Koncepce bezpečnosti

Ohrožení dat

Každý běžný uživatel by měl porozumět principům bezpečného využívání informačních a komunikačních technologií v každodenním životě. Samozřejmostí by mělo být používání odpovídající techniky a aplikací pro zajištění bezpečného připojení k počítačové síti, spolehlivé a bezpečné používání Internetu. Velmi důležitá je také správa dat.

Data a informace

Data je výraz pro údaje, používané pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. Představují formu prezentace reálných objektů (znaky, symboly, obrázky, fakta, události), odrážejí tedy stav reality v určitém časovém okamžiku.

Informace je zpráva, že nastal určitý jev. Vzniká přiřazením významu datům a existuje ve vztahu k příjemci. Slouží k informování o změnách ve vnímané realitě.

Počítačová kriminalita a nebezpečí ohrožení dat

Trestné činy zaměřené proti počítačům nebo trestné činy páchané pomocí počítače označujeme pojmem **počítačová kriminalita**. Jedná se o nemorální, nelegální a neoprávněné konání, které zahrnuje zneužití údajů získaných prostřednictvím ICT. Měli bychom rozlišovat mezi pojmy **hacking, cracking** a **etický hacking.**

Hacker je počítačový specialista či programátor s detailními znalostmi fungování systému. Hacker využívá své schopnosti pro dobré účely. Hacker nachází bezpečností chyby systému, a tak pomáhá k jeho větší bezpečnosti. Výraz hacker se často používá pro počítačové zločince a narušitele počítačových sítí, kteří jsou ale správně označováni termínem **cracker**.

Pojmem **etický hacking** označujeme prolamování bezpečnostních opatření s „dobrým" úmyslem. Může se například jednat o testování zabezpečení firmy vlastními zaměstnanci a následné zdokonalení ochrany.

Cracker (z anglického crack = lámat) je osoba s výbornými znalostmi z programování a bezpečnosti ICT. Své znalosti a dovednosti využívá zejména pro pronikání do počítačových systémů (pronikání do počítačových sítí, prolamování hesel). Takto může nelegálně získat software, ale i úmyslně poškozovat daný subjekt.

Naše data nejsou ohrožena pouze počítačovou kriminalitou, ale i **nebezpečím z vyšší moci**. Mezi taková nebezpečí řadíme požár, záplavy, válku nebo zemětřesení. Z tohoto důvodu je vhodné data zálohovat a zálohy ukládat na různá místa. Dále je důležité si uvědomit, že data jsou ohrožena i ze strany zaměstnanců, poskytovatelů služeb připojení na Internet a externích osob.

Hodnota informace

Ochrana osobních údajů a citlivých obchodních informací

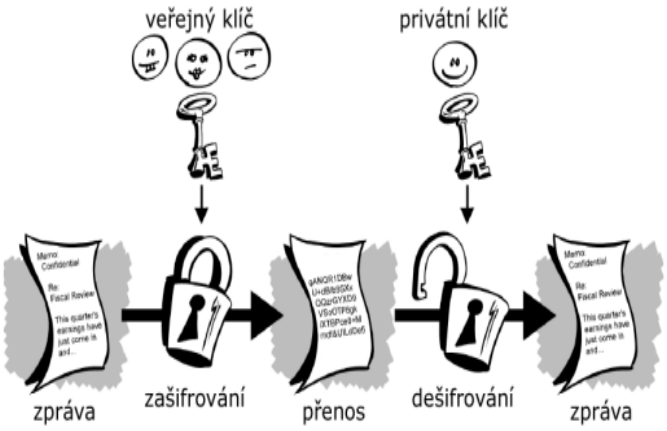
Mezi hlavní důvody pro ochranu osobních údajů patří **krádeže identity** nebo **finanční podvody**. Obdobně je důležitá ochrana obchodně citlivých informací. Mezi důvody pro jejich ochranu patří zejména riziko **odcizení nebo zneužití klientských údajů**, ale i **odcizení finančních informací**.

Zneužití osobní dat nebo obchodně citlivých dat může dané osobě přinést celou řadu problémů. Pokud se cizí osoba dostane k osobním údajům, můžeme přijít o peníze na bankovním účtu. Dále je také možné, že budeme muset nést následky trestného činu, který byl spáchán cizí osobou pod naší identitou.

