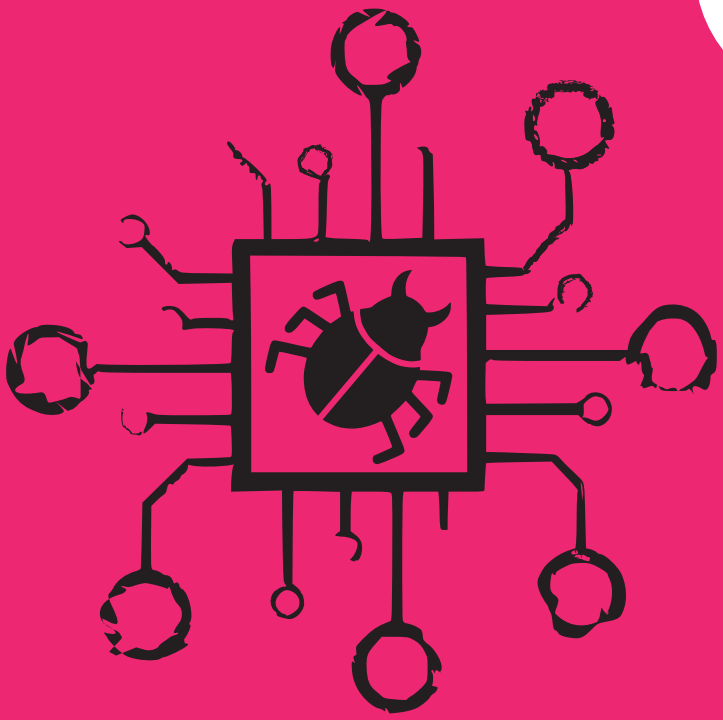
10.DÍL



KYBERNETICKÁ BEZPEČNOST

MARTINA ŘEJHOVÁ

SP3V

2021

Smíchovská průmyslovka třetího věku

10. díl

Kybernetická bezpečnost

Martina Řejhová

Tato brožura vznikla jako inspirační materiál pro volný čas studentů Smíchovské průmyslovky třetího věku. Pěkné čtení i zábavu vám přeje tým SSPŠ a jeho přátelé.

Tato brožura je součástí skupiny následujících brožur:

1. díl: Nanotechnologie pro začátečníky (Věra Krajčová) 

2. díl: Procházka Prahou fyzikální (Jan Mlynář) 

3. díl: Nebojme se robotů (Jaroslav Kořínek) 

4. díl: Magické čtverce (Marie Souchová) 

5. díl: Jedová chýše (Ivan Lukačina) 

6. díl: Fyzikální inspiromat (Věra Krajčová) 

7. díl: Grafika a 3D tisk (Lukáš Vrba) 

8. díl: Procházka Sluneční soustavou (Jan Veselý) 

9. díl: Geometrická zobrazení kolem nás (Tamara Mainzerová) 

10. díl: Kybernetická bezpečnost (Martina Řejhová) 

Grafik a autor loga: Lukáš Chochlovský

Kybernetická bezpečnost

Obecné pojmy

Kybernetická bezpečnost (Cyber Security) je odvětví výpočetní techniky známé také jako informační bezpečnost, uplatňované u počítačů, tabletů, chytrých telefonů a všech elektronických prvků sítě. Cílem informační bezpečnosti je ochrana informací a majetku před krádeží, korupcí nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Lze tedy zjednodušeně říci, že kybernetická bezpečnost se zabývá bezpečností na počítači tak, aby na něm uživatel mohl pracovat bezpečně a využívat ho bez omezení.

Termínem bezpečnost informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením či kolapsem neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánovanou událostí. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

Kyberstalking

Jedná se o nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty), jejichž cílem je např. vzbudit v oběti pocit strachu.

Informace o oběti pachatel získává nejčastěji z webových stránek, diskuzních fór nebo chatovacích místností („chat“ je způsob přímé on-line komunikace

dvou a více osob prostřednictvím internetu). Často je taková aktivita pouze mezistupněm k trestnému činu, který muže zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání.

Ukázka:

Paní Hana, vysoce postavená manažerka banky, se po dlouhodobém a ke konci nefunkčním manželství rozhodla podat žádost o rozvod. Důvodem byla neutuchající žárlivost jejího manžela, který ji k tomuto rozhodnutí přiměl neustálým obviňováním, že paní Hana má milence. Tajného milence hledal manžel paní Hany i v případě, že šla vynést koš.

Rozhodnutí podat žádost o rozvod nesl její manžel velice těžce a důvod stále spatřoval v tom, že má paní Hana milence. Paní Hana si však začala všímat, že se její manžel v rozčilení podřekl a sdělil jí skutečnosti, které věděla jen ona sama – např. s kým a co si píše na mobilním telefonu.

Paní Hana se obrátila na Polici ČR. V rámci prověřování nahlášeného případu nechala policie prozkoumat telefon paní Hany, kde byla nalezena aplikace sledující veškerou činnost v chytrém telefonu. Dle doby nainstalování bylo zřejmé, že aplikaci musel naistalovat manžel paní Hany, neboť v inkriminované době byli sami v bytě a data byla odesílána na e-mailový účet, ke kterému byl zaznamenán přístup převážně z domu paní Hany.

Kyberšikana

Kyberšikana nebo kybernetická šikana, počítačová šikana či cyberbullying je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií.

Do kyberšikany se řadí fyzické napadení oběti s natáčením videozáznamu, vyvedení oběti z rovnováhy spojené s natáčením videozáznamu, provokování a napadání uživatelů v diskuzních fórech, pomlouvání s využitím internetu a mobilních telefonů, odhalování cizího tajemství prostřednictvím internetu, vydírání s pomocí informačních a komunikačních technologií, obtěžování a pronásledování oběti, krádež identity, zneužití cizí identity ke kyberšikaně.

Ukázka 1:

Dva žáci 9. třídy Marek a Libor se snažili během hodiny vyprovokovat učitelku češtiny Marii K. (pokřikovali na ni, narušovali hodinu, nadávali jí apod.). Když učitelka situaci nezvládla, tajně ji natočili mobilním telefonem a záznam umístili na YouTube. Nahrávku zhlédlo přes 70 000 uživatelů. Učitelka se o její existenci dozvěděla, až když se na ni přišli zeptat rozčílení rodiče.

Ukázka 2:

Gábina chodila s Petrem. Když se s ním rozešla, Petr se s rozchodem nemohl smířit a začal ji doslova bombardovat různými zprávami. Prosil, ať se k němu vrátí, urážel ji, pomlouval před jejími známými, vyhrožoval, že sobě i jí fyzicky ublíží, obtěžoval i její rodiče a známé. Často také Gábině telefonoval.

Kybergrooming

Jako kybergrooming nebo také child grooming či cyber grooming se označuje chování uživatelů internetových komunikačních prostředků (chat, Skype atd.), kteří tyto prostředky využívají k navázání důvěrných vztahů se svými oběťmi, jimiž jsou nejčastěji děti. Po navázání důvěrného vztahu groomer (útočník) vyzve svou oběť k reálnému setkání, jehož cílem je sexuální nebo jiné zneužití důvěry vybrané osoby, případně manipulace vedoucí k extremistickým projevům a šíření nenávisti (osoba se ve jménu víry stává teroristou). Oběťmi kybergroomingu mohou být i dospělí a senioři.

