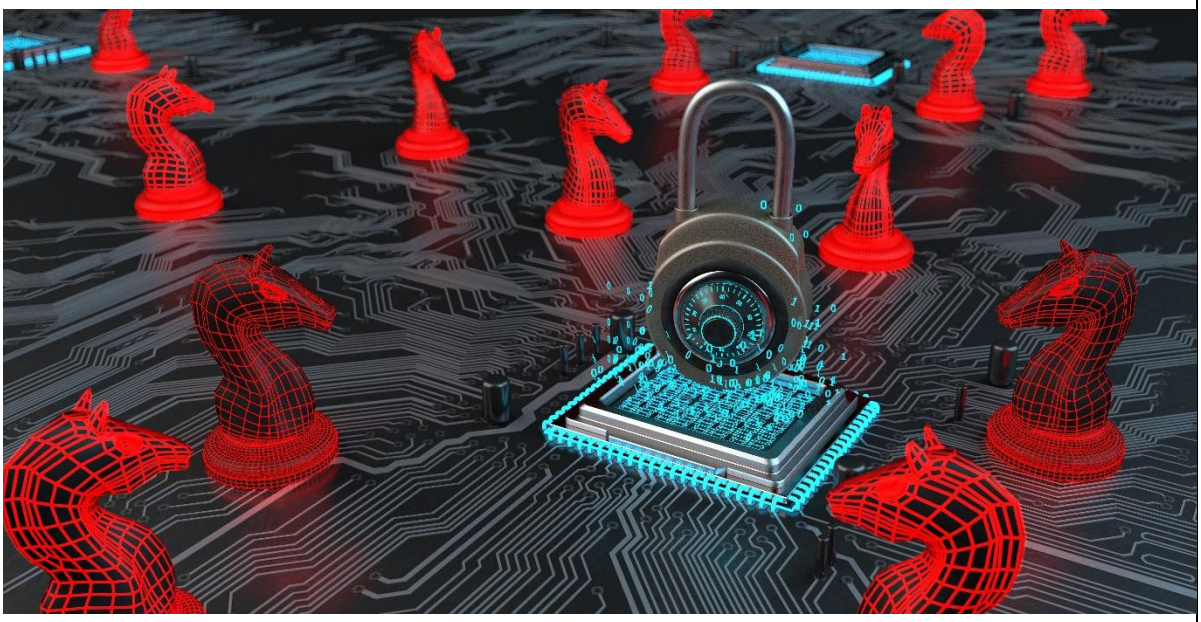
5 IT BEZPEČNOST

5.1 Téma

První seznámení

Zálohování dat bylo dříve mnohem snadnější než dnes. V minulosti byly důležité dokumenty (smlouvy, vkladní knížky atd.) z důvodu bezpečnosti uloženy v trezorech nebo ukryté na jiném místě. Díky tomu se neoprávněné osoby k datům nemohly dostat vůbec nebo jen s velkými obtížemi.

Dnes už to tak snadné není. Dokumenty a data jsou dnes digitalizována a často již nejsou fyzicky dostupné. Ukázkovým příkladem je online banking, kde jsou důležité smlouvy podepisovány elektronicky a posílány přes e-mail, nebo soukromá data jako jsou fotografie. Stejně jako analogové dokumenty bývaly uzamčené a schované i nyní musí být data dobře a bezpečně schovaná. Potenciální krádež dat nebo nezákonné zpracování a manipulace s daty mohou s sebou totiž nést vysoké riziko a vážné důsledky jak pro jednotlivce, tak pro celé firmy nebo organizace.



IT bezpečnost, jinak také “informační bezpečnost”, není zcela novým pojmem, aktuálně je čím dál tím důležitější vzhledem k rapidně rychlému vývoji digitálních technologií v posledních letech. My bychom měli být s tímto pojmem obeznámeni, protože digitální technologie jsou jednoduše součástí moderního života, ať už jsme si toho vědomi nebo ne.

Praktický význam – k čemu využijete znalosti a dovednosti

Od soukromého života po pracovní život, od jednotlivých společností ke globálním korporacím – data a informace jsou přítomny ve všech oblastech života a jejich přínos je veliký. Ať už se jedná o počítačovou kriminalitu, ztrátu dat nebo padělání dat, IT bezpečnost by se měla opravdu týkat každého. Tento dokument vám pomůže zajistit bezpečnost vašich soukromých dat a cenným způsobem přispět k zabezpečení dat ve vaší společnosti. Budete schopni v tomto ohledu správně a sebevědomě jednat.

Stručný přehled učebních cílů a kompetencí

V této kapitole se seznámíte s pojmem IT bezpečnost a jeho nejdůležitějšími aspekty. Dozvíte se více o jeho významu a cílech, ale také o tom, jaké hrozby a opatření v současné době existují v

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

oblasti IT bezpečnosti. Dozvíte se, jak můžete osobně přispět k bezpečnějšímu informačnímu prostředí, ať už v soukromí nebo v pracovním prostředí.
Učební cíle
Porozumíte obecným definicím IT bezpečnosti a poznáte její oblasti využití.
Dokážete pojmenovat a vysvětlit cíle a úkoly IT bezpečnosti.
Seznámíte se s aktuálními IT hrozbami, a budete je schopni správně přiřadit k oblasti využití IT bezpečnosti.
Poznáte opatření a obranné mechanismy ve využití IT bezpečnosti.