Šifrování a používání hesel

Neoprávněnému přístupu k datům lze zamezit **šifrováním** nebo **používáním hesel.** Pomocí šifrování se k datům dostane jen osoba, která k nim bude mít přístupové údaje. Šifrovat můžeme vybrané soubory, ale i složky nebo celé disky. Základním principem šifrování je, že se data převedou pomocí vybraného algoritmu do nečitelné podoby. Přečíst se dají pouze pomocí hesla nebo klíče, což umožní data převést do čitelné podoby. Šifrování může být symetrické nebo asymetrické. **Symetrické šifrování** používá k šifrování i dešifrování jediný klíč.

Asymetrické šifrování používá pro šifrování a dešifrování dva odlišné, navzájem provázané klíče. První klíč (veřejný) je použitelný pro šifrování dat. Naopak druhý (soukromý) klíč je používán pro dešifrování. Z výše uvedeného textu vyplývá, že veřejný klíč je nezbytné poskytnout každé osobě, se kterou chci komunikovat. Soukromý klíč nesmíme nikomu sdělovat.



Základní charakteristiky informační bezpečnosti

Mezi základní charakteristiky informační bezpečnosti patří **důvěrnost, integrita a dostupnost** informací. **Důvěrnost** představuje ujištění, že danou chráněnou informaci není schopná přečíst neoprávněná osoba. Důvěrnost tedy znamená ochranu před neoprávněným čtením. Jako obranu proti vyzrazení informací používáme nejčastěji šifrování.

Integrita dat v počítačové bezpečnosti představuje ujištění, že k datům mohou přistupovat a měnit je pouze ti, kteří k tomu mají příslušná oprávnění. Jedná se tedy o ochranu před neoprávněnými úpravami nebo zničením. **Dostupnost** představuje zajištění adekvátního přístupu k informacím. Může být ovlivněna například přírodními vlivy, ale i poškozením nebo chybou v systému.

Ochrana osobních údajů v ČR

Hlavní právní normou, která upravuje ochranu osobních údajů v České republice, je **zákon** č. 101/2000 Sb. **o ochraně osobních údajů.** Podle tohoto zákona si musí každý, kdo shromažďuje osobní údaje a informace za účelem dalšího zpracování, vyžádat k této činnosti souhlas. **Správce osobních údajů je povinen:**

úřad pro ochranu osobních údajů
the office for personal data protection

- stanovit účel, k němuž mají být osobní údaje zpracovány,
- stanovit prostředky a způsob zpracování osobních údajů,
- zpracovat pouze přesné osobní údaje, které získal v souladu se zákonem,
- shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,
- uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování,
- zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny,
- shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,
- nesdružovat osobní údaje, které byly získány k rozdílným účelům.

Osobní bezpečnost

Osobní bezpečnost narušuje tzv. **sociální inženýrství** nebo **krádeže identity**.

Sociální inženýrství

Sociální inženýrství je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Termín je běžně používán ve významu podvodu nebo podvodného jednání za účelem získání utajených informací organizace nebo přístupu do informačního systému firmy. Ve většině případů útočník nepřichází do osobního kontaktu s obětí. **Důsledkem** sociálního inženýrství může být **zneužití osobních informací, finanční podvody** nebo **získání neoprávněného přístupu.**

Mezi **metody sociálního inženýrství** patří:

- **Napodobování telefonního hlasového automatu** (IVR – Interactive voice respose) – je podvodná technika využívající falešného hlasového automatu. Může se jednat například o falešný hlasový automat našeho operátora nebo banky. Oběť takového útoku zpravidla nejdříve obdrží e-mail, který ho vyzývá kontaktovat např. banku na uvedeném telefonním čísle. Falešný hlasový automat se pak pokouší od klienta získat např. PIN, číslo platební karty apod.
- **Phishing (podvrhování falešných zpráv) –** je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů. Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messaging, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.
- **Shoulder surfing (odezírání z obrazovky)** – jedná se „koukání přes rameno", kdy může například docházet k odezírání přístupových údajů při jejich zadávání.

Krádeže identity

Podvodné jednání, kdy se někdo vydává za druhého člověka, s cílem získat finanční prostředky, důležité informace nebo jiné výhody, řadíme pod pojem Identity Theft, čili **krádež identity** nebo totožnosti. Dostanou-li se vaše osobní údaje do nepovolaných rukou, můžete velmi rychle přijít nejen o peníze na svém účtu, ale i zodpovídat za nezaplacené výdaje, za různé škody, dokonce i nést důsledky mnoha trestných činů, které sice spáchala cizí osoba, ale vašim jménem.

