ANALÝZA RIZIK

Přístupy k provedení analýzy rizik IS

Organizace se často obávají projektu analýzy rizik, který je nutný při zavádění Systému řízení bezpečnosti informací (ISMS – Information Security Management System). Jedním z důvodů je i rozhodnutí, jakým způsobem (přístupem) analýzu provést.

Norma ISO 17799 specifikuje dva přístupy k provedení analýzy rizik: základní, detailní, a jejich kombinaci. Tyto varianty se rozlišují podle způsobu hodnocení, použitých metrik, úrovně detailu vstupů a výstupů atd. V tomto článku jsem však zvolil jiný pohled a z pozice nezávislého konzultanta bych chtěl nastínit výhody a nevýhody přístupů definovaných podle toho, kdo analýzu provádí, kdo je za ni odpovědný apod. Podle těchto kritérií lze rozdělit přístupy na:

- *Dodavatelský přístup* – projekt analýzy rizik provádí dodavatel a nese za něj také odpovědnost.
- *Vlastní přístup* – projekt analýzy provádí pracovníci organizace vlastními silami s pomocí zakoupené nebo vlastní metodiky, odpovědnost za provedení je na těchto pracovnících.
- *Partnerský přístup* – projekt analýzy provádí pracovníci organizace pod metodickým i projektovým vedením dodavatelské nebo konzultační společnosti, odpovědnost je na dodavateli (konzultantovi).

Hranice mezi přístupy, které jsou dány zejména odpovědností za provedení analýzy, mohou být u dodavatelského a partnerského přístupu těžko rozeznatelné. I u dodavatelského přístupu je spolupráce mezi organizací a dodavatelem poměrně intenzivní. Hlavní rozdíl je v celkovém pohledu na bezpečnost. U partnerského přístupu se organizace sama učí, jak zabezpečit svoje informace. V druhém případě spoléhá ve výhledu do budoucnosti ve všem na dodavatele a jím dodané (popř. outsourcované) produkty či služby.

Dodavatelské a vlastní přístupy jsou známé a běžně používané. Partnerská varianta není tolik obvyklá, i když podle mého názoru, se kterým se nijak netajím nejen v tomto článku, je pro celou řadu organizací bez ohledu na jejich velikost optimálním řešením. Typickým příkladem partnerského přístupu může být jeden moravský průmyslový podnik, kam dojíždím párkrát do měsíce na pravidelné i několikadenní konzultace týkající se kompletního zavádění ISMS. Celý holding čítající několik akciových společností používá jednotně SAP včetně sdílené infrastruktury. Bezpečnost je v celém holdingu řešena podle jedné bezpečnostní politiky a její prosazení má na starosti jeden bezpečnostní ředitel. Pilotní projekt detailní analýzy rizik IS, na kterém spolupracuji se týká jedné společnosti z holdingu. Pracovníci bezpečnostního oddělení se učí jak identifikovat aktiva, jak vést rozhovory s respondenty nebo jak tvořit výstupy. Jsem přesvědčen, že po skončení pilotu budou schopni sami postupně zanalyzovat celý holding s minimální odbornou pomocí. Dodavatelský přístup by byl neúměrně drahý a provedení vlastními silami je nemožné, protože by ho prováděli lidé (bývalí informatici), kteří byli přijati do právě vytvořeného bezpečnostního oddělení s chabými zkušenostmi z bezpečnosti informací.

Jednotlivé přístupy mají své nesporné výhody – přínos do budoucna, vyškolení vlastních pracovníků, přenos odpovědnosti na dodavatele, ale i nevýhody – cena, nejisté výstupy, nesystémové provádění ad-hoc. V následujících odstavcích jsou všechny tři přístupy podrobně popsány.

