RAC®
RISK ANALYSIS CONSULTANTS

MÍSTO A ÚLOHA

FORENZNÍ ANALÝZY IS

Úvod

Průšvihy, na řešení kterých se podílel nějakým způsobem forenzní audit, se stávají nejenom v politických stranách a nejenom v oblasti hospodaření. V každodenním životě se setkáváme s problémy, které mohou mít dalekosáhlé následky na chod organizace. Informační technologie a informační systémy (IT/IS) jsou v současnosti jedním z nesmírně důležitých faktorů ovlivňujícím prosperitu a úspěšnost. V souvislosti s IS se můžeme setkat s pojmem forenzní analýza IS. Kde by vlastně mělo být její místo a čím se zabývá? Pochopení základního okruhu obecnějších pojmů kolem místa a obsahu forenzní analýzy IS je vlastně součástí chápání celkového sytému bezpečnosti IS.

Vstupujeme do informační společnosti

V posledních letech je naše společnost doslova zaplavena špičkovými technologiemi v oblasti zpracování informací. Přední světoví počítačoví odborníci hodnotí tuto skutečnost jako velkou výhodu pro státy střední a východní Evropy. Při budování informačních systémů si totiž můžeme vybírat jen ty nejvhodnější technologie a nemusíme brát ohledy na žádné předcházející systémy. Budujeme totiž prakticky všechno znovu, na zelené louce.

Nesporné výhody, které se nám díky uvedené skutečnosti nabízí, mají i svá rizika. Je to nepřipravenost naší společnosti k velmi rychlému nasazení informačních technologií do praktického života. Přeskakujeme ve vývoji celá desetiletí postupného prosazovaní určitého způsobu myšlení a určitého způsobu práce. Tento skok nám přináší nedostatky zejména v efektivním a systémovém využití toho mála kvalifikovaných odborníků, které máme. Přetrvává starý způsob organizace a řízení, který nepostihuje změněnou situaci. Projevuje se nekritické hodnocení všeho, co k nám přichází, a zapomíná se na zohledňování komerčního hlediska všech dodávek informačních technologií.

Za desetiletí vývoje jsme se naučili rozpoznávat padělky peněz a dokladů, naučili jsme se je proti padělání chránit. Jsou vyvinuty dostatečně efektivní metody jejich expertiz. V materializované podobě si informace dokážeme relativně dobře ochránit. Peníze chráníme v speciálních trezorech, umíme vyrobit pevné mříže, postavit všude kamery a detektory. Jak je to však s informacemi v elektronické podobě? Jsou dostatečně chráněné? Dokážeme tuto ochranu posoudit? Má občan nějakou možnost ”laické” kontroly nebo musí důvěřovat tomu, co mu počítač vypíše na tiskopis?

Počítače zasahují dnes a denně do života lidí, prakticky všechny oblasti jsou ovlivňovány informačním boomem. Stále větší objemy informací, velké rychlosti jejich zpracování a intenzivní rozšiřování počítačových sítí klade zvyšující se nároky na programové a technické zajištění. Počítače a systémy jsou stále složitější. Přehnaná důvěra v jejich bezpečnost a spolehlivost vytváří množství příležitostí pro jejich zneužití.

RAC®
RISK ANALYSIS CONSULTANTS

Prevence škod

Určitě lze říct, že dobře navržený IS je takový, který splňuje všechny funkční požadavky na něj kladené. Jelikož IS je určen primárně pro zpracování informací, musí tedy zpracovávat informace způsobem, kterým je od něj požadováno, z definovaných vstupních informací musí dávat požadované výstupy.

Protože převod veškerých důležitých informací do elektronické podoby se v současnosti stává objektivní nutností, stejnou nutností se stává i postupné uvědomování si možných a zejména reálných rizik s tímto procesem souvisejících (důkazem čehož je mimochodem i toto vydání Security Magazínu).

Co všechno obnáší dobře a bezpečně navržený IS však není možné jednoduše popsat a ani to není cílem tohoto článku. Dobře navržený IS, nezávisle od toho, v jaké formě a jaké informace zpracovává, je komplexem technických, programových, organizačních, personálních a mnohých dalších faktorů. Všechny tyto faktory je potřebné vzít v úvahu, když chceme navrhnout a hlavně zrealizovat skutečně kvalitní, funkční a bezpečný IS.

