ANALÝZA BEZPEČNOSTNÍCH RIZIK V BANKOVNÍM SYSTÉMU

Ing. Jiří Ludvík, CISA
Je konzultantem společnosti Risk Analysis Consultants, kde se zabývá zejména poradenstvím, řízením projektů, a dalšími pracemi v oblasti analýzy a managementu rizik, bezpečnostních projektů a řízení bezpečnosti.
(tento článek byl uveřejněn v časopisu Data Security Management 6/2000)

ÚVOD

K řešení bezpečnosti v podniku či organizaci je možné přistupovat různými způsoby. Jednou z metod, které jsou obecně uznávány za klíčové, je analýza a management rizik.

Analýza rizik je obvykle chápána jako proces určování druhů bezpečnostních rizik, stanovení jejich závažnosti a určení částí systému, v nichž by měla být použita bezpečnostní opatření, který zpravidla zahrnuje

1. **identifikaci aktiv** - vymezení systému a popis komponent z nichž se systém skládá,
2. **stanovení hodnoty aktiv** - určení ceny aktiv či jejich hodnoty v nefinanční podobě,
3. **identifikaci hrozeb a slabin** - určení druhů událostí a akcí, které mohou narušit bezpečnost, určení slabých míst v systému, které mohou umožnit působení hrozeb,
4. **stanovení závažnosti hrozeb a míry zranitelnosti** - určení pravděpodobnosti výskytu hrozby a míry zranitelnosti systému vůči dané hrozbě.

Management rizik je oproti tomu kompletní proces zjištění, kontroly, eliminace a minimalizace nejistých událostí, které mohou ovlivnit prostředky systému, a která kromě analýzy rizik zpravidla zahrnuje
1. výběr bezpečnostních opatření,
2. analýzu nákladů/přínosů,
3. implementaci opatření,
4. testování opatření,
5. a komplexní prověření bezpečnosti.

Kvalitní řešení jakéhokoliv problému v jakékoliv oblasti je vždy postaveno na kvalitní analýze. Totéž platí i pro management rizik v němž je analýza základním prvkem.

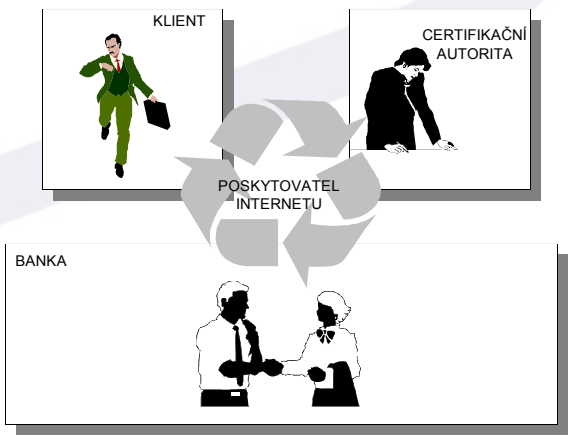
Principy analýzy a managementu rizik jsou v podstatě velmi jednoduché, zřejmě díky tomuto faktu bývá obvykle pomíjena skutečnost, že její praktické provádění v reálném prostředí může být velmi obtížným úkolem.
Článek bude dále ilustrovat postup analýzy rizik na příkladu systému elektronického bankovnictví v hypotetické bance, nazvané iBanka.

VÝCHOZÍ SITUACE

Management iBanky cítí v elektronickém obchodování velký potenciál, chce zlepšit služby poskytované stávajícím klientům a získat nové klienty tím, že jim umožní provádět běžné operace přes Internet. Ve fázi návrhu systému jsme postaveni do role bezpečnostního manažera, který má vyhodnotit rizikovost této služby, její vliv na stávající IT infrastrukturu a definovat základní bezpečnostní požadavky na technické řešení. Postup vedoucí k naplnění těchto požadavků bude vycházet z metodiky pro analýzu a zvládání rizik CRAMM.