5.2 Definice a oblasti využití

Hned na začátku je potřeba si vyjasnit jednu věc - **IT bezpečnost se netýká pouze bezpečnosti informací**, ačkoli jsou oba termíny často používány stejným způsobem (zejména pokud nejsou přesně přeloženy z angličtiny do jiného jazyka), existuje mezi nimi malý rozdíl, který vám pomůže oba výrazy přesněji definovat.

V principu je rozdílem především „T“ v názvu - protože „IT“ je zkratka pro „Information Technology“ neboli v češtině „informační technologie“. Jelikož je tento název poměrně dlouhý, budeme se raději držet pojmu „IT bezpečnost“.

Definice

Informační bezpečnost vs. IT bezpečnost

Pojem **informační bezpečnost** představuje ochranná opatření pro VŠECHNY systémy, které jakýmkoli způsobem zpracovávají nebo ukládají informace. Nezáleží na tom, zda jsou digitální nebo „analogové“. V tomto případě je brán v potaz počítač stejně jako hromada ručně psaných důvěrných dokumentů.

IT bezpečnost je podoblastí informační bezpečnosti. Ve skutečnosti se v rámci ní berou v potaz pouze ochranná opatření tzv. “sociálně-technických“ systémů. Sociálně-technické systémy nejsou ničím jiným než systémy, ve kterých lidé používají k ukládání a zpracování dat informační technologie.

Mimochodem, podle slovníku je **informační technologie** definována jako „technologie pro sběr, přenos, zpracování a ukládání informací pomocí počítačů a telekomunikačních zařízení“.

Zatím to zní všechno poměrně jednoduše. Jenže v dnešní době se jen ve výjimečných situacích nepoužívají žádné informační technologie, tudíž IT bezpečnost tvoří velmi velkou část informační bezpečnosti.

Příkladem využití informační bezpečnosti bez IT může být ručně psaný tajný recept uložený v trezoru vaší oblíbené restaurace. Ale o tom tato kapitola není. V oblasti IT bezpečnosti existují i další dílčí pojmy, mezi kterými má smysl si udělat hned na začátku jasno a zejména vysvětlit, jak jsou vzájemně propojeny:

- **Počítačová bezpečnost:** Týká se konkrétně bezpečnostních opatření lokálních i síťových počítačových systémů jako takových. Jak bezpečný je počítač před neoprávněným přístupem nebo manipulací? Co se stane, když je počítač „nabourán“?

Co-funded by the Erasmus+ Programme of the European Union

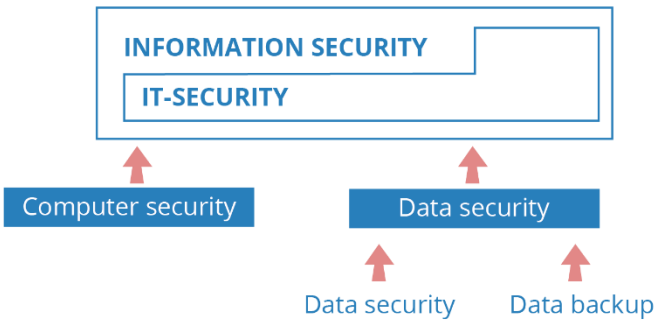
Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

- **Ochrana údajů:** Jedná se o skutečně moderní pojem, a to zcela oprávněně, protože „ochrana údajů = ochrana lidí“. Tento pojem je pro jedince nejdůležitější, protože se týká ochrany vlastních osobních údajů před zneužitím. Soukromí a anonymita jsou v digitalizovaném světě poměrně citlivým tématem.

- **Bezpečnost dat:** Tento pojem je opět technické povahy. Nejedná se tolik ani o právní otázky, ale spíše o to, jak chránit data před manipulací nebo ztrátou. Bezpečnost dat lze chápat jako předběžnou technickou fázi úspěšné ochrany údajů.

- **Zálohování dat**: Jedná se konkrétně o (vícenásobné) zálohy dat - nejspíše jste se s termínem „záloha“ již setkali. Zálohování dat tedy není nic jiného než správná duplikace dat, která má zabránit jejich ztrátě.

Následující diagram lépe objasní kontext výše uvedených pojmů:



IT bezpečnost tvoří velkou část informační bezpečnosti a skládá se zejména z počítačové bezpečnosti a bezpečnosti dat. Bezpečnost dat je základem pro úspěšnou ochranu údajů a zálohování dat.

Důležité

Data a informace

Nyní už jste viděli pojmy „data“ a „informace“ tolikrát, že určitě budete chtít znát rozdíly mezi nimi:

- Data jsou v podstatě zbytečné znaky a symboly, které bez kontextu zůstávají prázdná a nelze s nimi nic dělat. Vezměme si například posloupnost čísel 19081974.

