# Bezpečnost jako služba, nová dimenze vnímání informační bezpečnosti

Je možné ochránit informační systémy pouze pasívním použitím technologií? Co přináší bezpečnost jako služba a jak může pomoci naplnit např. požadavky kybernetické bezpečnosti a související legislativy?

Již léta se hovoří o tom, že kybernetická bezpečnost není jen otázkou technologií. Přesto se dnes aplikují prakticky výhradně obranná opatření založená především na pasívním použití technologií [1]. Běžné je nasadit některé z vyzkoušených bezpečnostních řešení, které sice systém podle zadaných pravidel spolehlivě izoluje od okolí, naprosto však neřeší jeho vlastní zranitelnosti. Bezpečnostní systémy, do nichž se investovaly a neustále investují nemalé prostředky, jsou přece povinny si poradit se všemi útoky. Je přinejmenším obtížné specifikovat, nakolik je takové řešení spolehlivé, není-li zbytečně robustní a nákladné či jak dobře a rychle se dokáže přizpůsobit změnám v bezpečnostním prostředí. Mnohé podniky a organizace sice mají poměrně dobře definovaná nejrůznější bezpečnostní pravidla a politiky, změny bezpečnostního prostředí jsou ale tak rychlé a málo předvídatelné, že většinou není v možnostech manažerů vše sledovat a neustále přizpůsobovat.

Bezpečnost jako služba řeší kybernetické hrozby jako komplexní problematiku, jejíž součástí je monitoring bezpečnostního chování systému, prevence před hrozbami a jejich detekce na úrovni prostředí, integrace bezpečnostních produktů do funkčních a srozumitelných řešení poskytujících celkové, ale současně s tím i nejlepší možné zabezpečení informačního systému.

## Kybernetická bezpečnost

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů [2], definuje v § 7 pojmy kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu. Současně ukládá příslušným osobám kybernetické bezpečnostní události detekovat a v § 8 také hlásit bezpečnostní incidenty ve významném informačním systému provozovateli národního CERT a v kritické informační infrastruktuře Národnímu bezpečnostnímu úřadu.

Se zaváděním opatření pro plnění požadavků zákona o kybernetické bezpečnosti souvisí celá řada procesních, technologických i organizačních opatření, která se musí mezi sebou provázat a skloubit. To není úplně jednoduchá záležitost a v mnoha případech bývá podceňována. Ani jedno opatření navíc není zdarma. Vyžaduje určitý rozpočet, který v původních plánech nemusel být. Je třeba platit za organizační a procesní změny, za vzdělávání, ale i za technologie. Aby se naplnila litera zákona, dochází často k hledání kompromisních řešení.

Prozíravé společnosti, které v minulosti dobře plánovaly, začaly na změnách pracovat s předstihem a aktivity související se zákonem začaly naplňovat. Nejde však jen o zákon, ale také o navazující aktivity. Např. o nejlepší praktiky, které jsou přímo definovány třeba ve standardech řady ISO 27000, či související zákony, jako je zákon o informačních systémech veřejné správy, zákon o ochraně osobních údajů a mnohé další. Je zřejmé, že problematiku kybernetické bezpečnosti je nezbytné řešit komplexně jako celek. Jde o multidisciplinární záležitost, do níž vstupuje celá řada ostatních disciplín, které bývají v podnicích a organizacích již nějakým způsobem realizovány. Příkladem implementace bezpečnosti jako služby pro naplnění zákonných požadavků organizace veřejné správy může být využití Security Expert Centra (viz Box 1).

## Vědět, co chránit

Každá informace má svoji cenu a útočníci si většinou vybírají aktiva, která jsou pro ně zajímavá, přinášejí přímý či nepřímý finanční zisk nebo poskytují něco, co se dá na peníze transformovat. Aktiva, která je třeba chránit před nežádoucím přístupem, zneužitím, zveřejněním, změnou nebo zcizením, mohou zahrnovat hardware, software a aplikace nebo jiné neveřejné informace. 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. Znalost hodnoty aktiv navíc umožní již v samém počátku výrazně omezit a přesněji plánovat náklady na implementaci i provoz bezpečnostních opatření. Obecně totiž platí, že investovat do bezpečnosti má smysl nanejvýš tolik, kolik činí potenciální ztráty z jejího porušení. Byť jsou identifikace a hodnocení aktiv jednou z nejméně atraktivních činností při zavádění informační bezpečnosti, bez nich rozhodování o způsobech ochrany, vynaložené úsilí a prostředky nejsou podložené a obvykle vedou pouze k bezúčelnému plýtvání penězi.

