Zabezpečení přístupu k datům

Kurz Vás seznámí se základy bezpečného chování v kyber světě. Nastíní problematiku hesel, přístupových práv a seznámí Vás s nejvíce používanými podvodnými praktikami ze strany počítačových pirátů.

Cílem studia je seznámit studenty s bezpečným chováním na Internetu a v kyber prostředí.

Obsah

1 | Informace ke studiu

Vzdělávání v oblasti základních registrů a dalších kmenových projektů eGovernmentu, registrační číslo projektu: CZ 1.04/ 4.1.00/A3.00004

Tento kurz byl vytvořen v rámci projektu financovaného z prostředků Evropského sociálního fondu ČR, operačního programu Lidské zdroje a zaměstnanost a je součástí souboru devíti eLearningových kurzů:

1. Použití základních registrů
2. Agendové informační systémy a Informační systémy veřejné správy
3. Služby soukromoprávního sektoru
4. Zabezpečení přístupu k datům
5. Zabezpečení připojení AIS
6. Programové období 2014 - 2020
7. CzechPOINT@office
8. Open data
9. Datové schránky

1.1 | Význam piktogramů

V kurzu se budete setkávat s piktogramy, které vám usnadní orientaci v textu, upozorní vás na důležité informace, právní předpisy, doporučenou literaturu apod. Piktogramy jsou společné pro všechny kurzy, je tedy možné, že s některými z nich se v tomto kurzu nesetkáte. Přesto je vhodné se před zahájením studia se všemi seznámit.

	odkaz na paragraf		rozmysli se
	kontrolní otázky		doporučená literatura
	shrnutí učiva		důležitá informace
	dobrý tip		odkaz na právní předpis

1.2 | Použitá terminologie 1/2

Aktualizace (anglicky update) – Soubor dat nebo program, který se používá pro zlepšování funkcí počítačového programu. Např. pro „seznámení“ antivirového programu s novými viry, aby je mohl rozeznávat.

Backdoor – Zadní vrátka. Program, který po nainstalování do počítače tento „otevírá“ pro další útoky: např. stahuje z internetu ovládací software či vypíná firewall (a počítač se tak stává zranitelnějším).

BFU – Zkratka z anglického **Bloody Fucking User**. Hanlivé označení běžného uživatele počítačové techniky. Používáno nejčastěji správci, administrátory a dalšími „neomylnými“ uživateli.

Blacklist – Černý seznam, tedy seznam zakázaných úkonů či atributů. Např. seznam pornostránek nebo odesílatelů, od nichž si nepřejeme dostávat e-maily.

CERT – zkratka z anglického Computer Emergency Response Team. Obdobně jako CSIRT (viz níže) tým určený pro předcházení a koordinaci řešení kybernetických incidentů. Provozovatelem vládního CERT je Národní centrum kybernetické bezpečnosti (NCKB), které představuje součást Národního bezpečnostního úřadu.

Cracker - Člověk, který neoprávněně využívá nedokonalostí nebo funkcí počítačových systémů, aby do nich pronikal. Cracker je správnější výraz pro „hackera“ (a mnoho skalních příznivců IT dodnes mezi hackery a crackery rozlišuje, i když v obecném povědomí je za „darebáka“ považovaný též hacker).

CSIRT – zkratka z anglického Computer Security Incident Response Team. Podobně jako CERT představuje tým určený pro koordinaci a řešení kybernetických útoků. Provozovatelem národního CSIRT pro Českou republiku je sdružení CZ.NIC.

Červ – Zvláštní případ škodlivého kódu (viru), který ke svému šíření využívá počítačovou síť. Šířit se může buď automaticky (často i pouhým otevřením infikované e-mailové zprávy) nebo s pomocí uživatele (např. poklikání na přílohu e-mailu).

EULA – **End User Licence Agreement**. Licenční smlouva s koncovým uživatelem. Ony dlouhé, nezáživné a bohužel důležité podmínky používání software, které skoro nikdo nečte při instalaci počítačového programu. Dohoda mezi výrobcem a uživatelem programu.

Falešný poplach - Situace, kdy bezpečnostní systém vyhodnotí korektní stav jako nebezpečný. Např. když oznámí, že nějaká aplikace obsahuje virus – a ona je ve skutečnosti „čistá“.

Firewall – Program, který slouží k filtraci žádaného a nežádoucího obsahu. Může se používat pro celou síť nebo pro jednotlivé počítače. Chrání před mnoha (nikoliv přede všemi! – např. virus putující v e-mailové poště považuje za korektní, protože hodnotí jen provoz – a e-mail tak z hlediska firewallu korektní je) typy útoků.

1.3 | Použitá terminologie 2/2

Greyware – Zkrácena verze anglického „grey software“ – šedý software, šedá zóna software. Jako greyware jsou označované aplikace, které mohou být užitečné i škodlivé – záleží jen na způsobu použití.

Hacker – V původním významu špičkový specialista, který upravoval programy tak, aby pracovaly přesně dle zadání. Časem ale dostalo toto slovo přesně opačný nádech: dnes jím označujeme jakéhokoliv počítačového útočníka.

Hoax – Smyšlenka, nesmyslná zpráva. Zpravidla řetězový e-mail využívající neznalosti nebo naivity uživatele, který jej dále rozesílá. Doporučené čtení: www.hoax.cz

Lama – Česká verze anglického „lamer“ (flákač). Hanlivé označení uživatele počítačů, který je (dle subjektivního mínění) se svými znalostmi a schopnostmi podprůměrný.

Malware – Zkrácená verze anglického „malicious software“, škodlivý program. Obecné označení všech škodlivých kódů, kterým se lidově (byť odborně nepřesně) říká „viry“.

NCKB – zkratka z českého výrazu „Národní centrum kybernetické bezpečnosti“, které je součástí Národní bezpečnostního úřadu (NBÚ) a sídlí v Brně. Úlohou centra je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

Phishing – Zkomolenina anglického „fishing“, což znamená rybaření. Ve světě počítačů metoda prachobyčejného podvodu, jejímž cílem je přimět uživatele k tomu, aby dobrovolně vydal útočníkovi citlivé údaje (typicky přístupová hesla k internetovému bankovnictví).

Spam – Nevyžádaná elektronická pošta. Různé obchodní aj. nabídky, o které jsme nikdy neprojevili zájem a které nám „zaplevelují“ naši e-mailovou schránku.

Spyware – Zkrácená verze anglického „spy software“, sledovací (či špionážní) software. Jedná se o škodlivý program, který slouží k tajnému monitorování uživatelů. Může být použitý např. k získávání hesel, ke shromažďování informací o systému...

Trojský kůň (někdy též **trojan**) – Program, který má kromě hlavní formálně deklarované funkce ještě další funkci, která je ovšem před uživatelem skryta – a s jejíž instalací by nejspíše nesouhlasil, kdyby o ní věděl. Častý způsob „vpašování“ škodlivých kódů do počítače: útočník je „zabalí“ do nějakého jakoby užitečného obsahu.

Virus – Typ škodlivého kódu, který se šíří sám bez vědomí uživatele. Nejde tedy o všechny nebezpečné programy obecně, ale jen o určitou skupinu – mezi lidmi se ale toto označení vžilo pro jakýkoliv nechtěný program, který vyvíjí jakoukoliv škodlivou činnost.

Whitelist – Seznam povolených aktivit či adresátů. Lze vytvořit např. whitelist webových stránek, na které mohou uživatelé internetu, nebo whitelist e-mailových adres (tedy seznam e-mailů, ze kterých nechodí spam).

Záplata (**patch**) – Záplatování je proces, při kterém jsou odstraněny z programů známé chyby a nedostatky. Záplata je pak blok počítačových dat nebo program, který umožňuje záplatování provést.

2 | Legislativní základy

2.1 | Úvod

Jede pán autem, které se najednou zastaví. Naštvaný řidič nechá vůz odtáhnout do servisu. Mechanik zvedne kapotu, pokývá hlavou, vezme kladivo a jednou do motoru třískne. Ten hned naskočí.

„Co jsem dlužen," ptá se řidič.
„125 dolarů," odpovídá mechanik.
„Cože? Za jednu ránu kladivem 125 dolarů!?!"
„Ta rána je za pět dolarů. Sto dvacet je za ´vědět kam´."

A takto je to s celou informační bezpečností. Statistiky ukazují (následující čísla jsou z Verizon 2012 Data Breach Investigations Report), že 96 procent útoků ve světě počítačů bylo provedeno „velmi jednoduše". A naopak: 97 procentům útoků jde „velmi jednoduše" zabránit.

V obou případech totiž stačí jedno jediné.

Vědět, kam upřít pozornost.

2.2 | Legislativa

Zkušenost nám ukazuje, že jsou dvě hlavní hybné síly, které nás přimějí „něco vykonat".

