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

INFORMATION SECURITY EXPERTS

WHITE PAPER

(Data security Management 2/2002): Článek podává úvodní informaci o místě a úloze forenzní analýzy informačních systémů, jako jednoho z nástrojů reakce na bezpečnostní incidenty. Forenzní analýza je zde uvedena jako nezbytný nástroj pro důsledné a ve své podstatě i ekonomicky efektivní řešení bezpečnostních incidentů a jako prostředek k možnému zmírnění jejich celkových ekonomických dopadů.

Místo a úloha forenzní analýzy IS

Ing. Marián Svetlík
Od ukončení vysokoškolského studia výpočetní techniky pracoval v různých oblastech výzkumu, vývoje a aplikací IT. Od roku 1992 se zabýval kriminalistickou a forenzní analýzou počítačů a sítí. Do roku 2000 vedl pracoviště počítačové expertizy Kriminalistického ústavu Praha. V současné době je vedoucím konzultantem společnosti Risk Analysis Consultants, spol. s r. o.

Všechno začalo jako obyčejně dobrým úmyslem. Na stole vedoucího servisu IT zazvonil telefon: *"Jaroušku, prosím, mně zase vypadl počítač... Přijdete si mi na to podívat? Mám tady frontu u přepážky... Děkuji moc!"* Pan Jaroslav byl za chvilku u přepážek. *"Vy jste tak šikovný!"*, přidávala si paní Marie. *"Než to spravíte, já si zajdu zapsat ty papíry do sešitu – aspoň mi tu přepážku chvilku pohlídáte"*. Když se vrátila, Jaroslav už neměl co na práci. *"Opravdu šikulka"* opáčila ještě jednou Marie. *"A nemohl byste pro nás ještě něco udělat? To psaní každého papíru do sešitu nás tu strašně otravuje a musíme odbíhat od přepážek, co určitě není moc správné ani bezpečné. Když už máme ty počítače, mělo by to jít nějak inteligentněji, ne? Od čeho je tu máme? A vy si s tím určitě lehce poradíte!"* dodala Marie s úsměvem. A měla pravdu. Za necelý týden Jaroslav ke spokojenosti dam na přepážkách instaloval na každou stanici malou aplikaci, kde mohla každá z nich zapisovat do databáze údaje o prodaných cenných papírech bez toho, že by odcházela od okénka a nechávala jej bez dozoru napospas dlouhým frontám zákazníků. Opět se potvrdilo, že výpočetní technika je schopna pomoct i v běžných každodenních problémech jedné obyčejné krajské pobočky jedné obyčejné banky.

Několik měsíců všechno fungovalo jak má být, na přepážkách panovala spokojenost. Až do chvíle, kdy denní uzávěrka odhalila v prodeji cenných papírů schodek přes 8 milionů korun. Nastal obvyklý proces dohledávání, přepočítávání, šetření, ale i přes několikadenní námahu se nic kloudného nenašlo. Muselo se jít s pravdou ven a ohlásit to vyššímu vedení. To zahájilo interní šetření a kolotoč se rozjel naplno. Dobrá pohoda na přepážkách skončila, začalo vzájemné podezřívání a práce přestala jít od ruky. Navíc lidí před dovolenými přibývalo a k tomu ještě to šetření! Ale ani několik týdnů práce kontrolních orgánů až z centrály nepřineslo konkrétní výsledky. Jediné co se dalo usoudit bylo, že někdo zmanipuloval data v počítačové evidenci prodaných cenných papírů tak, že peníze byly vydány na papír, který v době prověrky v evidenci jednoznačně byl, ale v době uzávěrky již ne. Pak padlo rozhodnutí požádat o forenzní audit počítače, na kterém byla evidence vedená, aby se vyjasnilo, jak a kdy k zjištěné manipulaci došlo a aby se dalo dovodit, kdo ji mohl provést.

Většinou je takovéto řešení bohužel posledním, které může zjistit skutečný průběh událostí. K tomu, aby mohlo být úspěšné, je však potřebné splnit několik málo předpokladů. Jak tento konkrétní případ skutečně skončil uvádět nebudu, jenom vás mohu uspokojit, že instituce, ze které pochází, už neexistuje.

Uvedený příběh je z reálného života, jen Jaroslav a Marie jsou jména smyšlená. Dalo by se na něm poukázat na mnohá narušení bezpečnostních pravidel, jak nám je doporučují normy. Stačilo by se podívat do ISO/IEC 17799:2000 a viděli bychom, že nebyla dodržena pravidla pro přijímaní požadavků na vylepšení IS, bezpečnostní pravidla pro vývoj, ověření a nasazení nových IS, doporučení pro monitorování bezpečnosti provozu, pravidla pro řízení přístupu atd. Ale to, co chci na tomto příkladu přiblížit, je právě problematika forenzního auditu, který byl tím posledním, co mohlo případ objasnit. O co se vlastně jedná?

V020611

Co je forenzní audit (nebo analýza)?

Audit je podle slovníku cizích slov kontrola účtů nebo účetnictví. Jeho cílem je, zjednodušeně řečeno, zjistit, zda finanční operace jsou v souladu se zákony a předpisy platnými pro jejich provádění. V poslední době se ale stal v našich sdělovacích prostředcích velice populární pojem **forenzní audit** - zejména v souvislosti s podezřením na finanční „nesrovnalosti“ v některých organizacích nebo politických stranách. V čem je tedy rozdíl obyčejného a forenzního auditu?

