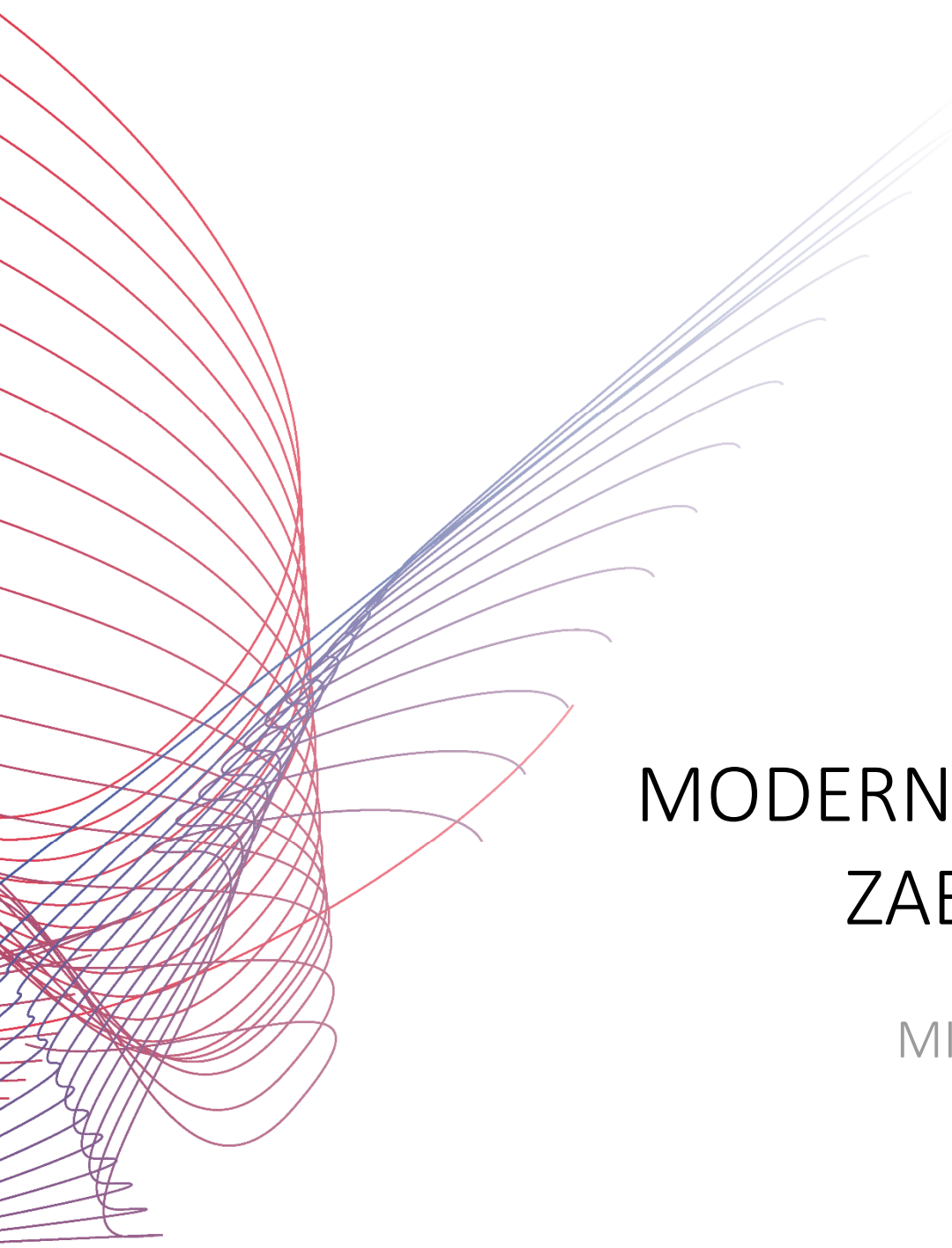




# TECH pedia



## MODERNÍ SYSTÉMY ZABEZPEČENÍ

MIGUEL SORIANO

**Název díla:** Moderní systémy zabezpečení  
**Autor:** Miguel Soriano  
**Přeložil:** Ivan Pravda  
**Vydalo:** České vysoké učení technické v Praze  
Fakulta elektrotechnická  
**Kontaktní adresa:** Technická 2, Praha 6  
**Tel.:** +420 224352084  
**Tisk:** (pouze elektronicky)  
**Počet stran:** 44  
**Edice (vydání):** 1. vydání, 2017  
**ISBN** 978-80-01-06206-7

**TechPedia**

European Virtual Learning Platform for  
Electrical and Information Engineering

<http://www.techpedia.eu>

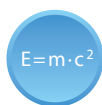


Tento projekt byl realizován za finanční podpory  
Evropské unie.

Za obsah publikací odpovídá výlučně autor.

Publikace (sdělení) nereprezentují názory Evropské  
komise a Evropská komise neodpovídá za použití  
informací, jež jsou jejich obsahem.

## VYSVĚTLIVKY



Definice



Zajímavost



Poznámka



Příklad



Shrnutí



Výhody



Nevýhody

---

## ANOTACE

Studijní modul definuje a vysvětluje pojmy nutné pro základní orientaci studentů v oblasti síťové bezpečnosti, a to včetně přehledu bezpečnostních služeb a užívaných bezpečnostních mechanismů, vymezení typů útočníků v souvislosti s bezpečnostními hrozbami a riziky a popisu klíčových komponent bezpečnostního systému sítě.

## CÍLE

Studijní modul poskytuje ucelený přehled o moderních bezpečnostních systémech. Je rozdělen do pěti bloků, resp. kapitol.

První kapitola definuje a vymezuje základní pojmy z oblasti síťové bezpečnosti, bezpečnostní služby a mechanismy. Druhá kapitola popisuje oblast možných bezpečnostních hrozeb a rizik, mezi které patří počítačové viry, červi, trojské koně; programy typu spyware a adware; útoky typu „Zero-Day“ a DoS (*Denial of Service*); odposlechy a krádeže dat; *Spoofing* a krádeže identity.

Třetí kapitola obsahuje popis klíčových komponent zajišťujících síťovou bezpečnost (antivirové programy, firewally, systémy pro detekci narušení, VPN a další). Čtvrtá kapitola uvádí přehled dalších metod zabezpečení sítí (tj. robustní ověřovací metody, zabezpečení integrity operačního systému, ochrana webových služeb, aj.)

Závěrečná pátá kapitola je věnována problematice mobilní bezpečnosti. „Chytré“ telefony (*Smartphones*) dnes hrají velmi důležitou roli na poli moderních komunikačních systémů a nikdo dnes nezpochybňuje jejich dopad a význam v každodenním životě. Avšak s ohledem na povahu těchto přístrojů a zařízení se objevují zcela nová bezpečnostní rizika a s nimi spojené typy útoků. V závěru kapitoly najdeme ilustrativní příklad, jaký užitek může přinést útočnickovi (*Hacker*) úspěšný útok na nedostatečně zabezpečený „chytrý“ telefon.

## LITERATURA

- [1] CVE. *A dictionary of publicly known information security vulnerabilities and exposures*. Dostupné z: <http://cve.mitre.org>; 2015. [on-line]
- [2] CHESWICK, W.; BELLOVIN, S.: *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, 1994. ISBN: 0-201-63357-4.
- [3] ZWICKY, E. D.; COOPER, S; CHAPMAN, D. B.: *Building Internet Firewalls*. O'Reilly and Associates, 2nd edition, 2000. ISBN: 978-1-565-92871-8.
- [4] DE ALBUQUERQUE, J. P.; DE GEUS, P. L.: *A Framework for Network Security System Design*.

- [5] BOLGE, L.; DUMITRAS, T.: *Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World*. ACM Conference on Computer and Communications Security, Raleigh, NC, 2012, pp. 833–844.
- [6] ZETTER, K.: *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*. AICMS 08. 2<sup>nd</sup> Asia International Conference on Modeling & Simulation, pp.77-82, 2008. ISBN: 978-0-7695-3136-6.
- [8] SHINDER, T. W.: *The Best Damn Firewall Book Period (2<sup>nd</sup> Edition)*. Syngress Publishing, Inc. 2007. ISBN: 978-1-59749-218-8.
- [9] SCARFONE, K.; HOFFMAN, P.: *Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-41, 1<sup>st</sup> Revision, 09/2009.
- [10] GEIER, E.: *Intro to Next Generation Firewalls*. Dostupné z: <http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html> 09/ 2011. [on-line]
- [11] CLIFF, A.: *Password Crackers - Ensuring the Security of Your Password*. Security Focus, 02/2001. Dostupné z: <http://online.securityfocus.com/infocus/1192>. [on-line]

# Obsah

<b>1</b>	<b>Úvod do problematiky .....</b>	<b>7</b>
1.1	Pojem síťová bezpečnost.....	8
1.2	Pojem bezpečnostní systém.....	9
1.3	Pojem bezpečnostní služby .....	10
1.4	Pojem bezpečnostní mechanismy.....	12
1.5	Klasifikace (kategorie) útočníků .....	14
1.6	Terminologie .....	17
<b>2</b>	<b>Potenciální hrozby zabezpečení sítí .....</b>	<b>19</b>
2.1	Malware: viry, červi, trojské koně a zombie .....	21
2.2	Spyware a adware.....	23
2.3	Zranitelnost a útoky typu Zero-day .....	24
2.4	Skenování a podvržený obsah (spoofing), krádež identity.....	26
2.5	Útok spojený s výpadkem služby DoS (Denial of Service) a distribuovaný útok typu DoS (DDoS) .....	27
2.6	Útoky spojené s pojmem sociální inženýrství .....	29
<b>3</b>	<b>Komponenty síťového bezpečnostního systému.....</b>	<b>30</b>
3.1	Anti-virus and anti-spyware .....	31
3.2	Firewall.....	33
3.3	Systémy detekce narušení IDS (Intrusion Detection Systems) .....	36
3.4	Virtuální privátní síť VPN (Virtual Private Network) .....	38
<b>4</b>	<b>Řešení pro zabezpečení sítí.....</b>	<b>39</b>
4.1	Využití bezpečných autentizačních metod .....	40
4.2	Vylepšené nastavení operačního systému .....	42
4.3	Fyzická bezpečnost.....	43
<b>5</b>	<b>Bezpečnost v mobilních sítích .....</b>	<b>44</b>

# 1 Úvod do problematiky

Svět se v globálním měřítku neustále zmenšuje, a to především díky síti Internet a implementaci nových síťových technologií. Jak je vidět z průběhu posledních dvou desítek let, prostřednictvím sítě Internet bylo možné dynamicky rozvíjet elektronické podnikání (*E-business*). Tato forma podnikání následně umožnila rapidně zvýšit efektivitu podnikatelských aktivit a přinesla s sebou citelný růst tržeb. I přes tyto nesporné výhody však dostupnost sítí širokému okruhu uživatelů a nárůst počtu využívaných aplikací přináší i celou řadu bezpečnostních rizik a potenciálních problémů, které jdou ruku v ruce s vyšší zranitelností sítí. Proto je důležité zajistit efektivní snížení míry ohrožení všech síťových transakcí. Síťová bezpečnost se tak stala velmi důležitou nejen pro oblast podnikání a pro armádní účely, ale i pro neziskové organizace a v konečném důsledku i pro jednotlivé koncové uživatele.



