en
cs de
sk es

TECH
pedia

# MODERNÉ BEZPEČNOSTNÉ SYSTÉMY

MIGUEL SORIANO

**Názov:** Moderné bezpečnostné systémy
**Autor:** Miguel Soriano
**Preložil:** Martin Broda, Vladimír Hajduk
**Vydalo:** České vysoké učení technické v Praze
Fakulta elektrotechnická
**Kontaktná adresa:** Technická 2, Praha 6, Česká republika
**Tel.:** +420 224352084
**Tlač:** (iba elektronická)
**Počet strán:** 43
**Edícia (vydanie):** 1. vydanie, 2017

**ISBN** 978-80-01-06210-4

**TechPedia**
European Virtual Learning Platform for
Electrical and Information Engineering
http://www.techpedia.eu

Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

# VYSVETLIVKY

| | |
|---|---|
|  | Definícia |
|  | Zaujímavosť |
|  | Poznámka |
|  | Príklad |
|  | Zhrnutie |
|  | Výhody |
|  | Nevýhody |

# ANOTÁCIA

Modul obsahuje dôležité informácie pre základnú orientáciu študentov v oblasti sieťovej bezpečnosti, pričom obsahuje poznatky o službách a mechanizmoch bezpečnosti, typoch útočníkov, bezpečnostných hrozbách a tiež popis zložiek sieťového bezpečnostného systému.

# CIELE

Tento modul poskytuje celkový prehľad v oblasti moderných bezpečnostných systémov, pričom obsahuje šesť kapitol.

Prvá kapitola sa zaoberá konceptom sieťovej bezpečnosti z pohľadu služieb a mechanizmov bezpečnosti. Druhá kapitola rieši problematiku bezpečnostných hrozieb v sieťach, pričom dôraz je kladený na koncept vírusov, červov, trójskych koní, ďalej na spyware a adware, útoky nultého dňa, odpočúvanie a krádež dát, spoofing a krádež identity.

Tretia kapitola obsahuje popis niektorých zložiek sieťového bezpečnostného systému (antivírus, bezpečnostné brány (firewally), systémy detekcie prieniku, VPN atď.). Štvrtá kapitola prezentuje ďalšie bezpečnostné riešenie v rámci problematiky sietí (napr. silnú autentifikačnú metódu, hardening (nastavenie) operačného systému, ochranu webových služieb atď.).

Posledná kapitola je venovaná mobilnej bezpečnosti, keďže v súčasnosti majú smartfóny nezastupiteľnú úlohu v našom živote ako prostriedok na modernú formu komunikácie. Z povahy týchto zariadení vyplýva možnosť aplikovať nové typy útokov. V tejto kapitole je znázornené ako môže útočník profitovať z nášho kompromitovaného smartfónu.

# LITERATÚRA


[1] CVE. A dictionary of publicly known information security vulnerabilities and exposures. http://cve.mitre.org; 2015

[2] W. Cheswick and S. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994. ISBN

[3] E. D. Zwicky, S. Cooper, and D. B. Chapman. *Building Internet Firewalls.* O'Reilly and Associates, 2nd edition, 2000. ISBN.

[4] João Porto De Albuquerque , Paulo Lício De Geus "A Framework for Network Security System Design".

[5] L. Bilge and T. Dumitraş, "Before we knew it: An empirical study of zero-day attacks in the real world," in ACM Conference on Computer and Communications Security, Raleigh, NC, 2012, pp. 833–844.

[6] Kim Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishers, 2014. ISBN: 978-0-7704-3617-9

[7] Adeyinka, O., "Internet Attack Methods and Internet Security Technology,", 2008. AICMS 08. Second Asia International Conference on Modeling & Simulation pp.77-82, ISBN: 978-0-7695-3136-6

[8] Thomas W. Shinder The Best Damn Firewall Book Period (Second Edition), Syngress Publishing Inc. 2007. ISBN: 978-1-59749-218-8

[9] Karen Scarfone, Paul Hoffman. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-41, Revision 1. Sept. 2009

[10] Eric Geier “Intro to Next Generation Firewalls” http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html September, 2011

[11] Cliff, A.: “Password Crackers - Ensuring the Security of Your Password”, Security Focus, Feb. 19, 2001. http://online.securityfocus.com/infocus/1192

# Obsah

# 1 Úvod

Svet je čoraz viac prepojený pomocou Internetu a nových sieťových technológií, pričom za posledných pár rokov služby ako e-biznis alebo nákup cez Internet zlepšili svoju efektivitu a rast tržieb. Avšak s nárastom rôznych sieťových služieb a aplikácií a so zvyšovaním počtu ich používateľov vzniká problém so zraniteľnosťou voči rôznym typom bezpečnostných hrozieb. Preto je dôležité bojovať proti týmto hrozbám a zabezpečiť, aby sieťové operácie nemohli byť kompromitované. Bezpečnosť sietí by mala byť hlavná otázka pri ich návrhu nie len v oblasti aplikácií pre biznis sféru a armádu, ale tiež pre bežné organizácie a osobné počítače používateľov.

V minulosti mohol byť hackerom len programátor s vysokou úrovňou znalostí, ktorý rozumie detailom počítačovej komunikácie. Dnes každý z nás môže byť hackerom pomocou stiahnutia softvérového nástroja z Internetu. Tieto softvérové nástroje pre rôzne typy útokov a otvorené počítačové siete zvyšujú potrebu riešiť otázku sieťovej bezpečnosti a dynamických bezpečnostných pravidiel. Veľký počet organizácií sa snaží klasifikovať zraniteľnosť a jej dôsledky.Jedna z najvýznamnejších klasifikácií je národná databáza zraniteľnosti (National Vulnerability Database) vytvorená organizáciou MITRE [1].

Oblasť sieťovej bezpečnosti je veľmi obsiahla a stále sa vyvíja, pričom počet bezpečnostných incidentov stúpa alarmujúco každý rok. Aj napriek značným pokrokom v oblasti sietí a počítačovej bezpečnosti v posledných rokoch sú systémy stále viac zraniteľnejšie ako kedysi. Každý technologický pokrok a zvýšenie výpočtovej výkonnosti prináša nové bezpečnostné hrozby, ktoré potrebujú nové bezpečnostné riešenia. Rozvoj nových technológií však postupuje rýchlejšie ako je možné objavovať nové bezpečnostné riešenia. Vzhľadom na to, že počet bezpečnostných hrozieb narastá je nutné sa zaoberať ochranou sietí.

## 1.1 Čo je sieťová bezpečnosť


Sieťová bezpečnosť zahrňuje všetky aktivity realizované za účelom ochrany siete. Tieto aktivity konkrétne zabezpečujú použiteľnosť, spoľahlivosť, integritu, bezpečnosť siete a dát. Sieťová bezpečnosť je vyžadovaná pre všetky typy komunikácie vrátane biznis sféry, hlavne ak je realizovaná prostredníctvom Internetu.

Zákazníci, dodávatelia a obchodní partneri potrebujú chrániť všetky zdieľané informácie. Špeciálne tie, ktoré považujú za citlivé ako napr. čísla kreditných kariet alebo dôverné detaily podnikania.

Sieťová bezpečnosť nie je reprezentovaná len bezpečnosťou počítača na koncových stranách komunikácie, ale tiež pri prenose dát môže byť komunikačný kanál náchylný k určitému typu útoku. Hacker môže zachytiť komunikačný kanál, získať dáta, dešifrovať ich a následne vložiť do komunikačného kanála falošnú správu. Z toho vyplýva, že zabezpečenie siete je rovnako dôležité ako zabezpečenie počítačov a šifrovanie správy. Efektívne zabezpečenie siete sa zameriava na rôzne typy hrozieb, pričom ich rieši už na vstupe resp. zabraňuje ich rozšíreniu do siete.

Zabezpečenie siete je nevyhnutným predpokladom každého biznisu na Internete. Dôležitá požiadavka bezpečnosti je vyhnúť sa výpadkom služieb, pretože každé prerušenie siete znamená straty pre všetky typy podnikania. Efektívna bezpečnosť dovoľuje pridávať nové služby a aplikácie bez zhoršenia výkonnosti danej siete. Pri ochrane dát je nevyhnutný proaktívny prístup, aby sme sa vyhli prerušeniu zákazníckych služieb napr. pri aktualizácii systému.

Výhody pre biznis, ktoré plynú z bezpečných sietí sú: dôvera zákazníka (ochrana používateľa), mobilita (bezpečný prístup bez zavedenia vírusov alebo ďalších hrozieb), zvýšenie produktivity (menej času zaberajú neproduktívne úlohy ako spam alebo riešenie problémov s vírusmi) a ekonomika (výpadok siete je nákladná záležitosť pre všetky typy biznisu).

## 1.2 Čo je sieťový bezpečnostný systém?


Sieťový bezpečnostný systém tvorí skupina zariadení hardvérovo alebo softvérovo založených, ktoré využívajú bezpečné protokoly a kryptografické algoritmy s cieľom ochrániť informácie a komunikačné systémy spoločností.

Medzi hlavné funkcie týchto zariadení patrí monitorovanie a kontrolovanie prichádzajúcej a odchádzajúcej komunikácie, detekcia útokov, ochrana sieťovej infraštruktúry, ktorá zahrňuje sieťovú šírku pásma, bezpečnosť služieb a priebežnú ochranu voči útokom spôsobujúcim výpadok služieb a pod.

Keďže bezpečnostné potreby organizácií sú viac komplexné, tak sieťové bezpečnostné systémy a tradičné prístupy ako firewall musia prejsť cez niekoľko úprav. Napríklad začlenenie distribuovaných mechanizmov na presadzovanie bezpečnosti, decentralizované riadenie dôvery, a široko rozšírené využitie kryptografických techník (ako je IPSec a virtuálne privátne siete (VPN)).

Bezpečnostný sieťový systém, je len malá časť (aj keď dôležitá) informačnej bezpečnosti infraštruktúry organizácie, pričom musí byť posudzovaná spoločne s niekoľkými ďalšími oblasťami ako je fyzická bezpečnosť, osobná bezpečnosť, prevádzková bezpečnosť, komunikačná bezpečnosť a sociálne mechanizmy.

