Kdo má plnit zákon?

V dnešní informační společnosti jsou informace považovány za hlavní zdroj ekonomického, sociálního a kulturního pokroku. Měřítkem úrovně informační společnosti není úroveň hardwaru, ale rozsah, kvalita, relevance a dostupnost informací a informačních služeb. Narůstající užití informačních a komunikačních technologií v činnostech organizací, firem i jednotlivců pak vyžaduje, aby při zpracování, přenosu, ukládání a opětovném využití objemů dat nedocházelo ke ztrátě životně důležitých údajů, ke vzniku chyb, kompromitaci nebo neoprávněné modifikaci dat. To vše a mnohem více má za úkol řešit kybernetická bezpečnost.

Svět kybernetické bezpečnosti se vyvíjí velmi dynamicky, pořád je to ale ještě svět, který nesmírně ovlivňují lidé, a právě u nich je potřeba začít. Rizika úniku a zneužití informací hrozí zejména zevnitř organizace. Podle výzkumů jsou lidé nejrizikovějším faktorem kompromitace, modifikace, vyzrazení, úniku a zničení citlivých dat a informací v organizaci (způsobují až 80 % kybernetických incidentů). Rizikovost tohoto faktoru ještě více umocňuje například rozmach BYOD. Většina nezabezpečených míst není zřejmá, o to užitečnější jsou pak rady profesionálů s bohatými zkušenostmi.

Problémem jsou ale také bezpečnostní chyby (zranitelnosti) v samotných zařízeních a jejich SW. Mezi ty nejaktuálnější lze zařadit například:

- kritickou zranitelnost v operačním systému iOS a Mac OS X dovolující útočníkům snadno získat přístup k citlivým uživatelským datům, např. k uloženým heslům pro jednotlivé služby;
- snadné zneužití mobilních telefonů z produkce společnosti Samsung – ovládání některých funkcí smartphonu na dálku a sledování jeho majitele;
- kritickou bezpečnostní chybu v programu Flash Player od společnosti Adobe;
- zadní vrátka do operačního systému Windows a webový prohlížeč Internet Explorer (v reakci na ně uvolněny aktualizace s označním kritické).

To vše se potom samozřejmě odráží také v průzkumech. Jeden z nich byl realizován agenturou Ponemon Institute, která oslovila téměř dva tisíce vedoucích manažerů a IT pracovníků s otázkami, které se týkaly toho, jaké hrozby pro IT vnímají jako největší. Výsledky ukázaly, že podle manažerů jsou největší hrozbou pro IT bezpečnost třetí strany, například dodavatelé cloudových služeb (49 %). IT pracovníci nejčastěji uváděli nezabezpečené webové aplikace (57 %) a nezodpovědné interní uživatele (56 %).

Jaké má taková situace řešení?

Když si v lepším případě vedení organizací uvědomí všechna hrozící rizika, často je jejich reakcí nákup různých zařízení a SW nástrojů a řešení renomovaných firem, které jim jsou prezentovány jako„všelék" na kybernetickou bezpečnost. Nelze říci, že tyto kroky nenapomáhají zlepšovat kybernetickou bezpečnost, naopak – jedná se o nezbytnou součást celkového řešení. V první řadě je ale nutné provést audit vlastních digitálních aktiv,

jehož výsledkem by měla být důkladná analýza rizik, která mohou nastat, a soubor opatření, jak na ně reagovat. K pořízení kvalitních technologií a nástrojů řešících kybernetickou bezpečnost a jejich správnému zapojení a provozování je v celkovém řešení naprosto nezbytné vytvoření a především dodržování systematické bezpečnostní strategie a kvalifikace a připravenost bezpečnostního týmu. Jakékoliv jednorázové investice nevedou k systematické bezpečnostní strategii, jen vyčerpávají rozpočet a způsobují provozní komplikace.

Další část řešení představuje implementace požadavků nového zákona č. 181/2014 Sb. (zákona o kybernetické bezpečnosti) a s ním souvisejících právních prováděcích předpisů (převážně vyhlášky č. 316/2014 Sb.) a platného mezinárodního standardu ISO/IEC 27001:2013. Ty do svých požadavků zapracovaly best practices v oblasti kybernetické bezpečnosti a jsou průběžně aktualizovány, což je především v této oblasti naprostou nezbytností.

Co se týče zákona o kybernetické bezpečnosti, jistě se nabízí otázka – kdo má plnit?

Na ni odpovídá samotný zákon, a to v § 3. Související a zajímavější otázkou je – měl by plnit jen ten, kdo má plnit? Vždyť nejen stát, ale i organizace samotné mohou čelit a také čelí problémům spojeným se ztrátou životně důležitých údajů, vznikem chyb, kompromitací nebo neoprávněnou modifikací dat. Ani u subjektů spadajících pod zákon o kybernetické bezpečnosti navíc nejde ani tak o to, že nesoulad může být potrestán pokutou, ale hlavně o skutečnost, že se tím značně minimalizuje riziko samotného kybernetického incidentu. A ten může být v důsledku mnohem horší než stotisícová pokuta. Pro organizaci by mohl být zcela likvidační a nejen v případě správců významných informačních systémů mít navíc také nedozírné následky pro všechny osoby, s jejichž daty se nakládá. Mimo to k samotným požadavkům zákona patří také povinnost v nezbytné míře zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro uvedené systémy. Správci tak musí promítnout požadavky ZKB do výběrových řízení jak na dodavatele služeb, tak i zboží. A který dodavatel splní tyto požadavky lépe než ten, jenž sám plní požadavky zákona?