POPIS SYSTÉMU

Popis systému je první problém analýzy a zároveň je jedním z nejpodstatnějších. Klíčová otázka v tomto kroku je: "Co vlastně by měl zahrnovat systém?" Vyhneme se zde



Obrázek 1 Organizační členění systému

RAC WHITE PAPERS

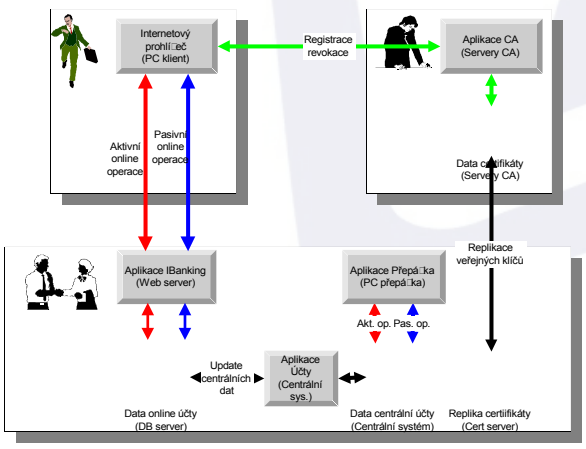
teoretickým diskusím o podstatě informačního systému a použijeme pracovní definici systému, který se skládá ze tří vrstev - vrstvy organizační, představující organizační členění systému, vrstvy logické, představující logické komponenty a toky v systému a vrstvy fyzické, která zahrnuje technické vybavení, propojující médium a fyzické umístění.
Při popisu jednotlivých vrstev je nutné mít na paměti, že vrstvy jsou jen určitou abstrakcí, že ve skutečnosti jsou neoddělitelně propojeny. Vytváření popisu systému není tedy jednoznačně lineární proces, při němž by se postupovalo vrstva po vrstvě. Jde o iterativní proces, při němž je systém popisován v jednom okamžiku vždy ve více vrstvách.

Organizační vrstva

U každé bankovní operace je možné identifikovat klienta a na druhé straně banku. U systému elektronického bankovnictví k těmto stranám ještě přibývá poskytovatel internetových služeb a důvěryhodná třetí strana zajišťující správu elektronických identit klientů - certifikační autorita.

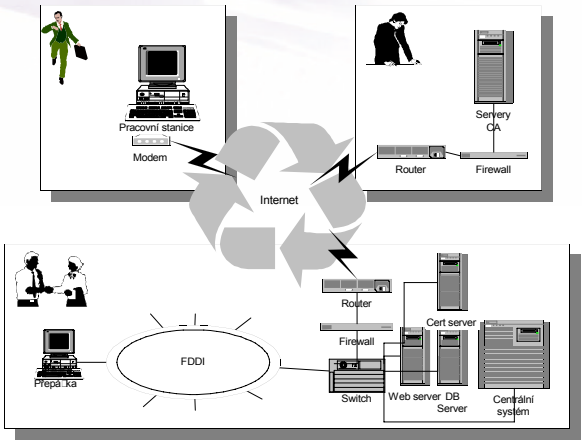
Logická vrstva

Popis na logické úrovni je o něco obtížnější. Protože je systém připojen k dalším systémům, klíčová otázkou zde je, které logické prvky (data a aplikace) a vazby (funkce a datové toky) jsou součástí systému, a které už ne. Po několika předběžných testech s popisem, jsme v případě systému iBanky dospěli k širšímu rozsahu analýzy, která zahrnuje jak systém elektronického bankovnictví, tak některé komponenty dalších systémů.



Obrázek 2 Logické vazby v systému

Systém iBanky je na straně klienta tvořen standardním internetovým prohlížečem, za jehož pomoci se klient banky nejprve registruje u certifikační autority, později může provádět aktivní či pasivní operace se svým účtem a v případě prozrazení soukromého klíče může revokovat (zneplatnit) svůj certifikát.