Dodavatelský přístup

Management organizace stále úzce spojuje bezpečnost informací s technologiemi a není tedy nic jednoduššího, než zadat odpovědnému řediteli úkol, aby vypsal výběrové řízení na dodavatele takového projektu. Stává se, že vítězem je dodavatel technologií, který analýzu rizik „spláchne“ jako součást dodání bez-

ANALÝZA RIZIK

Přístupy k provedení analýzy rizik IS

pečnostních karet pro přístup do systému.
Pokud je však vybrán dostatečně kompetentní dodavatel, je tento přístup optimální pro organizaci, která nemá k dispozici dostatečné know-how mezi vlastními pracovníky nebo je nechce projektem vůbec zatěžovat. Určitá spolupráce zaměstnanců s dodavatelem projektu je však nezbytná. Zejména úvodní činnosti týkající se popisu systému a tvorby modelů aktiv se neobejdou bez aktivní spolupráce. Bezpodmínečně nutná je spolupráce při hodnocení aktiv, hrozeb a zranitelností. Zde analytik klade otázky, na které znají odpověď pouze pracovníci dané společnosti.
V intenzitě spolupráce mohou být dodavatelský a partnerský přístup téměř adekvátní. Hlavní pointa je ale ve zpracování výstupů a prezentace výsledků analýzy. Výstupy by měly mít vždy dvě formy:

- ***pro management*** – stručné zprávy;
- ***pro konkrétní pracovníky odpovědné za bezpečnost*** – podrobné reporty včetně tabulek a dalších příloh.

Výstupy z analýzy provedené nekompetentním dodavatelem vypadají jako podklady ministrů při zasedání vlády. Zprávy o hodnocení aktiv nebo o analýze rizik mají i několik set stran včetně příloh s tisíci hodnot v nesrozumitelných tabulkách. Takové výstupy jsou ihned po dodání uloženy kdesi v archívu dvě patra v podzemí. Pokud ale tyto zprávy (zejména zprávu obsahující doporučení) tvoří společně dodavatel a pracovníci dané společnosti, tak se takový materiál stane kvalitním podkladem pro řízení bezpečnosti v organizaci. Ale tato spolupráce na výstupech projektu spadá do jiného přístupu. Výhodou dodavatelského přístupu je minimální zátěž pracovníků společnosti, protože kromě rozhovorů popřípadě vyplňování dotazníků dělá vše ostatní dodavatel projektu. Společnost tedy nepotřebuje nikoho, kdo ví, jak provádět analýzu rizik. Nemusí kupovat a studovat metodiky a hlavně nikdo z jejích pracovníků nemá odpovědnost za provedení analýzy. Zároveň však na konci projektu s posledním odborníkem od dodavatele odejde i know-how a vytvořené výstupy, jak již bylo zmíněno výše, se mohou stát nesrozumitelné. Pokud je analýza rizik jedním z prvních kroků velkého bezpečnostního projektu, nezřídka se stává, že celý projekt skončí nebo se minimálně na pár měsíců zastaví právě z toho důvodu, že v konečné zprávě jsou popsána tisíce doporučení, která potřebují dodatečnou interpretaci.

	Kdo analýzu provádí	Na kom je odpovědnost	Kdo prezentuje výsledky
Dodavatelský přístup	Dodavatel	Dodavatel	Dodavatel
Vlastní přístup	Pracovníci organizace	Pracovníci organizace	Pracovníci organizace
Partnerský přístup	Pracovníci organizace pod vedením dodavatele (konzultanta)	Dodavatel (konzultant)	Pracovníci organizace pod vedením dodavatele (konzultanta)

TAB.1: Rozdělení přístupů podle odpovědnosti

Vlastní přístup

Mnoho společností, které disponují vlastními odborníky, řeší bezpečnost informací svými silami. Jedná se o optimální řešení, pokud je k dispozici potřebné know-how podporované metodickými postupy či nástroji. V takovém případě provádějí analýzu rizik odborníci z vlastních řad, kteří kromě toho, že rozumí problematice, také znají informační systém organizace. Navíc je ze všech tří přístupů tento nejvíce nákladově efektivní.
Bez vlastních odborníků vede volba tohoto přístupu k jasné zkáze. Neexistuje horší varianta, než když se koupí metodika nebo software na provedení analýzy rizik a vyškolí se jeden z pracovníku oddělení IT. Ten dostane kromě svých každodenních povinností za úkol provést postupně detailní analýzu všech částí

Přístupy k provedení analýzy rizik IS

informačního systému včetně zpracování výstupů pro management či auditora. Takový přístup lze shrnout dvěma slovy: všechno špatně.