---

Hackeri byli v minulosti skupinou vysoce kvalifikovaných programátorů, kteří detailně rozuměli a znali principy používané u počítačových a komunikačních systémů a dokázali využívat jejich slabiny a nedokonalosti. Dnes se však hackerem může stát prakticky kdokoliv, pokud získá potřebné nástroje z Internetu. Tyto promyšlené nástroje využívané pro napadání nezabezpečených resp. nepřiměřeně zabezpečených sítí obecně poukázaly na potřebu zvýšení úrovně bezpečnosti sítí v souvislosti s uplatněním dynamických bezpečnostních opatření. Vyhledáváním potenciálních rizik a návrhem bezpečnostních opatření se v současnosti zabývá mnoho společností. Jednou z nejznámějších znalostních databází v oblasti zabezpečení sítí je databáze **NVD** (*National Vulnerability Database*), založená a spravovaná společností *MITRE*. [1]

---

Oblast vymezená pojmem síťová bezpečnost je dnes obrovská a neustále se dynamicky rozvíjí. Objem zachycených bezpečnostních událostí totiž každým rokem závratnou rychlostí narůstá. I přesto, že byla v posledních letech výrazně zlepšena síťová a počítačová bezpečnost, jsou systémy zranitelnější než kdy jindy. Jakýkoliv technologický pokrok a vylepšení výpočetní a komunikační techniky s sebou přináší i nové bezpečnostní hrozby a rizika, která vyžadují aplikaci nových bezpečnostních řešení. Technologický vývoj však ubíhá mnohem rychleji, než s jakou rychlostí jsou vyvíjena a nalezena přiměřená bezpečnostní opatření. Jelikož jsou útoky stále propracovanější, složitější a důmyslnější, tím více roste význam bezpečnostních opatření pro zabezpečení provozu počítačových a komunikačních sítí.

## 1.1 Pojem síťová bezpečnost

---



$E=mc^2$

Pojem síťová bezpečnost velmi úzce souvisí s činnostmi zvyšujícími míru zabezpečení sítí. Konkrétně tyto činnosti zvyšují použitelnost (*Usability*), spolehlivost (*Reliability*), celistvost (*Integrity*) a bezpečnost (*Safety*) sítí a dat. Síťová bezpečnost se tedy stala jedním z klíčových požadavků kladených na všechny typy komunikačních systémů používaných především v podnikové sféře, ale i koncovými uživateli, a to zejména těch, které pro svou činnost využívají přístup na Internet.

---

Zákazníci, dodavatelé a obchodní partneři vyžadují přiměřenou ochranu všech svých informací a dat, která sdílejí, jelikož jsou tato data a informace považována za velmi citlivá (např. čísla kreditních karet, důvěrné obchodní informace a celá řada dalších).

---



Síťová bezpečnost se však netýká pouze zabezpečení konkrétních počítačů umístěných na koncích příslušného komunikačního řetězce. Pokud probíhá přenos dat, pak by i komunikační kanál neměl být jednoduše napadnutelný. Pokud by totiž nebyl komunikační kanál dostatečně zabezpečen, pak by potenciální útočník (*Hacker*) mohl snadno získat přenášená data, dešifrovat je a znovu je v podobě falešné zprávy odeslat dál. Zabezpečení vlastní přenosové soustavy je tedy stejně důležité jako zabezpečení jednotlivých počítačů a šifrování přenášených zpráv. Efektivní síťové zabezpečení počítá se všemi možnými typy rizik a útoků, snaží se jim zabránit ve vstupu do sítě, a tím omezit jejich šíření.

---

Síťová bezpečnost je tedy nezbytným předpokladem pro zajištění bezproblémové funkce různorodých aktivit (podnikových i domácích) realizovaných ve spojení se sítí Internet. Důležitými kritérii pro posouzení míry efektivity zabezpečení jsou ochrana proti výpadku poskytované služby (služeb) a ochrana proti výpadku sítě jako celku pro všechny typy aktivit realizovaných v dané síti. Efektivní zabezpečení umožňuje přidávat nové typy služeb a aplikací bez narušení výkonnosti sítě jako celku. Ochrana dat je dalším nezbytným doplňkem síťové bezpečnosti, která omezuje výpadek poskytovaných služeb v případě změn jejich formy a obsahu.

Mezi výhody, které využívání zabezpečených sítí přináší, patří především důvěra zákazníka (utajení uživatelských dat), mobilita (zabezpečený přístup, který není narušen viry ani jinými potenciálními hrozbami), vyšší produktivita (méně času, který je třeba věnovat neproduktivním úlohám jako je administrace nevyžádaných zpráv (*Spam*) nebo boj s počítačovými viry) a ekonomické hledisko (výpadek sítě je často spojen s finanční ztrátou).



## 1.2 Pojem bezpečnostní systém

---



$E=mc^2$

Bezpečnostní systém je souborem zařízení a prostředků, resp. hardwarového a softwarového vybavení sítě, který využívá bezpečnostní protokoly a kryptografické algoritmy pro účely ochrany informačních a komunikačních systémů v podnikové sféře nebo u jednotlivců (např. domácí uživatelé).

---

Mezi funkce zajišťované bezpečnostními systémy patří sledování a kontrola příchozího a odchozího síťového provozu, detekce útoků, indikace ztráty nebo krádeže dat a ochrana integrity síťové infrastruktury včetně zajištění dostatečné úrovně výkonu sítě a poskytovaných služeb, zabezpečení provozu služeb a realizace nepřetržité ochrany proti výpadku poskytovaných služeb,...

V souvislosti s rostoucími nároky na bezpečnost sítí jsou bezpečnostní systémy stále složitější. Bezpečnostní systémy v tradičním pojetí, jakými jsou např. firewally, procházejí mnoha menšími či většími úpravami tak, aby se přizpůsobily novým bezpečnostním trendům, jakými jsou např. distribuované bezpečnostní mechanismy, komplexní správa zabezpečení a rozsáhlé využití kryptografických technik (např. protokol **IPSec** (*Internet Protocol Security*) v sítích **VPN** (*Virtual Private Networks*)).



Kromě toho, bezpečnostní systém tvoří jen dílčí část (i když velmi důležitou) celkové bezpečnostní infrastruktury instituce (podniku) nebo jednotlivce. Má-li být tato infrastruktura posuzována komplexně, pak musí být posuzována jako jeden celek spolu s dalšími opatřeními, jakými jsou fyzická bezpečnost, osobní bezpečnost, bezpečnost provozu, bezpečnost komunikace a začlenění sociálních mechanismů.

---

## 1.3 Pojem bezpečnostní služby



Bezpečnostní služba je služba, která zajišťuje odpovídající úroveň zabezpečení systémů nebo datových přenosů. Bezpečnostní služby vycházejí z bezpečnostních mechanismů, které jsou vytvořeny na základě předem deklarovaných bezpečnostních pravidel.

Po více než dvacet let je pod pojem informační bezpečnost zahrnovány pojmy důvěrnost (*Confidentiality*), úplnost dat (*Data Integrity*) a dostupnost (*Availability*). Tato trojice pojmů je často v literatuře označována jako triáda **CIA** (*Confidentiality, Integrity and Availability*) a tvoří tzv. základní princip informační bezpečnosti. Později byly k těmto původním základním prvkům informační bezpečnosti přidány ještě další, mezi které patří např. ověření identity (*Authentication*), řízení přístupu (*Access Control*), průkaznost (*Nonrepudiation*), a utajení dat (*Data Privacy*). Nicméně tato klasifikace je stále častým námětem debat bezpečnostních odborníků.

- Důvěrnost (*Confidentiality*) je spojena s ochranou informací (obecně dat) a procesem jejich zneprístupnění neoprávněným subjektům (společnosti, jednotlivci, stroje, procesy). Data jsou přístupná pouze jednoznačně určenému subjektu, resp. jednotce. Pojem informace je obecně chápán vlastní datový obsah zprávy, její velikost, doba existence, typ komunikace, atd.
- Úplnost dat (*Data Integrity*) vymezuje ochranu dat proti neoprávněnému zásahu ze strany neoprávněných subjektů (společnosti, jednotlivci, stroje, procesy) spojenému s vytvářením, změnou, odstraňováním, kopírováním nebo přeskupováním datového obsahu. Narušení úplnosti dat (*Integrity Violation*) je vždy způsobeno aktivním útokem. Přesněji řečeno, úplnost dat velmi úzce souvisí s důvěryhodností informačních zdrojů.
- Dostupnost (*Availability*) znamená mít aktuální přístup k informacím. Například havárie pevného disku nebo útoky typu **DoS** (*Denial of Service*) narušují dostupnost. Jakékoliv zpoždění, které překračuje očekávanou systémovou úroveň služby lze klasifikovat jako porušení dostupnosti dat. Informační systém, který není dostupný, když jej potřebujete, vlastně jako kdyby vůbec nebyl. Situace je tím horší, pokud jsou činnosti subjektu velkou mírou závislé na správné funkcionalitě počítačové a komunikační infrastruktury.
- Služba ověření identity (*Authentication*) zajišťuje ověření totožnosti komunikujících subjektů s následným potvrzením jejich identity. Komunikujícími subjekty mohou být lidé, stroje nebo procesy). K dispozici jsou tři nezávislé faktory pro ověření identity – povědomost (*Knowledge*), oprávnění (*Possession*) a vlastnictví (*Inherence*). Faktor povědomost deklaruje okruh znalostí, který musí uživatel mít, aby byl schopen se přihlásit. Faktor oprávnění deklaruje okruh prostředků, které musí mít uživatel k dispozici, aby byl schopen se přihlásit. Faktor vlastnictví zahrnuje okruh biologických znaků, které musí uživatel mít, aby byl schopen se přihlásit.

- Služba řízení přístupu (*Access Control*) je chápána jako ochrana informačních zdrojů nebo služeb z pohledu jejich zneužití ze strany neoprávněných subjektů (společnosti, jednotlivci, stroje, procesy). To znamená, že řízení přístupu je prevencí neoprávněného použití prostředků (tj. tato služba řídí oprávnění přístupu k určité množině prostředků, definuje, za jakých podmínek mohou být tyto prostředky použity a k jakým úkonům mají tyto prostředky povolení).
- Průkaznost (*Nonrepudiation*) je bezpečnostní službou, která využívá pro zajištění ochrany komunikujících subjektů evidenci jejich identifikačních údajů. V případě, pokud by jeden ze subjektů zapíral svou účast na komunikaci, lze pak tuto komunikaci jednoznačně prokázat, byť by se jí účastnil i jen částečně.
- Utajení dat (*Data Privacy*) je bezpečnostní službou, která zajišťuje individuální kontrolu nad údaji, která mohou být o komunikujícím subjektu shromažďována, resp. deklaruje způsob, jakým mohou být tyto údaje dále využívány a stanovit okruh subjektů, které je mohou využívat.

## 1.4 Pojem bezpečnostní mechanismy



Bezpečnostní mechanismus je proces, který v sobě zahrnuje bezpečnostní služby technického (hardware), logického (software), fyzického nebo administrativního charakteru. Bezpečnostní mechanismy zajišťují podporu pro bezpečnostní služby a provádějí specifické úkony k zajištění efektivní ochrany proti případnému útoku, resp. aby předešly negativním důsledkům potenciálního útoku.

Bezpečnostní mechanismy se dělí na skupinu mechanismů, které jsou začleněny na konkrétní protokolovou vrstvu referenčního modelu **RM-OSI** (*Reference Model of Open System Interconnection*) a na skupinu mechanismů, které nejsou svázány s konkrétní protokolovou vrstvou referenčního modelu **RM-OSI** nebo s konkrétním typem bezpečnostní služby. Následuje výčet vybraných typu bezpečnostních mechanismů:

- Mechanismus šifrování (*Encipherment*) chrání informační obsah zprávy. Je založen na matematických algoritmech, které transformují původní informační obsah zprávy na formát, který je pro neoprávněné subjekty nečitelný.
- Digitální podpis (*Digital Signature*) je mechanismem, který využívá vybranou kryptografickou transformaci konkrétní datové jednotky, která umožňuje ověřit pravost zdroje dat, celistvost informačního obsahu datové jednotky a zajišťuje tak ochranu proti padělání.
- Mechanismus řízení přístupu (*Access Control*) je ve své podstatě skupinou mechanismů, které definují okruh přístupových práv pro jednotlivé informační zdroje, tj. tento mechanismus realizuje správu přístupových práv k vybraným zdrojům.
- Celistvost dat (*Data Integrity*) zahrnuje soubor mechanismů používaných k zajištění integrity datových jednotek či datových toků.
- Výměna autorizačních informací (*Authentication Exchange*) je mechanismus sloužící ke zjištění totožnosti subjektu prostřednictvím výměny autentizačních údajů.
- Mechanismus provozní výplň (*Traffic Padding*) vkládá výplňové bity do mezer v datovém toku tak, aby znemožnil, případně zcela eliminoval, pokusy o analýzu síťového provozu.
- Řízení směrování (*Routing Control*) poskytuje výběr konkrétních fyzicky bezpečných tras pro přenos citlivých údajů a umožňuje změnu směrování v případě, pokud nastane podezření, že byla narušena bezpečnost používané trasy. Tento mechanismus v sobě zahrnuje mechanismus zabezpečení perimetru (*Perimeter Security*).
- Mechanismus certifikované ověření (*Notarization*) využívá služeb důvěryhodné třetí strany k nastavení určitých vlastností a parametrů pro bezpečnou výměnu dat.