Obrázek 3 Fyzická vrstva systému

Z hlediska interní architektury systému se tyto operace skládají z několika na sebe navazujících transakcí. Při provádění online operací jsou nejprve data zpracována aplikací s webovým rozhraním pracující s databází online účtů. Data z této databáze jsou dále v pravidelných krátkých časových intervalech využívána k aktualizaci centrálního systému spravujícího všechny klientské účty. Interní funkčnost systému je doplněna replikací veřejných certifikátů z certifikační autority do banky, kde slouží pro autentizaci klientů.

Kromě těchto transakcí spojených se základní funkčností systému byly do analýzy dodatečně zahrnuty klasické přepážkové operace, při nichž aplikace přistupují přímo k centrálnímu systému banky.

Fyzická vrstva

Popis fyzické vrstvy je odvozený od logického a organizačního pohledu na systém. Na straně klienta je fyzická infrastruktura představována pracovní stanicí a modemem, za jehož pomoci se klient připojuje k Internetu. Na straně certifikační autority tvoří infrastrukturu prvky zajišťující připojení k Internetu, kabeláž společně s dalšími komponentami lokální sítě a servery s webovými aplikacemi a adresáři obsahující klientské certifikáty. Jádrem systému je infrastruktura banky, která

je tvořena páteřní sítí napojenou na Internet, na níž jsou napojeny přes aktivní prvky sítě servery zajišťující funkčnost systému elektronického bankovnictví a mainframu centrálního systému banky.

STANOVENÍ HODNOTY AKTIV

Po popisu systému je dalším krokem v analýze stanovení hodnoty jednotlivých prvků. Protože je v našem případě zřejmé, že největší hodnotu v systému mají data, která představují elektronickou podobu finančních prostředků, bude v této fázi věnována pozornost především hodnotě dat.

Určení hodnoty dat je dalším klíčovým momentem v analýze. V prvním přiblížení vypadá stanovení hodnoty dat jako jednoduchá záležitost, bližší pohled ale odhaluje složitosti.

Bezpečnost informačních systémů se zabývá ochranou před událostmi, které mohou negativně ovlivnit systém. Z tohoto pohledu je tedy hodnota aktiv vyjádřena závažností následků potenciálních událostí, které mohou způsobovat narušení integrity, dostupnosti, důvěrnosti a případně odpovědnosti za činnosti v systému.

Dalším problémem, který je nutno v tomto kroku vyřešit, je charakter následků. Ačkoliv v případě iBanky představuje většina dat v systému finanční prostředky, není možné hodnocení provádět jen z finančního hlediska. Například úmyslnou modifikací platebního příkazu samozřejmě mohou vzniknout finanční ztráty, ale třeba prozrazením údajů o klientovi dojde k porušení bankovního tajemství a dlouhodobá nedostupnost systému pro zákazníky povede k poškození dobrého jména banky. Ve skutečnosti může mít narušení jednoho datového aktiva najednou různě závažné následky v několika výše zmiňovaných oblastech.

Aktivum	Dostupnost	Integrita	Důvěrnost	Odpovědnost
Data online účty	4	5	3	5
Data certifikáty	5	5	5	5
Data centrální účty	6	10	5	5
Replika certifikáty (veřejné)	5	5	0	5

Tabulka 1 Hodnota dat

Tabulka 1 shrnuje hodnotu datových aktiv v příkladě iBanky.

Pro hodnocení byla využita škála v rozsahu 1-10, v níž hodnota 1 představuje zanedbatelné následky a hodnota 10 znamená životní potíže pro celou banku.