## 1.3 Bezpečnostné služby


Bezpečnostná služba je služba, ktorá zaistí adekvátnu bezpečnosť systémov alebo prenosov dát. Tieto služby sú implementované pomocou bezpečnostných mechanizmov na základe bezpečnostných pravidiel.

Už viac ako dvadsať rokov je informačná bezpečnosť založená na dôvernosti (confidentiality), integrite (integrity) a dostupnosti (availability) (známe ako trojica CIA). To sú základné princípy informačnej bezpečnosti. Neskôr, boli tieto prvky informačnej bezpečnosti pridané do tradičných bezpečnostných atribútov. Tieto prvky sú autentizácia, riadenie prístupu, nepopierateľnosť a súkromie. Takáto klasifikácia je predmetom debát medzi profesionálmi v tejto oblasti.

- Dôvernosť sa vzťahuje na ochranu informácií pred sprístupnením pre neoprávnené subjekty (organizácie, ľudia, stroje, procesy). Nikto nesmie čítať dáta s výnimkou subjektu (alebo subjektov) pre ktoré boli určené. Informácia zahŕňa dátový obsah, veľkosť, komunikačné vlastnosti, atď.

- Integrita dát je ochrana dát pred zmenou, odstránením, duplicity alebo premenovaním pomocou neoprávnených subjektov (organizácie, ľudia, stroje, procesy). Narušenie integrity je vždy spôsobené aktívnymi útokmi. Presnejšie povedané integrita označuje dôveryhodnosť informačných zdrojov.

- Dostupnosť znamená mať aktuálny prístup k informáciám. Napríklad poškodenie disku alebo útok vo forme zabránenia poskytnutia služby narušuje dostupnosť. Akékoľvek oneskorenie, ktoré prekročí očakávané hodnoty pre daný systém možno opísať ako porušenie dostupnosti. Informačný systém, ktorý nie je k dispozícii vtedy, keď ho používateľ potrebuje, je vnímaný rovnako zle ako keby vôbec neexistoval. Je to tým horšie, čím viac sa daná organizácia spolieha na fungovanie počítačovej a komunikačnej infraštruktúry.

- Služba overovania sa zaoberá kontrolou, že komunikujúce entity sú relevantné, t. j. overuje identitu komunikujúcich partnerov (ľudia, stroje, procesy). K dispozícii sú tri samostatné kategórie autentizačných faktorov, t. j. znalostná (knowledge), vlastniaca (possession) a inherentná (inherence) kategória. Medzi faktory znalosti patrí to, čo používateľ musí vedieť, aby sa dokázal prihlásiť. Faktor vlastnenia zahrňuje všetko to, čo používateľ musí mať vo svojom vlastníctve na prihlásenie. Inherentné faktory sú všetky biologické vlastnosti, ktoré musí mať používateľ a ktoré používa na potvrdenie prihlásenia.

- Riadenie prístupu je ochrana informácií alebo služieb pred možnosťou prístupu alebo pred použitím neoprávnenými osobami (organizácie, ľudia, stroje, procesy). To znamená, že riadenie prístupu sa vzťahuje k prevencii neoprávneného použitia prostriedku. Táto služba riadi to, kto môže mať prístup k určitým zdrojom a za akých podmienok. Prípadne tiež aké právomoci majú nastavené oprávnení používatelia a pod..

- Odmietnutie (non-repudiation) je bezpečnostná služba, ktorá sa používa ako ochrana proti výpadku jedného zo subjektov zapojených do komunikácie, ktorý sa zúčastnil celej komunikácie alebo len jej časti.

- Ochrana osobných dát je bezpečnostná služba, ktorá umožňuje kontrolovať aké informácie sú zhromažďované, prípadne ako a kto ich môže používať.

## 1.4 Bezpečnostné mechanizmy


Bezpečnostný mechanizmus je proces, ktorý implementuje bezpečnostné služby založené na hardvéri (technické), softvéri (logické) a fyzické alebo administratívne prístupy. Takýto mechanizmus podporuje bezpečnostné služby a spúšťa konkrétne aktivity na ochranu voči útokom resp. ich výsledkom.

Bezpečnostné mechanizmy sú rozdelené na tie, ktoré sú implementované v konkrétnych protokolových vrstvách a na tie, ktoré nepatria k žiadnej protokolovej vrstve alebo bezpečnostnej službe. Niektoré z bezpečnostných mechanizmov sú napríklad:

- Šifrovanie je mechanizmus zameraný na ochranu informačného obsahu správy pomocou matematických algoritmov, ktoré transformujú dáta do formy nečitateľnej neautorizovaným subjektom.
- Digitálny podpis je mechanizmus, ktorý používa kryptografickú transformáciu odtlačku dát s cieľom zabezpečiť overenie zdroja a integrity dát, pričom sa zabráni ich falšovaniu.
- Riadenie prístupu prostredníctvom rôznych mechanizmov presadzuje prístupové práva k určitým zdrojom. Tieto mechanizmy zahrňujú autorizáciu prístupu niektorých zdrojov.
- Dátová integrita obsahuje rôzne mechanizmy používané na uistenie sa o integrite dátovej jednotky alebo toku dátových jednotiek.
- Autentifikačná výmena je mechanizmus určený na zabezpečenie totožnosti prostredníctvom výmeny informácií.
- Traffic padding je mechanizmus, ktorý vkladá bity do medzier v dátovom toku aby zmaril pokusy o analýzu sieťovej prevádzky.
- Kontrola smerovania dovoľuje výber konkrétnych fyzicky bezpečných ciest pre určité dáta a umožňuje zmeny smerovania hlavne v prípade porušenia bezpečnosti. Tento mechanizmus tiež zahrňuje perimeter bezpečnosti.
- Certifikácia je mechanizmus, ktorý využíva dôveryhodnú tretiu stranu na zabezpečenie určitých vlastností výmeny dát.
- Perimeter bezpečnosti je mechanizmus umožňujúci prijatie alebo zamietnutie dát z alebo pre určitú adresu alebo službu umiestnenú mimo lokálnej siete.

## 1.5 Klasifikácia útočníkov

Bezpečnostné hrozby sú realizované útočníkmi, ktorých vo všeobecnosti rozlišujeme na základe ich schopností a činností. Pomocou zosumarizovania vlastností, ktoré sa týkajú schopností a činností útočníkov môžeme vytvoriť výsledný systém triedenia.

Schopnosť. Schopnosť útočníka je typicky vyjadrená nasledovne:

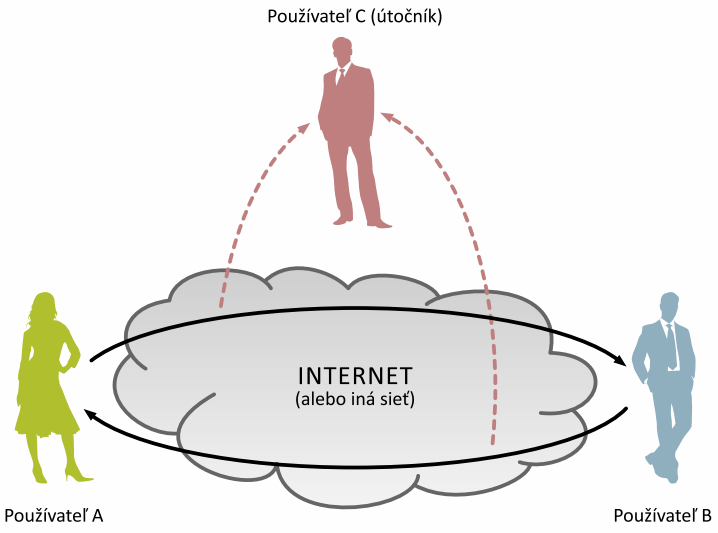
- Cena. Vzťahuje sa k nákladom, ktoré musí útočník vynaložiť z hľadiska zariadení, ktoré sú vyžadované na úspešné vykonanie útoku. Cena môže byť buď extrémne nízka, keď potrebuje napríklad len spájkovačku a nejaké káble alebo vysoká, pretože útočník potrebuje napr. kvalitné polovodičové testovacie zariadenie.

- Zručnosti. Pre úspešný útok musí mať útočník dobré znalosti a zručnosti. Niektoré typy útokov môže vykonávať neznalá osoba po vysvetlení inštrukcií. Na druhej strane iné útoky môžu vyžadovať pokročilé znalosti konkrétnych sieťových aplikácií resp. konkrétnu znalosť špeciálnych zariadení. (Táto vlastnosť môže byť tiež modelovaná ako cena.)

- Stopy. To sú stopy, ktoré sú zanechané po vykonaní útoku. Keď je po vykonaní útoku uzol v rovnakom stave ako pred útokom (nezmenený obsah pamäte), potom je ťažšie odhaliť daný útok ako v prípade útokov, ktoré spôsobujú fyzické zničenie uzla.

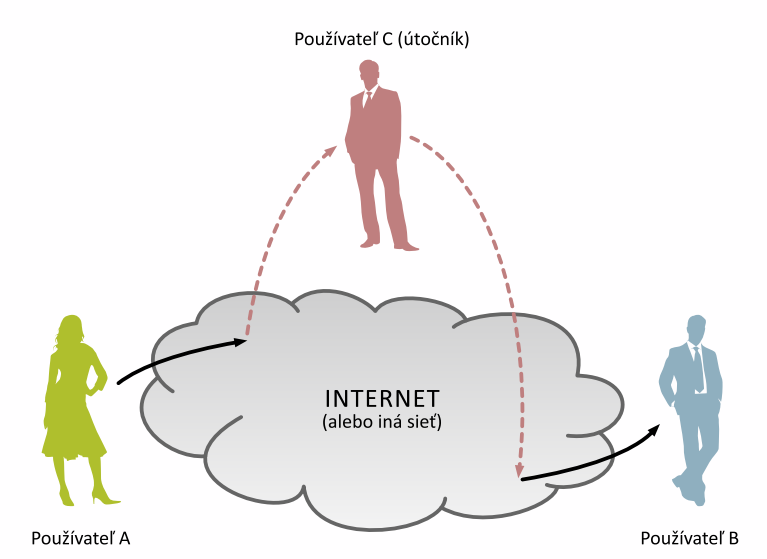
Aktivity. Útočiace aktivity môžu byť klasifikované ako pasívne a aktívne:

- Pasívne útoky. Tento typ útoku extrahuje informáciu zo siete jednoduchým monitorovaním komunikácie. Medzi tieto útoky patrí analýza záťaže siete, monitorovanie nechránenej komunikácie, dešifrovanie slabo šifrovanej prevádzky a zachytenie autentifikačných informácií ako sú heslá.




