# Základy počítačové bezpečnosti

1. rozdělení rizik
   1. Aktivní:
      1. virová rizika
      2. rizika spyware
      3. rootkity
      4. hacking/cracking
   2. Pasivní:
      1. spam
      2. hoax
      3. phishing
      4. krádež identity
      5. sociální marketing
   3. Nepřímá rizika (rizika nesouvisející přímo s konkrétním počítačem)
      1. Skimming
      2. Information diving
      3. Pretexting
2. Prevence
3. Řešení krizových stavů

**Virová rizika -** patří mezi aktivní rizika

Dnes nejčetnější a nejvíce medializované. Princip virového útoku spočívá v nepozorovaném vniknutí do počítače na uživatelův podnět (v poslední době i bez něj, respektive postačí například pouhá návštěva nakažené stránky). Následně se virus pokusí a sebereplikaci a šíření. Může, ale nemusí provádět přímé škodlivé akce.

Mezi primární škody způsobené viry patří:

* smazání nebo poškozování souborů
* vypouštění dalšího viru, případně rootkitu, spyware
* uvedení operačního systému do nestandardního stavu
* zařazování obětí do seznamu spam listů
* využití napadeného počítače jako zombie pro další útoky
* otvírání vstupů pro případné další škodlivé akce
* krádež dat a informací o uživateli

Viry se šíří v současné době nejčastěji formou webových stránek, nebo emailu, již velmi zřídka prostřednictvím vyměnitelných médií (CD,FDD,DVD). V současnosti je snahou virů se maximálně maskovat a provádět skrytou činnost (některé uváděné škodlivé akce jakými jsou např. mazání souborů, nebo blokování funkcí operačního systému, patří dnes mezi ty jen zřídka vídané). Více se prosazují viry, které mají kriminální podtext.

**Rizika spyware -** patří mezi aktivní rizika

Hlavním principem spyware je provádění výzvědné činnosti v počítači a poskytování takto získaných údajů útočníkovi. Útočník nemusí být žádný hacker, ale jedná se například o běžnou praxi používanou pro distribuci reklam a zpětné zjišťování tržního chování oběti. (sociální marketing viz dále). Spyware může být virem, ale nemusí, většinou nemá schopnost sebereplikace.

Spyware může pocházet buď z emailů, webových stránek, ale nejčastěji ve formě přídavných aplikací. V důsledku působení spyware dochází k masivnímu narušení soukromí a pokud oběť o přítomnosti spyware nemá ponětí, může znamenat poměrně velký problém.

**Rootkity**

Patří mezi aktivní rizika. Rootkit je velmi zvláštní formou viru, nebo spyware. Je to program, který se ukrývá v jádře operačního systému. Jelikož se mu podaří dostat se do takto hlubokých částí operačního systému je obvykle prakticky nezjistitelný pomocí běžných antivirových systémů. Jsou na to potřeba specializované nástroje. V minulosti byl využit tento typ software i v komerční sféře (kauza Sony a DRM). Je to jeden z nejzákeřnějších obecných útoků na počítače. Nicméně naprogramování takové aplikace je nesmírně obtížné a zvládne to jenom málokdo, navíc jsou rootkity obvykle vázány na konkrétní platformu (například na x64, nebo jen x86, nebo jen powerpc atd.), což poměrně značně omezuje jejich masivní rozšíření. Pokud se ale Rootkitu do počítače podaří dostat, je jeho likvidace obvykle spojena s přeinstalací operačního systému.

**SPAM, HOAX**

Patří mezi pasivní rizika.

V zásadě se nejedná o škodlivé jevy v pravém slova smyslu, pravý spam, nebo hoax nejsou programy a nejsou tedy samy o sobě schopné způsobit škodu.

