Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MPSV

Metodika dalšího vzdělávání v oblasti kybernetické bezpečnosti

Výstup KA 01, č. 13

DigiStrategie 2020 | rozvoj systémové podpory digitální gramotnosti

Metodika dalšího vzdělávání v oblasti kybernetické bezpečnosti

Výstup KA 01, č. 13

Název projektu:	Rozvoj systémové podpory digitální gramotnosti
Registrační číslo projektu:	CZ.03.1.54/0.0/0.0/16_020/0005634
Publikováno:	květen 2021
Zpracovali:	kolektiv autorů projektu DigiStrategie 2020
Grafická úprava:	Anna Lhoťanová

Obsah

Cílem dokumentu je obsáhnout potřebné informace, praktické rady a doporučení v oblasti kybernetické bezpečnosti pro další vzdělávání zaměstnanců působících na trhu práce. Seznámit uživatele internetu s pravidly bezpečnosti, riziky, hrozbami, ale také zásadami bezpečného chování na internetu. Metodika bude využitelná pro vzdělavatele, kterým bude návodem při vzdělávání. Jedná se o klíčový materiál na úrovni nastavení systému dalšího vzdělávání v oblasti rozvoje digitální gramotnosti.

1. Úvod

Důvod vzniku dokumentu

V současné době dochází k nebývalému nárůstu digitálních technologií. V souvislosti s pandemií koronaviru se rozšiřuje práce z domova, porady se dělají on-line, lidé nakupují v eshopech, školy a vzdělávací instituce přechází na on-line výuku a řada povolání hledá nové možnosti v on-line světě. To vše se děje v tzv. kyberprostoru, jehož hlavní vstupní branou je internet.

Je reálný předpoklad, že využívání digitálních technologií se bude neustále zvyšovat. Ten, kdo bude zručný v jejich využívání, bude mít větší šanci na lepší uplatnění v zaměstnání i mimo něj. Lidé si tento fakt uvědomují a zvyšují si své digitální kompetence, nejvíce se však zaměřují na oblasti, které přímo souvisí s využíváním digitálních technologií - Informační a datová gramotnost, Komunikace a spolupráce a Tvorba digitálního obsahu. Oblast bezpečnosti je ale často podceňována, ne-li zcela opomíjena.

Odvrácenou stranou je to, že lidé si neuvědomují, že na internetu a někdy i ve svých zařízeních mají velké množství dat, včetně těch osobních, o které mohou přijít. Prostřednictvím internetu provádí finančních transakce, sdílí zde svoje názory, umisťují sem svoje fotky a videa, komunikují s dalšími lidmi… S tím vším jsou spojená určitá rizika, díky kterým mohou přijít o své finance, o svá data i o svou pověst.

Záměrem tohoto materiálu je napomoci k tomu, aby se k cílovým skupinám dostaly patřičné informace o tom, že v kyberprostoru na ně číhá řada nebezpečí a občané ČR budou brát ochranu svých zařízení, programů, financí, dat i soukromí o mnoho vážněji.

Vymezení cílové skupiny

Dokument se zaměřuje prioritně na tři cílové skupiny:

a) Vzdělávací organizace, které se zabývají vzděláváním občanů v oblasti IT, pro které bude dokument metodikou pro vzdělávání.

b) Zaměstnanci působící na trhu práce.

c) Občané ČR, kteří mají základní znalosti a dovednosti v práci s internetem, nutně je nepotřebují k výkonu svého zaměstnání, ale využívají je ve svém soukromém životě. Minimálně nebo vůbec se věnuje své kybernetické bezpečnosti.

Obecný popis cílů a návrhy řešení

Cílem dokumentu je obsáhnout potřebné informace, praktické rady a doporučení v oblasti kybernetické bezpečnosti pro další vzdělávání zaměstnanců působících na trhu práce.

Seznámit uživatele internetu s pravidly bezpečnosti, riziky, hrozbami, ale také zásadami bezpečného chování na internetu.

Metodika bude využitelná pro vzdělavatele, kterým bude návodem při vzdělávání.

