BEZPEČNOST IT – ZKUŠENOSTI SE ZAVÁDĚNÍM

Milada Hrabalová
Otakar Fišer
Hutnická zaměstnanecká pojišťovna (HZP), Jeremenkova 11, 703 00 Ostrava-Vítkovice,
milada.hrabalova@hzp.cz, fiser@hzp.cz

ABSTRAKT
Příspěvek navazuje na naši loňskou prezentaci „Bezpečnost IT a vývoj informačních systémů“. Zabývá se zkušenostmi Hutnické zaměstnanecké pojišťovny se zaváděním procesu řízené bezpečnosti IT. Uvádí seznam dokumentů, které by organizace měla v souladu s normami vypracovat a strukturu bezpečnostního managementu. Seznámí účastníky se zkušenostmi se sestavováním havarijního plánu a strukturou školení zaměstnanců. Nakonec příspěvek popíše provedení penetračního testu pomocí sociálního inženýrství.

KLÍČOVÁ SLOVA:
Bezpečnost IT, normy, penetrační test, sociální inženýrství, školení bezpečnosti, havarijní plán.

1 ÚVOD

Hutnická zaměstnanecká pojišťovna (dále HZP) je zase o rok dále s řízenou bezpečností IT. Tento příspěvek navazuje na naši loňskou prezentaci s názvem „Bezpečnost IT a vývoj informačních systémů“. Zabývá se novými zkušenostmi HZP se zaváděním procesu řízené bezpečnosti IT.V našich přednáškách můžete postupně sledovat vývoj zavádění řízené bezpečnosti IT od jejího počátku a také vliv řešení praktických problémů na tento proces.

2 SOUČASNÝ STAV ZAVÁDĚNÍ ŘÍZENÉ BEZPEČNOSTI IT V HZP

2.1 Historie

Jak jsme již uvedli v loňském příspěvku, začala se Hutnická zaměstnanecká pojišťovna systematicky a dle norem zabývat bezpečností IT v roce 2003. Nechali jsme si dodavatelsky provést analýzu rizik a napsat základy potřebných dokumentů. Postupovali jsme dle norem, především dle ISO/IEC TR 13335 [2] a ISO/IEC 17799 [1]. Vybudovali jsme bezpečnostní management a ze základů dokumentů jsme si již sami vytvořili příslušné vnitřní předpisy.
V roce 2005 byla norma ISO/IEC 17799 [1] vydána v českém překladu, což jistě usnadnilo práci všem, kteří se chystali řízenou bezpečnost IT zavést.

2.2 Potřebné dokumenty

Dle doporučení normy [2] si HZP vytvořila z dodavatelského základu všechny potřebné dokumenty v této hierarchii:

a) **Strategie a politika HZP na období 2003 až 2006** – v tomto dokumentu jsou definovány cíle, strategie a politiky celé pojišťovny
b) **Politika bezpečnosti HZP** - definuje cíle, strategie a politiky v oblasti bezpečnosti obecně pro celou pojišťovnu
c) **Politika bezpečnosti IT** – definuje cíle, strategie a politiky postupu v oblasti bezpečnosti IT, vyjadřuje podporu ze strany managementu. Vychází z předchozích dvou dokumentů.

d) **Příručka bezpečnosti IT –** zabývá se zásadami bezpečnosti, stanovením zodpovědností a povinností v jednotlivých konkrétních případech. Přestože zásady uvedené v tomto dokumentu se dodržovaly již dříve jako nepsané, při přípravě jejich písemného tvaru došlo k jejich zpřesnění a konkretizaci.
e) **Plán bezpečnosti IT** – obsahuje seznam úkolů, které je třeba splnit v oblasti bezpečnosti IT v nejbližším roce pro dosažení stanovených cílů.
f) **Havarijní plán včetně Plánu obnovy** – popis kroků, které musí následovat bezprostředně po havárii, jmenování havarijních čet.
g) **Školení bezpečnosti IT** – určení zodpovědnosti za školení bezpečnosti IT, termíny a rozsah školení pro různé skupiny zaměstnanců

2.3 Bezpečnostní management

Dle doporučení normy [2] je nutno v organizaci přiřadit odpovědnosti a role a vytvořit organizační strukturu pro řízení bezpečnosti. Vedou k tomu tyto důvody:

a) je nutno zajistit, aby byly plněny všechny důležité úkoly v procesu řízené bezpečnosti IT (aby se na něco nezapomnělo) a aby byly prováděny efektivně,
b) bezpečnost IT se týká všech útvarů organizace (není možné, aby se jí zabývala pouze informatika)

V HZP byl proto vytvořen a obsazen konkrétními zaměstnanci tento management bezpečnosti:

- Bezpečnostní manažer
- Fórum bezpečnosti
- Auditor bezpečnosti

Dále byli pojmenováni vlastníci procesů a dat, správce systému a správci aplikací.