## Strategie a taktika realizace IT bezpečnosti

Při realizaci kybernetické bezpečnosti jsou zcela klíčovými faktory strategie a taktika. Neexistuje-li strategie a neuplatňuje-li se správná taktika k jejímu dosažení, nedostavují se ani výsledky, zvyšují se náklady a zbytečně se maří investice. Nestanoví-li se na začátku určitý koncept jak celý komplex bezpečnosti realizovat, může dojít k situaci, kdy se jednotlivá opatření realizují odděleně, rostou náklady, zpomaluje se postup a nezřídka vznikají závazky, které mohou v budoucnu významně komplikovat život. Zodpovědní manažeři jsou zavalováni operativou a na činnosti, jež by měly být hlavní náplní jejich práce, jim nezbývá čas.

**Security Expert Center pro kritické a významné systémy ve státní správě** — BOX 1

**Klient**
Organizace veřejné správy, která provozuje několik rozsáhlých agend s celostátní působností a současně informační systémy nezbytné pro svůj chod.

**Požadavky**
Systémy klienta byly klasifikovány jako kritické či významné a bylo třeba je uvést do souladu s požadavky zákona o kybernetické bezpečnosti a příslušných vyhlášek.

**Prostředí**
Systémové záznamy se v multiplatformním IT prostředí pouze shromažďovaly a ukládaly na lokální disky. Nevyužívaly se nástroje pro záznam aktivit uživatelů, neprobíhala detekce kybernetických bezpečnostních událostí a nebyl implementován ani nástroj pro ochranu před škodlivým kódem či sběr a vyhodnocení bezpečnostních událostí podle zákona o kybernetické bezpečnosti.

**Řešení**
V rámci správy záznamů byly nejprve instalovány dva kolektory pro záznam aktivit příslušných částí informačního systému klienta, jejich administrátorů a uživatelů. Záznamy se ukládají po dobu tří měsíců do důvěryhodného archivu a průběžně kontrolují analytiky SEC. Zjištěné bezpečnostně relevantní události a informace se odesílají do nástroje pro vyhodnocení kybernetických bezpečnostních událostí, který incidenty na základě pro zákazníka připravených a na doporučení analytiků neustále rozšiřovaných korelací automaticky vyhodnocuje. V rámci služeb SEC se v pravidelných intervalech uskutečňuje sken zranitelností a hrozeb. K detekci kybernetických bezpečnostních událostí, víceúrovňové ochraně před škodlivým kódem a filtraci internetového provozu mezi vnitřní a vnější sítí klienta se využívá služba O2 Next Generation Firewall. Byly rovněž nastaveny procesy zpracování a hlášení incidentů. Prostřednictvím webového rozhraní nezávislého tiketovacího systému jsou k dispozici informace o přístupech jednotlivých uživatelů do systému a k aktivům, o přístupech v rozporu s komunikačními a dalšími pravidly, o nejčastějších incidentech a s nimi spojených aktivech, o aktivech s největším počtem zranitelností a o řadě dalších.

**Přínosy**
Zatímco standardní implementace on-premise stejného rozsahu obvykle trvá několik měsíců, k přípravě, nastavení a kompletnímu uvedení služeb SEC do provozu stačilo pouhých šest týdnů. Požadavky zákona kybernetické bezpečnosti a souvisejících vyhlášek byly zcela naplněny a lze je navíc pružně rozšiřovat. Po celou dobu platnosti smlouvy má klient k dispozici profesionály SEC, kteří sledují aktuální stav bezpečnosti v organizaci a společně s analytiky reagují na vzniklé bezpečnostní hrozby v dohodnutém časovém intervalu. Náklady na bezpečnost se přesunuly z investičních do operativních.

