Bezpečnostní incidenty a jejich řešení
Jak řešit incidenty v praxi? (1)

Petr Doucek

Úvod

Jedním z významných zdrojů údajů a informací, sloužících jako zpětná vazba k vybudovanému systému řízení bezpečnosti IS/ICT v organizaci, je zpracovávání podnětů, které s sebou přinášejí bezpečnostní incidenty a zkušenosti získané jejich řešením. Pro bezpečnostní incidenty a jejich řešení platí všechny obecné manažerské zásady stejně jako pro každé jiné neočekávané situace, pouze s tím rozdílem, že s jejich řešením mají manageři všech hierarchických úrovní a odborné kvalifikace velmi malé zkušenosti. Vplížily se do běžné praxe managerů jaksi pokoutně a zadními vrátky. Přinesly je s sebou informační technologie a boom nasazování informačních systémů do celé společnosti. Spolu s tím, jak roste naše závislost na informačních technologiích, roste i význam bezpečnosti informačních systémů a důležitost efektivního řešení všech bezpečnostních incidentů v organizacích. První manažerskou zásadou pro řešení incidentů je nebrat bezpečnostní incidenty jako něco exotického, ale již při nasazování informačních systémů se systematicky připravovat na rutinní provoz. Jeho součástí je i vznik různých nestandardních situací, mezi něž bezpečnostní incidenty nesporně patří. Tedy nebát se incidentů, ale být na ně připraven, vědět a znát jak je řešit. K základnímu vybavení managerů – a to nejen managerů z oblasti informačních technologií – by měly patřit základní informace o tom, jak bezpečnostní incidenty řešit – tedy procesní stránka jejich řešení, a základní informace o klasifikaci bezpečnostních incidentů a o jejich závažnosti pro managerem řízenou organizační jednotku a jejich významu pro organizaci celou. Od těchto znalostí managerů se odvíjí rychlá identifikace bezpečnostního incidentu, jeho správná klasifikace a tím i možnost přijmout efektivní rozhodnutí pro jeho řešení při minimalizaci dopadů na chod a investice organizace. Významným základem pro řešení incidentů je široké bezpečnostní povědomí všech pracovníků organizace.

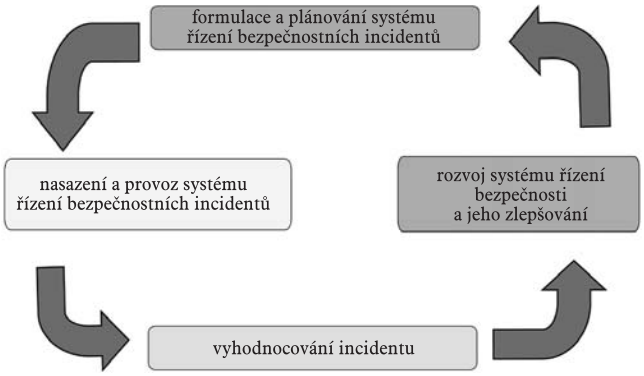
V různých organizacích je obvykle velmi různé bezpečnostní povědomí. V zásadě se můžeme setkat se třemi úrovněmi. První – vysoká – úroveň je obvykle representována velmi dobrými informacemi pracovníků organizací o základních aspektech bezpečnosti informačního systému. Bývají to organizace typu nadnárodních společností, bankovních a finančních institucí a speciálních státních úřadů jako je například Ministerstvo obrany, Ministerstvo vnitra, Národní bezpečnostní úřad apod. Druhá – střední – úroveň je representována převážně privátními firmami některé z nich se zahraniční účastí. V nich jsou znalosti pracovníků o bezpečnosti informačních technologií některým velmi dobře známy, znalosti jiných jsou naopak menší a někteří z nich nejsou tímto problémem poznamenány vůbec. Třetí – nejnižší – úroveň představují malé a střední firmy a organizace centrální a regionální státní a veřejné správy. Celkové bezpečnostní povědomí u většiny pracovníků je velmi nízké. Bezpečnostní povědomí je nutné budovat postupně a nejlepší formou jsou preventivní školení a informovanost pracovníků o bezpečnosti informačních technologií. Součástí bezpečnostního povědomí musí být i schopnost identifikovat bezpečnostní incident.

