

# Sít'ová bezpečnost z pohledu uživatele

Pojmem bezpečnost rozumíme nikoliv stav, ale neustálý proces, kterým se snažíme dosáhnout a udržet uspokojivé zabezpečení. Informační a komunikační technologie se velmi rychle vyvíjí a s nimi rovněž také znalosti a nástroje potenciálních útočníků. Potenciální hrozby z pohledu uživatelů jsou jednak lidé (nedbalost či neznalost nebo úmyslné útoky, krádeže apod.) a jednak přírodní faktory (blesk, požár, záplavy apod.). V souvislosti s možným výskytem bezpečnostních incidentů (narušení bezpečnosti) je třeba mít připraven plán jejich zvládnutí (adekvátních reakcí na ně) včetně návratu do původního stavu. Z uživatelského pohledu lze bezpečnost rozčlenit na **AAA**, **správu systému** a **chování uživatelů**. Rovněž uživatele můžeme z pohledu znalostí IT či jejich rolí rozdělit na několik skupin, např.: běžný uživatel, správce systému, specialista na bezpečnost v IT. Některé následující pasáže předpokládají, že uživatel může být zároveň správcem systému. Modře zvýrazněný text v prvních dvou sekcích označuje co by měl vědět i běžný uživatel, červeně označené části textu se spíše týkají pokročilejších uživatelů (jako správců systému apod.).

## 1. AAA

### ✓ správa hesel

- hesla jsou zásadně nepřenositelná
- hesla mají být dostatečně dlouhá (odolnost proti útoku hrubou silou)
- hesla mají být dostatečně složitá (nejlépe používat kombinace malých písmen, velkých písmen, číslic a speciálních znaků - odolnost proti slovníkovému útoku)
- hesla si nikam nepoznamenávat (a když, tak jedině v zakrytované podobě jedním nejtajnějším – tj. hodně složitým heslem)
- hesla pravidelně měnit (přispívá k odolnosti zejména proti útoku hrubou silou)
- používat pro každou službu jiné heslo (aby odhalením jednoho hesla nedošlo k průniku ke všem používaným službám)
- někdy se používají místo hesel také certifikáty, jednorázová hesla (znemožnění znovupoužití zachyceného hesla útočníkem), čipové karty (nepůjčít a neztratit) a/nebo biometrické prvky (otisk prstu, oční duhovka)
- délku hesla a jeho pravidelnou změnu lze vynutit systémem
- textová (nešifrovaná) hesla pokud možno nedávat do konfiguračních souborů služeb

### ✓ správa uživatelů

- poučení běžného uživatele ohledně zacházení s heslem
- každému přidělit pouze taková práva, jaká potřebuje (ne každý potřebuje být administrátorem systému)
- vytváření skupin uživatelů (např. skupina administrátoři nebo skupina běžní uživatelé)
- přidělení oprávnění uživatelů a/nebo skupin k jednotlivým souborům (čtení, zápis, spouštění)
- vyhnout se používání testovacích účtů s jednoduchými hesly (resp. takové účty zrušit či zakázat)

### ✓ protokolování (logování) činnosti počítače

- historie přihlašování uživatelů
- chybové zprávy a změny stavů aplikací a služeb
- historie spouštění aplikací

- historie síťové komunikace
- atd.

## 2. Správa systému

### ✓ instalace systému

- vybereme takový systém, který známe (případně s kterým nám pomůže okolí)
- instalujeme pouze z důvěryhodných zdrojů SW (zakoupená originální instalační média od důvěryhodného prodejce, či podepsaný instalační repozitář na Internetu od poskytovatele systému)
- v době instalace SW jsme pokud možno odpojeni od sítě nebo alespoň za firewallem

### ✓ aktualizace a záplatování systému

- adekvátní SW licence
- záplatování systému z důvěryhodných zdrojů (žádný systém se nevyhne chybám, takže proč to útočníkům usnadňovat)
- aktualizace používaných aplikací (ani aplikace nejsou bez chyb)

### ✓ vypnutí nepotřebných služeb

- málokterý počítač běžného uživatele potřebuje mít spuštěný např. Webserver

### ✓ používání základních bezpečnostních nástrojů

- správně nastavený a aktivovaný firewall (+ případně také např. filtrování obsahu)
- spuštěný antivirový program poslední verze s aktuální databází virů
- použití nějaké detekce narušení (IDS, IPS)
- prohlížení logů (resp. detekce abnormalit v nich)