- Mechanismus zabezpečení perimetru (*Perimeter Security*) umožňuje přijetí nebo odmítnutí dat pocházejících z konkrétní adresy či odesílaných na konkrétní adresu nebo služby nacházející se mimo lokální síť.

## 1.5 Klasifikace (kategorie) útočníků

Bezpečnostní hrozby jsou velmi často realizovány útočníky, které lze obecně rozdělit dle míry jejich schopností a intenzitou jejich činnosti. V této části uvedeme stručný souhrn charakteristik, které souvisí se schopnostmi a mírou aktivity daného typu útočníka a výsledné poznatky shrneme v přehledu jednotlivých kategorií útočníků.

Schopnost – Schopnosti útočníka jsou typicky vymezeny následujícími faktory:

- **Náklady**

- Tato oblast se velmi úzce dotýká objemu nákladů, které je schopen daný útočník utratit např. za nezbytné vybavení, které je vyžadováno pro realizaci úspěšného útoku. Vybavení může být extrémně levné, kdy je např. zapotřebí páječka a nezbytná kabeláž, až po neúnosně nákladné, kdy může být zapotřebí špičkové polovodičové testovací vybavení (např. rentgen).

- **Zkušenosti**

- Obecně se tento faktor vztahuje na dovednosti a znalosti, které musí útočník mít, aby byl tento schopen uskutečnit úspěšný útok. Některé typy útoků mohou být realizovány klidně i dětmi, pokud mají k dispozici detailní a jednoduché instrukce, naopak jiné typy útoků vyžadují hluboké znalosti konkrétních síťových technologií nebo součinnost osob, které jsou vyškoleny ve využívání speciálního vybavení. (*Pozn.: Tato poslední charakteristika však může být zahrnována i do kategorie Náklady.*)

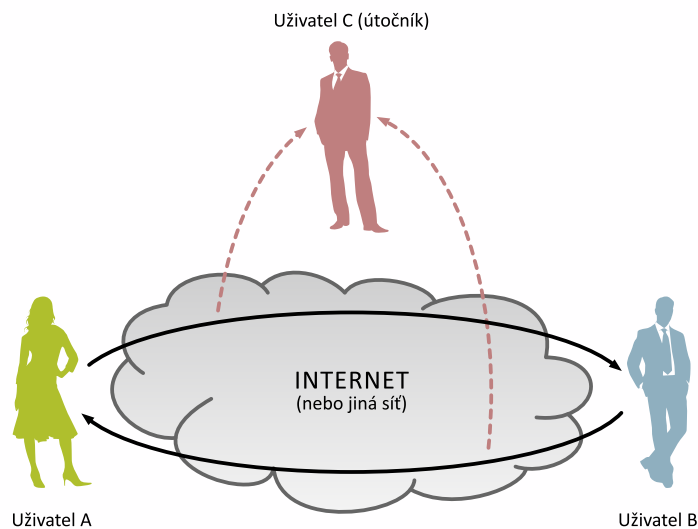
- **Nevystopovatelnost**

- Tato charakteristika se týká stop a indicií, které po sobě útočník může svou činností zanechat. Pokud bude síťový uzel po útoku ponechán v původním stavu (nastavení) jako před útokem, včetně nezměněného obsahu paměti, pak je jen velmi obtížné si útok povšimnout, pokud však nedojde k fyzickému zničení či poruše daného síťového uzlu.

Činnost – Aktivity útočníka mohou být obecně klasifikovány jako pasivní nebo aktivní:

- **Pasivní útoky**

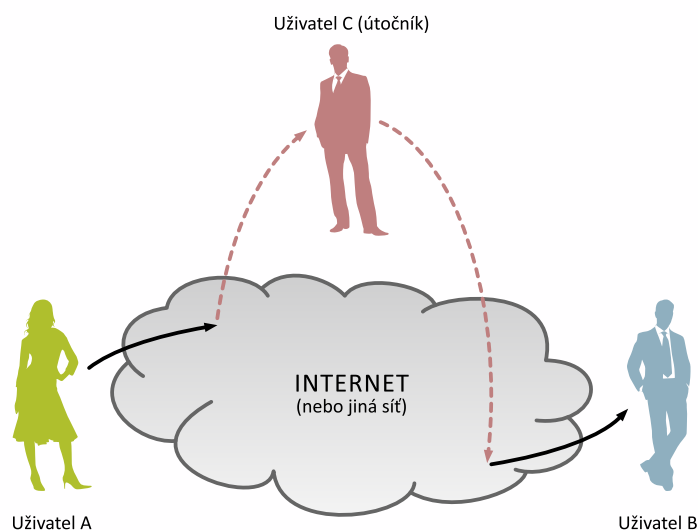
- Umožňují získat informace ze sítě pouhým sledováním právě probíhající komunikace. Tyto útoky zahrnují aktivity, jakými jsou analýza provozu, monitorování nechráněné komunikace, dešifrování slabě šifrovaného provozu a zachytávání autentizačních informací jakými jsou např. uživatelská jména a hesla. Tyto útoky tedy nemají přímý vliv na systémové prostředky.



Obr. 1.1 – Pasivní útok

- Aktivní útoky

- Cílem těchto útoků je naopak změna systémových prostředků (včetně dat) nebo ovlivnění jejich funkčnosti. Při tomto typu útoku se útočník snaží data přenášená příslušným kanálem odstranit, přidat nebo jinak měnit (Tampering), a to na kterémkoliv ze zařízení, které se účastní komunikace. Někdy mohou být pasivní útoky přípravnou fází pro útok aktivní.



Obr. 1.2 – Aktivní útok

Další možné dělení je na útoky neinvazivní, poloinvazivní a invazivní:

- Neinvazivní útoky – tento typ útoků neovlivňuje činnost napadeného zařízení.

- Poloinvazivní útoky – mění a manipulují s informačním obsahem napadeného zařízení, ale nemají přímý elektrický kontakt, resp. přístup k jeho integrovaným obvodům.
- Invazivní útoky – nemají prakticky žádná omezení z hlediska získávání informací z napadeného zařízení (př. průzkumné (sondovací) stanice).




---

Kategorii poloinvazivních nebo invazivních útoky nelze vždy zcela jednoznačně považovat pouze za útoky aktivní. Například pasivní poloinvazivní útok se může pokoušet získat citlivá data a údaje z paměťových nosičů, přičemž pasivní invazivní útok může využít sondovací stanici(e) pro snímání cenných datových signálů. Mezi příklady pasivních útoků patří analýza (monitorování) provozu a jeho kamufláž. Většina útoků je však útoky aktivními mezi které patří např. směrovací útoky, IP spoofing, odepření (výpadek) služeb (útok typu **DoS**), člověk uprostřed (*Man-in-the-Middle*), odposlech, replikace uzlu(ů), fyzické útoky atd.

---

Aby bylo možné posoudit schopnosti a míru aktivity útočníků, zavedla firma IBM následující taxonomii tříd útočníků:

- Třída I (chytří vnější útočníci) – často se jedná o velmi inteligentní osoby/jednotlivce, které/kteří ale nemusejí být detailně obeznámeni s napadaným systémem. Pro své útočné aktivity v zásadě využívají poměrně jednoduchá zařízení. Většinou se snaží využít již existující potenciálně slabá místa systému, než se snažit je vytvořit.
- Třída II (znalí vnitřní útočníci) – tento typ útočníků často disponuje poměrně vysokou úrovní technického vzdělání a bohatými zkušenostmi v oboru informačních technologií. Mohou mít různou úroveň znalostí o funkcionalitě napadaného systému, ale potenciálně mají ze své pozice k velké většině z nich přímý přístup. Pro své aktivity využívají velmi důmyslné nástroje a zařízení, umožňující detailní analýzu atakovaného systému.
- Třída III (organizované skupiny útočníků) – jedná se o týmy spolupracujících odborníků a specialistů s vhodně se doplňujícími schopnostmi a dovednostmi, kteří disponují dostatečnými finančními zdroji, které pro svou činnost účelně využívají. Jsou schopni detailní a hloubkové analýzy napadaného systému. Díky této analýze jsou poté schopni připravit velmi propracované útoky, často i za použití těch nejmodernějších analytických nástrojů. Součástí těchto týmů mohou být i útočníci ze třídy II.



## 1.6 Terminologie

Na úvod je možné konstatovat, že není v lidských silách poskytnout kompletní a ucelený slovníček pojmů zaměřený na oblast počítačové a síťové bezpečnosti. Tato kapitola je tedy pouze přehledem vybraných termínů a výrazů, se kterými se lze běžně a v rámci výše zmíněné problematiky setkat.

- Útok – v kontextu počítačové resp. síťové bezpečnosti je pojmem útok chápán pokus o přístup k informačním zdrojům počítače nebo prostředkům sítě bez potřebné úrovně autorizace, resp. pokus o obejítí nastavených bezpečnostních opatření.
- Audit – jedná se o proces sledování událostí souvisejících se zabezpečením systému, jakými jsou např. přihlášení do systému nebo sítě, přístup k vybraným objektům nebo nastavení uživatelských případně skupinových práv, resp. privilegií.
- Narušení – úspěšné prolomení bezpečnostních opatření směřující k získání kontroly přístupu k datům nebo prostředkům, a to bez potřebného oprávnění, nebo zpřístupnění dat či prostředků neoprávněným osobám, případně vymazání resp. změna obsahu počítačových souborů.
- Vyrovnávací paměť (Zásobník) – část paměti systému pro dočasné uchování dat.
- Přetečení zásobníku – možnost, jak způsobit pád systému, uložením většího objemu dat do zásobníku, než kolik je schopen zásobník (vyrovnávací paměť) pojmut.
- Protiopatření – kroky zajišťující prevenci před útoky nebo škodlivým kódem či reakci na ně.
- Cracker – označení jedince, který se specializuje na vyhledávání systémových hesel za účelem získání přístupu do počítačových systémů bez potřebné autorizace.
- Útok typu DoS – záměrná aktivita, která udržuje počítač nebo síť mimo provoz, tj. počítač nebo síť nejsou dostupné (př. uživatelé nemají možnost se přihlásit do sítě).
- Ohrožení – úroveň, do jaké míry jsou sítě nebo jednotlivé počítače napadnutelné v souvislosti s jejich potenciálními nedostatky resp. dobou trvání, kdy je možné tyto nedostatky ze strany útočníků (hackerů) možné využít.
- Hacker – jedinec, který se detailně zabývá počítačovým programováním a provozem operačních systémů, přičemž testuje jejich omezení a identifikuje tak potenciální zranitelná místa.
- Škodlivý kód – počítačový program nebo skript vykonávající činnosti, které mohou poškodit systém nebo jeho data, může však také poskytovat neautorizovaný přístup do systému.