- Informace jsou data, která jsou již dána do kontextu. Tato data tak získají smysl a přinášejí informace, např. „datum narození 08-19-1974“. Nyní je již jasné, co daná posloupnost čísel znamenala.

Mimochodem toto je také základní předpoklad šifrování bez ohledu na to, zda se provádí na počítači nebo ručně. Při šifrování data necháváte bez kontextu, možná je dokonce smícháte. Pouze někdo, kdo také zná kontext, může sledu čísel a znaků rozumět.

Pro koho je dnes zavedení IT bezpečnosti důležité?
V podstatě pro každého, kdo používá počítač, ať už se jedná o jednotlivce nebo celou organizaci. Nicméně, bude lepší oblasti implementace IT bezpečnosti trochu přesněji klasifikovat i z toho důvodu, aby bylo později možné správně přiřadit hrozby a odpovídající opatření k oblasti využití IT bezpečnosti. Hlavní rozdíl spočívá v tom, zda jsou zařízení a data užívána v soukromí nebo v organizaci.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Soukromý sektor: Týká se jednotlivých osob a zařízení, která se používají v soukromí. Patří sem například váš vlastní notebook nebo chytrý telefon. To, zda je používáte veřejně, například v univerzitní síti WLAN, má sekundární význam. Důležité je, že zařízení používáte ke správě svých soukromých dat.

Firmy a organizace: Jedná se o zařízení, která lze použít pro přístup k datům společností nebo organizací, například firemní notebooky nebo firemních telefony. To se týká jak komerčních podniků, tak i státních institucí a organizací. Jedná se o *sdílená data*, která patří konkrétní organizaci.

Jaké jsou konkrétně rozdíly mezi těmito dvěma oblastmi využití?

- **Soukromý sektor**
  Téměř každý software má vždy nějaké chyby v kódu. Mohou být způsobeny nepřesností, ale také jednoduše nevědomostí. Nikdo nemůže dopředu vědět, jakými „zadními vrátky“ nebo jakou speciální funkcí v softwarovém kódu může být získán nežádoucí přístup.
  To může představovat obzvlášť velký problém, protože většina zařízení je neustále připojena k internetu, ať už se jedná o osobní počítač, chytrý telefon, chytré hodinky, ale také televizi nebo hlasového asistenta. Ve většině případů dochází k „vloupání“ nebo k neoprávněnému přístupu k osobním údajům prostřednictvím internetu. Krádež dat ale může probíhat také fyzicky, např. vloupáním a odcizením počítače.

  Je třeba poznamenat, že k tomu může dojít velice rychle a v jednom momentě jsou vaše hesla pro online bankovnictví odcizena, důležité dokumenty ztraceny a vaše soukromé fotografie zveřejněny. IT bezpečnost je v soukromém sektoru důležitým tématem, ale i přesto jsou v této oblasti používány méně účinné prostředky než v podnikovém sektoru, ať už je to kvůli malé informovanosti osob, které systém používají, nebo kvůli menšímu množství technických možností.
- **Firmy a organizace**
  Co se týče IT bezpečnosti ve firmách, hlavní důraz je samozřejmě kladen na ekonomické zájmy. Ačkoli je technické zavedení IT bezpečnosti obvykle kvalitnější než v soukromém sektoru, četnost IT útoků je současně mnohem vyšší.

  Ať už se jedná o banky nebo pojišťovací společnosti, které spravují velké množství peněz, nebo „high-tech“ společnosti, které chtějí ochránit své prototypy a nápady před konkurencí, v obou případech jsou systémy IT připojeny přes internet.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Jako příklad by mohlo posloužit použití cloudových služeb z několika míst ve firmě najednou. Cloudový server poskytuje úložný prostor pro dokumenty, které lze číst a upravovat přes internet ze všech míst ve firmě. V tomto případě je třeba především zajistit, aby k těmto dokumentům měly přístup pouze oprávněné osoby.

Velké firmy mají v současné době celá vlastní oddělení, která mají na starosti pouze IT bezpečnost a investují spoustu peněz do jejich pravidelné aktualizace. I v tomto případě totiž platí, že JAK dojde k IT útoku není předem známo, tudíž je především potřeba být dobře připravený, POKUD k útoku dojde.

Mimochodem, již existují standardizované dokumenty pro IT bezpečnost, tzv. základní katalogy ochrany, které představují podrobné modely IT bezpečnosti. Nicméně, informační technologie se vyvíjejí tak rychle, že pouhé sledování těchto katalogů k zajištění bezpečnosti nestačí a některé z nich se rychle stávají neaktuálními.

Zapamatujte si

IT bezpečnost je podoblastí informační bezpečnosti a zahrnuje všechna ochranná opatření týkající se zpracování a ukládání dat pomocí systémů informačních technologií. To zahrnuje jak počítače, tak všechny ostatní telekomunikační prostředky v soukromém i podnikatelském prostředí.

IT bezpečnost může být také definována svými podoblastmi, které jsou vzájemně propojené:

- Počítačová bezpečnost
- Ochrana údajů
- Zálohování dat
- Bezpečnost dat

Oblasti využití IT bezpečnosti zasahují do soukromého i podnikatelského a veřejného sektoru. Protože je většina zařízení připojena k internetu, míra nebezpečí IT útoků a opatření pro IT zabezpečení je ve všech oblastech velmi podobná, rozdíly lze najít v povědomí jednotlivců o IT bezpečnosti a technologických faktorech.