Obr. 1.1 – Pasívny útok

Aktívne útoky. Cieľom týchto útokov je meniť systémové prostriedky (vrátane dát) alebo ovplyvniť ich prevádzku. Tieto útoky zahŕňajú pridávanie (injection), modifikáciu alebo blokovanie dát vo forme sieťových paketov a manipuláciu s akýmkoľvek zariadením, ktoré sa zúčastňuje komunikácie. Niekedy pasívne útoky predchádzajú aktívnym.




Obr. 1.2 – Aktívne útoky

Ďalšie delenie na neinvazívne, poloinvazívne a invazívne útoky.

- Neinvazívne útoky. Tento typ útoku neovplyvňuje zariadenie.
- Poloinvazívne útoky. Predstavuje manipuláciu s obsahom zariadenia ale nie až napr. v priamom elektrickom kontakte s povrchom čipu.
- Invazívne útoky. Nemajú prakticky žiadne obmedzenie z hľadiska získavania informácií zo zariadenia (napr. sondovacia stanica).

Nie všetky poloinvazívne alebo invazívne útoky sú aktívne útoky. Napríklad pasívny poloinvazívny útok môže iba skúšať prečítať citlivé dáta z pamäťových komponentov. Pričom pasívny invazívny útok môže použiť sondovaciu stanicu na snímanie cenných dátových signálov. Príkladmi pasívnych útokov sú analýza prevádzky a kamuflovanie. Väčšina útokov sú však aktívne útoky ako napr. smerovacie útoky, spoofing, výpadok služieb, muž v strede (man-in-the-middle), odpočúvanie, replikácia uzla, fyzické útoky atď.

Triedy. Ďalšiu možnosť ako triediť útočníkov ponúka IBM. Ich taxonómia pozná tieto triedy útočníkov:

- Trieda I (múdri outsideri). Sú často veľmi inteligentní, ale môžu mať nedostatočnú znalosť systému. Môžu mať prístup len k mierne sofistikovanému zariadeniu. Často sa snažia využiť existujúce slabé miesta v systéme a nevytvárajú nové.

- Trieda II (znalí zasvätenci). Majú značné špecializované technické vzdelanie a skúsenosti. Majú rôzne stupne pochopenia častí systému, ale potenciálny prístup k väčšine z nich. Tiež majú často veľmi sofistikované nástroje a nástroje pre analýzu.

- Trieda III (fundované organizácie). Sú schopní zostaviť tímy odborníkov s príbuznými a doplňujúcimi zručnosťami, pričom sú podporovaní veľkými finančnými zdrojmi. Realizujú hĺbkovú analýzu systému, projektujú sofistikované útoky aj za použitia najmodernejších analytických nástrojov. Súčasťou ich tímu môžu byť aj útočníci triedy II.

## 1.6 Terminológia

Nie je možné poskytnúť kompletný slovník pojmov spojených s bezpečnosťou v rozsahu tejto kapitoly. Táto sekcia obsahuje niektoré z častejšie sa vyskytujúcich slov a fráz s ktorými sa čitateľ môže stretnúť, keď začína študovať problematiku sietí a počítačovú bezpečnosť:

- Útok. V kontexte počítačovej/sieťovej bezpečnosti, útok je pokus o prístup k zdrojom počítača alebo k sieti bez autorizácie, prípadne obídenie bezpečnostných opatrení.

- Audit. Sledovanie udalostí súvisiacich so zabezpečením ako je napríklad prihlásenie do systému alebo siete, prístup k objektom alebo nastaveniu používateľských/skupinových práv resp. privilégií.

- Porušenie. Úspešné prelomenie bezpečnostných opatrení na získanie prístupu k dátam alebo zdrojom bez autorizácie alebo sprístupnenie dát k dispozícii neoprávneným osobám, prípadne vymazanie alebo modifikácia počítačových súborov.

- Vyrovnávacia pamäť (Buffer). Uchovávacia oblasť pre dáta.

- Pretečenie zásobníka (Buffer overflow). Spôsob pádu systému, keď je do vyrovnávacej pamäte uložených viac dát ako je schopná uchovať.

- Protiopatrenia. Kroky na zabránenie útoku alebo odpoveď voči útokom či škodlivému kódu.

- Cracker. Hacker, ktorý sa špecializuje na crackovanie resp. objavovanie systémových hesiel za účelom získania prístupu do počítačových systémov bez autorizácie.

- Útok – Výpadok služby (Denial of Service). Zámerný zásah, ktorý udržuje počítač alebo sieť mimo prevádzky (napríklad zabraňuje používateľom prihlásiť sa do siete).

- Expozícia. Miera, kedy je sieť alebo osobný počítač otvorený útoku, čo je dané na základe konkrétnej zraniteľnosti resp. doba trvania kedy útočníci majú možnosť útoku.

- Hacker. Osoba, ktorá sa zaoberá učením detailov počítačového programovania a operačných systémov, pričom testuje ich limity a identifikuje zraniteľnosti v týchto systémoch.

- Škodlivý kód. Počítačový program alebo skript vykonávajúci činnosti, ktoré môžu zničiť systém alebo dáta pričom môže poskytovať neautorizovaný prístup do systému.

- Spoľahlivosť. Pravdepodobnosť počítačového systému alebo siete vykonávať bežnú činnosť v normálnych prevádzkových podmienkach v konkrétnom časovom období.

- Risk. Pravdepodobnosť, že konkrétna bezpečnostná hrozba bude schopná využiť systémovú zraniteľnosť. Výsledkom môže byť zničenie, strata dát alebo ďalšie neočakávané výsledky. To znamená, že riziko je súčtom hrozieb a zraniteľnosti.

- Manažment rizík. Proces identifikácie, riadenia a tiež minimalizácie alebo úplnej eliminácie udalostí, ktoré zahŕňajú hrozbu pre spoľahlivosť systému, integritu a dôvernosť dát.

- Sniffer. Program zachytávajúci dáta, ktoré prechádzajú cez sieť. Tiež zvykne byť označovaný ako paketový sniffer.

- Hrozba. Potenciálne nebezpečenstvo pre dáta alebo systémy. Hrozba môže byť reprezentovaná napr. vírusom.

- Trójsky kôň. Počítačový program, ktorý môže mať vplyv na výkon, pričom obsahuje skrytý kód umožňujúci neautorizovaný zber dát, modifikáciu alebo deštrukciu dát.

- Vírus. Program, ktorý je zavedený do systému alebo siete za účelom vykonania neautorizovanej akcie, ktorá môže byť vo forme neškodných vyskakovacích (pop-up) okien až po zničenie všetkých dát na disku.

- Zraniteľnosť. Slabé stránky v hardvéri alebo softvéri prípadne v bezpečnostnom pláne, ktoré nechávajú systém alebo sieť otvorenú voči hrozbám neautorizovaného prístupu, resp. voči poškodeniu alebo zničeniu dát.

- Červ. Program, ktorý replikuje sám seba. Šíri sa z jedného zariadenia na ďalšie prostredníctvom siete.

# 2 Hrozby sieťovej bezpečnosti

Tam kde je sieť, tam sú aj hrozby. Typy možných hrozieb v oblasti sieťovej bezpečnosti sa stále vyvíjajú, pričom monitorovací systém počítačovej siete a bezpečnosť by mali byť prioritou pre každého správcu siete. Ak je bezpečnosť siete narušená, mohlo by to mať vážne následky ako napr. strata súkromia alebo krádež informácií.

Je dôležité zdôrazniť, že nie všetky bezpečnostné hrozby sú škodlivé. Neškodlivé hrozby obvykle pochádzajú od zamestnancov, ktorí nie sú skúsení v počítačovej oblasti a nie sú si vedomí bezpečnostných hrozieb a zraniteľnosti. Chyby a opomenutia môžu spôsobiť, že cenné dáta budú stratené, poškodené alebo zmenené. Navyše prírodné katastrofy sú tiež neškodlivé hrozby. V tejto kapitole sú podrobné opísané iba škodlivé bezpečnostné hrozby.


Škodlivé hrozby sa skladajú z vnútorných (inside) útokov, ktoré realizujú záškodnícki zamestnanci a externých (outside) útokov, ktoré vykonávajú iné osoby ako zamestnanci a chcú len poškodiť a narušiť organizáciu. Najnebezpečnejší útočníci sú zvyčajne insideri (alebo bývalí insideri), pretože poznajú mnoho kódov a bezpečnostných opatrení, ktoré sú aplikované v sieti.

Nástroje pre sieťové útoky sa vyvíjali. V minulosti hackeri museli mať sofistikované počítače, programovacie a sieťové zručnosti k využívaniu primitívnych nástrojov na realizáciu základných útokov. V súčasnosti sa sieťoví hackeri, metódy a nástroje enormne zlepšili. Pre hackerov už nie sú potrebné tak sofistikované znalosti a aj ľudia, ktorí sa predtým nepodieľali na počítačovej kriminalite sú dnes toho schopní.

Definícia „hacker“ sa v priebehu rokov zmenila. Hacker bol niekedy vnímaný ako niekto samostatný, kto mal za cieľ znefunkčniť systém. Dnes termín hacker vyjadruje ľudí, ktorí sa dostali do systému kde nemajú pristúp alebo prekračujú hranice na systémoch, pre ktoré majú oprávnený prístup. Správny termín používaný pre niekoho, kto sa vláme do systému je „cracker“. Medzi bežné metódy na získanie prístupu k systému patrí prelomenie hesla, pričom sa využívajú známe bezpečnostné slabiny, sieťové falšovanie (spoofing) a sociálne inžinierstvo.