Reálný život však není stav, ale proces. Je to neustále se vyvíjející souhrn vnitřních a vnějších faktorů, přicházejí neustále nové technologie, na trhu se objevuje stále nová konkurence, mění se přístupy a formy zpracování informací, mění se spolehlivost jednotlivých prvků IS, mění se lidé, roste odborná úroveň hackerů, … Mění se tedy i hrozby, které mohou ovlivňovat bezpečnost mnohdy životně důležitých firemních informací. Nelze se totiž prakticky vyvarovat situaci, kdy některá z hrozeb přivede systém jako celek, nebo některou jeho část do kritické situace. Lze přirozeně minimalizovat tyto možnosti, ale s určitou mírou rizika je nutné počítat.

Za této situace je potřebné si uvědomit, že škody způsobené různými selháními IS neustále rostou. Z jedné strany jsou sice IS budovány na neustále se zkvalitňující se technologické a programové základně, zvyšuje se spolehlivost jednotlivých jejich prvků, z druhé strany dynamicky roste hodnota informací v IS zpracovávaných a roste i kvalifikace lidí, kteří mají na nich neoprávněný zájem a které mohou mít zásadní důležitost pro jejich vlastníka. Tím vlastně roste i hodnota škod, která v případě (byť méně častého) selhání některého prvku IS vznikne.

Komplexní pojetí zajištění bezpečnosti informací v organizaci by mělo nalézt odraz v její celkové bezpečnostní politice. Ve své podstatě je to souhrn nemálo nákladných různorodých opatření. Rozsah a důkladnost aplikace jednotlivých doporučení závisí od hodnoty chráněných aktiv a tím i nezbytnosti jejich ochrany a od finančních možností organizace.

Přirozeně vzniká otázka, zda se vyplatí do projektu a realizace komplexní bezpečnostní politiky investovat, když jsou to vlastně investice, kterými lze ve svém důsledku zaručit pouze minimalizaci možných škod vniklých porušením, zcizením nebo zneužitím citlivých informací. Odpověď na takto položenou otázku je na čtenáři.

Návratnost investic do prevence bezpečnostních incidentů má ve své podstatě dlouhodobý charakter, avšak v systému bezpečnostních opatření je místo, které umožňuje vytvořit předpoklady pro ekonomickou návratnost i konkrétní škody vzniklé konkrétním incidentem.

RISK ANALYSIS CONSULTANTS

Lze získat ztracené peníze?

Metody ošetření škod vzniklých v souvislosti s výkonem povolání z jiných oblastí fungování organizace máme dobře propracované. Celkem přehledné mechanizmy jsou uplatňovány např. pro řešení dopravních nehod, zanedbání výrobních postupů, bezpečnosti práce apod. Existuje systém pravidelných školení řidičů, proškolování BOZP, servisní a technické prohlídky, pojištění, … Praktické zkušenosti však ukazují, že na kritické události související s činností resp. výpadky IS se tyto zaběhnuté postupy ne příliš často a ne příliš lehce uplatňují.

Jednak je fakt, že provoz IS/IT patří k velice speciálním a specifickým oblastem činnosti organizace, jednak je to oblast, která se intenzivně a masově nasazuje prakticky až posledních deset let. Pro vytvoření obecně platných norem a postupů (tak jako existují v jiných oblastech činnosti organizace) je to pro nás ještě stála poměrně krátká doba. Řešení však lze nalézt opět v dobře stanovených zásadách bezpečnostní politiky organizace.

Mezi množstvím opatření, které mají za úkol předcházet a nedopustit vznik bezpečnostních incidentů, se nachází jedna jejich skupina, která stanovuje reakce organizace na ně.

Reakce na bezpečnostní incidenty by měla řešit zejména následující tři skupiny problémů:

a) definovat okamžité reakce s cílem zamezit pokračování incidentu;
b) analyzovat narušení bezpečnostních mechanizmů s cílem poučit se z nich a odstranit nedostatky do budoucna;
c) analyzovat bezpečnostní incident s cílem zajistit a podat důkazy o chybovém nebo protiprávním jednání konkrétní osoby nebo skupiny osob pro účely možného pracovně-právního nebo trestně-právního postihu.

Takovou analýzou, která se zabývá získáváním důkazů o procesech spojených s bezpečnostními incidenty a nelegálním používáním nebo využíváním prostředků výpočetní techniky, je **forenzní analýza IS**. Výsledky takové analýzy mohou přímo sloužit jako důkazy při vymáhání náhrady vzniklých škod.

Provedení forenzní analýzy IS tedy může dát organizaci nástroj, pomocí kterého lze výrazně zvýšit pravděpodobnost návratnosti konkrétní škody, vzniklé porušením bezpečnostních nebo jiných opatření v souvislosti s provozem informačních systémů.

