údaje uloženy v systémech patřičných institucí a resortů státní správy a jsou tedy nepřímo také ohroženi. Autor se v příspěvku poohlédne a zhodnotí posledních 5 let v IT světě formou výčtu největších průniků a krádeží. Vyzdvihne největší bezpečnostní incidenty, rozdělí je na celosvětové a ty cílené na Českou republiku. Pokusí se v nich najít společné rysy. Zároveň se podívá na aktuální situaci na začátku roku 2016 a dovolí si představit výhled na nejbližší rok s důrazem na očekávané a nově vzniklé trendy, a jak se jim postavit.

Lidská společnost se stále více spoléhá na online prostředky, které tak nabývají na hodnotě a stávají se lákavým cílem pro útočníky všeho druhu. S tím roste význam zabezpečení těchto prostředků I související infrastruktury. Historie je v mnoha případech zdrojem poučení pro lepší přípravu na budoucnost.

S trochou nadsázky lze říci, že neuplyne týden, aby se neobjevila nová kritická zranitelnost, a měsíc, aby se nějaký incident neobjevil na předních stránkách novin. To, že se bezpečnost dostává do hlavního zpravodajství, je dobrá zpráva. Jednotlivci i organizace tak častěji vnímají bezpečnost jako důležitý faktor a nikoliv jako nutné zlo. Již dávno neplatí, že cílem útočníků jsou jen systémy umístěné v temných sálech velkých korporací, nýbrž každý jednotlivec, který pracuje s internetem a využívá nějaké služby. Zde jsou podle nás nejzajímavější události v oblasti kybernetické bezpečnosti minulých pěti let v ČR a zbytku demokratického světa[1].

1 Posledních pět let u nás a ve světě

Následující souhrn obsahuje jen několik málo nejzajímavějších a nejzásadnějších bezpečnostních událostí daného roku u nás a ve zbytku západního světa. Je ovšem na místě upozornit, že kritéria jako „nejzajímavější", „největší", „nejzásadnější" apod. jsou kritérii subjektivními. Neexistuje jednotné měřítko, podle kterého by se závažnost nebo zajímavost útoků měla posuzovat. Nejčastěji používaným měřítkem je velikost dopadu útoku na organizaci nebo jednotlivce, měřená penězi. Avšak i tak je velice zavádějící, neboť vždy se jedná o hrubý odhad, jak veliký finanční dopad měla ztráta daných dat na chod organizace.

Prezentovaný seznam je výběrem autorů.

1.1 2010

1.1.1 Svět

O zranitelnosti SCADA systémů se dlouho teoretizovalo, ale v červnu 2010 byl zachycen vzorek malwaru Stuxnet, který byl velmi přesně zacílen na sabotování íránského jaderného programu. Šlo navíc o první – oficiálně nepotvrzený – malware vytvořený státem, v tomto případě USA.

Závěr a přelom roku pak patřil WikiLeaks a s tím souvisejícím DDoS útokům skupiny Anonymous na společnosti Visa, Mastercard, Paypal a další.

1.1.2 ČR

V ČR byl rok 2010 poměrně klidný. Velké banky se potýkaly se skimmingem i phishingovými kampaněmi [1], Česká pošta před vánočními svátky čelila DDoS útoku na aplikaci zajišťující hromadné online objednávky [2].

1.2 2011

1.2.1 Svět

Tento rok probíhal ve znamení krádeží dat a hackingu skupin Anonymous a Lulzsec. Asi největším útokem bylo ukradení miliónů identit uživatelů herní konzole Playstation od Sony a hacknutí e-mailů

[1] Článek čerpá z mnoha veřejně dostupných zdrojů. Je však vhodné zmínit, že například o bezpečnostních incidentech v Číně existují jen strohé záznamy (pokud vůbec), a prezentovaný stav tedy odráží spíše realitu západního světa.

od největšího poskytovatele e-mailu zdarma, společnosti Google. V tomto případě jsou podezíráni hackeři z Číny. [3]

1.2.2 ČR

U nás jsme tento rok zaznamenali vlnu případů phishingu, napadeno bylo mnoho finančních institucí a pozor si museli dát například i zákazníci internetových providerů.

Česká spořitelna a Raiffeisenbank se potýkaly se zvýšeným počtem podvodných e-mailů, které se snažily vylákat z klientů využívajících internetové bankovnictví údaje o platebních kartách. Útočníci se snažili přimět adresáty kliknout na odkaz falešného internetového bankovnictví, a následně vložit údaje o jejich platební kartě [4,5]

1.3 2012

1.3.1 Svět

Počátek působení špionážního malware Turla se datuje do roku 2012 a sahá až do dnešních dnů. Tento malware se zaměřuje především na počítačové systémy vlád a velvyslanectví. Jeho působení není destruktivní, ale vykazuje prvky špionáže, neboť se zaměřuje na citlivé informace, které předává útočníkům. Celý kybernetický útok se dá rozdělit na tři hlavní části: V první části je využit spear phishing a watering hole útok pro infikování cíle trojským koněm Wipbot. V druhé části již zmíněný trojský kůň vytvoří v systému zadní vrátka, čímž připraví skrytou cestu pro infikování systému trojským koněm Turla. Zde nastává třetí část útoku, kdy Turla začíná dlouhodobě shromažďovat důležitá data. Turla se aktivuje vždy při zapnutí počítače.

1.3.2 ČR

Známé hackerské hnutí Anonymous v lednu 2012 zablokovalo pomocí DDoS útoku stránky České protipirátské unie (ČPU). Důvodem bylo prohlášení ČPU, ve kterém schvalovala zablokování stránek služby Megaupload. [6]

Další DDoS útok od hnutí Anonymous směřoval na stránky Ochranného svazu autorského (OSA); důvodem byl nesouhlas Anonymous s mezinárodní obchodní dohodou ACTA, jejímž účelem je vytvoření mezinárodního systému pro vynucování duševního vlastnictví. [7]

DDoS útokům skupiny Anonymous se nevyhnula ani Občanská demokratická strana (ODS). Útočníci nejprve provedli klasický DDoS útok a následně prolomili zabezpečení stránek a obsah nahradili svým vlastním. Podařilo se jim ukrást 30 000 jmen členů ODS. Tento seznam rozeslali médiím se vzkazem politikům, aby odmítli mezinárodní obchodní dohodu proti padělání ACTA. [8]

V únoru hacktivisté napadli web poslanecké sněmovny pomocí DDoS útoku; správci sítě se rozhodli web odpojit, a ten byl nedostupný až do časných ranních hodin. [9]

Jako událost s bezpečnostním přesahem je třeba vnímat i počin umělecké skupiny Ztohoven „Morální obroda“, kdy byli schopni v krátkém časovém úseku rozeslat poslancům PS PČR přes 500 podvržených SMS. [10]

1.4 2013

1.4.1 Svět

K události, která nenávratně změnila svět (nejen) IT bezpečnosti, došlo v květnu 2013, kdy bývalý systémový inženýr americké Národní bezpečnostní agentury (NSA) a senior advisor pro CIA Edward

Snowden zveřejnil přes 1,7 milionu tajných dokumentů NSA. K jejich ukradení použil svůj administrátorský účet a SSH klíče svých kolegů. [11] Snowdenovy dokumenty jsou stále zpracovávány, nicméně světu odhalily dlouhodobé masové sledování a odposlouchávání ze strany západních tajných služeb ve spolupráci s komerčními poskytovateli služeb a infrastruktury.

V říjnu 2013 došlo k uzavření největšího mezinárodního ilegálního obchodního portálu Silk Road a zatčení jeho majitele a provozovatele Rosse Ulbrichta. Tento portál používal systém TOR zajišťující anonymizaci uživatele při pohybu na internetu. Aféra měla bohužel za následek pouze zrod řady následovníků a upozornila veřejnost na existenci „darknetu“. K dopadení Ulbrichta nakonec zřejmě přispělo sledování a korelace pohybu bitcoinů, které mají (nepřesně) pověst naprosté anonymity.

Dne 20. března 2013 proběhlo v Jižní Koreji několik kybernetických útoků, které byly pojmenovány „DarkSeoul“. Tyto útoky cílily na řadu vládních webových stránek, jako například na webové stránky ministerstev, vojenských velitelství, amerických sil v Jižní Koreji a hlavních bankovních institucí v regionu. Odhaduje se, že bylo zasaženo okolo 40 vládních a firemních webových stránek. Při využití speciálního malware bylo možné provést útok typu DDoS. Pro tento útok se předpokládalo využití až 11 000 osobních počítačů, které byly nakaženy škodlivým kódem.

Od června 2013 bylo ruskou skupinou Dragonfly napadáno velké množství webových stránek organizací činných v odvětví energetiky. Nejvíce zasaženy byly organizace nacházející se v USA a západní Evropě. Internetové stránky byly infikovány škodlivým malware a přesměrovaly návštěvníky na stránky, které obsahovaly Lightsout exploit kit. Tento kit kontroloval software, který návštěvník používal. Toho bylo využito k získání kontroly nad napadeným počítačem. Z napadených počítačů v několika zemích získala skupina řadu informací, které mohou v budoucnu ohrozit operátory energetické rozvodné sítě, řadu podniků zabývajících se výrobou energie, provozovatele ropného potrubí a poskytovatele průmyslových zařízení.

Za největší krádež roku 2013 je v neposlední řadě považován únik až 110 milionů záznamů osobních údajů a kreditních karet zákazníků sítě obchodních domů Target.

1.4.2 ČR

V březnu do ČR nečekaně přišly masivní DDoS útoky a zastihly cíle nepřipravené. Po zpravodajských serverech byl úspěšně napaden největší lokální portál Seznam.cz a následující den také stránky řady českých bank, což v jednom případě vedlo i k výpadkům POS terminálů.

Poměrně primitivní útok v řádu jednotek Gbps byl veden zřejmě z Ruska a nikdo se k němu nepřihlásil, motivace zůstává nejasná. Dle délky výpadků lze usuzovat, že s tímto typem hrozby a v daném rozsahu chyběly praktické zkušenosti na všech úrovních infrastruktury, nicméně následné rychlé korektivní kroky CSIRTu i zasažených institucí tento typ útoků výrazně ztížily.

V červenci pronikl do hlavních zpráv bezpečnostní incident Penzijní společnosti Komerční banky, kdy bylo možné bez zvláštních nástrojů a zcela otevřeně získat osobní údaje přibližně 50 000 občanů z databáze kontaktů. Zranitelnost byla objevena náhodou a urychleně odstraněna, avšak bohužel pro KB až po zveřejnění. [12] Tento incident podtrhuje důležitost bezpečného životního cyklu softwaru, dohledu nad dodavateli a pravidelného penetračního testování.

V srpnu a září pak některé banky v ČR zasáhl zatím asi nejsofistikovanější útok, napadající dvoufaktorovou autentizaci a autorizaci pomocí SMS zpráv. Prvním krokem bylo získání přihlašovacích údajů do internetového bankovnictví. Útočníci poté pomocí velmi kvalitního phishingu přesvědčili oběti k instalaci „bezpečnostní aktualizace“ na svůj smartphone. Tento malware (Hesperbot) ve skutečnosti zachytával autorizační SMS zprávy a přeposílal je útočníkům. Výše ztrát, kterou cílové banky zaznamenaly, nebyla sdělena. Údajně však byli útočníci výjimečně rychlí ve vyklízení účtů, na které si prostředky převáděli. Následnou analýzou tohoto malware bylo zjištěno, že mohl být snadno použit pro útoky na další banky na českém a slovenském trhu. [13,14,15]

1.5 2014

1.5.1 Svět

V dubnu 2014 byla objevena jedna z doposud nejzávažnějších chyb v zabezpečení v historii internetu. Chyba s názvem Heartbleed v protokolu OpenSSL umožní útočníkům zachytávat datový přenos po do té doby důvěryhodném zabezpečeném protokolu HTTPS. Heartbleed otřásl především důvěrou veřejnosti v bezpečnost open source, přestože nikde nedocházelo k zatajování detailů o chybě. Dále došlo k několika mohutným krádežím dat – JPMorgan Chase (86 milionů záznamů zákazníků), Home Depot (56 milionů záznamů zákazníků), iCloud („citlivé“ fotografie a videa některých celebrit) a Sony (obrovský objem interní komunikace).

1.5.2 ČR

U nás byl rok 2014 ve srovnání se světem relativně klidný. Pokračovaly phishingové kampaně a skimming; incidenty však nijak nevybočovaly z běžné praxe a již se ani v tak hojné míře neobjevovaly v masmédiích.

1.6 2015

1.6.1 Svět

V únoru byla oznámena krádež osobních údajů klientů americké zdravotní pojišťovny Anthem. [16] V červnu obvinily USA Čínu z kybernetického útoku, při kterém byla ukradena data čtyřem miliónům zaměstnanců vládních organizací s bezpečnostní prověrkou. Cílem útoku byl vládní personální úřad (OPM) a ukradena byla citlivá data jako jména, čísla smluv sociálního pojištění a data narození osob, které byly „jen“ v evidenci tohoto úřadu. V červenci skupina „The Impact Team“ získala a posléze zveřejnila data 37 milionů uživatelů internetové seznamky „pro nevěrné“ Ashley Madison. Na tomto příkladu je nejjasněji vidět, že uživatelé služby utrpí mnohem větší škodu než cíl útočníka.

Kampaň Carbanak/Anunak, která byla objevena a popsána v únoru 2015, údajně způsobila bankám celkové ztráty ve výši jedné miliardy dolarů. Ponecháme-li stranou spornou výši škody a její rozsah, výjimečná je přesnost provedení, kdy útočníci při podvodných transakcích věrně napodobovali chování konkrétních uživatelů, aby transakce nevypadaly neobvykle a vyhnuly se tak odpovídající kontrole. [17]

1.6.2 ČR

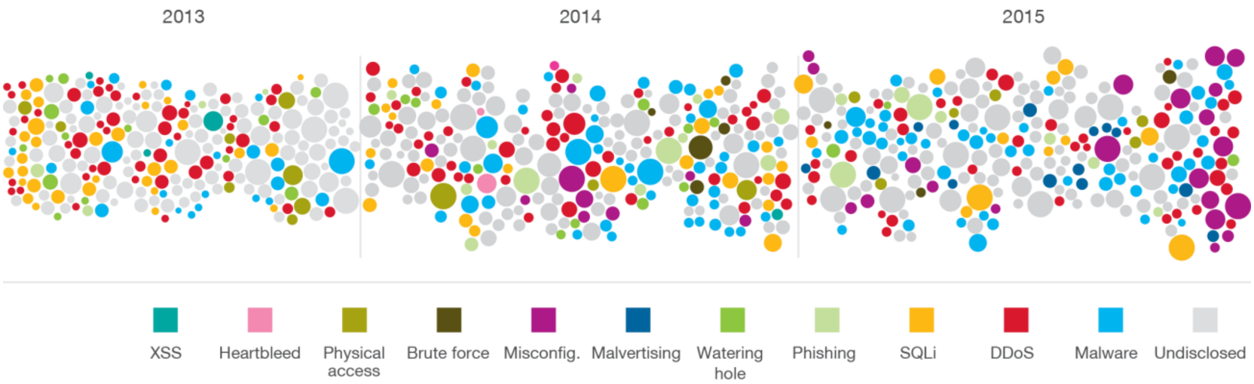
I Českou republiku zasáhla vlna ransomware. Zajímavá je perfektní lokalizace podpůrného „ekosystému“ včetně nastavení cen odpovídajících lokální příjmové rovině (v řádech tisíců korun). Platba probíhá vesměs v bitcoinech. Phishing se začal vyskytovat na sociálních sítích a kvalita standardního e-mailového phishingu trvale rostla. Na přelomu roku se útočníkům z rasistické skupiny White Media podařilo proniknout na soukromý e-mailový účet premiéra Bohuslava Sobotky a zveřejnit několik e-mailů z jeho schránky. Podle poskytovatele služby Seznam.cz se nejednalo o hackerský útok jako takový, protože na e-mailovém účtu nedošlo k žádné podezřelé aktivitě. Útočník už heslo musel znát, když se na e-mailový účet připojoval. Je tedy pravděpodobné, že útočníci premiérův počítač předem napadli. [18]

1.7 Historie ukazuje vzorce chování útočníků

V oblasti bezpečnosti je velice těžké vyvozovat trendy, neboť útočníci se již dávno nesnaží ohromit svět kreativitou, ale vydělat kriminální činností peníze, a je jedno, zda použijí deset let starý trik nebo úplnou novinku. Přesto je možné jisté závěry z minulosti vypozorovat.

1.7.1 Staré přístupy stále fungují

Obrázek 1 ukazuje porovnání posledních tří let z pohledu typu použitého útoku. Velikost kruhu značí závažnost průniku a barva poté typ útoku dle legendy.



Obrázek 1: Přehled největších útoků v letech 2013 až 2015 a jejich rozdělení podle druhu.

Tento přehled ve zkratce prozrazuje několik faktů:

- pro velké úniky dat se již pomalu vytrácí dříve velice hojně využívaný SQL injection útok;
- přes veškerou snahu výrobců bezpečnostních technologií a firem o jejich implementaci existuje značné procento útoků, u kterých se nepodaří zjistit jejich původ a provedení;
- každým rokem roste počet sofistikovaného malware;
- spíše než dlouhodobě plánované akce jsou DDoS útoky sezónního charakteru a reagují na okamžitou situaci;
- útočníci se mnohem více zaměřili na špatně nebo nevhodně nastavené prvky infrastruktury, kdy není třeba vysloveně zneužít zranitelnost, ale kde nepozornost nebo ledabylost administrátorů otevře dveře mnohem snáze;
- klasické phishingové kampaně jsou stále populární, dokonce mírně na vzestupu.

Jiný pohled na trendy v hrozbách poskytuje každoroční zpráva ENISA (Obrázek 2). Jak je vidět, v pořadí prvních pěti kategorií k žádné změně meziročně nedošlo, pouze roste jejich intenzita.

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	→	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	→	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓

Obrázek 2: Nejrozšířenější typy hrozeb dle ENISA.