Touto problematikou se zabývá i dokumentární film *V síti* (režie Barbora Chalupová a Vít Klusák) z roku 2020. Více informací k filmu lze najít na https://www.csfd.cz/film/720753-v-siti/prehled/. Dokument je možné zhlédnout například na portálu iprima.cz (https://www.iprima.cz/filmy/v-siti).

Ukázka 1:

Skutečný příběh: Britský pedofil Michael Wheeler používal k seznamování s dívkami veřejný chat. S jednou ze zneužitých dívek se seznámil, když jí bylo 11 let. Postupně jí manipuloval, až se na něm stala citově závislou. Krátce po jejích 13. narozeninách ji začal sexuálně obtěžovat. Kontaktoval a obtěžoval také její kamarádky. (11 sexuálních útoků a zneužití 2 dívek (13 let). Byl uvězněn na 3 roky.)

Ukázka 2:

Skutečný příběh: Usvědčený deviant Pavel H. (vrátný v tiskárnách) využíval k seznamování s oběťmi např. diskuzní fóra, chat či inzeráty. Předstíral, že vybírá děti z dětských domovů do soutěže Dítě VIP, apod. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce. (Znásilňování a zneužívání 20 chlapců. Byl uvězněn na 8 let).

Ukázka 3:

Skutečný příběh: Bývalý pošťák Douglas Lindsell získával sympatie dívek např. tvrzením, že má rakovinu. Vedl si databázi dívek, se kterými se seznámil online, plánoval si osobní setkání s nimi a znásilnění, některým posílal své nahé fotografie nebo je nutil např. k obnažování. Dvě dívky (13 a 14 let) dokonce přiměl k osobní schůzce. Jednu z nich se snažil nalákat do svého auta a znásilnit. (Sexuální obtěžování několika dívek, pokus o znásilnění. Byl uvězněn na 5 let.)

Sexting

Slovo sexting je spojením slov sex a textování a znamená posílání textového, fotografického, audio a video obsahu se sexuálním podtextem prostřednictvím informačních a komunikačních technologií.

Ukázka 1:

Skutečný příběh: Nezletilá žákyně deváté třídy vyfotila svůj vlastní intimní snímek pro svého kamaráda. Dívka si chlapce zřejmě chtěla získat. Ten ale fotografii rozeslal dalším přátelům, kteří začali snímek rozesílat dál. Do šíření fotografie se zapojilo přes 30 dětí. Fotografie dívky se dostala až k učitelům, kteří dívku identifikovali podle řetízku na krku a případ oznámili policistům s podezřením z šíření dětské pornografie.

Trestní zákon považuje posílání pornografických snímků osob mladších 18 let za šíření dětské pornografie, za které hrozí až tři roky vězení. U mladistvého se trest obvykle krátí na polovinu. Pokud by bylo „rozesílateli“ méně než patnáct let, nebyl by trestně stíhaný. Hlavní aktérka se trestu od soudu bát nemusí. Přesto už pouhé policejní vyšetřování přinese dívce i její rodině těžké chvíle. Pokud se ukáže, že mladiství aktéři se v minulosti ničeho závažného nedopustili, může soud upustit od potrestání.

Případ byl dořešen v říjnu 2009 a mladiství žáci, kteří se do šíření snímku zapojili, byli potrestáni tresty veřejně prospěšných prací.

Ukázka 2:

Skutečný příběh: Osmnáctiletá Jessica Loganová zaslala svému příteli v době, kdy spolu chodili, své intimní fotografie. Po rozchodu však Jessičin bývalý přítel začal rozesílat její fotografie dalším lidem, zejména spolužákům (Cincinnati, Ohio High School). Od té doby byla vystavena neustálému posměchu ze strany spolužáků i dalších, kteří fotografie viděli. Jessica se bála přijít do školy, začala tedy chodit za školu a její prospěch se rapidně zhoršil. S prosbou o pomoc se obrátila na školního policistu, který jí však nedokázal pomoci a poradil jí, aby vystoupila v místní kabelové televizi a svěřila se se svým příběhem. Útoky nepřestaly ani poté, co Jessie vystoupila v místní kabelové televizi (silueta a změněný hlas), vypověděla zde svůj příběh a požádala spolužáky, aby jí přestali ubližovat. To se ovšem nestalo. Pod tlakem neustálého posměchu a urážení Jessie 3. července 2008 spáchala sebevraždu (oběsila se v koupelně).

Ukázka 3:

Skutečný příběh: Třináctiletá žákyně 7. třídy floridské základní školy Hope Witsellová chtěla upoutat pozornost Alexe Eargooda, chlapce, který se jí líbil, a proto mu zaslala mobilním telefonem svou nahou fotografii. Jeho spolužačka si ale v autobuse od Alexe půjčila mobil, ve kterém našla nahou fotku Hope. Tuto fotku pak dívka přeposlala dalším spolužákům a spolužačkám. Během několika hodin začala fotografie kolovat po několika okolních základních a středních školách. Od této chvíle začala probíhat ve škole šikana – spolužáci se Hope smáli, uráželi jí, říkali o ní, že je děvka a coura.

Postupně se o sextingu a o Hopině nahé fotografii šířící se školou dozvědělo vedení školy, které Hope na týden vyloučilo ze školy.

Pod tlakem neustálého posměchu a urážení Hope 12. září 2009 spáchala sebevraždu (oběsila se ve svém pokoji).

Ukázka 4:

Skutečný příběh: Šestnáctiletá studentka mladoboleslavského gymnázia se nechala vyhecovat od kamarádů a o přestávce mezi vyučováním se svlékla. Spolužáci ji přesvědčili, aby se nechala natočit na mobil, jak masturbuje. Kauza došla tak daleko, že případ vyšetřuje Policie ČR. Video bylo ukradeno ze serveru www.libimseti.cz a dále pak putovalo internetem. Za jeho šíření bylo například propuštěno několik zaměstnanců mladoboleslavské společnosti Škoda Auto, dalším byl snížen plat.

Úkol:

Přečtěte si následující příběhy a rozhodněte, o který z výše popsaných kyberútoků se jedná.

Příběh 1:

Zbyněk chodil s Katkou. Danovi se ale Katka také líbila, a tak začal Zbyňkovi posílat výhružné SMS a e-maily. Hrozil, že pokud se s Katkou nerozejde, vyřídí si to s ním ručně.

Příběh 2:

Zpráva náctileté holčičce: Rodiče ti nerozumí, já ano, mně se můžeš svěřit se svými problémy. Neříkej o tom ostatním dětem, žárlily by. Neříkej o tom mamince. Nenáviděla by tě. Dospělí to nepochopí, já ano. Mně se můžeš svěřit, můžeme mít tajemství. Jsem na tom podobně, svěř se, zůstane to mezi námi.

Příběh 3:

14letá Jana se na internetu seznámila s 30letým Karlem. Z počátku jí bavilo si s ním psát SMS a e-maily, připadala si více dospěle, protože se baví se starším mužem. Po dvoutýdenním dopisování jí Karel začal posílat své intimní fotografie, o které Jana neměla zájem a velmi ji obtěžovaly. Snažila se Karlovi vysvětlit, že tohle opravdu nechce, a snažila se komunikaci ukončit. Karel ale začal posílat fotografie o to více, a dokonce i videa.