## Bezpečnost jako služba

Bezpečnost jako služba, Security as a Service (SECaaS), je model, při němž podnik nebo organizace nezajišťuje svoji informační bezpečnost vlastními silami, ale nakupuje ji nebo její části jako službu od externího poskytovatele. Nákup služby přináší několik zásadních výhod. K hlavním z nich patří:

- možnost soustředit se na vlastní aktivity,
- snížení nákladů na IT bezpečnost,
- zjednodušení správy a provozu IT bezpečnosti,
- rozšiřitelnost a variabilita,
- rychlé nasazení,
- optimalizovaná řešení,
- využití odbornosti a zkušeností,
- nepřetržitá aktualizace,
- soulad s legislativou.

Bezpečnost IT jako služba umožňuje poskytnout firmě nebo organizaci bez ohledu na velikost či oblast působnosti odpovídající přístup k vždy aktuálním bezpečnostním nástrojům a postupům. Solidní a renomovaný poskytovatel obvykle disponuje zkušenými odborníky a spolehlivými bezpečnostními nástroji, jejichž pořízení, provoz, obsluha a především

neustálá aktualizace a modernizace mohou přesahovat možnosti i relativně velkých subjektů. Počáteční náklady na implementaci IT bezpečnosti formou služby jsou oproti její realizaci vlastními silami zanedbatelné. Službu lze nasadit velmi rychle a později průběžně přizpůsobovat podmínkám, infrastruktuře a potřebám klienta. Příkladem takovéto aplikace služeb Security Expert Centra je situace (viz Box 2).

Poskytovatelé jsou rovněž odpovědni za provoz a správu nástrojů, hardware a software, které služby IT bezpečnosti doručují a zajišťují. Ve svém vlastním zájmu a především v zájmu svých klientů uskutečňují řízenou aktualizaci všech nástrojů, prostředků i znalostí, které využívají. Základní model poskytování je obvykle založen na měsíčních platbách, jejichž výše se odvíjí od rozsahu a množství bezpečnostních služeb, které klient využívá. Někteří poskytovatelé však nabízejí mnohem širší a variabilnější škálu modelů od jednoduchého paušálu až po převzetí do správy či dokonce odkoupení části nebo i celé IT infrastruktury klienta. Vytváří se tak zcela nová dimenze vnímání IT bezpečnosti, která zabezpečuje aktiva a současně umožňuje vyhovět legislativním požadavkům, např. zákonu o kybernetické bezpečnosti.

## Možnost soustředit se na vlastní práci

Řešení bezpečnosti IT formou služby zbavuje zákazníka nutnosti vykonávat složité a časově náročné činnosti spojené např. se zpracováním systémových záznamů (tzv. Log Management) nebo s monitorováním událostí. Sejme z jeho beder i mnoho pracných, namáhavých, složitých a zdlouhavých, povětšinou ale z hlediska bezpečnosti kritických činností a aktivit a umožní vedení, managementu i některým zaměstnancům se mnohem lépe soustředit na vlastní práci a předmět činnosti podniku nebo organizace. Poskytovatel nejenom vyhodnotí, zvolí a implementuje nástroje, prostředky, technologie a postupy pro dosažení maximální účinnosti v oblasti IT bezpečnosti, ale především dokáže zákazníkovi pomoci identifikovat a ohodnotit jeho aktiva. Služby IT bezpečnosti lze nasazovat postupně, počínaje základními, jako je právě správa systémových záznamů, jejichž správné nastavení a zpracování je nezbytnou podmínkou zajištění IT bezpečnosti, a na základě rozborů a analýz získaných výsledků je doplňovat a rozšiřovat. Typ, rozsah a množství poskytovaných bezpečnostních služeb je možné upravit a reagovat tím na okamžité, ale i dlouhodobé potřeby klienta (viz Box 3).

**Bezpečnost při vývoji či změnách** — BOX 2

**Klient**
Začínající společnost, která vyvíjí aplikační bezpečnostní brány pro zabezpečenou komunikaci mezi přenosnými zařízeními, jako jsou mobilní telefony, tablety nebo zařízeních pro internet věcí, a aplikačními servery umístěnými u zákazníka.

**Prostředí**
Klient na platformě Linux v hostovaném prostředí datového centra O2 vyvíjí a provozuje kompletně nové a originální řešení bezpečnostních bran. Vývoj je navíc velmi rychlý, až překotný.