1.7.2 Vlády nestojí stranou

Kromě vlny hacktivismu je jasně patrné rostoucí zapojování států na kybernetickém bojišti, což jde ruku v ruce s vývojem geopolitické situace. Po Snowdenově odhalení je navíc zřejmé, že tito aktéři disponují značnými prostředky a operují mimo rámec běžných zákonů.

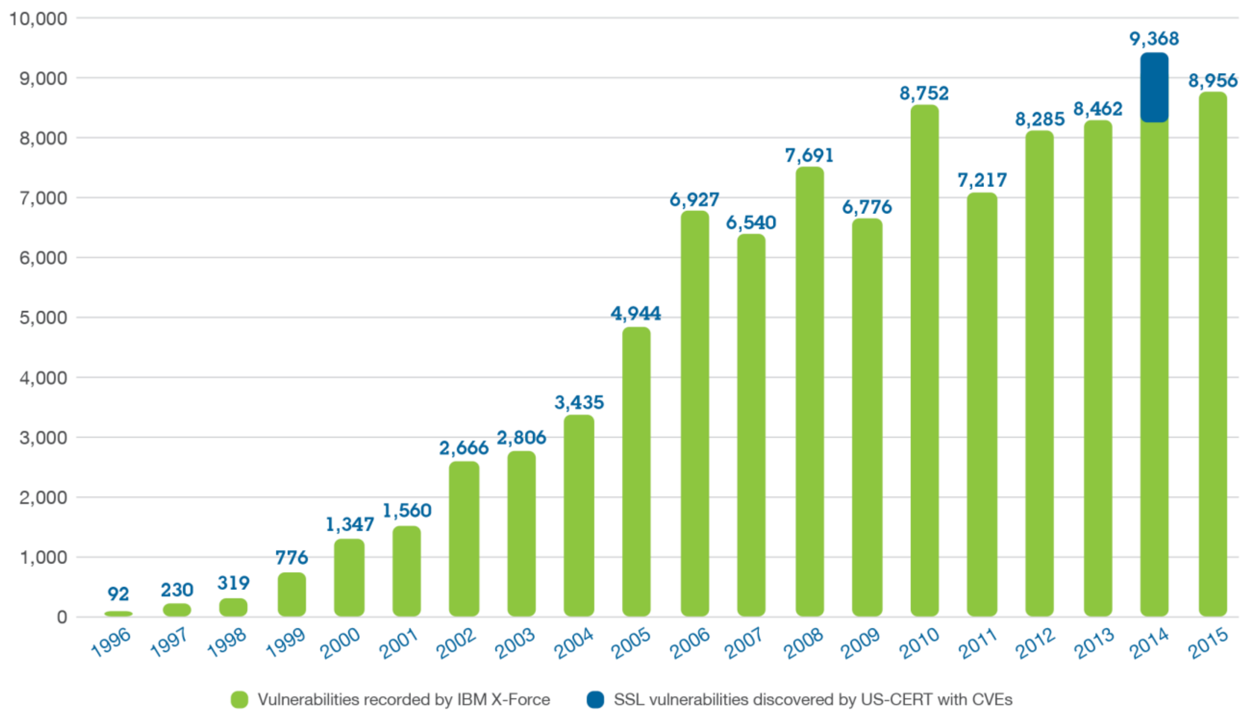
Ukrajinská krize naplno ukázala, že kyberprostor je regulérní součástí bojiště a že moderní armády jsou na válku připraveny. Kybernetické útoky se během posledních pěti let staly plnohodnotnou součástí zbrojního arzenálu a propagandy.

1.7.3 Phishing: větší zacílení, chatrnější identita

Pravděpodobně neexistuje e-mailová schránka, do které by nebyl někdy doručen alespoň jeden nigerijský (či podobný) dopis. Tento typ útoku stále přetrvává, ale celkově dochází ke specializaci. Malware Carbanak, za kterým stojí stejnojmenná kriminální skupina a které se připisuje krádež v součtu až 1 miliardy amerických dolarů, je toho příkladem. Nicméně přesnější zacílení a rostoucí kvalita je zjevná i v běžném spamu a také na sociálních sítích. Je to způsobeno i zvětšující se digitální stopou, kterou za sebou jednotlivci nechávají.

1.7.4 Technická zranitelnost se neřeší

Odstraňování zranitelnosti aplikací a infrastruktury se za posledních pět let nikam výrazně neposunulo, využití zranitelnosti tedy stále zůstává nejběžnějším způsobem průniku. Podle studie společnosti Verizon bylo v roce 2015 až 99,9 % zneužitých zranitelností známo více než 1 rok [19]. Z pohledu na Obrázek 3 je patrné, že počet nalezených zranitelností se za poslední léta výrazně nezvýšil, ale ani nesnížil.



Obrázek 3: Počet zranitelností.

1.7.5 Detekce incidentů stále pokulhává

Detekce bezpečnostních incidentů se zlepšuje, ovšem velmi pomalu. Podle studie Trustwave z roku 2013 činila průměrná doba odhalení bezpečnostního incidentu 210 dní, v roce 2015 to bylo 188 [20].

I v případě, že je incident detekován, je jeho následné řešení mnohdy také problémem. Řada organizací se věnuje primárně běžnému provozu a vyšetřování incidentu, kdy často není ztráta zřejmá ihned, má většinou podřadnou prioritu. Dobrou zprávou je rostoucí používání SIEM systémů a dohledových bezpečnostních center (SOC).

1.7.6 Budete úspěšně napadeni

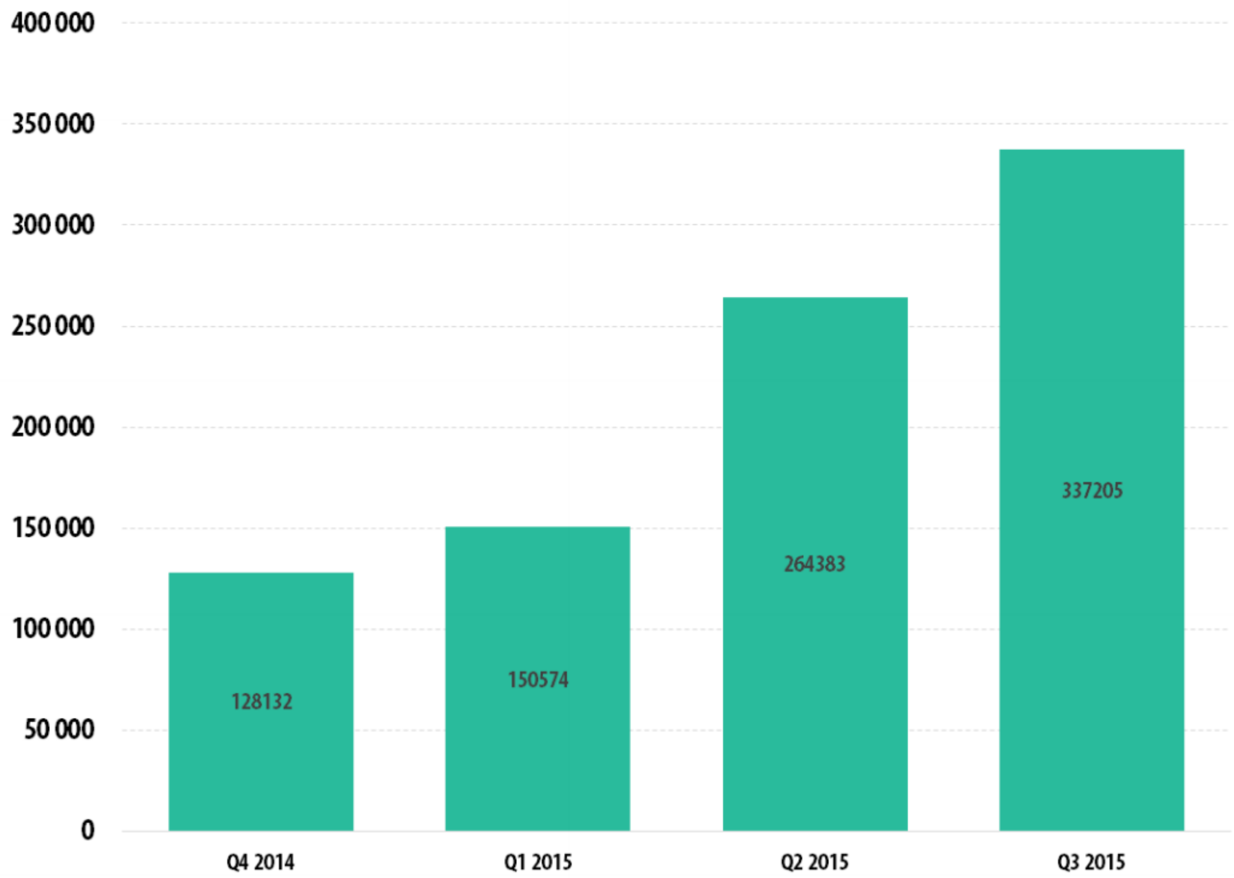
Pokud vaše společnost nebyla zatím úspěšně napadena, v nadcházejících letech zcela jistě bude. Případně platí v posledních letech velmi skloňovaná verze předchozí věty – pokud ještě nebyla vaše společnost napadena, jen o tom ještě nevíte. Velké úniky dat a informace nejen ze Snowdenova odhalení přispěly k tomu, že se idea neprostupné vrstvené hradby okolo IT prostředků ukazuje být utopickou. Výrobci se již několik posledních let snaží tomuto trendu přizpůsobit a postupně přechází s výrobky ze skupiny pro zamezení napadení (protože je nevyhnutelné) na typ pro detekci napadení (co nejdříve, co nejpřesněji).

Je vhodné si uvědomit, že vy nebo vaše organizace nemusí být útočníkovým cílem, ale pouze „přestupným bodem“, jak se dostat k informacím.

1.7.7 Ransomware

Ransomware je na silném vzestupu a díky dnes již běžnému využívání velkých úložišť i v domácím prostředí představuje velice úspěšnou formu útoku. V průběhu let vyzrál z triviálního blokování přihlášení do systému v sofistikovaný šifrovací malware a ochrana proti němu je zatím velmi obtížná.

FBI dokonce před časem vydala tiskovou zprávu, ve které doporučuje obětem „prostě zaplatit". I přes to, že se objevily varianty, kdy šlo o podvod a ani po zaplacení nedošlo k odšifrování obsahu, tak ve většině případů se jednalo o „legitimní" ransomware, kdy po zaplacení oběť dostala svá data zpět.



Obrázek 4: Počet uživatelů napadený Trojan-Ransom.

1.8 Světlá nebo temná budoucnost? Top trendy pro 2016

Stručný přehled incidentů za uplynulá léta jasně ukazuje, že rozhodně není na místě předpokládat snížení aktivity hackerů. Naopak, úspešnost řady útoků je dokladem toho, že kybernetický prostor je dnes nejvýdělečnějším odvětvím zločinu a mnohé skupiny dříve operující na černém trhu se zbraněmi, drogami a dalším nelegálním zbožím se dnes přesouvají do online světa. DDoS útoky dnes rutinně překračují 100 Gbps (zatím nepotvrzený rekord drží útok na BBC z ledna 2016 – 602 Gbps [21]). Požadavky na patchování rostou a společnosti stále nestíhají bezpečnostní záplaty aplikovat včas.

Je pravda, že malware se už dnes nešíří pomocí disket a místo USB klíčenek se dnes kradou celé laptopy, ale pro kvalitní zabezpečení je stále platným pravidlem mít základní bezpečnostní opatření v pořádku a používat zdravý selský rozum.

Kybernetická bezpečnost je závodem ve zbrojení, ve kterém jsou „ti dobří" z principu v nevýhodě. Staré hrozby nikam nemizí, s širší paletou útoků a jejich rostoucí kvalitou pouze stoupá „tlak" na bránící se stranu. Je dobrou zprávou, že povědomí o bezpečnosti v kybersvětě roste mezi organizacemi i běžnými uživateli, a proto se s některými typy hrozeb setkáváme méně než dříve, kde typickými představiteli této mizící skupiny jsou:

- SQL injection, session hijacking (penetrační test je prakticky nezbytný krok při publikaci webové aplikace).
- Odposlouchávání bezdrátových sítí (šifrování WEP již zcela vymizelo, uživatelé využívají end-to-end šifrování).
- Defaultní uživatelské účty a jejich hesla (to ovšem neplatí o používání slabých a odhadnutelných hesel, které jsou stále jedním z nejslabších míst).

To v žádném případě neznamená, že útočníci přestali tyto uvedené možnosti hledat. Pouze je nacházejí méně často.

1.8.1 Ransomware v první lize

Rok 2016 bude rokem ransomware. Dokud IT průmysl nepřijde s široce přijatelným řešením, jedná se pro útočníky o snadný výdělek. Výzkum Cisco poskytl výpočet, který ukazuje, že jen na jednom z rozšířených virů typu ramsomware (Angler) útočníci vydělávají až 34 milionů USD ročně [22]. Ransomware se začne masivněji rozšiřovat na mobilní telefony, kterým uživatelé svěřují stále více cenných dat, a zaměří se také na prostředí cloudových úložišť. První verze ransomware ukázaly i své sranitelné stránky a u některých se výzkumníkům podařilo nalézt klíč k odšifrování bez nutnosti zaplacení, ale útočníci se poučili a již na toto nelze spoléhat.

Doporučení: V případě jednotlivých uživatelů zde pomůže nejstarší opatření – obezřetnost a selský rozum. V mnohých případech se totiž ransomware šíří za pomoci naivních uživatelů, otevírající podezřelé přílohy od neznámých odesílatelů, než konkrétní technickou zranitelností. V korporátním prostředí je vhodnou prevencí především důsledné zálohování a kontrola konzistence.

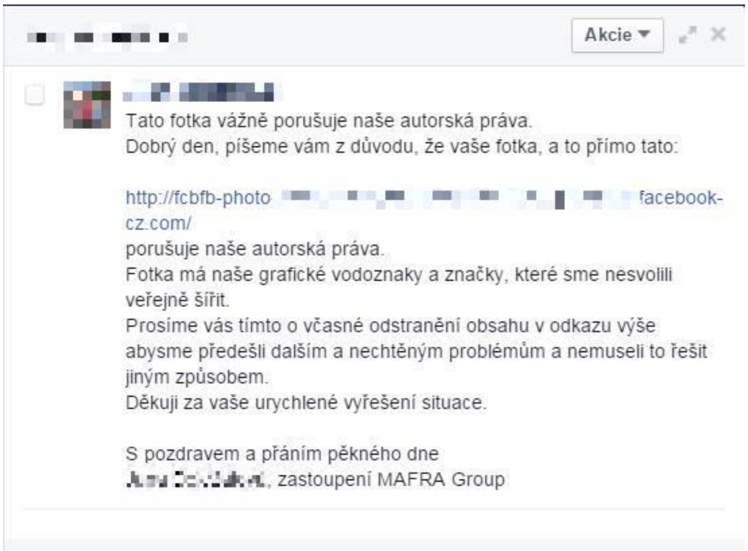
1.8.2 Mobilní malware

Nárůst mobilního malware je s neuvěřitelně rychlou adopcí chytrých zařízení všeho druhu raketový. Pro následující období předpokládáme rapidní nárůst škodlivých kódů a to především o dva typy malware – ransomware a sledování uživatelovy aktivity.

Doporučení: Zavést vhodné Enterprise Mobility Management řešení pro snížení rizika úniku citlivých dat, ale pamatovat na potřeby uživatelů. Velmi důležitým krokem také je přepracovat systém sdílení souborů ve společnosti a to z důvodů, aby uživatelé nemuseli v případě restriktivních omezení hledat nové snazší (a nebezpečné) způsoby, jak sdílet firemní dokumenty, nad kterými nebude mít společnost kontrolu (dropbox, soukromé emaily, atp.)

1.8.3 Phishing blíže uživatelům

Phishingové kampaně budou mnohem cílenější. Před lety byly v ČR běžné amatérsky a strojově přeložené e-maily plné pravopisných chyb a nekvalitní napodobeniny webových stránek. Jejich úspěšnost nebyla valná. Poslední dva roky ukázaly, že i malá Česká republika je pro útočníky zajímavým cílem a vyplatí se jim věnovat dostatečnou pozornost lokalizaci. Lze tedy čekat mnohem kvalitnější padělky e-mailů a celých služeb s cílem oklamat i zkušené oko profesionála. Posledním trendem jsou phishing útoky na sociálních sítích. Obchodní význam přítomnosti na těchto sítích pro společnosti roste, bývají i oficiálním komunikačním prostředkem např. pro podporu klientů. Hodnota facebook účtu takové firmy má pro útočníka vysokou cenu. Ve výzkumu Cloudmark 84 % dotazovaných společnosti uvedlo, že v posledních 12 měsících zaregistrovali úspěšný spear phishing.



Obrázek 5: Příklad facebook phishingu.

Doporučení: Aby bylo toto riziko akceptováno top managementem, je třeba ukázat jeho dopad v podobě provozního rizika. Snažit se vyčíslit škody, které takové kampaně způsobují. Dobrým způsobem je vedení prezentovat příklady malware, který se do instituce dostal díky takové kampani. V druhém kroku doporučujeme jednoduchý monitoring v podobě sledování hlaviček protokolu http, které snadno ukáží většinu případů phishingové kampaně.

1.8.4 Multi platformní malware

Uživatelé alternativních operačních systémů již nejsou v pozadí útočníků a drtivá většina moderního malware vzniká paralelně přinejmenším na 2 nebo všechny 3 hlavní platformy (Windows, Linux, MacOS). V roce 2016 se procenta ještě více vyrovnají a především ransomware bude vznikat na platformy Windows a MacOS simultánně.

Doporučení: Bohužel neexistuje jedno doporušení, které tento trend zvrátí, ale máme-li jmenovat, poté v první řadě bezpečnostní školení uživatelů světa Apple výroků, kteří v mnohem větší míře reprezentují skupinu ne-IT vzdělaných uživatelů, spoléhajících na automatiku platformy nastavenou výrobcem.