5.3 Cíle a úkoly IT bezpečnosti

Nejdůležitějším úkolem IT bezpečnosti je **sledování technického vývoje**. Digitalizace a propojení světa postupuje technologicky velmi rychle. Nové technologie vyžadují nové softwary a nové oblasti využití vyžadují nová bezpečnostní opatření. Zatímco v minulosti několik výkonných počítačů jednoduše převzalo úkoly celých společností a bylo provozováno hrstkou lidí, dnes existuje nesčetné množství malých, vzájemně propojených zařízení. Může být dokonce poměrně obtížné přesně určit, co má být před čím chráněno, jaké hrozby existují a jaké mezery v bezpečnostních systémech by mohly být zneužity. Nicméně, jsou definovány tzv. **cíle ochrany**, které jsou považovány za hlavní cíle IT bezpečnosti, jde o:

diskrétnost – integrita – dostupnost

Pokud si vědomě vezmete tyto tři cíle ochrany k srdci, již jste implementovali polovinu IT bezpečnosti.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Pojďme se na ně nyní podívat z blízka:

- **Diskrétnost**
  Data, informace a výsledné znalosti by měly být skryty před osobami, které na ně nemají právo nahlížet.

- **Integrita**
  Data, informace a výsledné znalosti by měly být ochráněny proti neoprávněnými změnami a manipulací.

- **Dostupnost**
  Data, informace a výsledné znalosti by měly být v případě potřeby dostupné všem, kteří k nim mají povolený přístup.

Tyto tři cíle jsou hlavní a velmi důležité jak v soukromém, tak i v obchodním kontextu. Pojďme se podívat na následující příklady:

Příklady
Tři cíle ochrany v soukromém kontextu pomocí příkladu „online bankovnictví“ Používáte online přístup ke svému bankovnímu účtu? Jedná se o poměrně citlivou záležitost, protože v sázce jsou vaše peníze. Jak jsou zde zajištěny cíle ochrany? • Diskrétnost: Váš přístup, hesla a data na účtu by měla být dostupná pouze vám. • Integrita: Nikdo jiný, než vy by neměl mít možnost provádět neautorizované online převody. • Dostupnost: Měli byste mít neomezený přístup ke svému účtu kdykoli a kdekoli. **Tři cíle ochrany v podnikovém kontextu pomocí příkladu „vývoje produktu“** Společnost vyvíjí zcela nový produkt, který by způsobil revoluci na trhu. K tomu by mělo samozřejmě dojít bez toho, aniž by z toho těžila konkurence. Jak by mohly být v tomto případě cíle ochrany splněny? • Diskrétnost: Na veškeré informace o vývoji nového produktu mohou nahlížet pouze oprávněné osoby. • Integrita: Data získaná z vývoje produktu jsou chráněna před sabotáží a manipulací zvenku. • Dostupnost: Všechny zúčastněné a pověřené osoby mají zabezpečený přístup k vývoji nového produktu a výsledným údajům.

Kromě toho existují také rozšířené cíle ochrany, které je také třeba na základě konkrétních požadavků brát v potaz. Ty nemusí být nutně zakotveny v IT zabezpečení a mohou se značně lišit v soukromém a v podnikovém kontextu.

- **Odpovědnost** nebo **anonymita**
  Úkon v IT prostředí může nebo nemusí být jasně přiřazen konkrétní osobě. V podnikovém kontextu lze například identifikovat osobu odpovědnou za interní sabotáž. V soukromém životě se však spíše setkáme s pravým opakem, konkrétně s tím, že daná osoba si chce v souvislosti se svými údaji zachovat co největší možnou anonymitu – například při vyhledávání témat na internetu spojených se zdravím.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

- **Pravost**
  Údaje, informace a výsledně získané znalosti by měly být ověřitelné z hlediska pravosti, například zda jsou předávané výsledky výzkumu originální nebo byly manipulovány třetí stranou.

- **Uznatelnost**
  Činnosti v prostředí IT by neměly jít snadno zamítnout – to je obzvlášť důležité pro elektronicky zpracované smlouvy, kde se například používají elektronické podpisy.

Jak je možné dosáhnout těchto cílů v praxi?

Tato otázka se především týká **slabých stránek** IT bezpečnosti. Nebo spíše jde o hledání a odstraňování zranitelných míst. Jak jste se již dozvěděli, každý software má slabiny. Ty nejsou předem jasně identifikovatelné. Často je to kvůli špatnému programování použitého softwaru nebo navržení IT systému. To nutně nemusí znamenat, že došlo k „špatnému“ programování, ale jednoduše to, že ne všechny známé hrozby IT systému byly brány při programování v potaz. Slabými stránkami však mohou být i lidé nebo nesprávné zacházení s IT systémy.

