

Volby strategie analýzy rizik celé společnosti

1 ZÁKLADNÍ PŘÍSTUP	2
2 NEFORMÁLNÍ PŘÍSTUP	3
3 PODROBNÁ ANALÝZA RIZIK	3
4 KOMBINOVANÝ PŘÍSTUP	4

Volby strategie analýzy rizik celé společnosti

Před zahájením jakékoli činnosti pokud jde o analýzu rizik by organizace měla mít hotovou strategii pro tuto analýzu, a její části (metody, techniky atd.) by měly být dokumentovány v politice bezpečnosti IT celé společnosti. V organizaci by měly být odsouhlaseny prostředky a kritéria pro výběr metody pro analýzu rizik. Strategie analýzy rizik by měla zajistit, že vybraný přístup je pro dané prostředí vhodný a že je soustředěn na snahu dosáhnout bezpečnosti tam, kde je to skutečně potřebné. Možnosti dále uvedené popisují čtyři různé přístupy k analýze rizik. Základním rozdílem mezi těmito přístupy je hloubka analýzy rizik. Protože je obecně příliš nákladné provádět u všech systémů IT podrobnou analýzu rizik, a není rovněž efektivní věnovat vážným rizikům jen okrajovou pozornost, je nutné docílit mezi těmito možnostmi určitou rovnováhu. Ponecháme-li stranou možnost nedělat nic a při akceptování skutečnosti, že systém bude vystaven určitému počtu rizik neznámého rozsahu a síly, existují čtyři základní volby strategie pro analýzu rizik celé společnosti:

- použít stejný základní přístup u všech systémů IT, bez ohledu na rizika, kterým jsou systémy vystaveny, a akceptovat skutečnost, že úroveň bezpečnosti nemusí být vždy odpovídající,
- použít neformální přístup k provedení analýzy rizik a soustředit se na systémy IT, které jsou vnímány jako systémy vystavené nejvyšším rizikům,
- provést podrobnou analýzu rizik s použitím formálního přístupu pro všechny systémy IT, nebo
- provést počáteční analýzu rizik „na hrubé úrovni“ a tím identifikovat systémy IT vystavené vysokým rizikům nebo kritické pro činnost organizace, a poté provést u těchto systémů podrobnou analýzu rizik, a aplikovat na všechny ostatní systémy základní bezpečnost.

Tyto různé možnosti pro řešení bezpečnostních rizik jsou v dalším popsány, a dále je uvedeno doporučení, kterému přístupu by měla být dána přednost. Jestliže se organizace rozhodne, že nebude pokud jde o bezpečnost dělat nic nebo že odloží implementaci ochranných opatření, management by si měl být vědom možných důsledků tohoto rozhodnutí. Pokud není organizace přesvědčena o nekritické povaze svých systémů IT, může tak být ponechána otevřená pro závažné následky. Je-li organizace předmětem narušení bezpečnosti a ukáže-li se, že nebyla přijata žádná preventivní opatření, může porušit zákony nebo předpisy a její pověst může utrpět. Jestliže má organizace s bezpečností IT velmi malé problémy nebo jestliže nevlastní žádné kritické systémy, může to být přijatelná strategie. Organizace je však ponechána v pozici, že neví, zda je situace opravdu dobrá nebo špatná, a to pravděpodobně pro většinu organizací není dobré řešení.

1 Základní přístup

Jako první možnost by organizace mohla aplikovat základní bezpečnost u všech systémů IT výběrem standardních ochranných opatření. V základních dokumentech a praktikách jsou navrženy různé druhy standardních ochranných opatření;

Tento přístup má řadu výhod, mezi něž patří:

- pro analýzu a management rizik je u každé implementace ochranných opatření potřebné pouze minimální množství zdrojů, je tedy snížen čas a úsilí věnované výběru ochranných opatření.
- základní ochranná opatření mohou nabídnout cenově výhodná řešení, protože pro mnoho systémů mohou být bez velkého úsilí přijata totožná nebo podobná základní ochranná opatření v případě, že velké množství systémů organizace pracuje ve společném prostředí, a jsou-li bezpečnostní potřeby srovnatelné.

Nevýhody této volby jsou:

- jestliže je základní úroveň nastavena příliš vysoko, může být bezpečnost pro některé systémy IT příliš nákladná

- je-li základní úroveň příliš nízká, pro některé systémy IT to může představovat nedostatek bezpečnosti, a výsledkem bude vysoký stupeň možného narušení bezpečnosti, a
- při řízení změn, týkajících se bezpečnosti, mohou nastat potíže. Například při aktualizaci systému může být obtížné odhadnout, zda původní základní ochranná opatření jsou ještě postačující.

Mají-li všechny systémy IT organizace pouze nízkou úroveň bezpečnostních požadavků, může to být pokud jde o náklady nejefektivnější strategie. V tomto případě musí být vybrána základní úroveň, odrážející stupeň ochrany požadovaný většinou systémů IT. Většina organizací bude vždy potřebovat splnit určité minimální standardy, aby ochránila citlivá data a byla ve shodě s legislativou a předpisy, např. legislativou na ochranu dat. Avšak tam, kde se systémy organizací liší v citlivosti, rozsahu a komplexnosti činnosti, nebylo by ani logické ani efektivní z hlediska nákladů aplikovat na všechny systémy obecný standard.