Existuje tu „komunikačná medzera“ medzi vývojármi bezpečnostných technológií a vývojármi sietí. Aj keď zabezpečenie siete je kritickou požiadavkou v rozvíjajúcich sa sieťach, existuje tu významný nedostatok zabezpečovacích metód, ktoré môžu byť ľahko implementované. V oblasti sieťového dizajnu nie je bezpečný návrh siete až tak rozvinutý a neexistuje metodika pre riadenie zložitosti bezpečnostných požiadaviek.

Veľa sieťových bezpečnostných hrozieb je v súčasnosti šírených cez Internet. Je dôležité poukázať na to, že inteligentné mobilné telefóny sa stali neoddeliteľnou súčasťou Internetu. Podrobný popis vlastností inteligentných mobilných terminálov a ľudského správania môže byť použitý na definovanie schémy ochrany v tomto prostredí.

## 2.1 Malvér: vírusy, červy, trójske kone a zombie


Škodlivý softvér (malvér) je softvér navrhnutý tak, aby úmyselne infiltroval alebo poškodil počítačový systém bez súhlasu majiteľa. To môže spôsobiť stratu alebo poškodenie v systéme. Počítačové vírusy tvoria veľkú triedu škodlivých kódov, ktoré sa môžu šíriť cez počítače a vykonávať škodlivé činnosti.

Spúšťanie škodlivého softvéru môže spôsobiť narušenie počítačových operácií resp. môže byť taktiež použité na zhromažďovanie citlivých informácií alebo na získanie neautorizovaného prístupu k počítačovému systému. Malvér nie je rovnaký ako chybný softvér, ktorý má legitímny účel a obsahuje bezpečnostné chyby, ktoré neboli známe pred vydaním. V skutočnosti sú počítačové vírusy akousi podmnožinou väčšej malvér rodiny, rovnako ako sú červy, trójske kone, spyware, adware, rootkity, atď.

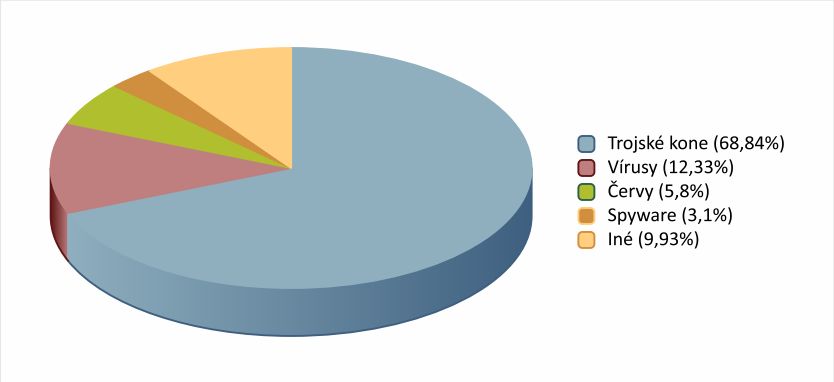
Podľa PandaLabs počas roka 2014 bolo zistených viac ako 75 miliónov nových vzoriek malvéru, čo predstavuje 34% všetkého malvéru. Je to viac ako dvakrát vyššia hodnota v porovnaní s predchádzajúcim rokom (30 miliónov). Ďalej nasleduje definícia najdôležitejších typov malvéru:

- Vírusy sú samoreplikačné programy, ktoré používajú súbory na infikovanie a šírenie. Po otvorení súboru bude vírus aktivovaný v rámci systému.

- Červ je podobný vírusu, pretože obidva sú samoreplikačné. Červ nevyžaduje súbor, aby sa mohol šíriť. Hlavným účelom červa je šíriť sa, pričom pôvodne boli používané na legitímne účely pri plnení povinností pre správu siete. Ich schopnosť šíriť sa bola rýchlo využitá hackermi k vytvoreniu škodlivých červov, ktoré môžu tiež využiť slabiny operačného systému a vykonávať škodlivé akcie. Existujú dva hlavné typy červov: hromadné mailové červy a sieťové červy. Hromadné mailové červy využívajú e-mail ako prostriedok k infikovaniu ďalších počítačov. Sieťové červy vyberú cieľ a akonáhle červ dosiahne cieľového hostiteľa, môže ho infikovať pomocou trójského koňa alebo iným spôsobom.

- Trójske kone sa zdajú byť benígne programy pre používateľov ale v skutočnosti vykonávajú akcie, ktoré používateľ programu nezamýšľal. Zjednodušene povedané, trojan môže vykonávať akcie, pre ktoré má používateľ oprávnenie. To znamená, že trojan je obzvlášť nebezpečný, ak sa nič netušiaci používateľ, ktorý ho nainštaluje stane správcom a má prístup k systémovým súborom. Typ škodlivého softvéru, ktorý sa zvyčajne šíri ako trojan je ransomware. Tento druh malvéru napáda počítačový systém, obmedzuje prístup k tomuto počítaču a požaduje, aby používateľ platil výkupné prevádzkovateľom za odstránenie obmedzení.

- Zombie je škodlivý softvér, ktorý sa šíri prostredníctvom siete. Po jeho úspešnom prieniku do počítačového systému ho možno diaľkovo ovládať a spravovať. Ak je niekoľko počítačov infikovaných rovnakým druhom škodlivého softvéru, jedná sa o botnet. Botnet možno ovládať z jedného vzdialeného počítača. Botnet núti infikované počítače vykonávať rovnaké príkazy. To umožňuje **DDoS** *(Distributed Denial of Service*) útok.




Obr. 2.1 – Typy nového malvéru, ktoré boli vytvorené počas roka 2014

## 2.2 Spyware a adware

Termín adware označuje softvér, ktorý zobrazuje reklamný obsah a je používateľom vkladaný do ďalšej aplikácie.

Adware je považovaný za legitímnu alternatívu pre spotrebiteľov, ktorí nechcú platiť za softvér. Existuje veľa podporovaných programov, hier alebo nástrojov, ktoré sú distribuované ako adware (alebo freeware). V súčasnej dobe rastie počet vývojárov softvéru, ktorí ponúkajú svoj tovar ako „sponzorovaný“ freeware (adware), kým si používateľ za daný softvér nezaplatí.

V prípade legitímneho adware, keď používateľ zastaví beh softvéru, reklamy by mali zmiznúť a používateľ by vždy mal mať možnosť zastaviť reklamy pomocou zakúpenia registračného kľúča.

Spyware je všeobecný termín používaný na popis softvéru nainštalovaného prostredníctvom Internetu na počítač bez súhlasu používateľa, ktorý vykonáva činnosti ako je reklama, získavanie informácií o jeho surfovaní na webe alebo zmenu konfigurácie počítača.

Získané informácie môžu byť zaslané cez Internet niekde na server, obvykle ako skrytý vedľajší účinok programu, pričom tieto informácie môžu byť zhromažďované na rôzne účely. Typické taktiky zahŕňajú dodávku nevyžiadaných „vyskakovacích“ reklám, krádež osobných informácií (vrátane hesiel do on-line účtov alebo finančné informácie ako sú čísla kreditných kariet), sledovanie činnosti na webe pre marketingové účely a smerovanie HTTP požiadaviek pre reklamné stránky.

Spyware môže byť inštalovaný spolu s iným softvérom alebo ako výsledok infekcie vírusom. V niektorých infekciách je jeho prítomnosť skrytá. Spyware je niekedy navrhnutý tak, aby bolo ťažké nielen ho odstrániť, ale aj detegovať. Iné druhy spywaru vykonajú zmeny v počítači, ktoré môžu byť nepríjemné a môžu počítač spomaliť alebo znefunkčniť.

Používatelia si často všimnú nechcené správanie a degradáciu výkonu systému. Spyware môže spôsobiť zvýšenú aktivitu procesora, disku a prevádzky siete.

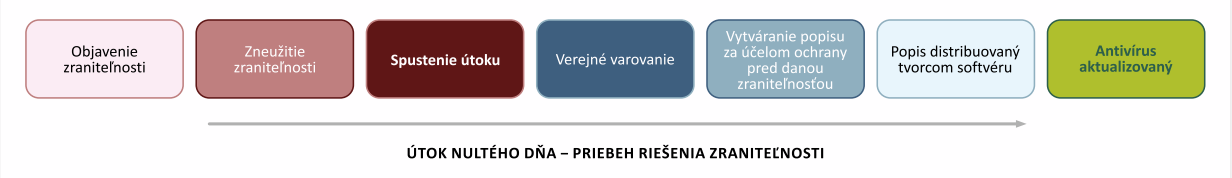
Anti-spyware programy môžu pracovať tak, že poskytujú ochranu v reálnom čase alebo skenovanie v pravidelných časových intervaloch. V prvom prípade tieto programy môžu skenovať všetky prichádzajúce sieťové dáta pre spyware a blokujú akúkoľvek hrozbu podobným spôsobom ako antivírus. V druhom prípade môžu byť použité iba pre detekciu a odstránenie spyware softvéru, ktorý už bol nainštalovaný do počítača.

## 2.3 Zero-day zraniteľnosť, útoky nultého dňa

Existuje niekoľko, ale mierne odlišných definícií zero-day zraniteľností. Niektoré definície označujú tento termín ako softvérové chyby, ktoré sú vystavené kybernetickým útokom pred vydaním záplaty. Nultým dňom sa tu chápe pôvodný stav až do odstránenia danej softvérovej chyby. Iní zvyknú označovať ako nultý deň (zero-day) ten deň, keď sa hrozba stane verejne známa. Doba ohrozenia útokom nultého dňa tak môže byť niekoľko dní, týždňov ale aj rokov a doba trvania je typicky plne v rukách autorov chybného softvéru.

Tieto útoky sú zriedkakedy objavené. V skutočnosti to často trvá nielen dni ale aj mesiace a niekedy aj roky, kým developer odhalí zraniteľnosť, ktorá viedla k útoku.