Mezi **metody krádeže identity** patří:

- **Information diving –** jedná se o obnovování smazaných dat, vyhledávání informací ve vyhozených datových médiích. Může se jednat o obnovování smazaných dat z vyhozených pevných disků (případně USB disků), ale i obnova dat z prodaných (nalezených, ukradených) chytrých telefonů apod.
- **Skimming –** představuje metodu používání technických zařízení ke krádeži dat nebo přihlašovacích údajů. S touto metodou se setkáváme nejčastěji při padělání platebních karet. Z magnetického proužku karty se bez vědomí držitele zkopírují potřebné údaje na novou padělanou kartu.

- **Pretexting** – je praktika využívající vymyšleného scénáře s cílem přesvědčit oběť k učinění potřebné akce nebo získání potřebné informace. Vymyšlený scénář se využívá k podvodu.

Bezpečnost souborů

Makra jako potenciální hrozba

Potenciální hrozbou pro soubory, se kterými pracujeme, mohou být makra. **Makra** v kancelářských balících označují posloupnost akcí, funkcí nebo příkazů, které usnadňují určitou činnosti. Používají se většinou jako posloupnost kroků při výpočtech nebo úpravách textu. Jsou naprogramována v jazyce VBA (Visual Basic for Applications).

Makra mohou představovat určité **nebezpečí**. Mohou v sobě obsahovat škodlivé kódy, které například způsobí stahování škodlivého softwaru. Jako uživatelé si můžeme nastavit úroveň pro povolování maker. Ukázka nastavení maker v centru zabezpečení kancelářského balíku je k dispozici ve videonávodech.

Výhody a nevýhody šifrování souborů

Obecnou **výhodou** šifrování souborů je jejich ochrana před zneužitím neoprávněnou osobou. Je důležité si promyslet, zda potřebuji šifrovat všechny soubory. **Nevýhodou** je, že čtení a zápis šifrovaných souborů je výpočetně náročnější než práce s obyčejnými soubory.

Jak již víme, šifrování může být symetrické nebo asymetrické. **Symetrické šifrování** používá k šifrování i dešifrování jediný klíč. **Asymetrické šifrování** používá pro šifrování a dešifrování dva odlišné, navzájem provázané klíče.

Podstatnou **výhodou symetrických šifer** je jejich nízká výpočetní náročnost. Algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší. Na druhou stranu velkou **nevýhodou** je nutnost sdílení tajného klíče, takže se odesilatel a příjemce tajné zprávy musí předem domluvit na tajném klíči.

Výhodou asymetrického šifrování je skutečnost, že nemusíme distribuovat soukromý klíč (snižuje se riziko jeho prozrazení). Toto šifrování je možné využít k vytvoření elektronického podpisu. **Nevýhodou** tohoto šifrování je výpočetní náročnost asymetrických algoritmů. K ověření pravosti veřejného klíče je třeba využít například certifikační autoritu.

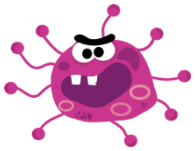
Škodlivý software

Definice a funkce

Malware je označení pro programy, které na počítači běží bez vědomí uživatele a nějakým způsobem ho poškozují. Škodlivý software pracuje různým způsobem:

- **Trojský kůň** – je skrytá část programu s funkcí, kterou si uživatel nevyžádal. Funkce je obvykle škodlivá. Tento typ malwaru nedokáže sám infikovat další počítače nebo programy.
- **Backdoor (zadní vrátka)** – název metody, která umožňuje obejít běžnou autentizaci, která za běžných okolností brání uživateli v neoprávněném využívání počítačového systému. Jedná se o programy, které umožňují útočníkovi získat kontrolu nad naším počítačem. Backdoory jsou součástí softwaru a mohou být využívány k seriózním účelům (servisní přístup).
- **Rootkit (softwarové maskování)** – jedná se o sadu počítačových programů a technologií, pomocí kterých lze maskovat přítomnost zákeřného software v počítači.

Druhy škodlivého software



- **Počítačový virus** – je program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů. Po otevření infikovaného souboru začne vir provádět škodlivou činnost.
- **Červ** – šíří se v podobě infikovaných paketů a je schopen se šířit sám bez nutnosti infikace hostitelského souboru.
- **Spyware** – je „špionážní" program, který bez vědomí uživatele vyhledává na počítači citlivá data (e-mailové adresy, hesla, navštívené internetové stránky) a odesílá je na určenou adresu. Z hlediska bezpečnosti se jedná o velkou hrozbu.
- **Adware** – označení pro produkty znepříjemňující práci nějakou reklamní aplikací. Ty mohou mít různou úroveň agresivity – od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti.
- **Botnety** – softwarový agent nebo internetový robot, který funguje anonymně nebo automaticky. Je spojován s malware, kdy botnet označuje síť počítačů infikovaných speciálním software, který je centrálně řízen z jednoho centra. Botnet pak provádí nežádoucí činnost jako je např. rozesílání spamu apod.
- **Keylogger (odchytávání stisknutých kláves)** – software, který snímá stisky jednotlivých kláves, slouží například ke zjišťování hesel jiných osob.