Během provádění detailní analýzy se (ne)zkušenost analytiků projeví zejména při rozhovorech s respondenty týkajících se zjišťování hodnoty informačních aktiv. Při takovém rozhovoru musí mít analytik nejen znalosti o daném systému a bezpečnosti obecně, ale musí být také trochu psychologem. Hodnotu informací lze vždy spolehlivě určit až tehdy, pokud se s nimi doopravdy něco negativního stane. Bez takové zkušenosti je pro respondenty velmi těžké si představit, jaký vliv bude mít například týdenní nedostupnost celého účetnictví. Před pár měsíci jsem vedl podobný rozhovor s hlavní účetní jedné významné státní instituce. Velmi striktně odmítla možnost modifikace platebního příkazu na několik desítek miliónů tak, aby tyto peníze došly na její osobní účet. Prý to není možné za žádných okolností. Po třiceti minutách „psychologického nátlaku“ paní účetní uznala, že to lze vcelku jednoduše provést. Ale nejsem si jist, zda bych toho byl schopen bez několikaletých zkušeností s podobnými rozhovory.

Tyto rozhovory tvoří zásadní vstupy do analýzy, ale stejně tak hodnocení hrozeb a slabin systému či samotný návrh bezpečnostních opatření. Zkušenost je při provádění těchto činností velmi cenná a nesprávná interpretace vstupů může významně znehodnotit závěry celé analýzy.

Jistou nevýhodou vlastního přístupu je možnost „vnitropodnikové slepoty“ ze strany analytiků, která je u ostatních variant eliminována externím pohledem dodavatele nebo konzultační firmy. Na druhou stranu je zde plno výhod plynoucích z využití vlastních odborníků. A pokud je navíc vlastní know-how kombinované s kvalitní metodikou pro provedení analýzy, není pro organizaci lepší volby.

DODAVATELSKÝ PŘÍSTUP	
Výhody	**Nevýhody**
Nezatěžuje organizaci – pouze rozhovory a dotazníky Není nutné mít vlastní odborníky Odpovědnost je na straně dodavatele Není nutné kupovat metodiku či nástroj	Nesrozumitelné výstupy Vysoká cena S posledním expertem odejde i know-how
VLASTNÍ PŘÍSTUP	
Výhody	**Nevýhody**
Všichni rozumí výstupům projektu Nejlevnější (i když se kupuje metodika či nástroj) Znalost interního prostředí Větší ochota respondentů spolupracovat s kolegy než externisty	Velmi zatěžuje organizaci Není jistota správného výsledku (pokud nejsou vlastní odborníci) Neefektivní spotřeba zdrojů (pokud analýzu provádí správce sítě vedle svých každodenních činností) „Vnitropodniková slepota“
PARTNERSKÝ PŘÍSTUP	
Výhody	**Nevýhody**
Všichni rozumí výstupům projektu Není nutné mít vlastní odborníky Odpovědnost je na straně konzultanta Odborné vedení a dohled se strany konzultanta Není nutné kupovat metodiku či nástroj (i když většinou se tak děje) Rozložení jednorázových nákladů do více projektů (např. nákup metodiky či nástroje)	Velmi zatěžuje organizaci (ale efektivně) Relativně vysoká cena Pracovník se v rámci projektu vyškolí a odejde

TAB.2: Souhrnný pohled na výhody a nevýhody přístupů.

