Logické kroky k **analýze rizik ve výrobních podnicích**

Jan Poduška I Senior IT Security Consultant, AEC a.s.

Výrobní podniky, tj. středně velké společnosti se zaměřením na výrobu či obchod, obvykle začínají řešit informační bezpečnost až ve chvíli, kdy dojde k významnějšímu incidentu, jako je např. únik obchodních dat či soudní spor s bývalým zaměstnancem. Může to být i ve chvíli, kdy podnik přeroste parametry rodinné firmy a IT oddělení začíná tušit, že pro bezpečnost svých dat nedělá dost. Zpravidla na to není čas, někdy ani know-how. A toto je první důležitý krok – uvědomit si, že potřebujeme řešit oblast informační bezpečnosti. Z toho plyne, že je nutné získat podporu vedení a tím i prostor a prostředky na realizaci.

Bezpečnost lze řešit buďto vlastními silami, například vytvořením a obsazením pozice bezpečnostního správce, nebo angažováním externího dodavatele – specialisty na otázky informační bezpečnosti.

Řekněme, že vedení tyto aktivity schválilo. Vyčlenilo na to prostředky a čas. Jak tedy začít?

„Pojďme udělat analýzu rizik,“ může zaznít na poradě. Dobře, zamysleme se tedy, jak na to.

Interní zaměstnanec bude s největší pravděpodobností trpět tzv. provozní slepotou a nebude schopen odhalit veškerá slabá místa a objevená rizika následně objektivně zhodnotit.

Nový interní zaměstnanec v pozici řešitele či externí dodavatel zase nebude mít detailní znalost prostředí.

Logickým krokem, jak se v prostředí výrobního podniku rychle zorientovat, je analýza současného stavu informační bezpečnosti. Ta bývá typicky realizovaná přes jednotlivé kapitoly definované normou ISO/IEC 27002:

- Hodnocení a zvládání rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Personální bezpečnost
- Klasifikace aktiv
- Řízení přístupu
- Šifrování
- Fyzická bezpečnost
- Řízení provozu
- Řízení komunikací
- Nákup, vývoj a údržba systémů
- Řízení vztahu s dodavateli
- Zvládání bezpečnostních incidentů
- Řízení kontinuity
- Zajištění shody s požadavky

Samotná procesní část analýzy může být poměrně rychlá; některé oblasti, jako např. kapitola zabývající se šifrováním, mohou být velmi krátké, jelikož šifrování nebývá v podnicích tohoto typu běžně používáno. Závěry analýzy popisují aktuální stav informační bezpečnosti v podniku a zpravidla zadavateli potvrdí jeho neblahé tušení. Ba co víc, otevřou mu oči i v oblastech a souvislostech, které neočekával.

Vhodným doplňkem analýzy současného stavu bývá interní penetrační test, který v prostředí výrobních podniků obvykle odhalí celou řadu kritických nedostatků a jeho typickým výsledkem pak je získání práv doménového administrátora hned několika různými způsoby. Povšimněme si, jak dramaticky rostou nároky na procesní a hlavně technické znalosti, pokud by řešitelem měl být interní zaměstnanec bez předchozích zkušeností s informační bezpečností.

Analýza současného stavu nám zmapovala zranitelná místa a přinesla také návrhy na jejich odstranění formou plánu implementace. A to včetně určení priorit řešení jednotlivých zranitelností, časování a odhadu nákladů. Při předložení tohoto plánu vedení společnosti by mohla padnout otázka typu:

„Opravdu potřebujeme tolik peněz investovat do bezpečnosti? Vždyť nejsme banka…“

Než předkladatel půjde za vedením, měl by se zamyslet: Kolik peněz bude reálně potřeba? Potřebujeme vyřešit všechny zranitelnosti? Co potřebujeme chránit prioritně a nejvíc? A právě v této chvíli nastává čas pro další logický krok – analýzu rizik.

Nezbytné výchozí podklady pro analýzu rizik máme – výstupy z analýzy současného stavu. Nyní potřebujeme identifikovat a ohodnotit informační aktiva, tedy vše, co má pro naši společnost nějakou hodnotu. Každé aktivum ohodnotíme např. na stupnici 1-3 z pohledu:

- důvěrnosti – jak důležité je u tohoto aktiva zajištění přístupu pouze oprávněným uživatelům,

Tab. 1: Několik příkladů z praxe

Citát	Možné technologické řešení
„Bojíme se úniku výrobních nákresů v elektronické podobě.“	Implementací technologie Data Loss Prevention lze účinně zabránit jednoduchému kopírování citlivých dat mimo interní síť.
„Trpíme častými útoky na naše webové stránky.“	Technologie Web Application Firewall představuje samostatnou vrstvu ochrany webové aplikace, která přejímá veškerý provoz místo webového serveru. Dekóduje komunikaci a odstraňuje či zahazuje nepovolené znaky či dotazy a normalizuje data.
„Máme pocit, že se nám v interní síti dějí nekalé věci.“	Technologie Network Behavior Analysis provádí inteligentní analýzu nad síťovými daty, a dokáže tak identifikovat veškeré, i velmi drobné anomálie provozu. Příkladem může být neobvyklá komunikace se serverem ve východní Asii, v nočních hodinách apod.
„Nemáme kontrolu nad používáním mobilních zařízení.“	Pomocí technologie Mobile Device Management je možné definovat a vynutit minimální bezpečnou konfiguraci každého firemního mobilního telefonu, ale například i vzdáleně smazat data z ukradeného zařízení.