Obvyklým problémem této fáze je také nejednotnost pohledu na hodnotu dat. Aby výsledná hodnota dat byla určena co možná nejobjektivněji, procesu stanovování hodnoty by se měla účastnit řada odpovědných pracovníků banky. Každý z nich přitom zpravidla vidí hodnotu dat z jiného úhlu pohledu. Jinak bude vidět hodnotu

Část systému	Interní		Externí	
Hrozby	Logická vrstva	Fyzická vrstva	Logická vrstva	Fyzická vrstva
HACKER Falšování identity Útok na komunikace Zneužití aplikace	-	-	X	-
ZLOVOLNÝ PRACOVNÍK Falšování identity Útok na komunikace Zneužití aplikace	X	X	-	-
TECHNICKÉ ZÁVADY Selhání základního SW Selhání aplikačního SW Nedostupnost síťových služeb Technická závada HW	X	X	X	X
SPRÁVCE Chyba správy SW Chyba údržby HW	X	X	-	-

Tabulka 2 Oblasti výskytu hrozeb a zranitelností

transakce vedoucí retailového bankovnictví, jinak právník, jinak pracovníci public relations. Aby hodnota dat byla objektivní, mělo by dojít ke společnému konsensu všech odpovědných pracovníků. Ten zpravidla závisí na míře komunikace, kterou se podaří mezi odpovědnými pracovníky dosáhnout.

Po ukončení hodnocení aktiv může analytik odpovědět na otázky typu: "Které části informačního systému jsou pro banku nejvíce cenné? Z jakého důvodu tomu tak je? Jaký by mohlo mít poškození systému nebo prozrazení dat v něm zpracovávaných vliv na podnikatelské činnosti banky? " a další.

IDENTIFIKACE HROZEB

Hrozba je nechtěná událost, která může potenciálně způsobit škodu organizaci. V různých zdrojích (např. (RAC99), (ISO98)) bývají uváděny typické kategorie hrozeb, které mohou působit na informační systém, a mezi něž se zpravidla počítají vlivy prostředí, technické závady, lidské chyby a úmyslné činy.

Počet možných potenciálních hrozeb, v podstatě nekonečný, se na úrovni kategorií zmenší na poměrně rozsáhlý seznam, a v této fázi analýzy je třeba určit, které hrozby budou brány v potaz. Konkrétní výběr oblastí hrozeb vychází z cílů analýzy a z analýzy zdroje hrozeb, přičemž výběr by měl dát odpověď na otázku:"Kdo, nebo co může potenciálně poškodit systém nebo data?"

Protože v analýze systému iBanky je cílem stanovit vliv nových služeb na rizikovost IT infrastruktury, výběr hrozeb je zaměřen na hrozby spjaté s informačními technologiemi. V takto definovaných hranicích jsme (my respektive bezpečnostní manažer) po expertní analýze identifikovali jako hlavní zdroje hrozeb hackera, zlovolného pracovníka, správce systému a technické závady.

Hrozby, které mohou tyto zdroje hrozeb způsobit a jejich působnost na systém jsou popsány v tabulce 2.

URČENÍ ZÁVAŽNOSTI HROZEB A ZRANITELNOSTÍ

Závažnost definovaných hrozeb a míra zranitelnosti vůči těmto hrozbám představují poslední veličiny nutné k zjištění celkového profilu a míry rizik. Klíčovou otázkou v tomto kroku je: "Jaká je pravděpodobnost výskytu hrozeb, které mohou působit na systém a do jaké míry je systém vůči těmto hrozbám zranitelný?"

V analýze systému iBanky bylo provedeno hodnocení hrozeb a zranitelností

Část systému	Interní		Externí	
Hrozba Zranitelnost	Logická vrstva	Fyzická vrstva	Logická vrstva	Fyzická vrstva
HACKER Falšování identity Útok na komunikace Zneužití aplikace	-	-	Malá Střední	-
ZLOVOLNÝ PRACOVNÍK Falšování identity Útok na komunikace Zneužití aplikace	Velmi malá Střední	Velmi malá Malá	-	-
TECHNICKÉ ZÁVADY Selhání základního SW Selhání aplikačního SW Nedostupnost síťových služeb Technická závada HW	Velmi malá Malá	Velmi malá Malá	Střední Malá	Velmi malá Střední
SPRÁVCE Chyba správy SW Chyba údržby HW	Velmi malá Malá	Velmi malá Malá	-	-