### ✓ zálohování

- pravidelné zálohování s popisem (co a kdy bylo zálohováno)
- způsoby zálohování mohou být (kromě RAID – viz níže) např. po síti či na externí média (CD, DVD, pevné disky, flash, ...)
- zálohování dat na úložiště v jiné lokalitě (ochrana nejen z důvodu např. havárie disku, ale také z důvodu ochrany před živelnou pohromou jako požár, záplava apod.)
- zálohy ochránit před neoprávněným přístupem (např. šifrováním a podepisováním tj. ochrana před vyrazením a/nebo změnou jejich obsahu)
- při vyrazení starých záloh dbát na jejich řádnou likvidaci (buď několikrát přepsat pseudonáhodnými daty nebo u přenosného média fyzicky zlikvidovat)
- zálohování napájení (UPS nebo např. používání notebooků s vlastní baterií)
- on-line zálohování disků (mirroring, RAID)
- typy záloh mohou být plné či přírůstkové

### ✓ fyzické parametry

- systém pokud možno renovovat tak, aby byl stále pod zárukou (popřípadě s možností kvalitního pozáručního servisu)
- systém postaven z kvalitních součástí splňující standardy
- v případě vyrazení systému provést důkladné přemazání paměťových médií (a případně provést jejich fyzickou likvidaci destrukcí)
- zákaz startování systému (BOOTování) z přenosných médií, případně jejich úplné blokování
- BIOS uzamykatelný heslem
- detekce otevření skříně počítače
- fyzické oddělení prostor se servery a hlavními síťovými prvky od běžných provozních

### 3. Chování uživatelů

- ✓ **www**
  - raději se vyhnout internetovým obchodům, které nepoužívají při přihlašování a/nebo zadávání osobních údajů nějaké zabezpečení (např. ssl, při jehož použití je v začátku URL uvedeno „https“ a před URL či zpravidla v dolní liště ikona zamčeného zámčičku)
  - při procházení webu mít zapnutou kontrolu stránek a sledovat (zejména při placení na internetu) ověření jednotlivých stránek (pokud je stránka v pořádku, prohlížeče zpravidla označují pozadí URL zeleně)
  - pokud možno vyhýbat se podezřelým stránkám (hazardní hry, porno apod.), nebo mít rovnou aktivní filtr tohoto typu webového obsahu
  - věnovat pozornost výstrahám prohlížeče a neodklikávat je bezmyšlenkovitě. Stránka s certifikátem, kterému prohlížeč nevěří by neměla být otevírána a už vůbec by na ní nemělo být nic vyplňováno
- ✓ **e-mail**
  - neotevírat e-maily od neznámých odesílatelů nebo jinak podezřelé e-maily (nevyžádané nabídky, e-maily v cizím jazyce apod.)
  - tam, kde je to potřeba používat elektronický podpis (viz. také PGP, CA, PKI)
  - bezhlavě nepřeposílat (např. různé řetězové e-maily, falešné poplachy apod.)
- ✓ **citlivé údaje**
  - vůbec nikomu nikdy žádným způsobem nesdělovat vlastní přístupové heslo či pin kód
  - nikomu (neověřenému či nedůvěryhodnému) přes (nešifrovaný) e-mail nesdělovat citlivé údaje jako číslo kreditní karty apod. (ani, když vás k tomu kdokoliv pod jakoukoliv záminkou nutí – pozor na sociální inženýrství)
  - pozor na nedůvěryhodné počítače (v internetových kavárnách, studovnách apod.)
  - obezřetně zvážit, jaké údaje vystavit (či nikoliv) na sociálních sítích
  - veškerá citlivá data chránit šifrováním s dostatečně silným heslem
  - při mazání citlivých údajů toto provést důkladně, tj. např. několikanásobným přepisem náhodnými daty, neboť „mazání“ v operačním systému rozhodně nestačí
  - při ztrátě či odcizení flash paměti či klíče k certifikátu neprodleně kontaktovat správce
- ✓ **přenosná média**
  - pozor na připojování cizích (neproověřených) přenosných médií (možnost nákazy různým škodlivým kódem)
  - nejpozději při připojení prověřit antivirem
  - pokud jsou na nich citlivé údaje, tak je šifrovat s dostatečně silným heslem
  - z důvodu potenciální možnosti jejich odcizení mít jejich obsah bezpečně zálohován na jiném médiu (optimálně v jiném místě)
  - při jejich vyřazení provést jejich (několikanásobné) přemazání náhodnými daty (a případně následně provést jejich fyzickou likvidaci destrukcí, aby je nebylo možné dále použít)
- ✓ **stahování dat**
  - pozor na tzv. trojské koně (tj. programy, které se tváří jako užitečné a přitom obsahují nějaký škodlivý kód)
  - stahovat pouze z důvěryhodných zdrojů (existují kontrolní součty jednotlivých SW

