Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Počítačová kriminalita a jej vyšetrovanie

František Soviš

2013

KPMG
cutting through complexity™

Cieľ prednášky:

1. Poukázať na:
- počítačové bezpečnostné incidenty javiace sa ako trestné činy
- podstatu vyšetrovania počítačovej kriminality
- metodiku zbieranie digitálnych stôp

2. poradiť:
- Na koho sa obrátiť o pomoc
- Čo je vhodné robiť (a čoho sa vyvarovať)

3. Upozorniť na to, čo nás čaká.

Obsah:

Definície bezpečnostného incidentu

Bezpečnostný incident (BI) je udalosť, ktorá spôsobí porušenie niektorej z bezpečnostných požiadaviek kladených na informácie, na spôsob spracovania informácií a na činnosť IKT (predovšetkým bezpečnostné požiadavky CIA: dôvernosti, integrity a dostupnosť).

BI je jedna alebo viaceré neželané a neočakávané udalosti, pri ktorých je vysoká pravdepodobnosť prezradenia, poškodenia alebo straty aktív organizácie a ohrozenia jej informačnej bezpečnosti.

BI spôsobujú hrozby vyvolané prírodnými javmi, prostredím alebo človekom.

- Časť BI spôsobených človekom (či už úmyselne alebo neúmyselne) spadá pod pojem počítačová kriminalita.

Primárne kategórie bezpečnostných incidentov

- Odmietnutie služby (Denial of Service, Distributed DoS)
- Škodlivý kód (Malicious Code)
- Neautorizovaný prístup (Unauthorized Access)
- Nevhodné použitie (Inapropriate Usage)
- Vymazanie alebo modifikácia dát
- Poškodenie/krádež komponentov IKT
- Viaczložkový komponent (kombinácia)

(viac v prednáške: Bezpečnosť prevádzky)

Štandardné zdroje indikácií o BI:

- Hlásenia bezpečnostného softvéru typu IDS
- Hlásenia antivírusového softvéru
- Hlásenia softvéru na kontrolu integrity súborov
- Hlásenia služby monitorovania treťou stranou
- Záznamy operačných systémov, služieb a aplikácií
- Záznamy sieťových zariadení
- Záznamy nástrahy („honeypot“)
- Verejne dostupné informácie o nových slabinách a exploitoch
- Verejne dostupné informácie o incidentoch v iných organizáciách
- Informácie od používateľov z vnútra organizácie
- Informácie od ľudí z vonka organizácie

Predpoklady úspechu zvládania BI

Základný predpoklad **úspešného zvládania BI** v organizácii je vymedziť dostatočné zdroje a primerané organizačné opatrenia, najmä:

- existencia osoby (role) **analytik BI** – najlepšie z útvaru IT,
- nepretržité monitorovanie hrozieb vhodnými nástrojmi (systémy na detekovanie prienikov IDS, pravidelná kontrola logov a antivírusová ochrana),
- všeobecne známe procedúry nahlasovania BI (smernica)
- zavedenie vhodných komunikačných mechanizmov medzi zainteresovanými útvarmi (právny, personálny, IT, manažér IB)
- pravidelné zálohovanie databáz a zálohy SW (smernica)
- správne odstupňované riadenie prístupov do IS.

V procese riešenia BI je najťažšou úlohou jeho detekcia a rýchlosť reakcie naň.

Počítačová kriminalita (a trestné činy)

Počítačová kriminalita je protiprávne konanie človeka, pri ktorom cieľom alebo nástrojom páchateľa sú informačné systémy alebo ich komponenty. (tiež „cybercrime“)

1. T.Č. vo vzťahu k hmotnému majetku IS (krádeže alebo poškodenia počítačov a ich príslušenstva, vrátane nosičov informácií).

2. T.Č. vo vzťahu k nehmotnému majetku IS (t.j. k programovému vybaveniu, databázam, informáciám - odcudzenie, pozmeňovanie, nelegálne používanie, infiltrácie).

3. T.Č., pri ktorých je počítačová technika prostriedkom k ich páchaniu (napr. hospodárska kriminalita - podvody, sprenevery, a iná trestná činnosť realizovaná prostredníctvom počítačov - podnecovanie alebo schvaľovanie trestného činu, detská pornografia, krádeže digitálnej identity).