Bezpečnostní incident

Prvním pojmem, s nímž se musíme seznámit, je bezpečnostní událost – kterou lze označit za identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo selhání některého protiopatření nebo dříve neznámá nebo nepředpokládaná situace, jež může ovlivnit bezpečnost. Samotný vznik bezpečnostní události není ještě incidentem. Teprve vyhodnocená bezpečnostní událost může být kvalifikována jako bezpečnostní incident. Bezpečnostní incident je jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních událostí, jimiž může být s vysokou pravděpodobností narušena podpora hlavních procesů organizace nebo díky nimž může dojít k narušení bezpečnosti informačního systému. S bezpečnostní událostí přichází obvykle do prvního kontaktu běžný uživatel. Do jaké míry právě on rozpozná, jedná-li se o skutečný bezpečnostní incident, na tom závisí rychlost reakce řešení zjištěné události.

Organizační struktury a odpovědnosti spojené s řešením bezpečnostních incidentů

Pro řešení bezpečnostních incidentů se sestavuje z pracovníků organizace specializovaný tým řešení bezpečnostních incidentů – tzv. ISIRT – Information Security Incidents Response Team dále „Tým řešení bezpečnostních incidentů“. Jedná se o organizační strukturu, která se používá výhadně pro potřeby řešení incidentů. Jeho členy se stávají zkušení a důvěryhodní pracovníci organizace, kteří mají zkušenosti s řešením takových situací. Ti se věnují řešení incidnetů po celý jeho životní cyklus až do závěrečné etapy vyhodnocení a zobecnění jeho závěrů a výsledků do celkové koncepce bezpečnosti informačního systému organizace. V některých případech je tento tým posilován o externí specialisty. Pokud dojde v organizaci vinou bezpečnostnímu incidentu ke krizové situaci, bývá Tým řešení bezpečnostních incidentů posílen experty podle povahy zjištěného incidentu. Pro praktické řešení je možné doporučit za vedoucího týmu osobu z vrcholového managementu organizace. Kromě něj by se měl na práci týmu podílet bezpečnostní manager IS/ICT, bezpečnostní manager IS/ICT příslušné organizační jednotky a podle charakteru incidentu odborníci



Obr.1 Schéma PDCA pro řešení bezpečnostního incidentu

na problém a případně i liniový manager pracoviště, kde incident vznikl. Tedy Tým řešení bezpečnostních incidentů má svoje trvalé členy a členy, kteří jsou do něj jmenováni pro řešení určitých konkrétních incidentů.

Životní cyklus řešení incidentů

Pro řešení bezpečnostních incidentů se využívá aplikace modifikovaného Demmingova procesního modelu PDCA [1], které je uvedeno na obr. 1. Celý životní cyklus řešení bezpečnostních incidentů se skládá ze čtyř etap:

- formulace a plánování systému řízení bezpečnostních incidentů,
- nasazení a provoz systému řízení bezpečnostních incidentů,
- vyhodnocování incidentu,
- rozvoj systému řízení bezpečnosti a jeho zlepšování.

Formulace a plánování systému řízení bezpečnostních incidentů vede k návrhu systému řízení incidentů. Vychází z bezpečnostní politiky IS/ICT (informačního systému a informačních a komunikačních technologií) organizace, respektuje i ostatní dokumenty tak, jak jsou uvedeny v [4]. Hlavními činnostmi jsou v této etapě životního cyklu zejména:

- sestavení a vyhlášení politiky řízení bezpečnostních incidentů, včetně přidělení příslušných pravomocí a odpovědností,
- sestavení, formalizace a popis procesu řešení bezpečnostních incidentů – jedno z možných je uvedeno na obr. 2,
- definice dokumentů a dokumentačních povinností pro pracovníky, kteří se podílejí na řešení bezpečnostního incidentu,
- ověření platnosti aktuálních bezpečnostních dokumentů a dokumentace vzhledem k procesu řízení bezpečnostních incidentů,
- sestavení týmu pro řešení bezpečnostních incidentů ISIRT (Information Security Incident Response Team) včetně určení práv a povinností v rámci týmu, určení kontaktních spojení,
- postupy pro sestavování krizových scénářů a procesů v případě krizového stavu organizace vinou bezpečnostního incidentu,
- plán proškolování pracovníků organizace v problematice bezpečnostních incidentů a jejich řešení,
- plány, postupy a způsoby testování procesu řešení bezpečnostních incidentů.