**Požadavky**
S velkým důrazem na pravidelnost a spolehlivost reportingu bylo třeba zajistit provozní a bezpečnostní dohled nově vyvíjených i provozovaných bran. K hlavním požadavkům patřily: sběr a ukládání systémových záznamů z provozovaných bezpečnostních bran, vyhodnocování kompromitovaných mobilních zařízení, možnost snadno připojit další brány umístěné kdekoli ve světě, nepřetržitý (24×7) provozní a bezpečnostní dohled v angličtině i češtině.

**Řešení**
Základem služby je správa systémových záznamů. Jejich sběr zajišťují dva kolektory umístěné přímo v datovém centru O2. Záznamy se uchovávají po dobu jednoho roku a slouží k vyhodnocování bezpečnostních událostí a incidentů. Součástí služby jsou nepřetržité bezpečnostní a provozní dohledy, nástroje pro tiketing a reporting. Byly rovněž navrženy konfigurace a dodán detailní návod na instalaci agentů pro sběr záznamů v již provozovaných nebo vyvíjených branách. Klient má k dispozici webové rozhraní pro komunikaci i různé způsoby upozorňování prostřednictvím tiketingu, e-mailu a SMS. Reporty jsou přizpůsobeny potřebám zadavatele. Obsahují např. výpis připojených mobilních zařízení a jejich přístupů, seznam kompromitovaných zařízení, přístupy k branám v rozporu se zadanými pravidly atd.

**Přínosy**
SEC velmi pružně řeší i překotné změny v zabezpečovaném systému a umožňuje na ně velmi rychle reagovat. Je dostupný celosvětově a nové bezpečnostní brány i další mobilní zařízení lze k systému připojovat jednoduše bez ohledu na jejich umístění. Konfigurace agentů pro správu záznamů zajišťuje plnou podporu všech systémů, i těch nově vyvíjených.

## Security Expert Center

Příkladem poskytování IT bezpečnosti je služba Security Expert Center (SEC), kterou poskytuje společnost O2 IT Services. Sleduje, zaznamenává, analyzuje a hodnotí bezpečnostní chování IT infrastruktury klienta. Na definované IT infrastruktuře uskutečňuje bezpečnostní dohled, který umožní identifikovat její zranitelnosti. Na základě výsledků hodnocení předkládá klientovi podklady pro realizaci bezpečnostních opatření a popřípadě je pomůže uskutečnit. Implementaci služby předchází prvotní sken, který identifikuje aktiva. Poskytne zákazníkovi základní přehled o tom, co chrání a co nikoli. Výsledkem je definice informací, které bude třeba sbírat, a způsobu jejich předávání.

Technologicky zavedení služeb SEC obvykle spočívá v instalaci do infrastruktury zákazníka tzv. kolektoru, zařízení, které shromažďuje potřebné údaje o bezpečnostních událostech. Nad získanými záznamy, které se ukládají do důvěryhodného

**Bezpečný informační systém obce** BOX 3

**Klient**
Obec s rozšířenou působností, pro komunikaci s občany provozuje několik informačních systémů.

**Prostředí**
IT technologie na platformách Windows a Linux jsou umístěny v technologických místnostech. Správu zajišťuje minimální počet zaměstnanců s nulovým přehledem o aktivech organizace, která je třeba chránit. Systémové záznamy byly shromažďovány a ukládány pouze lokálně, chyběla základní bezpečnostní dokumentace.

**Požadavky**
Bez zásadních a nákladných úprav IT systémů obce a bez rozšiřování personálního zabezpečení jejich obsluhy bylo třeba zajistit bezpečnost IT provozu a služeb poskytovaných občanům.

**Řešení a implementace**
Bylo nezbytné identifikovat a klasifikovat aktiva organizace, vypracovat základní sady bezpečnostních dokumentů a na základě výsledků analýzy rizik realizovat služby sběru a ukládání záznamů pro Windows a Linux servery. Do prostředí zákazníka byly poté instalovány kolektory pro sběr záznamů. Záznamy se archivují po dobu tří měsíců a průběžně vyhodnocují analytiky SEC. Rozsah vyhodnocení je možné kdykoli rozšířit. Hlavním komunikačním kanálem klienta je webové rozhraní, k dispozici jsou i různé způsoby notifikace na základě zvolené úrovně upozorňování: tiket, e-mail a SMS.