Ochrana

Antivirovým program je důležitou součástí ochrany proti virům. Důležitým prvkem při ochraně proti virům je samotný **uživatel.** Bezpečnostní software (antivirové programy) jsou pouze doplňkem k zodpovědnému přístupu uživatele. Velmi důležitá je **pravidelná aktualizace** antivirového programu a pravidelná aktualizace operačního systému a dalších programů.

Bezpečnost počítačových sítí

Počítačové sítě

Počítačovou sítí se rozumí zejména spojení dvou a více počítačů tak, aby mohly navzájem sdílet své prostředky. Přitom je jedno, zda se jedná o prostředky hardwarové nebo softwarové. Mezi **hlavní účely** využívání sítí patří **možnost sdílení dat nebo zařízení**. Počítačové sítě mají i svá rizika, která spočívají například ve vyřazení sítě z provozu nebo ve snadném šíření počítačových virů v rámci sítě.

Typy počítačových sítí

Počítače v síti mohou mezi sebou komunikovat:

- přímo (tzv. **peer to peer**) – to znamená, že počítači v síti jsou rovnocenné, data mohou být uložena na všech počítačích v síti, každý počítač služby nabízí i využívá,
- na základě architektury **klient/server** – kdy síť řídí nejvýkonnější počítače (servery), na kterých jsou uložena data a které služby pouze nabízejí, a do sítě jsou zapojeny počítače (klienti), které služby pouze využívají.

Obecně je možné počítačové sítě rozdělit podle mnoha kritérií. Mezi běžné typy počítačových sítí patří:

- **Lokální síť (LAN – Local Area Network)** – jde o vzájemné propojení počítačů rozmístěných v rámci jedné budovy (např. domácnost nebo firmy), respektive ve skupině blízkých budov.
- **Rozlehlá síť (WAN** – Wide Area Network) – propojení počítačů v rámci států, kontinentů, případně celého světa (např. Internet), při kterém se používají prostředky pro dálkový přenos dat.
- **Virtuální privátní síť (VPN)** představuje propojení počítačů prostřednictvím veřejné počítačové sítě (nejčastěji Internet). Spojené počítače mohou mezi sebou komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů. Prostřednictvím VPN se například zaměstnanci připojují k vnitřní firemní síti (když se nacházejí mimo firmu).

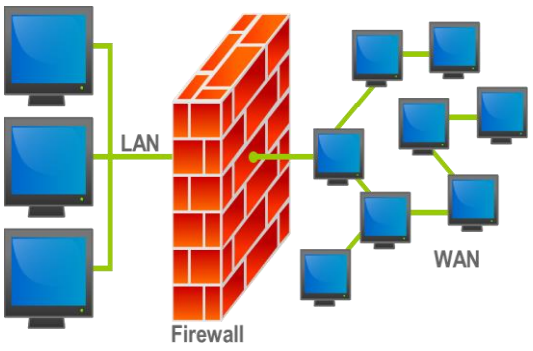
Správce sítě

Správce sítě má velmi důležitou roli při **ověřování identity uživatelů sítě, údržbě a správě uživatelských účtů v rámci sítě.** Správce sítě může měnit nastavení

zabezpečení sítě, instalovat software a hardware, vytváří a mění (případně maže) jiné účty. V prostředí firemní (školní) sítě se musí uživatel přihlašovat svým uživatelským jménem a heslem ve většině případů. Používá se přihlášení do domény – nepřihlašujeme se na počítač, ale na firemní (školní) server. Výhodou je, že se takto můžeme přihlásit na jakémkoliv počítači, který je připojen do firemní (školní) sítě.

Firewall

Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Firewall může být hardwarový nebo softwarový. Příkladem může být ochrana školní sítě před nepovolenými přístupy z Internetu.



Připojování k síti

K počítačové síti může uživatel své zařízení připojit prostřednictvím **kabelu** nebo pomocí **bezdrátového připojení**. Mezi hlavní **rizika** připojení k počítačové síti patří **škodlivý software**, **neoprávněný přístup k datům** a **k osobním údajům**.