Jak to celé řešit (z pohledu DiGi strategie)

Co máme

- Komplexní materiál o kybernetické bezpečnosti s popisem kybernetických hrozeb (Příloha B)
- Materiál Otázky a odpovědi (Příloha A)
- Příběhy o kybernetických útocích a jejich důsledcích
- Program Chyťme hackera (Příloha C)
- Metodiku pro vzdělavatele, jak s tímto programem pracovat (Příloha D)
- Zpravodaj ke kyberbezpečnosti
- Video Jak chránit své osobní údaje a soukromí na internetu (https://portaldigi.cz/digi-videa/jak-chranit-sve-osobni-udaje-a-soukromi-na-internetu/)
- Webovou stránku Portál Digi s články o kyberbezpečnosti

Co s tím

Poradenství

- Vytvořit informační a metodickou webovou stránku o kybernetické bezpečnosti (informační pro veřejnost, metodickou pro organizátory programů)
  - Popis situace
  - Kybernetické hrozby a obrana proti ním
  - Příběhy, které se staly a mohou se stát (+ případná videa)
  - Otázky a odpovědi
  - Sekce pro vzdělavatele (materiály programu Chyťme hackera, včetně materiálů pro organizátory
  - (On-line hra Chyťme hackera)
  - Sekce pro školní metodiky prevence
  - Inspirace z praxe
- K tomu využít facebookovou stránku Digistrategie
- Připavit a realizovat facebookovou kampaň s příběhy o kybernetických hrozbách

Program Chyťme hackera

- Dopracovat program (případná videa, další varianty otázek a úkolů, propagační a informační materiály, grafické zpracování…)
- Ideálně převést program do on-line podoby pro snadnější replikovatelnost
- Připravit e-learningovou podporu pro organizátory a školní metodiky prevence programu, včetně podpory konzultační
- Odpilotovat program v 5ti organizacích
- Dopracovat jej
- Informovat potenciální organizace a školní metodiky prevence
- Připravit možnosti finanční podpory
- Nabídnout k využití

2. Kontextualizace a zacílení

Strategie digitální gramotnosti ČR na období 2015 až 2020 a její Akční plán, legislativní opatření v oblasti bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí. Konkrétní plnění opatření daného akčního plánu, spolupráce s projektem Digi-Strategie 2020 (zadavatel), popis vzniku a konkrétní zacílení včetně definování výsledku při implementaci metod efektivního poradenství v oblasti internetové bezpečnosti a online příležitostí.

Doporučení z konference "Kybernetické výzvy a hrozby – CYBER":

„Bezpečný kyberprostor je nezbytnou podmínkou rozvoje, týkajícího se všech obyvatel společného prostoru svobody, bezpečnosti a spravedlnosti, a souvisejícího s koncepty eGovermentu."

V roce 2019 došlo k dalšímu nárůstu počtu kybernetických útoků proti naší zemi, z nichž některé lze označit za velmi vážné. Řada veřejných i soukromých institucí se musela vyrovnávat s obranou před těmito útoky a odstraňováním jejich následků. Národní úřad pro kybernetickou a informační bezpečnost v průběhu roku řešil 78 kybernetických incidentů. Jeho pracovníci pomáhali napadeným institucím státní správy, územní samosprávy, nemocnicím i firmám s obnovováním jejich systémů, a to jak formou doporučení a metodické pomoci, tak i fyzicky přímo na místech incidentů. Úřad byl této podpory schopen jen díky týmové práci, maximálnímu úsilí a pracovnímu nasazení všech jeho zaměstnanců.

V prosinci 2019 došlo ke kybernetickému útoku proti systémům Nemocnice Rudolfa a Stefanie Benešov, spádové nemocnici až pro 400 000 lidí. Ransomware zašifroval data na serverech, nemocničních přístrojích a pracovních stanicích. V ordinacích nebylo možné provádět standardní ošetření, rušily se plánované operace a hospitalizovaní pacienti museli být převezeni do okolních nemocnic, včetně pacientů na jednotce intenzivní péče. Obnovení plného provozu trvalo téměř měsíc a následky útoku byly vyčísleny na 40–50 milionů korun.

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019

Každý rokem se zvyšují počty kybernetické kriminality.