Tabulka 3 Ohodnocení hrozeb a zranitelností

Hrozba	Dostupnost	Integrita	Důvěrnost	Odpovědnost
HACKER	3	4	4	3
ZLOVOLNÝ PRACOVNÍK	3	4	3	3
TECHNICKÉ ZÁVADY	3	2	2	0
SPRÁVCE	2	2	3	0

Tabulka 4 Rizikovost hrozeb v systému

dotazníkovým šetřením s pracovníky odpovědnými za provoz a vývoj systému. Následující tabulka obsahuje souhrn úrovně hrozeb (ve škále velmi malá, malá, střední, vysoká, velmi vysoká) a zranitelností (ve škále malá, střední vysoká).

Kromě základní představy o závažnosti hrozeb a zranitelností můžeme po ukončení tohoto kroku získané informace využít pro odpověď na otázky typu: "Jsou závažnější vnější (neovlivnitelné) faktory, nebo vnitřní (ovlivnitelné) faktory?" a další.

STANOVENÍ RIZIKA

Na základě popisu systému, hodnocení aktiv a hodnocení hrozeb a zranitelností je za pomoci matematického aparátu obsaženého v metodice na závěr analýzy určena výsledná matice míry a rozložení rizik v systému.

Riziko v sobě zahrnuje hodnoty všech prvků, které byly během jednotlivých kroků hodnoceny a tedy obsahuje pohled na

jádro podnikání banky - hodnotu aktiv z hlediska podnikatelských cílů,
vnější okolí banky - profil a závažnost hrozeb působících na systém,
vnitřní mechanismy banky - zranitelnosti systému.

Aktivum	Dostupnost	Integrita	Důvěrnost	Odpovědnost
Transakce				
SKU1 Aktivní online operace	2	4	3	3
SKU2 Pasivní online operace	2	3	2	3
SKU3 Registrace	3	4	4	0
SKU4 Update centrálního systému	3	4	3	3
SKU5 Aktivní operace přepážka	2	4	3	2
SKU6 Pasivní operace přepážka	2	3	3	2
SKU7 Replikace veřejných klíčů	3	4	0	3
Aplikace				
A1 Aplikace účty	2	1	1	0
A2 Aplikace iBanking	1	1	1	0
A3 Aplikace Cert - CA	2	1	1	0
A4 Aplikace Přepážka	2	1	1	0
Služby				
I1 Internet	3	0	2	0
Technické vybavení				
N2 Router banka	2	1	3	0
N3 Firewall banka	3	1	2	0
N5 Router CA	3	1	3	0
N6 Firewall CA	3	1	3	0
S1 Centrální systém banka	2	2	2	0
S2 Web server banka	1	2	2	0
S3 DB Server banka	2	2	3	0
S5 Server Cert – CA	2	2	3	0
N1 Switch banka	2	1	3	0

Tabulka 5 Rizikovost prvků systému

Pokud proces analýzy rizik proběhl korektně, je možné tvrdit, že riziko určitým způsobem vyjadřuje vztah mezi informačním systémem, jeho bezpečností a podnikatelskými cíli banky.

Na základě zjištěných informací o rizikovosti jednotlivých oblastí, je možné po ukončení této fáze provádět interpretaci dat, nejlépe kladením vhodných otázek a hledáním odpovědi na ně. Důležité také může být nenechat se zaskočit velkým množstvím výstupních dat, která sama o sobě nemají příliš vysokou vypovídací hodnotu.

V případě iBanky můžeme například na 10 stranách výstupních dat, které jsou shrnuty do tabulek 4 a 5, nalézt odpověď na otázky: "Která oblast bezpečnosti (důvěrnost, integrita, důvěrnost, odpovědnost) je nejvíce

ohrožena? Která hrozba je v systému nejzávažnější?"
Odpověď na otázku "Které funkce a komponenty systému jsou nejrizikovější?" potom může znít následovně.

