FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
UNIVERZITY KOMENSKÉHO, Bratislava

D I P L O M O V Á P R Á C A

Reakcia na bezpečnostné incidenty.

Martin Trnovec

Školiteľ: RNDr. Jozef Vyskoč, PhD.

Bratislava 2005

Vyhlasujem, že som diplomovú prácu vypracoval

samostatne s použitím uvedenej literatúry.

Ďakujem p. RNDr. J. Vyskočovi, PhD rovnako doc. RNDr. Danielovi Olejárovi, PhD.
za odbornú pomoc pri tvorbe diplomovej práce a cenné pripomienky.

1 Obsah

2 Úvod

V dnešnom svete prudko narastá používanie domácich počítačov, notebookov, mobilných telefónov a iných zariadení postavených na informačno-komunikačných technológiách (IKT). IKT systémy umožňujú rapídne zvyšovať produktivitu práce a pomáhajú s riešením úloh, s ktorými sa človek v e-biznise, ale aj v bežnom živote stretáva. Na druhej strane používanie IKT zariadení so sebou prináša aj isté riziká. Poskytujú možnosť na zneužitie verejných, ale aj privátnych informácií prostredníctvom počítačových sietí, v dnešnej dobe hlavne pomocou celosvetovej počítačovej siete - Internet. Problém zneužitia IKT sa nazýva počítačová kriminalita. Ľudia ktorí sa nelegálnym spôsobom snažia získavať informácie z privátnych sietí domácich užívateľov, ako aj zo siete malých, či veľkých spoločností im týmto spôsobujú značné finančné straty. Organizácie využívajúce IKT systémy musia (obr. 1) efektívne reagovať na vzniknutú hrozbu a reakcia na incidenty (v anglickej terminológii známa pod pojmom Incident Response) sa stala neoddeliteľnou súčasťou programov pre informačné technológie. Reakcia na incidenty je predmetom tejto diplomovej práce. Cieľom práce je najskôr zhrnúť všeobecné informácie, potom stanoviť odporúčania v oblasti reakcií na incident a v závere ukázať aplikácie jednotlivých konkrétnych postupov na najrozšírenejších operačných systémoch.

Diplomová práca pozostáva z 10 kapitol a príloh. Prvou kapitolou je úvod.

V druhej kapitole sú uvedené definície základných pojmov, ktoré sa v práci používajú.

V tretej kapitole popisujeme klasifikáciu a kategorizáciu jednotlivých incidentov, potrebnú v metodikách samotnej odozvy na výskyt incidentov.

Zvládnuteľnosť a efektívnosť reakcie na incident je do značnej miery závislá od prípravy pred vznikom incidentu.. O tom, ako sa čo najlepšie pripraviť, ktoré všeobecné zásady by mali byť dodržané, pojednáva kapitola č. 4.

Kapitola č. 5 prináša prehľad o organizačnej štruktúre tímu pre reakcie na incidenty, prehľad funkcií jednotlivých členov tímu, ako aj diskusiu o veľkosti tímu v závislosti od typu incidentu a možností incidentom postihnutej organizácie.

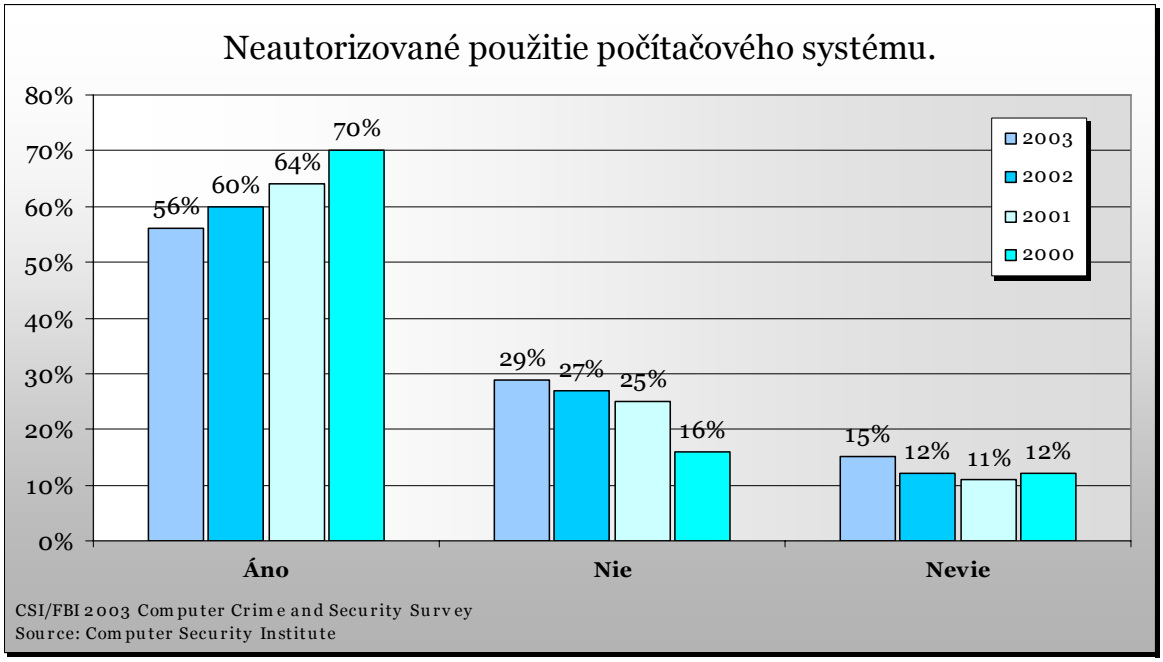
Samotnou metodológiou reakcie na incidenty sa zaoberá kapitola 6, ktorá navrhuje všeobecne aplikovateľné postupy nezávislé od platformy a typu infraštruktúry incidentom postihnutého IKT systému.

Praktické kroky a skripty určené pre platformu Windows NT a UNIX / LINUX, ktoré dopomáhajú tímu pri aplikovaní zásad z kapitoly 6, sú uvedené postupne v kapitolách 7 a 8.

Kapitola 9 obsahuje zoznam užitočných programov obsiahnutých na pripojenom CD-ROM ktoré pomôžu pri samotnej odozve na incident

Výsledky diplomovej práce a niektoré námety pre ďalší výskum v tejto oblasti sú stručne zhrnuté v závere práce.

V prílohe diplomovej práce je uvedená tabuľka, ktorá prehľadne zhŕňa jednotlivé zásady z kapitoly 6 ktorú je možné použiť ako rýchly návod pri praktickom riešení reálneho bezpečnostného incidentu



obr. č. 1. Obrázok ilustruje percentuálne zastúpenie zneužitia počítačového systému na vzorke 1500 náhodne vybratých správcov počítačových systémov.

3 Definície pojmov

V práci je použité veľké množstvo pojmov súvisiacich s oblasťou reakcie na incidenty. Nasledujúca kapitola upresňuje význam jednotlivých pojmov a ich chápanie v súvislosti s reakciou na incidenty. Nakoľko práca predpokladá základné vedomosti v oblasti IKT nebudeme sa venovať definíciam základných pojmov a budeme predpokladať, že ich čitateľ ovláda.

3.1 Aktíva

1. hardvér: procesory, základné dosky, klávesnice, terminály, pracovné stanice, tlačiarne, disky, komunikačné médiá, servery, smerovače;
2. softvér: zdrojové kódy, úžitkové, diagnostické programy, operačné systémy;
3. dáta: vzniknuté počas behu systému, uložené na médiách, archivované dáta, zálohy, protokoly udalostí, databázové dáta;
4. ľudia: užívatelia, správcovia systému;
5. dokumentácia: formuláre, magnetické média, manuály, procedúry;

- *zdroj: RFC 2196 Site Security Handbook*

3.2 Bezpečnostná politika

Formálny zoznam pravidiel, ktoré ľudia alebo procesy vlastniace prístup k aktívam spoločnosti musia dodržiavať.

- *zdroj: RFC 2196 Site Security Handbook*

3.3 Zdroj hrozby

1. vedomý postup zameraný na skúmanie zraniteľnosti
2. situácia alebo postup, ktorý môže podnietiť vznik zraniteľnosti

- *zdroj: Risk Management Guide for Information Technology Systems by NIST (National Institute of Standards and Technology), special publication 800-30*

3.4 Hrozba

Teoretická možnosť že zdroj hrozby využije (náhodne alebo vedome) existujúcu zraniteľnosť

- *zdroj: Risk Management Guide for Information Technology Systems by NIST (National Institute of Standards and Technology), special publication 800-30*

3.5 Incident

Každé narušenie bezpečnostnej politiky spoločnosti, pravidiel používania alebo zaužívaných bezpečnostných praktík.

- *zdroj: Computer Security Incident Handling Guide NIST (National Institute of Standards and Technology), special publication 800-61*

3.6 Riziko

Je funkciou pravdepodobnosti, že zdroj hrozby využije zraniteľnosť v systéme, čo zapríčiní nepriaznivý dopad na organizáciu.

- *zdroj: Risk Management Guide for Information Technology Systems by NIST (National Institute of Standards and Technology), special publication 800-30*

3.7 Útok

Je cieľavedomý pokus o uskutočnenie hrozby.

3.8 Zraniteľnosť

Chyba alebo slabosť v systémových bezpečnostných procedúrach, v návrhu, v implementácii alebo v interných kontrolách, ktorá môže byť náhodne alebo vedome využitá k narušeniu bezpečnostnej politiky.

- *zdroj: Risk Management Guide for Information Technology Systems by NIST (National Institute of Standards and Technology), special publication 800-30*

3.9 Reakcia na incidenty

Reakcia na incidenty (Incident Response) je odpoveď osoby alebo organizácie na incident (alebo inú skutočnosť ohrozujúcu) IKT systém alebo niektoré z aktív organizácie, ktorej cieľom je eliminovať alebo aspoň zmierniť dopad incidentu na aktíva organizácie.

- *Zdroj: SecurityFocus.com (Nov 2000*

3.10 Autorizovaný používateľ

Užívateľ vlastniaci skupinu legálnych prístupov k systému v súlade s bezpečnostnou politikou.

4 Kategorizácia incidentov

Množina incidentov je rozsiahla a neustále sa zväčšuje vďaka výskytu stále nových druhov útokov. Zaoberať sa možnými incidentami a vypracovávať postupy na ich riešenie jednotlivo, je neefektívne. Preto je potrebné incidenty kategorizovať a hľadať spoločné riešenia pre kategórie incidentov, ktoré sa budú mierne upravovať v závislosti od konkrétnych podmienok organizácie/ITK systému.

4.1 Kategorizácia podľa zdroja

Zdrojom incidentu môže byť človek, alebo prírodný jav. Primárne zdroje incidentov sa ďalej delia na podkategórie podľa nasledujúcej tabuľky.

Kategórie incidentov		
Prírodné incidenty	**katastrofy**	požiar, povodeň, zemetrasenie
	mechanické	poškodenie hardvéru, výpadky prúdu
Ľudské incidenty	**úmyselné**	Hackeri, technologická špionáž, teroristický útok
	neúmyselné	neinformovaní užívatelia alebo zamestnanci

4.1.1 Prírodné incidenty

4.1.1.1 Katastrofy

Patria sem všetky extrémne druhy počasia, prírodné fenomény alebo iné druhy katastrof, ktoré môžu spôsobiť škody na infraštruktúre organizácie. Príkladom poškodenia môže byť strata informácií, poškodenie hardvéru alebo dôležitého systému vplyvom prírodných procesov, čím sa znižuje produktivita práce. Týmto incidentom sa ťažko predchádza. Taktiež je ťažké vyvinúť všeobecné efektívne metódy na ich nápravu, ktoré by minimalizovali množinu poškodení. Výskyt incidentu často spôsobuje globálne a závažné narušenie infraštruktúry spoločnosti. Riešenie týchto typov incidentov často súvisí najmä s úplnou obnovou celkového systému, čo je detailne obsiahnuté v „disaster recovery“ dokumentoch jednotlivých postihnutých systémov.

4.1.1.2 Mechanické poškodenia

Patría sem všetky možné poškodenia hardvéru, siete alebo zariadení, ale aj výpadky prúdu. Samotný proces reakcie na incidenty tohto druhu zahŕňa vo väčšine prípadov výmenu poškodeného hardvéru a obnovu dát zo zálohovacích médií. Pre prípad výpadku prúdu sa používajú núdzové generátory napojené na dôležité systémy. Týmto incidentom je oveľa ľahšie predchádzať využitím redundancie rizikových častí informačného systému než odstraňovať ich následky.

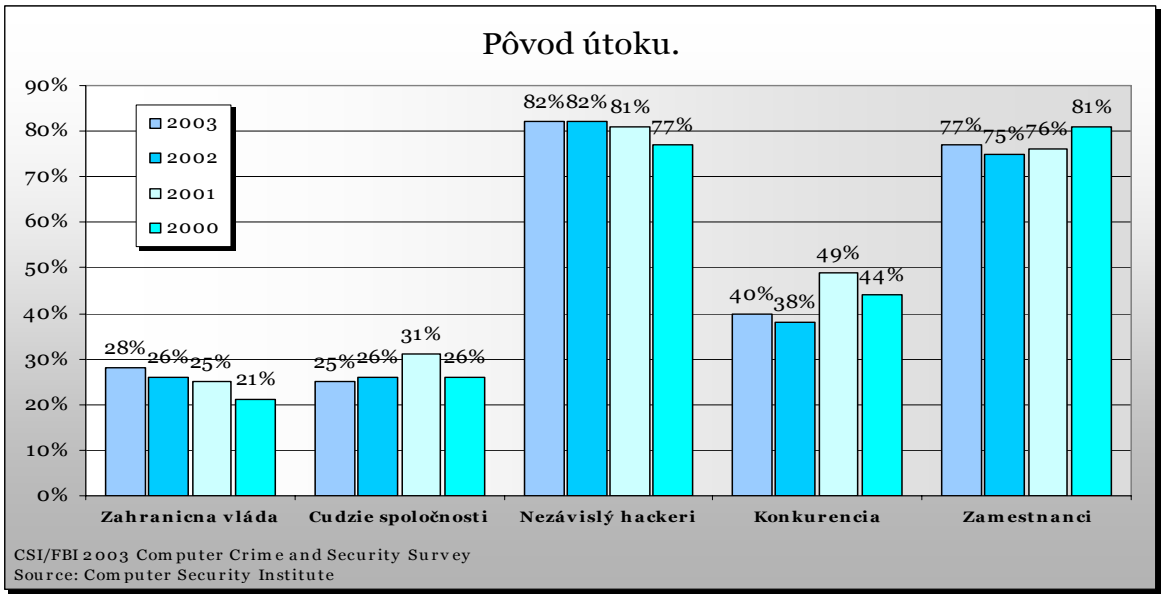
4.1.2 Ľudské incidenty

4.1.2.1 Incidenty spôsobené neúmyselne

Často sa stáva, že samotný incident spôsobil autorizovaný používateľ systému, ktorý si dostatočne neuvedomoval dôsledky svojho konania. Tieto chyby v správaní systému môžu spôsobiť značné škody organizácii, alebo vytvoriť priestor pre vznik závažnej zraniteľnosti systému. Nejedná sa len o manipuláciu a poškodenie dát, ale napríklad aj zmenu nastavenia systému alebo použitie neautorizovaných programov. Množina faktorov, ktorá môže spôsobiť tento druh incidentov, je dosť rozsiahla a je pomerne ťažké efektívne reagovať na všetky z nich.

4.1.2.2 Incidenty spôsobené úmyselne

Tento druh incidentov najčastejšie spôsobujú súčasní alebo bývalí zamestnanci spoločnosti alebo ľudia mimo samotnej organizácie. Ak je incident spôsobený človekom alebo ľuďmi z vnútra organizácie, často tým sledujú nejaký primárny cieľ a tieto osoby väčšinou majú legálny prístup k systému. Ich výhodou je detailná znalosť infraštruktúry a zraniteľností systému. Tento útok môže spôsobiť značné škody a detekcia a reakcia na tento druh útoku je mimoriadne náročná. Bývalí zamestnanci sa často snažia sabotovať a znefunkčniť systém, prípadne napáchať rozsiahle škody.



obr. č. 2. Obrázok ilustruje percentuálne rozlíšenie pôvodu útokov za jednotlivé uvedené obdobia.

4.2 Špecifikácia druhu incidentu

Okrem pôvodu (zdroja) sa incidenty líšia aj svojimi účinkami na samotnú infraštruktúru postihnutej/zasiahnutej organizácie. Nasledujúca tabuľka uvádza kategorizáciu jednotlivých incidentov podľa spôsobu ich pôsobenia.

Druhy incidentov	
Odmietnutie služby (DoS)	Nastáva v prípade, keď incident spôsobí znefunkčnenie systému alebo zahltí priepustnosť siete.
Neautorizovaný kód	Zahŕňa prípady, keď vírus napadne program alebo sa odhalí vážna systémová zraniteľnosť, ktorá naruší funkčnosť a celistvosť systému.
Zneužitie	Vzniká vtedy, keď užívateľ alebo útočník použije systém v rozpore s bezpečnostnou politikou.
Poškodenie	Zahŕňa prípady poškodenia, modifikovania alebo úplnej straty aktív.
Neautorizovaný prístup	Nastáva vtedy, keď osoba alebo proces získa logický alebo fyzický prístup k systému, aplikáciám alebo iným aktívam, ktorý je v rozpore s bezpečnostnou politikou.

Popíšeme teraz jednotlivé kategórie incidentov podrobnejšie.

4.2.1 Odmietnutie služby (DoS)

Vo všeobecnosti ide o najjednoduchšie uskutočniteľný útok, ktorý má úzky súvis s využívaním počítačových sietí. Je spôsobený neštandardným tvarom paketov, alebo neošetrenými, neočakávanými vstupmi v samotnom softvéri, ktorý organizácia používa. Umožňuje to nedostatočne bezpečný návrh architektúry TCP/IP protokolu.

Útok je nebezpečný v tom, že ho môže uskutočniť aj človek s malými skúsenosťami v odbore počítačových sieti. Dôsledkom je, že zasiahnutý počítač prestane obsluhovať požiadavky na službu, ktorú poskytuje. V prípade, že sa jedná o chvíľkový útok, ide o zanedbateľné riziko, ale naopak trvalý a intenzívny útok môže spôsobiť stratu prestíže, nespokojnosť zákazníkov a samozrejme aj nezanedbateľné finančné straty.

DoS útoky rozdeľujeme na tri kategórie:

- **chyby v návrhu programu alebo protokolu** – ide o prípad, keď TCP/IP paket obsahuje nastavenie či už v hlavičke alebo tele, ktoré spôsobí chybu vykonávania programu (samotným pádom programu, alebo zastavením jeho činnosti). Na útok často stačí len úzka množina paketov a efekt býva veľmi rýchly.
- **pretečenie zásobníka** – podobne ako v predchádzajúcom prípade, parameter poslaný programu spôsobí, že program zastaví svoju obvyklú činnosť, následne spustí nechcený kód, alebo pohltí všetky voľné zdroje, ktoré sú dostupné, a spôsobí tým nefunkčnosť celého systému.
- **zahltenie siete** – zneužitím architektúry siete sa môže dosiahnuť, že sieť je zapĺňaná nereálnymi požiadavkami na službu, ktoré sú generované programom útočníka. To spôsobuje, že reálne požiadavky na službu sú doručované pomaly alebo vôbec.

4.2.2 Neautorizovaný kód

Vzniká vtedy, ak útočník odoslaním neautorizovanej správy môže získať prístup do systému alebo k službe, ktorú systém obsluhuje. Pôvod tohto útoku vzniká nedostatočnou kontrolou kvality softvéru zabezpečujúceho jednotlivé služby. Objavenú chybu v bezpečnosti softvéru často využívajú autori vírusov. Najnebezpečnejšia je práve forma vírusov, lebo vo veľmi krátkom čase dokáže využitím tejto chyby nakaziť veľkú množinu počítačov. Príkladom môže byť vírus **Win32/SQL.Slammer,** ktorý napádal počítačové systémy disponujúce aplikáciami **MS SQL Server 2000** a **MS Desktop Engine 2000.**

4.2.3 Zneužitie

Vzniká keď užívateľ využíva zdroje na iné než na stanovené účely definované bezpečnostnou politikou. To zahŕňa prípady, keď útočník využíva svoje alebo cudzie prístupy v systéme k svojmu osobnému prospechu, napr. na získanie dôverných informácií. Zneužitie sa ťažko odhaľuje, nakoľko veľmi často ide o interných, legitímnych užívateľov s legitímnym prístupom k sieti.

4.2.4 Poškodenie

Nastáva vtedy, ak útočník modifikuje, poškodí alebo zničí dôležité aktíva informačného systému. Ide buď o zmenu konfigurácie, samotnú modifikáciu informácii uložených v zasiahnutom systéme, poškodenie hardvéru alebo infraštruktúry organizácie. Útok rovnako môže nastať z vonkajšieho, ako aj vnútorného prostredia.

4.2.5 Neautorizovaný prístup

Ide o najzávažnejší typ incidentu, pri ktorom býva náročné odhadnúť kedy incident nastal a teda ako dlho má útočník kontrolu nad systémom. Dôvodom pre útok býva získanie informácií, ktoré sa nachádzajú v systéme, alebo použitie systému ako zdroj ďalšieho plánovaného útoku.