Důležité
IT bezpečnost lze samozřejmě obejít nejen prostřednictvím softwaru, ale **také prostřednictvím hardwaru**. Je to však více „nepraktické“, protože k manipulaci nebo odcizení dat pomocí hardwaru musíte být fyzicky přítomni, například s USB klíčem v ruce nebo odcizením celého počítače. Přístup k softwaru pomocí internetu je tedy pohodlnější, a především je mnohem obtížnější jej vysledovat, pokud jste přichyceni uprostřed činu.

Pro dosažení cílů ochrany v IT bezpečnosti je proto nesmírně důležité identifikovat tyto slabiny a možné scénáře hrozeb. A tady se začínají věci stávat komplikovanějšími, protože stoprocentní pokrytí všech slabých stránek není kvůli neustálému vývoji systémů a obecně kvůli neschopnosti nahlédnout do budoucna vůbec možné – člověk může pouze co nejblíže odhadovat.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Zapamatujte si
IT bezpečnost **silně závisí na aktuálním technologickém vývoji** – nové oblasti využití informačních technologií přinášejí také nová nebezpečí. Je potřeba rychle reagovat, aby bylo možné navrhnout vhodná opatření. Ve všech oblastech využití musí být splněny následující **tři cíle ochrany**: • Diskrétnost • Integrita • Dostupnost Existují další tři cíle ochrany, které se liší v závislosti na oblasti využití a měly by být odpovídajícím způsobem zváženy: • Odpovědnost nebo anonymita • Pravost • Uznatelnost K dosažení těchto cílů ochrany je **klíčovým úkolem IT bezpečnosti identifikovat slabá místa systémů** a odpovídajícím způsobem je odstranit. Může se to také týkat hardwaru, ale v současné době spíše softwaru, a to především chyb nebo nezohledněných nedostatků v programování. K dokonalé IT bezpečnosti se lže přiblížit, ale nelze ji na 100 % docílit. Z tohoto důvodu musí být s IT bezpečností zacházeno jako s celkem.

5.4 Hrozby v IT

Hrozby v oblasti IT jsou rozmanité a nemusí být nutně úmyslné nebo mít trestní povahu. IT může být také ohroženo „vyšší mocí“ nebo technickým selháním, například zemětřesení by mohlo způsobit výpadek napájení, který by vedl ke ztrátě dat.

Samozřejmě je však myslitelná i lidská chyba. Klasickým příkladem je zapomenutí hesla pro online bankovnictví a ztráty přístupů k důležitým informacím. Nyní se dozvíte o možných IT hrozbách, přičemž mějte stále na paměti cíle ochrany z předchozí kapitoly.

Důležité
Potenciální hrozba nebo zranitelnost neznamená automaticky, že je IT v ohrožení. O skutečnou hrozbu se jedná pouze v případě, pokud se zranitelnost (např. chyba programování nebo snadno přístupná WLAN) setká s hrozbou (např. útok hackerů).

Cílené útoky lidí nebo organizací
V první řadě musí IT bezpečnost zabránit útokům, obvykle nazývaným jako „hacking“, které jsou prováděny záměrně. Jednotlivec nebo dokonce celá organizace obvykle získává neoprávněný přístup k cizím datům a pokouší se obejít cíle ochrany. To může probíhat za různými účely: krádež finančních prostředků, sabotáž konkurenčních společností, politická motivace a někdy dokonce jen „pro zábavu“. Vždy se ale jedná o získávání, manipulaci nebo ničení cizích informací prostřednictvím sítě, ke které jsou cílová zařízení připojena.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Nejdůležitější nástroje takových hackerských útoků jsou známé z hollywoodských filmů z přelomu tisíciletí a obvykle mají legrační jména - „viry“, „trojské koně“, „červi“, „spoofing“, „phishing“ a další. Podívejme se blíže na některé z těchto příkladů:

- **Viry**
  Počítačové viry jsou jednoduše programy, které automaticky provádějí své naprogramované úlohy v cílových systémech: například vysledují heslo. Viry potřebují k jejich šíření tzv. hostitele. Může se jednat o hromadný e-mail nebo o tzv. „vyskakovací okno“ - například samo otevírací web, který odkazuje na údajně nutnou aktualizaci.

- **Počítačoví červi**

  Jedná se o viry, které se dokáží samy aktivně šířit – to znamená, že aktivně detekují slabá místa v systémech a sítích a podle toho postupují vpřed bez nutné přítomnosti takzvaného „hostitele“.
- **Trojský kůň**
  Jedná se o na první pohled užitečné programy, které si oběť nainstaluje, ale v pozadí instalace trojské koně otevírají zadní vrátka v systému, předávají data a informace a mohou například zaznamenávat zadaná hesla.