Zabezpečení bezdrátové sítě

Pro přístup k zabezpečené bezdrátové síti je vyžadováno heslo. Důvodem je samozřejmě skutečnost, abychom eliminovali přístup do sítě neoprávněným osobám. Rozeznáváme různé typy zabezpečení bezdrátové sítě:

- **WEP (Wired Equivalent Privacy)** – zastaralé zabezpečení bezdrátových sítí. Cílem bylo poskytnout zabezpečení obdobné drátovým počítačovým sítím, protože radiový signál je možné snadno odposlouchat i na delší vzdálenost.
- **WPA (Wi-Fi Protected Access)** – přišlo po prolomení WEP.
- **MAC (Media Access Control)** – je jedinečný identifikátor síťového zařízení. Jedná se o kryptografickou funkci podobnou hašovacím funkcím (používány pro ochranu proti úmyslnému poškození dat). Rozdíl je, že funkce není jen výsledkem zpracovávaných dat, ale i klíče.

Pokud se připojujeme k **nezabezpečené bezdrátové síti**, musíme si uvědomit, že tím zvyšujeme nebezpečí neoprávněného přístup k našim datům.

Řízení přístupu k síti

Otázka **zabezpečení počítače** je v dnešní době uživateli v mnoha případech podceňována. Důležité je uvědomit si, že informace mohou mít velmi vysokou hodnotu. V některých případech nám ochranu důležitých informací ukládá i zákon (např. Zákon o ochraně osobních údajů).

Pro ochranu počítače je vhodné používat uživatelské jméno s **heslem**. Uživatel používá uživatelské jméno a heslo k prokázání identity při přihlašování na počítači. **Bezpečné heslo** je takové, které není snadno zjistitelné (nemělo by to být například vlastní jméno). Heslo by nemělo být krátké. Obvykle je uváděno, že **heslo by mělo mít minimálně 8 znaků,** mělo by obsahovat písmena (malá i velká), číslice a speciální znaky. Mezi **hlavní zásady pro práci s hesly** patří:

- nesdělování hesla,
- pravidelná změna hesla,
- přiměřená délka hesla,
- vhodná struktura hesla (kombinace písmen, číslic a speciálních znaků).

K počítačové síti je možné přistupovat také na bázi kontroly **biometrických údajů**. Mezi tyto techniky patří např. **sken oka** nebo **otisk prstu**.

Bezpečné používání Internetu

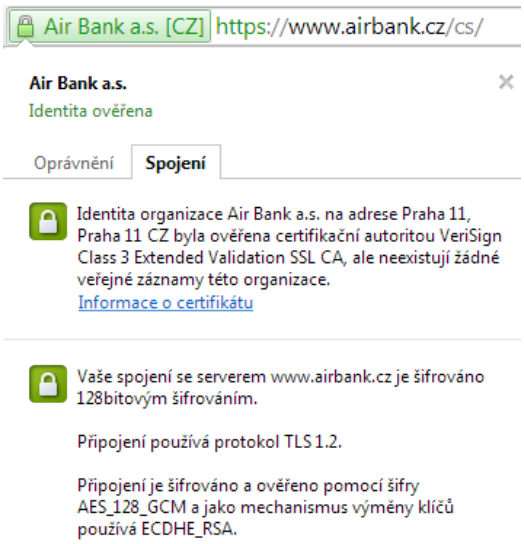
Prohlížení webových stránek

Internet nám nabízí celou řadu služeb. V případě, že tyto služby chceme využívat, musíme se ve většině případů registrovat k dané službě. Při registraci uvádíme celou řadu osobních údajů. Určité činnosti (například online nákupy nebo finanční transakce) bychom měli provádět pouze na **zabezpečených webových stránkách**.

Zabezpečené webové stránky

Pro bezpečnější komunikaci mezi uživatelem a konkrétní webovou stránkou (např. elektronickým bankovnictvím) se komunikace zašifruje na základě zabezpečeného protokolu **HTTPS** (HyperText Transfer Protocol Secured). **Šifrování** je zajištěno prostřednictvím **certifikátu**, poskytovaného příslušným webem. Při odeslání informací od klienta ne web dojde nejprve v počítači klienta k jejich zašifrování a po přenosu na webový server k následnému rozšifrování. Stejný postup samozřejmě platí i pro přenos dat ze serveru ke klientovi. Takto zabezpečenou internetovou stránku můžeme rozpoznat **podle protokolu** nebo podle **symbolu zámku**, který se zobrazí v adresním řádku internetového prohlížeče. Ukázku zabezpečené internetové stránky vidíte na obrázcích (postupně zobrazeno v prohlížeči Google Chrome, Internet Explorer, Mozilla Firefox).