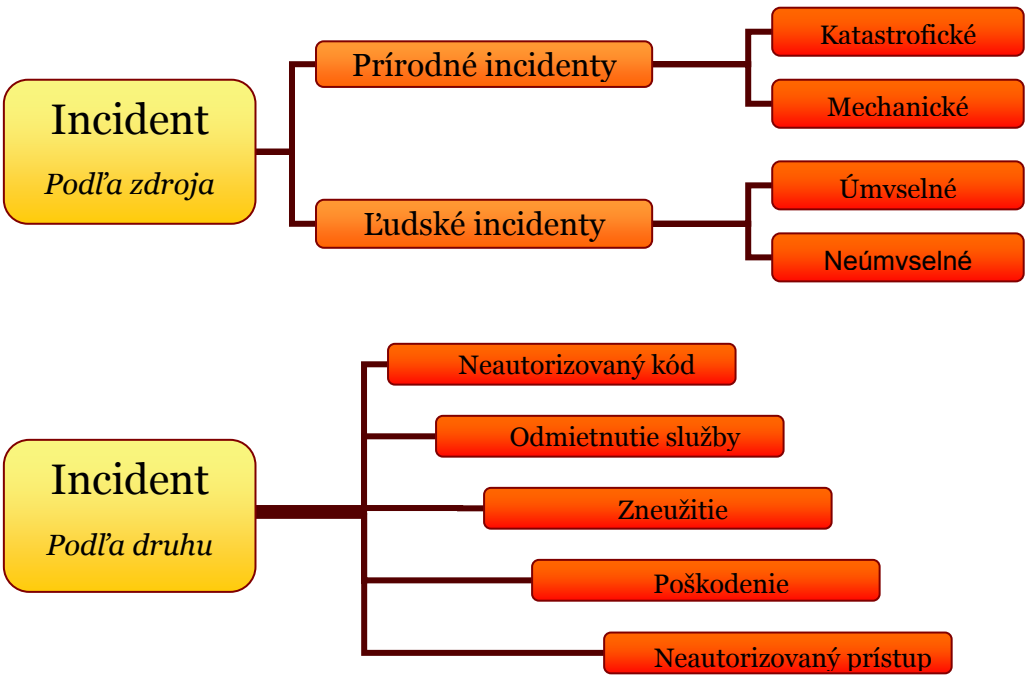
Tento útok je často spojený z nasledovnou činnosťou:

- **zbieranie informácií a hesiel** – Útočník môže použitím špecializovaného softvéru sledovať a získavať informácie a dáta prechádzajúce systémom.

Informácie mu môžu poskytnúť ďalšie možnosti na získavanie kontroly nad systémom.

- **poškodenie dát** – V tomto prípade útočník poškodzuje alebo obmieňa dáta jednotlivých programov alebo samotného systému.
- **stanica na ďalší útok** – Často sa stáva, že napadnutý systém nebýva koncovým cieľom útočníka. Systém použije ako medzistanicu na ďalší plánovaný útok. Výhoda pre útočníka spočíva v náročnejšom získaní skutočného miesta a pôvodu útoku.

obr. č. 3. Diagram schematicky znázorňuje rozdelenie jednotlivých typov incidentov do kategórií.



5 Príprava reakcie na incident

Celý výsledok priebehu reakcie na incident je značne závislý od jej prípravy. Kvalitná príprava využitím predpripravených nástrojov môže zaručiť bezproblémový proces nápravy dôsledkov incidentu. Každý typ incidentu (viď Klasifikácia a kategorizácia incidentov) je špecifický a príprava na ich výskyt závisí od celkovej architektúry infraštruktúry, ako aj použitej technológie. Preto nasledujúca časť ponúka všeobecne aplikovateľné postupy prípravy, ktoré pomáhajú zvládať jednotlivé druhy incidentov a prenecháva prípravu špecializovaných častí systému pre reakciu na incident na ich správcu.

5.1 Popis systému

V rámci všeobecnosti budeme predpokladať, že systém pozostáva z heterogénnej počítačovej siete. Samotná sieť obsahuje skupinu pracovných staníc používateľov a skupinu počítačových serverov. Servery môžu byť umiestnené v rovnakej sieti alebo oddelene v demilitarizovanej zóne (DMZ) pomocov iných hárdverových zariadení.

Servery pritom budú obsluhovať najrozšírenejšie služby ako mail server, databázový server, súborový server, server spracovávajúci tlačové úlohy a webový server.

Dáta, ktoré budú v celkovom systéme obsahnuté, budú dokumenty o vedení firmy, zákaznícke dáta, riadenie procesov, personálne dáta, know-how technológie, zmluvné dokumenty, dáta ekonomického charakteru a iné súbory súvisiace s predmetom činnosti spoločnosti.

Osoby, ktoré budú prichádzať do styku budú používatelia, správcovia systému a auditori systému.

Samotná organizácia má vypracovanú bezpečnostnú politku, identifikované jednotlivé hrozby a zraniteľnosti systému, prijaté smernice na správu rizík a má vyčlenený tím ľudí zodpovedajúci za správny chod systému.

5.2 Identifikácia aktív

V rámci spoločnosti sa nachádzajú primárne aktíva - sú to tie aktíva, ktoré sú životne dôležité pre jej správne fungovanie, aktíva ktoré ich podporujú - tie

nazývame sekundárne, a taktiež aktíva, ktorých funkcia nie je životne dôležitá. Je ťažké ochraňovať všetky systémy naraz a preto je vhodné ešte pred vznikom samotného incidentu správne identifikovať primárne aktíva, ktoré majú byť prednostne chránené.

5.3 Príprava zabezpečenia jednotlivých aktív

Po dôkladnej identifikácii primárnych aktív je dobré vykonať kroky, ktoré nám umožnia efektívne a rýchlo zvládnuť prípadný výskyt incidentu.

- v prípade, že primárne aktíva súvisia z dátami v podobe súborov vykonať kontrolné súčty týchto súborov
- dôkladný a detailný monitoring udalostí prebiehajúcich v systéme a ich zaznamenávanie;
- nastavenie a zabezpečenie serveru;
- zálohovanie dôležitých dát a ukladanie kópie na bezpečnom mieste;
- pravidelné školenie užívateľov o bezpečnosti informačných systémov;
- určenie tímu pre reakciu na incident;
- vytvorenie pomocnej sady nástrojov na odstraňovanie incidentu.

zdroj: RFC 2196 Site Security Handbook

5.4 Vytváranie kontrolných súčtov

Pri vzniku incidentu, najmä ak sa jedná o prienik do systému, je prvoradé určiť, ktoré súbory boli zmenené alebo nahradené útočníkom. Parametre súboru v systéme ako veľkosť, dátum a čas vzniku a dátum a čas modifikácie súboru sa dajú ľahko sfalšovať, preto je nutné použiť lepšiu metódu - hašovacie algoritmy, ktoré vytvárajú „odtlačky“ súboru vzhľadom na ich obsah. Porovnaním predtým získaného kontrolného súčtu originálneho súboru s kontrolným súčtom aktuálneho súboru je možné zistiť, či došlo k jeho modifikácii.

Najčastejším dnes používaným algoritmom je MD5, vytvorený Rosom Rivestom a publikovaný v apríli 1992 ako RFC 1321. Výhodou tohto algoritmu je, že vytvára 128-bitové kontrolné súčty a je použiteľný ako pre platformu LINUX, tak aj pre WINDOWS.

Existuje množstvo nástrojov a skriptov, ktoré proces vytvárania a archivovania kontrolných súčtov urýchľujú a automatizujú. Výstupom býva najčastejšie jeden súbor obsahujúci kontrolné súčty dôležitých súborov. Ich uloženie na pevnom disku počítača nie je vhodné vzhľadom na ich možnú modifikáciu útočníkom. Preto je potrebné ich uložiť na vhodnom mieste mimo počítača, najčastejšie na CD alebo iné zálohovacie médium, ktoré je uložené na bezpečnom mieste, mimo dosahu potenciálneho útočníka.

5.5 Monitoring systému

Pri výskyte a analýze incidentu je potrebné zistiť, čo sa vlastne v systéme udialo. Neoceniteľnú pomoc nám pri tom poskytujú protokoly udalostí pochádzajúce priamo z postihnutého počítača.

Medzi všeobecné pravidlá, ktoré je potrebné dodržiavať pri monitoringu systému, patria

- zaznamenávanie výskytu udalostí (logovanie) na dôležitých službách alebo aplikáciách v systéme
- ukladanie výsledkov monitoringu na bezpečné miesto
- záloha a archivácia výsledkov monitoringu.

Systém WINDOWS aj LINUX umožňujú vo svojom nastavení vykonávanie detailného monitoringu.

V operačnom systéme LINUX je to prostredníctvom služby *syslog*, ktorá umožňuje filtrovanie protokolovaných udalostí a ich posielanie na externý počítač. V dnešnej dobe je kapacita diskov dostatočná a preto sa odporúča zaznamenávanie všetkých udalostí a ich ukladanie na externý centrálny monitorovací server.

V systéme WINDOWS sa monitoring aktivuje a nastavuje prostredníctvom centrálnej doménovej bezpečnostnej politiky (DOMAIN SECURITY POLICY),

alebo prostredníctvom lokálnej bezpečnostnej politiky (LOCAL SECURITY POLICY). Na rozdiel od systému LINUX sa výsledky auditu ukladajú na lokálnom disku, čo je možné zmeniť prostredníctvom externých programov, ako napríklad *NTSyslog*, ktorého protokol je kompatibilný so službou *syslog* v systéme LINUX a teda je možné použiť ten istý centrálny monitorovací server v prípade heterogenity operačných systémov v sieti.

Takmer každá aplikácia poskytujúca nejaký druh služby umožňuje vykonávanie monitoringu (logovania), ktorý je vhodné správne nastaviť. Príkladom je HTTP, FTP, SMTP server. Formát výstupu, ako aj nastavenia sú však individuálne závisle od typu použitého softvéru.

5.6 Zabezpečenie servera

Typickým príkladom primárnych aktív je práve skupina serverov obsluhujúcich nejakú službu. Nakoľko je vždy lepšie incidentu predchádzať, ako znášať jeho dôsledky, je veľmi dôležité čo najviac redukovať pravdepodobnosť vzniku incidentu zo strany útočníka alebo procesu. Je ťažké predchádzať prírodným incidentom (najmä katastrofickým), ale proti vzniku ľudských incidentov sa dajú vytvoriť vhodné opatrenia. Medzi základné patria:

- **inštalácia firewallov, IDS systémov**
- **správna konfigurácia smerovačov**
- **vytváranie VPN sietí a šifrovanie dátovej komunikácie**
- **dôkladné monitorovanie siete**
- **vyžadovanie autentifikácie.**

5.7 Záloha dôležitých dát

Pravidelné zálohovanie dát a kontrola výsledkov zálohovania je podstatné pre efektívnu reakciu na incident. Záloha pomáha určiť príčiny vzniku incidentu, ako aj následnú obnovu systému. Prioritne by mali byť zálohované dáta, ktoré súvisia z primárnymi aktívami spoločnosti. Každý systém WINDOWS aj LINUX, umožňuje vykonávať zálohovanie prostredníctvom programov. Príkladom pre systém LINUX

sú napr. *dump, dd, tar* a pre systém WINDOWS *ntbackup,* alebo použitie špeciálnych zálohovacích programov od externých dodávateľov.

5.8 Školenie užívateľov v oblasti bezpečnosti systémov

Zabezpečenie systému je také silné ako je silný jeho najslabší článok.Človek (napríklad používateľ-neinformatik; riaditeľ, jeho sekretárka) býva neraz tým najslabším článkom systému. Prostredníctvom „social engineering“ útočníci často získavajú detailné informácie o vedení a konkrétnych krokoch súvisiacich s výkonávaním bezpečnostnej politiky od užívateľov, ktorí si často neuvedomujú následky svojho konania. Podobne by mali používatelia vedieť, ako sa správať v prípadne nezvyčajnosti správania sa systému, ktoré spozorovali a čo majú robiť v prípade výskytu incidentu.

6 Tím pre reakciu na incidenty

Kľúčovým úspechom pre dobré zvládnutie incidentu akéhokoľvek druhu je mať kohézny tím ľudí, ktorý má pripravené jednotlivé postupy, procedúry a metodiky na čo najjednoduchšie zvládnutie danej situácie. Je veľmi dôležité, aby boli v tíme zastúpené všetky odvetvia firmy, ktoré sú nápomocné pri odstraňovaní a vyšetrovaní incidentu. Úlohou tímu nie je len priama reakcia na incidenty, ale aj príprava systému na ich predchádzanie a v neposlednom rade aj ich skorú diagnostiku.

Tím pre reakcie na incidenty vykonáva viacero samostatných úloh, ktoré by si mal rozčleniť medzi jednotlivých členov podľa ich špecializácie. Samotné úlohy tímu pre reakcie na incidenty môžeme zhrnúť do nasledovných bodov:

- **vykonávanie dozoru nad systémom a neustály monitoring siete**
- **samovzdelávanie a aplikovanie záplat na známe a novo odhalené zraniteľnosti systému**
- **príprava jednotlivých počítačov a samotnej siete**
- **príprava procedúr a pracovných postupov pri výskyte incidentu**
- **tvorba a získavanie pomocných nástrojov a programov, ktoré napomáhajú pri reakcii na incidenty**
- **vyšetrovanie incidentu a jeho dokumentácia**
- **zbieranie dôkazov o pôvode a druhu incidentu na neskoršie vyvodenie dôsledkov**
- **náprava a minimalizácia škôd vzniknutá následkom incidentu.**

Samotný tím môžu tvoriť interní zamestnanci firmy, ale nie je vylúčená možnosť pôsobenia externých spolupracovníkov, ktorí možu pomôcť pri zvládnutí špecifických foriem incidentu. (napr. špecialisti na vírusové infekcie).

6.1 Jednotlivé funkcie členov tímu pre reakcie na incidenty

Nasledujúce rozdelenie ukazuje, ako by mal fungovať úplný – ideálny tím pre reakciu na incidenty. Sú v ňom zastúpené všetky zložky organizácie, ktorých činnosť môže prispieť k náprave vzniknutého incidentu. V závislosti od veľkosti organizácie by si sama mala určiť, aká bude konečná veľkosť tímu, k čomu by mala pomôcť záverečná diskusia obsiahnutá v tejto kapitole.

6.1.1 Primárni členovia tímu

Skupina zahŕňa funkcie tvoriace výkonnú časť tímu pre reakcie na incidenty, ich existencia je nevyhnutná pre samotnú odozvu.

6.1.1.1 Vedúci tímu pre reakciu na incident

Ako v každej oblasti, aj tu musí byť osoba poverená zodpovednosťou za vykonávanie jednotlivých krokov pri reakcii na incident. Vedúci tímu pre reakciu na incident je poverený koordináciou aplikovania pripravených procedúr, ako aj novo aplikovaných postupov, ktoré neskôr po osvedčení môžu viesť k úprave existujúcich procedúr určených pre budúce použitie.

6.1.1.2 Vedúci tímu pre priamu odozvu na incident

Jeho úlohou je zodpovednosť za koordináciu samotnej odozvy pri reakcii na incident. Pretože incident sa často skladá zo skupiny menších incidentov, ktoré vznikli ako následok iného incidentu, môže mu byť pridelená zodpovednosť za určitú skupina súvisiacich incidentov, alebo v prípade komplexnosti a náročnosti incidentu iba jeden konkrétny incident. Taktiež zastupuje ľudí v rámci svojho tímu a komunikuje s ostatnými vedúcimi v rámci koordinácie krokov celého tímu. V prípade vyskytnutia incidentu malého rozsahu, môže byť funkcia vedúceho tímu pre reakciu na incident a vedúceho tímu pre priamu odozvu na incident zastúpená jednou osobou.

6.1.1.3 Členovia samotného jadra tímu pre reakcie na incident

Tak, ako je dôležité mať jednotlivých vedúcich, je dôležité mať aj samotné osoby vykonávajúce kroky potrebné pri reakcii na incident.

6.1.2 Pridružení členovia tímu

Patria sem členovia veľkej skupiny odvetví a oddelení v samotnej organizácii, ktorí pomáhajú zmiernovať následky incidentu resp. uľahčujú reakciu na incident členom samotného jadra tímu pre reakcie na incident. Nie sú však členmi samotného jadra a ich existencia pri incidentoch menšieho rozsahu, resp. pri menších organizáciách nie je nevyhnutná.

6.1.2.1 IT kontakt

Jeho úlohou je koordinácia komunikácie medzi tímom pre reakciu na incidenty a zvyškom IT odborníkov. Jeho právomoc neumožňuje zásah alebo technické poradenstvo pri odozve na incident, naopak má za úlohu sprostredkovať ľudí zodpovedajúcich za jednotlivé časti systému.

6.1.2.2 Právny zástupca

Je často pracovníkom firmy, ktorý má za úlohu zabezpečiť právnu stránku reakcie na incident. Jeho úlohou je určiť, ako postupovať v procese reakcie na incident, aby sa minimalizovalo poškodenie právnych dôkazov a maximalizovala možnosť dostihnúť vinníka. Je dôležité celkové sledovanie, aby sa v procese reakcie na incident nedostala firma do konfliktu s právnymi vzťahmi platnými v postihnutej spoločnosti. Taktiež koordinuje ostatné právne kroky a komunikáciu s inými oddeleniami alebo s osobami mimo organizácie.

6.1.2.3 Hovorca organizácie

Mala by to byť osoba z oddelenia pre styk s verejnosťou. Jej úlohou je chrániť obraz spoločnosti, ktorý môže byť narušený v dôsledku incidentu. Táto osoba nemusí priamo vystupovať pred médiami a verejnosťou, ale podieľa sa a je zodpovedná za tvorbu jednotlivých vyhlásení spoločnosti. Taktiež riadi a koordinuje postup každého oddelenia, ktoré sa dostáva do styku s verejnosťou a s médiami.

6.1.2.4 Manažment

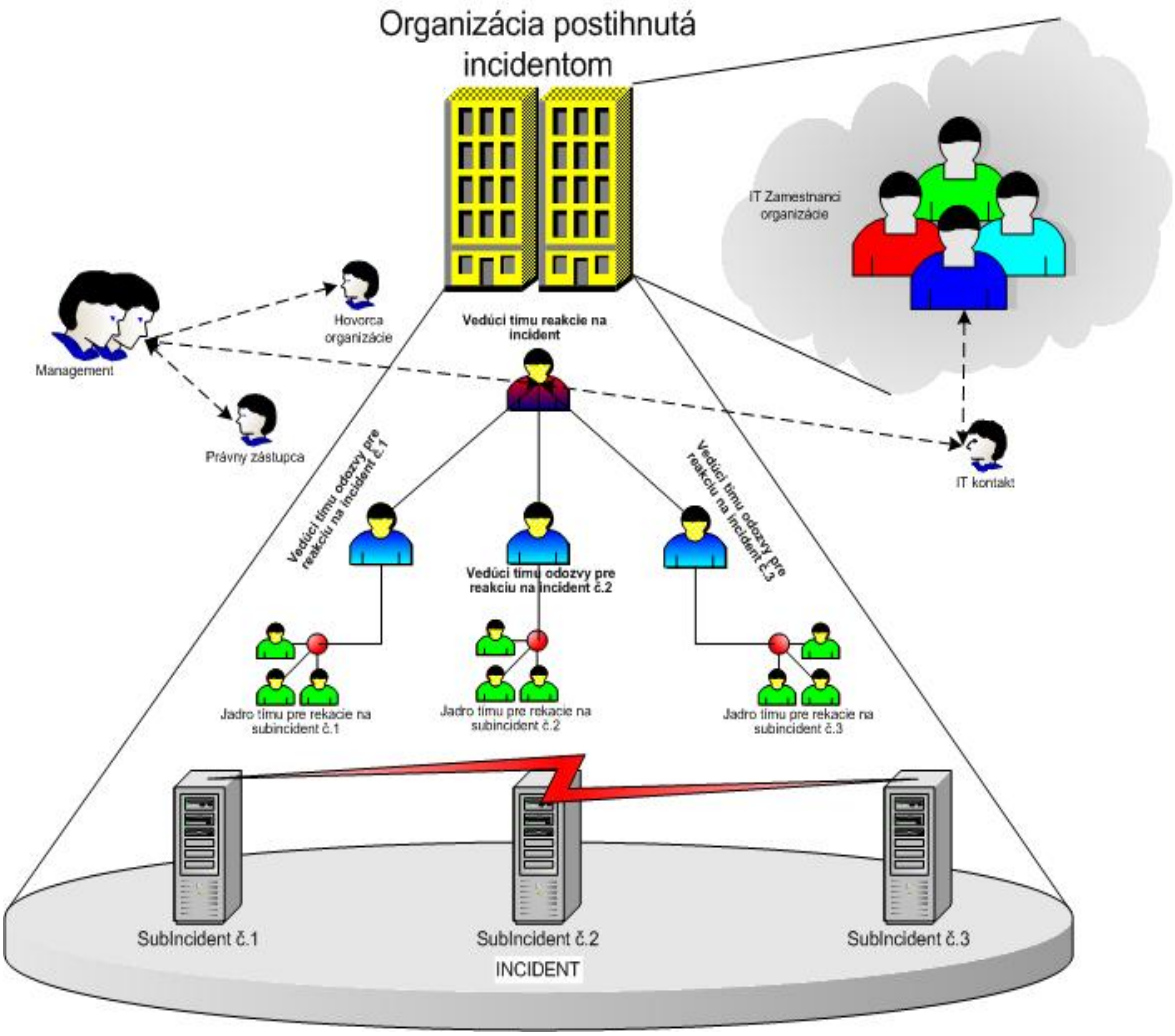
Jeho záber činnosti pri reakcii na incident je od najmenších oddelení až po oblasť celej organizácie. Úlohou manažmentu je vytvoriť jednotlivé odhady dopadu incidentu ako z hľadiska finančného, tak aj z nefinančného. Jeho zainteresovanie do činnosti často závisí od druhu a rozsahu incidentu. Riadi oddelenie hovorcu,

rozhoduje o tom, ktoré informácie môžu byť zverejnené a ktoré naopak nie. Často svoju činnosť koordinuje s právnym oddelením.

6.1.3 Veľkosť tímu pre reakciu na incidenty

Samotná veľkosť tímu pre reakciu na incident je závislá od dvoch hlavných faktorov: od závažnosti incidentu a od veľkosti organizácie. Taktiež zastúpenie jednotlivých funkcií v tíme pre reakciu je podmienená existenciou primeraných oddelení v postihnutej spoločnosti. V menších firmách môžu byť jednotlivé funkcie zjednotené a zastúpené jednou osobu. Minimálna veľkosť tímu by mala byť dve osoby, nakoľko nie je možné vylúciť možnosť, že za vznik incidentu je zodpovedná práve osoba patriaca do tímu pre reakcie na incidenty.