Příběh 4:

Bára se zamilovala do svého spolužáka Tomáše, ten však její lásku neopětoval. Bára se proto rozhodla ho získat všemi možnými způsoby. Psala mu desítky SMS denně, zahlcovala ho e-maily, nechávala před jeho dveřmi dárky. Ať šel

kamkoli, pronásledovala ho. Na ulici se s ním snažila srovnat krok, aby to alespoň vypadalo, že k sobě patří. Stále sledovala jeho profil na sociální síti, vše, co přidal, komentovala a psala na jeho profil, že spolu chodí.

Řešení:

Zde je řešení jednotlivých příběhů.

Příběh 1:

Dan se dopustil kyberšikany; pro vyhrožování použil textové zprávy a e-maily.

Příběh 2:

Jedná se o kybergrooming; útočník se snaží manipulovat náctiletou holčičkou a izolovat ji od okolí.

Příběh 3:

V tomto příběhu se Karel dopustil sextingu; posílal intimní fotografie slečně, kterou obtěžovaly.

Příběh 4:

Bára z příběhu se dopustila kyberstalkingu; svého spolužáka neustále obtěžovala.

Proč se chránit

Důvodů, proč si počínat v kyberprostoru (počítače, internet) bezpečně, je několik.

Ztráta dat

Základní bezpečnostní atributy jsou:

- **důvěrnost** – prevence neautorizovaného vyzrazení dat
- **integrita** – prevence neautorizované úpravy dat
- **dostupnost** – prevence ztráty přístupu k datům

Ztráta dat z pohledu důvěrnosti znamená, že data, která jsou soukromá, se dostanou k nepovolaným osobám.

Například: Přístupové údaje k internetovému bankovnictví nemají být volně dostupné pro jiné uživatele.

Ztráta dat z pohledu integrity znamená, že data nebudou při cestě od odesílatele k příjemci změněna.

Například: Zaslání daňového přiznání elektronicky je nutné zabezpečit tak, aby během jeho přenosu nebyla změněna data, která obsahuje.

Ztráta dat z pohledu dostupnosti znamená, že data nemusí být vždy k dispozici.

Například: Internetový obchod chce mít stránky dostupné nepřetržitě, aby si tam uživatelé mohli kdykoliv objednat výrobky či služby.

Ztráta peněz

Peníze mohou být odcizeny z účtu tak, že se útočník dostane do internetového bankovnictví klienta (například odcizením přístupových údajů) a peníze z účtu mu odčerpá (převede na jiný, anonymní účet, přímo zaplatí za službu či výrobek…).

O peníze můžete přijít ale i vydíráním. Útočník může získat například citlivé fotografie nebo zašifruje disk a žádá výkupné (více v části Typy útoků).

Zneužití osobních informací

Útočník páchá trestnou činnost pod jinou (ukradenou) identitou.

Například: Útočník využije ukradených osobních informací ke sjednání online půjčky nebo útočník prostřednictvím e-mailu oběti píše nevhodné zprávy.

Typy útoků

Existuje spousta typů útoků, kterými se útočníci snaží získat data či přístupy. Někteří útočníci sázejí na škodlivé programy, jiní na sociální inženýrství, ale velká část útočníků kombinuje oba dva způsoby.

Malware

Malware neboli škodlivý software, jehož název vznikl složením anglických slov **mal**icious soft**ware**, je program určený k poškození počítačového systému nebo vniknutí do něj.

Pro tento škodlivý software se velmi často používá nesprávné označení počítačové viry. Viry jsou pouze podskupina malwaru.

První škodlivé softwary byly původně napsány jako experimenty či žerty. Jejich původní záměr byl neškodný nebo pouze otravný, ale neměl způsobit vážné škody počítačovým systémům. V některých případech si pachatel ani nedokázal představit, jak velké škody může jeho výtvor napáchat. Mladí programátoři, kteří se učili o virech a jejich technikách, je psali pro jednoduché procvičování nebo aby zjistili, jak daleko se mohou rozšířit. První viry, které byly napsány především jako žert, jako virus Melissa nebo virus David, byly rozšířeny až v roce 1999.

Od doby rozšíření širokopásmového (vysokorychlostního) připojení k internetu začal být škodlivý software vytvořena pro zisk. Například od roku 2003 byla většina rozšířených virů a červů (podskupina malwaru) vytvořena tak, aby převzala kontrolu nad uživatelskými počítači pro zneužití na černém trhu.

Malware se dělí do několika kategorií:

- Viry
- Červi
- Trojští koně
- Grayware
- Rootkity
- Ransomware
- Backdoory, keyloggery, screen scrapery

Viry

Virus je spustitelný kód, který je schopen sám sebe replikovat a vložit se do spustitelného souboru. To se provádí při spuštění hostitelského souboru. Virus se není schopen šířit sám, ale šíří se sdílením infikovaných souborů. Viry často provádí škodlivou akci (smazání dat, zašifrování dat…).

Ukázka 1:

Virus Brain (1986) – Snad úplně první počítačovou hrozbou, se kterou se uživatelé setkali, byl virus Brain. V roce 1986 jej naprogramovali dva bratři z Pákistánu. V tomto případě je původ viru snadno prokazatelný, neboť se do něj oba sami podepsali, a to včetně názvu své společnosti a telefonního čísla. Bootovací virus, který se šířil po disketách, měl původně zabránit nelegální distribuci lékařského softwaru, který bratři Alviové naprogramovali. Škodlivý kód zpomaloval čtení disket, ale pevné disky nenapadal.

Ukázka 2:

Vienna (1987) – Jeden z prvních virů ve středoevropském prostoru byl virus Vienna. Detekovali jej Miroslav Trnka a Peter Paško, kteří na něj vytvořili i antivir. Setkání s virem Vienna tak stojí za vznikem společnosti ESET, kterou oba programátoři o několik let později založili.

Ukázka 3:

I Love You (2000) – Byl jedním z nejznámějších a nejničivějších virů – minimálně ve své době. Do počítače se dostal prostřednictvím přílohy e-mailu a poté mazal dokumenty, fotografie, hudební soubory, ale vyhledával i údaje o kreditních kartách. Virus, který se rozšířil z Filipín v květnu roku 2000, napadl až 10 procent všech počítačů připojených do internetové sítě a škody se odhadují na více než 5 miliard dolarů.

Červi

Červ je program, který se dokáže jak sám replikovat, tak i velmi rychle sám šířit do dalších počítačů. Červi jsou velmi nebezpeční, protože neustále prochází počítačovou síť a snaží se vyhledávat počítače s určitou chybou zabezpečení, aby se mohli zkopírovat na nové počítače, a tím přetěžují síť svými požadavky. Často způsobují škodu, například vypnutí počítače.

Ukázka:

Chernobyl (1998) – Červ Chernobyl dokázal přepsat kritické informace na infikovaném počítači a zničit BIOS. Jméno tohoto škodlivého softwaru, který vytvořil univerzitní student z Tchaj-wanu, vychází z data rozšíření, které náhodou připadlo právě na výročí černobylské katastrofy. [5]

Trojští koně

Jedná se o spustitelný soubor, který není schopen se sám replikovat ani šířit. Trojský kůň předstírá, že je něco jiného (např. spořič obrazovky, hra…), aby ho uživatel spustil. Při spuštění vykoná svůj škodlivý kód, který dokáže ukrást hesla a tajné informace (např. údaje o kreditní kartě), stahuje jiný malware, infikuje cílový počítač červem, špehuje činnost uživatele, rozesílá spam.