V každom prípade je výsledok rovnaký: používatelia sú otvorení útokom. Ako L. Bilge a T. Dumitras poznamenali v [5] „Kým zraniteľnosť zostáva neznáma, softvér nemôže byť zaplátaný a antivírusové produkty nemôžu rozpoznať útok cez skenovanie“. Zraniteľné miesta v softvéri môžu byť objavené crackermi, bezpečnostnými spoločnosťami alebo výskumnými pracovníkmi, samotnými predajcami alebo prostredníctvom používateľov softvéru. Ak zraniteľné miesto objavil cracker, exploit bude držaný v tajnosti tak dlho ako je to možné. Dostane sa na svetlo sveta len pre skupinu crackerov/hackerov, kým softvérová alebo bezpečnostná spoločnosť sa o ňom dozvie z útokov zameraných na dané zraniteľné miesto.




Obr. 2.2 – Perióda zraniteľnosti zero-day útoku

Útoky nultého dňa predstavujú jeden z najviac deštruktívnych a vysoko postavených útokov v posledných rokoch. Napríklad operácia Aurora (2009) využila zraniteľnosť Internet Exploreru s viac ako 20 cieľmi, zraniteľnosť služieb Morgan Stanley, Google, Yahoo, Dow Chemical, Adobe Systems, Juniper Networks a dokonca aj softvér pre zabezpečenie ako je Symantec.

Pravdepodobne najznámejší útok nultého dňa bol Stuxnet (2010). V skutočnosti Stuxnet červ používal štyri samostatné útoky nultého dňa k poškodeniu priemyselných regulátorov a k narušeniu zariadenia na obohacovanie uránu v Natanze. Stuxnet bol navrhnutý tak, aby manipuloval priemyselné programovateľné logické radiče (PLC) vyrobené nemeckou firmou Siemens, ktoré kontrolujú a monitorujú rýchlosť odstrediviek. Vzdialení útočníci nemohli dosiahnuť priamo tieto zariadenia, pretože počítače neboli pripojené k Internetu. Takže útočníci navrhli útok prostredníctvom infikovaných USB flash diskov.

Najprv infikovali počítače, ktoré patrili piatim externým spoločnostiam, ktoré sú pripojené nejakým spôsobom k jadrovému programu. Použitie štyroch zraniteľností nultého dňa je mimoriadne a je unikátne pre tento typ hrozby. Okrem toho, Stuxnet tiež používal rad ďalších zraniteľností čím ukazuje mimoriadnu prepracovanosť, myslenie a plánovanie prípravy tohto útoku.

## 2.4 Skenovanie a falošný obsah (spoofing). Krádež identity

V tejto súvislosti sa termín skener odkazuje na softvérový program, ktorý je používaný vzdialene hackermi na určenie možného zraniteľného miesta v danom systéme.

Správcovia tiež používajú skenery pre detekciu a opravu slabých miest v ich vlastných systémoch pred tým ako ich útočníci nájdu. Veľký počet skenovacích programov je k dispozícii ako freeware na Internete.

Dobrý skenovací program môže vyhľadať cieľový počítač na Internete (ten, ktorý je náchylný k útoku), zistiť aké služby TCP/IP sú spustené na danom stroji a skúmať tieto služby z hľadiska bezpečnostných chýb.

Spoofing útok je realizovaný vtedy, ak sa útočník vydáva za iné zariadenie alebo za iného používateľa na sieti.

Existuje niekoľko rôznych typov spoofing útokov vrátane e-mail spoofingu, spoofing IP adresy, ARP spoofing útoky a DNS server spoofing útok.

E-mail spoofing zahŕňa odosielanie správ z falošnej e-mailovej adresy alebo falšovanie e-mailovej adresy iného používateľa. Väčšina e-mailových serverov má bezpečnostné prvky, aby sa zabránilo odosielaniu správ od neoprávnených používateľov. Avšak je možné prijímať e-maily z adresy, ktorá nie je skutočnou adresou osoby, ktorá správu odoslala.

Pri spoofing útoku IP adresy, útočník pošle IP pakety z falošnej zdrojovej adresy s cieľom zakryť sám seba. IP spoofing spočíva v zasielaní adresy počítača, pričom ako zdrojová adresa je použitá adresa dôveryhodného počítača.

Existuje mnoho nástrojov a postupov, ktoré organizácie môžu využívať na zníženie hrozby spoofing útokov. Spoločné opatrenia, ktoré organizácie môžu považovať za spoofing prevenciu útokov zahŕňajú filtrovanie paketov, využitie detekčného spoofing softvéru a použitie kryptografických sieťových protokolov.

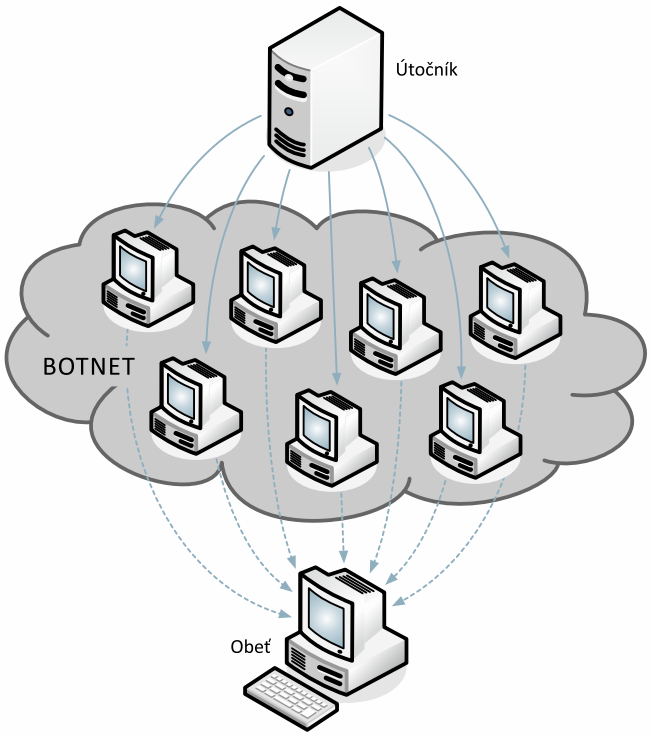
## 2.5 Útok výpadok služby DoS (Denial of Service) a distribuovaný DoS (DDoS)

Ako je podrobne uvedené v [8], „DoS útoky sú jedny z najpopulárnejších volieb internetových hackerov, ktorí chcú narušiť prevádzku danej siete. Nemajú zničiť alebo kradnúť dáta ako niektoré iné typy útokov. Cieľom útočníka DoS je zvrhnutie siete resp. odopretie služby svojim oprávneným používateľom. Útoky DoS sú ľahko realizovateľné. Softvér je ľahko dostupný z hackerských webových stránok, čo umožňuje aby niekto začal útok DoS aj s malými alebo žiadnymi technickými znalosťami.“

V tomto druhu útokov systém prijíma príliš veľa požiadaviek a nie je schopný vrátiť komunikáciu podľa požiadavky. Systém potom míňa zdroje na čakanie pre dokončenie handshake (tzv. potrasenie rukou). Nakoniec systém nebude reagovať na žiadne požiadavky, teda nebude poskytovať služby.

Distribuované DoS (DDoS) útoky používajú sprostredkujúce počítače označované ako „agenti“, ktoré sú často infikované trojanom. Tieto počítače predstavujú botnet a používajú sa na cielenie jednotného systému spôsobujúceho DoS útok.

Rozdiel oproti klasickému DoS útoku je použitie botnetu v distribuovanom DoS s mnohými počítačmi (môžu to byť stovky či dokonca tisíce) a viacerými pripojeniami k Internetu.




Obr 2.3. Schéma DDoS útoku

Útočník aktivuje na diaľku trójske programy, čo umožní sprostredkovateľským počítačom súčasne začať skutočný útok. Toto účinne znemožňuje zastaviť útok jednoducho tým, že je zablokovaná jedna IP adresa pretože útok prichádza z počítačov, ktoré môžu byť v sieťach kdekoľvek na svete. Okrem toho je veľmi ťažké rozlíšiť legitímny používateľský tok od útočiaceho, keď je rozprestretý na toľkých bodoch.

Je dôležité si uvedomiť, že DDoS útoky predstavujú dvojvrstvovú hrozbu. Nielenže sieť môže byť cieľom DoS útoku, ktorý zhodí servery a zabraňuje prichádzajúcej a odchádzajúcej prevádzke ale tiež počítače v sieti môžu byť použité ako nevinný muž v strede (man in the middle útok) na spustenie DoS útoku voči iným sieťam alebo stránkam.

DDoS útoky možno rozdeliť na základe cieľov útoku na objemové útoky, protokolové útoky a útoky na aplikačnej vrstve. V prvom prípade je cieľom nasýtenie šírky pásma siete, v druhom spotreba servera alebo sprostredkovateľského komunikačného zariadenia a v treťom prípade pád aplikačného servera.

# 2.6 Útoky sociálneho inžinierstva


Sociálne inžinierstvo je definované ako získavanie dôverných informácií pomocou ľudskej interakcie.

Hackeri sa pokúšajú získať rôzne typy informácií. Ak sa jedná o konkrétne osoby, tak sa zameriavajú hlavne na získavanie rôznych typov hesiel, bankových informácií, prípadne na to ako získať kontrolu resp. prístup do osobného počítača pomocou využitia škodlivého softvéru.

Na rozdiel od ostatných typov útokov, sociálne inžinierstvo sa nevzťahuje na technologickú manipuláciu s počítačovým hardvérom alebo na softvérovu zraniteľnosť. Tento typ útoku nevyžaduje veľké technické zručností. Namiesto toho tento typ útoku využíva ľudské slabosti ako napríklad nepozornosť alebo túžbu zoskupovať sa a registrovať sa do rôznych komunít na internetovej sieti. Schopnosti, ktoré útočníci využívajú pri tejto technike sa označujú ako tzv. "ľudské zručnosti" medzi ktoré patria napr. autoritatívne a vodcovské zručnosti, presvedčivé správanie a pod.