- Spolehlivost – míra pravděpodobnosti počítačového systému nebo sítě vykonávat bez potíží požadované činnosti, a to za normálních provozních podmínek ve vymezeném časovém období.
- Riziko – míra pravděpodobnosti, kdy jistá bezpečnostní hrozba využije potenciální zranitelnosti systému, což může mít za následek poškození případně ztrátu dat nebo jiné nežádoucí důsledky. To znamená, že míra rizika je závislá na míře pravděpodobnosti hrozby a stupni zranitelnosti.
- Omezení rizik – proces identifikace vzniku událostí, které představují hrozbu pro spolehlivost systému, celistvost a důvěrnost dat, a dohledu na jejich případnou minimalizaci resp. úplnou eliminaci.
- Sniffer – program, který umožňuje zachytávat data procházející sítě. Často bývá označován pojmem „Packet Sniffer“.
- Hrozba – potenciální nebezpečí pro data nebo systémy. Hrozbou může být virus, hacker, přírodní jev, jako např. tornádo, nespokojený zaměstnanec, konkurent a celá řada dalších.
- Trójský kůň – počítačový program, který nevykonává žádné zjevné funkce, má však nepříznivý vliv na výkonnost napadeného systému. Obsahuje skrytý kód, který umožňuje neoprávněné shromažďování, modifikaci nebo destrukci dat.
- Virus – program, který je úmyslně vložen do systému nebo sítě za účelem vykonávání neoprávněných činností, kterými mohou být např. neškodné vyskakovací (pop-up) hlášky, ale i poškození případně zničení všech dat na pevném disku.
- Zranitelnost – slabá místa hardwaru, softwaru nebo bezpečnostních opatření, která ponechávají síť nebo systém otevřený proti hrozbám neautorizovaného přístupu, poškození nebo zničení dat.
- Červ – program, který dokáže kopírovat (replikovat) sám sebe a šířit se z jednoho zařízení na druhé prostřednictvím dostupného síťového připojení.

## 2 Potenciální hrozby zabezpečení sítí

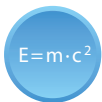
---



Všude tam, kde je dostupné připojení k síti, se vyskytují i bezpečnostní hrozby. Typy potenciálních hrozeb v oblasti zabezpečení sítí se neustále vyvíjejí. Neustálý dohled stavu síťových systémů a jejich zabezpečení je tak prioritou pro všechny správce sítí. Pokud by byla bezpečnost sítě narušena, může to mít vážné až fatální následky spojené např. se ztrátou soukromí nebo citlivých dat a údajů.

Je důležité zde ještě podotknout, že ne všechny bezpečnostní hrozby musejí být vždy jen závažné. Méně závažné hrozby pocházejí obvykle od zaměstnanců, kteří nemají příliš zkušeností s prací na počítači, a tak si často ani nejsou vědomi bezpečnostních hrozeb a rizik z nich plynoucích. Chyby a často i jen drobná opomenutí tak mohou způsobit ztrátu, poškození nebo nechtěnou změnu cenných dat. Do této kategorie méně závažných hrozeb patří i vliv přírodních jevů. V této kapitole se však budeme detailně věnovat pouze potenciálně závažným bezpečnostním hrozbám a rizikům.

---



Závažné hrozby v sobě zahrnují interní útoky zlomyslných zaměstnanců a externí útoky realizované ostatními typy útočnicků, kteří chtějí především narušit a ochromit chod dané organizace. K nejnebezpečnějším útočnickům patří ty osoby, které jsou detailně obeznámeny s infrastrukturou a fungováním dané organizace, protože vědí, jaká bezpečnostní opatření jsou organizací využívána.

---

Nástroje a metody používané pro síťové útoky se neustále vyvíjejí. Ještě nedávno využívali hackeři důmyslné počítačové systémy, museli umět programovat a mít dostatečné síťové znalosti, aby byli schopni realizovat primitivní nástroje pro uskutečnění základních útoků. V současnosti se možnosti hackerů, jejich metod a nástrojů enormně zlepšily. Hackeři již nemusejí mít tak rozsáhlé znalosti jako kdysi. Na počítačové kriminalitě se dnes podílejí i lidé, kteří by toho dříve schopni nebyli.

Definice pojmu „hacker“ se v průběhu let zásadně proměňuje. Hackerem byl dříve chápán jedinec, který hledal potěšení, pokud se mu podařilo napadený systém vyřadit z provozu. Dnes je za hackera považován každý, kdo získá přístup do systému nebo manipuluje se systémem bez potřebného oprávnění. Přesnějším označením pro přechodzí případy je pojem „cracker“. Mezi dnes běžně používané metody, které umožňují získat přístup do systému bez patřičného oprávnění, patří prolamování slabých hesel (password cracking), IP spoofing a metody sociálního inženýrství.

Velkým problémem je existence komunikačního vakuu mezi vývojáři bezpečnostních technologií a vývojáři sítí. Přestože je zabezpečení sítí významnou podmínkou pro úspěšný rozvoj sítí, existuje zde znatelný nedostatek zabezpečovacích metod, které mohou být jednoduše použitelné v reálném provozu. Na rozdíl od vlastního fyzického návrhu sítě není hledisko návrhu zabezpečení sítě příliš dobře rozpracováno, tj. neexistuje předepsaná metodika jak zapracovat bezpečnostní požadavky.

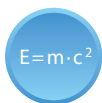


---

Celá řada bezpečnostních hrozeb je dnes distribuována přes Internet. Důležité je si uvědomit, že neodmyslitelnou součástí Internetu jsou dnes i mobilní telefony a tablety. Podrobná analýza jejich vlastností a lidského chování poskytuje cenné údaje a umožňuje tak vytvořit schéma zabezpečení.

---

## 2.1 Malware: viry, červi, trojské koně a zombie



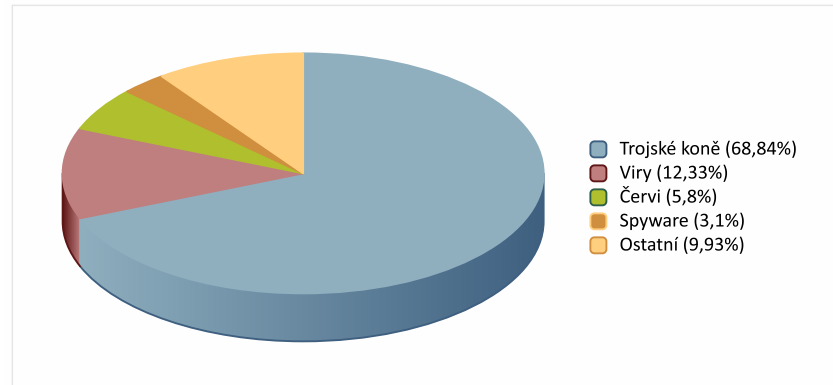
Škodlivý (zlomyslný) software (malware) je software záměrně navržený tak, aby infiltroval nebo poškodil počítačový systém bez souhlasu jeho majitele (provozovatele). Může způsobit ztrátu dat nebo poškození systému jako celku. Počítačové viry tvoří jednu rozsáhlou třídu škodlivých kódů, které se mohou šířit mezi počítači a provádět nežádoucí operace a aktivity.

Spuštěním malwaru můžeme poškodit bezproblémovou činnost počítače a jeho komponent, nebo může být tento software použit pro shromažďování citlivých informací a údajů, nebo umožní neautorizovaný přístup do počítačového systému. Malware není totéž co chybně fungující software. I chybně fungující software má totiž svůj legitimní účel použití, avšak obsahuje chyby a nedostatky, kterých si nikdo před jeho vydáním nevšiml. Ve skutečnosti jsou tedy počítačové viry pouhou podskupinou v rámci kategorie programů označovaných jako Malware. Patří sem také červi (*worms*), trojské koně (*Trojan horses*), adware, spyware, rootkity (*Rootkits*), a celá řada dalších.

Dle analýzy realizované PandaLabs bylo v průběhu roku 2014 identifikováno více než 75 miliónů nových vzorků malwaru, což představuje 34 % doposud známého malwaru, a jedná se téměř o dvojnásobek hodnoty zjištěné v předchozím roce 2013 (30 miliónů). Dále uvádíme definice nejdůležitějších kategorií malwaru:

- Viry jsou samokopírovatelné programy, které pro svou činnost a šíření využívají soubory napadeného systému. Jakmile jednou infikovaný soubor otevřeme, stává se virus aktivním v rámci systému.
- Červ je program podobný viru, a to z hlediska jeho samokopírovatelnosti, ale nepotřebuje pro účel svého šíření systémové soubory. Hlavním účelem červů je jejich vlastní rozmnožování (replikace). Původně byl tento typ programů využíván pro zcela legitimní účely v souvislosti se správou sítě, avšak jejich schopnost se velmi rychle šířit byla velmi brzy zneužita hackery pro zlomyslné účely a vytvoření škodlivých červů, které mohou využít slabiny operačního systému a provádět tak záškodnické aktivity. Existují dvě hlavní skupiny červů – hromadní e-mailoví červi a síťoví červi. Hromadní e-mailoví červi využívají e-mailu jako prostředku pro infikování dalších počítačů. Síťoví červi si nejprve vybírají vhodný cíl, avšak jakmile se dostane červ do svého cílového hostitele, může jej infikovat např. prostřednictvím trojského koně nebo i jinak.
- Trojský kůň je na první pohled nezahoubný uživatelský program, ale ve skutečnosti provádí akce, které uživatel neměl v plánu nebo si jich nebyl vědom. Zjednodušeně řečeno, trojský kůň může provádět veškeré akce, kterými disponuje uživatel přihlášený do systému. To znamená, že trojský kůň je obzvláště nebezpečný, pokud jej nainstaluje nic netušící uživatel s právy administrátora. Malware, který se obvykle šíří ve formě trojských koní, je označován termínem ransomware. Tento druh malwaru napadá počítačový systém, omezuje přístup k počítači a požaduje, aby uživatel zaplatil autorům za jeho odstranění ze systému.

- Zombie je škodlivý software, který se šíří prostřednictvím sítě. Po jeho úspěšném průniku do počítačového systému lze infikovaný počítač na dálku ovládat a administrovat. Pokud je infikováno stejným typem zombie více počítačů, je tato struktura označována pojmem botnet. Botnet infrastrukturu lze ovládat z jednoho vzdáleného počítače a je pak možné nutit infikované počítače provádět stejné příkazy. To umožňuje realizaci útoků typu **DDoS** (*Distributed Denial of Service*).



Obr. 2.1 – Nové typy malwaru, které byly vytvořeny v průběhu roku 2014

## 2.2 Spyware a adware

$E=m \cdot c^2$

Pojem adware označuje software, který zobrazuje reklamní obsah, jenž je po instalaci adwaru integrován do ostatních uživatelských programů a aplikací.

Adware je považován za legitimní alternativu pro spotřebitele, kteří nechtějí platit za licencovaný software. Existuje totiž celá řada užitečných programů, nástrojů a her distribuovaných právě formou adwaru (někdy označováno jako freeware). V současné době roste počet vývojářů softwaru, kteří nabízejí svůj produkt formou „sponzorovaného“ softwaru. Uživatel má však i nadále možnost koupit si plnou verzi programu, a to bez doplňkového reklamního obsahu.



V případě legálního adwaru by po ukončení běhu programu měla být odstraněna i všechna reklamní sdělení. Uživatel také může definitivně odstranit reklamní sdělení zakoupením registračního klíče.

$E=m \cdot c^2$

Spyware je obecný termín používaný pro software instalovaný prostřednictvím Internetu na počítač bez předchozího souhlasu jeho majitele, který vykonává různé činnosti, jakými jsou např. reklamní sdělení, shromažďování informací o pohybu uživatele na webu nebo změna konfigurace počítače.

Získané informace mohou být zaslány přes Internet někam na server, obvykle jako skrytý vedlejší efekt programu, přičemž tyto informace mohou být shromažďovány z různých důvodů. Typickou taktikou jsou nevyžádané „vyskakovací“ reklamy, krádež osobních informací (včetně hesel k on-line účtům anebo citlivé finanční informace, jako jsou čísla kreditních karet), sledování činnosti na webu pro marketingové účely a následné směřování HTTP požadavků na reklamní stránky.