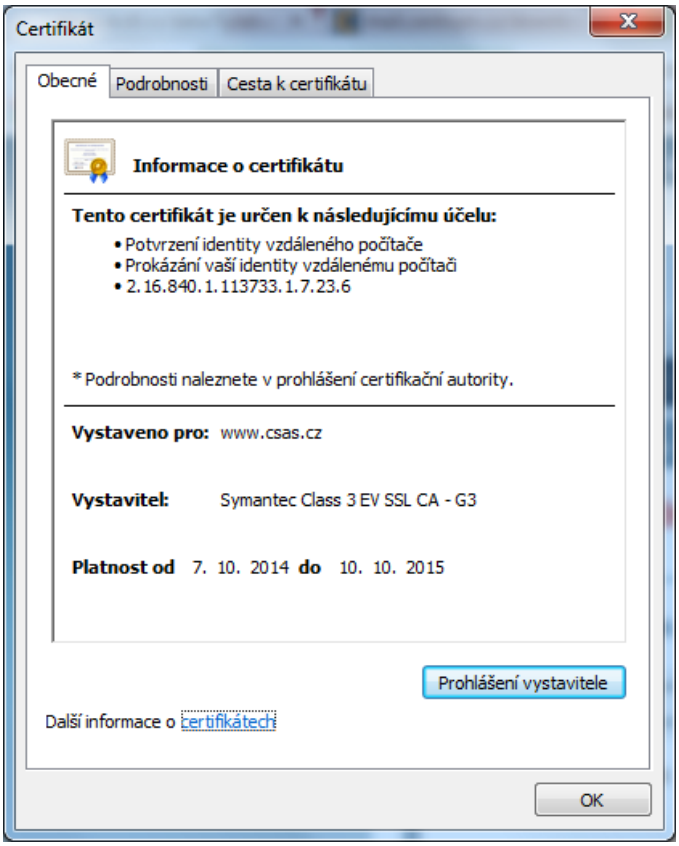
U zabezpečených internetových stránek si může uživatel zobrazit tzv. **digitální certifikát.** Digitální certifikát je soubor dat, který identifikuje osobu nebo server a může během komunikace mezi dvěma subjekty zajistit šifrování přenášených dat. Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení. Digitální certifikáty vystavuje **certifikační autorita.** V České republice fungují tyto: První certifikační autorita, a. s., Česká pošta, s. p., eldentity a. s.



Pharming

V souvislosti s prohlížením webových stránek se můžeme setkat s podvodnou technikou zvanou pharming. **Pharming** se používá k získávání citlivých údajů od obětí útoku. Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky např. internetového bankovnictví po napsání URL adresy banky do prohlížeče. Na falešných stránkách zadá uživatel své přihlašovací údaje nebo jiné citlivé údaje, které mohou být následně útočníkem zneužity.

Digitální certifikát



Bezpečnost internetové komunikace zvyšuje digitální certifikát. **Digitální certifikát** je nástroj, umožňující hodnověrně identifikovat svého držitele, jako například odesílatele zásilky elektronické pošty. Aby bylo možné digitálnímu certifikátu důvěřovat, musí být vydán třetí, nezávislou stranou. Ta se označuje jako **certifikační autorita.** Vydáním certifikátu autorita stvrzuje, že subjekt, jenž je držitelem certifikátu, skutečně vlastní potřebný pár klíčů (soukromý a veřejný), potřebných a platných k jeho identifikaci. Uživatel si certifikát od certifikační autority musí zakoupit a podle pokynů pak nainstalovat. Obrázek vpravo ukazuje informace o konkrétním digitálním certifikátu. Vystavitelem je myšlena konkrétní certifikační autorita. Digitální certifikát byl vystaven pro webové stránky banky Česká spořitelna. Vidíme, že certifikát má omezenou platnost.

Jednorázové heslo

Anglicky **One-time password** (zkratka OTP) je heslo, které je platné pouze pro jedno přihlášení nebo pro nějakou transakci. Jednorázová hesla se snaží vyhnout problémům spojeným se standardními statickými hesly, jako je například odposlechnutí hesla a znovupoužití. Pokud tedy útočník odposlechne jednorázové heslo, jeho znovupoužití již není možné.

Cookie

Soubory **cookie** jsou malé textové soubory, které si navštívené stránky samy uloží do vašeho počítače. Obsahem těchto souborů jsou informace o vás a vašich předvolbách. Při příští návštěvě stejných stránek pak může být přístup operativnější, protože odpadnou určité dotazy, které si server načte právě ze souboru cookie. Automatické ukládání souborů cookie lze považovat za ohrožení soukromí uživatele, proto je možné ukládání těchto souborů nastavit.