Národní strategie kybernetické bezpečnosti na léta 2015 – 2020

Jedním z požadavků Národní strategie kybernetické bezpečnosti na léta 2015 – 2020 je navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

1. ledna 2015 vstoupil v platnost Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon obsahuje komplexní zákonnou úpravou reagující na objektivně existující potřebu zabezpečení České republiky a jejích národních zájmů před kybernetickými bezpečnostními incidenty.

Zákon se nedotýká uživatelů ani poskytovatelů obsahu; orgány a osobami, na které zákon

dopadá, jsou subjekty, jejichž systémy, sítě nebo služby mají zásadní význam pro fungování státu nebo informační společnosti. Pouze při vyhlášení stavu kybernetického nebezpečí se okruh subjektů, majících na úseku kybernetické bezpečnosti povinnost provádět opatření, rozšiřuje i na ostatní poskytovatele služeb a správce systémů a sítí.

https://www.sagit.cz/info/sb-anotace-sb14181a

Strategie digitální gramotnosti ČR na období 2015 až 2020

Ve Strategii digitální gramotnosti ČR na období 2015 až 2020 se říká, že bezpečné využívání digitálních technologií je jednou ze základních kompetencí digitální gramotnosti a zaslouží si patřičnou pozornost. Zvyšování digitální gramotnosti, včetně povědomí o kybernetické bezpečnosti (rizicích i prevenci) je v současné době nutností a je třeba se zaměřovat, krom zaměstnanců veřejné správy, na zranitelné skupiny populace, jimiž jsou především děti a senioři.

K tomu je třeba:

- Zvýšit informovanost a digitální gramotnost rodinných příslušníků za účelem zvýšení schopnosti rodiny využívat příležitosti a čelit rizikům spojeným s digitálními technologiemi.
- Zajistit dostupné poradenství v otázkách bezpečnosti a příležitostí včetně internetového poradenství.
- Realizovat mezigenerační vzdělávací programy pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií.

3. Metodologie identifikace dostupného poradenství v otázkách bezpečnosti a online příležitostí včetně internetového poradenství

Popis využité metodologie, konkrétních přístupů, vybraných pramenů a zdrojů v oblasti podporující rozvoj jednorázového i dlouhodobého poradenství pro otázky bezpečnosti a podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí.

1) Otázky a odpovědi

Soubor nejčastěji kladených otázek a odpovědí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí.

Příloha A: Otázky a odpovědi

2) Popis s příběhy a návody, jak se bránit kybernetickým hrozbám

Metodika pro pracovníky organizací (školy, volnočasové instituce, knihovny, galerie, muzea aj.) poskytující poradenství rodičům, prarodičům a dětem v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí.

Příloha B: Kybernetická bezpečnost

3) Kooperativní program Chyťme hackera

Mezigenerační vzdělávací program pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.

Příloha C: Chyťme hackera

4) Příručka pro lektory k realizaci programu Chyťte hackera

Metodika pro lektory mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.

Příloha D: rozpracovaná do pokynů pro lektory

4. Identifikace (kritéria identifikace)

Popis klíčových otázek. Identifikace problémových oblastí, návrhy indikátorů v oblasti dostupného poradenství v otázkách bezpečnosti a online příležitostí včetně internetového poradenství, které se mohou překlopit do vhodných nástrojů na realizaci dostupného poradenství v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí.

Snahou autorů tohoto materiálu bylo připravit takovou podporu týkající se kybernetické bezpečnosti, aby vzdělávací instituce, lektoři, školní metodici prevence a další dokázali snadným způsobem připravovat své programy zaměřené na kybernetickou bezpečnost.

Při přípravě a realizaci poradenských programů je třeba přemýšlet o řadě otázek:

Cílí poradenské programy na problematiku kyberbetické bezpečnosti?

Důležité je v těchto programech držet téma kybernetické bezpečnosti a zaměřit se na ty nejdůležitější informace, které je k občanům ČR dostat:

- Vysvětlit, že kybernetická bezpečnost se týká každého z nás.
- Seznámit se základní terminologií kybernetické bezpečnosti.
- Vysvětlit, jaké mají kybernetické útoky cíle.
- Seznamovat občany ČR s celou řadou technik a nástrojů kybernetických útoků a s dalšími hrozbami. Jedná se zejména o tyto:
  - Malware (velká skupina různých typů škodlivého software)
  - Sociální inženýrství
  - Kyberšikana
  - Útoky na infrastrukturu
  - Úniky dat
  - Poškození zařízení
- Vysvětlit, jak se těmto hrozbám mohou občané bránit.
- Vysvětlit, že v případě kybernetických útoků se jedná o trestnou činnost.