**SPAM**

je jednoduše řečeno nevyžádaný email, původně vzniknul jako jeden z marketingových nástrojů s cílem oběť (potencionálního zákazníka) upozornit na aktuální nabídky firem atd. V současné době je hlavním cílem spamu zahušťovat internetovou komunikaci tak, aby vznikaly nepříjemnosti spojené s přetěžováním emailových serverů. Tyto výpadky pak mohou být použity pro eventuální další útok. V současné době je SPAM jedním z největších strašáků novodobého internetu.

Zákeřnost spamů ač pasivního rizika, spočívá ve značném přetěžování emailové infrastruktury (SMTP servery). Je dokázáno, že jen zhruba 10-30% veškerých emailů lze považovat za reálné, skutečné a vyžádané. Právě SPAM může za to, že je potřeba budovat poměrně sofistikované aplikace a systémy, které poměrně značně vytěžují hardware a tím i značně prodražují celou infrastrukturu firmy.

Základním rysem spamů, díky čemuž se s nimi velmi obtížně bojuje, je jejich náhodnost, nebo nahodilost.

Spamy jsou navíc velmi oblíbené jako přenosový prostředek pro viry, nebo spyware.

Spamy nemají snadno dohledatelného odesílatele.

Kritickým problémem (čehož spamy využívají) je obecný princip SMTP komunikace využívající zcela neautorizovaný přístup mailserverů mezi sebou (anonymní ověřování). Je díky tomu velmi obtížené (a hlavně nákladné) zjišťovat původ každého emailu.

To, co současné počítače paradoxně poněkud zachraňuje, je velmi nízká výkonnost poštovních systému, co se týče generování datového zatížení na WAN linkách (internetu). SMTP je protokol obecně značně pomalý, díky čemuž nelze zcela přehltit veškerá datová spojení. Do budoucna by problém spamů mělo řešit z větší části IPv6, které více dbá na identifikaci konkrétního počítače v síti a tím lze následně kontrolovat, kdo je skutečným odesílatelem příslušného emailu.

**HOAX**

Vychází částečně z principu spamu, je to také emailová zpráva, také s nevyžádaným obsahem, hlavní úlohou hoaxu je ale uvedení v omyl a následná reakce oběti na „varování“ obsažená v hoaxu. Zjednodušeně řečeno je možné hoax označit za poplašnou zprávu. Klíčovou vlastností Hoaxu je především donucení oběti k dalšímu šíření (rozeslání svým kamarádům). Dá se říct, že naplňuje podstatu pasivního viru. Hlavním účelem hoaxu je zapůsobit na psychologii člověka, na jeho city a emoce a pod jejich vlivem ho donutit k činnosti, kterou by normálně neprováděl.

V současné době velmi oblíbené a pokud uživatel podlehne, pak mohou mít phisingové útoky poměrně velký úspěch.

Hlavní nebezpečnost phisingu je v jejich narůstající rafinovanosti, kdy i člověk poměrně vycvičený a obezřetný může díky současné velmi uspěchané době, podlehnout.

**Hacking**

Ne příliš rozšířená metoda určená pro napadání běžných počítačů, naopak poměrně rozšířená metoda u některých důležitých, nebo zajímavých systémů. Hacker používá různých technik k nalezení cesty do vyhlédnutého počítače. Cílem je ovládnutí počítače a v určitých případech i zisk dat, které se na něm nacházejí. Hacker se dle naší současně platné legislativy dopouští trestného činu, nejčastěji pak neoprávněné nakládání s informacemi, ale i podvod, krádež atd. Hacking mívá také často záměrně kriminální podtext.

Vedle termínu hacking se uvádí i termín cracking. Rozdíl je, že cracker napadá systém z kriminálních důvodů. Naproti tomu hacker se do počítačů nabourává buď ze zvědavosti, nebo z důvodů určitého testu bezpečnosti atd. Nicméně z hlediska práva a obecně z hlediska určité síťové etikety, není mezi hackerem a crackerem žádný rozdíl. Je to podobné, jako v případě, že Vám auto poškrábe kdosi proto, aby vyzkoušel, zda je lak dost odolný (aby upozornil výrobce, že lak není dost dobrý, nebo naopak dobrý je), nebo když Vám někdo poškrábe lak na autě proto, že zrovna chtěl, nebo že si to někdo objednal.