Ukázka:

Zeus (2007) – Jde o typ trojského koně, který napadá systémy společnosti Microsoft Windows. Není primárně zaměřený jedním směrem, může vykonávat různé škodlivé funkce. Často je však využíván ke krádežím bankovních informací metodou keyloggeru, ale také k instalaci jiného malwaru. Zeus se prvně objevil v červenci roku 2007 a je znám hlavně tím, že dokázal vytvořit jednu z největších zavirovaných sítí světa, tzv. botnet. Miliony počítačů pak vytváří jeho další kopie k rozesílání škodlivých informací. Navíc jsou tyto počítače a systémy společně propojeny a při správném naprogramování škodlivého softwaru se pak dá docílit vzájemné spolupráce.

Grayware

Grayware je nežádoucí software, který není přímo klasifikovaný jako malware, ale stále negativně ovlivňuje výkon počítače a je významnou bezpečnostní hrozbou. Grayware zahrnuje spyware, adware a žertovné programy.

Spyware shromažďuje informace o uživateli pro marketingové účely a posílá je třetí osobě.

Adware je software s reklamním materiálem. Způsobuje nepříjemné vyrušování uživatele například ve formě vyskakovacích bannerů, pop-upů (vyskakovací okna) anebo přímo funguje jako přesměrování na podezřelé internetové stránky, kde se mohou nacházet jiné hrozby a formy malware.

Rootkity

Rootkit může upravit operační systém, aby zůstal nezjištěn, a také se dokáže bránit proti odstranění tím, že vytvoří nové kopie, zakáže antivirový software a mění různá nastavení.

Ransomware

Ransomware (neboli vyděračský program – název vznikl složením anglických slov ransom „výkupné“ a software) je druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná a pak požaduje od oběti výkupné za obnovení přístupu.

Ukázka:

Trojan AIDS (1990) – První ransomware spatřil světlo světa již na začátku devadesátých let. Oproti současnosti, kdy se používají k zaplacení výkupného prakticky výhradně kryptoměny, byl zvolen z dnešního pohledu poněkud nevšední způsob úhrady. Peníze se posílaly poštou do P. O. Boxu v Panamě. Jeho autor, který byl záhy dopaden, se hájil tím, že získané prostředky chtěl využít na výzkum léku právě proti této nemoci (AIDS).

Backdoory, keyloggery, screen scrapery

Backdoory (zadní vrátka), keyloggery, screen scrapery (snímače obrazovky) jsou programy, které kradou tajné informace nebo získávají přístup do počítače. Backdoory zajišťují nepozorovaný vstup do počítače třetí straně (útočníkovi). Keyloggery zaznamenávají stisknuté klávesy a záznamy posílají třetí straně. Screen scrapery vytvářejí otisky obrazovky s hesly a tajnými informacemi a předávají je třetí straně.

Sociální inženýrství

Sociální inženýrství je způsob manipulace lidmi za účelem provedení určité akce nebo získání určité informace.

Nejednoduší způsob, jak se něco dozvědět, je jednoduše se zeptat. Čím více důvěry si útočník získá, tím jednodušší je pro něj danou informaci získat.

Pretexting

Pretexting je utváření a využívání vymyšleného scénáře s cílem přesvědčit oběť k zamýšlené akci nebo k získání určité informace. Jedná se o skloubení lži

s kouskem pravdivé informace získané dříve. Může se jednat například o datum narození, rodné číslo, přihlašovací jméno, jméno nadřízeného atd. Cílem je přesvědčit oběť o legitimnosti akce, která je po ní požadována.

Tato technika je často používána například soukromými detektivy k získání neveřejných informací o firmě, jako jsou výpisy telefonních hovorů, výpisy bankovních účtů aj. od běžných zaměstnanců. Tyto informace mohou být následně použity při pokročilé komunikaci s vedoucími zaměstnanci, např. o změně účtu, příkazům k převodu peněz atp.

Velké množství firem stále ověřuje totožnost klienta podle rodného čísla, rodného jména matky či jiných relativně snadno dostupných informací, čímž usnadňují aplikování tohoto typu sociálního inženýrství.

Pretexting lze také použít při vydávání se za kolegu z práce, policejního vyšetřovatele, bankovního úředníka, zaměstnance finančního úřadu či jiného zaměstnance státní správy, který by mohl mít právo na dotazování dané oběti. Útočníkovi stačí být přichystán na možné kontrolní otázky oběti, ale někdy stačí pouze autoritativní a seriózní tón hlasu a dostatečně přesvědčivý obsah konverzace.

Termín je běžně používán ve významu podvodu nebo podvodného jednání za účelem získání utajených informací o organizaci nebo přístupu do informačního systému firmy.

Ukázka:

První rozhovor: Andrea Lopezová

Andrea Lopezová zvedla vyzvánějící telefon ve videopůjčovně, kde pracovala, a po chvíli se na její tváři objevil úsměv. Je příjemné, když zákazník říká, že je spokojený se službami firmy. Volající říkal, že má s touto půjčovnou velmi dobré zkušenosti a že by o tom chtěl napsat jejímu manažerovi dopis. Zeptal se na jeho jméno a korespondenční adresu. Andrea odpověděla, že manažer se jmenuje Tommy Allison a uvedla jeho adresu. Když už chtěla zavěsit, volajícího ještě něco napadlo, řekl: „Možná bych mohl napsat ještě na vaše ústředí. Jaké je číslo vaší půjčovny?“ Andrea mu sdělila i tuto informaci. Volající jí poděkoval, dodal něco milého o tom, jak mu pomohla, a rozloučil se. Takový telefon, pomyslela si, vždycky potěší a den rychleji uteče. Kéž by to tak bylo častěji.

Druhý rozhovor: Ginny

„Děkujeme za zavolání do VideoMasters, u telefonu Ginny. Co pro Vás mohu udělat?“ „Dobrý den, Ginny“ ohlásil se vesele volající, jako by hovořil s Ginny alespoň jednou týdně. „Tady Tom Allison, manažer z ForestPark, půjčovna číslo 863. Máme tu klienta, který by si chtěl půjčit film *Rocky 5*, ale nemáme žádnou kopii. Mohla by ses kouknout, jestli to tam náhodou nemáte?“ Po několika okamžicích se vrátila ke sluchátku a řekla: „Máme tu tři kopie.“ „Bezva, zeptám se, jestli by se nechtěl pro ten film zastavit u vás. Děkuji. Kdybys něco potřebovala z naší půjčovny, klidně zavolej a chtěj Tommyho.