1.8.5 Přemýšlení jako cílová skupina

Velikým trendem, který se začal objevovat až na konci roku 2015 a je tedy velice čerstvý, je změna přemýšlení útočníků. Starší útoky (libovolnou metodou) měly společný základ v tom, jak útočníci přemýšleli – nalézt velmi kredibilní oběť, vědět, co má smysl od takové zcizit a to ukrást. Příkladem je dostat se k bankovnímu účtu obsahující miliony korun a čím více na účtu uloženo tím lépe. Takové myšlení se mění, protože ukrást takovéto abnormálně veliké množství peněz bude jednak snáze detekováno a výrazně těžší takovou částku dostat do normálního oběhu. Útočníci přešli na přemýšlení uživatelů tím, že přestali být chamtiví a cílí na běžné uživatele. Příkladem je malware, který e vydává za oficiální program policie, usvědčující uživatele z porušování vlastnických práv a požadující zaplacená „pokuty“. Taková pokuta se pohybuje v řádu jednotek EUR nebo USD a je tedy uživateli akceptována a zaplacena. Navíc povahou odrazuje uživatele při takovém incidentu notifikovat policii, že došlo k útoku neboť předpokládá, že uživatel někdy v historii skutečně vlastnická práva porušil (stažení filmu, seriálu, hry, programu apod.) a nepůjde se dobrovolně udat.

Doporučení: Platí stejné doporučení jako v případě ransomware a obecného malware.

Reference

[1] HORÁČEK, Filip. Na bankomatech České spořitelny opět byly falešné čtečky – iDNES.cz [online]. c2010 [cit. 201604-05]. Dostupný na World Wide Web: http://ekonomika.idnes.cz/na-bankomatech-ceske-sporitelny-opet-byly-falesne-ctecky-pz0-/ekonomika.aspx?c=A100816_182730_ekonomika_fih.

[2] ŠŤASTNÝ, Jiří. Hackeři útočí na Českou poštu, firmy nemůžou podávat on-line objednávky – iDNES.cz [online]. c2010 [cit. 2016-04-05]. Dostupný na World Wide Web: http://ekonomika.idnes.cz/hackeri-utoci-na-ceskou-postu-firmy-nemuzou-podavat-on-line-objednavky-13o-/ekonomika.aspx?c=A101209_200754_domaci_js.

[3] 2011 CyberAttacks Timeline – HACKMAGEDDON [online]. c2011 [cit. 2016-04-05] Dostupný na World Wide Web: http://www.hackmageddon.com/2011/06/22/2011-cyberattacks-timeline/.

[4] FIŠER, Miloslav. Raiffeisenbank čelí phishingovým podvodům – Novinky.cz [online]. c2011 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.novinky.cz/internet-a-pc/221377-raiffeisenbank-celi-phishingovym-podvodum.html.

[5] MERAVÁ, Tereza. Podvodníci zaútočili na klienty UPC. Rozesílají jim falešné e-maily – iDNES.cz [online]. c2011 [cit. 2016-04-05]. Dostupný na World Wide Web: http://mobil.idnes.cz/podvodnici-zautocili-na-klienty-upc-rozesilaji-jim-falesne-e-maily-1d8-/mobilni-operatori.aspx?c=A111111_100559_mob_operatori_mer.

[6] WIFT. Útok Anonymous na web České protipirátské unie a co je to vlastně DDoS? – Útok na web ČPU a její reakce | Diit.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://diit.cz/clanek/utok-anonymous-na-web-ceske-protipiratske-unie-a-co-je-to-vlastne-ddos.

[7] NÝVLT, Václav – KUŽNÍK, Jan. Anonymous napadli servery OSA, web české vlády i Evropského parlamentu – iDNES.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://technet.idnes.cz/anonymous-napadli-servery-osa-web-ceske-vlady-i-evropskeho-parlamentu-1mp-/sw_internet.aspx?c=A120126_134112_sw_internet_nyv.

[8] Hackeři zveřejnili osobní data tisíců členů ODS — ČT24 — Česká televize [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.ceskatelevize.cz/ct24/domaci/1181108-hackeri-zverejnili-osobni-data-tisicu-clenu-ods.

[9] PELECH, Tadeáš. Web sněmovny byl nepřístupný – jak se bránit DDoS? | Computerworld.cz [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://computerworld.cz/analyzy-a-studie/web-snemovny-byl-nepristupny-jak-se-branit-ddos-44521.

[10] Morální Reforma [online]. c2012 [cit. 2016-04-05]. Dostupný na World Wide Web: http://ztohoven.com/mr/index-cs.html.

[11] ESPOSITO, Richard – COLE, Matthew. How Snowden did it – NBC News [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.nbcnews.com/news/other/how-snowden-did-it-f8C11003160.

[12] SLÍŽEK, David. Chyba v bankovnictví Komerční banky umožňovala přístup k datům o klientech – Lupa.cz [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.lupa.cz/clanky/chyba-v-bankovnictvi-komercni-banky-umoznovala-pristup-k-datum-o-klientech/.

[13] Komerční banka. ČBA varuje před novou formou hackerských útoků – Komerční banka [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.kb.cz/cs/o-bance/tiskove-

centrum/tiskove-zpravy/cba-varuje-pred-novou-formou-hackerskych-utoku-1712.shtml.

[14] PELANTOVÁ, Petra – Euro. Jak vysát konta. Hackeři dál útočí na české banky [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://euro.e15.cz/archiv/jak-vysat-konta-hackeri-dal-utoci-na-ceske-banky-1040752.

[15] PERMAN, Tomáš. ESET odhalil trojana, který ohrožoval klienty českých bank [online]. c2013 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/article/eset-odhalil-trojana-ktery-ohrozoval-klienty-ceskych-bank/.

[16] PERLROTH, Nicole. Anthem Hacking Points to Security Vulnerability of Health Care Industry – The New York Times [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0.

[17] GReAT. The Great Bank Robbery: the Carbanak APT – Securelist [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/.

[18] MIKULKA, Milan. Ochranu hackeři neprolomili. Znali heslo, nebo skenovali Sobotkův počítač, brání se Seznam – Aktuálně.cz [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://zpravy.aktualne.cz/domaci/utocnici-skenovali-premieruv-pocitac-nebo-znali-heslo-k-jeho/r~9fd7924cb55311e5928a002590604f2e/

[19] Verizon. 2015 Data Breach Investigations Report [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.verizonenterprise.com/DBIR/2015/.

[20] Trustwave. 2015 Trustwave Global Security Report [online]. c2015 [cit. 2016-04-05]. Dostupný na World Wide Web: https://www2.trustwave.com/GSR2015.html.

[21] KHANDELWAL, Swati. 602 Gbps! This May Have Been the Largest DDoS Attack in History [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[22] ČÍŽEK, Jakub. Cisco zmapovalo virus Angler. Záškodníci na něm vydělají až 34 milionů dolarů ročně – Živě.cz [online]. c2016 [cit. 2016-04-05]. Dostupný na World Wide Web: http://www.zive.cz/bleskovky/cisco-zmapovalo-virus-angler-zaskodnici-na-nem-vydelaji-az-34-milionu-dolaru-rocne/sc-4-a-181359/default.aspx.

Your genome and insurance: opportunity or threat?
Váš genom a pojištění: příležitost nebo hrozba?

Ondřej Antoš

Ondřej Antoš
ondrej.antos@squirepb.com

Ondřej Antoš aims to connect the worlds of legal practice and academia in the field of law and technology. After graduation from the Faculty of Law, Masaryk University (Master's degree, 2014) works on one hand as a legal trainee in the Prague office of a global law firm Squire Patton Boggs (mergers & acquisitions, intellectual property and information and communication technology) and on the other hand as an external Ph.D. student at the Faculty of Law, Masaryk University.

Ondřej Antoš se snaží propojovat světy právnické praxe a akademie v oblasti práva a technologií. Po absolvování Právnické fakulty Masarykovy univerzity (Mgr., 2014) pracuje na jedné straně jako koncipient v pražské kanceláři globální advokátní kanceláře Squire Patton Boggs (fúze a akvizice, technologie a duševní vlastnictví a telekomunikace) a na druhé straně jako externí Ph.D. student na Právnické fakultě Masarykovy univerzity.

Your genome and insurance: opportunity or threat?

The paper deals with legal matters arising in connection with the more and more common exploitation of genetic information in the provision of life insurance and private health insurance. Author of this paper aims to acquaint the reader with essential legally-philosophical conceptions and principles, existing law in the Czech Republic and comparison with other jurisdictions in this dynamically developing area.

Váš genom a pojištění: příležitost nebo hrozba?

Příspěvek se zabývá právními otázkami vyvstávajícími v souvislosti s čím dál tím běžnějším využíváním genetických informací při poskytování životního pojištění a soukromého zdravotního pojištění. Autor příspěvku si klade za cíl seznámit čtenáře se základními právně-filozofickými koncepcemi a principy, platným právem v České republice a srovnáním s ostatními právními řády v této dynamicky se rozvíjející oblasti.

1 Úvod

Obrovské pokroky v analýze DNA a jejím praktickém využití vytváří nové problémy v mnoha tradičních právních oborech. V tomto příspěvku se zabýváme zejména otázkou, zda mohou pojišťovny po potenciálních pojištěncích vyžadovat poskytnutí genetických informací. Tato otázka je relevantní zejména v kontextu životního a soukromého zdravotního pojištění.

2 Filozoficko-právní východiska

Od svých počátků je pojištění založeno zejména na principu solidarity a principu spravedlnosti.[1] Princip solidarity stanoví, že všichni pojištěnci se podílí na nákladech a užitcích spojených s pojištěním. Princip spravedlnosti oproti tomu vyžaduje, aby účast jednotlivých pojištěnců na pojištění byla přiměřená jejich individuálnímu riziku. Princip spravedlnosti pak slouží jako základ pro uplatňování zásady uberrimae fidei neboli zásady „všechno v dobré víře“. Při úvaze, zda jsou pojišťovny oprávněny vyžadovat po potenciálních klientech genetické informace, je nezbytné posuzovat, jestli není takové jednání ze strany pojišťovny diskriminací.

Při posuzování diskriminačního potenciálu genetických informací se otázka jejich využití redukuje na správnost požadování a následného využívání skutečnosti, která je mimo volní dispozici člověka. Pojišťovny posuzují také řadu dalších informací, jako je např. kouření tabáku či požívání alkoholu, které se primárně odvíjí od vůle každého člověka. Pojišťovny ale rovněž běžně požadují anamnézu potenciálního pojištěnce i členů jeho rodiny. Genetické informace jsou však každému vrozené a determinují naše pohlaví, tělesnou konstituci, zdravotní stav, ale i náchylnost k chorobám. Navíc i přes velký vědecký pokrok v genetických terapiích není možné geny běžně opravovat či vyměňovat.

Související otázkou, totiž diskriminací podle pohlaví v kontextu pojišťovnictví, se zabýval Soudní dvůr Evropské unie (dále jen „SDEU“) ve svém rozhodnutí ve věci Test-Achats ze dne 1. března 2011.[2] Tento případ se týkal žaloby jedné z belgických organizací na ochranu spotřebitelů, která tvrdila, že transpozice ustanovení čl. 5 odst. 2 směrnice Rady č. 2004/113/ES, který zavádí zásadu rovného zacházení mezi muži a ženami v přístupu ke zboží a službám a jejich poskytování (dále jen „Směrnice“), je v rozporu s Listinou základních práv Evropské unie, protože umožňuje diferenciaci pojistného podle pohlaví pojištěnce. SDEU souhlasil se stanoviskem žalobce, prohlásil čl. 5 odst. 2 Směrnice za odporující čl. 21 a 23 Listiny základních práv Evropské unie a zrušil jej.[3,4]

Je zřejmé, že čl. 23 Listiny základních práv EU[5] nelze přímo aplikovat na případ genetické diskriminace, jelikož se výslovně vztahuje pouze na rovnost mužů a žen. SDEU však rovněž aplikoval čl. 21 Listiny základních práv EU, který obsahuje obecný zákaz diskriminace a vypočítává její nejzávažnější formy. Vedle zákazu diskriminace podle pohlaví také uvádí neslučitelnost diskriminace na základě genetických rysů se základními právy uznávanými státy Evropské unie a tedy, slovy preambule, s: „duchovním a morálním dědictvím a nedělitelných a všeobecných hodnotách lidské důstojnosti, svobody, rovnosti a solidarity.“[6] V demonstrativním výčtu forem diskriminace v čl. 21 Listiny základních práv EU[7] jsou k nalezení zejména důvody, které jsou zcela mimo vůli jednotlivých osob (pohlaví, rasa, barva pleti, etnický nebo sociální původ, genetické rysy, zdravotní postižení, věk,

[1] Malpas, P.J.: Is genetic information relevantly different from other kinds of non-genetic information in the life insurance context? in *Journal of Medical Ethics*, Roč. 34, č. 7. s. 548.
[2] Rozhodnutí Soudního dvora Evropské Unie ve věci Test-Achats ze dne 1. 3. 2011, sp. zn. C-236/09 [online]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0236:cs:HTML.
[3] Rozhodnutí ve věci Test-Achats, op. cit. s.1.
[4] Listina základních práv Evropské unie ze dne 7. 12. 2000 vyhlášená pod č. 2007/C 303/01 [online]. Dostupná z: http://eur-lex.europa.eu/cs/treaties/dat/32007X1214/htm/C2007303CS.01000101.htm.
[5] Listina základních práv Evropské unie, op. cit. Čl. 23.
[6] Listina základních práv Evropské unie, op. cit. Preambule.
[7] Listina základních práv Evropské unie, op. cit. Čl. 21.

sexuální orientace) a některé volní důvody, které však jsou, převážně z historické zkušenosti, předmětem zvláštní ochrany ze strany ústavního práva (např. náboženské a politické přesvědčení či majetek).

Z výše uvedeného tak plyne, že evropská společnost zapovídá především diskriminaci na základě mimovolních skutečností. Malpas odůvodňuje ve svém článku[8], že diskriminace na základě mimovolních skutečností je zcela běžná a za příklad dává právě rozdílné pojistné plnění u životního pojištění pro muže (dožívají se průměrně nižšího věku) a ženy (dožívají se průměrně vyššího věku). Svůj argument ve prospěch používání genetických informací při poskytování pojištění tak odvozuje z obyčeje, tj. že určitá praxe je dostatečně dlouho zavedená (usus longaevus) a panuje přesvědčení o její závaznosti (opinio necessitatis). S tímto argumentem však nelze souhlasit. Pokud je určitá praxe v rozporu s vůlí zákonodárce přetavenou do uznávané formy (zákona), musí obyčej ustoupit. Navíc, obyčej nemůže za každých okolností odolávat právnímu vývoji. Argument, který se opírá pouze o fakticitu činnosti, je tudíž logicky nesprávný.

Wilkinson uvádí argumenty proti využívání genetických informací v pojišťovnictví: (1) jedná se o diskriminaci a ta je nepřípustná ze své podstaty; a (2) jedná se o akceptování genetického determinismu.[9] K prvnímu argumentu Wilkinson uvádí, že diskriminace spočívá v rozhodování na základě informací, které jsou irelevantní v kontextu rozhodování.[10] Protiargument je pak založen na tom, že je žádoucí, aby pojišťovna informace měla, a je dále podporován tezí, že potřeba jejich sdílení s pojišťovnou je navíc aprobována právem. Přijetí této normy by pak vedlo k tomu, že by se vytvářely celé skupiny osob, které by měly ztížený či zcela vyloučený přístup k životnímu pojištění. To by mělo za následek rozdělení podle dostupnosti určitých sociálních statků (např. pojištění, příp. některá zaměstnání, atp.) skupinám společnosti a v principu také alokace ekonomické hodnoty lidského života podle jeho genetických rysů. Právo a jeho výklad, který vede k nerovnosti mezi lidmi, je z pohledu evropské humanistické filozofie i ústavního práva nepřijatelný.[11,12]

Proti druhému Wilkinsonově argumentu míří teze, že lidský život je determinován genetickými informacemi. Tento směr, zpravidla označován jako „genetický determinismus“, nebere v potaz svobodnou vůli člověka a vkládá jeho život do zajetí genetických rysů. Genetický determinismus nebere v úvahu komplexitu biologických procesů, jejichž jsou genetické rysy obsažené v DNA pouze součástí a zpochybňuje lidskou podstatu, totiž houževnatost, píli a především vůli. Wilkinson rovněž uvádí, že genetický determinismus i genetickou diskriminaci je třeba odmítnout.

Argumentace proti genetickému determinismu má svoji oporu v ustanovení § 56 zákona o pojišťovnictví[13], který stanoví, že rozdílná výše pojistného musí být založena na přesných pojistně-matematických a statistických údajích. Adekvátní naplnění takové podmínky je však při současné absenci hlubšího porozumění vztahů a vazeb mezi geny a environmentálními vlivy téměř nemožné. Některé nemoci jsou sice prokazatelně determinované genetickou mutací, ale u většiny tuto jistotu nemáme. Obecné zákazy diskriminace obsažené v národních ústavách členských států EU, v čl. 14 Evropské úmluvy o ochraně lidských práv[14] a výslovné zapovězení diskriminace na základě genetických rysů podle čl. 21 Listiny základních práv EU[15] vedou k závěru, že by nejen na vertikální, ale i na horizontální úrovni měla být diskriminace na základě genetických informací zakázána.

---

[8] Pozn. autora: článek je z roku 2007, tj. čtyři roky před rozhodnutím SDEU ve věci Test-Achats. Prezentuje však druhý pohled na věc a proto jej zde uvádím.

[9] Wilkinson, Ruth.: Unjustified discrimination: is the moratorium on the use of genetic test results by insurers a contradiction in terms? in Health Care Analysis. Roč. 18, č. 3. s. 285.

[10] WILKINSON, op. cit. s. 285.

[11] Srov. např. Kant, Imannuel.: Groundwork of the Metaphysics of Morals (Cambridge Texts in the History of Philosophy), 2. vyd. Cambridge University Press, Cambridge, 2012.

[12] WILKINSON, op. cit. s. 285.

[13] Zákon č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů („zákon o pojišťovnictví“).

[14] Evropská úmluva o ochraně lidských práv, op. cit. čl. 14.

[15] Listina základních práv Evropské unie, op. cit. čl. 21.