Najdôležitejšiu úlohu v tíme tvorí vedúci tímu pre reakciu na incident a členovia jadra tímu pre reakciu na incident. V menšej spoločnosti môžu byť úlohy vedúceho tímu reakcie na incident a vedúceho tímu priamej odozvy na incident zjednotené a zastúpené osobou z manažmentu organizácie. Jadro tímu by mali tvoriť hlavne osoby zodpovedné za správu incidentom postihnutých systémov. V spoločnosti, ktorej rozsah činnosti a veľkosť to umožňuje, je vhodné, aby v tíme boli zastúpené aj funkcie z množiny pridružených členov tímu, čo napomáha zvládnuť ostatné aspekty incidentu. Táto kapitola ukazuje ako by mal existovať ideálny stav zloženia tímu reakcie na incidenty. Nakoľko takýto rozsah veľkosti tímu je pre samotnú organizaciu finančne náročný, stanovenie konečnej veľkosti a zastúpenie jednotlivých oblastí ponechávame už na samotnú organizáciu.



obr. č. 4. Schéma znázorňuje organizačné rozdelenie ľudí v tíme pre reakciu na incidenty. Plnou čiarou je znázornená priama podriadenosť, prerušovanou čiarou je znázornený komunikačný kanál medzi jednotlivými funkciami.

7 Metodológia plánu reakcie na incident

Vzhľadom na špecifickosť prírodných incidentov (viď kap. „Klasifikácia a kategorizácia incidentov“) sa nasledujúca kapitola bude zaoberať hlavne metodológiou reakcie na ľudské - úmyselné incidenty vyskytnuté na počítačových systémoch. Niektoré body z metodiky je však možné aplikovať aj pri ostatných druhoch incidentov.

Každý člen tímu pre reakciu na incident (viď kap. „Tím pre reakciu na incidenty“) musí vedieť, kedy má čo vykonať, aby sa predišlo zbytočným škodám. V procese reakcie na incident nie je zainteresovaný len samotný tím pre reakciu na incidenty, ale aj všetky zložky a oddelenia spoločnosti postihnutej incidentom. Samotní zamestnanci by mali upozorniť na neobvyklú činnosť alebo spôsob fungovania systému. Plán reakcie na incidenty by nemal byť utajovaným dokumentom, ale všeobecne známym nariadením pre všetkých IT špecialistov, aby sa dokázali efektívne zapájať, ale aj efektívne modifikovať postup pre reakcie na incidenty. Samotný proces sa skladá z nasledovných častí:

- **detekcia a odhad incidentu**
- **informovanie o incidente**
- **minimalizácia ďalšieho poškodenia**
- **identifikácia rozsahu incidentu a miery poškodenia**
- **formovanie plánu odstraňovania následkov incidentu**
- **ochrana dôkazov**
- **notifikácia externých organizácii**
- **obnova poškodeného systému**
- **zhrnutie vzniknutej dokumentácie o incidente**
- **výpočet vzniknutej škody**
- **aktualizácia plánov pre reakciu na incident a dodatočné zabezpečenie systému.**

zdroj: Microsoft corp.: Responding to Incidents; Incident Response: Investigating computer crime. Chris Prosise, Kevin Mandia, 2002.; www.securityfocus.com; Brian H. Karney CISSP Guidance Software Institution Senior Security Engineering

7.1 Detekcia a odhad incidentu

O výskyte incidentu sa môžeme dozvedieť mnohými spôsobmi. Detekciou neobvyklej aktivity v systéme, vykonávaním bežnej údržby v systéme administrátorom, alebo dnes často používanými "systémami na detekciu prieniku" (IDS). Tento systém nás však môže upozorniť aj na falošný incident, ktorý je často spôsobený veľkou citlivosťou IDS systému, preto je niekedy ťažké rozoznať či ide o skutočný incident. Základné postupy zahŕňajúce samotnú fázu detekcie incidentu môžeme zhrnúť do nasledovných bodov:

- vykonanie počiatočných krokov na rozlíšenie pravosti detekovaného incidentu a eliminácia falošných incidentov
- počiatočný odhad závažnosti a typu incidentu; tento odhad je potrebný v procese informovania o incidente a stanovenie tak dostatočne veľkého tímu, ktorý bude reagovať na incident
- dokumentácia všetkých vykonaných postupov a zistení, táto bude neskôr použitá pri aktualizácii plánov pre reakciu na incident a umožňuje tímu pre reakciu na incidenty získať predstavu o vzniknutej situácii; pri dokumentácii incidentu je dôležité uviesť minimálne nasledujúce údaje:
    - aktuálny dátum a čas
    - kto, resp. aký prostriedok viedol k pravdepodobnej detekcii incidentu
    - odhad, resp. presné určenie vzniku incidentu
    - akého systému sa incident týka
    - uvedenie kontaktu na osoby, ktoré vykonali dokumentáciu

7.2 Informovanie o incidente

Akonáhle je v systéme detekovaný pravý incident, je veľmi dôležité čo najrýchlejšie informovať vedúceho tímu pre reakciu na incidenty alebo jeho zástupcov. Na základe závažnosti incidentu sa následne vyberie z celkového tímu dostatočné množstvo ľudí na zvládnutie incidentu (viď kap. "Tím pre reakciu na incidenty"). To napomôže k tomu, aby bol tím dostatočne pružný a schopný efektívne reagovať na incident a tým sa minimalizoval rozsah vzniknutých škôd. Dôležité je, aby sa informácia o vzniknutom incidente rozšírila len medzi kompetentné osoby, čo znižuje možnosť zainteresovania médií a následné

využitie vzniknutej situácie konkurenčnými spoločnosťami, až do úplného zotavenia sa zo vzniknutého incidentu. O tom, kto má byť informovaný rozhoduje samotný vedúci tímu pre reakciu na incident, k čomu mu pomôžu informácie získané o vzniknutom incidente z prvej fázy reakcie na incident.

7.3 Minimalizácia ďalšieho poškodenia

Prioritou každej organizácie a ľudí zainteresovaných do reakcie na incident je jeho rýchle a úspešné zvládnutie, aby organizácia utrpela čo najmenšiu stratu. Skutočná odozva na incident je však závislá od typu a rozsahu incidentu, ako aj od samotnej štruktúry organizácie. RFC 2196 definuje základné priority, ktoré by mali byť dodržané pri odstraňovaní následkov škôd.

1. **Ochrana ľudského života a bezpečnosti ľudí -** ľudský život a bezpečnosť osôb má vždy najvyššiu prioritu v akejkoľvek oblasti. Dôležité je, aby sa zabránilo vzniku aj najmenšieho rizika, ktoré by mohlo viesť k ohrozeniu ľudí.
2. **Ochrana dôverných a citlivých dát -** ešte pred vznikom incidentu musí byť jasne definované, ktoré dáta sú dôverné alebo cenné a majú byť prioritne chránené. To umožňuje stanoviť prioritu jednotlivých krokov pri samotnej reakcii na incident.
3. **Ochrana ostatných dát, vrátane osobných, vedeckých, manažérskych dát -** ostatné dáta sú tiež hodnotné a preto by mali byť tiež chránené. Je preto dôležité, aby sa po dostatočnom zabezpečení dát spadajúcich do kategórie cenných, prešlo k ochrane zvyšných dát.
4. **Ochrana hardvéru a softvéru voči útokom -** to zahŕňa ochranu voči strate alebo obmene dát, alebo fyzickému poškodeniu hardwaru.
5. **Minimalizácia poškodenia počítačových zdrojov a procesov**

7.3.1 Možnosti minimalizácie poškodenia

Najjednoduchším spôsobom je odpojenie napadnutého systému od siete a zabránenie tak šíreniu sa ďalšieho poškodenia. Pred uskutočnením tohto kroku je dôležité ubezpečiť sa o tom, že útočníci už nemôžu získať prístup k systému inou cestou. Toto rozhodnutie však nebýva vždy najlepším riešením i keď vedie k najväčšej minimalizácii ďalších spôsobených škôd. Rozhodnutie závisí od

dôležitosti napadnutého systému a od možnosti vzniku ďalšej škody v prípade neodpojenia, prípadne straty vzniknutej nefunkčnosťou, napr. ponúkanej služby, ktorá je sprostredkovaná napadnutým systémom.

Niekedy je naopak dôležité, aby sa útočník nedozvedel o práve prebiehajúcej odozve na incident, čo umožňuje získanie väčšieho počtu dôkazov o pôvode incidentu, resp. o identite útočníka. To môže byť náročné, najmä ak ide o útok pochádzajúci z interného prostredia. Útočník sa môže dozvedieť o práve prebiehajúcich protiopatreniach, napr. ak sa uskutočňuje núdzové zasadanie tímu pre reakcie na incidenty, alebo prostredníctvom iných vnútroorganizačných kanálov.

Inou možnosťou, ktorá umožňuje získanie ďalších informácii a dôkazov, je **izolácia napadnutého** počítača a odpojenie nepostihnutej časti systému od izolovaného systému. Útočník tým získava menšiu možnosť identifikácie a odchytenia ďalších možných prístupov a iných citlivých dát.

Poslednou možnosťou je metóda označovaná ako **FISHBOWLING**. Tá je však náročná na technické zabezpečenie tímu pre reakciu na incidenty. Metóda je založená na dôkladnom filtrovaní prevádzky systému a kontrole prebiehajúcej komunikácie. Filtrovanie zabráni ďalšiemu napadnutiu nepoškodených systémov, ale nebráni ich funkcii pre zvyšok nepostihnutej siete. Cieľom je vytvoriť dokonale filtrovanú oblasť, ktorá z hľadiska útočníka vyzerá ako bežne fungujúci systém. Na dosiahnutie tohto stavu je často nutné zmeniť topológiu siete a blokovanie prístupov, ako aj dosadenie falošných prvkov do systému simulujúcich bežnú prevádzku.

Pred začatím samotnej odozvy sa odporúča urobiť duplikáciu systému (čo však môže byť značne časovo náročné a teda môže byť vynechaná) pre neskoršiu analýzu a vyšetrovanie pôvodu a identity útočníka a zmenu všetkých dôležitých hesiel zabezpečujúcich prístup k systému. Dôležité je, aby sa zistil prístupový bod útočníka k poškodenému systému a tým sa zabránil vznik podobných incidentov. To môže zahŕňať úpravu smerovacích tabuliek, dodatočné zabezpečenie firewallu, alebo odpojenie alternatívnych prístupových kanálov, akým je napr. modem.

7.4 Identifikácia rozsahu incidentu a miery poškodenia

Aby bol zákrok vedúci k náprave incidentu efektívny, je dôležité stanoviť rozsah závažnosti incidentu a určiť množinu poškodených systémov. Je dôležité stanoviť nasledovné:

- **zistiť typ incidentu -** zaradiť ho do kategórie (viď kap. „Klasifikácia a kategorizácia incidentov“)
- **zistiť pravdepodobné miesto pôvodu útoku**
- **zistiť zámer útoku –** či bol útok nasmerovaný priamo na poškodenú organizáciu, resp. bol útok zameraný na získanie alebo poškodenie konkrétnych dát, alebo či ide iba o náhodný útok
- **zistiť rozsah poškodenia a identifikovať zasiahnuté systémy**
- **identifikovať, ku ktorým dátam bolo pristúpené, či boli modifikované, a za akým účelom**
- **odhaliť prípadné externé hardvérové zariadenia pripojené ku zasiahnutým systémom alebo pomocným systémom**
- **preskúmať jednotlivé bezpečnostné skupiny užívateľov so zameraním sa na novo pridané, odstránené alebo na zmenené záznamy**
- **odhalenie nainštalovaného neautorizovaného softvéru, ktorý pomáha útočníkovi získať ďalšiu kontrolu nad systémom**
- **preskúmanie bežiacich procesov v systéme, resp. nových modulov v jadre systému a odhalenie zmeny v konfigurácii existujúcich procesov. (/etc/, registre systému)**
- **analýza protokolov udalostí so zameraním sa na skúmanie chýbajúcich častí, resp. neobvyklé záznamy**
    - skúmanie protokolov udalostí systémov na detekciu prieniku, (IDS) - ktoré systémy môžu byť napadnuté, ako dlho incident už trvá, ktoré systémové prostriedky boli používané
    - skúmanie protokolov udalostí na smerovačoch a firewalloch - neobvyklé spojenia, podozrivé prenosy dát, neúspešné a úspešné pokusy o nahlásenie sa do systému, zmena prístupových práv, zmena hesiel

- skúmanie protokolu udalostí napadnutých služieb - druhy požiadaviek, počet prístupov, požadované operácie

- **porovnanie štruktúry dát s posledným korektným stavom systému na determináciu zmenených, vymazaných alebo pridaných dát**
- **zaznamenávanie pokusov o vyhľadávanie citlivých dát, ako sú prístupové heslá, osobné údaje, finančné operácie alebo iné dáta, ako emaily, technologické dokumenty -** pri zistení tejto skutočnosti je veľmi dôležité, aby sa osoba spojila s právnym oddelením danej organizácie.

Množina týchto dát umožní ľahšie stanoviť ďalšie rozhodnutia a tým docieliť efektívnosť odozvy zo strany poškodenej spoločnosti. Aj keď sú jednotlivé typy incidentov navzájom odlišné, jednotlivé symptómy zasiahnutého systému sa prejavujú vo všeobecnosti v rovnakom poradí.

7.5 Formovanie plánu odstraňovania následkov incidentu

Táto fáza reakcie na incident je jedna z najdôležitejších. Chybným postupom sa môžu straty spôsobené incidentom rapídne zväčšiť, preto je dôležité formovať vhodný plán odstraňovania následkov incidentu. Na formovaní plánu sa zúčastňuje celý tím pre reakciu na incidenty, ktorý je informovaný o vzniknutej situácii a oboznámený s odhadom rozsahu škôd. Cieľom plánu je definovanie najvhodnejšej reakcie, ktorá by mala byť odsúhlasená zástupcami vrcholového manažmentu.

Formovanie vhodného plánu je závislé od škôd spôsobených incidentom. Preto je dôležité zodpovedať nasledujúce otázky:

- **Aké dôležité sú napadnuté systémy?**
- **Aké citlivé sú ukradnuté alebo poškodené informácie?**
- **Kto je potenciálnym útočníkom?**
- **Je o incidente informovaná verejnosť?**
- **Aká je úroveň neoprávneného prístupu získaná útočníkom?**
- **Aké sú schopnosti útočníka?**
- **Aké veľké výpadky systému je možné tolerovať?**

- **Aká je finančná náročnosť jednotlivých možných plánov?**

Každý priebeh a druh vzniknutého incidentu je špecifický a individuálny, napr. vírusová infekcia je odlišná od prieniku do centrálneho systému spracovania obchodných transakcií. Vírusová infekcia spôsobuje iba stratu produktivity práce, naopak prienik môže spôsobiť stratu postavenia spoločnosti na trhu, až jej krach. Preto je dôležité rozhodnúť sa, či bude snaha identifikovať útočníka s jeho následným postihom alebo nie. To znamená rozdiel medzi plánom získavania a ochrany informácií a dôkazov a stratégiou čo najrýchlejšej obnovy systému a produktivity práce. Práve detaily získané o incidente z predchádzajúcich fáz napomáhajú zvoliť vhodný plán. Formovanie stratégie značne ovplyvňuje aj schopnosti samotného tímu a možnosť využitia technických prostriedkov.

7.6 Ochrana dôkazov

Každá spoločnosť, v ktorej sa vyskytne incident, ktorým utrpí značné finančné straty ako aj straty iného druhu (napr. strata prestíže), chce vyvodiť dôsledky za vzniknutú situáciu. V závislosti od zvoleného plánu reakcie na incident z predchádzajúcej fázy (viď kap. „Formovanie plánu reakcie na incident“) sa tím bude alebo nebude snažiť vykonávať nasledujúce činnosti. V prípade, že zvolený plán reakcie na incidenty bude preferovať rýchlosť obnovy pred usvedčením vinníka, môže prejsť na ďalšiu fázu. V opačnom prípade práve dôkazy získané počas reakcie na incident sú tie, pomocou ktorých môže byť usvedčený človek zodpovedný za vzniknutý incident. Počas reakcie na incident je teda potrebné dohliadať na ochranu všetkých dostupných dôkazov, ktoré by mohli k tomu dopomôcť.

V mnohých prípadoch sa odporúča najskôr postihnutý systém úplne zálohovať, lebo proces odozvy na incident by mohol poškodiť alebo úplne zničiť zanechané stopy po útočníkovi a tým vylúčiť akúkoľvek možnosť postihu. Pri zálohovaní systému sa môžu použiť všetky dostupné médiá od CD, DVD až po magnetické pásky, ale veľmi dôležité je, aby sa použili nové, nikdy predtým nepoužité médiá, aby sa predišlo spochybneniu získaných dôkazov. Najlepšie je, ak sa vykonajú dve zálohy, jedna použitá pri obnove dát a druhá pri samotnom vyšetrovaní. Dôležité je, aby sa o celom procese zálohovania viedla úplná dokumentácia o tom, čo sa zálohovalo, aká metóda zálohovania bola použitá a samozrejme, kto a kedy

vykonal zálohu. Odporúča sa, aby pevné disky v napadnutom systéme boli odložené, a na obnovu systému boli použité nové. Proces je niekedy veľmi zdĺhavý a pomer medzi rýchlosťou obnovy systému a závažnosťou incidentu sa veľmi zvyšuje. Preto sa niekedy na urýchlenie zálohujú len dáta, ktoré pomáhajú pri neskoršom vyšetrovaní (ako napr. všetky protokoly udalostí, stav systému, konfigurácie). Pri procese ochrany dôkazov je vždy na prvom mieste dôležitá detailná dokumentácia, aby boli získané dôkazy v prípade vyvodenia dôsledkov incidentu vždy právne akceptovateľné.

Na základe zvolenej stratégie by malo byť jasné, či sa získavanie dôkazov bude diať na on-line alebo off-line systéme. Je nutné podotknúť, že on-line systém nám môže poskytnúť ďaleko rozsiahlejšie informácie, avšak proces získavania dôkazov je oveľa náročnejší vzhľadom na tlak spôsobený situáciou.

V prípade rozhodnutia analýzy on-line systému je najvhodnejšou metódou monitoring systému a prebiehajúcej komunikácie. Väčšinou je tento proces dlhodobý a prebieha od začiatku procesu reakcie na incident až do úplnej obnovy systému. Rozhodnutie monitorovať celý systém je rozumné, ale nie vždy najlepšie, vzhľadom na získanie množstva často neužitočných informácií. Preto je vhodné monitorovať len postihnuté a hraničné systémy (firewally a smerovače). V prípade znalostí techniky, ktorú použil útočník, je dôležité zamerať sa na monitoring udalostí charakteristických pre použitú techniku.

7.7 Notifikácia externých organizácii

Po zabezpečení dôkazov a počiatočnom odhade incidentu sa pristupuje k samotnej obnove systému. Predtým, než sa pristúpi k samotnej obnove, je vhodné informovať externé organizácie zaoberajúce sa bezpečnostnými incidentmi. Tie nám môžu poskytnúť cenné informácie v prípade skúseností s podobnými incidentmi.

Príkladom môžu byť nasledujúce celosvetové organizácie:

- Incident Response, Electronic Discovery, and Computer Forensics http://www.incident-response.org
- Security Focus

http://www.securityfocus.com

- The Federal Computer Incident Response Center (FedCIRC)
  http://www.fedcirc.gov
- CERT/CC: Computer Security Incident Response
  http://www.cert.org/csirts/
- CERT/CC: Responding to Intrusions
  http://www.cert.org/security-improvement/modules/m06.html
- SANS: S.C.O.R.E
  http://www.sans.org/score/
- SANS Reading Room: Incident Handling
  http://www.sans.org/rr/incident/
- SANS Forum: Incident Handling and Hacker Exploits Forum
  http://forum.sans.org/discus/messages/79/79.html?1047450013
- CIAC: Incident Reporting Procedures
  http://www.ciac.org/ciac/CIAC_incident_reporting_procs.html
- FIRST: Forum of Incident Response and Security Teams
  http://www.first.org/
- IETF: RFC 2196 - The Site Security Handbook (Chapter 5)
  http://www.ietf.org/rfc/rfc2196.txt?number=2196
- IETF: RFC 2350 - Expectations for Computer Security Incident Response
  http://www.ietf.org/rfc/rfc2350.txt
- CIO: CyberThreat Response and Reporting Guideline
  http://www.cio.com/research/security/incident_response.pdf
- ISS: Computer Security Incident Response Planning
  http://documents.iss.net/whitepapers/csirplanning.pdf
- Incident Response: Managing Security at Microsoft
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/msit/security/msirsec.asp

Príkladom sloveských inštitúcii sú:

- EMM s.r.o
  http://www.emm.sk

- Gordias s.r.o.
  http://www.gordias.sk/produkty/gincident.html
- CIT s.r.o.
  http://www.cit.sk/?ID_Menu=1

V niektorých prípadoch prieniku je vhodné informovať jednotlivé spolupracujúce spoločnosti, ktoré by mohli byť poškodené výskytom incidentu. Je pri tom dôležité brať ohľad na finančný dopad. V rozsiahlejších spoločnostiach sa musí počítať aj s účasťou médií. Účasť médií pri vzniku incidentu nie je nikdy žiadúca, ale niekedy sa jej nedá vyhnúť. Práve preto je potrebné dať vyhlásenie spoločnosti o vzniknutej situácii. Touto časťou reakcie na incident sa zaoberajú "hovorcovia organizácie", ktorí sú súčasťou tímu pre reakciu na incidenty. Určia, ako bude zverejnená informácia o vzniknutom incidentu na základe konzultácie s manažmentom spoločnosti.

7.8 Obnova poškodeného systému

Postup závisí od veľkosti poškodenia a miery dôležitosti on-line systému a podľa toho je potrebné rozhodnúť, či sa systém nechá stále interagovať s prostredím a obsluhovať prijaté požiadavky na služby, alebo sa celý systém nanovo vybuduje.

Obnovu je možné vykonať viacerými spôsobmi a závisí to od zvoleného plánu.

Všeobecná obnova a reštaurovanie systému z inštalačných médií sa pokladá za najúčinnejšiu a najspoľahlivejšiu metódu. Je však časovo náročná a býva použitá iba v prípade rozsiahleho poškodenia systému. Následne po reštaurovaní systému je dôležité zabrániť opakovanému zneužitiu zraniteľnosti systému k vzniku incidentu útočníkom, to zahŕňa napr. aplikovanie záplat, zmena hesiel, atď.