Počítačová kriminalita (2/3)

Nie každý bezpečnostný incident je trestný čin. Ale:

Útok na „hmotnú podstatu IKT“ je evidentne trestný čin.

(Hneď je zrejmé, že niečo v majetku chýba alebo je poškodené – preto sa tento čin posudzuje skôr ako klasická „majetková kriminalita“ – a aj spôsob jej vyšetrovania možno charakterizovať ako „klasický“).

BI súvisiace s „nehmotnou podstatou IKT“ je zložitejšie posúdiť z trestno-právneho hľadiska (zvyčajne nič nechýba – skôr „pribudlo“, a aj poškodenia sa nezisťujú triviálne).

Niekedy sa vyskytujú T.Č., ktoré sú kombináciou „hmotnej i nehmotnej podstaty IKT“ (napr. krádež počítača s cieľom zmocniť sa informácií v ňom obsiahnutých).

Ak je BI „s nehmotnou podstatou IKT“ posúdený ako T.Č., tak jeho vyšetrovanie používa iné postupy, kde kľúčovú úlohu zohráva tzv. digitálna stopa.

Počítačová kriminalita (3/3)

Klasifikácia T.Č. : prečin, zločin a obzvlášť závažný zločin.

V Trestnom zákone č.300/2005 Z.z. je tejto forme kriminality venovaný napr.:

§ 212 - Krádež (sadzba až 2 roky)

§ 215 - Neoprávnené užívanie cudzej veci (až 1 rok)

§ 247 -Poškodenie a zneužitie záznamu na nosiči informácií (až 3 r.)

§ 281 - Porušenie v oblasti duševného vlastníctva a obchodného mena (až 3 roky)

§ 282 - Porušenie priemyselných práv (až 3 roky)

§ 283 - Porušenie autorského práva

§ 286 - Ohrozenie verejného telekomunikačného zariadenia (až 5 r)

§ 374 – Neoprávnené poskytovanie OÚ

Digitálna stopa a dôkaz

Definícia podľa Scientific Working Group on Digital Evidence:

„Digitálna stopa je akákoľvek informácia s vypovedacou hodnotou uložená alebo prenášaná v digitálnej binárnej forme, ktorá môže byť predložená súdu ako vecný dôkaz s vypovedacou hodnotou.“

Definícia je otvorená všetkým technológiám záznamu:

- počítače, komponenty IS, pamäťové nosiče dát,
- digitálne prenosy dát (mobily, digitálna TV),
- digitálne fotografie, záznamy digi-kamier,
- digitálne audiozáznamy (napr. hovorov),
- digitálne záznamy z EPS a EZS a pod.

Dôraz je kladený na **predložiteľnosť** súdu – stopa vs. dôkaz.

Digitálna stopa – vlastnosti

Vlastnosti DS (rozdiely oproti reálnym stopám):

- Nehmotnosť (ale pre ich uloženie je nutné hmotné prostredie – vysoká variabilita rôznych druhov médií)
- Latentnosť (DS sú pre ľudské zmysly nezaznamenateľné – nutnosť špeciálnych prostriedkov na ich „zviditeľnenie“)
- Časová trasovateľnosť (DS sú spojené s veľmi presným časovým údajom – možnosť chronologického radenia DS – systémový čas
- Vysoká obsažnosť (vždy sa niečo dá nájsť – ale hrozí presýtenie)
- Veľký dátový objem (detto)
- Reštaurovateľnosť (aj zmazané sa dá niekedy obnoviť)
- Originálnosť (vhodne zhotovený duplikát je zhodný s originálom

Veľkosť geografického priestoru a zašifrované údaje sú komplikácie (prakticky nepoužiteľné).

Digitálna stopa – zbieranie (1/4)

Originálna DS sa nachádza na fyzickom objekte (počítač, pamäť).

Duplikát DS je presná digitálna reprodukcia na rovnaký typ fyzického objektu (rovnaký disk alebo rovnaké médium) v pomere 1 : 1.

