Budování ochrany důležitých informací

Jan Poduška, Maroš Barabas

Pod pojmem ochrana dat si pravděpodobně většina lidí jako první představí koupi a nasazení nějaké konkrétní technologie typicky DLP. Při podrobnějším zamyšlení ale zjistíme, že takto jednoduché to nebude. Aby DLP mohlo dobře fungovat, musí mít dobře nastavená pravidla a ta lze správně vytvořit, pokud máme jasnou představu, co chceme vlastně chránit. Při budování ochrany je tedy důležité začít od začátku.

Nejprve bychom se měli zamyslet, jaká je naše motivace začít řešit tuto oblast a tomuto potom přizpůsobíme následné kroky. Pokud je motivací zajištění souladu s určitou legislativou např. GDPR, bude nejefektivnější podniknout všechny následující kroky. Pokud je motivací např. reakce na únik dat, můžeme některé kroky vynechat.

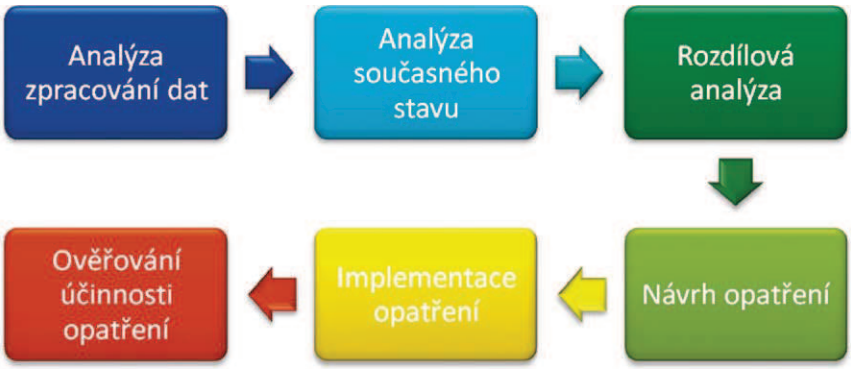
Následně bychom měli mít jasnou představu, jaká data chceme chránit, kde všude se vyskytují, jak se s nimi pracuje, jakými komunikačními kanály tečou. Důležité je rovněž zajistit, aby této aktivitě rozuměli i respondenti interview, zástupci jednotlivých oddělení, se kterými budeme celkový obraz pohybu dat dávat dohromady.

K dokreslení celkového obrázku a k zajištění toho, že jsme na žádnou aktivitu nezapomněli, nám pomůže zpracování celého životního cyklu všech důležitých dat v naší společnosti od okamžiku sběru informací, přes jejich zpracování, uchování v informačním systému, předání třetí straně po jejich skartaci. Především skartace bývá často opomíjeným krokem. Výstupem může být excelovská tabulka – mapa zpracování informací.

Analýza současného stavu

V průběhu identifikace dat obvykle narazíme na to, že data již dílčím způsobem chráníme např. pomocí řízení přístupu ke sdíleným složkám personálního či účetního oddělení. Pro identifikaci všech těchto opatření je vhodné provést analýzu současného stavu dle vybrané metodiky či normy. Vhodná je norma ISO/IEC 27002, která nám zajistí, že jsme na žádnou důležitou oblast jako je komunikace, šifrování, zálohování atd. nezapomněli. Zde je potřeba dobře definovat rozsah této aktivity. Pokud je motivací např. závažný únik dat a management společnosti je příznivě nakloněn řešení informační bezpečnosti, je ideální čas začít řešit informační bezpečnost komplexně, nejen se zaměřením na ochranu důležitých dat, ale se zaměřením na všechna aktiva společnosti. To je ale jiný příběh, přesahující rámec tohoto článku.

Nepovinným krokem závisejícím na naší motivaci je rozdílová analýza mezi popsaným současným stavem a cílový stavem, kterého chceme dosáhnout, nebo kterého musíme dosáhnout, protože to vyžaduje legislativa např. Zákon o kybernetické bezpečnosti.