ANALÝZA RIZIK

Přístupy k provedení analýzy rizik IS

Partnerský přístup

Tento přístup není využíván příliš často, i když pro většinu organizací by byl velkým přínosem. Jestliže není k dispozici vlastní know-how, nezbývá nic jiného než zvolit dodavatelský nebo partnerský přístup. Ten druhý však v sobě skrývá jednu zásadní výhodu: organizace postupně přechází z dodavatelského přístupu k vlastnímu řešení. Projekty související se zaváděním ISMS včetně detailní analýzy rizik nejsou jako dodání balíkového softwaru nebo vybavení serverovny pořádnou klimatizací. Bezpečnost informací protíná celou organizaci, zasahuje do drtivé většiny činností a procesů, a proto je vhodnější takové projekty provádět více interně než dodavatelsky.

Partnerský přístup je pro dotčené pracovníky prakticky školení o bezpečnosti. Konzultační firmy, které tento přístup nabízejí, přenáší na pracovníky organizace své know-how a tomu by také měla odpovídat cena za projekt. Ta může dosáhnout i 75% dodavatelské varianty a je tak významnou nevýhodou a tím i častým důvodem k odmítnutí ze strany managementu.

U detailní analýzy je celkové zatížení pracovníků společnosti srovnatelné s vlastním přístupem. Na provádění veškerých činností se významně podílí interní pracovníci pod vedením (dohledem) externího konzultanta, který má odpovědnost za projektové a metodické vedení. Spolupráce je velmi intenzivní po celý průběh projektu, ať už při rozhovorech o hodnocení aktiv nebo při zkoumání hrozeb a zranitelností. Nejintenzivnější spolupráce je však při tvorbě výstupů, které jsou ve skutečnosti tvořeny pod hlavičkou dané společnosti nikoli jako dodavatelský materiál. Zprávy včetně doporučení tvoří pracovníci sami a tudíž rozhodují o stylu i formě, aby byly všechny výstupy srozumitelné pro všechny zainteresované včetně managementu. Prakticky to vypadá tak, že externí analytik dodá šablonu dokumentu, kterou pracovníci doplní vlastními závěry formulovanými na základě výsledků analýzy.

Setkal jsem se také s jedním nezanedbatelným rizikem. Během projektu jsme vyškolili dva pracovníky, kteří se pár týdnů po dokončení analýzy rozhodli své čerstvě nabyté zkušenosti zužitkovat u jiné společnosti. Pokud však k tomuto nedojde a společnost dá prostor dalšímu vzdělávání svých lidí v oblasti informační bezpečnosti, může v nich získat velké odborníky a další projekty provádět pod jejich vedením s minimální podporou od konzultační firmy.

Závěr

Všechny tři přístupy jsou správné a vhodné, ale ne pro každého. Může rozhodovat velikost organizace, její obchodní zaměření nebo i počet uživatelů informačního systému. V praxi se však postupně opouští od striktně dodavatelského řešení „na klíč“ a organizace stále více využívají svých pracovníků a vlastního know-how nebo externích konzultantů na jeho získání.

Přístupy nemusí být aplikovány pouze na projekt analýzy rizik, ale i na celkové řešení bezpečnosti informací – zavádění a podporu ISMS. Při rozhodování o správném přístupu je nutné zohlednit zejména očekávané přínosy pro organizaci. Pokud jsou ve vlastních řadách k dispozici odborníci na informační bezpečnost, není nutné volit dodavatelský přístup. V opačném případě závisí na zvolené strategii do budoucna. Přenést odpovědnost na dodavatele a nechat si vše externě zajistit nemusí být špatná volba. Ale organizace by měla zvážit, zda není vhodnější zvolit partnerský přístup a postupně přebírat odpovědnost za bezpečnost svých dat a vychovávat si tak vlastní odborníky.

Jan Mikulecký
jan.mikulecky@rac.cz