Pre prípad vyšetrovania T.Č. a eventuálne súdne konanie **vždy** musia byť dva identické exempláre DS (originál + duplikát alebo dva identické duplikáty), z ktorých jeden je uložený ako referenčný (napr. v trezore) a s druhým – pracovným sa robí forenzná analýza.

Kópia DS sa zhotovuje, ak nemôžeme dosiahnuť duplikát DS (geograficky vzdialené DS alebo nemáme zhodný typ fyzického nosiča), opäť v 2 exemplároch a so snahou v pomere 1 : 1, čo však môže byť nerealizovateľné, napr. skryté údaje na vzdialenom úložisku). Kópia DS má slabšiu preukaznú hodnotu pred súdom.

Digitálna stopa – zbieranie (2/4)

Pre zbieranie DS je vhodné mať „pohotovostný kufrík“ (jump kit) s nasledovným obsahom:

- Laptop vybavený vhodným SW (napr. paketový sniffer, prehliadače)
- Zálohovacie prostriedky a prázdne média
- Základné sieťové zariadenia a káble
- Generačné médium s OS s aktuálnymi záplatami
- Aplikačné programové vybavenie
- Poznámkový blok, popisovače na médiá
- Fotoaparát (aj v mobile)

Súd vždy zaujíma ako boli DS zbierané a následne aj chránené.

Digitálna stopa – zbieranie (3/4)

O každej DS ako potenciálnom dôkaze musí byť vedený detailný záznam nasledujúceho zloženia:

- Identifikácia nosiča informácie (napr. umiestnenie, sériové č., číslo modelu, meno uzla, adresa MAC sieť.rozhrania, adresa IP sieťovej karty uzla)
- Meno a priezvisko každého jednotlivca, ktorý zbieral alebo narábal s DS počas analýzy
- Popis aktivity vykonanej s DS
- Dátum a čas každého narábania s DS
- Miesto uloženia DS (zamedzujúceho neoprávnenú manipuláciu).

Digitálna stopa – zbieranie (4/4)

Aké DS zbierať? Všetko relevantné, ale najmä:

- Kompletný „image“ disku napadnutého uzla
- Logovacie súbory (aj z firewalu – možná IP adresa útoku)
- Dynamické stopy (ak existujú – obsah operačnej pamäte)
- Správanie systému pri simulovanom opakovaní incidentu (!!)
- Správy z IDS (ak je implementovaný)
- Relevantné pamäťové médiá (CD, flopy, flash, a pod.)

Ale aj iné stopy:

- Všetky zapojenia káblov
- Popis architektúry
- Poznámky o mieste činu, relevantné papierové dokumenty
- Fotografie miesta a pod.

Proces vyšetrovania BI ako trestného činu

Vyšetrovanie BI ako trestného činu má štyri fáze:

1. Predspracovanie je prvotná analýza BI – prakticky ju vykonáva analytik BI pri jeho zistení a identifikovaní (čo sa asi stalo, odkiaľ to asi prišlo, čo treba rýchlo vykonať na zamedzenie eskalácie, ale nepoškodiť stopy).
2. Zbieranie stôp (mali by byť prítomné 2 osoby) a ich bezpečné zaistenie a uloženie.
3. Podrobná forenzná analýza, v ktorej sa skúmajú a extrahujú relevantné udalosti z DS, ich časové a príčinné zoradenia a priradenie ich pôvodcu (páchateľa).
4. Dokumentácia je prezentácia výsledkov analýzy, usporiadanie a vytvorenie podkladov predkladaných orgánom činným v trestnom konaní (súdu).

Identifikácia útočníka

Identifikácia útočníka „zvnútra“ je pomerne jednoduchá záležitosť – cez loginy (s výnimkou administrátorov).

Identifikácia útočníka „zvonku“ - treba zistiť jeho IP adresu – čo je ale obtiažná úloha (a v súčasnosti prakticky ťažko riešiteľná), lebo:

- Sfalšované IP adresy
- Veľa zdrojových adries
- Platnosť IP adresy
- Spolupráca poskytovateľov sieťových služieb
- Zákonom stanovená lehota uchovávania záznamov

Zákon č.351/2011 Z.z. o telekomunikač. službách – 6 mes.