Druhým spôsobom je čiastočná obnova systému. Na úspešnú obnovu systému je samozrejme potrebné mať zálohy dát, ktoré môžeme považovať za bezpečné (zálohy ktoré boli vytvorené pred uskutočnením incidentu). Protokoly udalostí, kontrola integrity dát a predchádzajúce zistenia napomáhajú stanoviť vhodnú zálohu pre obnovu systému. Náročnosť obnovy systému narastá s dĺžkou pôsobenia incidentu, lebo ten mohol poškodiť dáta už pred niekoľkými týždňami,

mesiacmi od detekcie incidentu. Niekedy však ani skupina záloh nepomôže úplne obnoviť systém, preto je potrebné aplikovať obnovy na nezapojenom systéme v karanténe, ktorý nemôže vyvolať poškodenie živého systému a z neho získať potrebné dáta.

7.9 Zhrnutie vzniknutej dokumentácie o incidente

Počas procesu reakcie na incident vytvorí tím veľké množstvo dokumentácie zaoberajúcej sa detekciou incidentu od počiatku cez jednotlivé detailné postupne aplikované kroky, až po samotné dôkazy získané počas tohto procesu. Vo fáze zhrnutia dokumentácie sa organizujú jednotlivé dokumenty, či už chronologicky alebo podľa druhu obsahu. Pri tomto procese sa osvedčuje prítomnosť dvoch osôb, čím sa vyhne modifikácii dokumentácie, resp. zlej organizácii, pretože pôvod útoku mohol viesť z vnútra spoločnosti a osoba zodpovedná za spracovanie vzniknutej dokumentácie môže byť spojená s útočníkom, čím môže byť motivovaná k jej zámernej modifikácii. Je treba mať na pamäti, že práve dokumentácia je to, čo pomáha usvedčiť a odhaliť útočníka.

Táto dokumentácia môže byť neskôr použitá pri nasledovných procesoch:

- **Trestné alebo občiansko-právne konanie -** Dokumentácia je často použitá ako dôkazový materiál svedčiaci o úmyselnosti činu a spôsobených škodách, ktorá môže byť použitá v trestnom alebo disciplinárnom konaní pri odhalení vinníka.

- **Tvorba záverečnej správy o incidente –** Vedenie spoločnosti chce mať často detailný prehľad o vzniknutej situácii, čo jej umožňuje práve záverečná správa. Mala by obsahovať detailný popis incidentu, prijaté opatrenia, priebeh odstraňovania a neskoršie dodatočné zabezpečenie.

- **Návrhy na zlepšenie celého procesu resp. zabezpečenia –** Skúsenosti nadobudnuté počas tohto procesu sú nenahraditeľné a umožňujú pri ďalších výskytoch incidentu zasiahnuť flexibilnejšie a efektívnejšie. Chybné kroky, ale naopak aj správne rozhodnutia by mali byť základom pre úpravu plánov pre reakciu na incident.

7.10 Výpočet vzniknutej škody

Počas tohto procesu je dôležité aby sa vyčíslili priame, ale aj nepriame škody spôsobené incidentom. To zahŕňa:

- Strata spôsobená únikom citlivých údajov.
- Priame straty.
- Náklady na ľudskú prácu, analýzu typu útoku, reinštaláciu software, obnovu dát.
- Strata spôsobená nefunkčnosťou systému, zníženie produktivity práce, únik zisku.
- Náklady na výmenu hardware, opravu zariadení zabezpečujúcich systém.
- Ostatné poškodenia, akou je strata spotrebiteľskej dôvery – reputácie.

7.11 Aktualizácia plánov pre reakciu na incident a dodatočné zabezpečenie systému

Potom, ako je incident odstránený a obnova systému je dokončená, je priestor na analýzu priebehu celého procesu: analýza práce tímu, ktoré kroky boli aplikované správne, úspešne a naopak, s ktorými ťažkosťami sa tím stretával, ako ich riešil, a aké boli nedostatky v procedúrach pre reakciu na incident.

Všetky tieto skúsenosti nadobudnuté počas tohto procesu môžu spôsobiť modifikáciu existujúcich procedúr a metodík a prispieť tým k zlepšeniu pre budúce použitie.

Dôležité je vyhnúť sa opätovnému vzniku incidentu podobného typu, na základe zistení o priebehu incidentu analyzovať jednotlivé zraniteľnosti systému a prijať potrebné protiopatrenia na zabránenie opätovného využitia týchto zraniteľností (jedná sa o dodatočné úpravy smerovačov, aplikáciu nových filtrovacích pravidiel na firewalli, resp. inštalácia záplat softvéru alebo nového hardvéru).

8 Reakcia na incidenty

Príprava reakcie na incidenty je určujúcim prvkom úspešnosti samotnej reakcie. Od nej závisí možnosť použitia rôznych prístupov a jednotlivé možnosti tímu. Operačné systémy z hľadiska funkčnosti poskytujú prácu s dátami, s prostriedkami a aj možnosť plnej kontroly nad systémom. Úloha bezpečnosti operačného systému je veľmi dôležitá a teda primárne možnosť vyskytu incidentu sa týka práve tejto úrovne. Z tohto dôvodu sa v tejto kapitole budeme výhradne zaoberať reakciou na incidenty v prostredí operačného systému.

Najskôr sa práca bude venovať jednotlivým krokom reakcie na incident v operačnom systéme Windows a neskôr bude aplikovať podobné postupy v operačnom systéme Linux.

8.1 Príprava reakcie na incidenty v prostredí Microsoft Windows NT, 2000, XP a 2003

V prípade, že medzi definované aktíva (viď kap. „Identifikácia aktív“) spoločnosti, ktoré treba chrániť, patrí aj počítačový systém Microsoft Windows, je vhodné predpripraviť si vlastnú sadu nástrojov, ktorá pomáha pri samotnej reakcii na incident. Celá táto fáza patrí do oblasti prípravy reakcie na incident (viď kap. „Príprava zabezpečenia jednotlivých aktív“).

8.1.1 Vytvorenie sady nástrojov

Táto činnosť patrí do oblasti prípravy reakcie na incident. Množina uvedených nástrojov účinne pomáha tímu pre reakciu na incidenty získavať informácie pri identifikácii rozsahu poškodenia, druhu incidentu, ako aj pri obnove systému. Táto sada nástrojov by mala byť pripravená a dostupná na použitie v prípade výskytu incidentu. Tieto nástroje by sa mali uložiť na CD alebo iné médiá, aby sa používali vždy originálne nemodifikované nástroje. Každé médium obsahujúce množinu týchto nástrojov musí obsahovať minimálne informácie o:

- **dátume a čase vytvorenia**
- **mene osoby, ktorá médium vytvorila**
- **obsahu média**

- **verzii sady nástrojov na médiu.**

8.1.2 Obsah sady nástrojov

Systém Windows obsahuje dva druhy aplikácií GUI (Graphical user interface) a CUI (console user interface). Pre reakciu na incident neodporúčame požitie GUI aplikácií, ale CUI, vzhľadom na ich vyššiu nezávislosť od systému, ktorý môže byť modifikovaný.

Nástroj	Popis	Linka
afind.exe	vypíše zoznam naposledy modifikovaných súborov	www.foundstone.com
arp.exe	vypíše zoznam o MAC adresách a arp protokole	-
at.exe	zobrazuje úlohy- spustenie nastavené časovačom úloh	-
auditpol.exe	nástroj na prácu so systémovým auditom počítača	www.microsoft.com (resource kit)
cmd.exe	shell prostredie pre operačné systémy založené na jadre NT	-
cryptcat.exe	vytvára šifrovaný komunikačný kanál medzi dvoma počítačmi	farm9.org/Cryptcat
doskey.exe	zobrazuje históriu príkazov shellu cmd.exe	-
dumpel.exe	vypíše protokol o posledných udalostiach v systéme	www.microsoft.com (resource kit)
eventvwr.msc	aplikácia na prezeranie protokolu udalostí	-
fport.exe	vypíše zoznam TCP/UDP portov a aplikácie, ktoré porty používajú	www.foundstone.com
hunt.exe	zobrazuje zoznam zdieľaných dát na vzdialenom počítači	www.foundstone.com
mmc.exe	program na manipuláciu s manažment konzolami	-
md5sum.exe	vytvára a overuje kontrolné súčty	http://www.etree.org/md5com.html
Nbtstat.exe	vypíše informácie o NETBIOS spojeniach	-
net.exe	multifunkčný nástroj	-
Netstat.exe	vypíše všetky TCP/UDP porty, ktoré sa používajú v systéme aj s opisom stavu spojenia, resp. s kým je spojenie nadviazané	-
ntlast.exe	vypíše zoznam posledne nahlásených užívateľov	www.foundstone.com
pskill.exe	program na ukončovanie bežiacich procesov	www.sysinternals.com
psloggedon.exe	program zobrazujúci zoznam užívateľov pripojených do systému	www.sysinternals.com
Psservice.exe	program na zobrazenie zoznamu dostupných služieb v systéme	www.sysinternals.com
reg.exe	nástroj na prácu so systémovým registrom	www.microsoft.com (resource kit)
sfind.exe	nástroj na odhalenie skrytých súborov využívajúcich ntfs streamy	www.foundstone.com
tlist.exe	vypíše zoznam bežiacich procesov a aj linkovaných knižníc k procesom	www.microsoft.com (support tools)
md5sum.txt	zoznam MD5 kontrolných súčtov jednotlivých nástrojov na médiu	

Toto je zoznam základných nástrojov, ktoré by mali byť v obsahu každej sady nástrojov tímu pre reakciu na incident. Do sady by mali byť doplnené nástroje závislé od druhu služieb alebo softvéru nachádzajúceho sa na chránených systémoch.

8.2 Reakcia na incidenty v prostredí Microsoft Windows NT, 2000, XP a 2003

Na úrovni operačného systému Microsoft Windows NT, 2000, XP a 2003 sa budeme zaoberať najmä množinou úmyselných ľudských incidenov (viď kap. „Kategorizácia incidentov“), nakoľko práve táto množina je najviac v tomto prostredí rozšírená. Jednotlivé kroky je však možné použiť aj pri iných druhoch incidentov.

8.2.1 Metódy uchovávania získaných dát

Získané informácie počas reakcie na incident je vhodné niekde koncentrovať. Existujú viaceré možnosti:

- ukladanie dát na záchrannú disketu alebo iné médium
- manuálne zapisovanie získaných informácií do počítača (notebooku)
- získané dáta uložiť na pevný disk v postihnutom systéme
- posielanie dát na špeciálne zriadenú vyšetrovaciu stanicu.

Posledná možnosť je najúčinnejšia metóda, z dôvodu centralizovania jednotlivých dôkazov, ako aj ich ochrany voči modifikácii resp. vymazaniu. Na vytvorenie komunikačného kanálu medzi postihnutou a vyšetrovacou stanicou môžme použiť nástroj cryptcat.exe, ktorý okrem vytvoreného spojenia umožňuje dátovú komunikáciu šifrovať, a zabrániť tak jeho odpočúvaniu.

Príklad:

Predpokladáme že vyšetrovacia, ako aj postihnutá stanica obsahuje CD-ROM označený ako disk D: a v ňom máme CD so sadou nástrojov spomínanej v predchádzajúcej kapitole v adresári d:\Toolkit.

Vyšetrovacia stanica uskutoční zaznamenávanie nasledujúcim príkazom.

```
C:\> D:\Toolkit\cryptcat -l -k secretkey -p 4100 > irdata.txt
```

Naopak: postihnutá stanica by mala každý príkaz uskutočňovať nasledujúcim postupom:

```
C:\> dir *.* | D:\Toolkit\cryptcat -k secretkey 172.168.0.100
4100
```

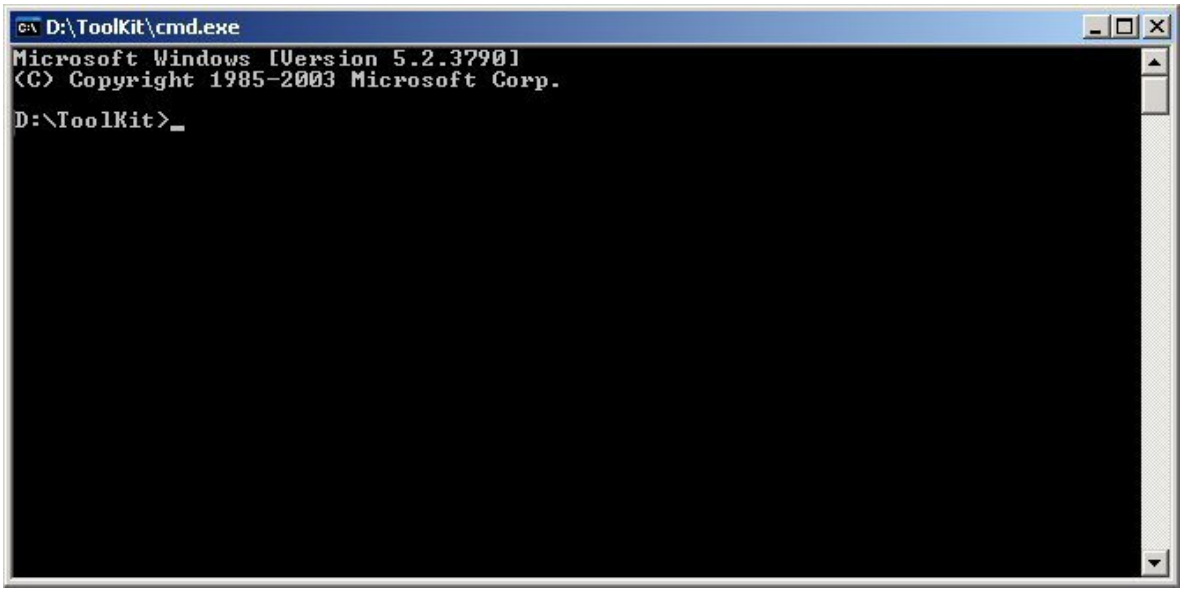
8.2.2 Získavanie dôležitých dát z on-line systému

Práve nasledujúce postupy by nám mali pomôcť zistiť počiatočný odhad typu a závažnosti incidentu (viď kap. „ Detekcia a odhad incidentu “) z on-line systému, na ktorom bol detekovaný incident, či už prostredníctvom systémov IDS alebo externých zdrojov (neobvyklé chovanie, reakcie od užívateľov apod.).

8.2.2.1 Spustenie originálneho shellu systému Windows

Ak útočník získal prístup k systému je treba predpokladať vždy to najhoršie , a preto nedôverovať žiadnej aplikácii nachádzajúcej sa v systéme. Pred plánovaným uskutočňovaním zberu informácií je potrebné spustiť dôveryhodný shell *cmd.exe.* To môžeme uskutočniť pomocou tlačidla Štart-> Run a do príkazového riadku napíšeme:

```
D:\Toolkit\cmd.exe
```



obr. č. 6. Spustenie originálneho shellu.

Od tejto situácie môžeme vykonávať ďalšie príkazy, ale treba mať vždy na pamäti, aby sme spúšťali len dôveryhodné programy. To môžeme docieliť buď spúšťaním z dôveryhodného média alebo najprv skontrolujeme ich integritu pomocou mechanizmu kontrolných súčtov (opäť budeme používať iba dôveryhodné nástroje na kontrolu súčtov) a porovnáme ich s predchádzajúcimi záznamami.

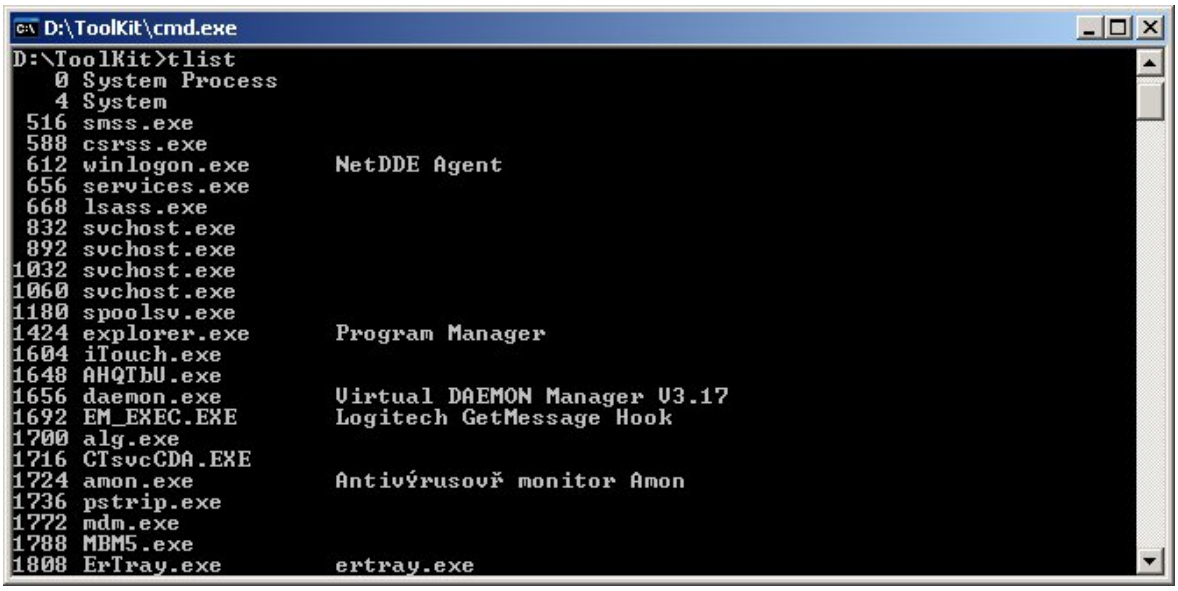
8.2.2.2 Zoznam aktuálne bežiacich procesov

Je dôležité zistiť, aké procesy bežia na systéme postihnutom incidentom. Pomáha to odhaliť novo nainštalované služby alebo programy, ktoré by napr. zbierali dáta od používateľov v systéme, resp. o práve prebiehajúcej aktivite v systéme. Tiež je dôležité zistiť, či boli nainštalované nejaké typy hookov do systému. To odhalíme napr. výpisom zoznamu používaných knižníc v systéme. Ak sa medzi nimi objaví nejaký druh neštandardnej knižnice, môžeme neskôr pristúpiť k jej analýze a druhu hooku, resp. inštalovaného softvéru. Je zrejmé, že tento proces vyžaduje dobrú znalosť systému a originály prítomných služieb a programov v systéme. Členom tímu by k tomu mala dopomôcť dôkladná dokumentácia, resp. kontakt na administrátora daného systému.

Príklad:

Výpis bežiacich procesov v systéme:

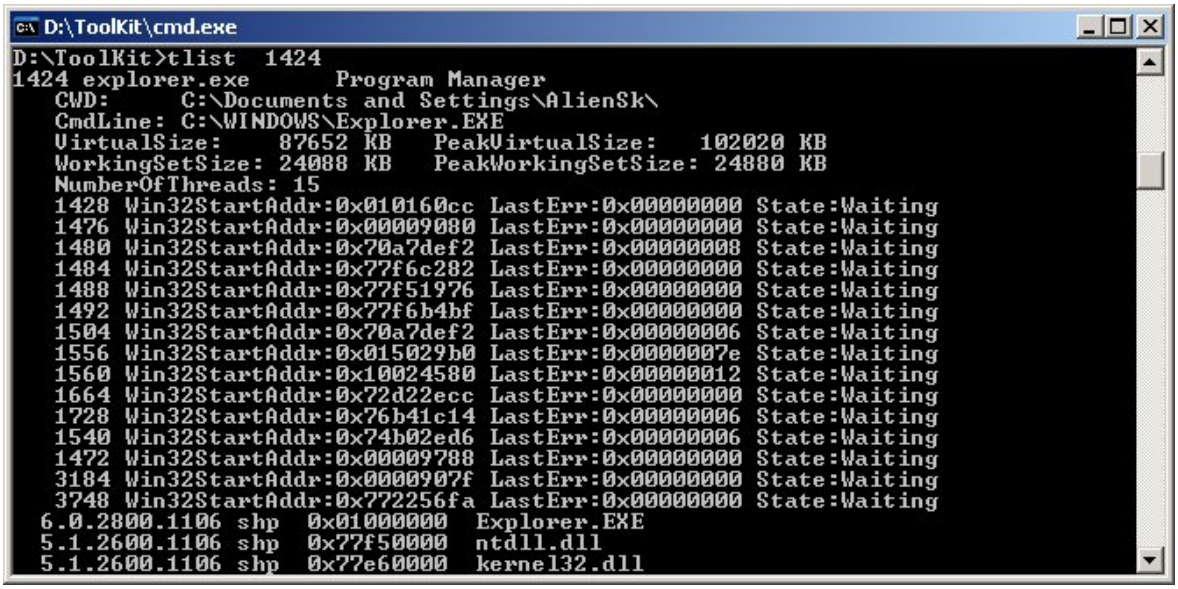
```
C:\> D:\Toolkit\tlist.exe
```



obr. č. 7. Výpis bežiacich procesov v operačnom systéme

Výpis linkovaných knižníc k procesu:

```
C:\> D:\Toolkit\tlist.exe 1424
```



obr. č. 8 Detailné informácie o bežiacom procese z identifikátorom 1424

V prípade oprávnenia môžeme podozrivý proces ukončiť pomocou príkazu pskill.exe:

```
C:\> D:\Toolkit\pskill.exe 638
```

Ak však ide o spustenú službu v systéme, príkaz pskill nám aplikáciu neukončí. Bežiaciu službu je v tomto prípade potrebné zastaviť použitím príkazu net.exe:

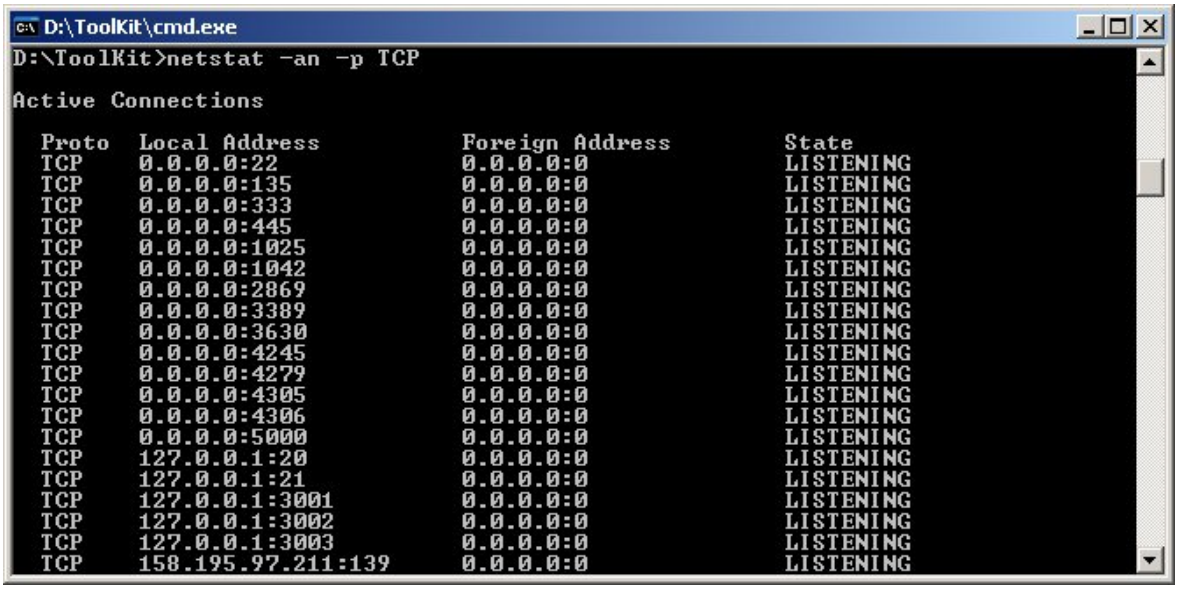
```
C:\> D:\Toolkit\net.exe stop TlntSvr
```

8.2.2.3 Zoznam sieťových spojení a ich bližšia analýza

Útočníci využívajú k svojej činnosti komunikačné spojenia, ktoré sú v štandardných prípadoch uskutočňované prostredníctvom protokolu TCP/IP a UDP/IP. Samotné spojenie je charakteristické použitým portom pre komunikáciu. Na výpis zoznamu spojení a otvorených portov použijeme dva nástroje *netstat.exe* a *fport.exe.*

Príklad:

```
C:\> D:\Toolkit\netstat.exe -an -p TCP
```



obr. č. 9 Výpis aktuálnych sieťových spojení spolu z ich stavom a adresou hostiteľa.