- První je prospěch – člověk (organizace) bude dělat něco tehdy, když z toho bude něco mít. Finanční zisk, osobní potěšení, společenské uznání apod.
- Druhou hybnou silou je legislativa – člověk (organizace) bude dělat něco, když to bude mít nařízeno, nebo naopak nebude něco dělat tehdy, když to bude mít zakázáno.

Problém počítačové bezpečnosti obecně je v tom, že **nemá přímý a okamžitý vyčíslitelný efekt**. Na typickou otázku nadřízených či managementu „jakou návratnost v horizontu tří let bude toto bezpečnostní opatření mít?" se opravdu špatně odpovídá. Na druhé straně si spousta organizací začíná hodnotu elektronických dat a reputace uvědomovat a ví, že otázka je ve skutečnosti postavena jinak: **„O co všechno můžeme přijít, když budeme bezpečnost ignorovat?"**

Na mnoha místech se pak nedá spoléhat pouze na lidskou čestnost, ale je dobré podpořit rozhodování i kvalitní legislativou. Což je ale často kámen úrazu, protože rozvoj informačních technologií je nesmírně překotný. Naproti tomu legislativa je neskutečně pomalá, těžkopádná a zraje nesmírně dlouho. A navíc musí být produktově a technologicky neutrální.

Svědčí o tom třeba **historická zkušenost** z tehdejšího socialistického Československa, kdy si represivní složky v sedmdesátých a osmdesátých letech nevěděly s prvními zločiny páchanými pomocí počítačů rady (tehdy se vyskytovaly jen ve firmách a školách). Stávající paragrafy prostě nešlo na virtuální svět nul a

jedniček „napasovat“. Ovšem kdo chce psa bít, hůl si najde, a tak byli první počítačoví útočníci odsouzeni za „neoprávněný odběr elektrické energie“!

 Problematiku informační bezpečnosti řeší v České republice celá řada legislativních dokumentů.

Tím nejdůležitějším je nový Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který nabyl účinnost od 1. ledna 2015 a dvě související prováděcí vyhlášky:

- 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích

Vzhledem k významu, který tento zákon má se na něj podíváme podrobněji v samostatné kapitole.

Mezi další právní předpisy zabývající se informační bezpečnosti a ochranou informací lze zařadit především:

- Zákon č. 365/2000 Sb. o informačních systémech veřejné správy
- Zákon č. 101/2000 Sb., o ochraně osobních údajů.
- Zákon č. 151/2000 Sb., o telekomunikacích.
- Zákon č. 127/2005 Sb., o elektronických komunikacích.
- Zákon č. 227/2000 Sb., o elektronickém podpisu.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti.
- Zákon č. 563/1991 Sb., o účetnictví.
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě.
- Plus další legislativa (vyhlášky, standardy atd.) MV ČR (MI ČR), ÚOOÚ a NBÚ.
- Mezinárodní normy a standardy (např. ISO).

A to není vše: neodmyslitelnou součástí informačních technologií je hardware a služby. Ty řeší Občanský zákoník nebo Zákon o obchodních korporacích.

2.3 | Zákon o kybernetické bezpečnosti

Nejdůležitější předpis v oblasti ochrany dat představuje **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti,** který nabyl účinnosti 1. ledna 2015. V duchu hesla „*Těžko na cvičišti, lehko na bojišti*“ se zákon snaží o to, aby jednotlivé úřady (a provozovatelé další infrastruktury) byly co nejlépe připraveni na možné útoky a nejlépe, aby hackerům a dalším živlům nedali šanci se do jejich systémů vůbec dostat.

Základní principy zákona

Lepší představu o tom, jak zákon funguje lze získat při pohledu na jeho čtyři základní principy, mezi které patří:

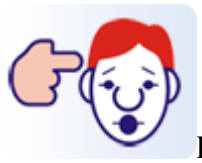
- **Důvěra** – vzájemné sdílení informací (vládní CSIRT), hlášení kybernetických incidentů. Pokud někdo zjistí útok, bude mít povinnost **nahlásit kybernetický incident.**
- **Zodpovědnost** – nikdo nezná IS lépe než jeho provozovatel/správce. Povinnost **zavést bezpečnostní opatření** a zajistit bezpečný chod (dokumentace, nastavení práv, odpovědnost…).
- **Spolupráce** – jen NCKB bezpečnost nezajistí, je třeba navázání spolupráce s dalšími subjekty.
- **Přiměřenost** – v návaznosti na závažnost incidentu může být **vyhlášen až stav kybernetického ohrožení**.

Povinnosti uložené zákonem

Zákon úřadům ukládá celou řadu povinností. Jejich splnění mají na úřadě na starosti konkrétní pracovníci jako **manažer, architekt či auditor kybernetické bezpečnosti**. Ti mají na starost správné nastavení systémů a včetně hlášení incidentů a Vás by měli s jednotlivými opatřeními zanesených ve vnitřních směrnicích seznámit.


Pro vás může být praktickým důsledkem např. nutnost pravidelné změny hesla či nutnost hlášení k vybraným systémům rovněž pomocí USB klíče, nikoliv jen uživatelského jména a hesla, které byste rozhodně neměli nechávat napsané na žlutém papírku nalepeném pod klávesnicí.

2.4 | Mantinely a problémy legislativy


Legislativa ovšem má své mantinely. Může přivést bezpečnost tam, kde dosud není. Realita legislativy je ale zpravidla taková, že když se něco musí udělat, tak se to prostě „nějak“ udělá. Ale neudělá se to tak, aby věc fungovala, nýbrž tak, aby byla splněna litera zákona. V takovém případě je samozřejmě otázkou, zdali je provedený úkon smysluplný.

Dalším problémem je, že **legislativa** je často bezzubá. Což znamená, že sice **ukládá povinnost, ale už neřeší, co se stane, když tato povinnost není dodržena**. Ona „bezzubost“ je často i důsledkem krátké historie oboru a překotných změn: než dojde ke schválení nějaké legislativy, svět informačních technologií je někde jinde. Stačí se podívat na pět nejnavštěvovanějších stránek na světovém internetu: čtyři z nich vznikly v posledních deseti letech (!), jen pátá (Google) je o něco málo starší.


Pozor, toto však **rozhodně neplatí** pro **zákon o kybernetické bezpečnosti**, za jehož porušení je možné uložit **pokutu až 100 000 Kč**.

Dále se některé věci ve světě informačních technologií **špatně prokazují**. Když už se podaří vystopovat spojení ke konkrétnímu zařízení, tak je **následně nutné prokázat** (a dokázat), kdo u něj skutečně fyzicky seděl.

 To jsme ještě nezmínili jednu z největších překážek, kterou je skutečnost, že **internet nezná hranice**. Dokážete si představit, že proti Vám jako jedinci bude provedený útok například z Argentiny, afrického Burundi nebo Severní Koreje? Co budete dělat, abyste se domohli svého práva? A co asi bude (může...) dělat policie nebo soud? Jistě, právo je na vaší straně.

Dále je to **nízké právní povědomí**. Svět je pak plný „babských rad“ nebo amatérských výkladů práva, jak legislativu obejít. Nebo naopak, jak ji vlastně dodržovat. A to už nemluvíme o nekonečných změnách legislativy: třeba Zákon o elektronickém podpisu byl po svém přijetí během šesti let dvanáctkrát (!) novelizován. Pokud někdo vážně uvažoval o používání elektronického podpisu, tyto neustálé změny (a z nich vyplývající nejistota ohledně budoucího vývoje) ho musely spolehlivě odradit.

 K neradostné situaci pak přispívá i **nedostatečná specializace advokátů a právníků**. Rozvodové řízení je přece jen jednodušší a výdělečnější. V informačních technologiích je totiž třeba znát nejen legislativu, ale mít přehled i o technologických aspektech věci. Takový právník (podotýkáme, že musí zvládat národní i mezinárodní právo!) je pak napůl IT specialistou: v Česku bychom podobě erudované specialisty spočítali na prstech jedné ruky ne příliš zručného tesaře.

Zkrátka a dobře: legislativa může pomáhat, ale v žádném případě není všelékem.

3 | Bezpečnostní hrozby

3.1 | Informační bezpečnost a finanční ztráta

Staré dobré úsloví praví, že nejlepší pomocnou ruku najdeme na konci svého ramene. V informační bezpečnosti to platí dvojnásob. **Žádná legislativa nezabrání útokům na naše počítače** (mobily, tablety...), žádná legislativa nevyřeší naše problémy.

Nejprve si pojďme zodpovědět otázku **„proč bychom vlastně měli na počítačovou bezpečnost klást důraz?“**

Velmi často můžeme slyšet, že

- nějaký virus vlastně není problém
- u mě v počítači by útočník těžko co hledal
- bez antivirového programu dá velmi slušně žít

Zkrátka, že si můžeme dovolit informační bezpečnost ignorovat.

Prvním a nejpodstatnějším důvodem je **finanční ztráta**. Třeba v případě mobilu napadeného virem: uvědomujete si, že každé zavolání nebo odeslání SMSky je finanční transakcí?