Aplikace rozhodnutí SDEU ve věci Test-Achats[16] na otázku diskriminace na základě genetických informací rovněž vede k závěru její nepřípustnosti. Je však nutné poznamenat, že pokud zákonodárce výslovně takovou diskriminaci nezakáže nebo SDEU či Ústavního soudu ČR nerozhodnou o její nepřípustnosti, nemůžeme s určitostí prohlásit, že je praxe požadování genetických informací protiústavní diskriminací.

3 Česká právní úprava

Uzavírání pojistných smluv je ovládáno přísnějšími principy a pravidly než jiné typy smluv zejména s ohledem na informační povinnosti v rámci kontraktace podle § 1728 a v kontextu pojistných smluv § 2788 občanského zákoníku.[17] Ten určí vzájemnou povinnost stran „pravdivě a úplně” jedna druhé odpovědět na dotazy, které mají význam pro jejich rozhodnutí týkající se uzavření pojistné smlouvy (je tedy materiálním požadavkem při uzavírání smlouvy). Tato povinnost vychází z principu uberrimae fidei,[18] který vyžaduje, aby si strany sdělily všechny relevantní informace, které jsou jim známy. Dalšími principy pojištění jsou zejména princip rizika a princip nejistoty.[19] Společně se snaží eliminovat riziko[20] a nejistotu, skrze maximální informovanost a další veřejnoprávní instituty regulace pojištění.[21]

Princip uberrimae fidei se v situaci, kdy pojišťovna vyžaduje sdělení genetických informací, a tyto jsou známy zájemci o pojištění, dostává do konfliktu s principem zákazu diskriminace podle čl. 3 odst. 1 Listiny.[22] Princip zákazu diskriminace se uplatní vždy ve vertikálních vztazích. V oblasti horizontálních, tj. soukromoprávních, vztahů se uplatní pouze na určité právní vztahy v mezích ustanovení § 1 antidiskriminačního zákona.[23]

Zákon o pojišťovnictví v ustanovení § 56 stanoví zvláštní úpravu zákazu diskriminace pro účely pojistného a zajistného, která zavádí následující režim: (1) obecně platí zásada rovného zacházení při určení výše pojistného plnění; (2) věk nebo zdravotní stav mohou však být použity jako určující faktory výše pojistného; (3) pohlaví může být použito pro hodnocení pojistného rizika za účelem zabezpečení splnitelnosti závazků z provozovaného pojištění nebo zajištění, pokud to nevede k rozlišování výše pojistného a pojistného plnění podle pohlaví na individuální úrovni; (4) určení výše pojistného a výpočet pojistného plnění na základě kritérií podle bodu č. 2 a 3 musí být založené na relevantních a přesných pojistně-matematických a statistických údajích; a (5) rozdíl ve výši pojistného či pojistného plnění na základě kritérií podle bodu č. 2 a 3 musí být přiměřený.

Tato úprava je výsledkem vážení principu materiality (který vychází z principu uberrimae fidei), a principu zákazu diskriminace. Testem materiality se vymezují informace relevantní k uzavření pojistné smlouvy, a tedy zahrnuje i genetické informace. Test spočívá v kladení otázky: „jaké informace považuje opatrný pojišťovatel za důležité při stanovování výše pojistného, resp. uzavře vůbec pojistnou smlouvu?”[24] Při posouzení hodnoty prediktivních genetických informací jsou pro pojišťovny relevantní zejména informace týkající se tzv. „single gene disorders“, tedy nemocí, které

---

[16] Rozhodnutí Soudního dvora Evropské Unie ve věci Test-Achats, op. cit.
[17] Zákon č. 89/2012 Sb., občanský zákoník („občanský zákoník”).
[18] HULMÁK, VLČEK, op. cit. s. 606.
[19] MORGAN, Donald P. The American Economic Review: Rating Banks: Risk and Uncertainty in an Opaque Industry. 2002. New York. Roč. 92. č. 4. s. 874-888.
[20] K opačnému pohledu např. TALEB, Nassim. *Černá labuť: následky vysoce nepravděpodobných událostí*. Vyd. 1. Praha: Paseka, 2011, 478 s. ISBN 9788074321283.
[21] Např. institut odpovědného pojistného matematika – § 80 a násl. zákona o pojišťovnictví.
[22] Listina základních práv a svobod, op.cit. čl. 3 odst. 1.
[23] Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací, ve znění pozdějších předpisů („antidiskriminační zákon“).
[24] WILKINSON, op. cit. s. 282.

způsobují individuální geny – např. Huntingtonova choroba.[25] Pojišťovny tedy mají zájem na tom, aby měly ke genetickým informacím přístup, a naopak pojištěnci mají zájem na tom, aby je pojišťovnám nemuseli sdělovat.

Pojišťovny argumentují, že pokud nebudou mít všechny relevantní informace, bude ve vztahu mezi nimi a pojištěncem přítomna informační asymetrie. Ta povede k nižšímu předepsanému pojistnému a vyšším výplatám pojistných náhrad a to dále povede ke zvýšení základního pojistného pro všechny pojištěnce.[26] Informační asymetrie může vést také k tomu, že zájemci o pojištění dosáhnou na vyšší pojistné krytí než by mohli získat za stejnou cenu v případě, že by genetické informace sdělili pojistitelovi.

Právní úprava v České republice podřazuje genetické informace pod pojem „zdravotní stav", na základě čeho mohou pojišťovny v rámci předsmluvních jednání i samotné kontraktace vyžadovat od prospektivních pojištěnců také genetické informace.

Občanský zákoník v ustanovení § 2828 do sporného pojmu zahrnuje i „zprávy a zdravotnickou dokumentaci", jejíž součástí jsou podle § 53 odst. 2 písm. d) - g) zákona o zdravotních službách[27] inter alia i informace o zdravotním stavu pacienta, ale také osobní, rodinná a pracovní anamnéza pacienta. Z § 28 odst. 3 písm. a) až b) ZSZS[28] a z § 2647 až 2650 občanského zákoníku vyplývá, že genetické informace jsou součástí této zdravotnické dokumentace (záznamů o péči o zdraví).[29] Tento závěr potvrzuje také Šulc, který srovnává genetické informace s informacemi o diagnóze AIDS či rakoviny u prospektivního pojištěnce.[30]

V současnosti pojišťovny působící v České republice aktivně nepožadují po zájemcích o pojištění sdělení genetických informací ani souhlas s jejich zjištěním podle § 2649[31] ve spojení s § 2828 odst. 1 občanského zákoníku,[32] i když jim v tom zákonná úprava nebrání.

Pojišťovny využívají ustanovení § 2828 odst. 1 občanského zákoníku[33] a spolu s pojistnými podmínkami[34] zakládají povinnost zájemce o pojištění sdělit relevantní informace o svém zdravotním stavu pojišťovně. Nesdělení takovýchto informací pak může mít různé soukromoprávní dopady, zejména v podobě odmítnutí poskytnout pojistné plnění či jeho snížení.[35]

Je rovněž možné kvalifikovat nesplnění informační povinnosti jako trestný čin pojistného podvodu ve smyslu ustanovení § 210 odst. 1 trestního zákoníku, resp. jako jeho přípravu podle ustanovení § 210 odst. 7 trestního zákoníku.[36] Životní pojištění sjednané pouze pro případ smrti s sebou nese jisté specifikum toho, že trestný čin bude s nejvyšší pravděpodobností spáchán, ale trestní stíhání nebude

---

[25] Encyclopeadia Britannica: Huntington disease [online]. Encyclopedia Britannica [cit. 29. 2. 2016]. Dostupné z: http://www.britannica.com/science/Huntington-disease.
[26] WILKINSON, op. cit. s. 283.
[27] Zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů („zákon o zdravotních službách").
[28] § 28 odst. 3 písm. a) až b) zákona č. 373/2011 Sb. o specifických zdravotních službách, ve znění pozdějších předpisů.
[29] Nonnemann, František.: Zdravotnická dokumentace po nabytí účinnosti nového občanského zákoníku in Právní rozhledy. Roč. 2013, č. 18. s. 638.
[30] Šulc, Jaroslav.: IHned.cz.: Expert: Zákony na zneužití informací z DNA laboratoří v Česku zcela chybí [online]. 2011, cit. [25. 2. 2014]. Dostupné z: http://byznys.ihned.cz/c1-51402920-expert-zakony-na-zneuziti-informaci-z-dna-laboratori-v-cesku-zcela-chybi.
[31] NOZ, op. cit. § 2649.
[32] NOZ, op. cit. § 2828.
[33] NOZ, op. cit. § 2828.
[34] Např. ING Pojišťovna: Všeobecné pojistné podmínky pro životní pojištění [online]. ING Pojišťovna [cit. 24. 2. 2014]. Dostupné z: https://www.ingpojistovna.cz/o-ing/pravni-ustanoveni/vseobecne-pojistne-podminky-pro-zivotni-pojisteni.html.
[35] ING Pojišťovna: *Všeobecné pojistné podmínky pro životní pojištění* [online], op. cit. čl. 3 odst. 2.
[36] Trestní zákoník, op. cit.

zahájeno z důvodu úmrtí jeho pachatele. Životní pojištění se dnes obvykle vztahuje také na nejrůznější méně či více závažná onemocnění, pracovní neschopnost atd. V těchto případech by trestné stíhání bylo možné zahájit.

4 Vybraná mezinárodní úprava

Řada členských států Evropské unie jako je Belgie, Dánsko a Francie zcela zakázala využívání genetických informací, resp. výsledků prediktivních genetických testů v pojišťovnictví. Další státy, např. Velká Británie, Finsko a Německo, uzavřely s pojišťovnami moratoria, která obsahují buď úplný zákaz využívání genetických informací, nebo je jejich požadování vázáno na splnění určitých podmínek.[37] Moratorium typicky bere v úvahu otázky informační asymetrie a samotných genetických informací prediktivního charakteru. Informační asymetrie je povolena pro nižší pojistné krytí, kde může pojišťovně způsobit pouze zanedbatelnou škodu, a je zapovězena vyššího pojistného krytí, jehož výše je pro každý stát specifická. Jako příklad může sloužit Velká Británie, kde nejsou prospektivní pojištěnci povinni sdělovat genetické informace prediktivního charakteru pojišťovně při uzavírání životního pojištění s pojistným krytím až do výše pět set tisíc liber.[38]

Otázka využívání prediktivních genetických informací pojišťovnami je řešena stejným způsobem. Vzhledem k tomu, že zatím není jasné, jaký vliv mohou mít prediktivní genetické informace na trh s životním pojištěním, omezilo moratorium jejich užívání tak, že lidé, kteří jsou si vědomi své genetické nemoci nemohou získat vysoké pojistné krytí. Pokud by mohli získat vysoké pojistné krytí, aniž by pojišťovna dokázala ocenit riziko, bylo by to vůči ní nespravedlivé. V konkordátu je uvedeno, že nesdílení genetických prediktivních informací má zanedbatelný vliv na výplatu pojistných krytí a potažmo tedy i na hospodaření pojišťoven.[39]

Odlišný přístup pak zvolila Austrálie a Nový Zéland, kde pojišťovny nesmí vyžadovat, aby prospektivní pojištěnec podstoupil genetické testování, ale pokud jsou mu už genetické informace známy, má pojišťovna právo vůči prospektivnímu pojištěnci, aby je pojišťovně poskytnul.[40] Tento přístup eliminuje informační asymetrii ve vztahu pojišťovny a pojištěnce. Na druhou stranu se vůbec nezabývá otázkou samé možnosti pojišťoven genetické informace požadovat.

5 Závěr

Vhodnost vyžadování genetických informací při poskytování životního a soukromého zdravotního pojištění se tak redukuje na dvě otázky: (1) jakou povahu přiznáme genetickým informacím v pojišťovnictví; a (2) zda se jedná o diskriminaci, protože naše genetické vlastnosti jsou nezávislé na naší vůli.

První otázka se zabývá tím, jestli obecně přiznáme genetickým informacím prediktivní vlastnosti. Zodpovězení této otázky vyžaduje srovnání genetických informací s ostatními zdravotnickými informacemi. Genetické informace nejsou homogenní skupinou, kde každá jednotlivá informace má stejné prediktivní atributy, ale naopak jsou heterogenní skupinou. Některé informace tak mohou znamenat jistotu vzniku určitého onemocnění, přičemž jiné představují pouze nepatrné riziko. Jsou však známa rizika a pravděpodobnost vzniku následků těchto předispozicí a pojišťovna je tedy schopna ohodnotit jejich riziko a promítnout jej do výše pojistného i výše pojistného krytí. Z hlediska pojišťovny je např. stejně pravděpodobné, že těžký alkoholik a člověk trpící patologickou mutací genu

[37] MALPAS, op. cit. s. 548.
[38] HM Government: Concordat and Moratorium on Genetics and Insurance [online]. HM Government website [cit. 29. 2. 2016]. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/216821/Concordat-and-Moratorium-on-Genetics-and-Insurance-20111.pdf.
[39] HM Government: Concordat and Moratorium on Genetics and Insurance [online], op. cit.
[40] MALPAS, op. cit. s. 549.

způsobující nevyléčitelnou nemoc zemře předčasně. Pro účely pojistné matematiky tedy mají genetické informace stejný charakter jako ostatní zdravotní informace.

Druhá otázka navazuje na první otázku a řeší, zda je správné, aby byly genetické informace v pojišťovnictví využívány i přesto, že jsou zcela mimo vůli prospektivního pojištěnce. Pojišťovny považují genetické informace za hodnotné, protože jsou na jejich základě schopny pojistně-matematicky ocenit riziko vzniku pojistné události u konkrétního člověka a tedy i stanovit pro pojišťovnu výhodnou výši pojistného. Přitom cílem pojišťoven je především vytvářet zisk. Toho dosáhnou tak, že získají co nejvíce pojištěnců s co nejmenším pojistným rizikem a zvýší pojistné či zcela odmítnou vysoce rizikové prospektivní pojištěnce.[41] Soukromé pojištění je tedy ze své podstaty diskriminační, ale jako celek je spravedlivé, protože oceňuje riziko každého pojištěnce zvlášť.

Otázka, jakým způsobem správně vyrovnat práva pojištěnců a pojišťoven při dostupnosti genetických informací tak zřejmě ještě nějakou dobu zůstane nezodpovězena. Lze se však domnívat, že i zvláštní postavení genetických informací bude odstraněno s praktickým rozvojem genetických terapií, které odstraní determinační charakter genetických informací.

Použité zdroje

[1] Encyclopeadia Britannica: Huntington disease [online]. Encyclopedia Britannica [cit. 29. 2. 2016]. Dostupné z: http://www.britannica.com/science/Huntington-disease.

[2] HM Government: Concordat and Moratorium on Genetics and Insurance [online]. HM Government website [cit. 29. 2. 2016]. Dostupné z: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/216821/Concordat-and-Moratorium-on-Genetics-and-Insurance-20111.pdf.

[3] ING Pojišťovna: *Všeobecné pojistné podmínky pro životní pojištění* [online]. ING Pojišťovna [cit. 24. 2. 2014]. Dostupné z: https://www.ingpojistovna.cz/o-ing/pravni-ustanoveni/vseobecne-pojistne-podminky-pro-zivotni-pojisteni.html.

[4] Kant, Imannuel.: Groundwork of the Metaphysics of Morals (Cambridge Texts in the History of Philosophy), 2. vyd. Cambridge University Press, Cambridge, 2012.

[5] Listina základních práv Evropské unie ze dne 7. 12. 2000 vyhlášená pod č. 2007/C 303/01 [online]. Dostupná z: http://eur-lex.europa.eu/cs/treaties/dat/32007X1214/htm/C2007303CS.01000101.htm.

[6] Malpas, P.J.: Is genetic information relevantly different from other kinds of non-genetic information in the life insurance context? in *Journal of Medical Ethics*, Roč. 34, č. 7.

[7] Morgan, Donald P.: Rating Banks: Risk and Uncertainty in an Opaque Industry in American Economic Review, Roč. 92. č. 4.

[8] Nonnemann, František.: Zdravotnická dokumentace po nabytí účinnosti nového občanského zákoníku in *Právní rozhledy*. Roč. 2013, č. 18.

[9] Rozhodnutí Soudního dvora Evropské Unie ve věci Test-Achats ze dne 1. 3. 2011, sp. zn. C-236/09 [online]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0236:cs:HTML.

[10] Šulc, Jaroslav.: *IHned.cz*.: Expert: Zákony na zneužití informací z DNA laboratoří v Česku zcela chybí [online]. 2011, cit. [25. 2. 2014]. Dostupné z: http://byznys.ihned.cz/c1-51402920-expert-zakony-na-zneuziti-informaci-z-dna-laboratori-v-cesku-zcela-chybi.

[11] Taleb, Nassim.: Černá labuť: následky vysoce nepravděpodobných událostí. Vyd. 1. Paseka,

[41] MALPAS, op. cit. s. 549.

Praha 2011. 478 s.

[12] Wilkinson, Ruth.: Unjustified discrimination: is the moratorium on the use of genetic test results by insurers a contradiction in terms? in *Health Care Analysis*. Roč. 18, č. 3.

[13] Zákon č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů.

[14] Zákon č. 373/2011 Sb. o specifických zdravotních službách, ve znění pozdějších předpisů.

[15] Zákon č. 277/2009 Sb., o pojišťovnictví, ve znění pozdějších předpisů.

[16] Zákon č. 89/2012 Sb., občanský zákoník.

[17] Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací, ve znění pozdějších předpisů.

GPS Radio Hacking – What the Hell Time Is It?
Radiohacking GPS – víme, která bije?

Tomáš Rosa

Tomáš Rosa
tomas.rosa@rb.cz

Dr. Tomáš Rosa holds Ph.D. in cryptology with the Best Doctoral Work Award of the Rector of Czech Technical University for 2004. He is focused on mathematical and physical methods of computer security, especially on embedded and radio applications. He helped to improve several worldwide standards, namely TLS protocol, EMV payment scheme, and Bluetooth.

Tomáš Rosa je doktorem v oboru kryptologie s Cenou rektora ČVUT za rok 2004. Věnuje se matematicko-fyzikálním metodám počítačové bezpečnosti, speciálně pak vestavěným a rádiovým aplikacím. Pomohl zlepšit několik celosvětových standardů, konkrétně protokol TLS, platební schéma EMV a bezdrátový standard Bluetooth.