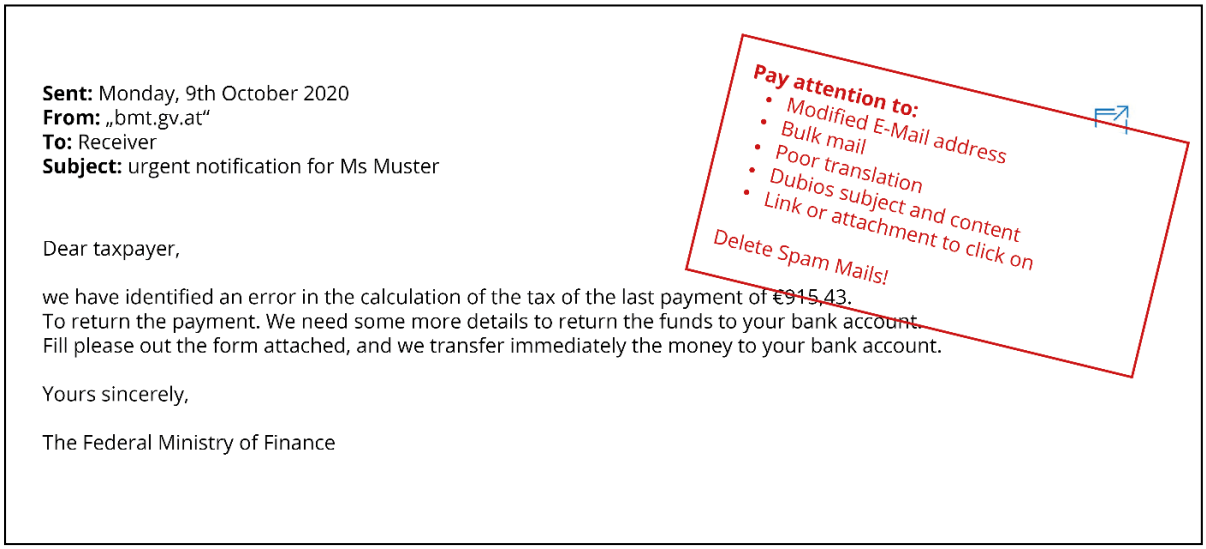
- **Odepření služby (anglicky „denial of service attacks“, zkráceně DoS)**
  V tomto případě je pravděpodobnější manipulace s daty – záměrným přetížením systému zvenčí (to lze provést například automatickým opakovaným vyvoláním webové stránky) se systém zastaví. Někdy se to stane, dokud například postižená organizace nezaplatí výkupné. Mimochodem, software pro metody vydírání je také označován jako „ransomware“ (složení anglických slov „ransom“ - výkupné a „software“).

- **Spoofing/Phishing**
  Jedná se zejména o krádež identity. Falešné weby na internetu a e-maily, které na ně odkazují, lákají oběť k aktivnímu sdílení hesel nebo informací o účtu. Vyskytují se hlavně v soukromém sektoru IT bezpečnosti.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

- **Spam**
  Asi nejznámější termín v oblasti IT bezpečnosti nepopisuje nic jiného než nevyžádané e-maily – může se jednat o obtěžující e-mail s novinkami, ale samozřejmě také o hostitele virů nebo phishingových pokusů.



Výše uvedený malware lze samozřejmě také osobně „vpustit“ do počítačového systému – informace mohou být odcizeny nebo manipulovány fyzickým vloupáním do budovy společnosti nebo do domu. Vzhledem k propojení počítačových systémů to však obvykle již není nutné.

K fyzické manipulaci však někdy dochází jednoduše interně. Například když pracovníci vaší společnosti ukradnou data o zákaznících nebo produktová tajemství bez povolení, aby je mohli externě prodat.

Neúmyslné ohrožení lidskými chybami
Hrozby pro IT bezpečnost však nemusí být vždy vysoce trestné a úmyslné. Někdy dochází k ohrožení jednoduše kvůli neznalosti zacházení s IT:

- **Hesla**
  Dobré heslo je v nejlepším případě těžko zapamatovatelné, což je samozřejmě nepraktické. Mnoho lidí stále používá hesla, která jsou příliš slabá. **12345** je například slabé heslo. Heslo **UfNS3-? SssDa-hUdk&** už vypadá trochu jinak. Čím více různých symbolů, speciálních znaků, čísel a písmen, tím lépe. Ale ne v případě, že je heslo zaznamenáno znovu na kus papíru a nalepeno přímo na obrazovku počítače.

  Jak vidíte, že najít vhodné a bezpečné heslo, které si dotyčná osoba zapamatuje, není tak snadné. Zejména proto, že mnoho systémů vás pravidelně vyzývá k změně hesel a stejné heslo se nedoporučuje používat víckrát než jednou.

Exkurz
Existuje tzv. **správce hesel**, který lze použít jak soukromě, tak i ve společnostech. Jedná se o programy, které mohou generovat a ukládat zabezpečená hesla pro weby nebo jiné programy. Samotný program je zabezpečen tzv. **hlavním klíčem**, tj. jedním hlavním heslem.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Výhody a nevýhody jsou zřejmé: můžete použít celou řadu různých zabezpečených hesel a nemusíte si je jednotlivě pamatovat. Pokud je však hlavní klíč odhalen, lze získat přístup ke všem uloženým heslům. Správce hesel je bezpečný pouze v případě, že hlavní heslo je silné a pokud možno pravidelně měněné.