Uvažujte jako útočník (a toto pravidlo si zapište za uši!): nebylo by príma do mobilního telefonu nainstalovat vlastní škodlivý kód, který by pak posílal SMSky nebo bez vědomí uživatele volal na nějaké mnou vlastněné a vysoce zpoplatněné číslo třeba na Kajmanských ostrovech?

3.2 | Napadení počítače

U napadeného počítače je zase možné napadnout **internetové bankovnictví**: víte, že existují **viry**, které při odeslání příkazu k úhradě z počítače do banky **změní číslo účtu**? Vy pak jen sdělíte autentizační kód (který vám přijde pomocí SMS zprávy) – ale **kontrolujete třeba číslo účtu v autentizační SMSce uvedené?** Tedy číslo, na které nakonec skutečně obnos odesíláte.

A co třeba **webové kamery**? Máte jistotu, že se Váš mobil, počítač, notebook či tablet skrze ně „nekouká“ do Vašeho soukromí?

Na internetu jsou stovky a tisíce stránek, které nabízejí fotografie nebo videosekvence nic netušících převlékajících se (zpravidla) uživatelek. Nejde jen o nějaké „hambaté obrázky“ – víte, že jste pak navždy **vydíratelní**? **Únosy webových kamer** jsou mnohem častější, než si připouštíme a

na internetu jsou **celá tržiště**, kde se nabízí **na prodej přihlašovací údaje** k hacknutým kamerám. Čím atraktivnější majitelka, tím vyšší cena...

Dále nezapomínejme, že útočníkům vůbec **nemusí jít o nás, ale o náš počítač** – hardware a připojení. Opět: uvažujte jako útočník . Když budete rozesílat třeba nevyžádanou elektronickou poštu (spam), proč byste si kupovali své počítače a platili internetové připojení?
Není lepší si hardware i komunikační linku „vypůjčit“ od hloupých uživatelů internetu? Nehledě na to, že když pak vystane nějaká sankce (zákonná, ze strany poskytovatele internetu...), proti komu míří? Proti skutečnému pachateli, nebo proti oběti, jejíž počítač zneužil?

Navíc útočníci často **„unesené“ počítače** (jak asi poznáte, že váš počítač je „sluhou dvou pánů“? – nepoznáte) spojují do větších sítí. Pro úplnost: uneseným počítačům se říká zombie, sítím pak botnety. A tyto sítě mají ohromné schopnosti: tisíce spojených počítačů je přece superpočítač! A takový superpočítač může lámat hesla nebo provádět útoky. Jinými slovy: váš domácí počítač se (bez vašeho vědomí, podotýkáme) stává součástí zločineckých aktivit.

3.3 | Nelegální data


Když už se někdo dostane **do počítače**, pak do něj může i **odkládat svá data**. Čtěte: **nelegální data**.

Třeba v České republice je zakázáno i pouhé držení dětské pornografie se sazbou až dva roky nepodmíněně. Uvažujte jako útočník: budete s tímto „Damoklovým mečem“ nad hlavou dětskou pornografii přechovávat ve svém počítači, nebo si ji odložíte na bezpečné místo do cizího počítače? (Z hlediska rozložení rizika pochopitelně několik kopií do cizích počítačů.) Když pak policie provádí vyšetřování, nekončí v počítačích skutečného pedofila (nedá se mu nic prokázat), ale v počítačích, do kterých se útočníci „nabourali“. Ano, v konečném důsledku vás neodsoudí, jenom se zdesíte, cože jste v počítači přechovávali.

Ale uvědomte si souvislosti: policie vám v první fázi vyšetřování zabaví všechny počítače, mobily a datové nosiče.

3.4 | Citlivá data

Nezapomeňte také, že **každý počítač obsahuje citlivá data**.

I řemeslník nebo malá firma, kteří nosí znalosti a vědomosti v hlavě, mají v počítači **seznamy svých klientů**. Nebo **účetnictví.**

Vždyť je dobré vědět, za kolik nakupuje konkurence nebo jak vysokou nabídku do soutěže předkládá!

I **na úřadech** je co „skrývat“: počítače obsahují **databáze** (nebo alespoň dokonce přístupy k nim) **plné osobních údajů.** Ty jde zneužít miliónem způsobů.

Existují **způsoby, jak založit účet** (a následně si na něm vzít nemalý úvěr) **pouze se znalostí osobních údajů,** bez nutnosti osobně zavítat na pobočku banky či úvěrové společnosti!


Takže **jméno, příjmení, adresa a kontaktní údaje mohou mít v nesprávných rukách cenu zlata.**

3.5 | Zodpovědnost k počítačovým datům


Je vhodné **k počítačovým datům**, která nám byla svěřena, **přistupovat se vší zodpovědností**. Aneb nakládejme třeba s osobními údaji druhých lidí, které máme k dispozici, úplně stejným způsobem, jako bychom chtěli, aby oni nakládali s osobními údaji našimi. Ostatně, internet můžeme

považovat za „věc společnou“: bude přesně takový, jaký si ho uděláme. I my můžeme přispět svou „troškou do mlýna“ k tomu, aby byl bezpečnější – nebo naopak nebezpečnější.

A teď přichází nejdůležitější otázka: **jak to udělat?** Čestně a upřímně si musíme přiznat, že **univerzální recept neexistuje**. Když bude nějaká definice typu „e-mail označený tak a tak je bezpečný“, budou právě útočníci první, kdo toto označení bezpečnosti zneužijí. Jde zkrátka o věčnou hru kočky s myší.

Nicméně jsou různá doporučení (jejich kompletní vyjmenování a vysvětlení pochopitelně mnohonásobně překračuje rozsah tohoto materiálu), která nám umožní zvýšit úroveň bezpečnosti.

Například používání elektronického podpisu zabrání modifikaci odesílané zprávy (třeba vložení viru do odesílané zprávy je právě takovouto modifikací). Šifrování zase brání „odposlouchávání“ pošty během přenosu (jedno ze základních doporučení praví, že do e-mailu bychom neměli svěřovat více, než na běžnou pohlednici). Jsou i další praktiky (ale mají své limity): třeba přijímání e-mailů pouze od prověřených adres (i z nich ale může přijít škodlivý kód stejně jako je takto limitována komunikace s cizími subjekty), využívání antivirové ochrany nebo filtru spamu (ani jedno však nemá a nikdy mít nebude stoprocentní úspěšnost) apod. Ostatně viz úvod: 97 procentům útoků jde velmi jednoduše zabránit.

3.6 | Heslo

Začneme nyní u **hesla**, které bývá často **nejslabším článkem systému**. V současné době představuje heslo základní prvek ochrany přístupu k datům a tak se s ním musíme naučit žít. Často se lze dozvědět, že čím delší heslo, tím lepší.

To je ale ryze technický pohled, lehce odtržený od reality.

- Pokud bude mít uživatel extrémně dlouhé heslo a pokud bude nucený ho často měnit, opravdu si ho bude pro všechny aplikace pamatovat?
- Nebo si ho bude různě poznamenávat (do počítače, na monitor...), či dokonce nařízení obcházet?

Každé bezpečnostní opatření je komplikace, takže i heslo musí být jakýmsi kompromisem.


Jak by takovýto heslo mělo vypadat, stanoví vyhláška č. 315/2014 Sb. o kybernetické bezpečnosti. Podle této prováděcí vyhlášky k zákonu o kybernetické bezpečnosti by každé heslo mělo:

- Mít minimálně 8 znaků
- Obsahovat kombinaci malých a velkých písmen, číslic nebo speciálních znaků jako je např. @ či _


Pro **snadnější zapamatování** hesla je dobré použít následující tip:

- vezměte si nějakou básničku či písničku

- a pak z každého slova vezměte první nebo druhé písmeno: a z nich vytvoříte heslo. **S**kákal **P**es **P**řes **O**ves, **P**řes **Z**elenou **L**ouku... SPPOPZL – jednoduché, zapamatovatelné, neodhadnutelné
- pro zvýšení bezpečnosti ještě doplňte o číslice a využijte velká a malá písmena. SPpo007PZl.

Na první pohled hrůzostrašné, ale ve skutečnosti snadno zapamatovatelné (po dvou písmenech střídáme velká a malá, doprostřed jsme dali snadno zapamatovatelné číslo britského agenta) a zároveň splňující požadavky vyhlášky o kybernetické bezpečnosti.

Podobně jako zubní kartáček by se i heslo mělo pravidelně měnit

Ani sebekomplikovanější heslo však již dnes nedokáže odolat útokům hrubou silou, kdy se jej budou supervýkonné počítače snažit rozlousknout. Čas od času může dojít též k nechtěnému úniku hesel díky některé z bezpečnostních chyb. Např. na začátku roku 2014 se jednalo o chybu tzv. Krvácejícího srdce (The Heartbleed Bug). Právě z těchto důvodů je hesla nutné pravidelně měnit. Vyhláška ke kybernetickému zákonu stanoví jako maximální interval 100 dnů, tj. něco málo přes 3 měsíce.