Softwarová kontrola

V některých případech potřebujeme regulovat přístup uživatelů na internetu nebo pouze k některému jeho obsahu. Takto můžeme kontrolovat obsah webových stránek, který si zobrazují například děti nebo naši zaměstnanci. Mezi základní nástroje softwarové kontroly obsahu webových stránek patří **filtrování obsahu** a **rodičovská kontrola.**

Sociální sítě

Sociální sítě nám přinášejí celou řadu výhod. Je třeba si také uvědomit rizika, která jsou s používáním sociálních sítí spojena. Při vytvoření účtu na sociální síti uvádíme zpravidla své jméno a příjmení. Jedním z důvodů je skutečnost, aby nás naši přátelé na sociální síti našli a mohli kontaktovat. **Uvádění dalších citlivých osobních údajů je považováno za velmi rizikové.** Není vhodné uvádět přesné datum narození, adresu bydliště, údaje o vzdělání apod. Ve statusech není vhodné uvádět informace, které mohou být použity proti vám (například odjezd na dovolenou).

S používáním sociálních sítí jsou spojena zejména tato potenciální nebezpečí:

- **internetová šikana**,
- **grooming (předstírání cizí identity)**,
- **zavádějící nebo nebezpečné informace**,
- **falešná totožnost**,
- **podvodné odkazy nebo zprávy**.

Komunikace

Elektronická pošta

Téměř každý denně používá emaily. Nevýhoda elektronických zpráv je, že se ve většině případů šíří po internetu naprosto otevřeně (jinak řečeno čitelně). Bezpečnostním řešením je nějaký způsob **šifrování**, buď provozu, nebo jednotlivých zpráv. Důvodů pro šifrování důvěrných a citlivých zpráv je několik. Jedná se zejména o následující rizika:

- zneužití osobních údajů,
- vyzrazení obchodního tajemství a ztráty konkurenční výhody,
- prozrazení výše chystané nabídky,
- vydírání pomocí získaných citlivých údajů.

Digitální podpis

Je jeden z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí Internetu. Pro digitální data zajišťuje podobné vlastnosti jako vlastnoruční podpis u běžných papírových dokumentů. Elektronický podpis ve formě datového souboru je tedy využíván jako přímá náhrada manuálního podpisu a má stejnou právní sílu a průkaznost. **Elektronický podpis** zajišťuje:

- **integritu dokumentu** – lze prokázat, že po podepsání nedošlo k žádné změně, soubor není poškozen,
- **autentizaci** – lze prokázat, že autorem je skutečně ten, kdo je pod dokumentem podepsán,
- **důvěryhodnost** – obsah odpovídá tomu, co autor podepsal,
- **nepopiratelnost** – autor nemůže popřít, že dokument podepsal.

Elektronický podpis potřebuje k potvrzení své platnosti digitální certifikát. Jak už víme, digitální certifikát může vydat tzv. certifikační autorita.

Rizika při práci s elektronickou poštou

Elektronická pošta je zneužívána k posílání **nevyžádaných mailů (spamů)** a různých **podvodných zpráv.** Taková činnost je nelegální, ale velmi těžko postižitelná. Mezi další rizika používání elektronické pošty patří infekce počítače virem. Uživatel by neměl otvírat nevyžádané maily (zejména jejich přílohy, které při svém otevření většinou infikují počítač, a to bez vědomí uživatele).

Spam (nevyžádaná pošta) je jednou z bezpečnostních hrozeb. Může se stát, že nám neznámá osoba zašle nevyžádanou zprávu s přílohou, ve které se nachází soubor, který

může být nakažen virem. Přílohy nevyžádané pošty od neznámé osoby bychom neměli otvírat, případně stahovat do počítače.

Bezpečnostním rizikem jsou také zprávy elektronické pošty s **přílohou**, která obsahuje **soubory s makrem** nebo **spustitelné soubory.** Makra v sobě mohou obsahovat škodlivé kódy, které například způsobí stahování škodlivého softwaru. Spustitelné soubory pak mohou obsahovat např. viry. Existují e-mailoví klienti, které uživateli nedovolí takový spustitelný soubor jako přílohu nahrát.

Phishing (podvrhování falešných zpráv) – je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů. Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messaging, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze. **Mezi charakteristické rysy phishingu patří:**

- používání oficiálních názvů firem,
- používání jmen kompetentních osob,
- používání falešných webových odkazů.