2.4 Školení bezpečnosti IT

Školení zaměstnanců je v HZP prováděno dvěma způsoby:

a) **školení přímým nadřízeným** – minimálně dvakrát ročně. Při tomto školení je kladena zodpovědnost na jednotlivé vedoucí, aby školení nebylo pouze formální, ale aby školená témata jejich podřízení opravdu ovládali. Podklady pro tato školení jsou připravována manažerem bezpečnosti IT a vyvěšována na intranetu.
b) **školení externí firmou** – jednou ročně je ve dvou dnech uspořádáno po skupinách školení pro všechny zaměstnance HZP. Školení pro jednu skupinu trvá cca 1,5 hodiny. Pracovník externí firmy provádí nejprve školení a poté se více zaměří na oblast, kterou si přejeme. Součástí tohoto typu školení je závěrečný anonymní test znalostí posluchačů. Tento test slouží k průzkumu znalostí mezi zaměstnanci a ukazuje, na co se další školení musí více zaměřit.

Kromě toho jsou školeni všichni zaměstnanci, kteří vstupují do zaměstnaneckého poměru a poučeni všichni, kteří dostanou k používání notebook. Management pojišťovny je o aktuálních problémech bezpečnosti IT informován vedoucím informatiky na poradách vedení.

Obsahem školení jsou zejména oblasti:

1. Cíle a principy bezpečného používání výpočetní a komunikační techniky
2. Vysvětlení základních pojmů bezpečnosti IT
3. Ochrana proti škodlivému SW - viry a antivirová ochrana, spam, spyware, hoax, phishing, pharming atd.
4. Elektronická pošta – správné chování při odesílání a příjmu
5. Elektronický podpis – význam, použití a ochrana
6. Hesla – volba správného hesla, uchování hesla, ochrana hesla

7. Internet – bezpečné chování na internetu
8. Ochrana dat - zákonné normy, klasifikace dat, uchovávání, přenos, likvidace, zálohování, archivace dat, kdo je vlastník dat
9. Sociální inženýrství – co to je, jak se proti němu bránit
10. Bezpečnostní incidenty – chování při mimořádných událostech
11. Ochrana přenosných počítačů

3 HAVARIJNÍ PLÁNOVÁNÍ

Vytvoření postupů pro chování za mimořádné situace a plánů obnovy pro návrat k předchozímu stavu je nutná podmínka pro řízení kontinuity činnosti organizace a je také doporučena normou [1].

3.1 Vytvoření havarijních plánů

V naší pojišťovně byla tvorba havarijního plánu nejdelším procesem z tvorby všech vnitřních předpisů, trvala cca 14 měsíců. Největším problémem bylo vytvořit ze všech informací, které v havarijním plánu mají být, přehledný dokument, podle kterého by se dalo v případě mimořádné situace postupovat a na kterém by se dohodli všichni klíčoví zaměstnanci informatiky. Teprve po roce jsme našli hranici, kdy v tomto dokumentu bylo vše nezbytné a zároveň zůstal přehledným.

Problémem přitom nebyl pouze samotný text havarijního plánu. Bylo potřeba vytipovat a smluvně zajistit místo mimo budovy HZP, kde by se v případě nedostupnosti budov mohla sejít havarijní skupina, případně rozjet alespoň nouzový provoz. Bylo třeba vybrat dokumenty a jiné materiály (zálohy IS, některý HW a SW), které bude třeba uchovávat ještě na jiném místě než na ústředí HZP, zajistit pro ně bezpečné umístění a způsob jejich výměny při aktualizaci.

Uvažovali jsme také, že havarijní plán bude mít každý velký útvar HZP. Nakonec jsme se vzhledem ke složitosti problematiky rozhodli zatím vytvořit havarijní plán jen pro informatiku a rozdělit jej na tři části. Důvodem pro rozdělení havarijního plánu bylo zestručnění a tím zvýšení přehlednosti Havarijního plánu pro případ havárie, což je pravděpodobnější stav:

a) **Havarijní plán pro případ havárie** – běžnější stav, počítá s dostupností budovy a místností, nedostupné jsou pouze prostředky IT. Je velmi útlý a přehledný, má pouze 6 stran.
b) **Havarijní plán pro případ katastrofy** – tento plán počítá se situací, kdy nebudou dostupné budovy s IT (např. požár) a bude nutno zahájit zpracování v jiných prostorách. Tento plán obsahuje totéž co havarijní plán pro případ havárie a má několik kapitol navíc. Má 11 stran.
c) **Přílohy** – společné pro oba předchozí havarijní plány, má 14 stran.
   Tyto přílohy obsahují:
   1. seznam klíčových obchodních partnerů,
   2. konkrétní umístění náhradních pracovišť,
   3. materiál, který by měl být zachráněn z případně zničených budov, v pořadí dle důležitosti,
   4. seznam zaměstnanců informatiky.
   5. uskutečněné kontakty na havarijní skupinu při jejím svolávání,
   6. kroky při obnově kritických funkcí,
   7. docházka a rozmístění osob,
   8. co má obsahovat zpráva o stavu pro krizový štáb,
   9. co zjistit od krizového štábu.

   Přílohy 5 - 9 slouží jako prázdné formuláře – vodítka při mimořádné události.

Oba Havarijní plány, pro případ katastrofy i havárie, obsahují:

1. návod jak postupovat bezprostředně po mimořádné události,
2. kontakty na členy havarijní skupiny,
3. seznam kritických funkcí vzhledem k IT a v jakém pořadí je třeba je obnovovat,
4. jaká jsou místa setkání havarijní skupiny,
5. náhradní pracoviště pro obnovu provozu,
6. způsob spolupráce s Krizovým štábem HZP,
7. seznam a umístění materiálů umístěných mimo sídlo HZP atd.

Vzhledem k tomu, že byl vytvořen Havarijní plán pouze pro odbor informatiky, nejsou v něm řešeny náhradní postupy zpracování při výpadku prostředků IT na jednotlivých odborných útvarech. Na těchto útvarech se v případě havárie používá většinou náhradní papírové řešení a existují pro něj vyzkoušené postupy, které ovšem nejsou zpracovány do podoby havarijního plánu. Dle praktických zkušeností je to dostačující.

3.2 Testování havarijních plánů

Dle doporučení normy [1] by mělo docházet také k testování havarijních plánů, tj. zda plány budou fungovat v reálném životě. Testování by mělo probíhat v několika vrstvách, od ověření od stolu přes simulaci pro zaměstnance v řídící pozici v krizových týmech, technické testy obnovy až po generální test – simulaci havárie, které se zúčastní všichni zaměstnanci a technika. Na toto testování se teprve připravujeme.

4 PENETRAČNÍ TEST

V HZP budujeme bezpečnost IT již několik let a začala nám chybět zpětná vazba. Bylo žádoucí dozvědět se, zda proces probíhá správně ne z pohledu norem, ale z pohledu faktického zajištění lepší bezpečnosti IT. Bylo nutné zjistit skutečný stav, a to zhruba v oblastech:

a) povědomí zaměstnanců o bezpečnost IT
b) slabá místa
c) směr dalšího školení a případně jeho zlepšení
d) kde musíme současný stav přehodnotit
e) co musíme znovu analyzovat

V loňském roce jsme se proto rozhodli provést test zaměstnanců pomocí metod sociálního inženýrství.

4.2 Sociální inženýrství

Sociální inženýrství je pojem, který „proslavil“ nejznámější americký hacker – Kevin Mitnick. Jedná se o metodu, která má přesvědčit člověka, že situace je jiná než se na první pohled zdá a donutit jej udělal věc, kterou by udělat neměl. Typickým příkladem sociálního inženýrství je přesvědčit uživatele, aby si sám nainstaloval virus zaslaný v e-mailu, ať už slibným názvem přílohy, např. anna.kournikova.jpg.vbs, nebo předstíráním, že e-mail odešel od důvěryhodného zdroje, např. od banky, v níž má uživatel svůj účet.

Sociální inženýrství používá silné nebo slabé metody.

Příkladem **slabých metod** je**:**

a) vydávat se za někoho, kdo má oprávnění (administrátor, servisní firma, klient)
b) vydávat se za někoho, kdo má moc (VIP, příkaz z vedení, státní úřad)
c) vydávat se za někoho, kdo potřebuje pomoc (nový zaměstnanec)

Příkladem silných metod **je např.:**

a) dlouhodobé **budování důvěry**
b) úplatky (peníze, různé výhody, sex, drogy...)
c) zastrašování a vydírání

4.3 Organizace testu

Pro náš test jsme zvolili pouze slabé metody sociálního inženýrství a dohodli jsme se s vybranou firmou na 4 dnech na jeho provedení, byl to tedy relativně krátký čas.
Pro tuto firmu jsme také vytipovali informace, které by se mohli pokusit získat.
O záměru provést tento test byl kromě manažera bezpečnosti IT a vedoucího informatiky informován pouze ředitel HZP, nevěděli o něm předem tedy ani zaměstnanci informatiky.
Námi poptaná externí firma použila několik způsobů při pokusech o získání informací, a to osobně, telefonicky a e-mailem. Např. při osobních návštěvách se jejich pracovník vydával za pracovníka naší dodavatelské firmy, která nám zajišťuje servis PC, a pokoušel se získat přístup k PC a síti.