Až se tak bude administrátor dožadovat toho, abyste opět změnili heslo, věřte, že to není jen jeho výmysl, jak Vám znepříjemnit práci, ale především bezpečnostní opatření vyžadované rovněž legislativou!

Hesla jsou jako zubní kartáček. Často je měňte, nikomu nepůjčujte (nesdělujte).

3.6.1 | Heslo - instruktážní video

https://www.youtube.com/watch?feature=player_embedded&v=9lxzBMRUuFs

3.7 | Administrátorská práva

Když už hovoříme o heslech, jejich prostřednictvím **si přidělujeme/získáváme práva**. Systém dle hesla uživateli dovolí pracovat s nejvyššími oprávněními (jako administrátor) nebo s různými přednastavenými druhy oprávnění. Rozšířeným zlozvykem přitom bývá, že si domácí uživatelé přidělují administrátorská práva – a stejně tak je často přidělují administrátoři v organizacích neoprávněným osobám (tedy takovým, které by je mít neměly). Často se takto řeší i problémy, protože administrátor má přece jen větší pravomoci a lépe se počítač konfiguruje. Proč jsou vlastně administrátorská práva špatná? Špatná nejsou, ale potřebujeme je pouze ve speciálních případech; pro běžnou práci (psaní e-mailu, dokumentů, tvorba prezentací, hraní her, brouzdání na internetu aj.) je vůbec nepotřebujeme. Kdo je ale potřebuje, to jsou útočníci a různé viry. Ano, začíná svítat: **bez administrátorských práv se virus do počítače (v drtivé většině případů) nenainstaluje**. Pokud jste neměli přidělená administrátorská práva, tak se Vás například v roce 2013 netýkala ani jedna chyba v Internet Exploreru. Ano, čtete správně: ani jedna chyba. V ostatních aplikacích či operačních systémech to bylo velmi podobné. Takže rychle pryč od administrátorských práv. Ta jsou skutečně jen na instalaci nových aplikací nebo zásadní změny v systému.

3.8 | e-mail

Další oblíbenou (a zároveň nebezpečnou službou) jsou e-maily. Hlavní **nebezpečí** se skrývá v **přílohách**. Svoji ostražitost bychom však měli zvýšit už v okamžiku, kdy nám v e-mailu přistane podezřelý e-mail a přílohu pak vůbec neotevírat. Jak ale takovýto e-mail poznám a jakými radami bych se měl řídit?

N**eexistuje bezpečná příloha** (dokonce ani bezpečný e-mail: virus se může skrývat přímo v jeho těle, takže dobře přemýšlejte, zdali opravdu musíte otevírat vše, co vám přijde do schránky). Nezáleží na tom, odkud přijde, jak se jmenuje nebo jakou má ikonku.
Snažte se rozhodovat podle „druhotných znaků“:

- Třeba když vám někdo, s kým si komunikujete výhradně česky, píše výzvu k otevření přílohy v angličtině.
- Nebo když jsou okolnosti jinak podezřelé: je príma vyhrál milión v loterii, ale jak je to pravděpodobné, když jsme si nikde nevsadili?
- Stejně tak se vyhněte otevírání a přeposílání různých legrácek typu flashových her, legračních prezentací nebo i prachobyčejných wordovských souborů.

Internetoví podvodníci jsou ale čím dál tím rafinovanější a své taktiky rychle mění. Místo výher milionů se tak může stát, že ve své schránce naleznete e-mail s výzvou k zaplacení relativně malé částky (do 10 000 Kč). Záminkou může být např. nezaplacený účet za roaming v zahraničí nebo objednávky z e-shopu. Již dávno také neplatí, že všechny podvodné e-maily jsou psané hodně špatnou češtinou.

Podlehnout otevření přílohy v podezřelém e-mailu byste neměli podlehnout ani tehdy, pokud Vám v e-mailu hrozí exekucí. Věřte, že exekutoři si sice často snaží práci usnadnit, výzvy e-maily však neposílají! Aktuální varování před podvodnými e-maily můžete nalézt např. na stránkách Národního bezpečnostního týmu CSIRT.CZ (https://www.csirt.cz/news/security/).

Samozřejmě, že se viry pokouší za podobné soubory často maskovat. A navíc se chráníte tím, že si nezvyknete na všechno bezhlavě klikat. Chce to trochu vůle a sebeovládání, ale právě disciplína a opatrnost jsou nejlepší opatření. Věřte nám, že se bez různých životabudičů typu „deset nejroztomilejších psích čumáčků“ opravdu obejdete.

3.9 | Šifrování

Dorozumívat se šifrou může být důležité nejen pro Jamese Bonda nebo fotbalové aktéry známé z „*Ivánku, kamaráde*“, ale pro každého, kdo chce ochránit svá data. Šifra označuje kryptografický algoritmus, který pomůže převést čitelnou zprávu do nečitelné podoby, kterou dokáže rozluštit jen držitel šifrovacího klíče. Dobře si to můžeme představit na známé morseovce. Co znamenají tečky a čárky ví jen ten, kdo tuto šifru ovládá. Při šifrování dat se používají mnohem složitější mechanismy a ten správný klíč obvykle zná jej jedna osoba.

Při ochraně dat se nám může šifrování hodit hned v několika oblastech:

- Šifrování **dat** ať již na pevném disku nebo či USB klíči. Zašifrování dat nás může ochránit především v případě ztráty, či krádeže našeho notebooku nebo přenosného média. Některé programy jako např. bezplatný Truecrypt umožňují dokonce šifrování celého disku, včetně té části, na které je uložen operační systém.
- Šifrování **elektronické komunikace**, především e-mailů, jejichž obsah je během přenosu chráněn před nežádoucím otevřením (vyzrazením) podobně, jako je dopis chráněn obálkou. Pro šifrování e-mailů je využíván elektronický podpis, který nám zároveň poskytne důvěryhodnou informaci o tom, kdo takovouto zprávu odeslal.
- Šifrování využívají rovněž tzv. **VPN sítě** (Virtual Private Network), kde jsou šifrovaná data posílána zvláštním kanálem přes internet. Díky šifrování jsou tato data pro útočníka, který by je někde cestou

odchytil nečitelná. VPN se často používá například pro připojení z domova do sítě na úřadě nebo při přístupu prostřednictvím veřejných Wi-Fi.


Chráněná (šifrovaná) komunikace je též důležitá v případě komunikace dvou informačních systémů, kdy u vybraných informací s vysokým či kritickým stupně důvěryhodnosti je povinnost používat kryptografické prostředky (nebo-li šifrování) povinně dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Minimální požadavky na takovéto kryptografické požadavky jsou obsaženy v Příloze č. 3 Vyhlášky 316/2014 Sb., o kybernetické bezpečnosti.

3.9.1 | Šifrování - instruktážní video

https://www.youtube.com/watch?v=CQFf1UTx2Tw&feature=player_embedded

3.10 | Zálohování

Jeden z Murphyho zákonů říká, že zálohování je operace, kterou nikdy nestihnete včas. Zkušenosti pak napoví, že zálohuje především ten, kdo již někdy o svá data přišel.

Ostatně, **ztráta dat** je tím **hlavním důvodem, proč** bychom měli **zálohovat**. Nezáleží přitom na tom, zda o svá data přijdeme díky vlastní chybě (např. neúmyslným smazáním či zformátováním disku), poškozením média (např. CD), ukradením či díky živelné pohromě jako oheň nebo povodeň.

Jak zálohovat?

Po rozmyšlení jaká data by bylo třeba zálohovat a po výběru vhodného datového úložiště přichází na řadu otázka jak zálohovat.

- Při zálohování na **paměťová média** můžeme využít buďto specializované programy pro vypalování, nebo zálohování, nebo v nejjednodušším případě správce souborů (Průzkumník, Total Commander). V posledním případě je vhodné na datovém úložišti vytvářet pro každou zálohu samostatnou složku, která bude stručně pojmenována včetně data pořízení zálohy. To pak urychlí případnou obnovu dat.


Po skončení zálohování je vhodné médium označit tak, aby bylo jasné, že jde o zálohu a umístit je na známé místo (nejlépe **v jiné místnosti, či objektu**), kde je v případě problémů spolehlivě najdeme a zároveň o něj např. v případě požáru nepřijdeme stejně rychle jako o původní data.

- V případě **online služeb** jako je např. Dropbox je zpravidla jediným krokem nainstalovat pomocný program, ve kterém si pak vybereme soubory, či složky které si přejeme sdílet. Vše ostatní se pak děje automaticky. U různých on-line záložišť (úschoven) často označovaných jako cloud však mějme na paměti, že u těchto dat hrozí riziko jejich zneužití a služby sídlící mimo EU (např. DropBox či Google) se při uchování údajů nemusí řídit evropskými předpisy. Přesto, že u smluvních podmínek často bezmyšlenkovitě odklikáváme náš souhlas, zde se vyplatí podmínky přečíst. Již jen proto, že v některých případech může být v těchto podmínkách ustanovení např. o udělení souhlasu k volnému a bezplatnému šíření Vašich fotografií.