GPS Radio Hacking – What the Hell Time Is It?

Possibility of position, velocity, and also time spoofing of civil GPS is a well known implication of the deliberately missing cryptographic protection of the L1 C/A satellite signal. Practical feasibility was already demonstrated several times, so is there anything new? It is in the massive rise of software-defined radio (SDR) phenomenon, that will soon allow even script kiddies to download the exploit code from the internet and let it run. Are you still sure where are you and what time is it? Does it hold for your infrastructure, too? Countermeasures are uneasy, proper understanding is the key.

Radiohacking GPS – víme, která bije?

Možnost podvržení polohy, rychlosti a také času civilní GPS je známým důsledkem záměrné absence kryptografické ochrany družicového signálu L1 C/A. Praktická schůdnost byla také už několikrát prokázána, ergo co je zde nového? Jde o masivní nástup fenoménu softwarového rádia (SDR), které brzy dovolí i hackerským zelenáčům stáhnout si útočný program z internetu a spustit ho. Stále jste si jisti, kolik je hodin a kde jste? Platí to i o vaší infrastruktuře? Obrana je nesnadná, klíčem je pochopení problému.

1 Introduction

GPS receivers for position, velocity, and time (PVT) measurements based on the civil service known as C/A (Coarse Acquisition) or L1 C/A [1], [8], [24], [37], [39], where L1 stands for the satellite downlink frequency of 1575.42 MHz, are almost ubiquitous. They have also successfully found their way into many IT systems where they help to establish the spacetime topology and synchronization [8]. Many of these systems are also parts of many critical infrastructures [10], [40]. This is not surprising, as this service seems to be a really marvellous gift coming to us from the sky in almost any place on Earth. There is, however, a considerable pitfall in that this service is by no means as robust and bullet-proof as we would like it to be [2], [10], [16], [17], [26], [31], [34], [35], [40], [41].

Before starting the main topic, three clarifications are apposite. First, we will often use the GNSS (Global Navigation Satellite System[s]) shorthand when referring to general properties that are common to most of the contemporary satellite navigation systems. Today, GNSS set includes mainly the following instances [1]:

- BeiDou-2 (former COMPASS) developed and maintained by China.
- Galileo of the Europen Union being built by the European GNSS Agency (GSA) residing in Prague.
- GLONASS (Globalnaja Navigacionaja Sputnikovaja Sistema) designed and operated by Russia.
- NAVSTAR Global Positioning System (GPS) of the United States.

The second note is on the service(s) we are going to talk about. Basically any GNSS offers two kinds of signal: open and reserved ones. In case of GPS, this division is classically made into the civil and military signals. Despite not serving a united army force, the European Galileo [28] also has its security enhanced flagship called Public Regulated Service (PRS) [1], [32]. However, it seems to be nearly impossible to get any plausible public review of these services, their security goals, protections that are effectively applied, and last but not least the end-user license policy. Their usage in civil applications seems to be therefore very limited. This is, unfortunately, also true for the PRS of Galileo, although ideas exist on how to theoretically overcome its restrictions [32]. Anyway, we will focus solely on the open or civil GNSS services here.

Finally, please note this is meant to be a relatively quick overview of the GNSS/GPS hacking state of the art to support the invited talk at IS2 2016. It has to be accessible to a broad audience, including technical experts as well as chief security officers, so the style has to be concise and clear. The result is a kind of author's essay, rather than a comprehensive study. The interested reader is kindly referred to the references, namely [1], [8], [24], [27], [37], [39] for GNSS theory and practice, and [10] for a monography devoted to GNSS vulnerabilities and attacks. The practical experiments touched here are detailed in author's technical presentation [31] that can be also seen as a kind of scholastic supplement to the recent practical hacking demonstrations [16] and [41].

The rest of this overview is organised as follows: In part two, we review the basic positioning principles of GNSS/GPS. We then continue with the vulnerabilities and possible attacks on the L1 C/A civil service in part three. Practical experiments [31] are then briefly noted in part four. In part five, we discuss on how much of help we can expect from the Satellite-Based Augmentation System(s) (SBAS) that are used, for instance, to elevate the L1 C/A service quality to conform with the increased aviation safety demands. In part six, we review the basic countermeasure ideas, and we finally conclude in part seven. In that part, the very recent GSA announcements on the emerging Galileo Open Service security enhacements [53] is also discussed.

2 GNSS/GPS Positioning and Timing Reviewed

Generally speaking, any GNSS consists of three major parts: the space, ground, and user segments. The space segment consists of several (in case of GPS at least 24) operational satellites that continuously broadcast their signal in space (SIS) towards the Earth [1], [24], [28]. The ground segment is responsible for satellite maintenance, including periodical checking of the SIS quality and uploading possible corrections to the respective space vehicles (SVs). The user segment encapsulates all those particular client receivers that consume SIS broadcasted from the selected satellites to compute user position, velocity, and time (PVT). In this paper, we are mainly interested in the SIS properties [1], [12], [15], [24], [27] and processing [37].

The method behind GNSS positioning is called a triangulation. Having given the position (x_1, y_1, z_1) of one SV and the actual distance r_1 in between this particular SV and the user, the receiver can deduce that its spatial coordinates (x_u, y_u, z_u) must be on a sphere satisfying

$$r_1 = [(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2]^{1/2}.$$

Having given one more SV distance r_2 and position (x_2, y_2, z_2), the receiver knows it must be on the intersection of two such spheres which is a circle in the plane of the intersection satisfying

$$r_1 = [(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2]^{1/2},$$
$$r_2 = [(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2]^{1/2}.$$

Third SV at distance r_3 and position (x_3, y_3, z_3) further reduces the possible user coordinates to at most two points in the space satisfying the equations

$$r_1 = [(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2]^{1/2},$$
$$r_2 = [(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2]^{1/2},$$
$$r_3 = [(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2]^{1/2}.$$

This remaining uncertainty is of no problem most of the time, since one of these points can be usually further eliminated basing on a contextual information, such as the receiver is supposed to be on the Earth surface and the second point is then too high to be true.

In GNSS, however, we cannot measure the distances directly. Instead, we are looking at the delay in between the SIS transmission from the respective SV (t_{send}) and its reception by the receiver (t_{recv}). Since the speed of light denoted c is finite and invariant, there is a known relation holding in free space

$$r_i = (t_{i,recv} - t_{i,send})c.$$

The receiver's clock is, however, not perfectly synchronized with the GNSS master time. Therefore, we are not getting the true ranges r_i this way, but a sort of pseudoranges denoted ρ_i instead. The aforementioned equations are then in the form

$$\rho_i = (t_{i,recv} + \delta - t_{i,send})c = [(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2]^{1/2} + \Delta_u,\ 1 \le i \le N,$$

where Δ_u is the value of the distance error, introduced by the fact we are observing pseudoranges instead of the direct true ranges, and N is the number of equations.

Seeing the positioning problem [37] this way, we can understand that instead of the three unknowns, we have to recover also the fourth variable denoted Δ_u. Assuming there is no generally usable dependence among these variables, it follows that instead of three equations we need at least four of them. That means $N \ge 4$, which in turn means we have to observe SIS for at least four satellites.

The good point is, however, that this way we are also implicitly getting the δ correction of the local receiver clock with respect to the GNSS master time with a precision that is approaching the atomic time [25] of the space segment (further supervised by the ground segment). Despite seeming as a by-product, this is so valuable output that in many applications the particular GNSS service is solely used for the precise timing purpose. In particular, the C/A service of GPS is the most widely used one here [8].

According to the way we observe $t_{i,send}$ it is important to emphasize GNSS is generally not a pulsed system. The time-sent information is continuously embedded into the SIS being generated by the respective SV [1], [8], [15], [24], [27] and we are recovering the $t_{i,send}$ values by continuously observing the respective SIS and maintaining a delayed replica clock for each SV. This procedure is known as a satellite tracking and it is directly linked to the number of receiver channels available. The receiver can track in parallel as many satellites as many channels it has.

Note also that we can in theory lower the number of equations, and so the satellites needed to be tracked, by knowing some of those PVT variables a priori. For instance, if we know the receiver position from another geoinformatical source, we can recover the precise timing signal by just a single channel receiver and at least one strong SV in the sky view [8].

A simple illustration of the whole tracking process leading to position, velocity, and time estimation is given in Figure 1. Please bear on mind the process of PVT computation [37] has been simplified here considerably to exemplify the main principle. In practice, there are further SIS distortions the receiver has to cope with, namely gravitational field perturbations affecting satellite orbits [25], ionospheric and tropospheric phase shifts, local neighbourhood reflections etc. [24], [28]. Lot of the atmospheric effects, for instance, are then much easier to correct provided we can observe their impact on signals being transmitted on at least two different frequencies (not just L1 only). This is the reason why the modernised GNSS services usually seek for an allocation of multiple frequencies for their SIS and declare this as one of their key benefits [1], [12], [28].

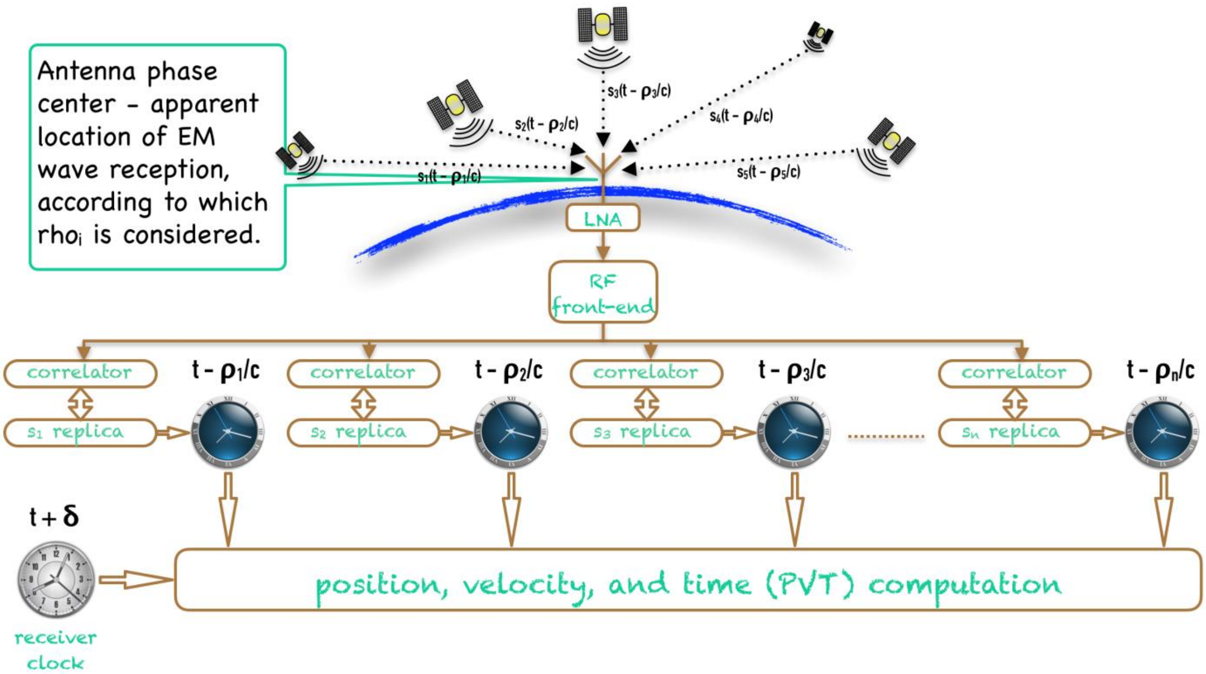


Figure 1: GNSS tracking loop showing the role of replica clocks derived from the satellite signals.

In Figure 1, there also is the antenna phase center indicated [1], [8], [20], [23]. For those who ever wondered of what place is the position, velocity, and time relevant to, this is the answer. It is an apparent spot at or close to the antenna where the incident electromagnetic wave seems to get converted to the electrical antenna current. So, for example, if we would have an antenna at the roof top connected with a processing device several floors below the roof, the PVT computation would be still valid with respect to a spot at the antenna on the roof. Antennas designed for precise PVT measurements have their phase center(s) (as it may vary with the angle of the wave arrival) marked in their data sheets.

3 GPS L1 C/A Vulnerabilities and Attacks

On one hand, we can hardly call the GPS L1 C/A service vulnerabilities a "discovery", since there was never any kind of a robust protection seriously considered [1], [24]. Perhaps, there was some hope that the attacks would not be easy to carry out [40], but that was apparently all. For those who required a better protection (and were also among the selected ones), there was the military-grade service developed. Unfortunately, practically all GNSS, including the modernised GPS services [1], continue with this "cold war" viewpoint, which is an obvious misconception nowadays [10].

The main reason why we shall also consider the GNSS civil services protection seriously, now can be called a software-defined radio (SDR) [13], [19], [36]. Generally speaking, this is a universal radioelectronic device that allows almost complete redesign of its signal processing parts by just loading the appropriate firmware. When it comes to hacking, we can tell that what used to be a question of deep radio understanding [30] together with a practical HW skill [33], is now becoming a question of a few off-the-shelf components [31], [36], [43], a basic course in DSP (Digital Signal Processing) [21], [22], and widespread SW frameworks [13], [36].

It is important to understand that the core of a contemporary radio attack is not the universal HW itself [49], but the software realizing the signal processing flow-graph [17], [50]. Being written just once, this piece of software can be then shared, downloaded, and executed all around the world very easily. Just like any other so-called exploit code, as we know them from computer security everyday practice very well. The practical experiments noted below fully support this argument [31].

So, what can the attacker do, having been equipped with the right SDR and having loaded the right exploit SW into it? The basic classification of GNSS attacks is as follows [10]:

- jamming,
- meaconing (record & replay),
- spoofing.

Jamming attack is basically a DoS (Denial of Service) that is illustrated in Figure 2. It seems like a trivial attack, but it can be really demanding, provided the attacker aims for a broad and reliable effect without being easily identified due to a big power transmission. Not surprisingly, several involved jamming strategies have been developed [10], [15].

Due to the ubiquitous implementation of GNSS receivers in our modern IT infrastructure, the jamming attack can have rather devastating consequences, nowadays. It seems like the developers had the assumption that unless there is the end of the world, the GPS L1 C/A service in particular must be always available. Several interesting real-life incidents are assembled in [10] illustrating the general public services practically collapsed after the GPS signal was jammed. This shall be fully reflected in our future risk analyses.

The jamming threat is even more emphasized by the fact it seems to be a radio-based attack on GNSS that can hardly be prevented by a cryptographic signal processing only [10] which otherwise is clearly a preferred approach (cf. the discussion below). Therefore, even in the case of military-grade signals, there is always a place for purely radio-oriented countermeasures, including the use of smart antennas [20], [23].

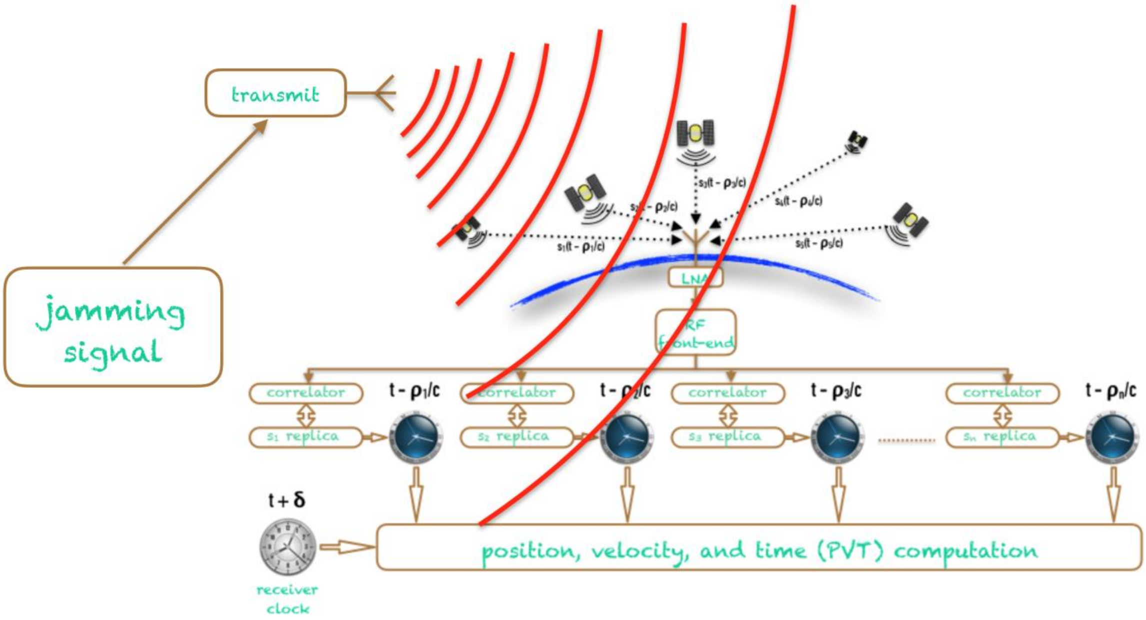


Figure 2: Denial of Service by the original satellite signal jamming.

Another attack on GNSS is the meaconing illustrated in Figure 3, which is basically another name for the record & replay attack. The record phase starts similarly to an ordinary receiver signal processing flow-graph. Instead of processing the RF signal samples towards getting PVT, however, the attacker just only records these samples to a suitable medium. During the replay phase, they use the captured samples as a source for the quadrature modulation [22] of a regenerated L1 carrier that is in turn transmitted towards the victim's receiver. That receiver then can see the fake signal like it was coming from the original satellites.

A simple variant of the meaconing attack can, instead of offline storing, transfer the original samples over e.g. internet to some other place and replay them in almost real time there. This way, we can instantly "move" the remote sensor to the place of our receiving antenna.