Pri výpise zoznamu otvorených a počúvajúcich TCP spojení je potrebné si najviac všímať spojenia, ktoré sú v stave ESTABILISHED a zistiť ich bližší charakter. To znamená, na akú službu sa spojenie viaže, či je to služba lokálna alebo je to spojenie na službu so vzdialeným serverom. Ak sa jedná o spojenie so vzdialenou službou, treba zistiť, ktorá aplikácia ho vyvolala. Dôležité je samozrejme všímať si aj spojenie v stave TIME_WAIT, ide väčšinou o nedávno ukončené spojenia.

Vypíše zoznam počúvajúcich UDP portov:

```
C:\> D:\Toolkit\netstat.exe -an -p UDP
```

Tak, ako pri UDP aj pri TCP je vhodné zistiť, či sa neobjavil nejaký druh služby čakajúcej na spojenie. V mnohých prípadoch sa môže jednať o backdoor programy nainštalované útočníkom. Na presnú identifikáciu počúvajúcich portov a prislúchajúceho procesu nám pomáha program *fport.exe*

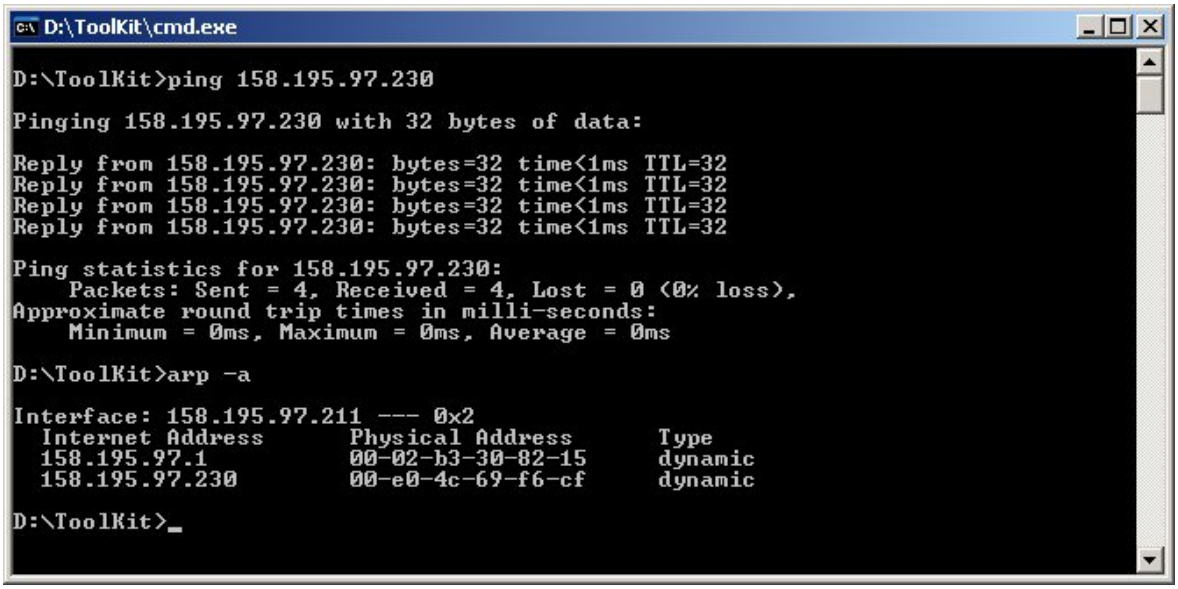
```
C:\> D:\Toolkit\fport.exe
```

Následne pomocou programu tlist.exe môžeme získať detailnejšie informácie o podozrivom procese.

```
C:\> D:\Toolkit\tlist.exe <pid podozrivého procesu>
```

V prípade podozrenia útoku zvnútra je potrebné okrem IP adresy získanej pomocou tohto zoznamu poznamenať si aj MAC adresu sieťovej karty z podozrivého počítača, ktorá môže slúžiť na dodatočnú identifikáciu útočníka. Nasledujúci príklad ukazuje ako ľahko zistiť MAC adresu počítača s IP adresou 158.195.97.230.

```
C:\> D:\Toolkit\ping.exe 158.195.97.230
C:\> D:\Toolkit\arp -a
```



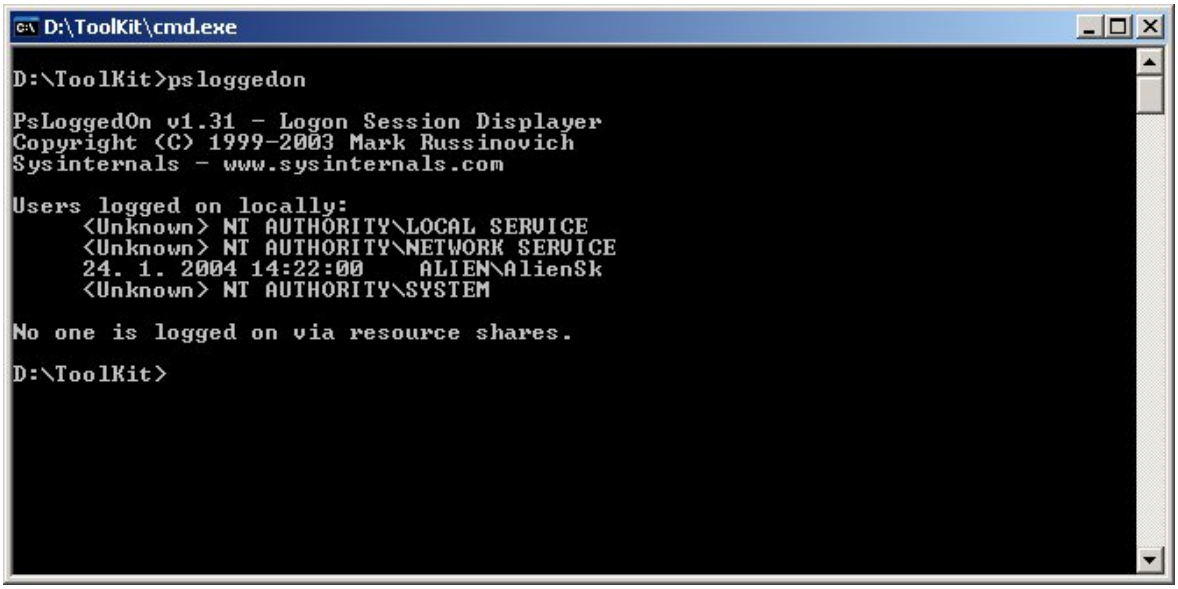
obr. č. 10. Obrázok ilustruje proces zistenia fyzickej adresy.

8.2.2.4 Zoznam aktuálne nahlásených užívateľov

Dôležitým údajom o systéme je zoznam aktuálne nahlásených užívateľov v systéme. Neskoršou analýzou oprávnenosti prítomnosti v systéme môžeme odhaliť zneužitie konkrétneho užívateľského účtu a viesť k páchateľovi. Výbornou utilitou slúžiacou práve na tento účel je program *psloggedon.exe.*

Príklad:

```
C:\> D:\Toolkit\psloggedon.exe
```



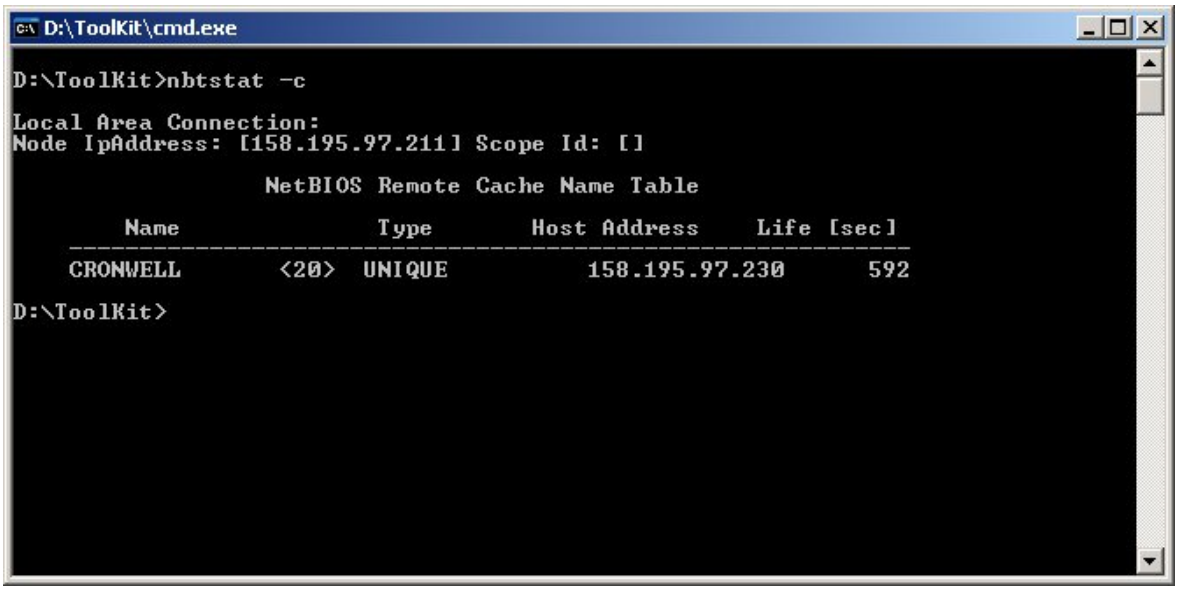
obr. č. 11 Zoznam aktuálne nahlásených užívateľov do systému.

8.2.2.5 Zoznam aktuálnych a nedávnych spojení so službou NETBIOS

Služba NetBIOS je základnou službou poskytovanou systémom WINDOWS. Autorizovaním pomocou tejto služby ako administrátor môžeme podstatne zasahovať do nastavenia operačného systému. Preto je dôležité zistiť, kto teraz alebo v nedávnej dobe využíval práve túto službu.

Príklad

```
C:\> D:\Toolkit\nbtstat.exe -c
```



obr. č. 12. Zoznam nedávnych spojení prostredníctvom služby NetBios.

8.2.2.6 Skript pre počiatočnú reakciu

Všetky tieto akcie sa dajú automatizovať do jedného skriptu. Jeho obsah je nasledovný.

```
@echo off
set WDIR=%~dp0

set f=psloggedon.exe
IF NOT EXIST "%WDIR%%f%" goto notcomplete
echo %f% [OK]

set f=netstat.exe
IF NOT EXIST "%WDIR%%f%" goto notcomplete
echo %f% [OK]

set f=fport.exe
IF NOT EXIST "%WDIR%%f%" goto notcomplete
echo %f% [OK]

set f=tlist.exe
IF NOT EXIST "%WDIR%%f%" goto notcomplete
echo %f% [OK]

set f=nbtstat.exe
IF NOT EXIST "%WDIR%%f%" goto notcomplete
echo %f% [OK]

echo Čas a dátum začiatku:
date /t
time /t
```

```
psloggedon.exe
netstat.exe -an
fport.exe
rem tlist.exe
nbtstat.exe -c

echo Čas a dátum ukončenia:
date /t
time /t
goto end

:notcomplete
echo Neexistuje súbor %f% v adresári %WDIR%

:end
```

8.2.3 Pokročilá analýza

Na získanie ďalších dôkazov a rozsahu poškodenia (viď kap. „Identifikácia rozsahu incidentu a miery poškodenia“) je potrebné pristúpiť k hĺbkovému skúmaniu systému. Na to nám poslúžia záznamy protokolu udalostí systému a databáza registrov. Túto analýzu môžeme vykonávať ako off-line, tak aj on-line.

8.2.3.1 Databáza registrových kľúčov

Poskytuje rozsiahle informácie o nastaveniach systému, nainštalovaných aplikáciách, ako aj o užívateľských profiloch a konfiguráciách. Vzhľadom na rozsiahlosť informácií uložených v databáze registrov môže útočník ľahko schovať zmeny vykonané v systéme, ako aj pravidelné spúšťanie istých aplikácií alebo služieb.

Na off-line analýzu potrebujeme nasledujúce súbory:

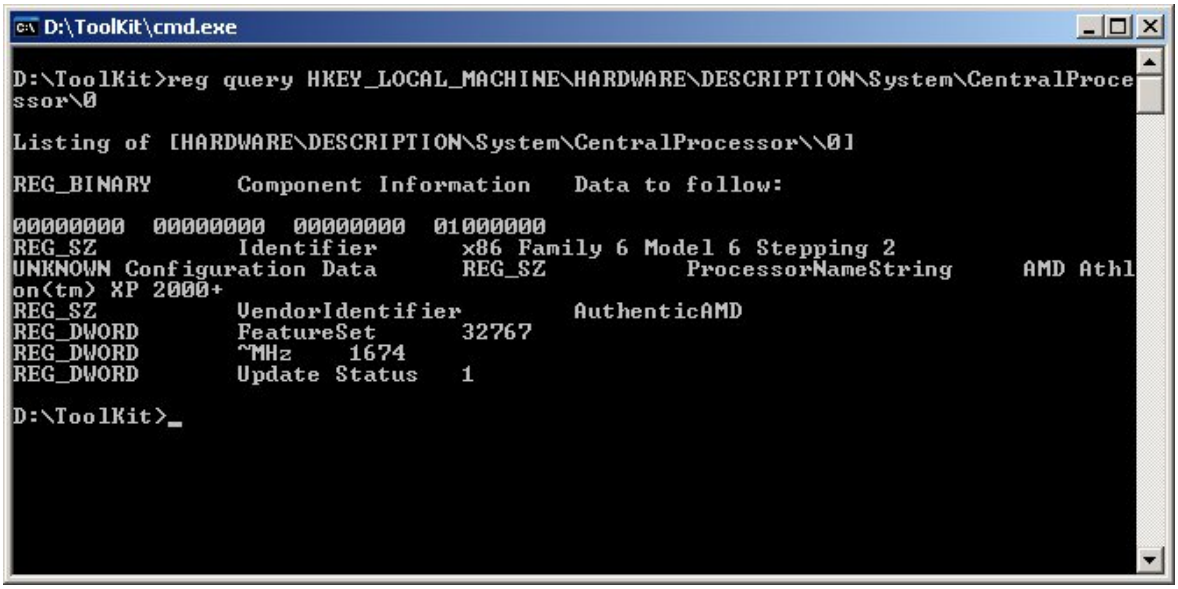
```
%SystemRoot%\system32\config\default
%SystemRoot%\system32\config\Sam
%SystemRoot%\system32\config\Security
%SystemRoot%\system32\config\software
%SystemRoot%\system32\config\system
%SystemRoot%\system32\config\userdiff
```

Následne môžeme súbory importovať na vyšetrovacej stanici prostredníctvom aplikácie *regedit.exe*, následne cez položku menu a voľby import môžeme vybrať jednotlivé súbory registrov pre hĺbkovú analýzu.

Na on-line analýzu registru systému môžeme použiť nástroj z našej množiny nástrojov *reg.exe.*

Príklad vypisujúci informácie o prvom procesore uložené v databáze registrov systému:

```
reg query
"HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0"
```



obr. č. 13. Príklad na uskutočnenie výpisu z databázy registrových kľúčov.

Pri výskyte incidentu je dôležité pozrieť sa do konkrétnych oblastí registrov, ktoré by mohli aktivovať rôzne druhy softvéru nainštalovaných útočníkom.

Najprv zistíme o aký skúmaný počítač sa jedná:

```
reg query "HKLM\SOFTWARE\Mircosoft\Windows
NT\CurrentVersion\RegisteredOwner"

reg query "HKLM\SOFTWARE\Mircosoft\Windows
NT\CurrentVersion\RegisteredOrganization"

reg query "HKLM\SOFTWARE\Mircosoft\Windows
NT\CurrentVersion\ProductID"

reg query "HKLM\SOFTWARE\Mircosoft\Windows
NT\CurrentVersion\ProfileList"
```

Aké užívateľské kontá sa v systéme nachádzajú:

```
reg query "HKLM\SAM\SAM\Domains\Account\Users\Names"
```

Zistiť, či je použitá originálna služba pre prihlásenie užívateľa:

```
reg query "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon"
```

Nasledujú zistenia ohľadom systémovej konfigurácie:

```
reg query
"HKLM\SYSTEM\ControlSet001\Control\ComputerName\ComputerName"

reg query "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\CSDVersion
```

Prezretie všetkých procesov spúšťaných pri štarte:

```
reg query
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run"

reg query
"HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"

reg query
"HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices"

reg query
"HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOn
ce"

reg query
"HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\Load"

reg query
"HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\Run"

reg query
"HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\UserInit"
```

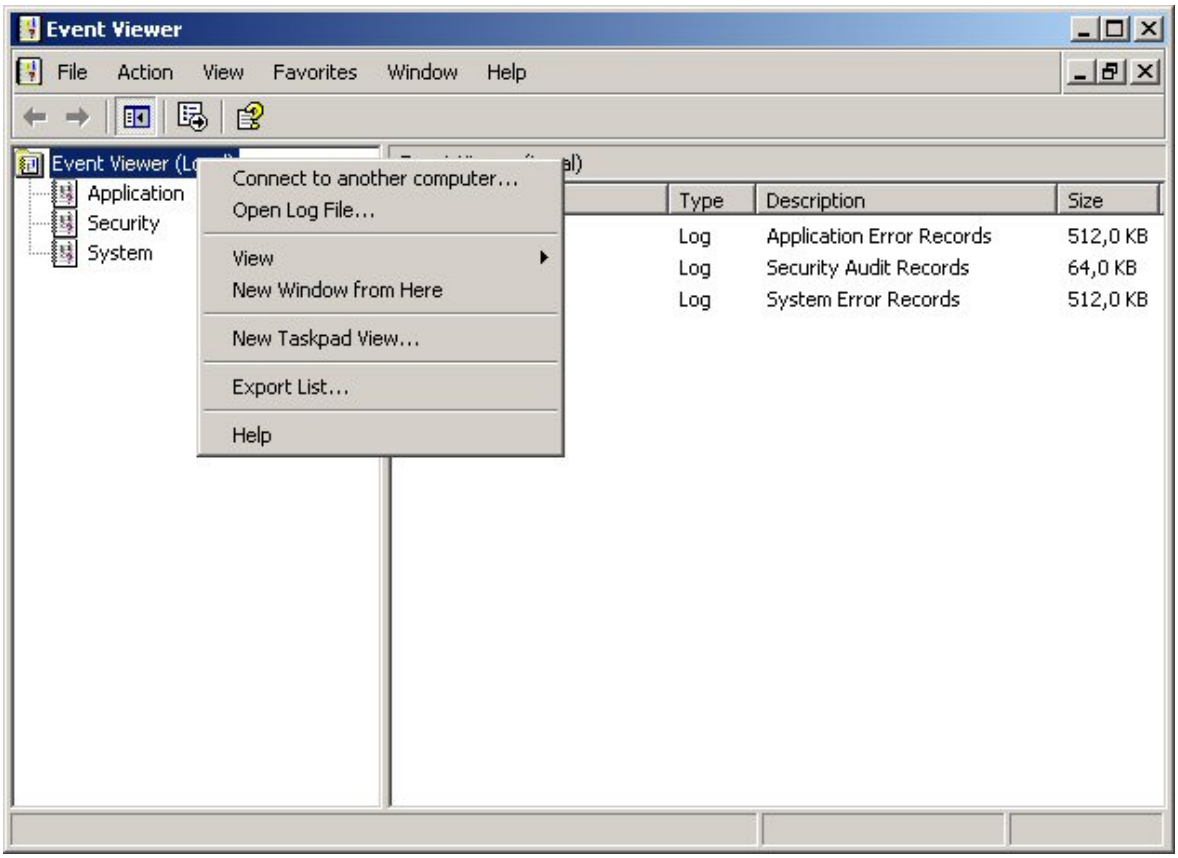
8.2.3.2 Skúmanie protokolu udalostí

Protokol udalostí je veľmi dôležitá súčasť systému, ktorá nám poskytne informácie o udalostiach, ktoré v systéme prebiehali za posledné obdobie. Jeho nedostatok je, že jeho veľkosť je obmedzená východiskovým nastavením na 512kb po dobu siedmych dní. Túto hodnotu je samozrejme dôležité zmeniť pri dôležitých systémoch na väčšiu, ale odporúča sa nastaviť ju na neobmedzenú. (viď kap. Zabezpečenie servera).