Jsou poradenské programy dlouhodobost a systematické?

Programy se vyznačují dlouhodobostí, systémem a návazností. Ideální je, když jsou dílčí programy součástí dlouhodobějšího programu. Jednorázové akce, bez návaznosti, nemají valný význam.

Program Chyťme hackera je lepší ve školách realizovat postupně po jednotlivých kolech a mezi ně vkládat další dílčí aktivity, které rozvíjí povědomost o kybernetických hrozbách, pravidlech bezpečnosti a zásadách bezpečného chování na internetu.

Jsou poradenské programy podávány srozumitelně?

Základem dobrého programu je srozumitelnost obsahu, kdy každý účastník musí porozumět tak těžkému tématu jako je kybernetická bezpečnost. Je nutné toto těžké téma vysvětlovat za pomoci interaktivních a zábavných prvků. Nudné a těžké přednášky prošpikované odbornými výrazy je třeba omezit na naprosté minimum.

Jsou poradenské programy variabilní?

Materiál srozumitelnou formou popisuje většinu kybernetických hrozeb. Silnou stránkou jsou příběhy, které ukazují, co se každému z nás, kdo je připojen k internetu, může stát. Každá hrozba je popsána (název, charakteristika, důsledky). Následuje poučení, jak se hrozbě bránit.

Tyto popisy hrozeb spolu s dalšími výstupy, které vznikají v Digistrategii (například videa) mohou být silným pomocníkem v poradenských programech týkajících se kybernetické bezpečnosti. Vzdělavatelé si tak mohou poskládat svůj program z řady dílčích programů, který se rozhodli realizovat s ohledem na svoje cíle a s ohledem na věk a potřeby potenciálních účastníků.

Je poradenský program realizován za pomoci digitálních technologií?

Důležitým aspektem rovněž je realizovat poradenské programy prostřednictvím digitálních technologií a ukazovat tyto technologie jako dobrého pomocníka pro fungování v normálním životě. Zároveň tím zvyšovat jejich digitální kompetence.

Navazuje na poradenské programy další podpora?

Na konci poradenského programu jsou účastníci trochu postrašení celou škálou možností, jak se dostat do problémů v souvislosti s podceněním ochrany svých zařízení a také svým slabým povědomím o této problematice. Jsou motivováni k tomu svůj přístup zlepšit. Zde musí dostat další informační materiály, odkazy na webové stránky s touto problematikou. Žáci a studenti mohou pokračovat v návazném on-line programu. Cílem je, aby se účastníci získali takové vědomosti a dovednosti, které jim pomohou ubránit se kybernetickým útokům.

Jsou organizátoři a lektoři vzděláváni, aby dokázali dobře realizovat připravené poradenské programy?

Organizátoři a lektoři musí být uvedení do problematiky kybernetické bezpečnosti. Nutně však musí umět realizovat připravené programy a znát jejich obsah, aby dokázali naplňovat jeho vzdělávací cíle. K tomu jsou dvě základní cesty - prezenční a on-line.

Vědí organizátoři, jak dostat poradenské programy k cílovým skupinám?

Jedna věc je umět poradenské programy realizovat, druhá věc je dostat k občanům ČR. Zde je třeba přemýšlet o možných cestách, jak toho dosáhnout. Je třeba zabývat se marketingem, rozhodnout se, zda půjdou občané ČR za programem do sálů a učeben, nebo naopak – programy půjdou za občany, například on-line způsobem.

5. Analýza

Analýza existujících forem a způsobů efektivních metod dostupného poradenství pro otázky bezpečnosti a podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí.

V ČR funguje řada organizací a projektů, které se zabývají poradenskou činností týkající se rizik internetu a chování v něm. Většina organizací a programů však cílí především na poradenství v kyberšikaně, zejména u dětí a mládeže.

Kyberkompas (https://security.muni.cz/cybercompass***)***
Šestidílný online kurz Masarykovy univerzity týkající se kyberbezpečnosti, která jej poskytuje svým studentům i široké veřejnosti.