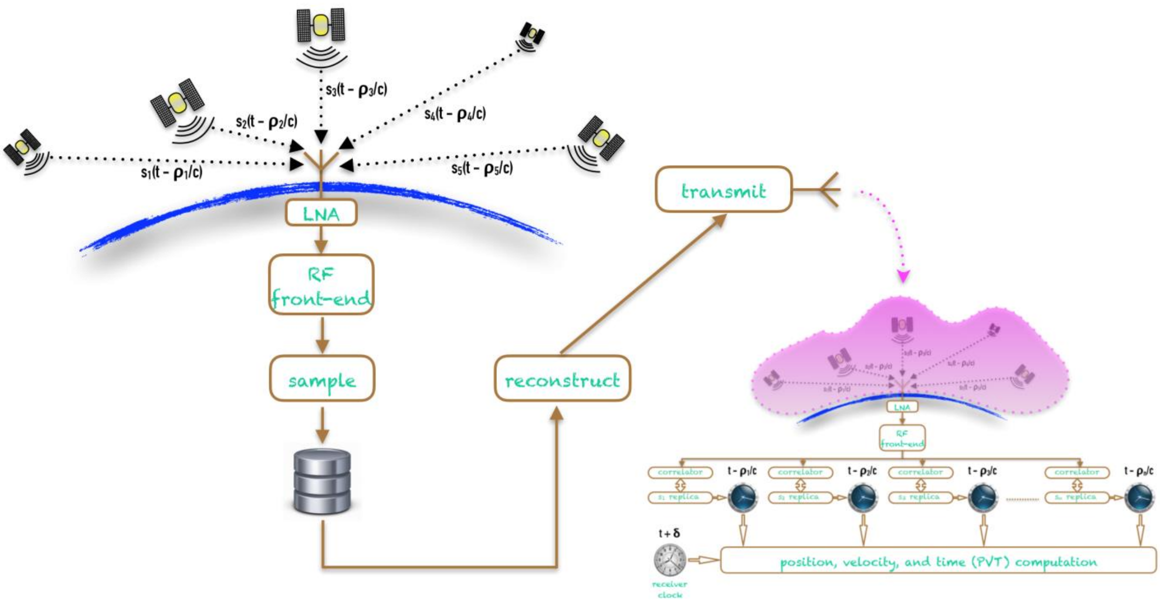


Figure 3: Meaconing (record & replay) attack on GNSS.

The third kind of attacks on GNSS, called spoofing, is illustrated in Figure 4. This time the fake signal is not based on a simple recording, but it is created synthetically instead. In particular, Figure 4 shows a robust way on how to generate the spoofing signal from scratch that is able to naturally mimic the physical properties of the original signal, namely a smooth Doppler shift [24], [28]. We use the PVT values as an input and according to the equations mentioned in part two we derive the expected values of the replica clocks dials together with their expected tick speed. Then we use the dial values as phase variables for the fake signal synthesis that is then modulated on the L1 carrier and transmitted.

It shall be understood that both meaconing and spoofing attacks can be in fact carried out by practically any GNSS radio debugging tool. Actually, it took a surprisingly long time till people recognized that these development simulators and testers, being equipped with a simple output power amplifier and antenna, can be also used for a real attack [40]. On the other hand, there are, however, reasons on why to develop a new line of these tools in parallel. The first is these "superprofessional" tools seem to be often somehow overpriced for the purpose we need them, while at the same time lacking security relevant functions such as, for instance, navigation data fuzzing modules to search for receiver firmware vulnerabilities and exploits [26]. It is questionable whether these functions would otherwise be ever implemented into those professional, development-style black boxes. According to author's own experience, their manufacturers do not seem to appreciate the potential of GNSS security research too much, as, for instance, a security conference review was unfortunately (as the device was really interesting) not enough to qualify for a "free" 14-day trial test period of one of them.

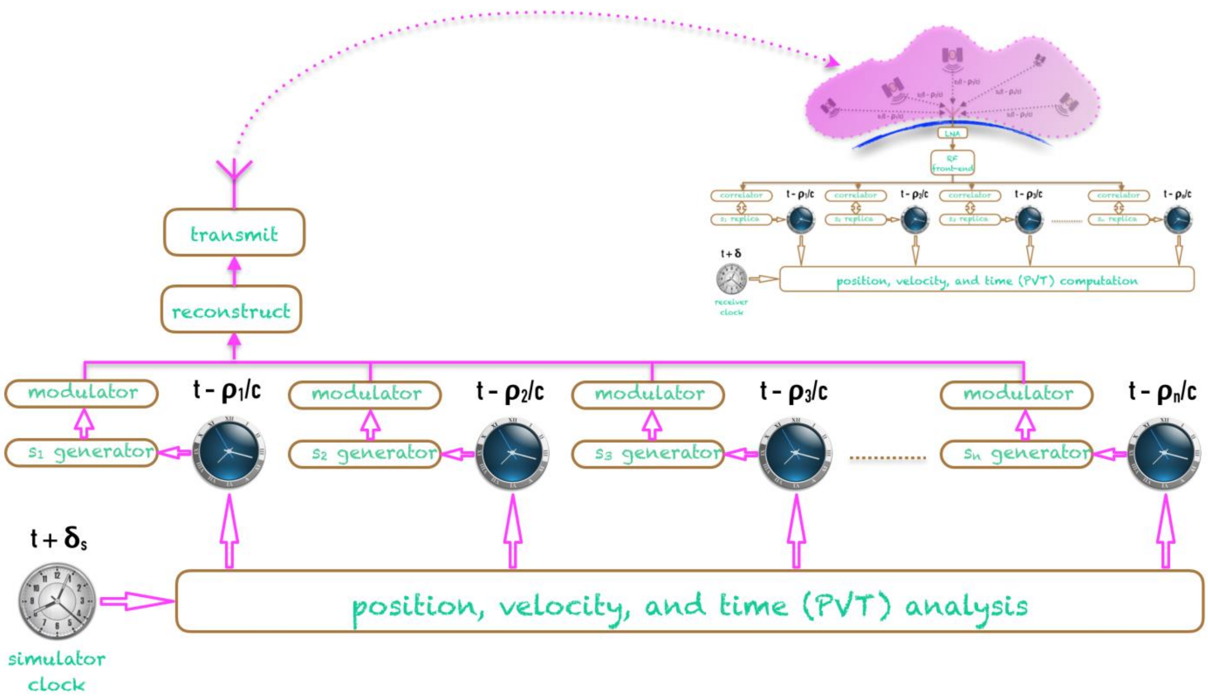


Figure 4: GNSS spoofing attack based on a synthetic signal generation
by the tracking reversal process.

The simple attack classification noted here can be further subdivided based on, for instance, what are the requirements on the targeted receiver. Some of them may require a cold start, while sometimes a warm start (by remembering the last PVT and satellite positions) is enough. There are even attacks that can hijack the receiver while it is actively tracking the original SIS [17]. This usually requires the spoofing devices to also track and estimate the original SIS and carefully blend its own fake signal with it. We can take the SCER (Security Code Estimation and Replay Attack) as an example [10], [51]. Another subdivision can be based on the amount of independent transmitters the attacker can use to improve the spatial diversity of the fake signal and so to bypass spatial diversity countermeasures [38].

4 Practical Experiments

The low-cost, simplistic meaconing and spoofing attacks were successfully verified on GPS L1 C/A in a rather simplistic setup. Details allowing objective replication of these experiments are given in [31]. As the SDR platform, we have used USRP N210 [49] with the UBX-40 daughterboard [48]. For the meaconing experiment, we also used a custom based front-end in between the active GPS antenna and the UBX-40 daughterboard that was, however, based solely on off-the-shelf components [43]. Its purpose was to carefully amplify the very weak GNSS signals without introducing too much additive noise [11] over the level inevitably captured by the antenna [20].

To verify the fake signal, we used a state-of-the-art GNSS receiver uBlox NEO-M8N installed as a USB component peripheral on a development breakout board, which is still an off-the-shelf product [44], [45]. After a proper attenuation and DC current blocking in between UBX-40 output port and the GNSS receiver input, we used a direct coaxial cable connection in between these two components. This way we could avoid any direct fake signal emanation, which is clearly more than desirable. The detailed report [31] also shows how to really transmit the forged signal, but this is just for the sake of completeness and we can by no means recommend this.

Data from the uBlox receiver were processed and presented via uCenter [46], [47], which is a free of charge development SW running on practically any reasonable platform equipped with MS Windows Vista or higher. uCenter dashboard example is shown in Figure 5 below.

Despite there being professional (and still somehow overpriced) SW tools for GNSS/GPS signal manipulation, we stayed with a very modest setup here to exemplify our argument of the massive attacks threat accelerated by the SDR phenomenon. In particular, for the meaconing (record & replay) attack experiment, we employed the `rx_samples_to_file` and `tx_samples_from_file` example codes that are installed together with the N210 device driver (USRP Hardware Driver – UHD) source tree. Details of their invocation are given in [31].

For the preparation of the fake signal used in the spoofing attack, we used a simple but very handy open source project GPS-SDR-SIM by Takuji Ebinuma et alia [50]. The core is a C module that is easy to compile almost everywhere, where we have the OpenMP framework for shared-memory parallel programming (open source code, not specific to GNSS). This utility prepares the simulated GPS L1 C/A signal as an offline file with its quadrature (complex) envelope samples [22]. The final transmission step is then, therefore, de facto the same as in the meaconing attack experiment. Since it uses a different data precision, however, `tx_samples_from_file` should be edited slightly. This would be really easy, but since GPS-SDR-SIM comes with its own "player" code [50], we have stayed with that. In particular, this player is a Python code that creates a simple flow-graph based on the GNU Radio framework [13]. This is again an open source project serving as the platform of first choice for many academic projects. All the details necessary for an independent verification of these experiments are given in [31].

5 SBAS to the Rescue?

Even without intentional attacks, the civil GPS C/A service is not as reliable as necessary to be directly and solely usable in safety-critical applications such as flight security. Services known as Satellite-Based Augmentation System [1], [28] have been devised to constantly monitor the integrity of C/A and report its safety status together with possible differential GPS (DGPS) correction parameters via geostationary satellites. To be easily accessible for simple receivers, the signals coming from these auxiliary satellites are also transmitted on L1 with almost the same CDMA [15] scheme. They differ in the data modulation speed and payload [1], but this is relatively easy to handle in the receiver.

In particular, the Europe is practically covered with SBAS named EGNOS (European Geostationary Navigation Overlay System) that is also operated by GSA [28]. Contrary to Galileo, however, this system is in the production grade version, now, being enjoyed by many civil pilots landing on the old continent.

Provided SBAS is such a wonderful safety system built around the C/A service, it is natural to ask whether it is also a countermeasure against the attacks discussed above. To understand the answer, it is important to see that SBAS provides a safety assurance based on SIS observed by its reference monitoring stations. It cannot check the local reception of the (possibly) fake signal being received by the individual users. It is oriented to measure and evaluate the quality of the original SIS as it is being transmitted by the original satellites globally. Therefore, a reception of local invalid signals transmitted by anybody else is not addressed by today's SBAS [1]. So, the answer is unfortunately no, it cannot prevent the attacks discussed here.

To practically demonstrate this, we present the Figure 5 that shows a dashboard of the reference GNSS receiver used in our meaconing attack experiment. Since there was also an EGNOS satellite in the sky view during the original SIS recording phase and since the EGNOS (as any other SBAS) produces RF signal that is highly compatible with L1 C/A, that augmentation signal had been recorded as well. In Figure 5, we can see the EGNOS channel was successfully recognized and employed by the receiver during the replay phase of our demo attack. So, as a kind of by-product, we also have a working example of the EGNOS replay attack here. Actually, we see a classical example of false sense of security as the receiver dashboard shows the EGNOS signal has been applied to get a DGPS (Differential GPS) precision grade [1], [24], [37] thereby suggesting everything should be more than fine.

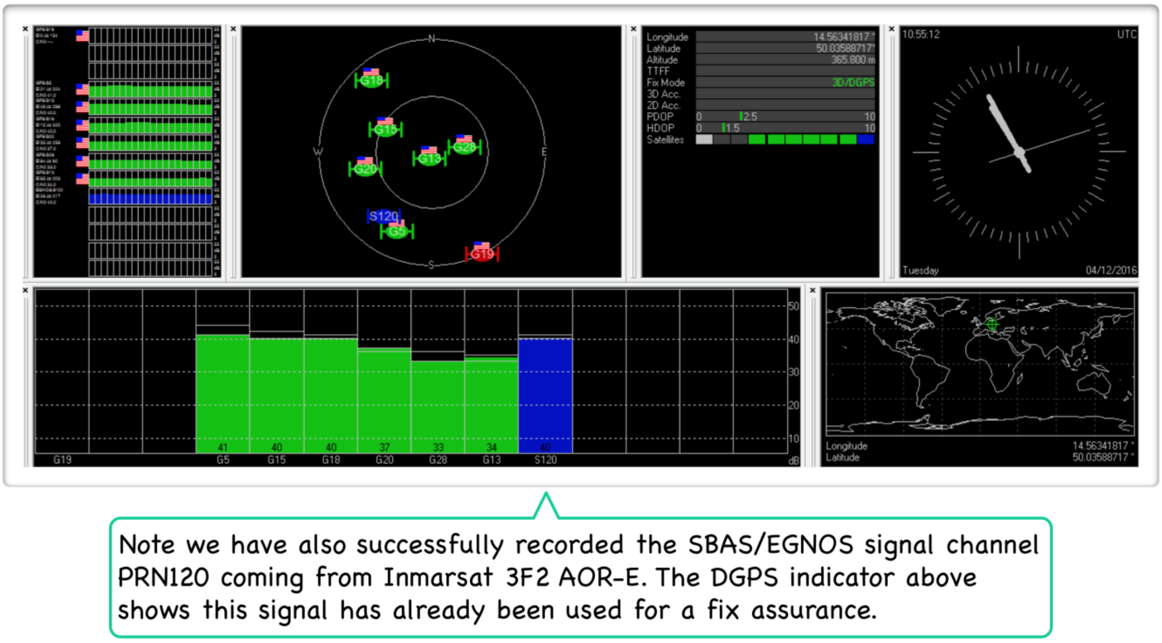


Figure 5: Successful meaconing attack on GPS L1 C/A that also covers the EGNOS signal.

6 Countermeasures

Actual and comprehensive review of countermeasures can be found in monography [10] as well the references noted there, cf. also [18], [23], [38]. Despite exposing the label “interference” in its title, it also covers jamming, meaconing, and spoofing as a special kind of man-made intentional interferences. Many classifications are also noted there, however, we will use a very simple three-category scheme for our purpose here:

- countermeasures that also improve SIS definition,
- methods based on receiver radio signal processing only,
- PVT postprocessing verifications.

Note we are still talking about the civil GNSS services, as these are the only ones that are granted for general IT companies. If we understand cryptography as the science bringing information protection constructions based on rigorous mathematical or physical arguments, then we have to clearly admit that cryptography shall be applied to SIS processing if we really want to get a robust GNSS security [10], [14], [51], [52]. That in turns means the first countermeasures category is the one that shall be preferred, so we pay a higher attention to it here. Truly, this is the case of e.g. military GPS signals. Unfortunately, the only “protection” explicitly noted, for instance, in the actual definition of the emerging Galileo Open Service SIS [12], besides a convolutional forward error correction (FEC) code, is a simple CRC. Interestingly, the sole inclusion of FEC with a binary interleaving [12] can actually work as a “spoofing obstacle”, but this is more or less a by-product of the receiver hijacking problem [17] and it is clearly no protection against direct meaconing or synthetic signal spoofing. On the other hand, the interleaved FEC can also potentially even help the attacker with the SCER attack [10], provided the detector [52] was not tailored properly to its presence by reflecting its impact on the processing flow-graph together with the residual attacker’s security code estimator advantage [51]. That said FEC incorporation is a tricky part deserving certain attention.

As we have the open signals without any cryptographic protection, now (hopefully, this will change), we have to focus on the remaining two categories. Anyway, it should be emphasized that even with a cryptographic protection in place, its verification needs to be understood as a probabilistic problem [51] to be able to defeat SCER-like attacks [10]. Instead of a simple yes-no algebraic algorithm, we need a statistical signal detector that allows us to distinguish between the original and fake signals [52]. It follows we still need some radio signal processing techniques to help us. This is especially true when coping with jamming. A question may arise on how far the cryptography is useful at all, provided it is hardly enough in itself. In this light, we shall see the cryptographic protection of SIS as a significant enabling factor that allows us to design and use much more powerful attack detection techniques than what remains when no cryptography was employed.

To that end, the cryptographic protection goals shall be precisely stated and the cryptosystem shall be then carefully tailored to the RF signal processing needs. We emphasize again, this is not only to achieve certain efficiency, but mainly to fulfil those security goals at all. As an example, we may consider the well-known method of “codeless” tracking that has been developed to gain some information from the military GPS signal that is in turn used to get rid of the effects like the ionospheric distortion [42]. At least, this is how it is known in the satellite navigation community. Practically the same article could had been, however, issued in proceedings on cryptology as a successful partial cryptanalysis of the military GPS scheme! This illustrates nicely that designing a broadcast radio signal protection is not as easy as solving a simple general data encryption exercise. We need to work with the low-level signal properties to fully understand on how to really achieve our security goals [51].

Anyway, the radio signal processing tries to identify both intentional as well as unintentional interferences basing on statistical properties of the RF samples being processed [10], [15], [52]. As the computational power of receiver controllers grows up, more and more involved methods can be used. Unfortunately, regarding the intentional interference (jamming, meaconing, and spoofing), no provable or at least universal purely radioelectronical countermeasure has been found and it does not seem there is something like that on the horizon [10].

PVT postprocessing addresses these problems from a different perspective. Instead of trying to get error-free receiver output, it combines the respective contributions of several independent PVT measurement technologies and devices. This way we can, for instance, combine the GPS service with GLONASS (or Galileo in the near future) or with inertial sensors like accelerometers, gyroscopes, barometers, etc., to be able to mutually cross-check the individual results. Mathematically speaking, this combination is typically based on the statistical Kalman filtering theory [27], [37].