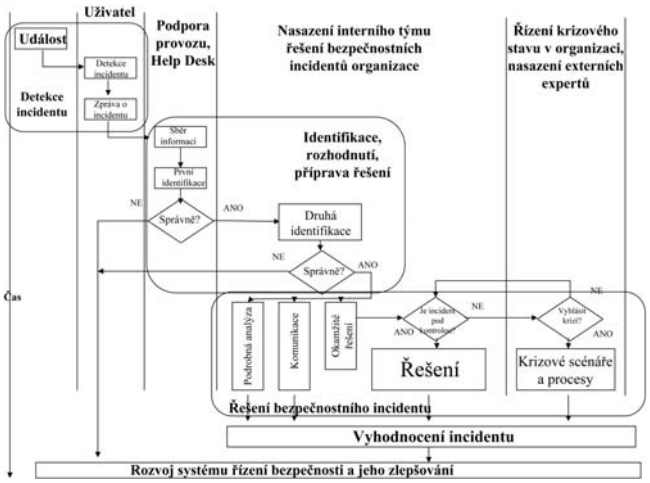
Nasazení a provoz systému řízení bezpečnostních incidentů představuje vlastní nasazení celého procesu do praktického používání v organizaci. V této etapě životního cyklu se provádějí zejména následující skupiny činností – fáze etapy životního cyklu:

- detekce události,
- identifikace, rozhodnutí, příprava řešení,
- řešení bezpečnostního incidentu.

Jejich návaznosti a rámcový obsah jsou uvedeny na obr. 2.

Detekce události

Jedná se o klíčový okamžik pro úspěšné vyřešení bezpečnostního incidentu. Zde se totiž uživatel setkává poprvé s bezpečnostní událostí, kterou musí umět rozpoznat a musí zvládnout její prvotní zařazení. Je událost bezpečnostním incidentem nebo není? To je základní otázka, kterou musí umět velice často zodpovědět neodborník – uživatel. Proto je nezbytné, aby pracovníci organizace, uživatelé informačního systému měli dobré bezpečnostní povědomí. Jenom tak bude systém řízení bezpečnosti efektivní. Pokud pracovníci nebudou schopni detekovat incident a budou opomíjet významná narušení bezpečnosti nebo pokud budou naopak hlásit jakoukoli situaci jako bezpečnostní incident, nebude nasazení Týmu řešení bezpečnostních incidentů smysluplné a efektivní. Buď tým nebude mít vůbec žádnou práci a aktiva organizace budou ohrožena, nebo bude řešit každou maličkost jako bezpečnostní incident a následně bude zahlcen prací. To může mít za důsledek, že jim může významné narušení bezpečnosti informačního systému uniknout. Oba dva případy, jak přehlcení,



Obr.2 Provoz – schéma průběh řešení bezpečnostního incidentu

tak neřešení, jsou pro organizaci velmi nebezpečné, neboť systém detekce bezpečnostních událostí neplní funkci, pro níž byl sestaven.

Další významný bod pro budoucí úspěšné řešení bezpečnostní události resp. bezpečnostního incidentu je množství primárních informací, které se o incidentu podaří zjistit. Proto musí být uživatel takové informace schopen zjistit a zajistit – zdokumentovat. Součástí procesu řešení bezpečnostních incidentů musí být i administrativa, vyplňování formulářů, sestavování zpráv o postupu řešení apod. a hlavně se celý postup řešení bezpečnostního incidentu dokumentuje, aby bylo možné incident dostatečně kvalitně vyhodnotit. Základními dokumenty jsou formuláře pro hlášení bezpečnostní události a bezpečnostního incidentu. Oba musí splňovat nelehkou podmínku. Tou je fakt, že musí shromáždit co nejvíce informací o události nebo incidentu a zároveň je musí být schopen správně vyplnit běžný uživatel informačního systému.

Literatura

[1] DOUCEK, P., NEDOMOVÁ, L.: Nasazení integrovaného systému řízení pro získání konkurenční výhody, In: AT&P journal, 12/2004, ISSN 1335-2237

[2] DOUCEK, P.: Bezpečnost IS/ICT a proces globální integrace – Proč bezpečnost?, In: AT&P journal, 01/2005, ISSN 1335-2237

[3] DOUCEK, P.: Budování systému řízení bezpečnosti IS/ICT - Jak bezpečnost realizovat?, In: AT&P journal, 02/2005, ISSN 1335-2237

[4] DOUCEK, P.: Dokumentace, kontrola a audit bezpečnosti IS/ICT – Jak bezpečnost kontrolovat?, In: AT&P journal, 03/2005, ISSN 1335-2237

[5] ISO/IEC TR 18044 – Information technology – Security techniques – Information security incident management

Pokračovanie v budúcom čísle.

Petr Doucek

Fakulta informatiky a statistiky
Vysoká škole ekonomická v Praze
nám. W. Churchilla 4
130 67 Praha 3, ČR
e-mail: doucek@vse.cz
http://fis.vse.cz