Postupy pro **zálohování na Vašem úřadě** by měla upravovat tzv. Bezpečnostní politika, jejíž vypracování ukládá úřadům vyhláška č. 316/2014 Sb. (vyhláška o kybernetické bezpečnosti). V této politice byste měli nalézt informace o tom, jak či v jakých intervalech probíhá zálohování Vašich pracovních dat.
Další Murphyho zákon říká, že pravděpodobnost poruchy harddisku roste úměrně k množství času uplynulého od posledního zálohování dat. Zálohovat jednou za rok tak určitě nestačí a zálohu našich dat bychom měli provádět pravidelně.


Držme se zlaté zásady: **zálohovat, zálohovat a zálohovat** a o naše data (alespoň ne všechna) už nikdy nepřijdeme!

3.10.1 | Zálohování - instruktážní video

https://www.youtube.com/watch?v=r_SNQv3E3wI&feature=player_embedded

3.11 | Internetové prohlížeče

Samostatnou kapitolou je používání internetových prohlížečů. Snažte se **vyhnout stránkám, které mohou být nebezpečné**:

- stránky s nelegálním softwarem
- MP3 soubory nebo filmy
- s pornografií
- s hackerskými materiály apod.

Jistě, virus může číhat i v regulérní stránce (stále uvažujte jako útočník: vždyť je to největší poklad, když svůj virus dokážete protlačit do důvěryhodného webu!), ale ta pravděpodobnost je mnohem menší.


Do prohlížeče také **neinstalujte vše**, co vám přijde pod ruku. Čím více doplňků, tím větší má útočník „plochu“, do které může mířit. **Více programů** se rovná **větší pravděpodobnost chyby** nebo zanedbání údržby: ostatně to platí nejen pro doplňky do prohlížeče, ale pro programy obecně.
A když už hovoříme o programech: **využívejte jen legitimní zdroje**. Polovina pirátských verzí na internetu obsahuje nějaký virus. Útočníci zkrátka infikují poptávané zboží a parazitují na touze po něm.

Záplaty, záplatování a aktualizace: smiřme se s tím, že programy obsahují chyby. Byť se jejich tvůrci snaží sebevíc, nikdy nedokážou všechny nedostatky „vychytat“ a nikdy nedokážou předvídat všechny situace, které mohou nastat. Proto je **důležité instalovat všechny dostupné opravy**. Bez nich máme v počítači chybu, o které ví naprosto přesně útočník, ale my z pozice obránce ji necháváme neošetřenou.


Nakonec bychom chtěli zdůraznit: **používejte bezpečnostní program** (typicky Něco Internet Security).

- Antivirový program
- firewall
- filtr nevyžádané elektronické pošty
- kontrolu stavu aktualizací...

To všechno jsou funkce, které nám nesmírně usnadní život.

Ale pozor! **Bezpečnostní program není všelékem**, jak se lidé často domnívají. Je to až poslední záchranná brzda, když selže všechno ostatní. Autem také nenajíždíme v plné rychlosti do betonové zdi s tím, že „přece máme air-bagy“.

3.12 | Ochrana mobilních zařízení

Mobilní telefon dnes zdaleka neslouží jen k telefonování či posílání SMSek, ale často i jako „elektronický společník“, kterému svěřujeme a prostřednictvím kterého sdílíme naše životy. Mobil je zároveň často naší vstupní branou do dalšího elektronického světa – do elektronického bankovnictví, ale i e-mailové schránky či systémů na úřadě. Při ztrátě (či odcizení) telefonu pak hlavně myslíme na to, jak obnovit kontakty či ztracené fotografie, méně již na zabezpečení telefonu – ať již před zloději, zneužitím osobních údajů či počítačovými viry.

Jak by měl být služební mobil či tablet ochráněn před krádeží či počítačovými viry by na ministerstvech a dalších správních úřadech měla stanovit tzv. Politika bezpečného používání mobilních zařízení, jejíž vypracování ukládá úřadům vyhláška č. 316/2014 Sb. (vyhláška o kybernetické bezpečnosti).

Přístup cizích lidí či krádež

Stejně, jako jsme zvyklí si chránit pomocí hesla přístup do počítače či e-mailu, měli bychom si chránit mobilní telefon. Minimální ochranu představuje tzv. **PIN kód** skládající se ze čtyř číslic, které bych si měl hned na začátku **změnit**. Tento kód však většinou chrání jen SIM kartu a je vyžadován zpravidla pouze při zapnutí telefonu.

Naše telefony ale zůstávají zapnuté skoro pořád, takže PIN zadáváme málokdy. Proto je nutné mobil **ochránit rovněž dalšími způsoby**, ať již se jedná o číselný kód, spojováním bodů (teček), otisk prstu či sítnice spojený s mrknutím oka.

Při volbě kódu bych určitě neměl volit snadno odhalitelné 1111 či spojit jen tři body, ale zkusit vymyslet komplikovanější heslo, které nebude možné snadno (zejména zkoušením) odhalit. Své heslo bych pak měl držet v tajnosti, nikam si jej nepsat, a když se mnou někdo bude chtít hrát hru „Řekni mi svůj PIN a já Ti zaplatím panáka“, raději si uhradit útratu sám.

Podobně, jako u počítače je pak vhodné nastavit **automatické zamknutí telefonu**. To umožňuje telefon ochránit i tehdy, pokud jej necháme např. ležet na stole v práci či odložíme u návštěvy. Situacím, kdy telefon nemám pod svoji kontrolou bychom se však měli snažit co nejvíce vyhnout a když telefon nechceme stále nosit sebou, tak jej alespoň zavřít do kabelky či batohu. Tím omezíme jak riziko zneužití telefonu, tak jeho krádeže.

Mobilní telefon bychom rovněž **neměli nikomu půjčovat**. Vedle zneužití telefonu např. k hovoru do zahraničí se takovýto člověk může dostat i k mým fotkám či aplikacím včetně internetového bankovnictví a pak převést peníze na svůj účet.


Některé aplikace (např. avast! Anti-Theft či AVG Antivirus) **pomohou v případě krádeže** s identifikací pachatele a jeho rychlejšímu dopadení. Mezi základní funkce takovýchto aplikací patří především zobrazení místa, kde se telefon právě nachází, uzamčení telefonu na dálku tak, aby se zloděj (či nálezce) nedostal k osobním informacím, případně rovnou smazání všech dat nebo upozornění na změnu SIM karty, kdy v případě krádeže telefonu a vložení nové SIM karty, může být nové číslo a poloha telefonu odeslána na zařízení některého z vašich přátel.


Pro snazší identifikaci telefonu je dobré si **poznamenat** jeho **IMEI** (International Mobile Equipment Identity - jedinečný patnáctimístný místný kód používaný k identifikaci každého mobilního telefonu, který je používán v rámci GSM sítě) a sériové (výrobní) číslo.

3.12.1 | Ztráta dat, viry

Ztráta dat

O kontakty či fotky v mobilu však můžeš přijít nejen krádeží či díky viru, ale i tehdy, pokud se tvůj mobil rozbije. Při životnosti některých přístrojů jen lehce nad dva roky (tj. zákonnou záruku) může takováto chvíle přijít velmi brzy. Proto si data z telefonu pravidelně zálohujte do počítače či na paměťové médium.

Viry

Stejně, jako je důležité mít antivirový program na svém počítači, je důležité jej mít i na svém mobilu či tabletu. Přes tato zařízení se dnes připojujeme k internetu stejně často jako přes počítač a proto zde hrozí stejné nebezpečí nákazy virem. Čím dál častěji se setkáváme s viry, které byly speciálně napsány právě pro mobilní zařízení (resp. konkrétní operační systém jako je Android). Zatímco některé takovéto viry dokáží telefon zneužít k útoku na jiný telefon či počítač, další dokážou získat naše osobní informace, např. kontakty a odeslat je neznámo komu. K tomu, aby nám antivirový program dobře sloužil a dokázal odhalit i nejnovějších viry bychom neměli zapomínat na jeho pravidelné aktualizace. Jen díky nim totiž můžeme odhalit ty nejnovější viry.

Antivirových programů pro mobily je dnes celá řada, mnohé z nich jsou pro nekomerční (domácí) použití ke stažení zdarma či dodávány jako součást antivirového programu, který máme doma. Z českých produktů se jedná především o Avast a AVG, tedy programy známé rovněž z prostředí osobních počítačů.

3.12.2 | Operační systém, instalace nových aplikací

Operační systém

Aktualizace systému přináší vedle nových funkcí také opravu bezpečnostních chyb. Pokud se o chybách útočníci dozvědí, a my nenainstalujeme prostřednictvím aktualizací jejich opravu, začnou tyto zranitelnosti útočníci zneužívat a náš mobil je pak snadněji napadnutelný.