Slovo **forenzní** znamená podle stejného slovníku soudní. Nejběžnější uplatnění tohoto slova lze nalézt v pojmu **forenzní vědy**, což jsou vědy, zabývající se metodami a postupy zkoumání jevů a skutečností s cílem podat nezávislé, hodnověrné a kdykoliv opětovně prokazatelné **důkazy** pro soudní účely (soudní lékařství, soudní psychologie apod.). V naší právní praxi se v trestním řízení na vyžádání orgánů činných v tomto řízení (soudy, státní zastupitelství, policejní orgány) a za použití výsledků forenzních věd provádí **znalecké zkoumání** a podávají **znalecké posudky**. Při splnění stejných požadavků na provedení se znalecké posudky vyžadují i v dalších občanskoprávních a majetkových procesech. Důležité ale na tom je, že tyto posudky jsou u nás podávány subjekty (organizacemi i jednotlivci), které mají speciální znalecké oprávnění a jsou zapsány do seznamu znalců a tlumočníků vedených u krajských soudů (zdůrazňuji, že v naší praxi se nepoužívá přívlastek forenzní).

Forenzní audit je tedy audit, který je prováděn za pomocí metod a prostředků, které vycházejí z poznatků forenzních věd a je zaměřen zejména na získávání objektivních a prokazatelných důkazů.

V oblasti IT lze také na mnoha místech výhodně využít výsledky **forenzní počítačové vědy**. Přimlouvám se ovšem za použití pojmu **forenzní analýza** místo forenzní audit, protože slovo audit vyjadřuje spíše „zjištění souladu“ (vhodné právě pro účetnictví). To se v případě IT prakticky stává zřídka a uplatnění forenzních metod lze spíše hledat na místech, kde se provádí analýza jevů a procesů spojených zejména s bezpečnostními **incidenty** – tj. tam, kde se požaduje hodnověrné, nezávislé a prokazatelné zjištění toho, co se v IS stalo.

Prakticky všechny názory na to, jak postupovat v případech řešení škod způsobených bezpečnostními inci-

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

INFORMATION SECURITY EXPERTS

RAC®

WHITE PAPER

V020611

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

INFORMATION SECURITY EXPERTS

WHITE PAPER

denty zjednodušují situaci na konstatování, že tato problematika je záležitostí managementu organizace. Jistě, v případech jednoduchých, modelových (DSM 6/99) nebo když škody jsou minimální lze s tímto postupem a doporučením souhlasit. Bezpečnostním incidentem však vznikají organizaci škody i značného rozsahu, může to vyžadovat relativně vysoké finanční, materiální nebo lidské zdroje, ztrátu konkurenceschopnosti nebo i řešení občansko- nebo trestně-právních otázek. V tomto okamžiku management potřebuje k tomu, aby rozhodl o způsobu dalšího postupu jednoznačné argumenty – důkazy, a ty mu poskytne právě forenzní analýza.

Dnes, kdy hackeři pronikají do cílového systému přes několik prostředníků, si dokonce nemůžeme být jisti ani tím, zda určitá podezřelá činnost, která mohla být na našem systému detekována (a nemusela mít žádný přímý dopad na náš informační systém), nezpůsobí vážné škody v jiném systému úplně jiné organizaci (DDoS útoky jsou toho názorným příkladem). Bez podrobného došetření každého detailu, každé podezřelé aktivity, se nám bude těžko dokazovat, že útok na poškozenou organizaci nebyl organizován právě z našeho systému.

Přínosy mohou být nezanedbatelné

Provedení forenzní analýzy IS tedy může dát organizaci užitečný nástroj, jehož účelem je zejména objektivně zjistit a zadokumentovat příčiny, průběh a následky bezpečnostního incidentu. Taková objektivní a nezávislá zjištění mohou:

- dát všem zúčastněným stranám (zaměstnancům, managementu a případně třetí straně) objektivní informaci o stavu věci;

- podat managementu organizace důkazy, které mu mohou napomoct při rozhodování o případném vymáhání způsobené škody;

- poskytnout managementu jistotu o správnosti, opodstatněnosti a legálnosti důležitých rozhodnutí ve věcech řešení škod způsobených bezpečnostním incidentem;

- chránit organizaci nebo její zaměstnance vůči podezření nebo obvinění ze strany poškozených subjektů (zaměstnanec, obchodní partner, konkurent, stát).

Význam forenzní analýzy je zdůrazněn i v současných normativních dokumentech, kdy např. ISO/IEC 17799:2000 otázkám sou-

V020611

visejícím s problematikou forenzní analýzy věnuje prakticky celou kapitolu. Tam lze nalézt i podrobnější podmínky pro úspěšné provedení forenzní analýzy.

Klíčová role informací ve společnosti (a také prostředků pro jejích zpracování) se odráží i v požadavcích na dodržování platných právních norem, zajištění podmínek stanovených zákony, prokazování jejich bezpečnostní úrovně apod. Požadavky státu, ale zejména na zvyšování samostatnosti a vlastní ochrana zájmů organizace jsou argumenty vedoucí k tomu, že forenzní analýza informačních systémů díky své nezávislosti, objektivnosti a prokazatelnosti se postupně posouvá ze soudních síní a z policejních vyšetřování do každodenního procesu zajištění bezpečnosti informačních systémů.

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

INFORMATION SECURITY EXPERTS

RAC®

WHITE PAPER

V020611