Bezpečnost IT jako služba

Jiří Sedlák

Platí, že investovat do bezpečnosti má smysl nejvýše tolik, kolik činí potenciální ztráty z jejího porušení. Ale jen málokdo dnes řeší kybernetické hrozby jako komplexní problematiku s cílem vytvořit skutečně funkční, srozumitelné a současně především z hlediska nákladů optimální zabezpečení.

Jsou firmy a organizace, které investují do bezpečnostních opatření, o jejichž účinnosti a spolehlivosti nejsou občas přesvědčeni ani realizátoři, ani jejich nejvyšší nadřízení, astronomické částky. Jiné, a je jich nejspíš více, aby dosáhly alespoň nějaké ochrany a dodržely minimální legislativní požadavky, vytvářejí z nedostatku znalostí, prostředků i odborníků obranné systémy, které jsou z pohledu kybernetických útočníků spíše úsměvné. Nejčastěji se nasazuje některé z vyzkoušených bezpečnostních řešení, které sice systém podle zadaných pravidel izoluje od okolí, naprosto však neřeší jeho skutečné zranitelnosti. Je přinejmenším obtížné určit, nakolik je takové řešení spolehlivé, nebo naopak není-li zbytečně robustní a nákladné.

Nikoli proč, nýbrž co, jak a kdo?

Problém digitálního světa je ve stírání hranic. Globální kybernetický svět poskytuje možnost zaútočit odkudkoli. Z Číny, z Ameriky, z Ruska nebo třeba ze sousední kanceláře. Následky útoku mohou nejenom negativně ovlivnit podnikání, poškodit důvěru, zničit dobré jméno a nezřídka otřást i samými základy existence firmy nebo organizace, ale i poškodit určité zaměstnance nebo zákazníky. Otázka proto už dávno nezní, zda své IT zabezpečit, nýbrž jak je zabezpečit, co z něho zabezpečit a komu zabezpečení svěřit.

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. Znalost hodnoty aktiv navíc umožní již v samém počátku výrazně omezit a přesněji plánovat náklady na implementaci bezpečnostních opatření. Byť jde o jednu z nejméně atraktivních činností při zavádění informační bezpečnosti, bez znalosti toho, co je třeba chránit, kde jsou chráněná aktiva umístěna a jakou mají hodnotu, jsou rozhodování o způsobech ochrany, vynaložené úsilí a prostředky nepodložené, mnohdy zbytečné a obvykle vedou pouze k bezúčelnému plýtvání penězi.

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. Přináší několik zásadních výhod. Patří k nim zejména:

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

Bezpečnost IT jako služba umožňuje poskytnout kterékoli firmě nebo organizaci bez ohledu na velikost či oblast působnosti odpovídající přístup k nejmodernějším bezpečnostním nástrojům a postupům. Solidní a renomovaný poskytovatel obvykle disponuje erudovanými a zkušenými odborníky i výkonnými a spolehlivými bezpečnostními nástroji, jejichž pořízení, provoz, obsluha a především neustálá aktualizace a modernizace může přesahovat možnosti i relativně velkých firem. 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. 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 zákazník 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.

Soustředit se na vlastní práci

Řešení bezpečnosti IT formou služby zbavuje zákazníka nutnosti vykonávat složité a časově náročné činnosti spojené například 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 není

problém upravit a reagovat tím na okamžité ale i dlouhodobé potřeby klienta.

Bezpečnost IT a zákon o kybernetické bezpečnosti

Se zaváděním 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 z opatření navíc není zdarma, ale vyžaduje určitý rozpočet, který v původních plánech nemusel být. 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 ale jen o samotný zákon o kybernetické bezpečnosti č. 181/2014 Sb., ale také o navazující aktivity, které jsou definovány např. v standardech ISO 27000, či související zákony, jako je zákon o informačních systémech veřejné správy, zákon o ochraně osobních údajů a mnohé další. Problematiku kybernetické bezpečnosti je nezbytné řešit komplexně jako celek, neboť jde o multidisciplinární záležitost, do níž vstupuje celá řada disciplín, které jsou v podnicích a organizacích již nějakým způsobem realizovány.

Strategie a taktika bezpečnosti

Nestanoví-li se na začátku určitý koncept, kterým se celý komplex bezpečnosti realizuje, může dojít k situaci, kdy se jednotlivá opatření realizují odděleně, zvyšují se náklady, zpomaluje se postup a nezřídka vznikají závazky, které mohou v budoucnu významně komplikovat život. Zodpovědní manažeři jsou zavalováni operativou a na strategii a taktiku, jež by měly být hlavní náplní jejich činnosti, jim nezbývá čas. Využití služeb IT bezpečnosti zbavuje zodpovědné vedoucí pracovníky nutnosti řešit operativu, implementovat projekty, shánět peníze a specialisty do realizačních týmů a umožňuje jim soustředit se na hodnoty, které se mají chránit, a na opatření, která je třeba učinit. Vytváří se tak zcela nová dimenze vnímání IT bezpečnosti, která zabezpečuje aktiva a současně umožňuje vyhovět legislativním požadavkům.

Dnešní svět, a to i svět IT, se decentralizuje a nebývale rychle se otevírá. Rozšiřují se cesty k útokům a raketově roste jejich počet. Bezpečnost se stává komplexní disciplínou, která zahrnuje například sociální inženýrství, legislativu, vzdělávání, technologickou bezpečnost nebo fyzickou ochranu. Identifikovat aktiva a chránit je bude v otevřené společnosti neodmyslitelným základem bezpečného podnikání a poskytování služeb i života samotného. ■

Ing. Jiří Sedlák

Autor článku 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.