Spyware může být nainstalován spolu s jiným softwarem nebo se může jednat o výsledek virové infekce. U některých typů infekcí může být jeho přítomnost uživateli skryta. Spyware bývá často navržen tak, aby bylo obtížné jej nejen odstranit, ale i detekovat. Jiné druhy spywaru realizují změny v počítači, které mohou být nepříjemné a mohou počítač zpomalit nebo i znefunkčnit.



Uživatelé si často povšimnou nežádoucího chování a snížení výkonnosti systému. Spyware může taktéž způsobit zvýšenou aktivitu procesoru, využití pevného disku a nárůst síťového provozu.

Antispyware programy mohou pracovat tak, že poskytují ochranu buď v reálném čase, nebo provádí scanování v pravidelných intervalech. V prvním případě mohou tyto programy scanovat všechny síťový provoz pro spyware a blokovat jakoukoliv hrozbu podobným způsobem jako antivirus [[https://en.wikipedia.org/wiki/Anti\\_virus](https://en.wikipedia.org/wiki/Anti_virus)]. Ve druhém případě jsou použity pouze pro detekci a odstranění spywaru, který již byl do počítače nainstalován.

## 2.3 Zranitelnost a útoky typu Zero-day

$E=m \cdot c^2$

Existuje několik definic zranitelnosti typu Zero-day, které se však od sebe mírně odlišují. Jedny z definic spojují tento termín s chybou softwaru, kdy může být systém vystaven kybernetickému útoku před vydáním tzv. záplaty, přičemž „nultým dnem“ (*Zero-day*) je chápán původní stav až do okamžiku odstranění konkrétní softwarové chyby. Jiné definice naopak označují „nultým dnem“ ten den, kdy se tato hrozba či riziko stane veřejně známým. Doba hrozby útokem typu Zero-day tak může být několik dní, týdnů, ale i roků. Doba jejího trvání je tedy plně v rukách tvůrců softwaru.



Tento typ útoku je však jen zřídka kdy objeven. Ve skutečnosti to často netrvá jen dny a týdny, ale i měsíce a někdy i roky, než developer odhalí zranitelnost, která umožnila realizaci kyberútoku.

V obou výše uvedených případech je však výsledek stejný – uživatelé jsou ohroženi útokem. L. Bilge a T. Dumitras shodně konstatují v [5]: „Pokud zůstává zranitelnost neznámou, systém nemůže být vhodně opraven a antiviry nemohou odhalit útok prostřednictvím scanováním signatur daného útoku.“ Zranitelná místa softwaru mohou být odhalena crackery, bezpečnostními společnostmi nebo výzkumníky, prodejci nebo prostřednictvím samotných uživatelů. Pokud bude odhaleno crackerem, pak bude drženo v tajnosti tak dlouho, jak jen to bude možné a bude kolovat pouze v rámci komunity crackerů/hackerů až do té doby, dokud softwarové nebo bezpečnostní společnosti tuto hrozbu neobjeví díky aktivně prováděným útokům směřovaným právě na toto zranitelné místo.



Obr. 2.2 – Interval zranitelnosti v rámci útoku typu Zero-day

Útoky typu Zero-day představují v posledních letech jedny z nejvíce destruktivních a specificky zaměřených útoků. Například operace AURORA (2009) využívala zranitelného místa programu Internet Explorer a zasáhla více jak 20 cílů včetně společností Morgan Stanley, Google, Yahoo, Dow Chemical, Adobe Systems, Juniper Networks a dokonce i bezpečnostní společnost Symantec.



Pravděpodobně nejznámějším útokem typu Zero-day byl STUXNET (2010). Ve skutečnosti využil červ STUXNET čtyři samostatné útoky Zero-day k poškození průmyslových řadičů, a narušil tak zařízení na obohacování uranu v iránském Natanzu. Útok STUXNET byl navržen tak, aby dokázal manipulovat s průmyslovými programovatelnými logickými řadiči (PLCs) vyráběnými německou společností SIEMENS, které kontrolovaly a sledovaly rychlost odstředivek. Útočníci se nemohli na dálku dostat přímo k těmto zařízením, protože



ovládací počítače nebyly v té době připojeny k Internetu. Proto útočníci založili svůj útok na infikovaných USB paměťových nosičích. Nejprve tedy infikovali počítače pěti externích společností, které se nějakým způsobem podílely na výše zmíněném jaderném programu. Využití čtyř útoků typu Zero-day je zcela mimořádné a unikátní na tento typ hrozby. Kromě toho používá STUXNET také celou řadu dalších zranitelností, kterými jen prokazuje svou mimořádnou míru propracovanosti, promyšlenosti a důsledného plánování.

---

## 2.4 Skenování a podvržený obsah (spoofing), krádež identity



$E=m \cdot c^2$

---

V kontextu se zaměřením tohoto modulu je pojmem scanner označován počítačový program, který umožňuje hackerům na dálku určit a vyhledat potenciálně slabě zabezpečená místa systému.

---

Scannery však mohou využívat i správci systémů pro analýzu a případnou opravu nalezených slabě zabezpečených míst v systému, a to ještě před tím, než by tato místa mohla být nalezena a zneužita případnými útočníky. Velké množství skenovacích programů je volně dostupné na Internetu.

Dobrý skenovací program umožňuje vyhledat cílový počítač na Internetu (a to především takový, který je slabě zabezpečen), zjistí, které služby TCP/IP jsou na zaměřeném počítači spuštěny, a provede analýzu těch služeb, které mohou být potenciálně bezpečnostním rizikem.



$E=m \cdot c^2$

---

Útok typu spoofing je uskutečněn tehdy, kdy se útočník vydává za jiné zařízení či uživatele v síti.

---

Existuje několik různých typů spoofing útoků – např. e-mailový spoofing, IP spoofing, ARP spoofing, DNS server spoofing.

E-mailový spoofing souvisí především s odesláním e-mailových zpráv z falešné e-mailové adresy nebo s falšováním e-mailové adresy jiného uživatele. Většina e-mailových serverů již dnes má integrovány potřebné bezpečnostní prvky, které brání v odeslání zpráv od neautorizovaných uživatelů. Avšak i tato opatření nezabrání přijímat e-maily z adres, které nejsou skutečnou platnou adresou uživatele, který zprávu odeslal.

IP spoofing spočívá v tom, že útočník odesílá podvržené IP pakety z falešné zdrojové IP adresy s úmyslem zakrýt svou vlastní identitu. IP spoofing tedy spočívá v zasílání zpráv (IP paketů) z adresy počítače útočníka s využitím zdrojové IP adresy některého důvěryhodného počítače v síti.



Flag

---

Dnes máme k dispozici širokou řadu nástrojů, metodických postupů a opatření, která jsou využitelná jak ze strany jednotlivců, tak ze strany společností a organizací, a kterými lze snížit míru rizika spoofingu na akceptovatelnou mez. Mezi obecná opatření, která lze chápat také jako prevenci spoofingu, lze zahrnout filtrování paketů (*Packet Filtering*), využití softwaru pro detekci spoofingu (*Spoofing Detection Software*) a aplikaci kryptografických síťových protokolů (*Cryptographic Network Protocols*).

---

## 2.5 Útok spojený s výpadkem služby DoS (Denial of Service) a distribuovaný útok typu DoS (DDoS)

$E=m \cdot c^2$

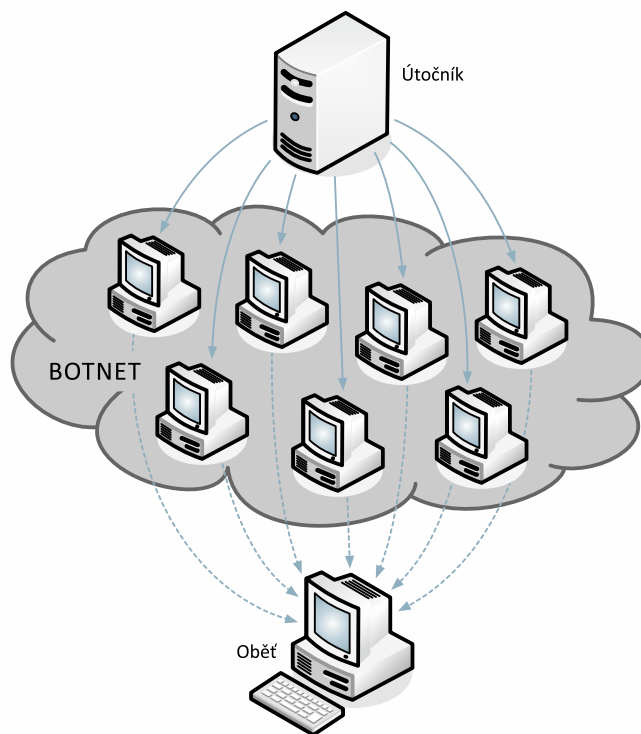
Jak je podrobněji uvedeno v [8], „Útoky typu **DoS** jsou jednou z nejoblíbenějších u hackerů, kteří tak svou aktivitou chtějí narušit provoz dané sítě či sítí. Tímto útokem nemá útočník možnost zničit nebo odcizit data, jako je tomu u jiných typů útoků, cílem útoku **DoS** je však znemožnit normální provoz v dané síti, resp. zamezit dostupnost síťových služeb oprávněným uživatelům. Útoky typu **DoS** jsou vcelku snadné realizovat; potřebný software je snadno dostupný z webových stránek hackerů, kteří tak umožňují komukoliv uskutečnit útoky typu DoS s malými nebo vůbec žádnými technickými znalostmi.“

U tohoto typu útoku přijímá napadený systém příliš mnoho požadavků, které však není schopen dlouhodobě odbavovat, tj. není schopen realizovat komunikaci dle doručených požadavků. Jinými slovy, spotřebovává veškeré své dostupné zdroje na dokončení tzv. handshake procedury. V konečném důsledku je pak množstvím příchozích požadavků natolik přetížen, že jej množství těchto požadavků uvede zcela mimo provoz, tj. přestane poskytovat původně nabízené služby.

$E=m \cdot c^2$

Distribuované útoky typu **DoS** (**DDoS**) využívají mezilehlé zprostředkující počítače nazývané pojmem agent (často se jedná o již ovládnuté systémy), které jsou často infikovány trójskými koni. Tyto systémy pak vytvářejí strukturu botnet, která záměrně útočí na jiný systém útokem typu DoS.

Rozdíl oproti klasickému útokem typu **DoS** tedy spočívá ve využití struktury botnet. Útok typu **DDoS** může využívat stovky nebo i tisíce počítačů a často i globálně sdíleného připojení k Internetu.



Obr. 2.3 – Schéma útoku typu DDoS

Útočník aktivuje na dálku infiltrované trójské koně, což umožní mezilehlým počítačům současně zahájit cílený útok. Tento mechanismus znemožňuje jednoduše zastavit útok tím, že zablokujeme jednu IP adresu, jelikož útok pochází ze systémů, které jsou rozmístěny na fyzicky odlišných místech. Kromě toho je také jen velmi obtížné odlišit provoz od oprávněného uživatele a útočníka.



Je důležité si uvědomit, že útoky typu **DDoS** představují hrozbu ve dvou rovinách. Jednak může být daná síť primárním cílem útoku typu **DoS** likvidujícím její servery a ochromujícím její provoz, na druhé straně může jít o útok s cílem zneužít její infrastrukturu pro útok typu **DoS** proti jiným sítím.

Útoky typu **DDoS** lze rozdělit z hlediska cíle útoku na objemové útoky, protokolové útoky a útoky na aplikační vrstvě. V prvním případě je cílem zahlcení dostupné šířky pásma napadené sítě, ve druhém případě jde o zahlcení kapacity serveru nebo dostupných zdrojů komunikačního zařízení a ve třetím případě jde o zhroucení funkcionality aplikačního serveru.

## 2.6 Útoky spojené s pojmem sociální inženýrství



$E=mc^2$

---

Sociální inženýrství (*Social Engineering*) je definováno jako proces získávání důvěrných informací pomocí lidské interakce.