Instalace nových aplikací

Mobilní aplikace jsou jedním z největších rizik pro náš mobil. Některé aplikace mohou obsahovat viry, zatímco jiné „jen“ budou odesílat naše data (např. o tom, kde právě jsme a jaké je výrobní číslo. Při instalaci mobilních aplikací bychom tak měli využívat oficiálních tržišť (marketů), jako je Google Play pro Android či App Store pro iPhone a iPad.

Na těchto „tržištích“ správci aplikace před zveřejněním kontrolují včetně toho, zda jsou podepsány digitálním certifikátem autora, který je vytvořil. Z tohoto důvodu bychom nikdy neměli mobilní aplikace z neznámých zdrojů, např. odkazů z e-mailu, kabelem přes počítač či paměťových karet.

Pozor – ani instalace aplikací z oficiálních tržišť nám však nezaručí, že aplikace je 100% bezpečná a už vůbec, že nebude shromažďovat informace (např. IMEI telefonu či naši polohu), které ke své funkcionalitě nepotřebuje.

3.13 | Podvody

Navíc jsou **typy útoků, před kterými žádný technický prostředek neochrání**. Jedním z nich jsou **podvody**. Přitom princip podvodů je v podstatě stejný, ať jsou páchané v reálném světě nebo v prostředí kybernetickém. Naopak: čím méně komplikovaný a technicky náročný útok, tím je vyšší pravděpodobnost úspěchu. Aneb dobrý příběh hraje při získávání lidské důvěry mnohem větší roli než harašení technickými vymožeностmi.

Protože právě o získání důvěry všechny podvody jsou. Jde o to **navodit situaci, která vypadá jako maximálně důvěryhodná** – jako by podvodníkova lež byla pravdou. Platí to, ať hovoříme o bankovních podvodech, o podvodnících sňatkových nebo internetových…

Přitom **internetoví podvodníci mají svoji roli** ovšem poněkud **usnadněnou**. A ruku na srdce: často jim ji usnadňujeme sami slepou důvěrou v některé skutečnosti, které přijímáme tak, jak jsou.


Když nám v reálném světě někdo zatelefonuje, že je z banky a zdali bychom mu nesdělili své osobní údaje a informace potřebné k manipulaci s účtem, vyhovíme mu? Pravděpodobně ne, i kdyby hlasem medovým hovořil. A když nám přijde e-mail od někoho, kdo se za banku vydává s tím, že je nutné vyplnit takový a makový formulář? Často tak bez hlubšího přemýšlení učiníme…

3.14 | Bankovní podvody


Podívejme se blíže třeba právě na ony internetové **bankovní podvody**. Čím si podvodníci budují svoji důvěru? Třeba jen **zprávou** zaslanou **do e-mailové schránky** své oběti, která je **graficky velmi podobná třeba jako web banky nebo obchodu.**

Nicméně tato pouhá podobnost ve většině případů stačí k tomu, aby byla zpráva považována za důvěryhodnou a jako taková akceptována příjemcem. Samozřejmě, že existují i propracovanější metody útoků, ale s nimi se útočníci zpravidla neobtěžují, když značná část uživatelů sedne na lep už těmto jednoduchým podvůdkům.

Problémům se lze vyhnout dodržováním několika **jednoduchých pravidel:**

- ověřujte si, že ten, s kým komunikujete, je skutečně tím, za koho se vydává
- informace (www stránky, telefonní čísla…) si vyhledávejte sami – útočníci vám pro „ověření“ zcela logicky podsouvají údaje podvržené.
- k informacím přistupujte kriticky, nepřijímejte slepě vše, co je vám sděleno.
- komunikujte jen dohodnutými kanály. Banka si neověřuje heslo e-mailem.

3.15 | Sociální inženýrství

Dobře se to sice napíše, ale hůře vykoná. Útočníci totiž často používají neskutečně účinnou metodu nazývanou **sociální inženýrství**. To je vlastně **umění klamu**.
Jeho cílem je vytvořit v člověku nějakým způsobem dojem, že situace je jiná, než ve skutečnosti je. Jinými slovy: **podváděný nepozná, že mu telefonuje nebo e-mailuje nebo ho jinak oslovuje podvodník,** ale na základě některých uměle vytvořených indicií se domnívá, že komunikuje s někým úplně jiným (důvěryhodným). Sociální inženýrství má ostatně kořeny i v klasických podvodech reálného světa: falešní výběrčí doplatků za vodu, plyn či elektřinu jsou velmi jasným příkladem.

Přitom **v kybernetickém prostoru** je sociální inženýrství **zneužíváno více než kde jinde** – díky standardizované komunikaci a díky nesmírně jednoduchému ústupu i špatnému zajišťování stop v globálním médiu, jakým je internet. V zásadě přitom není podstatné, jakým způsobem je sociální inženýrství prováděno, mnohem důležitější je určit, kam směřuje. Tento směr nám následně dá nápovědu o tom, jak se chránit a bránit.


Abychom si názorně ilustrovali nebezpečí sociálního inženýrství pro dnešní uživatele, připomeňme nedávný téměř neuvěřitelný kousek nejmenovaného německého bezpečnostního konzultanta.

Ten od managementu jedné firmy (protože šlo o penetrační test, nebylo její jméno zveřejněno) dostal zakázku na odhalení bezpečnostních slabin. Konzultant se bez větších obtíží (= jen s pomocí své výřečnosti) dostal do firmy, kde se na několik dní „usídlil“ v jedné ze zasedacích místností. Zde ale nebyl zabarikádovaný a po budově se volně pohyboval. Navštívil mnoho kanceláří, serveroven, skladovacích prostor... Využíval interní telefonní systém, obvolával pracovníky a vydával se za zaměstnance interního IT oddělení, čímž z nich „tahal“ hesla a další informace. Z dvaceti oslovených uživatelů přihlašovací jména a hesla poskytlo sedmnáct. Mezitím se vesele stýkal se zaměstnanci, s mnoha si začal tykat. A to včetně ochranky, což mu nakonec umožnilo do budovy „protáhnout“ i svého kolegu, který provedl přímo zevnitř analýzu informačního systému.

Pravdou je, že ač je sociální inženýrství starší, než počítače samy, **jde o techniku neustále a dynamicky se vyvíjející**. Slovo „sofistikované“ v souvislosti s útoky vedenými pomocí sociálního inženýrství je přitom zcela na místě.

Aneb k ošálení uživatelů už nestačí to, co před deseti lety. „Klikni na jakoukoliv přílohu e-mailu“ už nefunguje – nebo alespoň ne tak dobře jako dříve. **Uživatelé jsou opatrnější a poučenější. Ale stále jsou stejně zranitelní**: útočníci to dobře vědí a dělají vše pro to, aby onu obezřetnost otupili.

3.16 | Phishing

A tak si různými způsoby připravují půdu pro to, aby jejich podvod prošel.

Například před dvěma lety se objevil v České republice první masový phishing směřující na zákazníky České spořitelny (jehož strojové překlady typu „Drahoušek zákazník“ vpravdě zlidověly) a naše e-mailové schránky byly zasypané stovkami podobných laciných pokusů o vylákání osobních údajů. Pak náhle ale přišel jiný e-mail. Perfektní styl slohový i grafický, precizní provedení, decentnost sama, nechyběly zpětné kontakty a mnoho dalších „detailů“ – celá zpráva pak byla pojata jako varování klientům od banky před právě probíhající vlnou podvodů. A na první pohled nebyla ani agresivní: požadovala pouze „verifikaci“ e-mailové adresy přistoupením na určenou www stránku (na první pohled vypadala jako oficiální stránka internetového bankovnictví, ale ve skutečnosti směrovala na jiný web). Zde byl uživatel v rámci „verifikace“ slušně a nenásilně požádaný o své přihlašovací údaje včetně bezpečnostního kódu.

Není přitom podstatné, zdali první a druhá vlna útoků byly nějak spojené nebo jen jiná skupina kyberzločinců velmi obratně využila půdu, kterou jim někdo jiný předchystal. Podstatné je právě ono využití rozdělané půdy: po primitivních útocích (které nečiní uživateli problém odhalit) přichází předstíraný a nevtíravý zájem „banky“ (což uživatele pochopitelně potěší). A dokonce se po něm na první pohled nevyžadují žádné citlivé informace – jen ověření e-mailové adresy, a to v zájmu vlastní bezpečnosti!

3.17 | Pharming

Do podobné kategorie sofistikovanějších „dvoustupňových“ útoků patří třeba i **pharming**, což je technologie využívající DNS Cache Poisoning“ – **otrávení uložených DNS záznamů.**
Dochází při ní **ke změně záznamu IP adresy**, který je dočasně uložený v lokálním disku: ten je provedený třeba útokem škodlivého kódu. Následuje ona „druhá vlna“ útoku, kdy je uživatel **donucen k návštěvě určité stránky** a přestože zadá zcela korektní adresu, je díky změně DNS záznamů přesměrovaný na web útočníka.