In summary, the only rigorous approach to meaconing and spoofing, however, remains via cryptography. Anything else can be seen like a cat-and-mouse game or the virus-antivirus fight. Once we take the current best spoofer, for instance, we can look at its signal artefacts and design our detector to go especially after them [10]. The spoofing device author, however, can learn this, tweak their device a little bit and our detector falls short. And the whole story repeats again, and again…

7 Conclusion

The possibility of easy jamming, meaconing, and spoofing attacks, thereby of the free manipulation with the receiver apparent position, velocity, and time, is a long overlooked problem of practically any open GNSS service. The most popular target seems to be the widespread GPS L1 C/A signal. Any other unprotected GNSS service can, however, follow soon, including the emerging Galileo Open Service [12]. Furthermore, this is all getting accelerated by the software-defined radio paradigm that has successfully established its place in many hacker arsenal toolboxes [16], [41]. Since SDR allows a variant of the “write once, run anywhere” approach, we can expect even so-called “script kiddies” will be soon able to play with GNSS attacks all around the world.

One may argue this is not a discovery, since a robust protection of the civil services was never seriously considered. However, this is right the point that needs to be radically revised, now as the threat model has clearly changed. We can see the public GNSS hacking and security research papers mainly as an appeal on designers of these services, as well as a clear warning to its application engineers to be careful with what they trust to.

As the cold war era is over and the civil sector plays important role in the critical infrastructure today, it is right the civil service that deserves a robust security protection, now. Designing a new service such as the Galileo Open Service without any solid cryptographic protection would be actually bringing up a new system that is by-design broken. We can hardly agree with the position like that civil applications do not deserve an accessible and robust protection of their GNSS signals. On one hand, it is understood that services such as Galileo Public Regulated Service (PRS) should exist. Their role shall be, however, mainly seen in the possibility to temporarily (!) restrict the access to the GNSS service in time of war, severe terrorist attacks, dramatic regional destabilization, etc. They can also broadcast some additional data that can be used for investigation, international police coordination, natural disaster recovery, and so on. Their role is, however, by no means in distinguishing the usable (i.e. protected and safe) GNSS services from the unusable (i.e. unprotected and unsafe) ones.

Interestingly, in the time of finishing this manuscript, GSA announced it will provide the Navigation Message Authentication (NMA) protection [10], [52] right with the Galileo Open Service signal as of 2018 [53]. Cryptographically speaking, NMA allows the navigation data origin authentication by a form of a digital signature or message authentication code (MAC). As any such protection embedded into a broadcast data, in itself, it can only protect against a very harsh meaconing or a totally synthetic signal spoofing, but it usually fails against a bit more clever variants of these attacks. To be robust and useful, it needs to be made in a form of a statistical signal detector allowing to distinguish also the relevant SCER variants [10], [51], [52], as we have discussed it in part six above. This all needs to be detailed in the new SIS definition to fairly get all the receiver manufacturers to the same ground, as we clearly cannot assume all users will check the particular implementations by themselves to see whether they are vulnerable or not. Since it is actually less than two years to the planned start of this new Open Service version and the SIS definition remains practically intact [12], this all brings more questions than answers. This is somehow unfortunate, as such an unprecedented (with respect to the rest of the GNSS world) step would otherwise deserve clear ovations.

Acknowledgement

The author is grateful to Jiří Buček (FIT, Czech Technical University in Prague), Tomáš Jabůrek and Radek Komanický (Raiffeisen Bank), and Martin Opava (truconneXion). They all have contributed with a non-trivial effort to make the GNSS security research possible and pleasant.

References

[1] Betz, J.-W.: *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*, IEEE Press, John Wiley & Sons, 2016.

[2] Bonebrake C. and O'Neil, L.-R.: Attacks on GPS Time Reliability, *IEEE Security & Privacy*, May/June 2014, pp. 82-84, 2014.

[3] Borre, K., Akos, D.-M., Bertelsen, N., Rinder, P., Jensen, S.-H.: *A Software-Defined GPS and Galileo Receiver A Single-Frequency Approach (Applied and Numerical Harmonic Analysis Series)*, Birkhauser Boston, 2007.

[4] Chen, J., Zhang, S., Wang, H., and Zhang, X.: Practicing a record-and-replay system on USRP, *In Proc. of the second workshop on Software radio implementation forum*, pp. 61-64. ACM, 2013.

[5] Di, R.: *A USRP-Based Flexible GNSS Signal Recording and Playback System: Performance Evaluation and Study*, M.Sc. Thesis, Miami University, Oxford, Ohio, 2013.

[6] Di, R., Peng, S., Taylor, S., and Morton, Y.: A USRP-Based GNSS and Interference Signal Generator and Playback System, *In Position Location and Navigation Symposium (PLANS) 2012*, pp. 470-478, IEEE, 2012.

[7] Diggelen, van F.: A-GPS: *Assisted GPS, GNSS, and SBAS (GNSS Technology and Applications Series)*, First Edition, Artech House, 2009.

[8] Doberstein, D.: *Fundamentals of GPS Receivers – A Hardware Approach*, Springer, 2011.

[9] Dong, L.: *IF GPS Signal Simulator Development and Verification*, M.Sc. Thesis, University of Calgary, Alberta, 2003.

[10] Dovis, F. (Ed.): *Gnss Interference, Threats, and Countermeasures (Gnss Technology and Applications Series)*, Artech House Publishers, 2015.

[11] Etten, van W.-C.: *Introduction to Random Signals and Noise*, First Edition, Wiley, 2005.

[12] *European GNSS (Galileo) Open Service (OS), Signal In Space (SIS) Interface Control Document (ICD)*, Europen Union, November, 2015.

[13] Grayver, E.: *Implementing Software Defined Radio*, Springer, 2012.

[14] Hernandez, I.-G., Rodriguez, I., Tobias, G., Calle, J.-D., Carbonell, E., Seco-Granados, G., Simon, J., and Blasi, R.: Galileo Commercial Service – Testing GNSS High Accuracy and Authentication, *Inside GNSS*, January/February 2015, pp. 38-48, 2015.

[15] Holmes, J.-K.: *Spread Spectrum Systems for GNSS and Wireless Communications (GNSS Technology and Applications Series)*, Artech House, 2007.

[16] Huang, L. and Yang, Q.: GPS Spoofing – Low-cost GPS Simulator, *DEF CON 23*, Las Vegas, August 6th – 9th, 2015.

[17] Humphreys, T.-E., Ledvina, B.-M., Psiaki, M.-L., O'Hanlon, W.-O., and Kintner, P.-M., Jr.: Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer, *In Proc. of the ION GNSS international technical meeting of the satellite division*, vol. 55, p. 56, 2008.

[18] Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS vulnerability to spoofing threats and a review of antispoofing techniques, *International Journal of Navigation and Observation*, 2012.

[19] Johnson, C.-R., Jr., Sethares, W.-A., and Klein, A.-G.: *Software Receiver Design – Build Your Own Digital Communications System in Five Easy Steps*, Cambridge University Press, 2011.

[20] Kraus, J.-D. and Marhefka, R.-J.: *Antennas For All Applications*, Third Edition, McGraw-Hill, 2003.

[21] Lathi, B.-P. and Green, R.-A.: *Essentials of Digital Signal Processing*, Cambridge University Press, 2014.

[22] Lyons, R.-G.: *Understanding Digital Signal Processing*, Third Edition, Prentice Hall, 2011.

[23] McMilin, E.-B., Chen, Y.-H., De Lorenzo, D.-S., Akos, D.-M., Walter, T.-F., Lee, T.-H., Enge, P.-K.: Single Antenna, Dual Use: Theory and Field Trial Results for Aerial Applications of Anti-Jam and Spoof Detection, *Inside GNSS*, September/October 2015, pp. 40-53, 2015.

[24] Misra, P. and Enge, P.: *Global Positioning System – Signals, Measurements, and Performance*, Revised Second Edition, Ganga-Jamuna Press, 2012.

[25] Montenbruck, O. and Gill, E.: *Satellite Orbits: Models, Methods and Applications*, HAR/CDR edition, Springer, 2011.

[26] Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., and Brumley, D.: GPS Software Attacks, *In Proc. of the 2012 ACM conference on Computer and communications security*, pp. 450-461, ACM, 2012.

[27] Noureldin, A., Karamat, T.-B., Georgy, J.: *Fundamentals of Inertial Navigation, Satellite-based Positioning and their Integration*, Springer, 2013.

[28] Nurmi, J., Lohan, E.-S., Sand, S., and Hurskainen, H. (Eds): *GALILEO Positioning Technology*, Springer, 2015.

[29] Perring, A., Canetti, R., Tygar, J.-D., and Song, D.: The TESLA Broadcast Authentication Protocol, *In CryptoBytes*, 5:2, Summer/Fall 2002, pp. 2-13, 2002.

[30] Razavi, B.: *RF Microelectronics*, Second Edition, Prentice Hall, 2011.

[31] Rosa, T.: *GNSS/GPS Radio Hacking – From Beautiful Equations to Serious Threats*, In QuBit Conference 2016, Prague, April 12th – 14th, 2016, [http://crypto.hyperlink.cz/files/rosa-qubit-2016.pdf].

[32] Rugamer, A., Stahl, M., Lukcin, I., Rohmer, G.: Privacy Protected Localization and Authentication of Georeferenced Measurements using Galileo PRS, *In Position, Location and Navigation Symposium-PLANS 2014*, 2014 IEEE/ION, pp. 478-486, IEEE, 2014.

[33] Rutledge, D.: *The Electronics of Radio*, Cambridge University Press, 1999.

[34] Shepard, D.-P. and Humphreys, T.-E.: Characterization of Receiver Response to Spoofing Attack, *In Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation*, p. 2608, 2011.

[35] Shepard, D.-P., Humphreys, T.-E., and Fansler, A.-A.: Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks, *International Journal of Critical Infrastructure Protection 5*, no. 3, pp. 146-153, 2012.

[36] Stewart, R.-W., Barlee, K.-W., and, Atkinson, D.-S.-W.: *Software Defined Radio using MATLAB & Simulink and the RTL-SDR*, Strathclyde Academic Media, 2015.

[37] Strang, G. and Borre, K.: *Algorithms for Global Positioning*, Wellesley-Cambridge Press, 2012.

[38] Tippenhauer, N.-O., Poepper, C., Rasmussen, K.-B., and Capkun, S.: On the requirements for successful GPS spoofing attacks, *In Proc. of the 18th ACM conference on Computer and communications security*, pp. 75-86. ACM, 2011.

[39] Tsui, J.-B.-Y.: *Fundamentals of Global Positioning System Receivers: A Software Approach, Second Edition*, Wiley-Interscience, 2005.

[40] John A. Volpe National Transportation Systems Center: *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report for the Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, August 29, 2001.

[41] Wang, K., Chen, S., and Pan, A.: Time and Position Spoofing with Open Source Projects, *BlackHat EU 2015*, November 12th – 13th, 2015.

[42] Woo, K.-T.: Optimum Semicodeless Carrier-Phase Tracking of L2, *In Proc. of the 1999 International Technical Meeting of the Satellite Division of the Institute of Navigation*, also appeared in *Navigation 47*, no. 2, pp. 82-99, 2000.

[43] Mini-Circuits, RF/IF Microwave Components DC to 40 GHz, http://www.minicircuits.com.

[44] uBlox GNSS module overview, UBX-14000426-R06, uBlox, http://www.u-blox.com.

[45] NEO-M8, u-blox M8 concurrent GNSS modules, Data Sheet, UBX-13003366-R10, uBlox, http://www.u-blox.com.

[46] u-center, GNSS evaluation software, UBX-13003929-R06, uBlox, http://www.u-blox.com.

[47] u-center, GNSS evaluation software for Windows, User Guide, UBX-13005250-R10, uBlox, http://www.u-blox.com.

[48] UBX Daughterboard, Data Sheet, Ettus Research, http://www.ettus.com

[49] USRP N210, Data Sheet, Ettus Research, http://www.ettus.com

[50] GPS-SDR-SIM: Software-Defined GPS Signal Simulator, https://github.com/osqzss/gps-sdr-sim

[51] Humphreys, T.-E.: Detection strategy for cryptographic GNSS anti-spoofing, *IEEE Transactions on Aerospace and Electronic Systems*, 49(2), pp. 1073-1090, 2013.

[52] Wesson, K., Rothlisberger, M., and Humphreys, T.-E.: Practical cryptographic civil GPS signal authentication, *Navigation*, 59(3), pp. 177-193, 2012.

[53] GSA: Assuring authentication for all, April 18th, 2016, http://www.gsa.europa.eu/news/assuring-authentication-all

eIDAS and GDPR regulations
Nařízení eIDAS a GDPR

Martin Maisner

Martin Maisner
Maisner@rowanlegal.com

Martin Maisner is a founding partner of ROWAN LEGAL. He is a respected expert in the field of IT law; in reflection of for his deep understanding of this field and his extensive knowledge and experience, he was awarded the Lawyer of the Year award in 2012. In his practice, Martin focuses on IT law, data protection, contracts and IT dispute resolution. He also acts as recognized arbitrator in national and even international disputes. He has written several publications and multiple articles on topics relating to IT law, outsourcing and resolving of IT disputes and alternative dispute resolution. He lectures commercial law at NEWTON COLLEGE and is an external member of the Department of Commercial Law at the Faculty of Law at University of West Bohemia; he regularly gives lectures at the University of Economics in Prague and at the Technical University of Ostrava. Martin is a member of many international professional and scientific societies and speaks regularly at international conferences.

JUDr. Martin Maisner, PhD., MCIArb., je zakládajícím partnerem kanceláře ROWAN LEGAL. Je uznávaným právním odborníkem v oblasti práva ICT, v roce 2012 získal titul Právník roku v této specializaci. Specializuje se na právo informačních technologií, ochranu dat, smluvní vztahy a řešení sporů v IT. Je uznávaným rozhodcem na domácí a mezinárodní úrovni. Napsal více než deset publikací a řadu článků na téma internetového práva, outsourcingu odpovědnosti a sporů v oblasti IT a alternativního řešení sporů. Přednáší obchodní právo na NEWTON COLLEGE, je externím členem katedry obchodního práva na Právnické fakultě Západočeské Univerzity v Plzni; pravidelně přednáší na Vysoké škole ekonomické v Praze a Vysoké škole báňské – Technické Univerzitě Ostrava. Je členem řady mezinárodních odborných a vědeckých společností a pravidelně vystupuje na zahraničních konferencích.

eIDAS and GDPR regulations

In 2016, we expect two major things with a huge impact on the European single digital market to happen. Firstly, a majority of the Regulation No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market comes to effect and secondly, the approval of the General Data Protection Regulation is also expected. These regulations will have considerable impact on the security industry and the obliged entities will in many cases have to adapt their internal processes as well as the used legal documents. This paper describes the most significant changes brought by these regulations from the security perspective.

Nařízení eIDAS a GDPR

V roce 2016 dojde ke dvěma významným událostem, které budou mít velký dopad na evropský digitální trh. V účinnost vstoupí Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS) a předpokládá se schválení Všeobecného nařízení o ochraně osobních údajů. Tyto legislativní změny budou mít významný dopad do oblasti bezpečnosti a povinné subjekty budou muset v mnoha případech změnit své interní a klientské procesy i používané právní dokumenty. Tento příspěvek popisuje nejvýznamnější změny, které tato nařízení z hlediska bezpečnosti přinášejí.

1 Nařízení eIDAS a všeobecné nařízení o ochraně údajů

Rok 2016 je pro legislativu v oblasti počítačové bezpečnosti rokem velkých změn. Zejména na evropské úrovni přichází řada nových právních předpisů, jejichž přijetí se v nejbližší době očekává a bude třeba se na ně začít připravovat, nebo již brzy vstoupí v účinnost a stanou se součástí našeho života. Mezi tyto předpisy patří směrnice o vysoké úrovni bezpečnosti v síťových a informačních systémech, nařízení eIDAS a všeobecné nařízení o ochraně osobních údajů. V tomto příspěvku se věnujeme druhému a třetímu jmenovanému předpisu.

2 Nařízení eIDAS

Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (nařízení eIDAS), které vychází ze strategie „Europe 2020" a její iniciativy „Digital Agenda for Europe". V souladu se svým názvem nařízení upravuje dvě oblasti – elektronickou identifikaci a služby vytvářející důvěru. Klíčová ustanovení tohoto nařízení týkající se elektronických podpisů, elektronických pečetí a služeb vytvářejících důvěru vstoupí v účinnost již 1. července roku 2016. Plná účinnost nařízení eIDAS, se kterou je spojena zejména povinnost uznávat prostředky elektronické identifikace jiných členských států, nastane po uplynutí tří let ode dne použitelnosti prováděcích aktů, tedy v září roku 2018.

Jedním z hlavních principů nařízení eIDAS je podpora důvěryhodnosti elektronických transakcí poskytnutím jednotného základu pro bezpečnou elektronickou komunikaci mezi občany, podniky, ale také orgány veřejné moci. Důsledkem by mělo být posílení efektivnosti on-line služeb, elektronického podnikání a elektronického obchodu v EU. Nařízení dále cílí na odstranění již existujících překážek mezinárodního užívání prostředků pro elektronickou identifikaci, které se momentálně v rámci používání takových prostředků v jednotlivých státech objevují.

K elektronické identifikaci, což je první z hlavních upravovaných oblastí, stanovuje nařízení povinnost vzájemného uznávání prostředků pro elektronickou identifikaci při přístupu k online službám poskytovaným veřejným sektorem v rámci EU. Nařízením určeno jedno konkrétní řešení, které by členské státy EU musely jednotně implementovat, nicméně pro dané prostředky eIDAS stanovuje jasné technické požadavky a konkrétní podmínky pro jednotlivé tzv. úrovně záruk. Pro každou úroveň záruk pak budou muset členské státy uznávat při přístup k službám veřejné správy prostředky pro elektronickou identifikaci jiných členských států všude tam, kde bude služba přístupná pod národní elektronickou identitou stejné úrovně záruky.