---

Typy informací, které se hackeři tímto způsobem pokoušejí získat, mohou být velmi odlišné. Avšak pokud jsou cíleně klamáni jednotlivci, pak se hackeři hlavně zaměřují na získávání různých typů hesel, citlivých bankovních údajů (např. přístupových údajů k bankovním účtům), případně jak získat kontrolu resp. přístup do jejich počítačů využitím skryté instalace škodlivých programů.

Na rozdíl od jiných typů útoků, sociální inženýrství nemá žádnou spojitost s využitím technických slabin počítačového hardwaru nebo softwaru a samo o sobě ani nevyžaduje příliš rozsáhlé technické dovednosti. Namísto toho tento typ útoku využívá zcela přirozených lidských slabostí – jakými jsou např. nepozornost, naivita nebo přílišná důvěřivost či touha se sdružovat s ostatními a registrovat se v rámci různých komunit a seskupení na Internetu. Všechny tyto slabosti umožňují útočníkovi získat přístup k legitimním síťovým oprávněním, která následně zneužije. Schopnosti a dovednosti, které jsou pro útočníka těmi nejužitečnějšími, se opírají o techniku, která bývá v anglické literatuře označována termínem *people skills*, a mezi které lze zcela jistě zahrnout kouzlo či charisma osobnosti nebo třeba i autoritativní či přesvědčivé vystupování.



---

Mnoho bezpečnostních analytiků považuje za nejslabší článek v bezpečnostním řetězci právě člověka, resp. lidský faktor, který bývá svými slabostmi velmi často ovlivněn ve svém chování. Mezi časté a dnes již zcela běžné útoky sociálního inženýrství patří podvrhnuté e-mailové zprávy zaslané od „přátel“, které však obsahují odkazy nebo přímo soubory ke stažení s přiloženým škodlivým softwarem, nebo které vás žádají o pomoc a očekávají vaši okamžitou reakci či posílání falešných e-mailů z bankovních institucí, které vás vyzývají k zadání vašich přihlašovacích údajů k bankovnímu účtu, apod. V posledních dvou předchozích případech se jedná o podvodnou techniku nazývanou *phishing*.

---

## 3 Komponenty síťového bezpečnostního systému

Pokud chcete výrazně snížit zranitelnost vašeho počítače připojeného do sítě, pak je důležité vědět, že existuje velké množství dostupných produktů a řešení, které vám s tímto problémem pomohou. Jednotlivci i firmy či organizace mají možnost výběru ze široké palety technologií od základních balíčků antivirových programů až po specializovaný hardware primárně zaměřený na síťovou bezpečnost, jakými jsou např. bezpečnostní brány (*firewalls*), a které poskytují ucelenou ochranu všech částí a komponent v síti.



Na tomto místě je důležité upozornit na jeden mimořádně důležitý aspekt. Tímto aspektem je fakt, že žádné jednoduché bezpečnostní řešení neochrání váš systém před všemi možnými typy bezpečnostních hrozeb a rizik. Bezpečnostní systém sítě se obvykle skládá z mnoha komponent. V ideálním případě by měly všechny komponenty bezpečnostního systému sítě spolupracovat, a pokud by přeci jen byla některá z nich překonána či by selhala, ostatní by ji měly zastoupit, a tím udržet bezpečnost a celistvost (integritu) systému nenarušenu. Tyto komponenty mohou být realizovány hardwarově a/nebo softwarově. Softwarové komponenty by však měly být pravidelně aktualizovány, a to z důvodu doplnění ochranných prostředků proti případným novým potenciálním hrozbám.

Firmy a organizace dnes využívají kombinace bezpečnostních bran (*firewalls*), systémů **IDS** (*Intrusion Detection System*), šifrování (*encryption*) a sofistikovaných autentizačních mechanismů pro vytvoření interních podnikových sítí označovaných termínem „intranet“, které jsou následně připojeny k Internetu, ale zároveň jsou její jednotlivé součásti jednotně a centrálně chráněny před hrozbami z Internetu. Intranet je tedy soukromá uzavřená počítačová síť, která však využívá internetové protokoly. Intranet se od „extranetu“ odlišuje především v tom, že přístup k jeho infrastruktuře a funkcím je všeobecně omezen výhradně na zaměstnance firmy či organizace, zatímco extranet může být zpřístupněn i pro zákazníky či klienty, dodavatele případně i o další kategorie autorizovaných účastníků.


## 3.1 Anti-virus and anti-spyware



$E=mc^2$

Viry, červi a trójské koně patří k představitelům škodlivého softwaru, který je často označován pod pojmem Malware. Speciální tzv. anti-malwarové nástroje jsou pak používány k prevenci, detekci a případnému odstranění nalezeného malwaru, jakými jsou viry, počítačové červi, trójské koně, spyware a adware. Antivirový software je dnes již dodáván s většinou počítačů a poskytuje tak ochranu před většinou virů, ale pouze v případě, pokud je tento software pravidelně aktualizován a správně udržován, jinak by totiž neposkytoval adekvátní ochranu zejména proti novým virům.

Celý antivirový průmysl se opírá o rozsáhlou síť uživatelů, kteří mu poskytují včasná varování týkající se nových virů. Protiopatření tak mohou být pružně vyvíjena a rychle distribuována. Každý měsíc vznikají tisíce nových virů nebo jejich variant a je tedy přímo nezbytné, aby byla virová databáze stále a průběžně aktualizována. Virová databáze je uchovávána jako antivirový balíček, který umožňuje identifikovat všechny známé viry ještě před tím, než zaútočí. Antivirové programy renomovaných firem pravidelně uveřejňují nové aktualizace virových databází na svých webových stránkách, přičemž často i samotné programy automaticky upozorňují uživatele na potřebu své aktualizace. Základním pravidlem síťové bezpečnosti je garance, že všechny počítače v síti budou udržovány v aktuálním stavu a v ideálním případě tak budou chráněny identickým antivirovým balíčkem. Cílem je udržet náklady na údržbu a aktualizace na co nejnižší úrovni. Taktéž je velmi potřebné pravidelně aktualizovat samotný antivirový program.



Bez ohledu na to, jak užitečným je antivirový software, mohou se občas projevit i některé jeho nevýhody. Antivirový software totiž může např. snížit výkonnost počítače. Nezkoušení uživatelé mohou mít také potíže pochopit některé jeho pokyny a reagovat správně na výzvy, které program uvádí. Nesprávná rozhodnutí uživatele tak potenciálně mohou vést až k narušení resp. ohrožení jeho bezpečnosti.

Odstranění viru je termín používaný pro proces očisty počítače od škodlivého kódu. Existuje několik způsobů odstranění viru – odstranění kódu z infikovaného souboru, který odpovídá danému typu viru; odstranění infikovaného souboru nebo jeho umístění do tzv. „karantény“, což je místo, kde ho není možné spustit.

Obvykle jsou pro výše uvedené postupy využívány různé metody.

Jednou z metod detekce je detekce viru na základě jeho signatury, což představuje vyhledávání známých vzorků dat v rámci spustitelného kódu programu. Viry se rozmnožují infikováním hostitelských aplikací, což znamená, že kopírují část svého spustitelného kódu do již existujícího programu. Aby byla zajištěna správná funkce viru, jsou viry naprogramovány tak, že nikdy neinfikují stejný soubor vícekrát. To je zajištěno tak, že viry vkládají sérii bajtů do infikovaného souboru resp. aplikace a následně kontrolují, zda už nebyl soubor infikován – tento proces je označován jako virová signatura (podpis). Antivirové programy vyhledávají právě tyto signatury, které jsou vždy jedinečné pro každý virus, a proto je nalezení této signatury využitelné pro jejich vlastní detekci. Tato metoda se nazývá detekcí na

základě signatury (*Signature Based Detection*). Jedná se o nejstarší metodu detekce virů používanou antivirovými programy.

---



Výše uvedená metoda však není schopna detekovat viry, jejichž signatury nebyly uloženy do virové databáze vydavatelem antivirového programu. Kromě toho programátoři virů často svým produktům dodávají různé maskovací funkce, aby bylo jejich podpis složité odhalit. V ideálním případě takto maskovanou signaturu nelze vůbec odhalit. Pokud tedy chceme efektivně čelit této nové hrozbě a chránit tak svůj počítač i před novými typy virů, musíme využít heuristický přístup detekce virů.

---

Jedním z představitelů heuristického přístupu, jsou tzv. generické signatury. Tyto generické signatury dokáží identifikovat i nové viry nebo modifikované varianty již existujících virů tím, že hledají známý škodlivý kód nebo nepatrné změny tohoto kódu uloženého v infikovaných souborech. Metoda heuristické analýzy tedy zahrnuje takovou analýzu chování aplikací s cílem detekovat aktivity podobné těm, které vykonávají a kterými se projevují již známé viry.

---



Tento typ antivirových programů je schopen detekovat viry, i když nemá nejnověji aktualizovanou virovou databázi.

---



Na druhou stranu se tyto antivirové programy mohou ve své detekci mýlit, a tím pádem pak vyvolávají falešný poplach.

---



## 3.2 Firewall



$E=mc^2$

Bezpečnostní brána (Firewall) je typický kontrolní hraniční mechanismus často značovaný jako tzv. perimetr obrany. Účelem firewallu je zabránit neoprávněnému přístupu do vyhrazené sítě resp. z okolních sítí, omezením odchozího a příchozího provozu vyhrazené sítě.

Všechna příchozí a odchozí data dané sítě tedy procházejí firewallem, který podrobně zkoumá každý paket a blokuje ty pakety, které nesplňují nastavená bezpečnostní kritéria. Firewally mohou být implementovány jako čistě hardwarové či softwarové nebo jako kombinace obou platform [8].



Firewallly uplatňují nastavené zásady zabezpečení tím, že omezují přístup k vymezeným síťovým prostředkům. V analogii s fyzickým zabezpečením je firewall ekvivalentem k zámku na vstupních dveřích nebo na dveřích uvnitř budovy – umožňuje tak vstup pouze oprávněným uživatelům, kteří jsou vlastníky klíče nebo přístupové karty umožňující vstup. Firewallly jsou dnes dostupné i v provedeních vhodných pro domácí použití. „Domácí“ firewall vytváří ochrannou vrstvu mezi sítí uživatele a vnějším síťovým prostředím. Ve skutečnosti firewall replikuje chráněnou síť přímo na jejím vstupu tak, že umožňuje příjem a vysílání autorizovaných dat bez výrazného navýšení zpoždění. Jsou zde však integrovány vestavěné filtry provozu, které brání průniku neautorizovaným nebo potenciálně nebezpečným materiálům do systému. Kromě toho, firewallly poskytují důležité přihlašovací a prověřovací funkce. Díky těmto funkcím mohou správci získat poměrně detailní přehled o provozu v dané síti, např. jaký typ a objem provozu je danou sítí přenášen včetně počtu pokusů o průnik do dané sítě.

Národní institut pro standardy a technologie **NIST** (*The National Institute of Standards and Technology*) 800-41, [9] dělí firewallly do tří základních kategorií – nastavový firewall (paketový filtr – *Packet Filter Firewall*), stavový firewall (*Stateful Packet Inspection Firewall*) a aplikační firewall (brána, resp. *Proxy Firewall*). Předchozí tři kategorie však nepředstavují tři zcela nezávislé jednotky, ale naopak navzájem spolupracující jednotky. Většina moderních firewallů totiž integruje všechny tři výše uvedené funkcionality v jednom fyzickém zařízení, a to z důvodu celkového zlepšení funkčnosti a případně i výkonnosti firewallu.

Nestavový firewall (paketový filtr) je ve své podstatě směrovací zařízení (Router), které má navíc funkce umožňující správu přístupových práv na systémové úrovni a umožňuje tak propracované řízení komunikačních relací. Díky těmto funkcím je pak možné detailně filtrovat síťový provoz na základě charakteru analyzovaného provozu. Tyto firewallly jsou obvykle cíleně rozmístěny v rámci síťové infrastruktury založené na modelu **TCP/IP**. Hlavními přednostmi nastavových firewallů jsou jejich operační rychlost (*Speed*) a pružnost konfigurace (*Flexibility*). Naopak jejich slabinou je jejich neschopnost zabránit útokům, které využívají potenciálně zranitelná místa konkrétních aplikací (tyto firewallly totiž neumožňují kontrolu dat na vyšších (aplikačních) vrstvách referenčního modulu **RM-OSI** (*Reference Model of Open System Interconnection*)).