Komunikace na síti v reálném čase

Instant Messaging (IM) – je komunikace v reálném čase. Jedná se o internetovou službu, která umožňuje svým uživatelům sledovat, kteří uživatelé jsou právě připojeni. Podle potřeby jim pak můžeme posílat zprávy, soubory a jinak komunikovat. Nástroje, které umožňují komunikaci v reálném čase: chat, ICQ, Skype, sociální sítě, Windows Live Messenger, Miranda IM atd. S komunikací v reálném čase jsou spojena zejména tato **rizika:**

- škodlivý software,
- přístup „zadními vrátky" (backdoory),
- neoprávněný přístup k datům.

Pro **zabezpečení důvěrných informací** při komunikaci v reálném čase používáme **šifrování**, **nezveřejňujeme důležité informace** a **nesdílíme soubory**.

Bezpečná správa dat

Bezpečnost a zálohování dat

Bezpečnost

Důležité je také zajistit **fyzickou bezpečnost** konkrétního zařízení s daty. Z tohoto důvodu je vhodné umístit takové zařízení (např. počítač) na **vhodně zabezpečeném místě**. Pro notebooky je pak typické použití **kabelových zámků.** Kabelový zámek slouží jako ochrana před odcizením přenosného počítače. Pomocí takového zámku připoutáme notebook k nějakému pevnému předmětu. Kabelový zámek se připevňuje do speciálního otvoru, který je součástí většiny notebooků. Dále je vhodné vzít v úvahu **omezení** a **zabezpečení přístupu** k takovému zařízení.

Zálohování dat

Data je vhodné **zálohovat.** Je třeba si uvědomit, že současná digitální média mají životnost jen několik let. Mezi zásady správného zálohování patří:

- **Pravidelnost** – data by měla být zálohována v pravidelně se opakujícím časovém intervalu (můžeme využít nástrojů automatického zálohování nebo data pravidelně zálohovat ručně).
- **Frekvence zálohování** – záleží na datech, která zálohujeme. Ve firemním prostředí je na frekvenci zálohování kladen daleko větší důraz, než v případně domácího prostředí.
- **Umístění datového úložiště –** úložiště pro datové zálohy se má nacházet mimo budovu, ve které se nachází primární data. Firmy velmi často využívají služeb tzv. datových center. Domácnost pak může využít některou z online zálohovacích služeb na Internetu.
- **Plán zálohování** – každá firma by měla mít vlastní zálohovací plán a zpracované procesy, jak bude postupovat v případě nenadálé ztráty dat. Jen při dodržení pravidelného zálohování budete ušetřeni starostí při nenadálém kolapsu počítače. V případě firemních dat je potřeba analyzovat důležitost jednotlivých dat pro bezproblémový chod firmy po nenadálé ztrátě dat. Po této analýze stanovíme optimální způsob zálohování dat a sestavíme vhodný zálohovací plán.

Bezpečná likvidace

Je třeba rozlišovat mezi **mazáním** a **trvalým odstraněním dat**. Data můžeme vymazat do koše, případně později z koše odstranit. Pro odstranění dat bez použití koše můžeme využít klávesovou zkratku Shift+Delete.

Paměťový prostor, kde jsou data umístěna, není vymazán. Data jsou v tomto paměťovém prostoru stále uložena. Pouze je tato oblast označena jako prázdná. Pokud ukládáme další data, tato nová data přepisují data stará. I takto přepsaná data se dají v mnoha případech ještě obnovit (může však docházet ke ztrátě kvality takových dat).

Metody trvalého odstranění dat

V některých případech potřebujeme vymazat data z disku a datových médií tak, aby již **nemohla být obnovena.** Mezi metody pro trvalé odstranění dat patří:

- **Fyzická likvidace zařízení a médií** – v podstatě se jedná o nejúčinnější způsob trvalého odstranění dat. V případě pevného disku musí dojít ke zničení ploten disku (nikoliv pouze obalu). Pokud budeme fyzicky likvidovat optická média (CD a DVD), stačí disk rozlámat na malé kousky. Můžeme použít i speciální skartovačku.
- **Demagnetizace (degaussing) –** při této metodě je pevný disk vystaven magnetickému poli, které zničí jednotlivé vrstvy na plotnách a tím pádem i uložená data. Tato metoda ovšem způsobí, že se disk stává nepoužitelným, protože dochází k jeho trvalému poškození.
- **Použití programových nástrojů na likvidaci dat –** můžeme také využít specializované programy. Výhodou je, že disk můžeme používat dál. Nedojde k jeho fyzickému poškození.