Sociální inženýrství navíc může nabývat **mnoha různých podob**. S jeho pomocí lze třeba velmi **snadno těžit ohromná množství osobních dat.**

A je to přitom tak jednoduché – stačí si dát na **inzertní weby nabízející práci** atraktivní nabídku. **Životopisy zájemců** o práci s **veškerými osobními údaji** (data narození, adresy, telefony, vzdělání, záliby apod.) budete během několika hodin počítat na stovky...

Toto není nabádání k nekalé činnosti – to je varování před typem útoku na osobní údaje, který se v poslední době velmi rozmáhá. Osobní data jsou následně zneužívána k mnoha následným kriminálním či přinejmenším neetickým úkonům jako je **zneužití identity** nebo **oslovování s obchodními nabídkami.**

Sociální inženýrství je zkrátka velmi nebezpečnou zbraní.

N**ejsilnější obranou** je naše **obezřetnost** a **sledování aktuálních trendů**. Zajištění informační bezpečnosti je nekonečným příběhem.

3.18 | Nebezpečí připojování z veřejných sítí

Připojovat se z notebooku, tabletu či mobilu na internet prostřednictvím Wi-Fi je pohodlné a často i výhodné (např. když už máme vyčerpaný datový limit, tzv. FUP). Wi-Fi síť, ke které se můžeme připojit, může být buď **soukromá** (např. na úřadě nebo u nás doma), nebo **veřejná** (např. v hotelu, ve vlaku či v knihovně)., kde se připojujeme pomocí tzv. **hotspotů** - veřejných míst pro bezdrátové připojení k internetu.

Pozor na to, jaké stránky si přes tuto bezdrátovou technologii prohlížíme, bychom si měli dát především u těch veřejných Wi-Fi, resp. **hotspotů** – veřejných míst pro bezdrátové připojení k internetu. Pod veřejnou Wi-Fi přitom myslíme nejen sítě bez hesla, ale i takové, ke kterým může univerzální heslo kdokoliv snadno získat – např. je napsáno na jídelním lístku, palubním časopisu nebo visí na nástěnce v konferenční místnosti.

K veřejným Wi-Fi hotspotům se lze zpravidla připojit bez hesla. Pokud k těmto sítím existuje nějaké heslo, je často nejen velmi jednoduché, ale zároveň ho sdílí více uživatelů (např. všichni hosté). Pro zkušenějšího útočníka pak není problém tuto komunikaci sledovat a „odposlouchávat“ např., jaké máte heslo k e-mailu či k profilu na sociální síti. Stejně snadno lze pak odchytit rovněž fotografii zasílanou přes internet z mobilu, o které rozhodně nechceme, aby ji viděl i někdo jiný než příjemce.

Ochranu před odposloucháváním nám může poskytnout zabezpečený přenos dat, tj. na stránky začínající HTTPS. Zatímco u počítače na stole mnozí z nás tuto adresu sledují, v mobilu prohlížené stránky sledujeme mnohem méně, než na počítači a tak se nám může snadno stát, že se připojíme i na nezabezpečené stránky, tj. „jen“ ty HTTP. Stejné zabezpečení prostřednictvím SSL je pak možné využít nejen pro přístup k webovým stránkám, ale i k poště.


U mobilů či tabletů se další nebezpečí může skrývat v **automatickém připojování k Wi-Fi**. Tato funkce je sice pohodlná a může ušetřit čas. Ale! Spotřebovává baterii a rozhodně nepřispívá k bezpečnosti našeho telefonu. Nikdy totiž nevíme, co všechno telefon do připojené sítě posílá, a jaké údaje mohou uniknout. Někteří podvodníci pak mohou této funkce a důvěřivosti uživatelů zneužít a vytvořit hotspot, který slouží především k odposloucháváni cizích hesel nebo informací o kreditních kartách v okamžiku, kde platíte v některém (nezabezpečeném) e-shopu.

V souvislosti s automatickým připojením k bezdrátovým sítím je nutné si uvědomit, že telefon se zapnutou Wi-Fi se automaticky připojí na již známou síť (tu však na základě informací vysílaných telefonem může podvodník záměrně vytvořit a dát ji stejné jméno, jako má např. naše síť doma či v zaměstnání) a začne synchronizovat data. V souvislosti s tím odešle přihlašovací údaje k různým službám – pravděpodobně i k našemu e-mailu či profilu na sociální síti.


Pokud chceme zůstat v bezpečí, určitě se vyplatí **automatické připojování k Wi-Fi vypnout**. Nejen, že si tím ušetříme baterii, ale rovněž ztížíme práci případným útočníkům.

3.19 | Další nebezpečí

Aniž bychom Vás chtěli nějak strašit, je třeba myslet na to, že ti, kteří se chtějí dostat k Vašim datům, mají stále nové a nové nápady jak to udělat. Nebezpečí se tak může skrývat prakticky všude – v „náhodně“ pohozeném USB disku či CD na stole, který Vám při vložení zaviruje počítač, stejně tak jako např. v počítačové myši, ve které může být umístěn špionský software se kterým myš bude nadále plnit i svoji běžnou funkci.


Stejně, jako jste všímaví ke svému okolí a např. podezřelým zavazadlům v autobuse bychom měli být **všímaví a obezřetní** (neuškodí ani zdravá podezřívaví) **k nebezpečím spojených s ochranou dat**. Víte například, že takové nebezpečí mohou skrývat i QR kódy, které Vás po naskenování do mobilu přesměrují na zavirovanou stránku?

4 | Kontrolní otázky

1. Je napadání webových kamer (tedy jejich zneužití k nahlížení do našeho soukromí) činností vyloučenou, vzácnou nebo obvyklou?
2. Co všechno může útočník získat tím, že získá přístup do našeho počítače?
3. Co byste řekli tomu, kdo bude tvrdit, že počítačová bezpečnost je chiméra a že u něho by útočníci stejně nikdy nic nehledali?
4. Proč je nutné dbát nejen na bezpečnost počítačů, ale také mobilních telefonů?
5. Jak vytvořit kvalitní heslo a jakou by mělo mít minimální délku?
6. Proč bych měl zálohovat a jaké existují zásady pro dobré (účinné) zálohování?
7. Jaké jsou výhody legálního software (z hlediska počítačové bezpečnosti)?
8. Používat nebo nepoužívat bezpečnostní program a proč?
9. Co má společného elektronický podpis se šifrováním?
10. Jak si mohu ochránit svůj mobil před ztrátou dat či jeho zneužití např. zlodějem?

5 | Doporučená literatura a odkazy

Webové zdroje:

- Národní centrum kybernetické bezpečnosti - www.govcert.cz - vládní centrum provozují Vládní bezpečnostní tým CERT České republiky.
- Aktuálně z bezpečnosti - https://www.csirt.cz/news/security/ - upozornění na aktuální hrozby včetně např. podvodných e-mailů z Národního bezpečnostního týmu CSIRT.CZ.
- Saferinternet: www.saferinternet.cz – Aktuální informace o dění v informační bezpečnosti.
- Securityworld: www.securityworld.cz - Webový portál čtvrtletníku o informační bezpečnosti.
- Viry.cz: www.viry.cz – Web věnovaný nejen počítačovým virům, ale i další aspektům informační bezpečnosti.
- Microsoft: http://www.microsoft.com/cze/digitalni-svet/bezpecnost.aspx - Informace o bezpečnosti od výrobce nejrozšířenějšího desktopového operačního systému.
- Hoax.cz: www.hoax.cz – Seznam různých poplašných zpráv.
- Zpráva společnosti Mandiant o rozsahu čínské kybernetické špionáže (anglicky): http://intelreport.mandiant.com/

Knihy:

- Kevin Mitnick: Umění klamu (Helion, 2003). Nadčasová publikace věnovaná technikám sociálního inženýrství. Její autor se stal prvním hackerem, který se dostal na seznam deseti nejhledanějších osob americkou FBI.

- Daniel Dočekal a Lenka Eckertová: Bezpečnost dětí na internetu (Computer Press, 2013). Informační bezpečnost týkající se dětí, ale poučí se i dospělí.
- Johnny Long: Google Hacking (Zoner Press, 2005). Úžasná kniha, která přináší návod, jak na internetu najít prakticky cokoliv. Vynikající materiál především z hlediska bezpečnosti: jak skrýt informace, co o mě mohou vidět ostatní apod.
- Richard Clarke: Cyber War (Ecco, 2010). Anglicky. Vynikající publikace upozorňující na rizika spojená s využíváním kybernetického prostoru.

6 | Souhrn

V kurzu jste se seznámili se základy zabezpečení dat jak v soukromém, tak pracovním životě.