Největším rizikem v systému iBanky je modifikace přenášených a zpracovávaných dat. Na úrovni fyzické infrastruktury je riziko modifikace velmi nízké; více rizikové (na nízké a střední úrovni) jsou logické transakce představující operace prováděné klientem, obsluhou systému nebo automaticky systémem samým.

Druhou nejzávažnější oblastí bezpečnosti v systému elektronického bankovnictví je riziko prozrazení dat. U většiny logických i fyzických komponent systému je toto riziko velmi nízké. Výjimku ale tvoří aktivní prvky sítě, u nichž je riziko nízké až střední, což asi odráží relativní snadnost chybné konfigurace těchto prvků. Na logické úrovni je zvýšená míra rizika zejména u transakcí v nichž jsou přenášeny osobní údaje klienta (registrace, revokace, replikace údajů), tato míra se ale stále pohybuje na nízké až střední úrovni.

Riziko nedostatečné odpovědnosti za činnosti provedené v systému elektronického bankovnictví se projevuje ve velmi dobře ohraničené oblasti transakcí, představujících přenos finančních prostředků. Rizikovost těchto transakcí se pohybuje na nízké až střední úrovni.

Riziko nedostupnosti služeb či dat je v interních systémech iBanky a certifikační autority velmi nízké, malou až střední míru rizika představuje nedostupnost služeb Internetu a nefunkčnost rozhraní interních systémů a veřejné sítě.

Po vyhodnocení rizika si ale také můžeme v roli bezpečnostní manažera iBanky odpovídat na specifičtější otázky, jako například: "Jsou rizikovější přepážkové operace nebo operace prováděné přes Internet? Je rozdíl v rizikovosti aktivních a pasivních operací? Jak velké riziko představuje outsourcing funkcí certifikační autority?" a další.

TECHNICKÉ POŽADAVKY NA SYSTÉM IBANKY

Následující seznam shrnuje oblasti, v nichž bezpečnostní tým iBanky detailněji specifikuje technické požadavky na bezpečnost systému elektronického bankovnictví.

Identifikace a autentizace transakcí
Bezpečné uložení certifikátů
Ochrana certifikátů heslem
Přihlašovací dialog
Bezpečná distribuce certifikátů

Kontrola přístupu k systému
Kontrola přístupu v aplikacích
Kontrola přístupu v operačním systému

Evidence událostí
Evidence událostí
Synchronizace času
Bezpečnost auditovacího subsystému
Kapacita prostředků pro vedení záznamů

Audit
Nástroje pro audit
Nástroje pro detekci průniku
Bezpečné mazání objektů
Integrita programového vybavení

Kontrola přístupu v síti
Autentizace aplikací
Oddělení segmentů sítí
Oddělení firewally

Bezpečnost off-line systémů
Potvrzování předání
Autentizace původu
Kontrola doručení

Integrita a důvěrnost přenášených dat

Dostupnost síťových služeb

RAC WHITE PAPERS

Zásady úspěšné analýzy

1) Při jednáních, které jsou součástí analýzy, buďte diplomatičtí
2) Pokuste se co nejvíce porozumět prostředí v němž se systém nachází
3) Dívejte se na systém jako komplex zahrnující prostory, výpočetní techniku, programové vybavení, data a procesy
4) Snažte se o zachování jednoduchosti popisu
5) Neočekávejte, že jakýkoliv nástroj na podporu analýzy rizik vykoná práci za vás, nástroje pouze pomáhají
6) Zajistěte si, že zadavatel souhlasí se vstupy, které jste získali
7) Ve složitých situacích nezapomeňte používat zdravý selský rozum

NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

Na analýzu rizik navazuje navržení bezpečnostních opatření, která mají eliminovat či snižovat riziko. Tato opatření zpravidla představují technické požadavky na systém, organizačními požadavky na zajištění systému, nebo obecněji na procesy v oblasti informatiky.