Protokol udalostí sa skladá z viacerých kategórií, ktoré závisia od verzie operačného systému. V systémoch pre pracovné stanice, ako sú Windows 2000 Professional, Windows XP Home a Professional sa nachádzajú len tri kategórie v protokole udalostí a to Application, Security a System, ale systémy Windows 2000 Server, Advanced Server, Datacenter a Windows 2003 Standard, Enterprise, Datacenter Web Server môžu okrem týchto kategórií obsahovať ešte DNS, Directory service a ďalšie.

Na off-line vyšetrovanie budeme potrebovať záznamy z protokolu udalostí, ktoré sú taktiež uložené v adresári *%SystemRoot%\system32\config*. Sú to všetky súbory s príponou *evt.* Po prenesení týchto súborov na vyšetrovaciu stanicu môžeme začať ich samotnú analýzu. Načítanie príslušného protokolu môžeme vykonať cez manažment konzolu s názvom Event Viewer nasledujúcim príkazom:

```
C:\> %systemroot%\system32\mmc.exe /a eventvwr.msc
```



obr. č. 14. Ukážka spôsobu otvorenia protokolu z postihnutého systému na vyšetrovacej stanici.

Následne cez pravé tlačidlo myši môžeme vykonávať otvorenie nového protokolu udalostí. Po výbere protokolu na analýzu je dôležité zvoliť typ protokolu z dostupných kategórií.

Na on-line analýzu nám stačí vykonať príkaz:

```
C:\> D:\ToolKit\mmc.exe /a D:\ToolKit\eventvwr.msc
```

Pred spustením je dôležité overiť si pravosť spúšťaných súborov, poprípade môžeme použiť konzolovú aplikáciu z našej sady nástrojov *dumpel.exe.*

Príklad:

```
C:\> D:\Toolkit\dumpel.exe -l security -t
```

alebo

```
C:\> D:\Toolkit\dumpel.exe -l systém -t
```

Niekedy sú záznamy v protokole udalostí viazané na nainštalované súčasti systému, a teda pri off-line analýze na vyšetrovacej stanici nemusíme dostať všetky detailné informácie o udalosti. Na získanie príslušnej informácie použijeme registre systému zo skúmaného systému a pomocou metód opísaných v predchádzajúcej časti preskúmame kľúč:

```
KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
```

V kľúči sú zaznamenané všetky potrebné nainštalované súčasti postihnutého systému, ktoré je potrebné previesť na vyšetrovaciu stanicu.

Najdôležitejšou súčasťou protokolu udalostí je kategória Security, ktorá nám ponúka informácie získané z auditu systému. Audit systému nie je pri východiskovej inštalácii aktivovaný. Program *auditpol.exe* pomáha zistiť, či je v systéme zapnutý audit, a ak je tomu tak, aké druhy udalostí sú zaznamenávané.

Príklad:

```
C:\> D:\Toolkit\auditpol.exe
```

Pretože zoznam security protokolu je rozsiahly, stačí najprv prezrieť udalosti s nasledovnými identifikátormi:

Event ID	Popis
516	Niektoré nastavenia udalosti pre audit boli zrušené.
517	Nastavenia udalostí pre audit boli zmazané.
528	Úspešné prihlásenie do systému.
529	Neúspešné prihlásenie do systému.
531	Neúspešné prihlásenie do systému, účet bol zablokovaný.
538	Úspešné odhlásenie.
576	Priradenie a použitie práv užívateľa.
578	Použitie privilegovanej služby.
595	Nepriamy prístup k objektu.
608	Zmena politiky oprávnenia.
610	Bola pridaná nová dôveryhodná doména.
612	Zmena nastavenia udalostí pre audit.
624	Vytvorený nový užívateľský účet.

626	Bol povolený užívateľský účet.
630	Užívateľský účet bol zakázaný.
636	Nastala zmena v skupine užívateľov.
642	Nastala zmena v užívateľskom účte.
643	Zmenená doménová politika.

Podobne program *ntlast.exe* veľmi prehľadným spôsobom vypíše zoznam naposledy prihlásených užívateľov do systému, vyžaduje však zapnutý audit na úspešné/neúspešné prihlásenia do systému.

Príklad:

Zobrazí všetky lokálne úspešné prihlásenia:

```
C:\> D:\Toolkit\ntlast.exe
```

Zobrazí všetky lokálne neúspešné prihlásenia:

```
C:\> D:\Toolkit\ntlast.exe -f
```

Zobrazí všetky vzdialené úspešné prihlásenia:

```
C:\> D:\Toolkit\ntlast.exe -r
```

8.2.3.3 Kontrola modifikácie a vytvorenia súborov

Takmer každý vyvolaný incident zanecháva stopy vo forme zmenených alebo nových súborov na pevnom disku. Je vhodné teda vyhľadať všetky posledne modifikované a novovytvorené súbory. V systéme Windows NT, 2000 a 2003 sa ukladajú tri druhy systémových dátumov s presným časom:

- dátum poslednej modifikácie súboru alebo adresára
- dátum vytvorenia súboru alebo adresára
- dátum posledného prístupu k súboru alebo adresáru.

Tieto dátumy sa nastavujú pre adresáre osobitným spôsobom, ich hodnoty sú závislé od súboru, ktorý posledne modifikoval svoje nastavenia. To znamená, že pre počiatočné zistenie stačí príkaz vykonať len na adresároch, a potom pri

detailnejšej analýze skúmať bližšie jednotlivé súbory v tom ktorom adresári. Na tieto účely stačí systémový príkaz *dir:*

-vypíše všetky adresáre spolu s dátumom posledného prístupu na disku C

```
dir /t:a /a /s /o:d c
```

- vypíše všetky adresáre spolu s dátumom poslednej zmeny na disku C

```
dir /t:w /a /s /o:d c
```

- vypíše všetky adresáre spolu s dátumom vytvorenia na disku C

```
dir /t:c /a /s /o:d c
```

Súborový systém NTFS umožňuje ukladanie viacerých prúdov dát pod spoločným názvom, preto je niekedy dôležité podozrivé súbory prehľadať programom *sfind.exe* zo sady nástrojov na odhalenie, či súbor obsahuje viacero prúdov dát. Tento program prehľadá z aktuálneho adresára všetky súbory a vypíše nám súbory, ktoré obsahujú viaceré dátové prúdy.

```
C:\> D:\Toolkit\sfind.exe c:
```

8.2.3.4 Kôš systému

Je nástroj, pomocou ktorého sa dajú obnoviť zmazané súbory. Často však nie všetky, len niektoré aplikácie pracujúce na úrovni systémových súborov ukladajú zmazané súbory do koša, iné tieto súbory priamo mažú zo súborového systému. Napriek tomu však kôš môže obsahovať súbory, ktoré nám pomôžu odhaliť podstatu incidentu.

Prezeranie obsahu koša on-line/off-line je jednoduché. Stačí poklikať myšou na ikonu na ploche v systéme a zistíme jeho obsah a pomocou tohto prostriedku môžeme obnoviť súbory nachádzajúce sa v ňom. Cez príkazový riadok sa k obsahu koša dostaneme pomocou príkazu:

```
C:> dir / a c:\recycler
```

Pokiaľ adresár *recycler* na disku neexistuje, je možné, že kôš neobsahuje žiadne položky, alebo nebol vymazaný žiaden súbor. Tento adresár sa totiž na

diskovej jednotke vytvára automaticky, akonáhle dôjde k vymazaniu nejakého súboru na disku.

8.2.3.5 Skúmanie dočasných súborov

Množstvo aplikácií používa výhodu dočasných súborov. Tie vznikajú najmä pri inštalácii jednotlivých programov. Preto je v procese vyšetrovania incidentu nutné preskúmať oblasť, kde sa ukladajú dočasné súbory, taktiež aj ich vyhľadanie na disku. Je ťažké identifikovať, čo je dočasný súbor. Ako spoľahlivá pomôcka môže byť použitie štandardnej prípony *.tmp*, alebo generovaný názov súboru.

Príklad dočasných súborov:

```
{0fca3656-4925-4f62-8ff3-4cc076d3a72d}.dat
~DF10C1.tmp
$wc0
```

Prehľadanie adresára pre dočasné úložisko uskutočníme príkazom:

```
C:> dir /a /s %TEMP%
C:> dir /a /s %TMP%
C:> dir /a /s %Systemroot%\temp
C:> dir /a /s %Systemroot%\system32\temp
C:> dir /a /s c:\temp
```

Nie všetky úložiská dočasných súborov musia existovať, uviedli sme iba zoznam najčastejšie používaných.

8.2.3.6 Skúmanie odkladacieho súboru

Odkladací súbor umožňuje v prípade nedostatku fyzickej pamäte uložiť časť pamäte na disk a tým získať voľné miesto pre práve prebiehajúcu požiadavku na alokáciu pamäte. Z tohto dôvodu je užitočné prehľadať tento súbor, keďže v tomto súbore sa môžu nachádzať dôležité údaje.

Informácie o mieste uloženia odkladacieho súboru získame z databázy registrov:

```
C:>reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management\Pagingfiles"
```

Skúmanie odkladacieho súboru je možné iba off-line, z dôvodu exkluzívneho prístupu pre zápis a čítanie operačným systémom. Preto pred samotným vypnutím systému je potrebné overiť, že odkladací súbor sa nevyprázdňuje, to dosiahneme nasledujúcim príkazom:

```
C:>reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Memory Management\ClearPageFileAtShutdown"
```

Hodnota 0 znamená, že súbor nie je vyprázdňovaný, naopak hodnota 1 znamená, že súbor je vyprázdňovaný. V tomto prípade je treba pred uvedením systému do stavu off-line túto hodnotu zmeniť.

Samotnú analýzu odkladacieho súboru je najlepšie vykonávať v hexadecimálnom editore, keďže na jeho skúmanie nie sú špeciálne nástroje.

8.2.3.7 Kontrola nastavenia zdieľania adresárov

Často, najmä pri incidentoch pochádzajúcich z internej siete, dochádza k zapnutiu zdieľania adresárov. To umožňuje neskôr pristupovať k dátam zo vzdialeného systému. Preto je dôležité vyšetriť, čo je nastavené na zdieľanie a s akými právami.

Off-line analýzu môžeme previesť výpisom nasledovného kľúča z registra vyšetrovaného systému:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanse
rver\Shares
```

- informácie o použitých právach môžeme získať v kľúči:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanse
rver\Shares\Security
```

V procese on-line analýzy na výpis zoznamu existujúcich zdieľaných adresárov môžeme použiť aplikáciu *hunt.exe* z našej sady nástrojov.

Príklad:

```
C:> D:\Toolkit\hunt.exe \\server01
```

Je treba overiť najmä zdieľania, ktoré sú ukončené znakom $, nakoľko tieto zdieľania nie sú viditeľné pri prehľadávaní, ale je k nim možnosť dostať sa uvedením úplnej cesty napr. \\*server01**c$*. V systéme sa od inštalácie nachádzajú tzv. administrátorské zdieľania, sú to:

```
\\<názov počítača>\<názov dostupnej jednotky v systéme>$
\\<názov počítača>\admin$
\\<názov počítača>\ipc$
```

O prístupe k jednotlivým zdieľaniam sa môžeme dozvedieť prostredníctvom auditu, ktorý však musí byť správne nastavený.

8.2.3.8 Analýza zoznamu vykonávaných procesov pomocou „Časovača Úloh“

Systém Windows umožňuje pravidelné alebo jednorazové nastavenie spúšťania úloh v systéme. Útočník môže pomocou tejto služby pravidelne vykonávať isté operácie, ako zasielanie získaných hesiel.

Off-line analýzu vykonáme prezretím adresára:

```
%systemroot%\tasks
```

Na on-line analýzu môžeme použiť systémový príkaz: *at.exe*

```
C:> D:\Toolkit\at.exe
```

8.2.3.9 Skúmanie cache a histórie internetových prehliadačov

Pri špecifických druhoch incidentu je potrebná analýza práve týchto oblastí systému. Jedná sa najmä o incidenty, ktoré sú spôsobené vírusovou infekciou, inštaláciou nelegálneho softvéru, resp. spywaru alebo prezeraním webových stránok s nepovoleným obsahom. Tieto súbory je možné zo systému odstrániť, ale často poskytujú dôležité informácie o použití internetového prehliadača.

Keďže v operačnom systéme sa od procesu inštalácie nachádza zároveň najrozšírenejší internetový prehliadač “Microsoft Internet Explorer” budem sa venovať najmä jemu.

Aplikácia Microsoft Internet Explorer ukladá informácie o histórii v adresári:

```
%USERPROFILE%\Local Settings\History\History.IE5
```

Tá je však zapísaná v binárnych súboroch, a preto je treba ich prehliadať cez externé aplikácie napr. “Microsoft Explorer History Viewer”.

Cache sa nachádza v adresári:

```
%USERPROFILE%\Local Settings\Local Settings\Temporary
Internet Files\Content.IE5
```

Obsahom sú uložené webové stránky, obrázky a stiahnuté súbory, ktoré môžeme jednoducho prehliadať.

8.2.4 Obnova poškodeného systému

Na základe predchádzajúcich zistení, by malo byť jasné, aký je rozsah a miera poškodenia systému. Podľa zvoleného plánu reakcie na incident (viď kap. „Formovanie plánu reakcie na incident“) je možné pristúpiť k úplnej alebo čiastočnej obnove systému (viď kap. „Obnova poškodeného systému“). V prípade čiastočnej obnovy systému nám môžu pomôcť dokumenty „Disaster recovery“, publikované v technickej internetovej knižnici TechNet spoločnosti Microsoft.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/support/recovery.asp

8.3 Príprava reakcie na incidenty v prostredí Unix / Linux

Ak medzi aktíva spoločnosti (viď kap. „Identifikácia aktív“) patria systémy s nainštalovaným operačným systémom LINUX / UNIX, je vhodné predpripraviť sa na výskyt prípadného incidentu (viď kap. „Príprava zabezpečenia jednotlivých aktív“).

8.3.1 Vytvorenie sady nástrojov

Podobne, ako pri reakcii na incidenty v systéme Windows, je treba vytvoriť istú sadu nástrojov, ktorá nám tento proces uľahčuje. Problém pri vytváraní týchto nástrojov je ten, že niektoré nástroje nemusia správne fungovať v jednotlivých verziách, preto je nutné urobiť sadu nástrojov pre každú verziu operačného systému použitú v podnikovej sieti. Nakoľko pri výšetrovaní incidentu môže byť kompromitované samotné jadro resp. dynamické knižnice operačného systému, je

vhodné aby nástroje obsiahnuté v sade boli kompilované staticky a teda vylučovali možnosť použitia modifikovaných dynamických knižníc.

Nástroj	Popis
ls	nástroj na výpis obsahu adresára
find	nástroj na vyhľadávanie súboru na základe zvoleného kritéria v adresárovej štruktúre
netstat	nástroj na prácu zo sieťovými socketmi
more	pomocná utilita na zobrazovanie rozsiahleho výpisu na obrazovku
dd	utilita na kopírovanie a konverziu súborov a zariadení
lcat	nástroj na prácu so súborovými uzlami
pcat	nástroj na prácu so súborovými uzlami
gzip	komprimačný nástroj
bash	prostredie pre príkazový riadok
df	utilita zobrazujúca voľné miesto na diskoch
modinfo	nástroj na zobrazenie informácie o moduloch v jadre
file	nástroj na zistenie typu súboru
last	príkaz zobrazujúci posledne nahlásených užívateľov do systému
md5sum	utilita vytárajúca md5 kontrolné súčty
ps	príkaz zobrazujúci bežiace procesy
vi	textový editor
w	príkaz zobrazujúci aktuálne nahlásených užívateľov
lsmod	príkaz zobrazuje aktuálne moduly v jadre systému
cryptcat	program na vytvorenie šifrovaného dátového spojenia medzi počítačmi
strace	program na sledovanie systémových volaní a signálov
cat	nástroj na výpis súboru na obrazovku
rm	príkaz na odstránenie súborov
ifconfig	program zobrazujúci informácie o sieťových adaptéroch
top	zobrazuje procesy zoradené podľa zaťaženia CPU
lsof	utilita na zobrazenie otvorených súborov

8.4 Reakcia na incidenty v prostredí Unix / Linux

Systém Unix / Linux je nekomerčným voľne šíreným operačným systémom. Systém sa používa najmä pre servery, ale začína sa rozširovať aj v oblasti klientskych staníc. Proces reakcie na incidenty je podobný reakcii v operačnom systéme Windows, avšak existujú diferencie v oblasti získavania dát pre vyšetrovanie incidentu čo sa týka možnosti použitých techník. Operačný systém Unix / Linux na rozdiel od systému WINDOWS môže bežať na viacerých platformách ako x86, Solaris. Taktiež sú rozšírené viaceré distribúcie, ako RedHat, Debian, SuSE, Mandrake a preto môžu nastať isté odlišnosti vo vykonávaní jednotlivých krokov. Väčšina krokov je však univerzálna pre každú platformu a použitú distribúciu. Kapitola sa bude venovať najmä operačnému systému RedHat Linux na platforme x86.

8.4.1 Metódy uchovávania získaných dát

Tento proces je rovnaký ako metóda uchovania získaných dát pre Windows. A teda prioritne sa odporúča vytvorenie šifrovaného komunikačného kanála prostredníctvom programu cryptcat.

Príklad:

V ďalšom texte budeme predpokladať, že naša sada nástrojov je uložená na cd a do systému je pripojená CD-Rom s týmto CD príkazom mount -t iso9660 /dev/cdrom /mnt/cdrom

-na vyšetrovacej stanici je teda potrebné spustiť:

```
[irteam@irstation /]# /mnt/cdrom/cryptcat -l -k secretkey -p
4100 > irdata.txt
```

- na systéme ktorý je zasiahnutý incidentom nasledujúci príkaz:

```
[root@devsys /]# /mnt/cdrom/ls | /mnt/cdrom/cryptcat -k
secretkey 172.168.0.100 4100
```

8.4.2 Získavanie dôležitých dát z on-line systému

Nasledujúci postup napomáha určiť počiatočné odhady o incidente (viď kap. „Detekcia a odhad incidentu“) a zároveň vytvoriť predstavu o miere poškodenia systému (viď kap. „Identifikácia rozsahu incidentu a miery poškodenia“).

8.4.2.1 Sady administrátorských nástrojov

Niekedy ani dôveryhodné programy nemusia stačiť na získanie reálneho obrazu o stave systému. Môže to byť spôsobené modifikáciou samotného jadra systému pomocnou modulov. Keďže programy vykonávajúce napr. výpis bežiacich procesov sú závislé od API funkcií jadra, ktoré je kompromitované, nemôžu poskytnúť správne výsledky. Práve útočníci sa snažiaci skryť svoju činnosť, v systéme využívajú túto možnosť inštalovaním sady administrátorských nástrojov (root kit). Existuje množstvo programov, nástrojov ohlasujúcich pokusy inštalovať sadu administrátorských nástrojov.