Tabulka 1 – příklady sad pravidel pro nestavový (paketový) firewall – tabulka převzata z [9]

	Zdrojová adresa	Zdrojový port	Cílová adresa	Cílový port	Akce	Popis
1	libovolná	libovolný	192.168.1.0	> 1023	povoleno	Pravidlo povolující návrat TCP spojení do interní subsítě
2	192.168.1.1	libovolný	libovolná	libovolný	zakázáno	Chrání systém firewallu před přímým připojením
3	libovolná	libovolný	192.168.1.1	libovolný	zakázáno	Omezuje přímý přístup externích uživatelů k systému firewallu
4	192.168.1.0	libovolný	libovolná	libovolný	povoleno	Interní uživatelé mohou přistupovat k externím serverům
5	libovolná	libovolný	192.168.1.2	SMTP	povoleno	Umožňuje externím uživatelům zasílat e-maily
6	libovolná	libovolný	192.168.1.3	HTTP	povoleno	Povoluje externím uživatelům přístup na WWW server
7	libovolná	libovolný	libovolná	libovolný	zakázáno	Vše, co není v předcházejících případech povoleno, je explicitně zakázáno

Stavový firewall (*Stateful Packet Inspection Firewall*) umožňuje tzv. dynamické filtrování paketů. Jedná se tedy o zařízení, které monitoruje stav aktivních připojení a následně pak používá tyto informace pro rozhodnutí, které síťové pakety mohou přes firewall projít, a které naopak ne. Tyto firewally již umožňují analýzu paketů až po úroveň aplikační vrstvy modelu **RM-OSI**. Zaznamenáním informací o konkrétní relaci jakými jsou např. IP adresa a čísla portů, pak může dynamické filtrování paketů realizovat mnohem vyšší míru zabezpečení a prověřováním určitých hodnot v záhlaví přenášených paketů sledovat stav jednotlivých připojení po určité vymezenou dobu. Odchozí pakety, které očekávají určitý typ příchozích paketů, jsou firewallem sledovány a pouze ty příchozí pakety, které nesou tu správnou informaci resp. správnou odpověď na odeslaný dotaz, jsou přes firewall přeneseny. Každý nově přijatý paket je porovnáván se stavovou tabulkou firewallu tak, aby bylo možné určit, zda stav paketu není v rozporu s jeho očekávaným stavem. Tradiční stavové firewally neprověřují užitečnost obsahu dat síťových paketů a ve své podstatě ani nemají dostatečnou inteligenci pro rozlišení jednoho druhu webového provozu od druhého (např. provozu legitimní aplikace a případného útoku).

Aplikační firewall (*Proxy Firewall*) neboli aplikační brána, je poměrně novým přírůstkem mezi tradičními bezpečnostními zařízeními. Navíc však v sobě aplikační firewall kombinuje klasické stavové kontrolní technologie se schopností provádět hloubkovou kontrolu aplikací. Tato schopnost v sobě zahrnuje možnost analýzy protokolů na aplikační vrstvě, např. u protokolů **HTTP** (*Hyper Text Transfer Protocol*) a **FTP** (*File Transfer Protocol*) a monitorováním provozu

porovnávat neškodné aktivity protokolů s aktuální aktivitou daného protokolu, a tím identifikovat potenciální odchylky v jejich chování, které mohou znamenat potenciální útok. Tyto vlastnosti umožňují firewallu povolit či naopak zakázat přístup aplikaci k dostupným síťovým prostředkům v závislosti na tom, jakým způsobem se aplikace chová v síti.

Firewall nové generace **NGFW** (*Next-Generation FireWall*) je integrovanou síťovou platformou, která kombinuje tradiční firewall s dalšími síťovými zařízeními s filtrovací funkcionalitou. Do kategorie firewallů nové generace patří např. aplikační firewally využívající přímou hloubkovou analýzu paketů **DPI** (*Deep Packet Inspection*), systémy prevence potenciálních útoků **IPS** (*Intrusion Prevention System*) a/nebo další techniky jakými jsou např. odposlechy **SSL** (*Secure Socket Layer*) a **SSH** (*Secure SHell*), filtrování webových stránek (*Website Filtering*), správa kvality služeb **QoS** (*Quality of Service*) a šířky pásma (*Bandwidth Management*), antivirovou kontrolu a integraci řešení třetích stran (např. *Active Directory*) [10]. Ve skutečnosti tyto techniky představují sjednocený koncept správy hrozeb **UTM** (*Unified Threat Management*). Hlavní nevýhodou firewallů **NGFW** je, že často využívají samostatné interní moduly pro zajištění jednotlivých bezpečnostních funkcí. To znamená, že analyzovaný paket pak může být podroben několikanásobnému procesu posuzování, aby bylo možné určit jeho oprávnění vstupu do dané sítě. Tento vícenásobný systém zpracování však zvyšuje dobu zpoždění, a následně tak může zcela zásadním a negativním způsobem ovlivnit výkonnost celé sítě.

### 3.3 Systémy detekce narušení IDS (Intrusion Detection Systems)



$E=mc^2$

Systém detekce narušení **IDS** (*Intrusion Detection System*) je dalším ochranným opatřením, které pomáhá s odražením počítačového útoku monitorováním síťového provozu, využitím databáze signatur a pomocí heuristické analýzy označující podezřelé vzorky, které mohou signalizovat síťový nebo systémový útok s úmyslem průniku do systému nebo alespoň jeho ohrožení.

Systémy **IDS** používané pro detekci útoků mohou být softwarové i hardwarové. Zařízení **IDS** jsou využívána pro monitorování připojení a detekci již zahájeného útoku. Některé systémy **IDS** pouze monitorují provoz a upozorňují na útok, zatímco jiné se snaží útok zablokovat. Funkci systému **IDS** lze porovnat s videokamerou a snímačem pohybu; které detekují neoprávněné nebo podezřelé aktivity a následně mohou zcela automaticky varovat ochranku, aby této aktivitě zamezila.



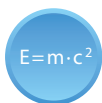
Systémy **IDS** se od firewallu liší především tím, že firewall hledá primárně průniky, které následně eliminuje. Firewall omezuje přístup mezi sítěmi, aby zabránil případnému průniku, ale nesignalizuje útok, který se odehrává uvnitř sítě. Systém **IDS** naopak vyhodnocuje podezření na průnik do sítě a poté, co k němu dojde, spustí alarm. Systém **IDS** je schopen zaměřit i útoky vzniklé uvnitř systému.

Systém **IDS** využívá tzv. ohodnocení zranitelnosti systému (někdy bývá tento proces označován jako skenování (*Scanning*)), což je technologie vyvinutá k posouzení bezpečnosti počítačového systému nebo sítě. Funkce detekce narušení v sobě zahrnuje sledování a analýzu uživatelských i systémových aktivit, analýzu konfigurace systému a jeho zranitelnosti, vyhodnocovací systém a integritu souborů, analýzu vzorků neobvyklých aktivit a sledování porušení zásad uživatele. Existuje několik různých způsobů, jak lze dělit systémy **IDS**:

- Detekce narušení (*Misuse Detection*) vs. detekce odchylek (anomálií) (*Anomaly Detection*)
  - Detekce narušení – systém **IDS** analyzuje informace, které shromažďuje a porovnává je s rozsáhlou databází signatur útoků. V podstatě systém **IDS** vyhledává konkrétní útok, který již byl zdokumentován. Technika detekce narušení založená na signatuře útoku spočívá ve vyhledávání signatur (typické posloupnosti znaků pro útok) ve všech relacích realizovaných v síti. Tento způsob detekce umožňuje odhalit útoky na úrovni aplikací, a to i přesto, že odpovídají standardům protokolové komunikace mezi aplikacemi; jelikož je doplněn o proces dekódování protokolové komunikace mezi aplikacemi. Podobně jako u antivirových systémů, software pro detekci narušení je tak dobrý, jak rozsáhlá je databáze signatur známých útoků, která je využívána pro porovnávání jednotlivých paketů mezi sebou. To znamená, že je nutné udržovat a často aktualizovat databázi signatur útoků na zařízeních, jejichž činnost je na správné funkci této techniky založena.

- Detekce odchylek (anomálií) – správce systému definuje základní resp. normální stav odpovídající běžnému zatížení síťového provozu, určí jeho členění, stanoví užívané protokoly a typickou velikost paketů. Detektor odchylek (anomálií) monitoruje jednotlivé síťové segmenty, porovnává jejich stav s normálním stavem a snaží se vyhledat a následně označit nalezené odchylky (anomálie).
- Síťově založené systémy (*Network-based*) vs. klientsky založené systémy (*Host-based*)
  - Síťově založené systémy **NIDS** – jednotlivé pakety procházející sítí jsou analyzovány. Systém **NIDS** však dokáže detekovat i pakety se škodlivým obsahem, které jsou navrženy tak, aby je případný firewall neobjevil díky svým jednoduchým filtrovacím pravidlům.
  - Klientsky založené systémy **HIDS** – tyto systémy **IDS** prověřují veškerou aktivitu na každém jednotlivém počítači nebo hostiteli.

## 3.4 Virtuální privátní síť VPN (Virtual Private Network)



**VPN** je zkratkou používanou pro „virtuální privátní síť“. Virtuální privátní síť **VPN** jsou síťovou technologií, která umožňuje využití veřejných datových sítí jako je Internet pro soukromou komunikaci vytvořením zabezpečeného (šifrovaného) připojení k síti.

Virtuální privátní síť **VPN** jsou často využívány pro bezpečné připojení vzdálených uživatelů k jejich soukromé síti, a tímto způsobem je tak možné rozšiřovat infrastrukturu intranetů v celosvětovém měřítku. Jinými slovy, virtuální privátní síť **VPN** umožňují výměnu dat mezi dvěma počítači pomocí směrovací infrastruktury poskytované sdílenými nebo veřejnými sítěmi (jako je např. Internet) a to takovým způsobem, že emulují vlastnosti privátní linky typu bod-bod (*Point-to-Point*). Zabezpečené připojení se pak uživateli jeví jakoprivátní komunikační síť, a to navzdory skutečnosti, že je tato komunikace realizována prostřednictvím veřejné sítě. Z tohoto principu je právě odvozen název virtuální privátní síť.

Existuje několik důvodů pro budování sítí **VPN**, ale společným jmenovatelem je, že všichni uživatelé sdílejí požadavek na „virtualizaci“ určitého objemu podnikové komunikace – jinými slovy, aby určitý objem komunikace (nebo i veškerá komunikace) byla ve své podstatě „neviditelná“ pro externí pozorovatele, a přitom využívala výhod a efektivitu veřejné komunikační infrastruktury. Mezi společně využívané vlastnosti sítí **VPN** patří – zabezpečený vzdálený přístup k podnikovým prostředkům prostřednictvím Internetu a vzájemné propojení sítí přes Internet. Řešení sítí **VPN** by měla poskytovat především tyto bezpečnostní služby:

- **Ověření uživatele (*User Authentication*)** – Síť **VPN** umožňují přístup pouze oprávněným uživatelům; z tohoto důvodu je důležité vždy ověřit jejich totožnost, resp. identitu. Kromě toho by měly síť **VPN** poskytovat a uchovávat kontrolní záznamy o provedených auditech.
- **Šifrování dat (*Data Encryption*)** – Data, která jsou přenášena prostřednictvím veřejných sítí, nesmí být přístupná a dostupná neoprávněným uživatelům.
- **Správu klíčů (*Key Management*)** – Před vlastním šifrováním dat je nutné, aby uživatelé nejprve definovali a nastavili klíčové parametry pro šifrování (algoritmy, klíče, ...).