Problém je však také předávání hesel, což nemusí být úmyslně nedbalé. Chcete pomoci kolegovi a rychle mu dát svůj vlastní přístup do systému. Nebo správce systému požaduje heslo pro kontrolu. To může vést ke kritickým situacím, zejména pokud se jedná o lidi, kteří tímto způsobem záměrně hesla ukradnou.

- **Přines si vlastní zařízení (anglicky „Bring Your Own Device“)**
  "Přines si vlastní zařízení" - to neznamená divoký vánoční večírek ve firmě, ale spíše nošení vlastních zařízení, jako jsou externí pevné disky, USB klíče, chytré telefony a podobně do firmy. Pokud jsou interní informace společnosti uloženy nebo upravovány na těchto zařízeních, pak interní IT bezpečnost opravdu nedokáže pomoci. To je potřeba si obzvlášť uvědomit v případě tzv. „home office“, tj. práci pro firmu z domova.

  Mimochodem, paměťová média mohou být někdy záměrně třetími stranami „připravena“ s malwarem a poté distribuována lidem, kteří pracují například pro určité společnosti. To se děje například na profesionálních veletrzích, kde jsou USB klíče často rozdávány.

- **Instalace neautorizovaných aplikací**
  Váš firemní notebook je příliš pomalý, takže se o něj „staráte sami“ pomocí instalace antivirových programů a dalších věcí. Nebo rádi hrajete ve svém volném čase v práci hry a stahujete malware do svého firemního počítače. To také může kvůli nedostatečnému věnování pozornosti vést k ohrožení IT bezpečnosti.

Toto jsou v podstatě největší hrozby pro IT bezpečnost. Jak již bylo vysvětleno, zcela nepředvídatelné události mohou samozřejmě také ohrozit IT, například přírodní katastrofy, jako je požár, zásahy bleskem nebo povodně, mohou zcela ochromit nebo zničit počítačové systémy.

Zapamatujte si

O skutečné hrozbě, co se IT bezpečnosti týče, mluvíme v případě, **když se interní zranitelnost setká s externí hrozbou**. Takovou hrozbou může být úmyslný útok nebo může být neúmyslně způsobena lidmi nebo „vyšší mocí“ jako jsou přírodní katastrofy.

Úmyslné útoky:

- Malware jako jsou viry, počítačoví červi a trojské koně
- Fyzické vniknutí a krádež nebo manipulace s informacemi nebo počítačovými systémy
- Krádež identity nebo vydírání pomocí phishingu, ransomwaru a odepření služby.

Neúmyslné nebezpečí:

- Slabá nebo předaná hesla
- Používání soukromých zařízení v prostředí firmy
- Instalace neautorizovaných aplikací

Vyšší moc

- Přírodní katastrofy, které následně vedou ke zničení nebo ochrnutí počítačových systémů

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

5.5 Opatření IT bezpečnosti

IT zabezpečení nabízí různá opatření nejen po technické stránce. **Informovanost lidi o malwaru nebo škodlivému nevědomému chování ve firmě nebo jejich soukromém životě** už obvykle znamená hodně.

Za tímto účelem jsou často nabízeny školení a workshopy, které mohou zabránit tomu či onomu IT problému ve vašem soukromém životě. V rámci společností jsou někdy navrženy celé strategie tak, aby integrovaly zabezpečení IT do procesů komplexně a co nejúplněji. To však nemůže fungovat bez předchozího zvýšení povědomí zaměstnanců.

Investice do informování a zvyšování povědomí jako taková však samozřejmě nestačí. Co tedy ještě IT bezpečnost zahrnuje?

Software
V první řadě samozřejmě existuje tzv. **antivirový software**, který automaticky kontroluje váš IT systém a hledá, zda se v něm nevykytuje malware. K tomu by mělo docházet v krátkých, pravidelných intervalech a je užitečný v soukromém i podnikatelském prostředí. Bezpečnostní mezery a škodlivé programy, které chceme stáhnout z internetu, tak mohou být včas detekovány a zakázány.

Jak již dobře víte, stále se na něj ještě nelze stoprocentně spolehnout. Někdy jednoduše malware jako takový není detekován nebo je zabezpečený software identifikován jako malware a poté je automaticky odstraněn a počítač přestane fungovat. Slepá důvěra v antivirový systém se proto nedoporučuje.

Takzvané brány **firewall** jsou také oblíbeným prostředkem IT bezpečnosti v soukromém i obchodním prostředí. Zabývají se síťovými připojeními IT, například sítí WLAN. Dokáží detekovat a zabránit neoprávněnému přístupu zvenčí přes síť. Ve většině případů jsou takové brány firewall již integrovány do antivirových softwarových produktů.

Sandbox (česky „pískoviště“) je něco obzvláště zajímavého, nejen pro děti. V oblasti IT zabezpečení představuje program, který uzamkne malware. Tento relativně nový koncept je zvláště účinný pro speciální typy dat. Například dokumenty PDF se otevřou v samostatném „sandboxu“ odděleně od ostatních programů. Pokud je soubor PDF poškozen, v nejhorším případě je napaden pouze sandbox a zbytek systému je ušetřen.