**Krádež identity**

Je pasivním rizikem a bohužel se lze s tímto rizikem setkávat stále častěji. Pomocí různých nepřímých metod může útočník vytvořit pro své účely kompletní profil identity oběti. S tou pak může v zásadě libovolně nakládat. Oběti může způsobit nenahraditelné škody a sám přitom zůstat zcela neviditelný. Pohnutky pro takové jednání jsou vždy kriminální, ale mají různé podtexty. Může se jednat jak o ekonomický zájem, tak i o např. tzv. kyberšikanu, případně přímo o stalking. Útočník potřebuje získat maximální množství dat proto, aby mohl své už viditelné útoky provádět efektivně a způsobit co možná největší újmu své oběti.

**Sociální marketing**

Nejedná se o kriminální činnost. Přesto jí zahrnujeme do rizik. Sociální marketing funguje na principu sledování činností uživatele a v úpravě reklamních sdělení podle způsobu chování. Problém je, že riziko social marketing technik si jen málo lidí uvědomuje a proto je velmi účinný. Pro představu je nejlepší navštívit několik úzce profilovaných specializovaných stránek a následně zavítat na Youtube. Jaké překvapení, že reklama bude zaměřena přesně ve smyslu navštívených odkazů. Nefunguje to naštěstí ve 100% případů, ale je potřeba si na to dávat pozor. Protože cílenému marketingu se velmi, velmi těžko odolává.

**Nepřímá rizika**

Nemají souvislost přímo s jedním počítačem, ale obecně se jedná o rizika, která hrozí z používání technologií, které počítače využívají.

**Skimming** – pomocí technických prostředků dochází k odpozorování tajných privátních údajů (například PIN kódů k platební kartě, nebo hesla do počítače). Nejčastěji se dnes používají různá zobrazovací zařízení typu kamer, scannerů, ale můžeme se setkat i s tzv. keyloggerem. Je to nebezpečné především proto, že se skimming používá na místech, kde by to člověk nečekal. Bránit se proti skimmingu lze jen pomocí důsledné kontroly příslušného zařízení (např. kamerová kontrola bankomatu, technická kontrola klávesnic, sledování podezřelého chování atd.)

**Information diving** – spočívá v pokusech restaurovat z různých druhů médií data tak, aby bylo možné získat cizí data pro vlastní potřebu. Může a nemusí mít kriminální podtext

**Pretexting** – doslova zneužití vymyšlených scénářů k podvodu (například podvodnému vylákání přihlašovacích údajů)

**Prevence**

Nejlepší prevencí je především opatrnost a to vždy a všude. Čirou opatrností se ochráníme před 75% všech útoků. Mezi základní pravidla patří například obezřetné otevírání emailových zpráv, omezení prohlížení stránek s pochybným obsahem, zdravá nedůvěra k obsahu různých sdělení. Nejlépe se to dá vystihnout souslovím: „Být vždy ve střehu“

Pro prevenci lze kromě vlastního rozumu použít i několik speciálních nástrojů, které nám pomáhají těmto rizikům odolávat.

1. **Antivirové programy** – zavedená skupina produktů s dlouholetou tradicí, mezi základní úkoly antiviru patří detekce i prevence proti virům na všech možných úrovních operačního systému a aplikací (rezidentní ochrana, nízkoúrovňová ochrana, ochrana emailových klientů, ochrana souborů). Jedná se z 90% o programy postavené na definičním principu. Specializovanou funkcí je tzv. heuristika, což je prevenční metoda vyhledávající potencionální rizika, která nesplňují definiční pravidla. V současnosti se používá ještě tzv. telemetrie, kdy data získaná z heuristických analýz jsou zasílána antivirovým společnostem, které pak na základě heuristik provádějí úpravu definic.