**Přínosy**
Klient má k dispozici spolehlivou a účinnou službu, která řeší bezpečnost jeho informačních systémů a jimi poskytovaných služeb jako celek bez nutnosti pořizovat nákladné řešení on-premise a zaměstnávat další specialisty. Vytvořená dokumentace urychluje práci, určuje správné postupy a procesy a minimalizuje množství nejen procesních, ale i systémových a bezpečnostních chyb obsluhy. Pro řešení nenadálých nebo nepředvídaných situací je kdykoli k dispozici expertní tým SEC.

archivu, se provádí základní filtrování, jehož úlohou je identifikovat podstatné údaje. Následuje hodnocení bezpečnostních událostí, s jehož výsledky již pracují operátoři SEC. Ti spolu s analytiky identifikují bezpečnostní incidenty, hrozby, zranitelná místa a další bezpečnostní aspekty, a na jejich základě připravují návrhy bezpečnostních řešení, která projednávají s klientem. Nejčastěji jde o doporučení pro konfiguraci bezpečnostních systémů, jako jsou firewally, systémy IDS nebo IPS, může však jít také o návrhy velmi komplexních řešení a změn IT prostředí klienta včetně úprav procesů. V případě výskytu kybernetického bezpečnostního incidentu systém vygeneruje zprávu podle § 32 vyhlášky č. 316/2014 a po konzultaci s klientem ji odešle na kompetentní úřad. SEC rovněž organizuje následné kroky po vydání opatření NBÚ a podřízených orgánů dle § 33 vyhlášky č. 316/2014. Modulární řešení SEC umožňuje zákazníkovi zvolit služby tak, aby naplnily jeho poptávku po IT bezpečnosti.

## Důvěryhodný partner

Bezpečnost jako služba může přinést i některá rizika a úskalí, s nimiž by se měl uživatel seznámit. Vždy by měl vědět, jaké informace, v jakém rozsahu a za jakých podmínek poskytovatel využívá či přenáší. Přístup k informacím, způsob jejich přenosu a využití na straně poskytovatele by měly být ošetřeny smluvně a kontrolovány jako součást služby. Je důležité si uvědomit, že implementace služby IT bezpečnosti se v řadě případů dotkne i bezpečnostního nastavení v samotné infrastruktuře zákazníka. Může například dojít k instalaci nových senzorů či zařízení pro sběr dat nebo ke změnám v nastavení bezpečnostních prvků a systémů, např. firewallů. Důležité proto je, aby poskytovatel služeb byl vybaven nejen odbornými certifikacemi a oprávněními k provozování služeb bezpečnosti, ale aby byl pro zákazníka i důvěryhodným a spolehlivým partnerem.

## Závěr

Využitím služeb IT bezpečnosti se snímá z managementu klientů problém operativního řízení monitoringu a zajišťování IT bezpečnosti, získávají se informace pro práci ve strategicko-taktické rovině a umožňuje se vedení více soustředit na vlastní předmět činnosti. Významně se podpoří aktivity klienta při plnění podmínek zákona o kybernetické bezpečnosti a podmínek pro certifikaci ISO 27001 a ISO 22301, efektivně se ochrání klíčové procesy a zájmy a výrazně se posiluje IT bezpečnost klienta. Poskytovatel služby se pro klienta stává partnerem, s nímž může bezpečnostní situace nebo hrozby rychle a efektivně konzultovat i řešit.

Jiří Sedlák
*jiri.sedlak@o2its.cz*

**Ing. Jiří Sedlák**

Jako krizový manažer má více než 15 let zkušeností z transformací společností a optimalizací modelů a systémů jejich řízení. Prošel významnými manažerskými pozicemi v prostředí telekomunikačních operátorů a energetických korporací, např. jako ředitel odboru Bezpečnosti ICT ve společnosti ČEZ ICT Services nebo bezpečnostní ředitel Telco Pro Services. V současné době je ředitelem Security Expert Center ve společnosti O2 IT Services.

**POUŽITÉ ZDROJE**

[ 1 ] Petr Hampl: *Nové paradigma internetové bezpečnosti*. DSM 4/2015, str. 36.
[ 2 ] Zákon 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), Sbírka zákonů České republiky, Částka 75, 29. srpna 2014.