balíků, či GPG, PGP klíče, nejlépe zase ochrana elektronickým podpisem s certifikátem podepsaným důvěryhodnou třetí stranou)

- důvěryhodnost daného programu je možné dokonale ověřit pouze analýzou zdrojových kódů, což je bohužel v praxi většinou nereálné
- pozor na P2P sítě (v případě stahování se může stát, že stahovaný obsah je automaticky nabízen také ostatním ke stažení)
- nestahovat autorsky chráněná data bez oprávnění
- ✓ **vzdálený přístup**
  - pozor na nedůvěryhodné počítače (v internetových kavárnách, studovnách apod.) zejména z důvodu potenciální přítomnosti škodlivého SW (záškodnického zachytávání kláves, viry apod.)
  - používat výhradě zabezpečené protokoly (HTTPS, SSH, SSL, IPSEC, SMTPS, IMAPS, FTPS apod.)
  - ověření otisku (fingerprintu) klíče/certifikátu kvůli detekci útoku typu „Man in the Middle“
  - pokud možno omezit vzdálený přístup tak, aby se bylo možné připojit pouze z nějaké omezené množiny počítačů
  - používat jiné porty, než jsou pro danou službu běžně používané (např. pro SSH použít místo obvyklého 22 nějaký jiný port vyšší než 1023)
- ✓ **informační stopa**
  - zanechává ji za sebou každý uživatel internetu (či obecně IT prostředí vůbec)
  - na serverech zůstávají logy o činnosti uživatele (kdo a kdy se přihlásil, z jaké IP adresy, jaké soubory stahoval apod.)
  - podle IP adresy a/nebo uživatelského jména a času připojení je možné dohledat konkrétního fyzického uživatele
  - historie navštívených stránek v prohlížeči, zapamatování hesel v prohlížeči
  - v případě odstranění dat z webových stránek a/nebo sociálních sítí mohou být nadále dohledatelné v archivech (google, cache apod.)
- ✓ **dohled nad počítačem**
  - nenechávat počítač bez dozoru (útočník může vyjmout a zkopírovat a/nebo upravit či smazat pevný disk)
  - zákaz startování systému z přenosných médií (CD, DVD, USB apod.)
  - zaheslovat BIOS a/nebo zavaděč systému
- ✓ **jak poznat napadený počítač**
  - vyskakuje množství automaticky otevíraných oken, která nejdou zavřít
  - neočekávané změny nastavení počítače, které jste neprovedli (nové panely nástrojů, odkazy, oblíbené položky, jiná domovská stránka, ukazatel myši, vyhledávací program apod.)
  - počítač je pomalejší než obvykle (velké zatížení procesoru)
  - přesměrování stránek v prohlížeči někam úplně jinam
  - antivirus hlásí napadení virem či jiným škodlivým kódem
  - přicházející množství nevyžádané pošty (spamu)
  - pevný disk pracuje nadměrně i když k tomu není důvod
  - nezvyklý program/proces ve správci úloh (task-manageru)
  - jiné nezvyklé chování PC, výpis logů apod.
- ✓ **co dělat v případě napadení**
  - obecně postupovat podle plánu obnovy po havárii (DRP - Disaster Recovery Plan), viz. také dokument o síťové bezpečnosti
  - zaznamenat co nejpřesnější čas zjištění (případně trvání) incidentu
  - kontaktovat odpovědnou osobu (nejlépe správce, u dětí rodiče, ve škole učitele, v práci