Příklady: ESET Antivirus, Symantec Antivirus, AVIRA, F-Secure, Panda, CA Antivirus atd.

1. **Antispyware programy** – fungují na podobném principu jako antiviry, jsou ale stoprocentně závislé na definicích. Dnes se obvykle tyto nástroje integrují do antivirů.
2. **Antispam nástroje**

Dají se rozdělit do dvou základních skupin. Buď jsou založené na principu definic, nebo jsou postavené na principu Bayesovského filtru, tedy filtru postaveného na bázi samostudia, dle chování uživatele určuje, zda email odpovídá chování uživatele, či nikoliv. Nejvhodnější praktikou je používání obou dvou typů. Mezi další metody boje proti spamu patří různé databáze spamming serverů (black listy), nebo i jednoduché DNS záznamy (SPF). Největším problémem je v současné době především to, jak daný email správně označkovat, zda se jedná, nebo nejedná o spam. Je zde příliš mnoho proměnných. Velkou komplikací při boji se spamem jsou i různé jazyky, znakové sady, které značně ztěžují korektní detekci. Velmi oblíbeným mezi spammery je i jednoduchý obrázek, který je antispam nástroji poměrně obtížně detekovatelný. V současné době jsou do všech emailových klientů integrovány antispam nástroje.

Příklady: Cloudmark, GFI MailSecurity, Spam Assasin, Spamhaus, DNS BL

1. **Antiphishingové filtry** – fungují často na bázi definic, ale také za použítí předdefinovaných šablon chování phishingového útoku. Integrují se dnes do internetových prohlížečů, nebo emailových klientů. Jejich efektivita je ovšem často sporná.
2. **Aktualizace operačního systému a příslušných aplikací** – výrobci software často reagují na některé zveřejněné hrozby formou vydaní aktualizované verze, je proto nutné tyto verze instalovat a tím snižovat možnost eventuálního rizika. Nejdůležitější jsou opravy na bázi operačního systému. Ale je potřeba brát v potaz i aktualizace obvyklých internetových komponent jako je např. Flash, nebo Java Runtime (viz Apple útok z minulého týdne)
3. **Hardwarové komponenty** v podobě stavových firewallu, routerů, vhodné především k obraně před elementárním typem útoků. Nejpokročilejšími hardware zařízeními jsou především tzv. UTM (unified Threat management)

Současnost je především ve znamení komplexních řešení na bázi hardware i software. Mezi nejznámější výrobce bezpečnostních řešení patří například firmy Symantec, nebo Computer Associates. Mezi výrobci hardware má největší bezpečnostní prestiž firma Cisco. V našich končinách jsou také oblíbená řešení firmy Mikrotik.

Ve firemním prostředí se setkáváme obvykle s celým spektrem různých bezpečnostních prvků. Zde se navíc bezpečnost musí řešit na principu tzv. interní a externí bezpečnosti. To je poměrně značný rozdíl proti běžným domácím počítačům, kde řešíte především hrozby přicházející z internetu.

Externí bezpečnost ve firmách je obvykle postavena na kombinaci routerů, firewallů, UTM zařízení a tzv. IPS systémech.

Běžně se staví proti internetu hradba skládající se z routeru (nebo routerů), aplikačního firewallu a mezi nimi je tzv. IPS. IPS = Intrusion prevention system – je speciální zařízení, nebo software, který sleduje provoz mezi dvěma i více uzly a buď na základě definic, nebo pomocí heuristiky, hledá tzv. anomálie. Anomálie pak následně hlásí, nebo přímo blokuje. IPS zařízení nepracují na IP adresách, ani na MAC adresách, ale umí fungovat přímo přes první vrstvu OSI, proto je jejich přítomnost obvykle nezjistitelná (to platí především pro sofistikované velké systémy. Nevýhodou IPS je především jejich cena, ale hlavně obrovská složitost.