Bylo by mi potěšením, kdybych mohl pro tebe něco udělat.“ Během několika následujících týdnů měla Ginny více telefonátů od Tommyho, který prosil o pomoc v různých záležitostech. Byly to obyčejné prosby a Tommy byl vždycky velmi příjemný a nic nenasvědčovalo tomu, že by ji chtěl nějak využít. Byl trošku povídavý, říkal například: „Slyšelas o tom požáru v OakPark? Prý uzavřeli několik ulic.“ Jeho telefonáty pro ni byly příležitostí odtrhnout se na chvíli od běžné práce a ona byla vždy ráda, když se ozval. Jednoho dne byl Tommy trochu nervózní a zeptal se: „Neměli jste nějaké problémy s počítači?“ „Ne,“ odpověděla Ginny. „Proč?“ „Nějaký chlápek naboural do telefonního sloupu a údržbář z telekomunikační firmy říkal, že celá čtvrť bude bez internetu, dokud to nespraví.“ „To je hrůza! Stalo se někomu něco?“ „Toho řidiče odvezli sanitkou. Hele, mohla bys mi pomoci? Mám tu vašeho zákazníka, který si chce půjčit třetí díl *Kmotra*, ale zapomněl si průkazku. Mohla by ses na něho mrknout?“ „Samozřejmě.“ Tommy uvedl jméno a adresu zákazníka. Ginny ho našla v počítači a sdělila mu číslo zákaznického účtu v systému. „Nějaká zpoždění při vracení nebo nedoplatky?“ ptal se Tommy. „Nic tu není.“ „Bezva. Vložím ho do databáze později, až nám pojede internet. Chtěl by zaplatit Visa kartou, kterou prý platí ve vaší půjčovně, ale nemá ji tu u sebe. Jaké je číslo karty a datum platnosti?“ Ginny uvedla číslo i datum. „Díky za pomoc. Tak zatím.“ řekl Tommy a zavěsil.

Analýza podvodu:

První Tommyho telefonáty měly u Ginny jen vybudovat důvěru. Když přišel čas na útok, Ginny nechala ostražitost stranou a brala Tommyho jako pracovníka jiné půjčovny téže sítě. Proč by ho tak neměla vnímat? Vždyť už ho znala. Samozřejmě spolu hovořili jen po telefonu, ale stihli už navázat obchodní známost, která je základem důvěry. Jakmile ho přijala jako někoho, kdo pracuje ve stejné firmě, byl už zbytek jednoduchý.

Ukázka je z knihy *Umění klamu*

Phishing

Phishing je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce, vyzývajících adresáta k zadání jeho údajů na odkazované stránce. Tato stránka může například napodobovat přihlašovací okno internetového bankovnictví a uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

Ukázka:

Obrázek 1: Ukázka podvodné e-mailové zprávy (phishing)

Na obrázku 1 je vidět podvodná e-mailová zpráva, která se snaží uživateli namluvit, že je poslaná z banky.

Adresa odesílatele sice vypadá jako adresa skutečné banky, ale již v předmětu je zarážející jakési číslo za slovem Aktualizovat. Samotná zpráva má spoustu jazykových chyb (vypadá, jako by někdo zadal cizojazyčný text do překladače). V posledním řádku je uveden odkaz, který rozhodně nevede na stránky konkrétní banky.

IVR neboli telefonní phishing

Tato technika využívá falešného hlasového automatu (IVR) s podobnou strukturou, jakou má originální bankovní automat („Pro změnu hesla stiskněte 1, pro spojení s bankovním poradcem stiskněte 2“). Oběť je většinou vyzvána e-mailem k zavolání do banky za účelem ověření informace. Zde je pak požadováno přihlášení za pomoci PIN kódu nebo hesla. Některé automaty následně oběť kontaktují s útočníkem vystupujícím v roli telefonního bankovního poradce, což mu umožňuje pokládat další otázky.

Baiting

Baiting je považován za trojského koně v reálném světě.

Při tomto způsobu útoku útočník nechá infikované CD, flashdisk nebo jiné paměťové médium na místě, kde jej oběť s velkou pravděpodobností nalezne, například v koupelně, ve výtahu, na parkovišti. Poté již nechá pracovat zvědavost, díky které oběť dříve či později vloží toto médium do svého počítače. Tím dojde k instalaci viru, za jehož pomoci útočník získá přístup k počítači nebo celé firemní počítačové síti.

Quid pro quo aneb něco za něco

Něco za něco znamená náhodné vytáčení čísel společnosti člověkem, který se představí jako pracovník technické podpory. Existuje šance, že útočník nalezne zaměstnance nespokojeného s nějakým problémem a předstírá, že se mu pokusí po telefonu pomoci. Na oplátku požádá oběť o instalaci infikovaného programu nebo o provedení zvolené akce ve firemním informačním systému.

Hoax

Hoax neboli poplašná zpráva je záměrně vytvořená lež, která se vydává za pravdu. Většinou takováto zpráva obsahuje i prosbu o šíření mezi co největší skupinu přátel.

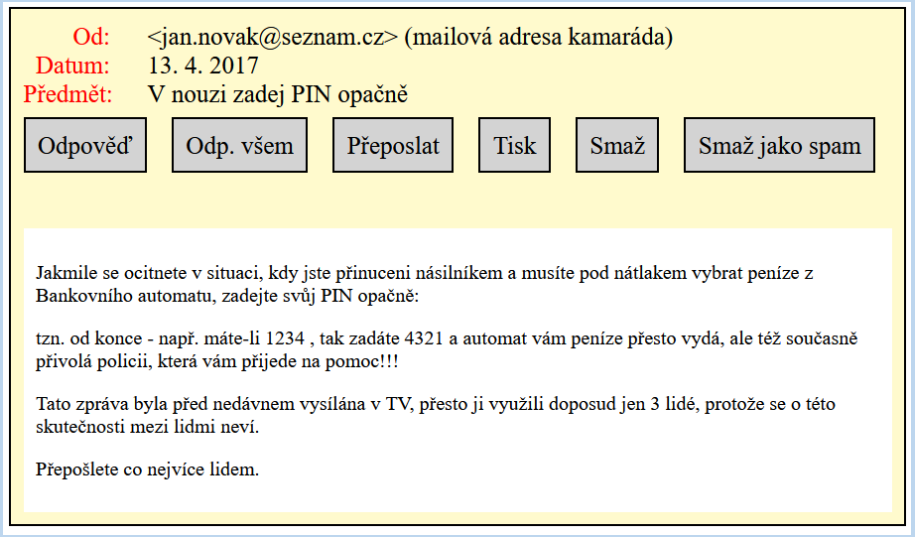
Hoaxy mají několik cílů. Jedním z důvodů, proč hoax někdo vytvoří, je poškození jednotlivce, firmy, určité značky či výrobku. Například se nám určitá zpráva snaží říct, že ten či onen výrobek způsobuje rakovinu nebo je testován na zvířatech.

Dalším cílem hoaxu je vystrašit příjemce zprávy. Jedná se například o zprávy o zpoplatnění Facebooku, WhatsApp.

Některé hoaxy se ale snaží z důvěřivých lidí vylákat i peníze nebo citlivé údaje. Zpráva například využije nějakou mediálně známou katastrofu ve světě a nabádá lidi k finančnímu přispění na účet, ze kterého ovšem peníze nejdou na pomoc obětem.

Webová stránka, která se zabývá hoaxy, shromažďuje zprávy a vysvětluje podstatu lží, je https://www.hoax.cz/.

Ukázka:



Obrázek 2: Ukázka poplašné e-mailové zprávy – hoaxu

E-mailová zpráva přišla od kamaráda, který hoaxu uvěřil a s dobrým úmyslem ji poslal dál.

Zpráva o tom, že zadání PIN kódu do bankomatu pozpátku umožní výběr hotovosti a zalarmuje policii, je zcela nesmyslná. Ke každé kartě patří jedinečný PIN. Pouze správně zadaný PIN umožní provádět v bankomatu transakce s kartou. PIN kód zadaný pozpátku je chybný PIN kód a po jeho zadání nelze provést žádnou transakci (ani výběr hotovosti).