4.4 Výsledky testu

Výsledky testu víceméně potvrdily naše přesvědčení, že lidé jsou nejslabším článkem bezpečnosti IT, a byly dle sdělení provádějící firmy zcela v průměru. Lepší výsledky měl test u středního managementu než u ostatních zaměstnanců, zřejmě si lépe uvědomuje svou zodpovědnost. Vrcholový management nebyl testován.
Mezi zaměstnanci bylo mnoho takových, kteří věděli, jak se zachovat. Žádost odmítli, případně se informovali u manažera bezpečnosti IT, na kterého se pracovník provádějící test odvolával. Našli se ale i takoví, kteří se nechali přesvědčit a udělali něco, co neměli.
Prezentace výsledků vrcholovému managementu HZP byla provedena bez uvedení konkrétních jmen zaměstnanců ať se správným nebo chybným jednáním. Bylo rozhodnuto, že test se bude s určitým časovým odstupem opakovat a mezitím se zintenzivní školení zaměstnanců.

5 JAK DÁL

Proces řízené bezpečnosti IT je proces ustavení a aktualizace programu bezpečnosti IT. Sestává z činností, které je nutno cyklicky v pravidelných kratších či delších intervalech opakovat. Hlavní aktivity jsou [2]:

a) stanovení cílů v oblasti bezpečnosti IT organizace
b) organizační zajištění – definice rolí a zodpovědností
c) analýzy rizik a z ní vzniklá doporučení pro bezpečnost IT
d) vytvoření (aktualizace) politik bezpečnosti IT
e) vytvoření (aktualizace) plánu bezpečnosti IT
f) implementace ochranných opatření
g) budování povědomí o bezpečnosti
h) aktivity sledování (aktualizace, audity, monitorování, řešení incidentů)

V HZP jsou prováděny všechny potřebné aktivity, jak ale se ukazuje po penetračním testu, musíme se více zaměřit na budování povědomí o bezpečnosti. Přestože jsou všichni

zaměstnanci několikrát ročně školeni, je bohužel bezpečnost IT u některých zaměstnanců brána jako formalita, jako obtěžování, jako něco, co zdržuje od práce. U některých dalších, kteří berou bezpečnost IT zodpovědněji, převáží zase někdy ochota pomoci klientovi nad vědomostmi ze školení. Správné bezpečné jednání není většinou automatické, každý se musí nejprve zamyslet a teprve poté jednat.
Budeme muset zaměstnance více motivovat, ať už pozitivně (odměna, pochvala) nebo negativně (snížení odměn, pokárání) za jejich chování v oblasti bezpečnosti IT.

6 ZÁVĚR

Náš svět je z hlediska bezpečnosti IT čím dál horší, vynořují se nové a nové hrozby a je třeba přijímat proti nim adekvátní opatření. Je jedno, v které zemi žijeme, čím více je organizace závislá na IT technologiích, tím je zranitelnější. Vyšší riziko představuje také vnitřní síť organizace a připojení na internet.
Přesto všechno není vhodné zaměřit se pouze na technická opatření, jako jsou firewally, antivirové programy, programy pro detekci průniků atd. Přestože i tato opatření jsou důležitá, většinou zabraňují pouze náhodným útokům. Cílené útoky budou zřejmě přicházet pomocí pokusů o průnik nebo získání informací přímo od zaměstnanců organizace. Je to jednodušší a levnější. Proto je nutné věnovat velkou péči lidem, jejich vzdělávání, zvyšování povědomí o bezpečnosti IT, zvyšování firemní kultury, hrdosti na svou firmu a loajality. Jen tak lze snížit nebezpečí nevědomých nebo dokonce vědomých bezpečnostních incidentů.

7 LITERATURA

[1] ČSN ISO/IEC 17799:2005 – Informační technologie – Soubor postupů pro řízení informační bezpečnosti
[2] ČSN ISO/IEC TR 13335:1997 - 2000 – Informační technologie – Směrnice pro řízení bezpečnosti IT.