- dostupnosti – jak kritická je dostupnost aktiva oprávněnými uživateli,
- integrity – jak důležité je zachování bezchybnosti aktiva,
- hodnoty – jakou má aktivum cenu, jak snadno či obtížně aktivum dokážeme nahradit?

Hodnocení můžeme podle zvolené metodiky sečíst či vynásobit a dostaneme „žebříček“ aktiv podle jejich kritičnosti.

Jaká rizika plynou pro naše nejhodnotnější aktiva, jestliže známe naše zranitelná místa z analýzy současného stavu? To záleží na tom, zda existuje konkrétní hrozba, která dokáže využít některou zranitelnost konkrétního aktiva. Musíme identifikovat a ohodnotit reálné hrozby. K tomu vytvoříme katalog hrozeb, nebo nám dobře poslouží nějaký již existující, nad kterým se zamyslíme a doplníme ho o hrozby specifické pro naše prostředí. Ohodnotíme je z hlediska pravděpodobnosti uplatnění např. rovněž na stupnici 1-3.

Informační aktivum – vše, co má pro společnost určitou hodnotu, např. obchodní data, účetní informační systém, fyzické servery, zálohovací média.

Zranitelnost – slabé místo společnosti (ve vztahu k informačním technologiím), např. chybějící bezpečnostní záplaty operačního systému, chybějící proces zálohování, ale i nezamčené dveře do serverovny.

Hrozba – vnější škodlivé vlivy, které nemůžeme ovlivnit, např. požár, povodeň, zloděj atd.

Riziko – míra uplatnění konkrétní hrozby vůči konkrétnímu aktivu využitím konkrétní zranitelnosti aktiva.

Nyní přichází na řadu nejnáročnější část analýzy rizik. Pro každé kritické aktivum potřebujeme nalézt související zranitelnosti, relevantní hrozby a sepsat konkrétní scénář uplatnění rizika, protože jinak při závěrečné prezentaci může padnout věta:

„Co z těch čísel plyne? Rád bych slyšel konkrétní scénáře uplatnění rizika, co se může stát.“

Uvedu jeden příklad za všechny: aktivem mohou být obchodní smlouvy. Zranitelnost představuje chybějící šifrování na pevných discích notebooků. Hrozbu představuje krádež notebooku. Scénář uplatnění rizika může znít například takto:

V případě krádeže notebooku může vzhledem k absenci šifrovacího SW dojít k úniku citlivých informací obchodního charakteru, které využije konkurence. To v konečném důsledku povede k finanční ztrátě našeho podniku.

Nyní máme popsaná, a pokud jsme použili podpůrný matematický model vybrané metodiky, i spočtená rizika. Víme, která rizika jsou nejvyšší, kterých aktiv se tato rizika týkají a jaké zranitelnosti mají k těmto aktivům vztah.

S aktivy nic moc neuděláme, pořád pro nás budou mít svou hodnotu. Hrozby jako požár, povodeň či krádež také neovlivníme, můžeme se na ně pouze připravit formou havarijního plánu v rámci Business Continuity Managementu – řízení kontinuity činností. Jediné, co můžeme ovlivnit, jsou naše zranitelnosti. Z analýzy rizik už víme, jak poskládat priority řešení jednotlivých zranitelností.

Řadu zranitelností lze efektivně vyřešit vhodným administrativním opatřením, ovšem můžeme se setkat i s komentářem:

„Jsme výrobní podnik. Papírová opatření nás až tak nezajímají. Potřebujeme reálná doporučení, co dělat v praxi.“

Administrativní opatření jsou levnou variantou řešení, zpravidla však přinášejí „práci navíc“ a nemusejí být plnohodnotným řešením každého identifikovaného problému. V praxi vám mohou s přímým odstraněním nálezů pomoci bezpečnostní technologie, které však zase mohou představovat nemalé náklady. Záleží na tom, jaké problémy nás pálí nejvíc a jakým disponujeme rozpočtem.

Pokud chceme v našem podniku začít seriózně řešit informační bezpečnost, logické kroky nás dovedou k analýze rizik. S jejími závěry pak lze pracovat podle finančních a časových možností tak, aby bylo dosaženo akceptovatelné úrovně informační bezpečnosti. Řešení jednotlivých bezpečnostních problémů existuje celá řada, od levných administrativních opatření s omezenou účinností až po vyspělé technologie poskytující komplexní a komfortní pokrytí problémových oblastí. I zde bude nejspíš nejúčinnější jít tzv. zlatou střední cestou, tzn. nasadit kombinaci technologií s administrativními opatřeními, s využitím externích dodavatelů v oblastech, ve kterých si nejsme jistí. To nám poskytne optimální řešení informační bezpečnosti přizpůsobené na míru našemu provozu za přijatelnou cenu.

Jan Poduška

je absolventem Vojenské Akademie v Brně, fakulty letectva a PVO, oboru automatizované systémy řízení. Po dokončení studia v roce 2002 nastoupil do Vojenského technického ústavu letectva. Začínal jako programátor – analytik projektů modernizace systémů řízení protiletadlového raketového vojska. Později některé z projektů vedl. V roce 2006 působil ve společnosti e-commerce.cz jako analytik. Od roku 2007 pracuje ve společnosti AEC a.s. jako konzultant informační bezpečnosti, kde se podílí na analýzách rizik IS, řízení informačních rizik, penetračních testech, testech metodami sociálního inženýrství apod.