Úkol

Rozhodněte, které e-maily jsou podvodné a proč.

Zpráva 1:

Obrázek 3: Úkol – zpráva 1

Zpráva 2:

Od: <jan.novak@seznam.cz> (mailová adresa kamaráda)
Datum: 1. 12. 2020 8:15
Předmět: Ahoj všichni, kdo máte CZ-mobily !!!!!!!!!!

Odpověď | Odp. všem | Přeposlat | Tisk | Smaž | Smaž jako spam

Ahoj všichni, kdo máte CZ-mobily !!!!!!!!!!

Tohle není přeposlaný mail, ani hoax, stalo se mi to dneska.

Byla jsem dnes celý den pryč a po návratu domů jsem měla na mobilu 8 nepřijatých hovorů v rozsahu tak hodinu mezi telefonáty, vše z telefonního čísla +420 477 100 111. Když jsem to nevěřícně studovala, začal mi telefon zvonit v ruce znovu....

Protože mi to začalo být hodně podezřelé, začala jsem pátrat po tomto telefonním čísle na nternetu, a narazila jsem na diskusi, kde si lidé stěžují, že jim toto číslo číslo volá taky pravidelně, a když telefon zvednou, hovor se automaticky přeruší, nicméně ve vyučtování na konci měsíce mají tzv. dárcovské volání t.j.,jak jsem to snad správně pochopila, objeví se jim ve výpisu stržena jakási částka, kterou vůbec neprotelefonovali # s poznámkou, že jde o tzv.. dárcovské volání.

Takže, prosím, toto číslo si někam všichni napište a když se objeví na mobilu, tak nezvedat !!!!!!!

Tady odkaz na stránky, které jsem o tom na internetu našla:

http://www.tet.cz/forum/viewtopic.php?p=13638

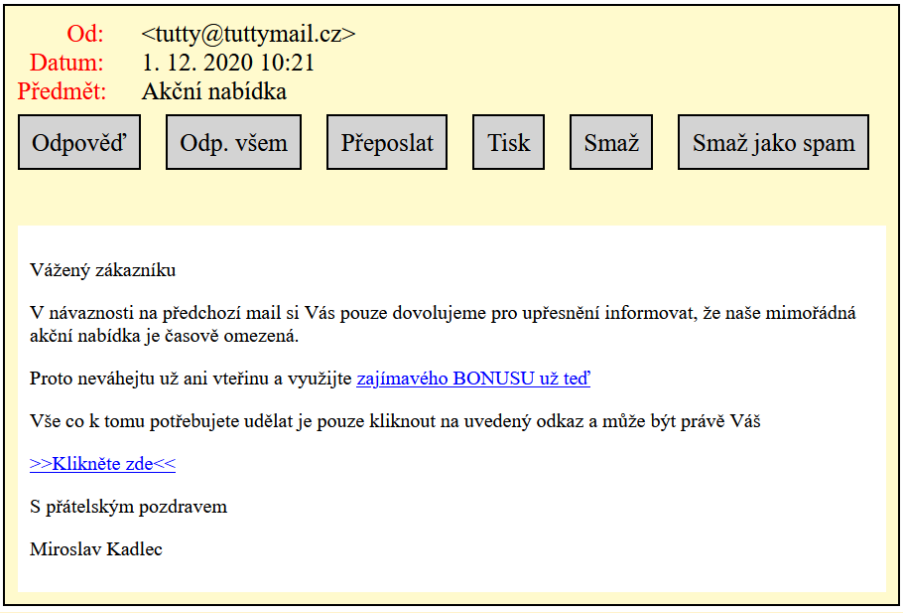
Během doby, než jsem napsala tento mail, zvonil ještě dvakrát....

PROSÍM POŠLETE DALŠIM KAMARÁDŮM A ZNÁMÝM.

DÍKY.

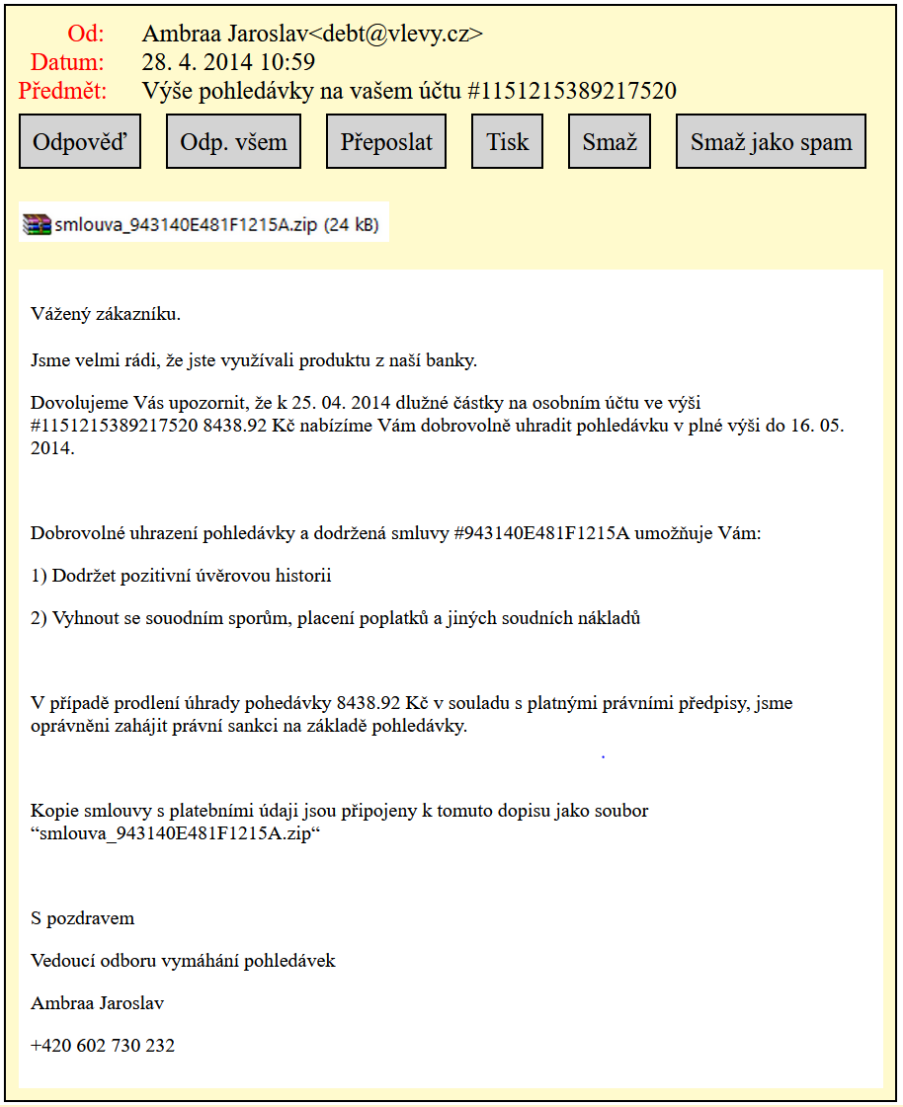
Obrázek 4: Úkol – zpráva 2

Zpráva 3:



Obrázek 5: Úkol – zpráva 3

Zpráva 4:



Obrázek 6: Úkol – zpráva 4

Zpráva 5:

Od: <dotaznik@sperky4u.eu>
Datum: 16. 1. 2021 16:12
Předmět: Ohodnoťte Šperky4U.eu na základě vašeho nákupu

Odpověď | Odp. všem | Přeposlat | Tisk | Smaž | Smaž jako spam

OVĚŘENO ZÁKAZNÍKY Heureka

Vážený zákazníku,

děkujeme za váš nákup v obchodě Šperky4U.eu před 9 dny. Ohodnoťte, prosím, obchod a zakoupené produkty: Ocelový řetízek, šíře 3 mm (šíře řetízku: 3 mm, délka řetízku: 60 cm) OPE1092-030-60

Doporučili byste obchod Šperky4U.eu svým známým?