Názov	Linka
chkrootkit	http://www.chkrootkit.org/
rkdet	http://vancouver-webpages.com/rkdet/
tripwire	http://www.tripwire.org/
dtk	all.net/dtk/example.html

8.4.2.2 Spustenie originálneho shellu systému Linux

Operačný systém Linux má na rozdiel od operačného systému Microsoft Windows k dispozícii viacero programov interpretujúcich príkazy (shell-ov). Ich použitie je ekvivalentné a výber záleží len na človeku vykonávajúcom získavanie dát. Budeme používať bash (bourne again shell), ktorý je použitý pri východiskovej inštalácii systému RedHat Linux. V prípade prístupu ku kompromitovanému systému je najlepšie s ním pracovať lokálne (z konzoly) a tým sa vyhnúť možnému spusteniu kompromitovaných programov vykonávajúcich diaľkovú správu. Systém môže byť v režime X-Window, čo je grafické rozhranie systému Linux alebo textovej konzoly, preto je potrebné ukončiť systém X-Window a vykonať návrat do textovej konzoly. Spustenie shellu vykonáme jednoduchým príkazom.

```
[root@devsys /]# /mnt/cdrom/bash
```

Pre zvýšenie bezpečnosti spúšťaných programov je potrebné nastaviť premenu prostredia PATH na . a tým sa vyhnúť spusteniu modifikovaných programov v systéme. To vykonáme príkazom:

```
[root@devsys /]# export PATH=.
```

8.4.2.3 Zoznam aktuálne bežiacich procesov

Podobne ako Windows, aj Linux je multitaskové prostredie a preto v systéme bežia viaceré procesy. Nakoľko množstvo procesov v systéme je dosť rozsiahle a závislé od nainštalovaných služieb, je ťažšie determinovať nedôveryhodné procesy. Úspech závisí od dobrej dokumentácie systému a kontaktu s administrátorom postihnutého systému. Výpis spustených procesov vykonáme nasledovným príkazom:

```
[root@devsys /]# /mnt/cdrom/ps –aux
USER   PID %CPU %MEM   VSZ  RSS TTY  STAT START   TIME COMMAND
root     1  0.0  0.0  1372  492 ?    S    Okt12   0:11 init [3]
root     2  0.0  0.0     0    0 ?    SW   Okt12   0:00 [keventd]
root     3  0.0  0.0     0    0 ?    SWN  Okt12   0:00 [ksoftirqd_CPU0]
root     4  0.0  0.0     0    0 ?    SWN  Okt12   0:00 [ksoftirqd_CPU1]
root     5  0.0  0.0     0    0 ?    SW   Okt12   0:00 [kswapd]
root     6  0.0  0.0     0    0 ?    SW   Okt12   0:00 [bdflush]
root     7  0.0  0.0     0    0 ?    SW   Okt12   0:02 [kupdated]
root     8  0.0  0.0     0    0 ?    SW   Okt12   0:00 [scsi_eh_0]
root     9  0.0  0.0     0    0 ?    SW   Okt12   0:00 [scsi_eh_1]
root    10  0.0  0.0     0    0 ?    SW   Okt12   0:05 [kjournald]
root 27198  0.0  0.0     0    0 ?    SW   Okt12   0:00 [kjournald]
```

```
root 28179  0.0  0.0  1428  580 ?    S    Okt12   0:03 syslogd -m 0
root 31006  0.0  0.0  1364  452 ?    S    Okt12   0:00 klogd -x
root  5812  0.0  0.0  1528  672 ?    S    Okt12   2:45 /sbin/apcupsd -f
root   403  0.0  0.1  2912 1312 ?    S    Okt12   0:02 /usr/sbin/sshd
root 13003  0.0  0.0  2136  904 ?    S    Okt12   0:00 xinetd -stayalive
root 18286  0.0  0.1  4592 1768 ?    S    Okt12   0:29 sendmail
root  8421  0.0  0.3 73100 3988 ?    S    Okt12   0:10 /usr/sbin/httpd
```

Program *top* je tiež veľmi užitočným nástrojom zobrazujúcim procesorové zaťaženie jednotlivých procesov, a tým môžeme odhaliť zvýšenú aktivitu v systéme napr. pri dos útokoch a identifikovať zodpovedný proces.

```
[root@devsys /]# /mnt/cdrom/top
  8:55pm  up 12 days, 21:31,  3 users,  load average: 0.02, 0.01, 0.00
67 processes: 66 sleeping, 1 running, 0 zombie, 0 stopped
CPU0 states:  0.0% user,  0.2% systém,  0.3% nice, 99.0% idle
CPU1 states:  0.0% user,  0.0% systém,  0.0% nice, 100.0% idle
Mem:  1033728K av,  412740K used,  620988K free,   0K shrd,   90228K buff
Swap: 1535992K av,       0K used, 1535992K free            192112K cached

  PID USER  PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME COMMAND
 4246 mysql  19  10 18752  18M  1956 S N   0.5  1.8  12:59 mysqld
 9433 root   13   0  1064 1064   856 R     0.3  0.1   0:00 top
    1 root    9   0   492  492   428 S     0.0  0.0   0:11 init
    2 root    9   0     0    0     0 SW    0.0  0.0   0:00 keventd
    3 root   18  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU0
    4 root   19  19     0    0     0 SWN   0.0  0.0   0:00 ksoftirqd_CPU1
    5 root    9   0     0    0     0 SW    0.0  0.0   0:00 kswapd
    6 root    9   0     0    0     0 SW    0.0  0.0   0:00 bdflush
    7 root    9   0     0    0     0 SW    0.0  0.0   0:02 kupdated
    8 root    9   0     0    0     0 SW    0.0  0.0   0:00 scsi_eh_0
    9 root    9   0     0    0     0 SW    0.0  0.0   0:00 scsi_eh_1
   10 root    9   0     0    0     0 SW    0.0  0.0   0:05 kjournald
27198 root    9   0     0    0     0 SW    0.0  0.0   0:00 kjournald
28179 root    9   0   580  580   488 S     0.0  0.0   0:03 syslogd
31006 root    9   0   452  452   388 S     0.0  0.0   0:00 klogd
 5812 root    9   0   672  672   556 S     0.0  0.0   2:45 apcupsd
  403 root    9   0  1312 1312  1172 S     0.0  0.1   0:02 sshd
13003 root    9   0   904  904   732 S     0.0  0.0   0:00 xinetd
18286 root    9   0  1768 1768  1284 S     0.0  0.1   0:29 sendmail
```

Ukončenie podozrivého procesu môžeme vykonať príkazom *kill*

```
[root@devsys /]# /mnt/cdrom/kill -9 <pid podozrivého procesu>
```

8.4.2.4 Analýza adresára /proc

Súborový systém proc nie je v skutočnosti reálnym súborovým systémom. Ide o virtuálny systém reprezentujúci prístup k nastaveniam a štruktúram jadra systému. Tu sa môžeme dozvedieť množstvo informácii o samotnom systéme, ale najmä o spustených procesoch.

Každý spustený proces v systéme má na základe svojho identifikátora vytvorený adresár */proc/<pid procesu>,* v tomto adresári sa nachádzajú dôležité informácie o procese, ktoré nám pomôžu zistiť identitu spusteného procesu. Samotný adresár prislúchajúci jednotlivému procesu obsahuje nasledovné položky:

```
[root@devsys 3100]# ls -al
total 0
dr-xr-x---    3 apache   wheel           0 Jan 25 21:45 .
dr-xr-xr-x   80 root     root            0 Jan 13 00:24 ..
-r--r--r--    1 root     wheel           0 Jan 25 21:45 cmdline
-r--r--r--    1 root     wheel           0 Jan 25 21:45 cpu
lrwxrwxrwx    1 root     wheel           0 Jan 25 21:45 cwd -> /
-r--------    1 root     wheel           0 Jan 25 21:45 environ
lrwxrwxrwx    1 root     wheel           0 Jan 25 21:45 exe -> /usr/cap
dr-x------    2 root     wheel           0 Jan 25 21:45 fd
-r--r--r--    1 root     wheel           0 Jan 25 21:45 maps
-rw-------    1 root     wheel           0 Jan 25 21:45 mem
-r--r--r--    1 root     wheel           0 Jan 25 21:45 mounts
lrwxrwxrwx    1 root     wheel           0 Jan 25 21:45 root -> /
-r--r--r--    1 root     wheel           0 Jan 25 21:45 stat
-r--r--r--    1 root     wheel           0 Jan 25 21:45 statm
-r--r--r--    1 root     wheel           0 Jan 25 21:45 status
```

Najdôležitejšie položky sú adresáre *exe*, *fd*, a *cmdline.* Položka *cmdline* informuje s akými parametrami bol daný súbor spustený. Adresár *fd* informuje o otvorených súboroch daného procesu. Za otvorený súbor sa považuje aj sieťový socket.

```
[root@devsys fd]# ls –al
total 0
dr-x------ 2 root   wheel  0 Jan 25 22:10 .
dr-xr-x--- 3 apache wheel  0 Jan 25 21:45 ..
lr-x------ 1 root   wheel 64 Jan 25 22:10 0 -> /dev/null
l-wx------ 1 root   wheel 64 Jan 25 22:10 1 -> /dev/null
l-wx------ 1 root   wheel 64 Jan 25 22:10 15 -> /var/log/httpd/error_log
lrwx------ 1 root   wheel 64 Jan 25 22:10 18 -> socket:[959]
l-wx------ 1 root   wheel 64 Jan 25 22:10 19 -> /var/log/httpd/access_log
l-wx------ 1 root   wheel 64 Jan 25 22:10 2 -> /var/log/httpd/error_log
lrwx------ 1 root   wheel 64 Jan 25 22:10 4 -> /tmp/sess0.sem (deleted)
```

Položka *exe* ukazuje na súbor, ktorý proces spustil, pomocou nej sa môžeme dozvedieť, kde je súbor s programom uložený. Veľa útočníkov sa snaží zakryť pôsobenie v systéme napr. spustením a následným vymazaním súboru, ktorý je až do ukončenia procesu v skutočnosti iba odpojený zo súborového systému. V prípade takejto skutočnosti by informácia vyzerala nasledovne:

```
lrwxrwxrwx 1 root  wheel     0 Jan 25 21:45 exe -> /usr/cap (deleted)
```

Táto informácia znamená, že k súboru majú prístup už len procesy, ktoré ho mali predtým otvorený. Tento súbor je však možné obnoviť na základe nástrojov pracujúci na úrovni uzlov súborového systému.

8.4.2.5 Obnova vymazaných súborov

Systém LINUX pracuje tak, že každý súbor má pridelený počet odkazov na bežiaci proces. Ak sa súbor pokúsime vymazať príkazom *rm.* a neexistuje žiaden odkaz, potom sa súbor označí ako zmazaný a jeho miesto môže nahradiť nový súbor. Ak však počet odkazov procesov na súbor je nenulový, súbor sa len fyzicky odpojí zo súborového systému a čaká kým sa počet odkazov nezníži na 0. Počas tejto fázy môžu k súboru pristupovať len procesy, ktoré ho otvorili ešte pred zmazaním, teda pri výpise príkazu *ls* ho nie je vidno.

Na obnovu súboru môžeme použiť nástroj *icat.* Na to, aby sme súbor obnovili, musíme vedieť, v ktorom uzle súborového systému sa nachádza. To môžeme docieliť príkazom *lsof*

```
[root@devsys /]# /mnt/cdrom/lsof | grep sess0.sem
COMMAND     PID USER FD TYPE DEVICE SIZE  NODE   NAME
libhttpd.   917 root 3u REG  8,2       0  211798 /tmp/sess0.sem (deleted)
libhttpd.   917 root 4u REG  8,2       0  211801 /tmp/sess0.sem (deleted)
libhttpd.  3100 root 3u REG  8,2       0  211798 /tmp/sess0.sem (deleted)
libhttpd.  3100 root 4u REG  8,2       0  211801 /tmp/sess0.sem (deleted)
```

Práve stĺpec NODE nám vypisuje identifikátor uzlu, kde je súbor uložený, a to použitím príkazu:

```
[root@devsys /]# /mnt/cdrom/icat | /dev/hda5 211798 > /tmp/sess0.sem.recovery
```

- obnovíme zmazaný súbor.

8.4.2.6 Zoznam aktuálne otvorených sieťových spojení a ich bližšia analýza

Na rozdiel od systému Windows je utilita *netstat* postačujúca na kompletnú analýzu sieťových spojení. Zoznam počúvajúcich portov spolu s aplikáciou, ktorá daný port obsadila, dostaneme nasledujúcim príkladom:

```
[root@devsys /]# /mnt/cdrom/netstat –anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State  PID/Program name
tcp   0      0      0.0.0.0:3306  0.0.0.0:*       LISTEN 29008/
tcp   0      0      0.0.0.0:139   0.0.0.0:*       LISTEN 27586/smbd
tcp   0      0      0.0.0.0:80    0.0.0.0:*       LISTEN 8421/httpd
tcp   0      0      0.0.0.0:22    0.0.0.0:*       LISTEN 403/sshd
tcp   0      192    192.168.0.14:22 192.168.0.10:4240 ESTABLISHED
9788/sshd:
udp  0       0      0.0.0.0:137  0.0.0.0:*              27389/nmbd
udp  0       0      0.0.0.0:138  0.0.0.0:*              27389/nmbd
```

V prípade detekcie podozrivého procesu s neznámym otvoreným portom tcp/ip alebo udp/ip je dôležité ho detailne preskúmať. Podozrivé resp. nebezpečné programy často pracujú zo súborovým systémom do ktorého môžu ukladať zozbierané údaje. Na detekciu zoznamu súborov s ktorým podozrivý proces pracuje môžeme využiť príkaz lsof.

Nasledujúci príkaz zistí množinu používaných súborov podozrivým procesom *suir*

```
[root@devsys /]# /mnt/cdrom/lsof | grep 1005
suir  1005  root  mem  REG     8,2    41324     32803 /lib/libnss2.3.2.so
suir  1005  root  0u   CHR  136,10                12 /dev/pts/10
suir  1005  root  1u   CHR  136,10                12 /dev/pts/10
suir  1005  root  2u   CHR  136,10                12 /dev/pts/10
suir  1005  root  3w   REG     8,2       257   655920 /opt/suir/serve.log
suir  1005  root  5u   REG     8,2         0   655922 /opt/suir/SUIR.lck
suir  1005  root  6u  IPv4     322               TCP *:19010 (LISTEN)
suir  1005  root  7r  FIFO     0,5           4274323 pipe
suir  1005  root  8w  FIFO     0,5           4274323 pipe
suir  1005  root  9w   REG     8,2      7961   655924 /opt/suir/cfg.log
suir  1005  root 10w   REG     8,2    184167  1228905 /opt/suir/index.log
suir  1005  root 11w   REG     8,2      1322  1228906 /opt/suir/query.log
suir  1005  root 12w   REG     8,2     36835  1228907 /opt/suir/app.log
suir  1005  root 13u   REG     8,2        80  1228913 /opt/suir/dba.db
suir  1005  root 14u   REG     8,2  28056812  1228946 /opt/suir/dbc0.db
suir  1005  root 15u   REG     8,2 182059848  1228940 /opt/suir/dbd0.db
```

Príkaz odhalil, že podozrivý proces *suir* má otvorené súbory /opt/suir/dbd0.db a /opt/suir/dbc0.db, ktoré majú značnú veľkosť 182MB a 28MB. Mnohé parazitujúce procesy, ktoré sú nainštalované útočníkom do systému a zachytávajú dáta prechádzajúce systémom používajú veľké súbory na ukladanie všetkých získaných dát. Takýmto spôsobom môžeme získať bližšie informácie o charaktere podozrivého procesu.

Je takisto dôležité zistiť informáciu o stave sieťových adaptérov.

```
[root@devsys /]# /mnt/cdrom/ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:E0:4C:39:08:06
          inet addr:192.168.0.1 Bcast:195.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:4076919 errors:3 dropped:0 overruns:0 frame:0
          TX packets:2567018 errors:0 dropped:0 overruns:0 carrier:0
          collisions:11213 txqueuelen:100
          RX bytes:2426483034 (2314.0 Mb)  TX bytes:471660484 (449.8 Mb)
          Interrupt:12 Base address:0x6000
```

Potrebné je všimnúť si najmä tretí riadok, ktorý vypovedá, či je sieťový adaptér v promiskuitnom móde, a teda zachytáva všetku komunikáciu, ktorá ním prechádza. V prípade, že je tomu tak, môže to vypovedať o inštalovanom snifferi sieťovej komunikácie, a to znamená, že útočník má root prístup k systému.

8.4.2.7 Zoznam aktuálne nahlásených užívateľov

Systém Linux už od svojho vzniku umožňuje prihlásenie viacerých užívateľov do systému. Prítomnosť užívateľov v systéme môžeme zistiť príkazom: *w*,

```
[root@devsys /]# /mnt/cdrom/w
9:18pm  up 12 days, 21:54,  3 users,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
rastisla pts/0    192.168.0.9   Thu 9am  3days  0.06s  0.06s  -bash
rastisla pts/1    192.168.0.9   Thu 9am  2days  0.05s  0.00s  psql -U
martin   pts/2    192.168.0.10   8:36pm  0.00s  0.09s  0.01s  w
```

Tu je dôležité všimnúť si stĺpec TTY, ktorý hovorí či je užívateľ nahlásený lokálne alebo diaľkovo, v prípade tty/*n* kde n je nezáporné číslo ide o užívateľa nahláseného lokálne, v prípade pts/n alebo ttyp/n ide o užívateľa, ktorý je nahlásený diaľkovo. Položka IDLE nám môže odhaliť dĺžku pripojenia užívateľa a tým napr. odhadnúť časový rámec začiatku útoku. Stĺpec WHAT nám zas hovorí o práve vykonávanom procese užívateľa.

8.4.3 Pokročilá analýza

Nasledujúce kroky je možné vykonať rovnako offline aj online, záleží to od rozhodnutia samotného tímu pre reakcie na incident (vid. Formovanie plánu odstraňovania následkov incidentu). Pokiaľ nie je nevyhnutné, aby systém fungoval aj ďalej bez odstavenia, resp. pri incidentoch veľkých rozsahov, kde nemôžeme vylúčit možnosť kompromitácie jadra odporúčame offline analýzu. Offline analýza na rozdiel on online analýzy eliminuje možnosť získania falošných údajov, ktoré vznikajú modifikáciou jadra resp. dynamických knižníc operačného

systému. Samotnú offline analýzu odporúčame vykonať reštartom systému a nabootovania čistého nekompromitovaného systému z dôveryhodného média.

8.4.3.1 Protokoly udalostí systéme

Operačný systém Linux má v sebe zabudované účinné nástroje na monitorovanie udalostí v systéme. Stará sa o to služba *syslogd,* ktorá je spúšťaná pri štarte. Na základe zvolených kritérií vo svojom konfiguračnom súbore ukladá udalosti do protokolu na súborovom systéme.

V konfigurácii služby syslog môžeme nastaviť rôzne filtre pre logovania spolu z nastavením priority, podobne aj miesto uloženia protokolu na súborovom systéme. Jeden záznam o protokolovaní istej udalosti sa skladá z 3 častí položky FACILITY, PRIORITY a ACTION.

- Položka FACILITY označuje proces, ktorý danú udalosť vyvolal a môže sa jednať napr. o službu sshd alebo httpd, podobne ako aj vykonávanú aplikáciu.
- Položka PRIORITY zas stanovuje závažnosť zaznamenávanej udalosti v systéme, kde sú preddefinované jednotlivé stupne závažnosti, a to: *debug, info, notice, warning, err, crit, alert a emerg.*
- Posledná položka ACTION určuje, aké kroky systém podnikne pri výskyte popisovanej udalosti. Systém vykoná najčastejšie zápis udalosti do protokolu, resp. odoslanie udalosti na centrálny *syslogd* server.

Vzhľadom na súčasnú veľkosť diskového priestoru je vhodné monitorovať a zaznamenávať všetky udalosti a to nám napomáha neskôr pri vyšetrovaní incidentu. Nasledujúci riadok ukazuje, ako monitorovať všetky udalosti v systéme.

```
*.*  /var/log/allmessages
```

Po reštarte služby *syslogd* vytvorí v adresárovej štruktúre /var/log súbor allmessages, v ktorom budú protokolované všetky udalosti generované systémom. Ako už bolo spomenuté, pri prieniku útočníka do systému nie je možné zabrániť modifikácii protokolu systému, a tým znemožniť identitu útočníka, resp. sťažiť

vyšetrovanie incidentu. Odporúčame všetky udalosti zaznamenávať na bezpečnom centrálnom systéme, ktorý bude dostatočné chránený pred incidentmi (napr. bude poskytovať prístup len k syslogd službe). Takéto nastavenie vykonáme nasledujúcim riadkom v konfiguračnom súbore služby syslogd.

```
*.*  @syslogserver
```

Množstvo dôležitých služieb, ktoré sa samotné môžu stať cieľom útoku, má svoje vlastné monitorovanie udalostí (napr. služby httpd alebo sendmail). Tieto protokoly udalostí generované práve týmito službami nám poskytujú rozšírené informácie pri vyšetrovaní incidentu. Podobne, ako pri službe *syslogd,* aj tu sa dá nastaviť druh protokolovaných udalostí, ako aj zaznamenávané detaily o udalosti vyskytnutej v systéme.

8.4.3.2 Skúmanie protokolov udalostí

Samotné informácie poskytnuté protokolmi udalostí sú neoceniteľné pri samotnom procese reakcie na incident. Existuje úzka skupina udalostí, na ktoré by sme sa mali zamerať v počiatočných štádiách reakcie na incident.

Pokusy o prihlásenie je prvá kategória, na ktorú by sme mali zamerať. Tie poskytujú záznamy o úspešných alebo neúspešných pokusoch na prihlásenie do systému. Najviac by sme sa mali zamerať najmä na pokusy prihlásenie do systému s užívateľským menom root resp. v prípade podozrenia na ten ktorý užívateľský účet.

Služba *cron* je často využívaná na opakované spúšťanie nástrojov na získavanie informácii a dát v systéme. Táto služba všetky pokusy o spustenie zaznamenáva v protokole systému a preto je ich potrebné vyhľadať a vyšetriť.

Pomocou protokolu udalostí môžeme s dostatočne veľkou presnosťou určiť časový rámec začiatku incidentu a na základe toho zvoliť potrebnú stratégiu pre obnovu systému, resp. vyhľadanie modifikovaných súborov.

8.4.3.3 História použitých príkazov a spustených aplikácii

Operačný systém Linux poskytuje efektívny nástroj na prezeranie spustených procesov užívateľom systému. Pomocou príkazu *lastcomm* alebo *acctcom* si môžeme históriu ľahko prezrieť. Aj napriek tomu, že súbor je binárny, nezabráni to útočníkovi tento súbor modifikovať.

Takmer každý štandardný shell umožňuje zaznamenať použité príkazy v systéme. Najrozšírenejší shell je *bash*. Každému užívateľovi v systéme vytvorí vo jeho domovskom adresári súbor *.bash_history,* do ktorého sa jednotlivé použité príkazy zaznamenávajú.

```
[root@devsys /]# /mnt/cdrom/less ~martin/.bash_history
```

Týmto príkazom môžeme jednoducho prezrieť históriu použitých príkazov a vyhľadať podozrivé úkony užívateľa *Martin*.

8.4.3.4 Skúmanie súborového systému

V systéme Linux/Unix existujú isté špecifické typy súborov, ktoré sa pravidelne vyskytujú pri incidentoch. Sú to súbory, ktoré majú nastavené atribúty SUID a SGID, skryté súbory a adresáre, konfiguračné súbory a obsah adresára /tmp.

Súbory s atribútmi SUID a SGID

Tieto zvlášť dôležité atribúty sú v systéme používané na zmenu užívateľských práv. Môže ísť o zvýšenie úrovne práv ako aj o jej zníženie. V prípade, že atribúty spúšťaný súbor nemá nastavené, znamená to, že nedochádza k zmene úrovne prístupových práv a teda súbor je spustený s rovnakými právami ako sú práva užívateľa ktorý súbor spustil. V prípade, že súbor ma atribút SUID (set userid) nastavený, súbor bude spúšťaný s právami vlastníka súboru. Podobnú funkciu má aj atribút SGID rozdiel je len, že program bude spustený s pravidlami skupiny ktorá súbor vlastní.

Práve v zneužití tejto funkcie môže útočník získať prístup s právami root. Preto je vždy pri výskyte incidentu potrebné tieto súbory vyhľadať. Nasledujúci príkaz nám práve tieto súbory v systéme identifikuje.