- máte přehled o významu termínů používaných v souvislosti s kybernetickými hrozbami, např. cracker, hacker, hoax, malware
- uvědomujete si problémy, které přináší nedostatečná legislativa a jak těžké je pro legislativu držet krok s kybernetickým zločinem
- znáte nejčastější způsoby, jak dochází k napadení počítače a zneužití citlivých dat
- dostali jste užitečnou radu pro tvorbu hesla
- víte, co je sociální inženýrství a jak ho podvodníci využívají

a na úplný závěr to nejdůležitější:

- Stoprocentní bezpečnost neexistuje.
- Kdo vám ji slíbí, buď vědomě lže, nebo neví, o čem mluví.
- Lze se jí ale významným způsobem přiblížit.

Test:

1.1 | Administrátorská práva

- jsou z hlediska bezpečnosti stejná jako práva uživatelská. Je lepší, když je mají přidělena všichni uživatelé, protože to zjednodušuje práci s počítačem.
- jsou z hlediska bezpečnosti stejná jako práva uživatelská pouze v případě domácích počítačů. Ve firmách je důležité kvůli odpovědnosti striktně oddělit administrátory od uživatelů.
- jsou silně nebezpečná a neměla by být přidělována běžným uživatelům. Drtivá většina útoků je totiž potřebuje pro instalaci škodlivých kódů apod.

1.2 | Co je hotspot?

- Veřejné místo pro bezdrátové připojení k internetu
- Druh počítačového viru
- Operační systém pro mobilní telefony

1.3 | Co označuje zkratka IMEI?

- Jedinečný kód používaný k identifikaci mobilního telefonu, který je používán v rámci GSM sítě.
- Jiné označení pro PIN kód.
- Speciální antivirový program určený pro mobilní zařízení.

1.4 | Hoax je

- smyšlená a nesmyslná zpráva, která se snaží tvářit důvěryhodně a které přímo či nepřímo vyzývá uživatele k dalšímu šíření.
- speciální typ bezpečnostního programu, který blokuje viry při vstupu do počítače.
- situace, kdy počítač „zatuhne“ a nedá se s ním déle pracovat. Problém pak řeší jen tvrdý restart (např. vyhození a nahození pojistek na celém patře).

1.5 | Které přílohy v e-mailech (z hlediska odesílatele i typu souboru) jsou nebezpečné?

- Pouze ty od neznámých osob nebo z neznámých e-mailových adres.
- Pouze spustitelné programy. Dokumenty a další typy souborů mohu otevírat bez obav.
- Všechny; počítač si může zavirovat (a tudíž se stát zdrojem nákazy) kdokoliv.

1.6 | Počítačové útoky se mobilních telefonů

- netýkají. Mobily mají jiný princip fungování, než počítače a nelze je napadnout.
- týkají. Třeba počítačový virus je program jako každý jiný – pokud dokážeme do mobilu instalovat program, můžeme mít nainstalovaný i virus.
- netýkají. Veškerý provoz v případě mobilů jde skrze operátory, kteří útoky spolehlivě filtrují.

1.7 | Počítačové útoky se...

- ...nedají se zastavit, útočník se vždy prosadí. Nemá smysl používat bezpečnostní programy, jsou to jen vyhozené peníze.
- ...dají bez problémů zastavit bezpečnostními programy; pokud je máme, můžeme být v pohodě.
- ...nedají se zastavit všechny, ale bezpečnostní program a jednoduchá bezpečnostní opatření mají smysl. Bez nejmenších problémů zastaví devatenáct z dvaceti útoků.

1.8 | Pokud nepoužívám Windows, pak bezpečností program (antivir, firewall aj.)

- nepotřebuji. Windows jsou nebezpečný systém, viry pro ostatní aplikace neexistují.
- potřebuji, ale pouze v případě, že se chovám rizikově (instaluji nelegální software, navštěvuji pochybné stránky apod.).

- potřebuji. Existují různé viry, které nejsou závislé na použitém systému, stejně jako existují tisíce virů třeba pro Android, Linux apod.

1.9 | Pokud webová stránka začíná písmeny HTTPS, znamená to, že:

- Stránka poskytuje zabezpečený přenos dat, jako např. ochranu před odposloucháváním
- Stránka obsahuje neověřitelná data, ve kterých je zvýšené riziko výskytu viru
- Stránka nemá žádné výhody ani nevýhody oproti klasickému HTTP, jde pouze o modernější vyjádření toho samého

1.10 | Zákon o kybernetické bezpečnosti nabyl účinnosti:

- 1.11.2014
- 1.1.2015
- 1.5.2015

Test – správné odpovědi:

1.1 | Administrátorská práva

- jsou z hlediska bezpečnosti stejná jako práva uživatelská. Je lepší, když je mají přidělena všichni uživatelé, protože to zjednodušuje práci s počítačem. (nesprávná odpověď)
- jsou z hlediska bezpečnosti stejná jako práva uživatelská pouze v případě domácích počítačů. Ve firmách je důležité kvůli odpovědnosti striktně oddělit administrátory od uživatelů. (nesprávná odpověď)
- jsou silně nebezpečná a neměla by být přidělována běžným uživatelům. Drtivá většina útoků je totiž potřebuje pro instalaci škodlivých kódů apod. (**správná odpověď**)

1.2 | Co je hotspot?

- Veřejné místo pro bezdrátové připojení k internetu (**správná odpověď**)
- Druh počítačového viru (nesprávná odpověď)
- Operační systém pro mobilní telefony (nesprávná odpověď)

1.3 | Co označuje zkratka IMEI?

- Jedinečný kód používaný k identifikaci mobilního telefonu, který je používán v rámci GSM sítě. (**správná odpověď**)
- Jiné označení pro PIN kód. (nesprávná odpověď)
- Speciální antivirový program určený pro mobilní zařízení. (nesprávná odpověď)

1.4 | Hoax je

- smyšlená a nesmyslná zpráva, která se snaží tvářit důvěryhodně a které přímo či nepřímo vyzývá uživatele k dalšímu šíření. (**správná odpověď**)
- speciální typ bezpečnostního programu, který blokuje viry při vstupu do počítače. (nesprávná odpověď)
- situace, kdy počítač „zatuhne“ a nedá se s ním déle pracovat. Problém pak řeší jen tvrdý restart (např. vyhození a nahození pojistek na celém patře). (nesprávná odpověď)

1.5 | Které přílohy v e-mailech (z hlediska odesílatele i typu souboru) jsou nebezpečné?

- Pouze ty od neznámých osob nebo z neznámých e-mailových adres. (nesprávná odpověď)
- Pouze spustitelné programy. Dokumenty a další typy souborů mohu otevírat bez obav. (nesprávná odpověď)
- Všechny; počítač si může zavirovat (a tudíž se stát zdrojem nákazy) kdokoliv. (**správná odpověď**)

1.6 | Počítačové útoky se mobilních telefonů

- netýkají. Mobily mají jiný princip fungování, než počítače a nelze je napadnout. (nesprávná odpověď)
- týkají. Třeba počítačový virus je program jako každý jiný – pokud dokážeme do mobilu instalovat program, můžeme mít nainstalovaný i virus. (**správná odpověď**)
- netýkají. Veškerý provoz v případě mobilů jde skrze operátory, kteří útoky spolehlivě filtrují. (nesprávná odpověď)

1.7 | Počítačové útoky se...

- ...nedají se zastavit, útočník se vždy prosadí. Nemá smysl používat bezpečnostní programy, jsou to jen vyhozené peníze. (nesprávná odpověď)

- ...dají bez problémů zastavit bezpečnostními programy; pokud je máme, můžeme být v pohodě. (nesprávná odpověď)
- ...nedají se zastavit všechny, ale bezpečnostní program a jednoduchá bezpečnostní opatření mají smysl. Bez nejmenších problémů zastaví devatenáct z dvaceti útoků. (**správná odpověď**)

1.8 | Pokud nepoužívám Windows, pak bezpečností program (antivir, firewall aj.)

- nepotřebuji. Windows jsou nebezpečný systém, viry pro ostatní aplikace neexistují. (nesprávná odpověď)
- potřebuji, ale pouze v případě, že se chovám rizikově (instaluji nelegální software, navštěvuji pochybné stránky apod.). (nesprávná odpověď)
- potřebuji. Existují různé viry, které nejsou závislé na použitém systému, stejně jako existují tisíce virů třeba pro Android, Linux apod. (**správná odpověď**)

1.9 | Pokud webová stránka začíná písmeny HTTPS, znamená to, že:

- Stránka poskytuje zabezpečený přenos dat, jako např. ochranu před odposloucháváním (**správná odpověď**)
- Stránka obsahuje neověřitelná data, ve kterých je zvýšené riziko výskytu viru (nesprávná odpověď)
- Stránka nemá žádné výhody ani nevýhody oproti klasickému HTTP, jde pouze o modernější vyjádření toho samého (nesprávná odpověď)

1.10 | Zákon o kybernetické bezpečnosti nabyl účinnosti:

- 1.11.2014 (nesprávná odpověď)
- 1.1.2015 (**správná odpověď**)
- 1.5.2015 (nesprávná odpověď)