Doporučuji | Nedoporučuji

Vaše hodnocení pomůže zlepšit naše služby a poslouží ostatním nakupujícím při výběru vhodného obchodu.

Předem děkujeme za váš názor.

Obchod Šperky4U.eu

OVĚŘENO ZÁKAZNÍKY Heureka

Získali jsme zlatý certifikát Ověřeno zákazníky na základě reálných recenzí našich zákazníků, zaslaných touto cestou. Nezávislé hodnocení nakupujících poskytuje Heureka.cz.

Obrázek 7: Úkol – zpráva 5

Řešení

Zde je řešení jednotlivých příběhů.

Zpráva 1:

První zpráva vypadá dle adresy odesíláte jako zpráva od poskytovatele e-mailové schránky na stránkách www.seznam.cz. Odkaz ale odkazuje na podvodnou stránku, která se snaží vylákat z uživatele přihlašovací údaje do jeho mailové schránky.

Jedná se tedy o podvodný e-mail.

Zpráva 2:

Druhou zprávu odeslal kamarád, který mail přeposlal v dobré víře, že informace v něm jsou pravdivé. Na internetové adrese uvedené v textu řetězové zprávy byl uveden odkaz na skutečné diskuzní fórum, kde se o tomto telefonním čísle diskutuje. Některé příspěvky potvrzují, že z uvedeného čísla jim bylo několikrát voláno, což možné je. Objevují se zde však i různé rádoby zajímavé příspěvky o částkách naúčtovaných za přijatý hovor, nebo dokonce SMS. Pokud by pisatel dodal, že byl v zahraničí a hovor byl uskutečněn přes roaming, dalo by se tomu i věřit, ale pokud se jednalo o tuzemský hovor přes klasického operátora, je toto tvrzení pochybné. Za přijaté hovory se neplatí. Jediná možnost je volání na účet volaného, ale tuto informaci se příjemce dozví při přijetí hovoru a musí s platbou souhlasit.

Jedná se tedy o poplašnou zprávu.

Zpráva 3:

Třetí zpráva přišla z neznámé a neoficiální mailové adresy. Zpráva se snaží nalákat uživatele na akční nabídku, ale již nezmiňuje jakého produktu. Snaží se na uživatele naléhat časovým omezením. Nutí tak uživatele jednat okamžitě, aby neměl čas na rozmyšlenou. Samotné odkazy jsou skryté pod textem.

Jedná se tedy o podvodný e-mail.

Zpráva 4:

Čtvrtá zpráva se snaží vzbudit v uživateli strach, že dluží určitou částku za úvěr a hrozí mu exekuce. Odesílatel dokonce posílá v příloze uživateli soubor se smlouvou. Příloha je typu zip (tedy zabalený soubor, kdy není jasné kolik souborů a jakého typu jsou uvnitř tohoto zip souboru), a může tedy obsahovat malware (škodlivý software). Časová naléhavost a strach z exekuce nutí uživatele stáhnout přílohu a ujistit se, zda se jedná o chybu či skutečnost. Podpis odesílatele obsahuje i telefonní číslo, aby zpráva působila důvěryhodně (telefon na tomto čísle ale pravděpodobně nebude nikdo zvedat nebo bude náhodně vygenerované a člověk na druhém konci nebude mít o ničem ani tušení).

Jedná se tedy o podvodný e-mail.

Zpráva 5:

Zprávu 5 poslal e-shop, kde byl uskutečněn nákup. Informace v e-mailu souhlasí s uskutečněným nákupem. Portál Heuréka, který je uvedený v e-mailu, skutečně existuje (je to cenový srovnávač a nákupní rádce, který funguje na základě zkušeností uživatelů) a snaží se získat od uživatele informace o zakoupeném produktu tak, aby mohl udělit doporučení pro další potenciální zákazníky.

Jedná se tedy o bezpečný e-mail.

Způsoby ochrany

Existuje spousta možností, jak se před útočníky chránit.

Fyzický přístup

Jedním ze způsobů ochrany je zamezení samotnému přístupu k počítači či dalším prvkům sítě, jako je například router (to je zařízení, které spojuje počítač a síť nebo sítě mezi sebou). Doma si také zamykáme a neumožňujeme tak snadný přístup zlodějům k našim cennostem.

Hesla

Jedna z nejdůležitějších věcí pro ochranu je použití hesel.

Heslo do systému

Pro případ, že by se někdo mohl k vašemu počítači dostat, je dobré zabezpečit vstup do systému heslem.

Operační systém Windows 10 má toto nastavené již po nainstalování systému. Nastavení hesla lze provést v nastavení uživatelských účtů.

Nejjednodušší způsob přidání nebo změny hesla v systémech Windows je stisknutí tří kláves najednou: CTRL + ALT + DELETE a vybrání volby „Změnit heslo“.

Hesla k účtům

Dále je důležité mít nastavená hesla i pro další aplikace, které uživatel používá (například: e-mail, internetové bankovnictví, přístup do diskuzního fóra).

Pravidla

Existuje několik pravidel pro práci s hesly.

Použití silných hesel

Udává se, že minimální délka hesla by měla být alespoň 8 znaků.

Heslo by nemělo mít žádnou spojitost s osobou, která jej používá (tedy žádná jména, přezdívky, data narození, jména mazlíčků…). Dokonce se doporučuje, aby heslo neobsahovalo žádné smysluplné slovo. Existují seznamy slov, které útočníci používají k prolomení hesla, a není pro ně tedy překážka „uhádnout" heslo, i když nemá s danou osobou žádnou spojitost.

V heslu by se měly objevit znaky z minimálně čtyř znakových sad:

- Malá písmena: a–z (26 znaků)
- Velká písmena: A–Z (26 znaků)
- Číslice: 0-9 (10 znaků)
- Speciální znaky: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (32 znaků)
- Písmena s háčky: ěščřžťňďĚŠČŘŽŤŇĎ (16 znaků)
- Dlouhé hlásky: áéíóúůýí (8 znaků)

Na typu účtu záleží, které znakové sady jsou k tvorbě hesla povolené.

Existují internetové stránky, které Vám heslo dle zadaných kritérií vytvoří:

- hsgi.cz/generator-hesel
- generator-hesel.cz

Použití správce hesel

Každé heslo by mělo být použito právě jednou, tedy pro jeden účet. Heslo by nemělo být zapsané nikde na papírku ani v textovém či jiném souboru v počítači. A hesla by se také měla pravidelně měnit. V dnešní době není výjimkou, že lidé používají i několik desítek účtů. Není pak v lidských silách si všechna tato hesla zapamatovat.