Mezinárodní standard ISO/IEC 27001:2013, pro který je vypracován i jeho český ekvivalent ČSN ISO/IEC 27001:2014 a jehož propojení se zákonem o kybernetické bezpečnosti zmiňuje v § 29 samotný zákon, lze vnímat jako výchozí bod jak pro naplnění požadavků zákona, tak i pro kybernetickou bezpečnost jako takovou. Normu tvoří požadavky na ISMS, nebo-li systém řízení bezpečnosti informací. Do těla normy je včleněn dobře známý PDCA cyklus, protože ISMS je potřeba nejen zavést a provozovat, ale i monitorovat, průběžně vyhodnocovat jeho účinnost a neustále zlepšovat. Standard evokuje těchto pět funkcí:

- identifikace (řízení aktiv, posouzení rizik, navázání na cíle, zúčastněné strany, vedení a aktivity organizace, definice procesů, postupů a politik);
- ochrana (kontrola přístupu, povědomí a školení, bezpečnost dat, údržba a opravy komponent, dodržování procesů a postupů k ochraně informací, řízení technických bezpečnostních prvků);
- detekce (neustálé sledování bezpečnosti, nastavení detekčních procesů);
- reakce (plánování reakcí, řízení komunikace, provádění analýzy, případná zmírnění dopadu incidentu a jeho eliminace, zlepšování reakčních činností);
- obnova (provádění a udržování obnovovacích procesů a postupů).

Důležitou součástí jak požadavků normy, tak vyhlášky o kybernetické bezpečnosti jsou požadavky na bezpečnostní role. Bezpečnostní role garant aktiva znamená totéž, co v mezinárodním standardu vlastník aktiva, odpovědnosti jsou pro ně definovány stejně – odpovídají za rozvoj, použití a bezpečnost aktiva.

- **Roli manažera** kybernetické bezpečnosti, tedy osoby odpovědné za systém řízení bezpečnosti informací, by měl zastávat interní zaměstnanec organizace, protože jinak si lze velmi těžko představit správné nastavení a řízení ISMS, navázání na vrcholové vedení organizace, na její cíle a strategie. A bez toho bude systém nefunkční a spíše než přínos bude znamenat přítěž.
- **Role architekta**, tedy osoby zajišťující návrh a implementaci bezpečnostních opatření, by mohla být zajištěna i externě, ale pouze při úzce navázané spolupráci s manažerem kybernetické bezpečnosti a garanty (vlastníky) aktiv.
- **Roli auditora**, tedy osoby provádějící audit kybernetické bezpečnosti, by měla vykonávat osoba odborně způsobilá (praxe s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let) a výkon této role by měl být nestranný a striktně oddělený od výkonu všech ostatních bezpečnostních rolí. To vše evokuje jediné – tato role by měla být zajištěna externě.

ezú elektrotechnický zkušební ústav

Konečné řešení

Cesta k co možná nejvyšší úrovni kybernetického zabezpečení je cestou složitou. Je nutné dívat se na kybernetickou bezpečnost z mnoha různých úhlů pohledu a řešit ji komplexně. K tomu samotné pořízení a instalování technologií nestačí. Pro účinnou ochranu je důležité pochopit, jaké informace organizace má a jakou hodnotu pro ni znamenají. Je také zásadní uvědomit si cíle a reálné fungování organizace. Jen tak lze navrhnout opravdu účinné a efektivní řešení kybernetické bezpečnosti. Cílem není pouze jeho zavedení, ale také zaručená dlouhodobá funkčnost a rozvoj. Právě proto musí být v pravidelných intervalech ověřováno a certifikováno. Mělo by být schopné reagovat na změny organizace i jejího okolí. Jediným způsobem, kterým lze takového stavu dosáhnout, je zapojení vrcholového managementu organizace a pravidelné školení zaměstnanců o kybernetické bezpečnosti. Vedlejším důsledkem je pak snížení nákladů ICT a celkově vyšší efektivita procesů.

My nabízíme řešení a pomocnou ruku ve vaší snaze vydat se touto cestou.

Bc. Michal Hager

NAŠE ŘEŠENÍ

- Situační analýza kybernetické bezpečnosti
- Certifikace kybernetické bezpečnosti
  - Základní certifikát kybernetické bezpečnosti (Essential Certificate of Cybersecurity)
  - Rozšířený certifikát kybernetické bezpečnosti (Enhanced Certificate of Cybersecurity)
  - Certifikát nejvyšší úrovně kybernetické bezpečnosti (Top-level Certificate of Cybersecurity)
- Školení kybernetické bezpečnosti
- Osobní certifikace
  - Manažer kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Auditor kybernetické bezpečnosti
- Zajištění role auditora kybernetické bezpečnosti podle zákona č. 181/2014 Sb.
- Implementace, zajištění a instalace potřebných technologií ve spolupráci s partnery