Protože však forenzní analýza IS svými závěry může s velkou pravděpodobností přesáhnout hranice organizace, při jejím provedení ne nezbytné dodržet dvě základní pravidla:

a) musí být provedena co nejdříve po výskytu resp. zjištění analyzované události, aby byla zajištěna kompletnost a konzistentnost zajištěných důkazů, tj. vysoce kvalifikovaně, speciálním způsobem a v co nejkratší době po kritické události zajistit a zadokumentovat všechny potřebné informace;
b) musí být provedena způsobem, který je obecně platný a obecně uznávaný pro forenzní analýzy IS, tj. v závislosti od charakteru kritické události všechny získané informace podrobit požadovaným specifickým analýzám. To všechno by mělo být provedeno způsobem uznávaným v soudní praxi, protože nezřídka závěry takových situací mohou až k soudnímu řešení dospět.

Součástí reakcí na bezpečnostní incidenty by tedy mělo být, po rychlém vyhodnocení výše škody nebo dopadu incidentu na chod organizace, vytvoření vhodných podmínek pro provedení nezbytných úkonů nutných ke korektnímu provedení forenzní analýzy IS.

Mezinárodní, ale i naše zkušenosti jednoznačně doporučují obrátit se pro provedení forenzní analýzy IS na specializované organizace nebo instituce. To však ale znamená, že vymezený okruh určených pracovníků organizace by měl být v obecné rovině pravidelně proškolován a seznamován s požadavky, které jsou na provedení forenzní analýzy IS kladeny, aby mohl poskytnout externímu znalci-analytikovi nebo organizaci, neznalému konkrétních detailů používaného IS, účinnou součinnost.

Podle charakteru bezpečnostního incidentu je v současné době možné se s požadavkem na forenzní analýzu IS obrátit na:

a) Policii ČR, která v případech trestné činnosti provádí ve svých vysoce specializovaných expertizních pracovištích zkoumání prostředků výpočetní techniky;
b) soudní znalce z oboru výpočetní technika, kybernetika, bezpečnost informačních systémů, počítačová kriminalita apod., jejichž seznam lze nalézt na webu Ministerstva spravedlnosti ČR;
c) renomované forenzní počítačové auditorské organizace, kontakty na které lze rovněž najít na Internetu, i když ty skutečně renomované se na starém kontinentu hledají těžko.

Jestliže se ale organizace pro řešení takových kritických situací rozhodne přijmout třetí stranu, musí mít jednoznačné smluvní záruky, že nedojde k zveřejnění informací jinými kanály, než těmi, které má pod kontrolou. Nekontrolované úniky takových informací jsou vlastně v příkrém rozporu z bezpečnostní politikou dobře postaveného IS.

Jsou však situace, kdy není vždy z hlediska organizace vhodné, aby samotná informace o bezpečnostním incidentu byla zveřejněna. Je to přirozené a logické, protože se může stát, že její zveřejnění může způsobit mnohem větší škodu, než selhání IS samotné. Jisté zkušenosti s podobnými situacemi jsme již asi všichni, kdo sledujeme problematiku informační bezpečnosti, zaznamenali u jistých finančních institucí a nejsou zrovna lichotivé pro jejich aktéry. Tady by pomohla existence vlastního týmu, který je patřičně vzdělán a odborně vyškolen na specifickou práci forenzního charakteru a má v rámci organizace dostatečně nezávislé postavení. Toto řešení je ale spíše teoretické, protože patří k nejnákladnějším. Takový tým není jednoduché postavit a je jen málo způsobů, jak jej naučit zásady forenzní práce. I kdyby se to povedlo, zvně organizace nezávislým nikdy nebude, takže výsledky jeho práce bude možné použít pouze interně.

* * *

Jak naše, tak i zahraniční průzkumy jednoznačně dokazují prakticky exponenciální nárůst počtu IT bezpečnostních incidentů (o 250% za poslední dva roky podle Secure Computing, April 2000). Také výše škod jimi způsobené se jenom za poslední tři roky zvýšily podle ”1999 CSI/FBI Computer Crime & Security Survey" o 100%! Je to skutečnost, kterou již nelze přehlížet, byť u nás lze ještě uvažovat o určitém zaostávání prosazování se IT v celospolečenském životě. Škody způsobené zneužitím prostředků IT závratně rostou a forenzní analýza IS je jedním ze způsobů, jak je možné napomoct minimalizaci jejich konkrétních dopadů.