Příklady bezpečnostních prvků externí bezpečnosti: IPS=Snort, Tippingpoint, McAfee, Firewally: Cisco, Fortinet, H3C, Zyxel (levnější), Baracuda, Checkpoint. Existují i software varianty firewallů = Microsoft Threat Management Gateway, Kerio Control

Routery – Cisco, H3C, Huawei, Nortel.

Interní bezpečnost ve firmách – hlavním důvodem, proč toto řešit jsou především:

1. Hosté ve firmě (kteří mohou přijít i s nekalými úmysly)
2. Interní zaměstnanci
3. Rizika pocházející z počítačů pohybujících se mimo hlavní LAN síť (notebooky, netbooky atd.)

*Jak se to řeší:*

Na fyzické úrovni můžeme řešit bezpečnost pomocí ochrany přípojných míst (například kryty zásuvek na klíč, nebo na čip, servery v racku pod zámkem a elektronickým bezpečnostním systémem tzv. EZS).

Na úrovni sítě se dnes především skloňuje tzv. dynamické řízení sítě, kdy po připojení fyzického konektoru dojde k bezpečnostnímu scanu celého počítače a teprve na základě vystaveného certifikátu o úrovni zabezpečení dojde k příslušnému odblokování části sítě, kam daný počítač patří. Čili zjednodušeně řečeno: Pokud nemáte na počítači aktualizovaný antivir, nebo nemáte kompletní aktualizace, nedostanete přístup k interním zdrojům firmy, jste přesměrování na síť, kde se Vám sesynchronizuje antivir a nainstalují aktualizace. Pokud jsou podmínky splněny, je Vám povolen přístup do sítě.

Naprosto zásadním je u větších firem i implementace IPS technologie (na této úrovni naprosto neskutečně nákladné řešení). Často se také implementuje tzv. SSL inspekce (čili dekódování HTTPS provozu), důvodem je nutnost hlídat např. interní patenty, aby se nedostaly do rukou konkurence. Tato věc je ovšem z hlediska práva poněkud diskutabilní.

**Řešení krizových stavů:**

Nejdůležitějším základem je neztrácet hlavu. Pokud narazíme na známky některého z rizik (chodí mi hodně spamu, internetový prohlížeč nefunguje korektně, internetové připojení chodí pomalu, nebo vůbec atd.), je důležité identifikovat alespoň základní druh útoku.

Dále by měl následovat popis jednotlivých nástrojů. (taskmgr, eventvwr, nouzový mód, analýza protokolů bezpečnostních prvků).

Neunáhlovat se. Nebláznit. Pokud se jedná o počítačovou síť, je potřeba zjistit zdroj problému a ten pokud možno co nejdříve izolovat od zbytku sítě, aby nedošlo k jejímu ohrožení.

Vždycky je dobré podívat se z nějakého nezávislého zdroje (díky bohu za GPRS) na internet a zadat příslušné symptomy.

Využívejte určitě české portály informující o virech, spamech, spyware, hoaxech atd.

Je vhodné mít po ruce záchranná DVD, pomocí kterých je možné provést relativně komfortní a rychlé čištění počítačů. Taková DVD se dají stáhnout na internetu jako ucelené bezpečnostní balíky (SysresCD, Ultimate BootCD), nebo jako specializované nástroje (obvykle od výrobců antivirů).

**Přehled nejčastějších (nekomerčních) nástrojů:**

HiJackThis – program na detekci spuštěných aplikací a aplikací v registru určených pro automatické spouštění

The Avenger – program na ničení havěti, je však nutno podotknout, že se jedná o nástroj pro odborníky (a nefunguje pod x64), funguje na principu skriptu a dokáže odstranit i neodstranitelné. Skripty však musí někdo napsat.

RSIT – aplikace pro screening systému, tj. pro detekci, umí x32 i x64

ComboFix – speciální nástroj poslední záchrany – jen pro odborníky

Zajímavý web: [www.viry.cz](http://www.viry.cz) a [www.hoax.cz](http://www.hoax.cz)