Použití odlišných softwarů a někdy i důvěra v menší poskytovatele se může vyplatit, mimochodem, **čím rozmanitější je systém IT, tím obtížnější je prolomit jej jako celek**. Útoky hackerů někdy postihují nejznámější antivirové softwarové společnosti jednoduše proto, že jsou nejobvyklejší.
Kontrola přístupu
Kontrola přístupu neznamená pouze příliš dlouhé heslo. Společnosti si v tomto případě navzájem pomáhají s různými uživatelskými právy. **Pouze velmi málo lidí ve společnosti má přístup ke všem údajům**, které jsou obvykle omezené a rozdělené podle funkce ve společnosti.

Lze také zavést **omezený přístup k internetovým stránkám** nebo prevenci před externími softwary na firemních počítačích. WLAN ve firmě může být také navržena tak, aby bylo možné stahovat a používat pouze velmi omezený výběr aplikací a programů.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Kromě toho existuje také možnost zabránit „aktivnímu obsahu“ - tímto způsobem je vypnut samočinný software (často se jedná o pomocné programy), což může být také účinné v použití proti možnému malwaru. Zde uvedená opatření se samozřejmě spíše uplatní v obchodním kontextu. **Kryptografie** neboli šifrování dat může být použita pro obchodní i soukromé účely. To znamená, že přístup k datům je nejen zabezpečen heslem, ale samotná data jsou také „šifrována“.

Exkurz
Koncové šifrování dat a informací Koncové šifrování (angl. „end-to-end encryption“, zkr. E2EE) je běžným standardem v kryptografii dat. V tomto případě používá odesílatel i příjemce dat šifrovací kód. Zprávy nebo obrázky jsou zaslány odesílatelem. Šifrovací kód však automaticky změní data zprávy na nepochopitelné posloupnosti čísel a symbolů. Příjemce je obdrží a zprávu nebo obrázek dokáže přečíst v původní podobě opět díky dešifrovacímu klíči. Tento proces jednoduše slouží k tomu, **aby data, která mohou být v průběhu odesílání zachycena, nemohla být přečtena a uvedena do kontextu** a zůstala tak pro třetí stranu nepochopitelná.

Zálohy a aktualizace
Pravidelná aktualizace softwaru také samozřejmě pomáhá. Čím starší je software, tím dříve jsou objeveny jeho slabiny. Zejména operační systémy a antivirové programy by měly být co nejdříve aktualizovány, protože největší hrozbu představují externí přístupy.

Proti ztrátě dat může samozřejmě pomoci pouze jedna věc (například pokud je počítač poškozen nebo odcizen): pravidelné zálohy, tj. vlastní kopírování dat a informací, nejlépe oddělené od IT systému na externím pevném disku nebo na takzvaném „cloudu“. Cloudové systémy jsou externí servery a úložiště, které jsou dostupné přes internet. Zde lze zálohovat také automaticky, ale samozřejmě opět existuje riziko, že se samotný poskytovatel cloudu stane obětí IT útoku.

Zapamatujte si
Pouhá informovanost lidí o správném zacházení s IT bezpečností, ať už v soukromí nebo v podnikovém prostředí, se sama o sobě vyplatí. Existuje také řada bezpečnostních opatření v oblasti IT: **Software** • Antivirové programy • Firewall • Sandboxy • Rozmanité sestavení IT systému **Kontrola přístupu** • Různá uživatelská oprávnění • Omezený přístup k webovým stránkám a internetovým programům • Kryptografie **Dodatečná opatření** • Pravidelné zálohování • Poslední aktualizace

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

5.6 Shrnutí

IT bezpečnost je podoblastí informační bezpečnosti a představuje všechna ochranná opatření při zpracování a ukládání dat v IT systému v soukromém i podnikovém sektoru. To zahrnuje **počítačovou bezpečnost, ochranu údajů, zálohování dat a bezpečnost dat.**

IT bezpečnost do značné míry závisí na **současném technologickém vývoji**. Především je nutné rychle reagovat na změnu, abychom mohli použít vhodná protiopatření. Ve všech oblastech činnosti musí být splněny **tři základní cíle ochrany**:

diskrétnost - integrita – dostupnost

K dosažení těchto cílů ochrany je **hlavním úkolem IT bezpečnosti identifikovat slabiny v systémech a odpovídajícím způsobem je odstranit**. Skutečnou hrozbou ve smyslu IT bezpečnosti je situace, kdy se interní zranitelnost setká s externí hrozbou.

Takovou hrozbou může být **úmyslný útok** za účelem krádeže nebo manipulace s daty (např. prostřednictvím malware přes internet nebo fyzickým vloupáním do IT oddělení společnosti).

IT systém však může být **ohrožen i neúmyslně**, například slabým heslem nebo přírodními katastrofami, při nichž dojde k poškození počítačových systémů.

Informovanost lidí o správném zacházení s IT bezpečností může pomoci jak v soukromém, tak i v podnikovém sektoru. Kromě toho existují **ochranné softwary, omezení přístupu** a další bezpečnostní opatření v oblasti IT, která mohou minimalizovat potenciální hrozby.

Co-funded by the Erasmus+ Programme of the European Union

Tento projekt byl realizován za finanční podpory Evropské unie. Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.