- nadřizného)
  - dále je potřeba zajistit (ve spolupráci s odpovědnou osobou - správcem):
    - co nejdříve zabránit útoku (např. omezením přístupu útočnicka do sítě)
    - shromáždit důkazní materiály o útoku
    - zkontrolovat integritu zabezpečení
    - informovat okolí (kolegy, nadřizného) o útoku
    - zvážit možné následky útoku (odchycení hesel, čísel účtů, platebních karet aj.)
    - potrestání pachatele (u lokálních útoků dle vnitřních předpisů organizace)
    - v případě útoku zvenčí upozornit zodpovědného správce (vytvořit a poslat hlášení o incidentu)
  - technicky bývá zpravidla potřeba aktualizovat (v horším případě přeinstalovat) systém, antivirový program, používané aplikace, změnit hesla (v některých případech bývá potřeba systém alespoň dočasně odpojit od počítačové sítě)
- ✓ **vzdělávání uživatelů**
  - předpisy BOZP a jiná adekvátní legislativa
  - interní předpisy a bezpečnostní politika
  - bezpečnostní hrozby a obrana proti nim
  - řešení zjištěných bezpečnostních incidentů
  - komunikace a spolupráce se správcem
  - správné ovládání nainstalovaného SW
- ✓ **co nedělat**
  - vůbec nikomu nikdy žádným způsobem nesdělovat vlastní přístupové heslo či pin kód
  - nikomu (neověřenému či nedůvěryhodnému) přes (nešifrovaný) e-mail nesdělovat citlivé údaje jako číslo kreditní karty apod. (ani, když vás k tomu kdokoliv pod jakoukoliv záminkou nutí – pozor na sociální inženýrství)
  - neotevírat e-maily od neznámých odesílatelů nebo jinak podezřelé e-maily (nevyžádané nabídky, e-maily v cizím jazyce apod.)
  - neklikat na neznámé odkazy
  - neskenovat 2D kódy ze zdí
  - vyhýbat se podezřelým stránkám (hazardní hry, porno apod.)
  - bezhlavě nepřeposílat e-maily (např. různé řetězové e-maily, falešné poplachy apod.)
  - nestahovat autorsky chráněná data bez oprávnění

## 4. Slovníček pojmů

2D ... dvourozměrné

AAA ... Authentication Authorization Accounting (ověřování, autorizace a protokolování činnosti uživatelů)

BIOS ... Basic Input-Output System (základní vstupně výstupní funkce počítače – programové vybavení od výrobce – firmware)

BOZP ... Bezpečnost a Ochrana Zdraví při Práci

CA ... certifikační autorita (entita vydávající digitální certifikáty)

CD ... Compact Disk

DRP ... Disaster Recovery Plan (plán obnovy po havárii)

DVD ... Digital Video Disc

firewall ... zařízení či programové vybavení filtrující síťový provoz a chráníci tak síť či počítač před nevyžádaným provozem v počítačové síti

GPG ... GNU Privacy Guard, svobodná alternativa k PGP  
HW ... HardWare (výpočetní technika – počítače, tiskárny, síťové prvky)  
IDS ... Intrusion Detection System (HW či SW systém detekce narušení počítače či sítě)  
IPS ... Intrusion Prevention System (HW či SW systém prevence narušení počítače či sítě)  
IT ... Informační Technologie (HW, SW, ...)  
mirroring ... zrcadlení disků - zápis stejných dat na více (alespoň 2) disků z důvodu ochrany dat proti selhání disku  
PC ... Personal Computer (osobní počítač)  
PGP ... Pretty Good Privacy (počítačový program umožňující šifrování a podepisování)  
PKI ... Public Key Infrastructure (infrastruktura správy a distribuce veřejných klíčů z asymetrické kryptografie)  
RAID ... Redundant Array of Inexpensive/Independent Disks (diskové pole s alespoň 2 disky zabezpečující data proti selhání disku)  
sociální inženýrství ... zde způsob manipulace lidí za účelem provedení nějaké akce či získání určité informace  
SW ... SoftWare (programové vybavení počítače včetně operačního systému)  
task-manager ... správce úloh v operačním systému  
  
UPS ... Uninterruptible Power Source (nepřerušitelný zdroj napájení – záložní zdroj energie)  
  
URL ... Uniform Resource Locator – řetězec znaků, který představuje jednoznačný identifikátor zdroje na Internetu (např. odkaz na webovou stránku na Internetu)  
USB ... Universal Serial Bus (univerzální sériová sběrnice umožňující připojit periferie jako např. disky, flash paměti, klávesnice, myši, tiskárny apod. k počítači)