Je třeba rovněž zmínit další institut, který s elektronickou identifikací souvisí a který je nařízením eIDAS regulován, a to elektronický podpis. Stávající česká právní úprava v podobě zákona č. 227/2000 Sb. o elektronickém podpisu, ve znění pozdějších předpisů tak bude z větší části nahrazena přímo samotným nařízením, doplněn bude zákonem o službách vytvářejících důvěru, který je momentálně připravován k projednání legislativními orgány a jenž by měl vstoupit v účinnost společně s nařízením. Nařízení eIDAS zachovává pojem zaručený elektronický podpis, kterým se stejně jako dle stávající české úpravy rozumí podpis, který je jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou a rovněž je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat. Vyšší úrovní elektronického podpisu, nově definovanou v nařízení eIDAS, je kvalifikovaný elektronický podpis, který musí být vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů, tedy např. podepisovacím zařízením jako je čipová karta. Taková zařízení jsou již v současnosti komerčně dostupná, jejich rozšíření však dosud není velké. Využití kvalifikovaných elektronických podpisů bude do budoucna vyžadováno na straně veřejné správy, je však stanoveno přechodné období dvou let, kdy bude možné využívat uznávaný elektronický podpis, kterým se i nadále bude rozumět zaručený elektronický podpis založený na kvalifikovaném certifikátu (tento pojem však není definován v nařízení eIDAS a objeví se tak pouze jako legislativní zkratka v našem zákoně o službách vytvářejících důvěru).

Nařízení eIDAS také nově zavádí pojem služby vytvářejících důvěru, kterým se označují elektronické služby, poskytované obvykle za úplatu a spočívající ve vytváření, ověřování shody a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami, nebo ve vytváření, ověřování shody a ověřování platnosti certifikátů pro autentizaci internetových stránek, anebo v uchovávání elektronických podpisů, pečetí nebo certifikátů souvisejících s těmito službami.

Rozlišuje se přitom prostá a kvalifikovaná služba vytvářející důvěru, která splňuje stanovené požadavky zejména v oblasti bezpečnosti a jejíž kvalifikovaný poskytovatel je evidován v důvěryhodném seznamu, který udává stav kvalifikace jeho služeb v době dohledu, čímž napomáhá budování důvěry mezi tržními subjekty. Významný rozdíl mezi kvalifikovaným a nekvalifikovaným poskytovatelem služeb vytvářejících důvěru bude v případě uplatňování odpovědnosti za škodu. Zatímco v případě škody způsobené nekvalifikovaným poskytovatelem bude břemeno tvrzení i důkazní na straně domáhající se osoby, v případě kvalifikovaného poskytovatele služeb vytvářejících důvěru se úmysl nebo nedbalost poskytovatele v případě vzniklé škody předpokládá, pokud daný kvalifikovaný poskytovatel služeb vytvářejících důvěru neprokáže, že škoda nastala bez jeho úmyslu nebo nedbalosti.

3 Všeobecné nařízení o ochraně údajů

Nakládání s osobními údaji je v současnosti v EU regulováno směrnicí 95/46/ES a každý členský stát EU má svoji národní právní úpravu, která směrnici implementuje. V České republice jde o zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Po dvaceti letech fungování směrnice však začalo být víc než zjevné, že její úprava na jednu stranu neposkytuje dostatečnou ochranu našemu soukromí v kontextu internetu a moderních sledovacích nástrojů a na druhou stranu vytváří umělé překážky pro rozvoj digitální ekonomiky např. formou složitého předávání osobních údajů do zahraničí. Z těchto důvodů Evropská komise v roce 2012 představila návrh nového všeobecného nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR). Jednání o textaci GDPR trvala téměř 4 roky a jejich výsledkem je finální text, který byl dojednán v prosinci roku 2015. Formální schválení GDPR se očekává na přelomu května a června roku 2016 a účinnost ve smyslu nutnosti přizpůsobit zpracování požadavkům GDPR nastane dva roky po jeho uveřejnění, na jaře 2018.

Účelem GDPR je posílit práva fyzických osob na ochranu údajů a usnadnit volný tok osobních údajů v rámci jednotného digitálního trhu, mimo jiné prostřednictvím snižování administrativní zátěže. V mnoha ohledech GDPR nepřináší revoluční změny, dřívější šedé zóny jsou však ve většině případů vyjasněny směrem ke striktnějšímu výkladu. S ohledem na tento fakt některé postupy, které bylo dříve možné považovat za hraniční, avšak stále přijatelné, tak podle GDPR již nebudou možné.

GDPR bude přímo účinné v celé EU, nebude tedy nutné přijímat národní právní úpravu a dojde tak k překonání rozdílnosti současných národních úprav, které byly na překážku volnému pohybu služeb v oblasti zpracování osobních údajů. GDPR také reaguje na požadavky nejnovější judikatury a řadu z nich zapracovává přímo do svého textu, např. právo být zapomenut. Současně ale upravuje řadu nových práv subjektů údajů a zejména povinností správců a zpracovatelů. Jednou z významných změn, které GDPR zavádí, je úprava územní působnosti. GDPR se budou muset řídit i společnosti, které nemají své sídlo v EU, ale mají zde pobočku a zpracování se týká této pobočky, a také ty společnosti, které nabízejí své služby či zboží fyzickým osobám v EU nebo monitorují chování těchto fyzických osob v EU.

GDPR staví na principech, jako je zákonnost, férovost a transparentnost, omezení účelem, minimalizace dat, přesnost, omezení uchovávání, integrita a důvěrnost, odpovědnost správce a povinnost prokazování. Zejména zásada zákonnosti, férovosti a transparentnosti se přitom promítá jak do oblasti získávání souhlasu, tak do oblasti informační povinnosti. V souladu s principem transparentnosti musí být např. subjektům údajů zřejmé, jaké osobní údaje jsou shromažďovány, užívány nebo jiným způsobem zpracovávány a v jakém rozsahu jsou osobní údaje zpracovávány (nebo budou v budoucnosti zpracovávány). V souladu s principem transparentnosti musí být dále také informace týkající se zpracování osobních údajů jednoduše dostupné a jednoduše srozumitelné a musí být při jejich poskytování užíván jednoznačný a srozumitelný jazyk. V souladu se zásadou zákonnosti potom musí být osobní údaje zpracovávány na základě souhlasu subjektu údajů nebo jiném základě stanoveném v GDPR nebo jiném předpise členského státu nebo právu Unie.

Vymezení základních pojmů se v GDPR významně nemění. Osobními údaji jsou dle GDPR i nadále veškeré informace o identifikované nebo přímo či nepřímo identifikovatelné fyzické osobě. Definice nově zdůrazňuje, že při posuzování zda je osoba identifikovatelná je třeba hledět také na lokalizační údaje a elektronické identifikátory jako jsou síťové adresy či cookies. Zpracováním se i nadále rozumí jakýkoli úkon nebo soubor úkonů s osobními údaji. Definice souhlasu subjektu údajů byla oproti směrnici 95/46/ES upravena souhlasem se rozumí „jakýkoli svobodný, výslovný, vědomý a jednoznačný projev vůle, kterým subjekt údajů dává, a to buď prostřednictvím prohlášení, nebo jasnou kladnou akcí, své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování“. Na základě doplněné definice proto nebude možné udělit souhlas se zpracováním osobních údajů mlčky, tj. například konkludentním jednáním, ze kterého by za určitých okolností bylo možné dovozovat udělení souhlasu. Je přitom třeba zdůraznit, že souhlasy se zpracováním osobních údajů získané před účinností tohoto GDPR budou po jeho účinnosti nadále platné jen v tom případě, kdy byly získány v souladu s podmínkami GDPR.

GDPR nově ukládá správci i zpracovateli velké množství povinností, jejichž splnění má povinnost prokazovat. Jak správce, tak zpracovatel, jsou proto povinni vést záznamy o zpracování osobních údajů, jejichž obsah je nově podrobněji vymezen. Na výzvu musí správce, resp. zpracovatel tyto záznamy předložit orgánu dozoru ke kontrole. V GDPR jsou upraveny tři nové instituty, které mohou správcům a zpracovatelům usnadnit zmíněné prokazování plnění povinnosti dle GDPR. Prvním z nich je kodex chování, kterým se správce či zpracovatel zavazuje dodržovat určité chování, které splňuje nároky specifikované v GDPR. Dalšími instituty jsou osvědčení, pečeti a známky o ochraně údajů a standardní smluvní doložky. Tyto nástroje je možné využít k prokázání splnění celé řady povinností, jako například povinnosti zabezpečovat osobní údaje, a to jak u správce, tak u zpracovatele, či povinnosti zajistit vhodné záruky ochrany při předávání osobních údajů do třetích zemí.

Zcela novým institutem je pozice inspektora pro ochranu osobních údajů. Zřizovat ji musí správce i zpracovatel, pokud je orgánem veřejné moci, pokud se jejich klíčové aktivity sestávají z operací, které z důvodu své povahy, rozsahu či účelu vyžadují pravidelné a systematické monitorování subjektů osobních údajů ve velkém měřítku, anebo pokud se jejich základní činnosti sestávají ze zpracovávání speciální kategorie osobních údajů (např. údaje o zdravotním stavu). Inspektor pro ochranu osobních údajů musí splňovat expertní znalost práva a praxe v oblasti ochrany osobních údajů. Co se týče vztahu ke správci či zpracovateli, může svou činnost vykonávat jak v pracovním poměru, tak na základě smlouvy o poskytování služeb. Správce resp., zpracovatel dále musí zajistit, aby byl inspektor informován o aktivitách správce, resp. zpracovatele spojených se zpracováváním osobních údajů. Inspektor musí být ohledně své činnosti nezávislý, odpovídat přímo nejvyššímu vedení a je vázán mlčenlivostí ohledně výkonu svých úkolů. Dále má informovat správce či zpracovatele o jeho povinnostech vyplývajících z GDPR a dohlížet na jejich dodržování, poskytovat správci, resp. zpracovateli rady ohledně posuzování dopadu na ochranu osobních údajů, spolupracovat s orgánem dohledu a sloužit jako kontaktní osoba pro otázky související s osobními údaji.

Nově také nemusí správce oznamovat orgánu dozoru svůj záměr zpracovávat osobní údaje. Tato povinnost je nahrazena povinností vést záznamy a také povinností provést posouzení dopadů na ochranu osobních údajů v případě, kdy zpracování může představovat s ohledem na povahu, rozsah, kontext a účely zpracování vysoké riziko pro práva a svobody jednotlivce (zejména při využití nových technologií).

4 Závěr

Oba diskutované právní předpisy, tedy nařízení eIDAS i GDPR, budou mít podstatný dopad do oblasti bezpečnosti. Zatímco nařízení eIDAS bude za pár měsíců realitou, se kterou se budeme muset vyrovnat, GDPR je zatím spíše budoucností. To však neznamená, že by nebylo třeba tuto právní úpravu brát v potaz – ba naopak, řada požadavků stanovených GDPR bude vyžadovat zásadní změny dosud využívaných procesů, které si vyžádají svůj čas, proto je vhodně se na ně začít připravovat již nyní.

Panel Discussion
Panelová diskuse

Path to eHealth in the Czech Republic

Cesta k eHealth v ČR

Jiří Borej
Vlastimil Černý
Leoš Heger
Soňa Měrtlová
Petr Pavlinec

Jiří Borej
Jiri.Borej@mzcr.cz

Ministerstvo zdravotnictví
Koordinátor Národní strategie elektronického zdravotnictví

Jiří Borej se aktuálně věnuje elektronizaci zdravotnictví a tvorbě Národní strategie elektronického zdravotnictví. Pracuje na Ministerstvu zdravotnictví jako Koordinátor Národní strategie elektronického zdravotnictví. Profesní praxi v oboru IT získal jako poradce v oblasti řízení ICT, zpracování strategií rozvoje informatik státní správy i komerčních podniků a v posledních třech letech jako Enterprise architekt vytvářející podnikové architektury a architektury komplexních agend, jako např. elektronické volby. Tomu předcházela dvanáctiletá praxe v pozicích ICT nebo Operations manažerů významných telekomunikačních společností jako Eurotel, British telecom a Aliatel.

Vlastimil Černý
vlastimil.cerny@vfn.cz

Všeobecná fakultní nemocnice v Praze
Náměstek pro informatiku

Leoš Heger

hegerl@psp.cz

Parlament ČR
Poslanec

Member of the Czech Parliament, Member of the City Board of Hradec Králové, former Minister of Health, former director of the University Hospital in Hradec Kralove. Since the early 90s he was active not only at the faculty (as Dean for Development), but gradually became a member of the Scientific Council of the Ministry of Health, the chairman of the Association of Hospitals and Vice Chairman of the Board of Trustees of the Internal Grant Agency of the Ministry of Health. In the period 1993-2009 he worked as medical deputy director and later director of University Hospital. In connection with the entry into the big league politics he resigned as director of UH HK. In 2010 he was elected as Member of Parliament (representing TOP 09) and later became Minister of Health. He defended mandate of the Member of the Czech Parliament in the autumn of 2013.

Poslanec PČR, zastupitel Hradce Králové, bývalý ministr zdravotnictví ČR, bývalý ředitel FN Hradec Králové. Od počátku 90. let se aktivně angažoval nejen na fakultě (jako proděkan pro rozvoj), ale postupně se stal také členem Vědecké rady ministerstva zdravotnictví, předsedou Asociace nemocnic a místopředsedou Správní rady Interní grantové agentury Ministerstva zdravotnictví. V období let 1993-2009 působil ve funkci lékařského náměstka a posléze ředitele Fakultní nemocnice Hradec Králové. V souvislosti se vstupem do vysoké politiky se vzdal postu ředitele FN HK. V roce 2010 byl již za TOP 09 zvolen poslancem Parlamentu ČR a posléze se stal ministrem zdravotnictví. Poslanecký mandát na podzim 2013 obhájil.

Soňa Měrtlová

Mertlova.S
@kr-vysocina.cz

Kraj Vysočina
Zástupce vedoucí odboru zdravotnictví

Soňa Měrtlová graduated from the Faculty of Economics and Administration at Masaryk University in Brno, Department of Public Economics and Administration, with a focus Economy and Health Management – Bachelor studies and Faculty of Business and Economics of the Czech Agricultural University in Prague, Department of Public Administration and Regional Development - Master's degree.
Now she works as an economist and Deputy Head of the District Office in Jihlava – Health department (state administration in the health sector, management of health facilities, economic analysis, budget adjustments – the budget chapter Health, control activities).

Soňa Měrtlová vystudovala Ekonomicko-správní fakultu Masarykovy univerzity v Brně, obor Veřejná ekonomika a správa se zaměřením Ekonomika a řízení zdravotnictví – bakalářské studium. A Provozně ekonomickou fakultu České zemědělské univerzity v Praze, obor Veřejná správa a regionální rozvoj – magisterské studium.
Nyní pracuje na pozici ekonom a zástupce vedoucí referátu na Okresním úřadě v Jihlavě – – referát zdravotnictví (výkon státní správy v oblasti zdravotnictví, správa zřizovaných zdravotnických zařízení, ekonomické rozbory, úpravy rozpočtu Kapitoly Zdravotnictví, kontrolní činnost).

Petr Pavlinec

Krajský úřad Kraje Vysočina
Vedoucí odboru informatiky

Currently Head of the Department of Informatics of the Regional Authority of Vysocina Region (one of 14 Czech Regions). Born in 1976, graduated from the University of Economics in Prague in the fields of information technology, knowledge engineering and economics. His professional career in ICT began in 1996 as a programmer and systems administrator CAD BOSCH Automation.
Since 2001 he is working as head of the Department of ICT (CIO) in Regional Authority. During his work at the regional office became vice-president of Commission of Informatics, Association of Czech Regions (2002-2004), chairman of the GIS Working Group of Czech Regions (since 2005) and member of The Government Council for Information Technology (2013).

V současné době vedoucí odboru informatiky Krajského úřadu Kraje Vysočina. Narozen v roce 1976, vystudoval Vysokou školu ekonomickou v Praze v oborech informační technologie, znalostní inženýrství a ekonomie. Svoji profesionální kariéru v ICT zahájil v roce 1996 jako programátor a správce CAD systémů firmy BOSCH Automatizace.
Od roku 2001 pracuje jako vedoucí oddělení a později odboru informatiky Krajského úřadu Kraje Vysočina. Během působení na krajském úřadě se stal místopředsedou Komise informatiky AKČR (2002-2004), předsedou pracovní skupiny GIS krajů (od 2005) a členem Řídícího výboru Rady vlády pro konkurenceschopnost a informační společnost ČR (2013).

Path to eHealth in the Czech Republic?

eHealth is actually a hot topic of Czech Republic health care for many reasons – searching for efficiency, achieving better services, digitalization of agendas, etc. eHealth area has faced the experience of successful projects (regional communications Ambulance / Hospital) and failures (IZIP ...) as well. Currently there is the National Strategy for eHealth (NSeZ) under preparation, which should significantly help the development of eHealth in the Czech Republic. We would like to focus our panel discussion on:

- Where are we going within eHealth in the Czech Republic?
- Are all the necessary basics ready to allow digitalization?
- Are there formulated the right priorities – registers, insurance houses?
- How the experience of successful projects and failures can help us?
- Security goes hand in hand with the digitalization – Do we have security in mind when creating eHealth?

Cesta k eHealth v ČR

eHealth je aktuálním tématem ve zdravotnictví v ČR z mnoha důvodů – hledání efektivity, poskytování lepších služeb, elektronizace agend atd. V ČR máme v oblasti eHealthu zkušenosti, ať již úspěšné projekty (krajské komunikace Záchranka/Nemocnice), tak i nezdary (IZIP,...). Aktuálně se připravuje NSeZ – Národní Strategie elektronického Zdravotnictví, která by měla významně pomoci rozvoji oblasti eHealth v ČR.

V naší panelové diskusi se budeme věnovat následujícím tématům a otázkám:

- Kam směřujeme v ČR v rámci eHealthu?
- Jsou k dispozici všechny potřebné základy, které elektronizaci umožní?
- Existují formulované správné priority – registry, pojišťovny?
- Jak nám mohou pomoci zkušenosti z úspěšných projektů i nezdarů?
- S elektronizací jde ruku v ruce bezpečnost – máme ji na paměti při tvorbě eHealth?

A magazine on information systems security, administration and management for middle and higher management.

Časopis o bezpečnosti, správě a řízení rizik informačních systémů určený pro střední a vyšší management.

Publisher's address / adresa redakce:

TATE International, s.r.o.

DSM – data security management

Hořejší nábřeží 21

150 00 Praha 5

tel.: +420 257 920 319-20, fax: +420 257 313 695

e-mail: dsm@tate.cz

www.tate.cz

ISBN 978-80-86813-29-5