Z této aktivity vzejde seznam rozdílů – nálezů, ke kterým již můžeme hledat nejefektivnější konkrétní opatření. Jednotlivé nálezy je vhodné ohodnotit z hlediska jejich závažnosti a náročnosti implementace opatření. Výstup nám dává základ pro plán implementace doplněný o termíny realizace a odpovědné osoby.

Procesní opatření

Opatření lze obecně rozdělit na procesní a technická. Typickým procesním opatřením je zavedení klasifikace informací, kdy rozdělíme data podle jejich citlivosti pro organizaci, definujeme stupně (např. chráněné, interní, veřejné) a způsoby přípustného zacházení s jednotlivými stupni. Například definujeme, že data označená jako „chráněná“ mohou být emailem posílaná jedině v šifrované podobě.

Dalším procesním opatřením může být zavedení či revize bezpečnostní politiky, příruček pro uživatele, provozních postupů apod., revize stávajících procesů zpracování informací např. zavedení mazání CV neúspěšných uchazečů o zaměstnání či zavádění nový procesů, typicky procesů pro evidenci žádostí a samotného naplňování práv subjektů údajů ve lhůtě stanovené GDPR.

Při ochraně důležitých informací jsou technická bezpečnostní opatření podpůrným řešením. Při výběru řešení doporučujeme postupovat v logických navazujících krocích a vycházet z implementovaných procesních opatření. Z první fáze bychom měli mít představu, zda se jedná o strukturovaná nebo nestrukturovaná data, kdo k nim má přístup a práva k těmto datům a to na úrovni úložišť (data at rest), koncových stanic a aplikací (data in use) a na úrovni sítě a přenosových medií (data in motion). Například klasifikace informací a dat je zásadní

Opatření	Může pomoct v identifikaci a detekci informací/dat?
Klasifikační nástroj	**Ano**, klasifikací získáme identifikaci citlivých dat při jejich vytváření.
Data Loss Prevention	**Ano**, DLP může pomoci při identifikaci dat, zejména technologie s tzv. „discover" funkcí.
Monitorování sítě	**Ne**, tyto nástroje nejsou schopny identifikovat osobní údaje a citlivé informace v obsahu síťového toku, případně z meta-dat. Jedná se o podpůrnou technologii.
SIEM technologie	**Ne**, funkcionalita SIEM technologií se obecně odvíjí od událostí, ne obsahu dat a rozlišovací schopnost SIEM je pod možností identifikace konkrétních údajů a dat. Jedná se o podpůrnou technologii, která je důležitá v celkové ochraně a detekci událostí vedoucích např. k ztrátě dat.
Monitorování uživatelů a stanic	**Ne**, tyto technologie se zaměřují na činnost uživatele a nedokáží identifikovat, zda pracuje s citlivými informacemi.
Databázový Firewall	**Ano**, může pomoct při identifikaci důležitých/citlivých informací a detekci úniku.
Webový aplikační Firewall	**Ano**, může pomoct v případě, že se informace nacházejí ve webových aplikacích.

Opatření	Může pomoct při ochraně a prevenci vůči únikům informací/dat?
Šifrování dat	**Ano**, důsledné šifrování všech úložišť chrání důvěrnost chráněných dat.
Šifrování provozu	**Ano**, v případě přenosu osobních údajů by měla být všechna média šifrována.
Řízení přístupů	**Ano**, systémy pro řízení přístupů jsou velice důležité pro vymezení oprávnění pro autorizované uživatele.
Data Loss Prevention	**Ano**, v preventivním režimu může zabránit krádeži nebo ztrátě dat.
Monitorování uživatelů a systémů	**Ne**, monitorovací nástroje nedokáží ochránit data, dokáží jen zjistit, že k úniku došlo.
Monitorování sítě	**Ne**, stejně jako v případě monitorování uživatelů nedokáže zjistit, zda se jedná o citlivá data.
SIEM	**Ne**, SIEM nástroje se zaměřují na vyhodnocování událostí tzv. „post mortem" a nedokáží data chránit, mohou ale pomoct v detekci úniků dat.
Zabezpečení koncových stanic (AEP, AV)	**Částečně**, zabezpečení koncových stanic chrání data vůči útokům na systémy, i když se nezaměřují přímo na ochranu osobních údajů, patří mezi základní vrstvu ochrany.
Firewall a IDPS	Ne, mohou ale pomoct při detekci úniku.
Webový aplikační firewall	**Ano**, v případě, že osobní údaje se nachází ve webových aplikacích.
Databázový firewall	**Ano**, v případě, že osobní údaje se nachází v databázích.