Pokud (jako v případě iBanky) používáme podpůrný nástroj na analýzu rizik, je naším úkolem v této fázi přejít od všech možných opatření k opatřením doporučeným (viz rámeček Technické požadavky na systém iBanky). Prvním krokem, kterým se přibližujeme tomuto cíli, je zjištění existujících opatření v systému a v procesech jejichž prostřednictvím je systém řízen.

To ve fázi návrhu systému elektronického bankovnictví znamená posoudit z hlediska bezpečnosti funkční návrh systému, existující technickou infrastrukturu, která systém bude podporovat a v neposlední řadě organizační zajištění provozu.

Opatření obsažená v bezpečnostních standardech či podpůrném nástroji nemohou být specifikovány až na úroveň konkrétních produktů; na to je současný vývoj informačních technologií a jejich rozmanitost příliš velká Databáze metodiky CRAMM, které je asi typickým příkladem seznamu opatření, například obsahuje největší počet opatření na úrovni bezpečnostních zásad, pravidel a bezpečnostních funkcí. Důležitým faktorem při návrhu opatření je potom schopnost interpretace takto určených opatření do konkrétního technologického prostředí.

Protože jde o úkol specificky technického charakteru, svěřuje jej v iBance bezpečnostní manažer své skupině technických specialistů. Sám se zaměřuje na opatření organizační, která jsou mnohem citlivější politicky; jejich dopad na fungování banky je větší a tím pádem i jejich realizace bývá obvykle obtížnější

Pragmatický postup radí kombinovat nebo alespoň porovnávat opatření zjištěná na základě analýzy rizik s profily opatření představující obecně uznávané nejlepší řešení. V případě iBanky mohou být těmito obecně uznávanými nejlepšími způsoby řešení například kombinace standardů (BSI99) pro řízení bezpečnosti informací, třídy F-C2 podle (EU92) pro technickou bezpečnost a využívání certifikátů pro zajištění identifikace, autentizace a nepopiratelnosti odpovědnosti (HUN99). Jiným adekvátním přístupem pak může být využití specifického bankovního standardu (BA99).

Dalším krokem, který logicky následuje po návrhu opatření, je jejich implementace. Konkrétní podoba implementace z velké části závisí na takových běžných věcech, jako je množství finančních prostředků, dostupné lidské zdroje, časové možnosti a podobně. Ale to už je jiná kapitola, která není jen o bezpečnosti.

UPOZORNĚNÍ

Části článku popisující proces a problémy analýzy odrážejí realitu provádění analýzy rizik v bankovní instituci. Avšak hodnoty vstupních údajů popisované v příkladu iBanky je nutno považovat za fiktivní a není možné je zobecňovat.

SOUHRN

Článek se zabývá praktickými aspekty analýzy rizik. Ilustruje klasický postup analýzy - identifikace a určování hodnoty aktiv, identifikace a hodnocení hrozeb, zranitelností a návrh opatření - z pohledu bezpečnostního manažera fiktivní banky postaveného před problém určit bezpečnostní požadavky na budovaný systém elektronického bankovnictví. Ukazuje, že při provádění analýzy rizik je samotný metodický aparát sice nutnou, ale nikoliv postačující podmínkou. Dalšími faktory klíčovými pro úspěch analýzy je zejména komplexní popis všech aspektů systému, interpretace výsledků a skutečné zapojení managementu a pracovníků do klíčových kroků analýzy.

Váš úspěch s naším přispěním.

RAC WHITE PAPERS

Risk Analysis Consultants s. r. o.
Národní 9, 110 00 Praha 1, CZ
tel: +420 2 2207 5340
fax: +420 2 2422 8273
rac@rac.cz, www.rac.cz