Jendou z možností je vytvořit si systém tvorby hesel. Například: Pro tvorbu hesla si zvolím oblíbenou písničku.

Měla babka čtyři jabka a dědoušek jen dvě.

Pro tvorbu hesla využiji z věty vždy počáteční písmeno slov, pro počet jablek číslovku, místo spojky „a“ znaménko + a na konec přidám ještě vykřičník. Výsledné heslo je: **Mb4j+dj2!**

Druhá možnost je použití některého správce hesel. Jedná se o programy, do nichž se zadají všechna hesla. K přístupu k heslům pak stačí jedno heslo, kterým je zabezpečen tento program. Tyto programy existují i v cloudové verzi (informace jsou uložené na serveru na internetu a člověk po zadání svých přístupových údajů má svůj učet k dispozici na jakémkoliv zařízení připojeném k internetu).

Nejznámější programy pro správu hesel, které jsou zadarmo:

- StickyPassword.com/cz – česky
- LastPass.com
- Dashlane.com

- Nordpass.com
- Bitwarden.com

Úkol

Pokuste se vytvořit silné heslo.

Svoje heslo si ověřte na stránce passwordmeter.com (nebo speedweb.cz/index.php?akce=pass – stránka česky).

Vícefázové ověření

Pro přístup k účtu je zapotřebí více faktorů (důkazů) potvrzujících vaši identitu. V praxi se nejčastěji používá dvoufázové ověření. Prvním ověřením bývá zpravidla uživatelské jméno a heslo, druhým pak například otisk prstu, snímek sítnice oka nebo PIN kód, který přijde jako SMS zpráva na mobilní telefon a je časově omezen.

Aktualizace softwaru

Aktualizace softwaru je v informatice postup, při kterém je do počítače instalována novější verze jeho programového vybavení. Výhoda aktualizací není jen novější verze s novými funkcemi, ale aktualizace hlavně obsahují tzv. záplaty (tedy opravy bezpečnostních děr systému).

Programy z ověřených zdrojů

Programy stažené z neověřených zdrojů mohou obsahovat škodlivý software, který si uživatel nainstaluje s programem. Tento škodlivý software většinou

obsahuje i nelegální software (to znamená, že pokud produkt není zadarmo a někdo ho zadarmo nabízí nebo k němu nabízí tzv. crack (malý program sloužící k odstranění či omezení funkčnosti ochranných prvků jiného programu). V dnešní době existuje téměř ke každému komerčnímu produktu jeho volně šiřitelná varianta.

Antivirový program

Antivirový program (zkráceně *antivir*) je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého softwaru (malware). K zajištění této úlohy se používají dvě odlišné techniky:

- Virová databáze – prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.
- Nebezpečné chování – detekce podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Při kontrole souboru antivirový program zjišťuje, zda se nějaká jeho část neshoduje s některým ze známých virů, které má zapsány v databázi. Pokud je nalezena shoda, má program tyto možnosti:

- Pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)

- Umístit soubor do karantény (škodlivý software se nemůže dále šířit, protože ho nelze dále používat)
- Smazat infikovaný soubor (i se škodlivým softwarem)

K dosažení trvalého úspěchu ve středním a dlouhém období vyžaduje virová databáze pravidelné aktualizace, které obsahují informace o nových virech. Pokud je antivirový program neaktualizovaný, představují viry přinejmenším stejné nebezpečí, jako kdyby antivir v počítači vůbec nebyl! Uživatelé mohou sami zaslat svůj infikovaný soubor výrobcům antivirových programů, kteří informaci o novém viru začlení do databáze virů.

Metoda zjištění nebezpečného chování se oproti virovým databázím nesnaží najít známé viry, namísto toho sleduje chování všech programů. Pokud se takový program pokusí zapsat data do spustitelného programu, antivirus označí toto nebezpečné chování a upozorní uživatele, který je antivirovým programem vyzván k výběru dalšího postupu.

Tento postup zjištění nových virů má tu výhodu, že ačkoli je virus zcela nový a neznámý ve virových databázích, můžeme ho snadno odhalit. Nicméně i tato metoda má své nevýhody. Stává se, že antivirový program hlásí spoustu falešných „nálezů“ viru. To může vést k tomu, že uživatel postupem času přestane vnímat „pravá“ varování. Pokud tedy uživatel automaticky povolí pokračování programu, je jasné, že v takovém případě antivirus již neplní svoji funkci varovat uživatele před možným nebezpečím. Z tohoto důvodu tento postup stále více moderních antivirových programů přestává využívat.

Dnešní antivirové programy neslouží pouze jako ochrana před viry, ale také jako komplexní zabezpečení zařízení. Je například možné nainstalovat doplněk do webového prohlížeče a upozornit na nebezpečné webové stránky, mít vlastního správce hesel a mnoho dalšího.

Mezi nejpoužívanější antivirové programy nejen pro počítače, ale i pro chytrá zařízení se aktuálně řadí Norton, Kaspersky, Avast, AVG nebo například ESET.

Zálohování dat

Ztráta dat nemusí být způsobena pouze odcizením, kdy k datům má uživatel stále přístup. Počítač je jen stroj, který se může rozbít, a uživatel tak může o data přijít. Je tedy nutné důležitá data zálohovat.

Záloha je kopie dat uložená na jiném datovém nosiči (např. externí pevný disk, flashdisk) nebo na jiném místě (např. cloudové úložiště – místo na internetu).

Záložní data jsou využívána v případě ztráty, poškození nebo jiné potřeby práce s daty uloženými v minulosti. Zálohování probíhá nepravidelně (např. v domácnostech) nebo pravidelně podle rozvrhu (např. ve firmách).

Zdravý rozum

Nejdůležitější v bezpečnosti je používání tzv. zdravého rozumu. Vždy je vhodné dobře si rozmyslet, na jaký odkaz klikáme, jaké informace, komu a jak posíláme.

Seznam obrázků

Seznam literatury

[1] *Bezpečná síť: I internet může být nebezpečný!* [online]. c2014 [cit. 2021-01-19]. Dostupné z: https://bezpecnasit.webnode.cz/

[2] *CyberSekurity.CZ* [online]. c2010 - 2021 [cit. 2021-01-11]. Dostupné z: https://www.cybersecurity.cz

[3] *Internetem BEZPEČNĚ* [online]. Karlovy Vary [cit. 2021-01-18]. Dostupné z: https://www.internetembezpecne.cz/

[4] *E-bezpečí* [online]. Olomouc, c2008-2020 [cit. 2021-01-19]. Dostupné z: https://www.e-bezpeci.cz/. ISSN: 2571-1679

[5] MATĚJÍČEK, Pavel. Deset nejznámějších virů historie. *Computerworld: Deník pro IT profesionály* [online]. Praha: Internet Info DG, 31. 05. 2018 [cit. 2021-01-19]. Dostupné z: https://computerworld.cz/software/deset-nejznamejsich-viru-historie-54722

[6] MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6

[7] Zeus Virus. *Kaspersky* [online]. AO Kaspersky Lab, c2021 [cit. 2021-01-19]. Dostupné z: https://usa.kaspersky.com/resource-center/threats/zeus-viru

Poznámky:


PROCHÁZKY
PRAHOU


MATEMATIKA