Mnoho bezpečnostných analytikov považuje za najslabší prvok bezpečnosti práve človeka a jeho slabosti. Medzi niektoré bežné útoky sociálneho inžinierstva zaraďujeme napr. prijatie emailu od akože nášho priateľa. Ten môže obsahovať odkaz na stiahnutie, kde je často umiestnený škodlivý softvér alebo posielanie falošných emailov z bankových inštitúcií, ktoré vyzývajú napríklad na zadanie prihlasovacích údajov (phishing) a pod.

# 3 Komponenty sieťového bezpečnostného systému

Na zníženie zraniteľnosti počítačov, ktoré sú pripojené do siete existuje množstvo dostupných produktov. Organizácie majú na výber medzi rôznymi technológiami od základných antivírusových balíčkov až po vyhradený hardvér pre sieťovú bezpečnosť ako napr. bezpečnostné brány (firewally).

Je dôležité poukázať na to, že žiadne jednoduché bezpečnostné riešenie neochráni systém pred všetkými typmi hrozieb. Sieťový bezpečnostný systém zvyčajne pozostáva z viacerých komponentov. Ideálne by všetky komponenty mali pracovať spoločne lebo pri výpadku jedného z nich ostatné stále zabezpečujú bezpečnosť siete. Komponenty môžu byť vo forme hardvéru ale aj softvéru, ktorý by mal byť pravidelne aktualizovaný voči prípadným novým hrozbám.

Organizácie dnes používajú kombináciu firewallov, IDS, šifrovania a autentizačných mechanizmov s cieľom vytvoriť tzv. „intranet“, ktorý je pripojený na Internet ale je chránený pred hrozbami z tejto siete. Intranet je súkromná počítačová sieť, ktorá využíva internetové protokoly. Intranet sa líši od „extranetu“ v tom, že intranet je vo všeobecnosti obmedzený na zamestnancov organizácie. Extranet môže byť prístupný aj pre zákazníkov, dodávateľov alebo pre ďalších povolených účastníkov.

## 3.1 Antivírus a anti-spyware

Vírusy, červy a trójske kone sú príklady škodlivého softvéru, ktorý sa zvykne označovať aj ako malvér (malware). Špecializovaný anti-malvér nástroj sa používa na prevenciu, detekciu a odstránenie škodlivého softvéru ako sú vírusy, počítačové červy, trójske kone, spyware a adware. Antivírusový softvér je dodávaný s väčšinou počítačov a môže čeliť väčšine vírusových hrozieb v prípade, že je softvér pravidelne aktualizovaný a správne udržiavaný. Inak nebude zabezpečená ochrana proti novým vírusom.

Antivírusový priemysel zahrňuje rozsiahlu sieť používateľov, ktorá poskytuje včasné varovania týkajúce sa nových vírusov. Preto môžu byť riešenia vyvíjané a distribuované rýchlo. Tisíce nových vírusov sú generované každý mesiac a preto je nevyhnutné, aby vírusová databáza bola stále aktuálna. Vírusová databáza je nahrávaná antivírusovým softvérom. Pomáha identifikovať známe vírusy, keď sa pokúšajú realizovať svoju záškodnícku činnosť. Známe antivírusové programy zverejňujú posledné známe riešenia (liečivá) na svojich webových stránkach. Často aj samotný softvér vyzýva používateľov, aby pravidelne zbierali nové dáta. Bezpečnostná politika siete by mala stanoviť to, že všetky počítače v sieti sú udržiavané v aktuálnom stave a v ideálnom prípade sú chránené rovnakým antivírusovým balíčkom. Cieľom je udržať náklady na údržbu a aktualizácie na minimálnej úrovni. Tiež je potrebné pravidelne aktualizovať samotný softvér.

Aj napriek tomu, že antivírusový softvér je veľmi užitočný môže mať nejaké nevýhodné vlastnosti. Antivírusový program zvykne narúšať najmä výkon počítača a neskúsení používatelia môžu mať niekedy problém pochopiť výzvy a rozhodnutia, ktoré tento softvér vykonáva. Pritom nesprávne rozhodnutia, či zlé nastavenie antivírusového programu môžu viesť až k narušeniu bezpečnosti.

Odstránenie vírusu je termín používaný pre čistenie počítača od škodlivého kódu. Existuje niekoľko spôsobov odstránenia. Odstránenie kódu z infikovaného súboru, ktorý zodpovedá vírusu. Odstránenie súboru alebo umiestnenie infikovaného súboru do karantény, čo predstavuje miesto, kde ho nie je možné spustiť.

Obvykle sú použité rôzne stratégie.

Detekcia na základe signatúr (podpisov) zahŕňa vyhľadávanie známych vzorov dát v rámci spustiteľného kódu. Vírusy sa reprodukujú pomocou nakazenia hostiteľskej aplikácie čo znamená, že kopírujú časť spustiteľného kódu do existujúceho programu. Aby bolo zabezpečené, že vírusy vykonajú svoju činnosť tak ako bolo naplánované, infikujú rovnaký súbor viackrát. To je realizované tak, že vkladajú sériu bajtov do infikovaného súboru a následne kontrolujú, či už súbor bol infikovaný – to je označované ako vírusová signatúra (podpis). Antivírusové programy sa spoliehajú na tento podpis, ktorý je jedinečný pre každý vírus a je použitý pre následnú detekciu. Táto metóda sa nazýva detekcia na báze podpisu (signature based detection) a je to najstaršia metóda používaná antivírusovým softvérom.

Predchádzajúcu metódu však nie je možné použiť na detekciu vírusov, ktoré nie sú známe vydavateľovi, resp. tvorcovi antivírusového softvéru. Okrem toho tvorcovia vírusov často kamuflujú rôzne znaky týchto známych vírusov, aby ich podpis bolo ťažké odhaliť. Ak chceme čeliť aj takejto hrozbe a chrániť počítač aj pred novými typmi vírusov, môžeme použiť heuristický prístup detekcie.

Jeden typ heuristického prístupu, generické signatúry, môžu identifikovať nové vírusy alebo modifikované varianty existujúcich vírusov tým, že hľadajú známy škodlivý kód, či kód s nepatrnými zmenami v súboroch. Metóda heuristickej analýzy zahŕňa analýzu správania aplikácií s cieľom detegovať aktivitu podobnú tej, ktorú vykonávajú známe vírusy.

Tento druh antivírusového programu teda môže detegovať vírusy aj keď vírusová databáza nebola aktualizovaná.

Na druhej strane sú náchylné na falošnú detekciu a tým aj na neoprávnené výstrahy.

## 3.2 Firewall


Bezpečnostná brána (firewall) je typický hraničný kontrolný mechanizmus alebo perimeter obrany. Účelom firewallu je, aby zabránil neoprávnenému prístupu do alebo zo siete pomocou blokovania prevádzky zvonka alebo zvnútra tejto siete.

Všetky dáta vstupujúce alebo opúšťajúce sieť cez firewall sú skúmané vo forme každého paketu, pričom firewall blokuje tie, ktoré nespĺňajú stanovené bezpečnostné kritériá. Firewally môžu byť implementované v hardvéri aj softvéri alebo v kombinácii oboch [8].

Firewally presadzujú bezpečnostné pravidlá organizácie pomocou obmedzenia prístupu ku konkrétnym sieťovým zdrojom. Bránu (firewall) môžeme prirovnať k zámku na vstupných dverách alebo k dverám do miestnosti vo vnútri budovy – tie sú prístupné len autorizovaným používateľom, ktorí musia mať pre vstup kľúč alebo prístupovú kartu. Technológia firewallu je k dispozícii aj vo verzii vhodnej pre domáce použitie, pričom vytvára ochrannú vrstvu medzi sieťou a vonkajším svetom. V skutočnosti firewall replikuje sieť na mieste vstupu tak, že môže prijímať a vysielať autorizované dáta bez značného oneskorenia. Obsahuje vstavané filtre, ktoré znemožňujú neautorizovaným alebo potencionálne nebezpečným materiálom vniknúť do reálneho systému. Okrem toho firewall poskytuje dôležitú záznamovú (logging) a kontrolnú (audit) funkciu. Správca siete môžu využiť tieto informácie na prehľad o danej sieti, napr. aký typ a objem prevádzky sa prenáša cez danú sieť alebo aké boli pokusy o vniknutie do danej siete.

Národný inštitút pre štandardy a technológie (NIST) 800 - 41, [9] rozdeľuje firewall na tri základné typy: paketové filtre, kontrola stavu firewallu a proxy. Tieto tri kategórie nevytvárajú samostatné jednotky ale naopak spolupracujú, pretože väčšina moderných firewallov predstavuje kombináciu všetkých typov na zlepšenie funkčnosti.

Brány typu paketový filter sú v podstate smerovacie zariadenia, ktoré obsahujú funkciu riadenia prístupu pre adresy systému a komunikačné relácie. Tiež môžu filtrovať sieťovú prevádzku na základe určitých charakteristík tejto prevádzky. Sú zvyčajne rozmiestnené v rámci sieťovej infraštruktúry TCP/IP. Ich hlavné prednosti sú rýchlosť a flexibilita. Naopak najväčšou slabinou je ich neschopnosť zabrániť útokom, ktoré cielia na konkrétne zraniteľnosti aplikácií (pretože neskúmajú údaje hornej vrstvy).