Cena za prešetrovanie BI

- Zbieranie a analyzovanie DS je náročná a zdĺhavá činnosť, ktorá predpokladá vysokú odbornú erudovanosť a skúsenosť odborníkov.

- Tí majú svoju cenu – ich denná sadzba začína pri sume 1 000 eur. Príprava na súdne konanie sa môže vyšplhať na niekoľko desiatok tisíc eur (čo pre štátne inštitúcie môže byť problém).

- Výsledok súdu je veľmi neistý (dnes je veľmi nízka akceptácia DS v právnej praxi).

Kde hľadať odbornú pomoc:

- znalci /znalecké organizácie
- CSIRT.SK
- kriminalisti PZ SR
- špecializované súkromné firmy

Znalecká činnosť (1/3)

Znalec je štátom uznávaný odborník, ktorý spĺňa podmienky stanovené zákonom č. 382/2004 Z.z. (o znalcoch, tlmočníkoch a prekladateľoch a o ...) a je zapísaný v Zozname znalcov MS SR.

MS SR určuje odbory a v ich rámci **odvetvia** znaleckej činnosti označované 6-miestnym kódom (niekoľko tisíc znalcov pre asi 100 rôznych odvetví).

Ďalšie výhody pri riešení BI za pomoci znalca:

Znalec disponuje identifikačným preukazom znalca vydaným MS SR a znaleckou **pečiatkou so štátnym znakom** (dôležité pri zaisťovaní DS).

Podľa zákona pri výkone znaleckej činnosti musí každý poskytnúť znalcovi **súčinnosť** (inak ide o marenie spravodlivosti).

Znalecká činnosť (2/3)

Pre posudzovanie BI a zbieranie DS majú význam znalecké odvetvia technického zamerania:

10 1000 – Bezpečnosť a ochrana informačných systémov

10 0600 – Elektronické komunikácie

10 0200 – Elektronika

10 0800 – Nosiče zvukových a zvukovo-obrazových záznamov

10 0701 – Odhad hodnoty elektrotechn. zariadení a elektroniky

10 0400 – Riadiaca technika a výpočtová technika

49 2000 – Kriminalistická informatika

Podobne je to aj u špecializovaných znaleckých ústavoch.

Znalecká činnosť (3/3)

Oblasti, kde môže byť znalec/znalecký ústav nápomocný, sú:

- Zabezpečovanie DS a ďalších analytických úkonov s nimi,
- Vypracovanie posudkov pre orgány činné v trestnom konaní,
- Spracovanie odbor. podkladov pre podanie trestného oznámenia,
- Posudzovanie plnenia a kompletnosti dodávok a zmlúv (obch.spory),
- Posudzovanie IT projektov pred, pri a po realizácii,
- Posudzovanie závad a hodnoty IT zariadení a progr. vybavenia,
- Vypracovanie rôznych odborných stanovísk (napr. ochrana dát).

Organizácie typu CERT/CSIRT

Computer Security Incidents Response Team (CSIRT) **a Computer Emergency Response Team** (CERT) – sú súkromné, vládne a firemné organizácie pre riešenie problematiky informačnej bezpečnosti.

Prvá organizácia CERT vznikla v roku 1988 v USA (pod DARPA), dnes je po celom svete viac ako 250 organizácií typu CERT/CSIRT.

Agentúra ENISA (European Network and Information Security Agency) vznikla v roku 2004 na základe nariadenia Rady ES č. 460/2004 s cieľom na koordináciu a zdieľanie informácií v oblasti IB medzi členskými štátmi EÚ.

Podľa Uznesenia Vlády SR č.479/2009 bol zriadený CSIRT.SK ako špecializovaný útvar DataCentra (rozpočtová organizácia Min.Fin.SR) s cieľom zabezpečiť primeranú ochranu národnej informačnej a komunikačnej infraštruktúry SR. (člen ENISA, Terena)

CSIRT.SK

CSIRT.SK poskytuje pre vlastníkov a správcov IS verejnej správy najmä tieto aktívne a proaktívne služby:

-Varovania /upozornenia na aktuálne bezpečnostné riziká,
-Odporúčania na reakcie na BI a ich koordinácia,
-Analýzy bezpečnostných rizík, zraniteľností a škodlivého SW,
-Technologický dozor v oblasti IB,
-Vzdelávanie a konzultačná činnosť v oblasti IB,
-Organizovanie cvičení na zvládanie BI,
-Pomoc pri konfigurácii a údržbe bezpečnostných nástrojov a aplikácií IB,
-Asistencia a zaškolenie pri budovaní vlastných tímov pre riešenie BI a pod.