součástí ochrany důležitých informací a proto ji doporučujeme podpořit vhodným technickým nástrojem pro označování dokumentů např. DocTag. Souvisejícími kroky jsou výběr vhodné klasifikační politiky a edukace zaměstnanců.

Technická opatření ochrany informací

Po identifikaci pohybu informací napříč společností můžeme přistoupit k jejich ochraně. Na technické opatření ochrany informací a dat se můžeme dívat různými pohledy. Je potřeba se ale zamyslet, zda posuzované řešení je opravdu vhodné pro ochranu dané oblasti a zda neexistuje jednodušší a vhodnější opatření procesního nebo jiného charakteru. Technické opatření můžeme pro přehlednost rozdělit do dvou skupin – detekční a prevenční (pro zjednodušení nebudeme dále dělit na korektivní, direktivní atd.). Detekční technická opatření mohou pomoct při identifikaci, kde se nacházejí důležité citlivé informace a data a při detekci jejich úniku.

Prevenční technická opatření pomáhají v ochraně dat. Zásadní otázkou při výběru správného bezpečnostního opatření je pohled na komplexnost ochrany – zda jsou data chráněna v průběhu celého životního cyklu (in motion, at rest, in use) a zda poskytuje opatření ochranu (vůči narušení důvěrnosti, integrity a dostupnosti, nebo jen části) nad nejčastějšími vektory úniku dat (emailová komunikace, webová komunikace a přenosná média a zařízení).

Když navážeme na předcházející proces ochrany informací a dat, po identifikaci a klasifikaci informací je potřeba zabezpečit datová úložiště, ideálně silným šifrovacím mechanizmem a to nejen jejich uložení (např. šifrování databází, datových disků) ale i jejich přenos (např. šifrování přenosných zařízení, síťového toku ...).

Dalším krokem implementace technických opatření může být zavedení řízení přístupů, a to na systémové, síťové a aplikační úrovni. Implementaci vhodné technologie by mělo předcházet vytvoření procesní podpory v podobě směrnice/pravidel. Je nutné dodržovat least-privilege princip, kdy subjekt má přístup k objektu jen v případě, že je nezbytně nutný. Dále následují pravidla pro přidělování přístupu, jejich pravidelné monitorování a audit.

V neposlední řadě je možné doporučit jako nejvhodnější nástroj pro ochranu informací a dat implementaci vhodného DLP řešení. Samotné implementaci by měla předcházet analýza nasazení, kdy je vybrán nejvhodnější nástroj dle prostředí a povahy chráněných informací, dále je navržena politika a plán nasazení. Politika by měla vycházet a podporovat zavedený proces klasifikace pro maximalizaci efektivity DLP ochrany.

Závěrem

Z výše uvedeného plyne, že přístup k ochraně důležitých informací ve společnosti by měl být komplexní a zodpovědný. O co více energie vložíme do prvotní fáze sběru informací, do identifikace datových toků a návrhu opatření, o to jednodušší bude implementace procesních opatření a jednodušší výběr s levnější implementací technických opatření. ■

Ing. Jan Poduška

Autor článku působí jako Head of Risk & Compliance Division ve společnosti AEC.

Ing. Maroš Barabas, Ph.D.

Autor článku působí jako Head of Product Management ve společnosti AEC.