Tabuľka 1 ukazuje jednoduchý paketový filter s nastavením pravidiel, uvedené v [9]

| | Zdrojová adresa | Zdrojový port | Cieľová adresa | Cieľový port | Akcia | Popis |
|---|---|---|---|---|---|---|
| 1 | Akákoľvek | Akýkoľvek | 192.168.1.0 | > 1023 | Povelená | Pravidlo povoľujúce návrat TCP spojení do internej podsiete |
| 2 | 192.168.1.1 | Akýkoľvek | Akákoľvek | Akýkoľvek | Zakázaná | Chráni systém firewallu od priameho pripojenia |
| 3 | Akákoľvek | Akýkoľvek | 192.168.1.1 | Akýkoľvek | Zakázaná | Zabraňuje externým používateľom priamo pristupovať k firewallovému systému |
| 4 | 192.168.1.0 | Akýkoľvek | Akákoľvek | Akýkoľvek | Povolená | Interní používatelia môžu pristupovať k externým serverom |
| 5 | Akákoľvek | Akýkoľvek | 192.168.1.2 | SMTP | Povolená | Povolenie externým používateľom posielať emaily |
| 6 | Akákoľvek | Akýkoľvek | 192.168.1.3 | HTTP | Povolená | Povolenie externým používateľom prístup k WWW serveru |
| 7 | Akákoľvek | Akýkoľvek | Akákoľvek | Akýkoľvek | Zakázaná | Všetko, čo nie je v prechádzajucom povolené je explicitne zakázané |

Kontrola stavu firewallu známa tiež ako dynamické filtrovanie paketov je technológia, ktorá monitoruje stav aktívnych pripojení a používa tieto informácie na určenie toho, ktoré sieťové pakety môžu prejsť cez firewall. Tento typ firewallu analyzuje pakety až do aplikačnej vrstvy. Pomocou zaznamenaných informácií o relácii ako sú IP adresy a čísla portov, môže dynamický paketový filter realizovať oveľa prísnejšie bezpečnostné zásady pomocou skúmania určitých hodnôt v protokolových hlavičkách s cieľom monitorovať stav každého pripojenia v čase. Odchádzajúce pakety, ktoré požadujú konkrétne typy prichádzajúcich paketov sú sledované a iba tieto prichádzajúce pakety tvoria správnu odpoveď, ktorá je povolená a bude prepustená cez firewall. Každý nový paket je porovnávaný so stavovou tabuľkou firewallu, čím sa určí či je stav paketu v rozpore s jeho očakávaným stavom. Tradičná stavová kontrola firewallu nekontroluje užitočný obsah sieťových paketov a ani nemá inteligenciu na rozlišovanie jedného druhu webovej prevádzky od inej (napr. legitímne aplikácie a útoky).

Proxy firewally alebo Application Gateway firewally sú pomerne novým prírastkom do oblasti bezpečnosti. Proxy firewally kombinujú známu stavovú kontrolu so schopnosťou vykonávať hĺbkovú kontrolu aplikácií. Táto funkcia umožňuje analýzu protokolov na aplikačnej vrstve, ako je HTTP a FTP a monitorovanie prevádzky. Jej cieľom je porovnať neškodnú činnosť protokolu s aktuálnou aktivitou a tým identifikovať prípadné odchýlky, ktoré môžu znamenať

príznaky útoku. Toto umožňuje firewallu povoliť alebo zakázať prístup na základe toho ako aplikácia beží v rámci siete.

Next-Generation Firewall (NGFW) je integrovaná sieťová platforma, ktorá kombinuje tradičný firewall s ďalšími sieťovými zariadeniami na filtrovanie ako je napríklad proxy firewall využívajúci in-line hĺbkovú inšpekciu paketov (deep packet inspection DPI), systém pre prevenciu narušenia (intrusion prevention system IPS) a/alebo ďalšie techniky ako je SSL a SSH zachytávanie, filtrovanie webových stránok, QoS / správa šírky pásma, antivírusová kontrola a integrácia tretích strán (napríklad Active Directory) [10]. V skutočnosti tieto techniky predstavujú zjednotený manažment hrozieb UTM (unified threat management). Hlavnou nevýhodou NGFW je to, že zvyčajne NGFW má tendenciu používať samostatné interné moduly na vykonanie jednotlivých bezpečnostných funkcií. Preto môže byť paket skúmaný niekoľkokrát rôznymi modulmi, aby sa zistilo či má povolenie od siete. Tento prístup pridáva oneskorenie (latenciu), čo môže mať negatívny vplyv na výkon siete.

## 3.3 Systémy pre detekciu narušenia (Intrusion detection systems (IDS))

Systém pre detekciu narušenia je ďalšie ochranné opatrenie, ktoré pomôže odraziť počítačové narušenia pomocou monitorovania prevádzky v sieti. Pracuje s databázou signatúr a pomocou heuristickej analýzy identifikuje podozrivé vzorky, ktoré môžu indikovať siete alebo systémové útoky pokúšajúce sa prelomiť alebo napadnúť systém.

IDS systémy môžu byť softvérové a hardvérové zariadenia používané na detekciu útoku. IDS produkty sú používané na monitorovanie konektivity s cieľom zistiť, či je realizovaný nejaký útok. Niektoré systémy IDS len monitorujú a upozorňujú na útok, zatiaľ čo iné sa ich aj snažia zablokovať. Fungovanie IDS možno prirovnať k videokamere so snímačom pohybu, ktorá deteguje neoprávnené alebo podozrivé aktivity a následne automatizované reakčné systémy môžu varovať ochranku na zamedzenie tejto aktivity.

IDS sa líši od firewallu tým, že firewall hľadá prieniky, aby im zabránil a tak nedovolil spôsobiť škody. Firewall obmedzuje prístup medzi sieťami, aby sa zabránilo vniknutiu a nesignalizuje útoky zvnútra siete. IDS vyhodnocuje podozrivé narušenia a ak ich zistí, následne to signalizuje varovaním. Navyše IDS sa zameriava na útoky, ktoré pochádzajú z vnútra systému.

IDS používa hodnotenie zraniteľnosti (niekedy označované ako skenovanie), čo je technológia vyvinutá na posúdenie bezpečnosti počítačového systému alebo siete. Funkcie detekcie narušenia zahŕňajú monitorovanie a analýzu používateľa a systémových aktivít, analýzu systémových konfigurácií a zraniteľností, hodnotiaci systém a integritu súborov, analýzu nezvyčajných vzoriek a sledovanie porušení zásad používateľa. Existuje niekoľko spôsobov ako kategorizovať IDS:

- Detekcia zneužitia (misuse detection) vs. detekcia anomálií (anomaly detection)
    - Detekcia zneužitia: IDS analyzuje informácie, ktoré zhromažďuje a porovnáva ich s veľkou databázou podpisov (signatúr) pre útoky. V podstate IDS hľadá konkrétny útok, ktorý už bol zdokumentovaný. Technika detekcie narušenia je založená na podpise útoku. Spočíva v tom, že hľadá „podpisy“ (typická charakteristika postupnosti útoku) vo všetkých spojeniach v rámci siete. IDS môže detegovať aj útoky na úrovni aplikácií a to aj vtedy, ak vyhovujú štandardom medziaplikačných protokolov. Ako antivírusové systémy, tak aj softvér detekcie zneužitia je len taký dobrý aká dobrá je databáza podpisov pre útoky, ktorá sa používa na porovnanie paketov. To znamená udržiavanie a častú aktualizáciu databázy podpisov pre útoky na zariadeniach využívajúcich túto technológiu.
    - Detekcia anomálií: Správca systému definuje základné línie alebo normálny stav napr. zaťaženia siete, zlyhania, protokol a typickú veľkosť paketu. Detektory anomálií monitorujú sieťové segmenty a porovnávajú ich s normálnym resp. základným stavom a tým vyhľadávajú anomálie.

- Sieťovo založené (network-based) vs. klientsky založené (host-based) systémy
    - Sieťovo založené systémy alebo NIDS (network based intrusion detection systems): Individuálne pakety prechádzajúce cez sieť sú analyzované. NIDS môže detegovať škodlivé pakety, ktoré sú vytvárané tak aby boli prehliadnuteľné pomocou jednoduchých filtrovacích pravidiel firewallu.
    - Klientsky založené systémy alebo HIDS (host based intrusion detection systems): IDS skúma celú aktivitu na každom individuálnom počítači alebo klientovi.

## 3.4 Virtuálne privátne siete (Virtual Private Network (VPN))


VPN je skratka pre virtuálnu privátnu sieť. Virtuálna privátna sieť je sieťová technológia, ktorá umožňuje použiť verejnú sieť ako Internet pre privátnu komunikáciu pomocou vytvorenia zabezpečeného (šifrovaného) sieťového pripojenia.

VPN sú často používané na bezpečné pripojenie vzdialených používateľov k privátnej sieti a týmto spôsobom sa môže rozšíriť intranet po celom svete. Inými slovami VPN umožňuje posielanie dát medzi dvoma počítačmi pomocou smerovacej infraštruktúry, ktorá je poskytovaná cez zdieľanú alebo verejnú sieť (ako je Internet) a to spôsobom, ktorý emuluje vlastnosti súkromného spojenia point-to-point. Zabezpečené spojenie sa používateľovi javí ako súkromná sieťová komunikácia a to napriek skutočnosti, že táto komunikácia sa realizuje cez verejnú sieť (odtiaľ názov virtuálna privátna sieť).

Existuje niekoľko motivácií pre budovanie VPN spojenia ale spoločným menovateľom je to, že všetci zdieľajú požiadavku na „virtualizáciu“ určitej časti organizačnej komunikácie. Inými slovami, aby určitá časť komunikácie (alebo možno celá) bola v podstate „neviditeľná“ pre externých pozorovateľov a pritom využila efektívnosť spoločnej komunikačnej infraštruktúry. Hlavné použitia VPN sú: bezpečný vzdialený prístup k podnikovým zdrojom cez Internet a prepájanie sietí cez Internet. VPN riešenie by malo poskytnúť tieto bezpečnostné služby:

- Overenie používateľa. VPN obmedzuje prístup iba pre oprávnených používateľov. Z toho dôvodu musí byť overená ich pravosť. Okrem toho by mala VPN poskytovať kontrolne záznamy.
- Dátové šifrovanie. Dáta vymieňané cez verejnú sieť musia byť nečitateľné pre neautorizovaných používateľov.
- Manažment kľúčov. Pred dátovým šifrovaním je vyžadované, aby používatelia medzi sebou nastavili detaily šifrovania (algoritmy, kľúče,…).

# 4 Sieťové bezpečnostné riešenia

Sieť je len taká bezpečná ako jej najslabší článok. Okrem použitia metód opísaných v predchádzajúcej kapitole existuje aj súbor opatrení, ktoré by mali používatelia a/alebo správcovia sietí vykonávať s cieľom posilniť bezpečnosť systému a sú popísané nižšie.