2 Neformální přístup

Tato možnost představuje neformální, pragmatickou analýzu rizik. Neformální přístup není založen na strukturovaných metodách, ale využívá znalosti a zkušenosti jednotlivců

Výhodou této volby je:

- nevyžaduje obvykle mnoho zdrojů nebo času. K provedení této neformální analýzy není nutné se naučit nové dodatečné dovednosti a tato analýza je provedena rychleji než podrobná analýza rizik. Existuje však také několik nevýhod:
- bez určitého typu formálního přístupu nebo detailních seznamů kontrol vzrůstá pravděpodobnost opomenutí některých důležitých detailů,
- je obtížné obhájit implementaci ochranných opatření ve vztahu k rizikům odhadnutým tímto způsobem,
- jednotlivci, kteří mají minimum předchozích zkušeností z oblasti analýzy rizik, by měli dostat malý návod, který by jim s tímto úkolem pomohl,
- v minulosti byly některé přístupy založeny na zranitelnostech, tj. byla implementována bezpečnostní ochranná opatření založená na identifikovaných zranitelnostech, aniž by se zvažovalo, zda existovaly některé hrozby, které by pravděpodobně využily tyto zranitelnosti, tj. zda vůbec existovala reálná potřeba ochranných opatření
- může se vyskytnout určitý stupeň subjektivity; specifická předpojatost pracovníka provádějícího revizi může ovlivnit výsledky, a
- v případě, že osoba provádějící neformální analýzu rizik opustí organizaci, mohou vzniknout problémy.

Pro mnoho organizací tato volba s ohledem na výše uvedené nevýhody nepředstavuje efektivní přístup k analýze rizik.

3 Podrobná analýza rizik

Třetí možností je provést u všech systémů organizace podrobnou analýzu rizik. Podrobná analýza rizik zahrnuje hloubkovou identifikaci a ohodnocení aktiv, odhad hrozeb pro tato aktiva a odhad zranitelností. Výsledky těchto aktivit jsou potom použity k odhadu rizik a tedy k identifikaci zdůvodnitelných bezpečnostních ochranných opatření.

Výhody tohoto přístupu jsou:

- je pravděpodobné, že budou pro potřeby každého systému identifikována vhodná ochranná výsledky podrobné analýzy mohou být využity v řízení změn týkajících se bezpečnosti. opatření, a

Nevýhody této volby jsou:

- tato volba vyžaduje k získání výsledků značný objem času, úsilí a expertizu,
- existuje možnost, že bezpečnostní potřeby kritického systému budou řešeny příliš pozdě, protože všechny systémy IT by měly být posuzovány na stejné úrovni podrobností a k dokončení takové analýzy je potřeba značného objemu času.
- Není proto žádoucí používat podrobnou analýzu rizik u všech systémů IT. Jestliže je zvolen tento přístup, existuje několik možných implementací:
- použití standardního přístupu, který splňuje kritéria uvedená v tomto TR
- použití standardního přístupu různými způsoby vhodnými pro danou organizaci; výhodou pro některé organizace by mohlo být použití „technik modelujících rizika“ (popsaných v kapitole - Kombinovaný přístup hodnocení rizik 3).

4 Kombinovaný přístup

Čtvrtou možností je nejprve provést počáteční analýzu rizik na hrubé úrovni pro všechny systémy IT, která se soustřeďuje u každého případu na hodnotu systému IT pro činnost organizace a na vážná rizika, jimž je systém IT vystaven. U systémů IT, které jsou identifikovány jako významné pro činnost organizace a/nebo vystavené vysokým rizikům, by měla být přednostně provedena podrobná analýza rizik. Pro všechny zbývající systémy IT by měl být zvolen základní přístup. Tato volba, která je kombinací nejlepších charakteristik možností popsanych v 8.1 a 8.3 umožňuje minimalizaci času a úsilí věnovaného na identifikaci ochranných opatření, přičemž stále ještě zajišťuje, že jsou vysoká rizika systémů chráněna příslušným způsobem. Mezi další výhody této volby patří:

- začlenění jednoduchého a rychlého přístupu pravděpodobně získá souhlas s přijetím programu analýzy rizik,
- bude možné rychle vytvořit strategický obraz organizačního bezpečnostního programu, který se stane pomocí při plánování,
- zdroje a peníze mohou být použity tam, kde to bude nejvýhodnější, a systémy, které budou pravděpodobně potřebovat nejvíce ochrany, budou řešeny jako první, a
- aktivity sledování budou úspěšnější. Jedinou potenciální nevýhodou je:
- protože počáteční analýzy rizik jsou provedeny na hrubé úrovni a potenciálně jsou méně přesné, nemusí být některé systémy identifikovány jako systémy vyžadující podrobnou analýzu rizik. Tyto systémy by však měly být stále ještě pokryty základní bezpečností. Proto bychom se měli k těmto systémům vrátit v případech, kdy by bylo nutné zkontrolovat, zda-li vyžadují více než jen základní přístup.

Přijetí přístupu analýzy rizik na hrubé úrovni, kombinovaného se základním přístupem, a provedení podrobné analýzy rizik tam, kde je to vhodné, představuje pro většinu organizací nejefektivnější cestu. Tento přístup je doporučen a bude více zkoumán v kapitole (Kombinovaný přístup hodnocení rizik)