Vypíše súbory vlastniace SUID atribút

```
[root@devsys /]#/mnt/cdrom/find / -perm -004000 –type f –print
```

Vypíše súbory vlastniace SGID atribút

```
[root@devsys /]#/mnt/cdrom/find / -perm -002000 –type f –print
```

Vypíše súbory vlastniace aspoň jeden z atribútov SUID alebo SGID

```
[root@devsys /]#/mnt/cdrom/find / -perm +006000 –type f -print
```

V prípade, že hore uvedený príkaz nájde neznáme podozrivé súbory často sa práve jedná o systémový shell. Preto je potrebné nasledujúcim spôsobom overiť a skontrolovať identitu podozrivého súboru.

```
[root@devsys /]#/mnt/cdrom/ls –al /tmp/.gwfa
-rwsr-xr-x    1 root root       626124 Apr  9  2003/tmp/.gwfa

[root@devsys /]#/mnt/cdrom/md5sum /bin/bash
8d0019403be9b4f25e15f666bc2b9c92  /bin/bash
[root@devsys /]#/mnt/cdrom/md5sum /tmp/.gwfa
8d0019403be9b4f25e15f666bc2b9c92  /tmp/.gwfa
```

Skryté súbory, adresáre, blokové a znakové zariadenia

V systéme Linux sa všetky súbory začínajúce znakom (bodka) považujú za skryté, a teda pri nepoužití prepínača –a v príkaze *ls,* sa súbor neobjaví v jeho výstupe. Útočníci často využívajú zdanlivo neškodné názvy, aby tým nevzbudili pozornosť. Detailná znalosť systému napomáha pri odhalení prítomnosti nových blokových alebo znakových zariadení resp. pri zmene nastavení prístupových práv k týmto zariadeniam. Obvykle sú tieto zariadenia uložené v adresári /dev.

Nasledujúci príkaz nájde všetky blokové zariadenia prítomné v systéme.

```
[root@devsys /]#/mnt/cdrom/find / -type b –print
```

Nasledujúci príkaz nájde všetky znakové zariadenia prítomné v systéme.

```
[root@devsys /]#/mnt/cdrom/find / -type c –print
```

Skúmanie a identifikácia týchto zmien na súborovom systéme vyžaduje neobyčajnú pozornosť a znalosť postihnutého systému. Samotnému tímu by mala napomôcť detailná dokumenácia o systéme resp. kontakt na osobu, ktorá systém spravuje.

Dočasné súbory a adresár /tmp

Dočasné súbory v systéme často poskytujú informácie o dianí v systéme. Medzi súbormi môžeme odhaliť podozrivé súbory, ktoré môžu odhaliť podozrivé procesy, alebo prebiehajúcu aktivitu v systéme. Systém Linux má pre dočasné súbory určený adresár */tmp*, ktorý vzniká pri inštalácii operačného systému.

Konfiguračné súbory

Konfiguračné súbory dokážu úplne modifikovať podstatu určenia systému, čo útočníci často využívajú. Pomocou nich si zabezpečujú prístup k jednotlivým častiam systému. Je vhodné skontrolovať konfiguračné súbory, resp. ich porovnať so zálohou a odhaliť prípadné zmeny či už v samotnom obsahu resp. nastavení atribútov pristupových práv k týmto súborom. Príkladom modifikovaných súborov môžu byť súbory:

```
/etc/host.allow
/etc/host.deny
/etc/sysconfig/iptables
/etc/inetd.conf
/etc/httpd/httpd.conf
```

Je potrebné skontrolovať časti systému, ktoré zaručujú spúšťanie jednotlivých procesov v systéme. Je to najmä služba *cron,* preto je potrebné skontrolovať súbor:

```
/etc/cron.conf
/etc/cron.hourly
/etc/cron.daily
/etc/cron.weekly
/etc/cron.monthlyo
```

Ďalšími miestami sú zavádzajúce oblasti systému, určené pre konkrétny *runlevel*.

Súbory určené pre spustenie aktuálne použitého *runlevelu* nájdeme v adresári /etc/rc.d, ktorý je symbolickým linkom na adresár použitého runlevelu. Tam sa okrem štandardných služieb môžu nachádzať aj podozrivé programy nainštalované útočníkom a teda je potrebné okrem novo vzniknutých súborov

skontrolovať aj modifikáciu štandardných súborov. Často zneužívanými sú aj súbory *.login*, *.profile*, *.bashrc*, *.cshrc* a *.exrc*, ktoré sa nachádzajú v domovskom adresári jednotlivých systémových užívateľov, preto je ich potrebné dôkladne preskúmať pre prítomnosť podozrivých záznamov.

8.4.3.5 Prezeranie súborov určených pre užívateľské účty a užívateľské skupiny

Najdôležitejšími súbormi zasluhujúce si pozornosť sú súbory:

`/etc/passwd` – Tento súbor je primárne určený na zaznamenanie užívateľských účtov v systéme spolu z ďalšími informáciami.

```
gobles:x:38:54:Jan Gobles:/home/gobles:/bin/bash
```

Jedná sa o riadok z tohto súboru, okrem názvu užívateľského mena *gobles* sú v ňom uložené ďalšie informácie.

- x – miesto pre zašifrované heslo x znamená, že heslo je uložene v súbore */etc/shadow*
- 38 – identifikačné číslo užívateľského účtu
- 54 – identifikačné číslo užívateľskej skupiny
- Jan Gobles – dodatočná informácia o užívateľskom účte
- /home/gobles – miesto domovského adresára
- /bin/bash – použitý shell

Najviac dôležité je prezrieť si, či sa v systéme nachádza užívateľský účet s id 0, to by vypovedalo o účte s rootovskými právami.

`/etc/shadow` - tento súbor väčšinou obsahuje zašifrované heslá pre jednotlivé užívateľské účty.

`/etc/groups` – Súbor udržuje informácie o členstve jednotlivých užívateľských účtov v užívateľských skupinách.

8.4.4 Obnova poškodeného systému

Operačný systém linux je zo zálohovacích médií pomerne ľahko obnoviteľný. V prípade detailnej znalosti, ktoré súbory boli zmenené resp. následkom incidentu poškodené, k čomu nám pomôže metóda kontrolných súčtov (viď kap. „Vytváranie kontrolných súčtov“), resp. čas a dátum modifikácie súborov, v mnohých prípadoch stačí obnoviť dané súbory a netreba reštaurovať systém z inštalačných médií.

9 Prehľad nástrojov na priloženom CD

Väčšina programov umiestnená na CD je dynamicky linkovaná, preto v prípade podozrenia na kompromitáciu jadra resp. dynamických linkovaných knižníc, odporúčame vykonať offline analýzu nabootovaním operačného systému z dôveryhodného média.

Nástroj	Popis
/RH80	
bash	prostredie pre príkazový riadok
cat	nástroj na výpis súboru na obrazovku
cp	nástroj na kopírovanie obsahu súborového systému
cryptcat	program na vytvorenie šifrovaného dátového spojenia medzi počítačmi
dd	utilita na kopírovanie a konverziu súborov a zariadení
depmod	nástroj na zistovanie závislostí dynamických modulov jadra
df	utilita zobrazujúca voľné miesto na diskoch
du	program pre zistovanie použitého diskového priestoru
file	nástroj na zistenie typu súboru
find	nástroj na vyhľadávanie súboru na základe zvoleného ktitéria v adresárovej štruktúre
grave-robber	nástroj na získavanie rôzných informací o stave systému
gzip	komprimačný nástroj
chgrp	program na modifikáciou skupiny súboru
chmod	nástroj na modifikáciu prístupových práv k súboru
chown	program na modifikáciou vlastíka súboru
chroot	utilita spúštajúca príkaz alebo shell v špeciálnom korenovom adresári
icat	nástroj na prácu z súborovými uzlami
id	program na zobrazenie identifikačných údajov užívateľa
ifconfig	program zobrazujúci informácie o sieťových adaptéroch
ils	nástroj na zobrazovanie informácií uzla súborového systému
insmod	program na nahratie dynamického modulu do jadra
kill	nástroj ukončovanie procesu
last	príkaz zobrazujúci posledne nahlásených užívateľov do systému
lastcomm	prikaz na prehliadanie posledne spustených príkazov
ls	nástroj na výpis obsahu adresára
lsmod	príkaz zobrazuje aktuálne moduly v jadre systému
lsof	utilita na zobrazenie otvorených súborov
mactime	nástroj na vyhľadavanie súborov modifikovaných/vytvorených/pristúpených v istom časovom intervale
md5sum	utilita vytárajúca md5 kontrolné súčty
mkdir	príkaz na vytváranie adresárov
modinfo	nástroj na zobrazenie informácie o moduloch v jadre
more	pomocná utilita na zobrazovanie rozsiahleho výpisu na obrazovku
mv	program na presúvanie premenovanie súborov resp. adresárov
netstat	nástroj na prácu so sieťovými socketmi
pcat	nástroj na kopírovanie obsahu pamete procesu
ps	príkaz zobrazujúci bežiace procesy
rm	príkaz na odstránenie súborov
rmdir	nástroj na mazanie prázdnych adresárov
rmmod	utilita na odstranenie dynamického modulu z jadra
shutdown	nástroj na ukončenie behu systému

strace	program na sledovanie systémových volaní a signálov
su	utilita spúšťajúca shell pod iným užívateľom a skupinou
tail	nástroj na zobrazenie konca súboru
tar	nástroj na prácu z súbrovými archívmi
top	zobrazuje procesy zoradené podľa zaťaženia CPU
unix_tools	Kontrolný md5 súčet pre obsah adresára RH80
vi	textový editor
w	príkaz zobrazujúci aktuálne nahlásených užívateľov
/WinNT/gui_tools	
AccessEnum.exe	Nástroj na analýzu užívateľského prístupu k adresárom a súborom
autoruns.exe	Nástroj vypisujúci zoznam všetkých programov automaticky spúšťaných pri štarte systému
eventvwr.msc	Konzolový snap-in modul pre čítanie protokolu systémových udalostí
gui_tools.md5	Kontrolný md5 súčet pre obsah adresára gui_tools
mmc.exe	Kontajner pre systémové konzoly
PORTMON.EXE	Nástroj na analýzu komunikácie cez sériové porty
procexp.exe	Nástroj na manipuláciu bežiacich procesov v systéme
Regmon.exe	Nástroj slúžiaci na sledovanie práce zo systémovými registrami
RFV.exe	Nástroj na offline analýzu registrov systému
RootkitRevealer.exe	Nástroj slúžiaci na odhalenie prítomnosti root-kitov
Tcpview.exe	Nástroj na sledovanie otvorených TCP/UDP portov
TDIMON.EXE	Nástroj na sledovanie stavu TCP/UDP komunikácie
TOKENMON.EXE	Nástroj na sledovanie získavania systémovych tokenov procesmi
/WinNT/ir_script	
Fport.exe	Konzolový nástroj na sledovanie otvorených TCP/UDP portov
ir.bat	Dávkový súbor pre okamžitú analýzu stavu systému
ir_script.md5	Kontrolný md5 súčet pre obsah adresára ir_script
nbtstat.exe	Konzolový nástroj pre manipuláciu s protokolom netbios
netstat.exe	Konzolový nástroj pre zobrazovanie otvorených TCP/UDP spojení
psloggedon.exe	Konzolový nástroj zobrazujúci zoznam posledných prihlásení do systému
psservice.exe	Konzolový nástroj na prácu zo systémovými službami
tlist.exe	Konzolový nástroj zobrazujúci zoznam bežiacich procesov v systéme
/WinNT/shell_tools	
AFind.exe	Konzolový nástroj vyhľadávajúci súbory podľa posledného prístupu k nim
arp.exe	Konzolový nástroj pre protokol ARP
at.exe	Konzolový nástroj pre manipuláciu naplánovaných úloh
Audited.exe	Konzolový nástroj na analýzu protokolovaných súborov v systéme
Auditpol.exe	Konzolový príkaz na zobrazenie stavu auditu v systéme
autorunsc.exe	Konzolový nástroj zobrazujúci súbory spúšťajúce sa pri štarte
cmd.exe	Originálny shell pre WinNT
cryptcat.exe	Konzolový nástroj pre šifrovanú TCP/UDP komunikáciu
doskey.exe	Konzolový príkaz zobrazujúci históriu príkazov
dumpel.exe	Konzolový nástroj na analýzu protokolov
FileStat.exe	Konzolový príkaz získavajúci informácie o NTFS security záznamoch
Fport.exe	Konzolový príkaz zobrazujúci otvorené tcp/udp porty a ich vlastníkov
HFind.exe	Konzolový nástroj vyhľadávajúci skryté súbory s posledným prístupom
Hunt.exe	Konzolový príkaz získavajúci zoznam zdieľaných adresárov v systéme
LISTDLLS.exe	Konzolový príkaz analyzujúci pripojené DLL knižnice k bežiacim procesom
md5sum.exe	Konzolový príkaz na vytváranie kontrolných súčtov algoritmov md5
nbtstat.exe	Konzolový nástroj na získavanie informácii o netbios protokole
net.exe	Konzolový nástroj na rozličnú manipuláciu zo systémom
netstat.exe	Konzolový príkaz zobrazujúci existujúce TCP/UDP spojenia resp. servery
NTLast.exe	Konzolový príkaz informujúci o posledne nahlásených užívateľoch
psexec.exe	Konzolový príkaz umožňujúci diaľkové spúšťanie procesov
psfile.exe	Konzolový príkaz zobrazujúci používané súbory cez službu zdieľanie
psgetsid.exe	Konzolový príkaz získavajúci SID identifikátor
Psinfo.exe	Konzolový príkaz na získavanie informácie o systéme
pskill.exe	Konzolový príkaz ukončujúci bežiace procesy v systéme

pslist.exe	Konzolový príkaz zobrazujúci bežiace procesy v systéme
psloggedon.exe	Konzolový príkaz zobrazujúci o prihlásených užívateľoch do systému
psloglist.exe	Konzolový nástroj na získavanie dát z protokolu udalostí
pspasswd.exe	Konzolový príkaz na zmenu hesla na lokálnom alebo vzdialenom systéme
psservice.exe	Konzolový príkaz, ktorý zobrazuje a ovláda služby v systéme
psshutdown.exe	Konzolový nástroj na ukončenie behu systému
pssuspend.exe	Konzolový príkaz ktorý pozastaví a prebudí bežiaci proces v systéme
Reg.exe	Konzolový nástroj na prácu z registrami systému
rootkitrevcons.exe	Konzolový nástroj na odhalenie prítomnosti „root-kitov“ v systéme
SFind.exe	Konzolový nástroj na vyhľadávanie alternatívnych prúdov súboru na disku
shell_tools.md5	Kontrolný súčet programov v aktuálnom adresári
tcpvcon.exe	Konzolový nástroj na analýzu TCP/UDP spojení
tlist.exe	Alternatívny konzolový nástroj zobrazujúci bežiace procesy v systéme

10 Záver

Práca priniesla všeobecný pohľad do úvodu reakcie na incidenty, využitím spomínaných metodík a postupov môže tím pre reakciu na incidenty dostatočne minimalizovať škody napáchané výskytom incidentu. Práca sa najprv zamerala na vysvetlenie pojmu incident a reakcie na incident, spolu s uvedením kategorizácie jednotlivých incidentov. Práca sa snažila vysvetliť problematiku reakcie na incidenty a stanoviť odporúčania, ktoré by organizácia mohla využiť na tvorbu svojich vlastných plánov reakcie na incident. V poslednej kapitole boli uvedené konkrétne kroky reakcie na incident v prostredí operačných systémov WINDOWS a LINUX.

Práca však detailne nerozoberá špecifické postupy, ktoré treba aplikovať v prípade postihnutia špecifických systémov a použitých technológii. Reakciu v týchto prostrediach prenecháva na samotný tím pre reakciu na incidenty, ktorému k tomu môže dopomôcť dodávaná dokumentácia a analogické použitie postupov spomínaných v tejto práci.

Využitie práce spočíva v prevzatí jednotlivých odporúčaní v oblasti reakcie na incident samotnou organizáciou a doplnením reakcie na incidenty pre špecifické systémy, ktoré organizácia obsahuje.

Problematika reakcie na incident sa bude ďalej vyvíjať vzhľadom na neklesajúci počet incidentov, čo prinesie nové modernejšie postupy. Doplnením nových poznatkov a použitím uvedených odporúčaní by mal byť tím vždy dostatočne pripravený reagovať na vzniknutý incident.

A. Smernica pre reakciu na incidenty

Všeobecné pravidlá pre reakciu na incidenty	
Všetko zdokumentovať. Vhodné doplniť o včasné komentáre o tom, kto, čo kedy a prečo.	
Používať metodologické postupy schválené tímom pre reakciu na incidenty.	
Používať komunikáciu nezávislú od napadnutého systému ako telefón, fax alebo osobné stretnutia. Útočník môže komunikáciu odpočúvať.	
Udržiavať pravidelnú komunikáciu medzi jednotlivými časťami tímu pre reakciu na incidenty alebo inými zainteresovanými osobami.	
Predísť reštartu, odhláseniu resp. nahláseniu do systému, alebo spúšťanie akéhokoľvek podozrivého kódu.	
Detekcia a počiatočný odhad.	
1.1	Kontaktovať tím pre reakciu na incident, ak ide o pravý incident.
1.2	Preskúmať záznamy stavu systému pre neobvyklú aktivitu alebo chýbajúce záznamy o stave systému.
1.3	Prehľadať systém pre nástroje používané hackermi (nástroje na lámanie hesiel, trojské kone a pod.).
1.4	Skontrolovať, či sa v systéme pri štarte nespúšťajú neautorizované aplikácie.
1.5	Preskúmanie užívateľských účtov vzhľadom na zvýšenie privilégií alebo novo vytvorené účty alebo skupiny.
1.6	Skontrolovať výskyt podozrivých procesov.
1.7	Zistiť, či dôkazy o incidente majú byť zachovávané.
1.8	Priradiť prioritu incidentu a ustanoviť vedenie obnovy pre incident.
Informovanie o incidente	
2.1	Informovať o incidente manažment a vedúceho tímu pre reakciu na incident.
Minimalizácia poškodenia	
3.1	V závislosti od závažnosti incidentu a bezpečnostnej politiky, zvážiť izoláciu systému resp. ich vypnutie.
3.2	Zmeniť prístupové heslá na postihnutých systémoch.
Zistenie rozsahu a miery poškodenia	
4.1	Určenie presného typu a zámeru útoku.
4.2	Identifikácia zasiahnutých systémov.
4.3	Prehodnotenie, a ak je nutné zmena priority incidentu.
Formovanie plánu reakcie	
5.1	Vytvorenie postupu, ktorý bude použitý pri zbieraní dôkazov a následnej obnovy systému.
Ochrana dôkazov	
6.1	Odzálohovanie celého systému.
6.2	Ochrániť dôkazy a dokumentovať kto, kedy a ako pristúpil k systému.
Notifikácia externých organizácii	
7.1	Notifikovať organizácie zaoberajúce sa bezpečnostnými incidentmi podľa vopred vypracovaného zoznamu.
7.2	Ak je nutné, informovať verejnosť resp. partnerov pomocou hovorcu organizácie.
Obnova systému	
8.1	Identifikácie poslednej nepoškodenej zálohy a následná obnova z nej.
8.2	Overiť správnosť fungovania obnoveného systému.
8.3	Dodatočné zabezpečenie systému voči vyskytnutému incidentu.
Zhrnutie vzniknutej dokumentácie	
9.1	Zhrnutie poznámok, záznamov a získaných údajov do záverečnej správy.
9.2	Zhodnotenie dôvodu výskytu incidentu a možnosti predchádzania.
Výpočet vzniknutej škody	
10.1	Vyčísliť vzniknutú škodu ako finančnú, tak aj nefinančnú.
Aktualizácia plánov pre reakciu na incident.	
11.1	Úprava postupov pre reakciu na incident podľa nových získaných skúseností.

B. Zoznam literatúry

- Borodkin Michelle. 2001. Computer Incident Response Team. © SANS Institute http://www.sans.org
- Bull Jon. 2001. An Introduction to Incident Response and Handling in a Microsoft Environment: A Primer for the Unprepared Administrator © LabMice http://www.labmice.net
- Burke Joseph. 2003. Windows Forensic How-to: Incident Response Plan or Abuse of Corporate Assets © SANS Institute http://www.sans.org
- Carvey H.Win2K First Responder's Guide. 2002 © SecurityFocus http://www.securityfocus.net
- Computer Incident Handling and Response. © LabMice http://www.labmice.net/Security/incidentresponse.htm
- Cook Chad. 2000. An Introduction to Incident Handling © SecurityFocus http://www.securityfocus.net
- Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd Edition
- Fast Path to Security Incident Response and Recovery 2000 © Microsoft Corporation http://www.microsoft.com/technet/security/tips/IRespDR.asp
- Feringa Alexis, Goguen Alice, Stoneburner Gary. 2001 Risk Management Guide for Information Technology Systems Special Publication 800-30 © National Institute of Standards and Technology
- Fraser B. SEI/CMU . 1997. RFC 2196 - Site Security Handbook http://www.faqs.org/rfcs/rfc2196.html
- Grance Tim, Kent Karen, Kim Brian. 2004 Computer Security Incident Handling Guide Special Publication 800-61. © National Institute of Standards and Technology
- Chakravarthy Sannedhi. 2002 . Incident Response Checklist http://www.dpo.uab.edu/~kalyan/incidentchecklist.html
- Karney Brian .2003 . Incident Response and Forensics © Guidance Software

- Kelver Linda. 2002. Incident Response in A Global Environment Version 1.2b. © SANS Institute http://www.sans.org
- Mandia Kevin, Initial Response to Windows NT/2000 © Foundstone inc.
- Musson William. Basic Incident Response
- Prosise Chris, Mandia Kevin. 2002. Incident Response: Investigating computer crime. © Osborne
- R. van Wyk, Kenneth & Forno, Richard. 2001 Incident Response O'Reilly
- Richardson Robert. 2003. CSI/FBI Computer Crime and Security Survey
- Securing Windows 2000 Server. 2003. © Microsoft Corporation
- Theunissen David. 2001. Corporate Incident Handling Guidelines Version 2.0 © SANS Institute http://www.sans.org
- Tidd Ronald 2003.Incident Response- Investigation Cyber Crime, Security & Computer Forensics
- Windows 2000 Server Disaster Recovery Guidelines. 2000 © Microsoft Corporation http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/recovery.asp