## 4.1 Používanie bezpečných autentifikačných metód

Niekoľko organizácií vyžaduje použitie „silných autentifikačných metód“, najmä pri on-line transakciách, ktoré zahŕňajú platobné služby. Existuje niekoľko definícií silnej autentifikácie. Niektorí autori sa odvolávajú na overovaciu metódu s multifaktorovou autentifikáciou, ktorá vyžaduje použitie najmenej dvoch z týchto faktorov (vedomosť, vlastníctvo a existencia), spomínané v kapitole 1.3. Iní autori (A.J. Menezes, P.C. van OORSCHOT a S.A. Vanstone) považujú za silnú autentifikačnú metódu takú, ktorá vyžaduje kryptografický challenge response protocol, bližšie vysvetlený v [11].

Je dôležité vedieť, že spoľahlivosť autentifikácie je ovplyvnená nielen počtom faktorov, ale tiež ich implementovaním. V každej kategórii voľba pravidiel pre overovanie veľmi ovplyvní bezpečnosť každého faktora. Zlé alebo chýbajúce pravidlá pre heslá, môžu mať za následok napríklad vytvorenie hesiel ako je „host“, ktoré úplne znehodnotia zabezpečenie formou hesla. Medzi osvedčené postupy patrí neodmysliteľne vyžadovanie silného hesla, ktoré je pravidelne aktualizované. Slabé pravidlá a nezodpovedná realizácia má za následok oslabenie bezpečnosti. Alternatívne môžu lepšie pravidlá priniesť zlepšené zabezpečenie na faktor a lepšie celkové zabezpečenie pre multifaktorové autentifikačné systémy.

V prípade použitia hesiel je nevyhnutné vytvoriť kvalitné zásady pre heslá, aby sa zabránilo hádaním hesiel prípadnému prelomeniu. Existuje tiež početné množstvo dostupných nástrojov pre prelomenie hesla využiteľné priemerným človekom bez nejakých špeciálnych znalostí. Väčšinou sa však stáva, že používateľ uprednostní heslo ľahko zapamätateľné pred ťažko uhádnuteľným.

Prelomenie hesla je proces zisťovania alebo zlomenia hesla za účelom získania neoprávneného vstupu do systému alebo účtu. Heslá môžu byť prelomené pomocou rôznych techník. Najjednoduchšie je použitie zoznamu slov alebo slovníka pomocou ktorých je možné prelomiť heslá hrubou silou. Tieto programy porovnajú zoznamy slov alebo kombináciu znakov voči heslu kým nenájdu zhodu. Z tohto dôvodu je zrejmé, že ako heslá by nemali byť používané slová zo slovníka, vlastné mená alebo cudzie slová.

Nástroje na prelomenia hesla môžu byť použité aj na zabezpečenie toho, aby používatelia implementovali (volili si) bezpečné heslá. Správcovia systémov ich môžu aplikovať na testovanie sily hesiel používateľov a potom prípadne môžu informovať tých používateľov, ktorých heslá sú málo bezpečné.

Ďalší spôsob objavovania hesiel útočníkmi je prostredníctvom sociálneho inžinierstva. Mnoho používateľov vytvára heslá, ktoré obsahujú osobné údaje a preto je možné často uhádnuť dané heslo pomocou získania malého množstva informácií o danom používateľovi. Z toho vyplýva varovanie, že heslá by nemali obsahovať žiadne osobné informácie.

Mnoho používateľov si ukladá rôzne heslá v počítačových súboroch. Za účelom zníženia rizika odhalenia takéhoto súboru s heslami je potrebné takýto súbor

šifrovať. Toto odporúčanie je užitočné nielen pre súbor s heslami ale tiež pre všetky súbory, ktoré obsahujú nejaké citlivé informácie.

## 4.2 Hardening (nastavenie) operačného systému


Hardening (nastavenie) operačného systému je proces konfigurovania OS, jeho aktualizácie, vytvárania pravidiel a zásad, napomáhanie riadenia systému bezpečným spôsobom a odstraňovanie zbytočných aplikácií a služieb.

Hardening operačného systému znamená robiť OS bezpečnejším. To sa zvyčajne vykonáva odstránením všetkých nepodstatných softvérových programov a nástrojov z počítača, použitím najnovších záplat, mazaním nepoužívaných súborov, uzamknutím používateľských účtov, atď. Zatiaľ čo tieto nepodstatné programy môžu ponúknuť užitočné funkcie pre používateľa, poskytujú tiež „zadné vrátka“ pre prístup do systému a musia byť v priebehu optimalizácie systému odstránené.

Aj keď odobratie aplikácií, deaktivácia služieb, plátanie, hotfixing a inštalácia aktualizačných servisných balíčkov sú dôležité, ale nie sú jedinými spôsobmi ako realizovať hardening operačného systému. Administrátorské práva by mali byť používané s rozumom a zásady by mali byť zadefinované tak, aby presadzovali pravidlá organizácie.

Existujú nastavovacie kontrolne zoznamy pre populárne operačné systémy, ktoré môžu správcovia nasledovať. Operačné systémy Macintosh a Windows môžu byť nastavované. Nastavovanie systému sa častejšie vykonáva na počítačoch so systémom Windows, pretože u nich je viac pravdepodobné, že ich bezpečnosť môže byť ohrozená.

## 4.3 Fyzická bezpečnosť

Zaistenie fyzickej bezpečnosti sieťového prostredia je prvý krok v riadenom prístupe k citlivým dátam a systémovým súborom, ale je to iba časť dobrého bezpečnostného plánu. V súčasnosti to má ešte väčší význam ako v minulosti, pretože siete môžu pracovať rôznymi spôsobmi. Stredná alebo veľká sieť môže mať niekoľko prístupových bodov, serverov VPN a vyhradenú stálu konektivitu k Internetu. Dokonca aj u malej siete je pravdepodobné, že bude pripojená k Internetu nejaký čas.

Útočníci nikdy nevyužívajú priamo cieľový počítač alebo cieľovú sieť. Oni môžu pristupovať k sieti cez ulicu alebo cez polovicu sveta. Môžu spôsobiť rovnaké škody ako zlodeji, ktorí preniknú do spoločnosti s cieľom zničiť alebo ukradnúť citlivé dáta. Pritom je ich oveľa komplikovanejšie vypátrať. Zabezpečiť fyzickú prístupovú kontrolu „vonkajšieho perimetra" siete znamená:

a) Riadenie fyzického prístupu k serverom.

b) Riadenie fyzického prístupu k sieťovým pracovným staniciam.

c) Riadenie fyzického prístupu k sieťovým zariadeniam.

d) Riadenie fyzického prístupu ku káblu.

e) Riešiť bezpečnostné úvahy s bezdrôtovými médiami.

f) Riešiť bezpečnostné úvahy spojené s prenosnými počítačmi.

g) Zaoberať sa bezpečnostným rizikom, ktoré je spôsobené povolením tlače dát.

h) Zaoberať sa bezpečnostným rizikom, ktoré spôsobujú USB disky, externé disky, CD nosiče a iné prenosné média.

# 5 Mobilná bezpečnosť

Mobilné zariadenia rýchlo nahrádzajú alebo dopĺňajú osobný počítač doma alebo na pracovisku. Rýchly nárast v používaní smartfónov a tabletov v posledných dvoch rokoch viedol aj k nevyhnutnému nárastu zacielenia útokov na tieto zariadenia. Navyše niektoré neregulované trhy s aplikáciami (app markets) zvyšujú problémy súvisiace so škodlivým softvérom v týchto zariadeniach. Tvorcovia mobilného malvéru vedia, že najlepší spôsob ako napadnúť čo najviac mobilných zariadení je zaútočiť práve na centrálny trh s aplikáciami.

Existuje mnoho rôznych spôsobov ako môže hacker profitovať z napadnutého mobilného zariadenia. Niektoré z nich ako napríklad ransomware, botnet činnosti a krádež dát sa len preniesli z útokov na tradičné počítače. Vzhľadom na povahu mobilných zariadení sú tieto otvorené aj pre nové typy útokov. Práve ich prenositeľnosť spôsobuje častú stratu týchto zariadení. To spôsobuje vo väčšine prípadov stratu dát, ak tie nie sú nejakým spôsobom zaistené alebo šifrované.

Rozvoj aplikácií pre osobnú alebo obchodnú komunikáciu poskytuje možnosti pre ďalšie typy útokov. Hlavne pre podvody v rámci sociálneho inžinierstva a útoky zameriavajúce sa na získavanie dôverných dát. Adresár kontaktov, vzťahy a osobné údaje tvoria veľmi podstatné informácie pre útočníkov rôzneho druhu. Mobilné a webové kontrolne aplikácie pre podnikových používateľov pomôžu zmierniť toto riziko.

V súčasnej dobe vývoj mobilného bankovníctva predstavuje potenciálne ďalšie riziko pre používateľa. Výkonné mobilné zariadenia s takýmito aplikáciami už môžu predstavovať bezpečnostné riziko, keďže umožňujú realizovať finančné transakcie na cestách. Cieľom útočníka je získať a odcudziť údaje k týmto aplikáciám resp. priamo finančné prostriedky. Preto ochrana smartfónu pred škodlivým softvérom alebo napr. pred softvérom zaznamenávajúcim stlačenie kláves (keylogger), musí byť základným princípom bezpečného mobilného bankovníctva.

Bezpečnostní experti varujú pred hrozbou mobilného malvéru už niekoľko rokov. Zvyšovanie počtu mobilných zariadení a objavovanie nových mobilných malvérových hrozieb iba zvyšuje pravdepodobnosť, že hlavne mobilné malvérové útoky budú v dnešnom svete čoraz častejšie.

Povedal Kaspersky v Bermingham-e, „Keďže spotrebitelia a podniky prechádzajú k používaniu mobilných zariadení stále vo väčšej miere, útočníci kladú dôraz práve na mobilné platformy – konkrétne napr. Android alebo prelomené zariadenia so systémom iOS (tzv. jailbreak).“