## **4** Řešení pro zabezpečení sítí

Síť jako celek je tak bezpečná jak bezpečný je její nejslabší resp. nejméně zabezpečený článek. Vedle využití metod a komponent popsaných v předchozích kapitolách, je níže podrobněji popsán i soubor opatření, který by měl být dodržován a uplatňován jak uživateli, tak správci sítí, aby bylo dosaženo zvýšení bezpečnosti daného systému či sítě.

## 4.1 Využití bezpečných autentizačních metod

Existuje celá řada podniků a institucí, které pro účel a funkci svých systémů a sítí využívají „robustní ověřovací, resp. autentizační metody“, a to zejména u tzv. „online“ transakcí, jejichž součástí jsou i platební služby (*Payment Services*). Definovat pojem „robustní autentizace“ lze několika různými způsoby. Někteří autoři se odkazují na princip autentizačních metod založených na tzv. multifaktorovém ověření, jež vyžaduje využití nejméně dvou ale i více faktorů z následujících tří kategorií (vědomost (*Knowledge*), vlastnictví (*Possession*) a existence (*Inherence*)), uvedené již v kapitole 1.3. Jiní autoři (A. J. Menezes, P. C. van Oorschot a S. A. Vanstone) berou do úvahy i další okolnosti, mimo jiné například tu skutečnost, že metody robustní autentizace mohou vyžadovat součinnost s bezpečnostním protokolem typu výzva-odpověď (*Challenge&Response*), blíže vysvětleno v [11]. V každém případě však robustní a odolný autentizační protokol nemůže být založen na pouhém přenosu hesla.



Je důležité vědět, že spolehlivost autentizace je ovlivněna nejen počtem použitých faktorů, ale také jakým způsobem jsou tyto faktory do systému implementovány. Volbou pravidel pro ověření v každé kategorii významně ovlivníme míru bezpečnosti každého z faktorů. Nedostatečná nebo zcela chybějící pravidla pro hesla, mohou mít například za následek vytvoření hesla pro tzv. hosta (*Guest*), jehož existence úplně znehodnotí smysl systému zabezpečení heslem. Mezi osvědčené postupy týkající se hesel patří požadavek na využívání „silných“ hesel, která jsou pravidelně aktualizována. Nedbalá pravidla a jejich nevhodná implementace jsou častou příčinou oslabení bezpečnosti; z toho plyne, že vylepšení pravidel může zlepšit bezpečnost jednotlivých faktorů, a tím i bezpečnost multifaktorového autentizačního systému jako celku.

V případě využívání hesel je zcela nezbytné vytvořit kvalitní zásady pro hesla, aby byl vyloučen jednoduchý odhad správného hesla nebo jeho snadné prolomení (*Cracking*). Možnost snadného prolomení hesla usnadňuje hackerům odhad správného hesla. Dnes je bohužel dostupná široká paleta programů a nástrojů na prolamování hesel, které jsou využitelné i průměrným uživatelem, který ani nemusí mít žádné speciální znalosti. Bohužel i dnes existuje stále poměrně velké množství uživatelů, kteří preferují snadno zapamatovatelná hesla před těmi obtížně prolomitelnými.

Prolamování hesla je procesem vedoucím k získání hesla tak, aby bylo možné neoprávněně vstoupit do systému nebo účtu. Hesla mohou být prolomena mnoha různými způsoby. Nejjednodušším je využití seznamu hesel, resp. slovníku hesel, který umožňuje prolomení hesla tzv. „hrubou silou“. Tyto programy porovnávají seznamy slov nebo jejich charakteristické kombinace s hledaným heslem, dokud nenaleznou shodu. Z výše uvedeného plyne, že jako heslo bychom neměli používat slova z těchto slovníků, vlastní jména nebo cizí slova.

Nástroje na prolomení hesla však mohou být využity i pro účely zabezpečení, pokud si totiž díky nim uživatelé volí bezpečnější hesla. Správci systémů je také mohou využít k testování síly uživatelských hesel, a následně pak mohou informovat uživatele s nevyhovujícím heslem.



Dalším způsobem prolamování hesel útočníky je tzv. sociální inženýrství. Řada uživatelů totiž vytváří hesla, která obsahují jejich osobní údaje, a heslo je tak často možné odhadnout i jen s minimem znalostí údajů o uživateli. Hesla by tedy neměla obsahovat vaše osobní údaje.

Mnoho uživatelů si také ukládá svá hesla do počítačových souborů. Abychom omezili riziko jejich odhalení, je vhodné tyto soubory šifrovat. Toto doporučení se však netýká jen souborů s hesly, ale i ostatních souborů, kde jsou uloženy jakékoliv citlivé údaje.

## 4.2 Vylepšené nastavení operačního systému



---

Vylepšeným nastavením operačního systému **OS** (*Operating System*) je chápán proces jeho vlastní reinstalace a bezpečné konfigurace, průběžné aktualizace, vytváření pravidel a zásad, které usnadňují řízení a bezpečnou správu systému a odstraňování nadbytečných aplikací a služeb.

---

Vylepšit nastavení operačního systému **OS** znamená dělat **OS** bezpečnějším. To je obvykle realizováno tím, že z počítače odstraníme všechny nepotřebné programy a nástroje, aplikujeme nejnovější opravy systému, odstraníme nepoužívané soubory a uzamkneme uživatelské účty. Doplnkové programy často poskytují uživateli řadu zajímavých a užitečných funkcí, ale taktéž mohou, často i zcela nechtěně, poskytovat i tzv. „zadní vrátka“ pro vstup do systému, a proto je vhodné je v průběhu optimalizace nastavení operačního systému odstranit.

I když je důležité průběžně odebírat nepoužívané aplikace, deaktivovat nadbytečné služby, instalovat různé opravné, aktualizací a servisní balíčky, přesto se nejedná o jediný způsob, jak vylepšit nastavení operačního systému. Administrátorská oprávnění by měla být užívána s rozumem, tj. tam, kde je to nezbytně nutné, zásady zabezpečení by měly být definovány tak, aby byly v souladu s pravidly daného podniku či instituce.

Na Internetu lze najít celou řadu vylepšených nastavení a bezpečnostních doporučení pro nejvíce rozšířené operační systémy. Tato vylepšená nastavení mohou být po zralé úvaze následně aplikována i správci systémů. Nastavení operačních systémů firem Macintosh (MacOS) a Microsoft (OS Windows) je reálně možné, častěji však bývá realizováno na pracovních stanicích s OS Windows, jelikož je u nich vyšší míra pravděpodobnosti ohrožení jejich zabezpečení.

## 4.3 Fyzická bezpečnost

Zajištění fyzického zabezpečení síťového prostředí je prvním krokem pro zajištění kontroly nad přístupem k citlivým datům a systémovým souborům. To je ale pouze jedna část promyšleného plánu zabezpečení. V současné době má tato část zabezpečení snad ještě větší význam než v minulosti, jelikož současné sítě jsou založeny na mnohem širší základně dostupných síťových prostředků a služeb. Střední nebo velká síť může mít až několik desítek i stovek přístupových bodů, VPN serverů a časově neomezenou vyhrazenou konektivitu k síti Internet. Dokonce i v případě malých sítí lze dnes předpokládat, že budou po jistý, časově vymezený interval, připojeny k síti Internet.

Virtuální útočníci nikdy nevyužívají přímo cílový počítač nebo cílovou síť. Mohou k těmto systémům přistupovat třeba jen přes ulici, ale klidně i přes polovinu světa, přičemž mohou způsobit stejné škody jako zloději, kteří proniknou do ústředí firmy s cílem zničit nebo ukrást citlivá data – virtuální útočníky je však mnohem složitější vypátrat. Zabezpečení fyzické kontroly přístupu k tzv. „venkovnímu perimetru“ znamená:

- a) Zajištění kontroly fyzického přístupu k serverům.
- b) Zajištění kontroly fyzického přístupu k pracovním stanicím v síti.
- c) Zajištění kontroly fyzického přístupu k síťovým zařízením.
- d) Zajištění kontroly fyzického přístupu ke kabeláži.
- e) Řešení zabezpečení na úrovni bezdrátových sítí.
- f) Řešení zabezpečení na úrovni přenosných zařízení (notebooky, tablety, apod.).
- g) Zabývat se bezpečnostními riziky spojenými s povolením tisku dat.
- h) Zabývat se bezpečnostními riziky spojenými s přenosem dat na externích datových nosičích (USB flash disky, externí pevné disky, CD a DVD nosiče a další přenosná datová média).

## 5 Bezpečnost v mobilních sítích

Mobilní zařízení dnes často zcela nahrazují nebo vhodně doplňují portfolio nabízených funkcí osobních počítačů, a to jak doma, tak na pracovišti. Rapidní nárůst počtu chytrých telefonů a tabletů a jejich masivní rozšíření v průběhu posledních dvou let logicky vedl i k nevyhnutelnému nárůstu počtu cílených útoků na tento typ zařízení. Navíc některá neregulovaná úložiště aplikací (*App Markets, App Stores*) zapříčinila nárůst problémů spojených s malwarem i u těchto zařízení. Tvůrci mobilního malwaru jsou si dobře vědomi, že nejlepším způsobem jak ohrozit a případně úspěšně napadnout co nejvíce mobilních zařízení na konkrétní platformě, je zaútočit právě na jeho centrální úložiště s aplikacemi.

Existuje mnoho odlišných způsobů, jakými může hacker profitovat z útoku na mobilní zařízení. Některé z nich známe již z oblasti tradičních osobních počítačů, např. ransomware, botnet a krádeže dat. Díky povaze mobilních zařízení je i tento typ zařízení potenciálně ohrožen těmito typy útoků. Hlavní riziko však spočívá především v jejich mobilitě, což často vede k jejich fyzické ztrátě, a tím ke ztrátě uložených dat, pokud nejsou data určitým způsobem řádně zajištěna nebo šifrována.



---

Rozvoj aplikací pro osobní nebo obchodní komunikaci otevírá nové možnosti pro další typy útoků, hlavně v oblasti sociálního inženýrství a útoků zaměřených na získávání důvěrných dat. Adresář s uloženými sociálními kontakty a další osobní údaje jsou pak velmi cennými informacemi pro útočníky různého druhu. Mobilní a webové aplikace umožňující správu podnikových uživatelů pomáhají velmi výrazně toto riziko zmírnit.

---

V současnosti představuje dynamický rozvoj mobilního bankovníctví další z řady potenciálních rizik pro jejich uživatele. Výkonná mobilní zařízení jsou často terčem malwaru, který je navržen tak, aby dokázal odcizit nejen citlivá data, resp. peníze, jelikož tato zařízení umožňují jednoduchou realizaci finančních transakcí i na cestách. Cílem útočníka je získat a odcizit přihlašovací údaje k těmto aplikacím nebo přímo ukradnout určitý finanční obnos. Právě proto je ochrana chytrého telefonu před škodlivým softwarem, např. před softwarem zaznamenávajícím stisknuté klávesy (*Keylogger*), základním principem bezpečného mobilního bankovníctví.

Bezpečnostní experti varují před riziky mobilního malwaru již několik let. Skutečnost, že se doposud neuskutečnily rozsáhlejší útoky, narušují důvěryhodnost předchozího tvrzení a mnoho uživatelů jej tak vůbec nebere vážně a nechová se ostražitě. Zvyšování počtu mobilních zařízení a s tím spojený vznik nových mobilních malwarových útoků naopak zvyšuje pravděpodobnost, že rozsáhlé mobilní malwarové útoky budou v dnešním světě stále častější.

Společnost Kaspersky v Berminghamu uvedla: „Jelikož spotřebitelé a jednotlivé podniky využívají pro stále větší procento svých každodenních aktivit mobilní zařízení, budou kyberzločinci klást mnohem větší důraz na napadání těchto mobilních platform – konkrétně jde o platformu Android a zařízení se systémem iOS od fy. Apple (tzv. jailbreak)“.