“20 Critical Security Controls“ - 20 prioritizovaných opatrení, ktoré sú aplikovateľné na rôzne typy organizácií a ktoré sú efektívne na blokovanie v súčasnosti najčastejšie sa vyskytujúcich známych útokov a útokov očakávaných v budúcnosti.

Viac na http:/www.csirt.gov.sk

Postup orgánov činných v trestnom konaní (OČvTK)

Ak je situácia evidentne jasná (bezpečnostný incident je trestným činom), treba sa obrátiť na ktorýkoľvek útvar Policajného zboru SR alebo na Prokuratúru SR. Tieto orgány v zmysle zákonných postupov a zákonných právomocí už zariadia následné aktivity.

Ale:

1. Pre oblasť počítačovej kriminality majú OČvTK málo kvalifikovaných odborníkov – obzvlášť pri zaisťovaní DS si prizývajú na pomoc príslušných znalcov.

2. Pre úspešné vyšetrenie trestného činu sám PZ odporúča oznamovateľovi priložiť všetky materiály a dokumenty (aj DS), ktoré môžu byť nápomocné pri vyšetrovaní daného bezpečnostného incidentu ako T.Č. (opäť úloha pre znalcov).

Kriminalistický a expertízny ústav PZ v Bratislave.

Orgány činné v trestnom konaní (OČvTK)

Slovensko je členom **EUROPOL** (European Police) - zastúpenie:

Úrad medzinárodnej policajnej spolupráce
Národná ústredňa Europol
Račianska 45, 812 72 Bratislava

EUROPOL má od roku 2012 špec. pracovisko **EC3** (European Cyber-Crime Centre) s centrálou v holandskom Haagu.

hppt:/www.europol.europa.eu

hppt:/www.

Pozn. US treba riešiť s NBÚ, resp. s Min.Obrany

Praktické rady „čo robiť“

1. Realizujte dobré bezpečnostné opatrenia a dodržujte bezpečnostnú politiku.
2. Určite min. 1 analytika na riešenie BI, ktorému sa nahlasujú BI, a Smernicou o BI zaviažte zamestnancov k ich nahlasovaniu.
3. Pravidelne preškolujte používateľov IKT o informačnej bezpečnosti a zvyšujte ich bezpečnostné povedomie.
4. Pri komplikovanejších BI sa nesnažte všetko robiť „svojpomocne“, ale prizvite na pomoc odborníkov (CSIRT.SK, znalci, renomované firmy).
5. Ak BI naznačuje trestnú činnosť, konzultujte to s právnikom (svojim) a až následne informujte orgány činné v trest. konaní.
6. Vyhnite sa publikovaniu BI na verejnosti – obzvlášť v médiách.

Praktické rady „čo robiť“

7. Pred dôsledným zanalyzovaním BI a prekonzultovaním výsledku analýzy s právnikom rozhodne nekomunikujte s protistranou, prípadne s páchateľom.

8. Pokiaľ sa dá, vyhnite sa súdnemu sporu, ideálne je mimosúdne riešenie alebo dohoda o urovnaní a pod. Samozrejme, ak ide o trestný čin alebo iné kriminálne konanie, súdne riadenie je nutnosťou.

9. Ak oznámite spáchanie trestného činu OČvTK, spúšťa sa zákonný postup, ktorý by mal byť zavŕšený súdnym konaním.

Na záver

Najbližšie nás čakajú **tri významné udalosti**, ktoré s určitosťou významne zvýšia výskyt bezpečnostných incidentov, obzvlášť útoky na IKT štátnej a verejnej správy „z vonku“:

Rok 2014 – predsedníctvo SR vo Višegradskej skupine

Rok 2015 – predsedníctvo SR v Európskej únii

Dlhodobo – e-Government (informatizácia štátnej správy).

Otázky a diskusia

Ďakujem za pozornosť.