Kurz zvyšuje uživatelské kompetence v oblasti zabezpečení zařízení, nastavení hesel nebo i hlášení incidentů.

Témata kybernetické bezpečnosti: Malware, Phishing, Obrana…

Internetem bezpečně (https://www.internetembezpecne.cz/***)***
Projekt spolku you connected, z.s., v rámci kterého vznikl informační web, osvětová videa, přednášky a vzdělávací učebnice.

Témata kybernetické bezpečnosti: Malware, Viry, Ransomware, Botnet, Sociální inženýrství, Phishing…

Buď safe online (https://www.avast.com/cz/besafeonline/***)***
Osvětový online projekt antivirové společnosti Avast, který poskytuje materiály a interaktivní hry pro učitele, rodiče i děti. S youtuberem Jirkou Králem byl připraven soubor vzdělávacích videí zaměřených na jednotlivé hrozby v kyberprostoru.

Témata kybernetické bezpečnosti: Phishing, malware nebo ransomware.

Junior centrum excelence informační bezpečnosti (https://www.nsmcluster.com/doc/_JCE_Koncepce.pdf)
Autorem koncepce středoškolských Junior center excelence je Network Security Monitoring Cluster (NSMC), sdružení dvaceti českých firem a expertů v oblasti informační a kybernetické bezpečnosti. Junior centrum excelence informační bezpečnosti se zaměřují na výuku informační a kybernetické bezpečnosti, kdy poskytují odbornou i technickou pomoc při výuce kybernetické bezpečnosti celému regionu. Cílem je, aby v každém kraji byla minimálně jedna střední škola, která bude zastávat úlohu juniorního centra.

Témata kybernetické bezpečnosti: Úvod do IB, Kybernetický prostor, Sociální inženýrství, Právo v oblasti IB

Bezpečně na netu (https://www.bezpecnenanetu.cz***)***
Osvětový projekt sdružení CZ.NIC, jehož záměrem je bezpečnější internet. Projekt se zabývá poradenskou činností, tvorba metodických materiálů pro učitele a rodiče a nabízí celou řadu vzdělávacích kurzů.

Témata kybernetické bezpečnosti: Kurz Bezpečnost a soukromí na Internetu

Jak na internet (https://www.jaknainternet.cz/***)***

Druhý projekt sdružení CZ.NIC. Jedná se o zábavná, dvouminutová videa, moderovaná Romanem Zachem, která přibližují divákům širokou problematiku Internetu. Mezi desítkami videí je několik videí zaměřených na kybernetickou bezpečnost

Témata kybernetické bezpečnosti: Phishing, Malware

Kraje pro bezpečný internet (https://www.kpbi.cz/#***)***

Projekt Kraje pro bezpečný internet je výsledkem iniciativy Asociace krajů ČR spojené s úsilím zvýšit informovanost o rizicích internetu a možnostech prevence a pomoci.

Témata kybernetické bezpečnosti: některé otázky v kvízech

E-Bezpečí (https://www.e-bezpeci.cz***)***

E-Bezpečí je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi.

Témata kybernetické bezpečnosti: -

Digitální stopa (https://moodle.nic.cz/course/view.php?id=15***)***

V roce 2019 byla upravena a zdokonalena online vzdělávací aktivita Digitální stopa; zábavný interaktivní příběh pro žáky 5. a 6. třídy, který hravou formou představuje aktuální rizikové jevy a učí bezpečnému chování na internetu.

Témata kybernetické bezpečnosti: -

Chytrá škola (https://www.o2chytraskola.cz/***)***

Portál poskytující informace především pedagogům a rodičům. Témata se týkají toho, jak mluvit s dětmi o online bezpečí, kybernetické šikany a kybergoomingu.

Témata kybernetické bezpečnosti: -

Městečko Kybernetov (https://zizalice.cz/produkt/mesteckokybernetov/***)***

Desková hra je určená dětem od 5 do 9 let věku, nenásilnou formou představuje problémy závislosti na komunikačních technologiích, kyberšikany a kybergroomingu a zdraví.

Témata kybernetické bezpečnosti: -

Senzační senioři (https://www.sensen.cz/***)***

Sdružení Senzační senioři (SenSen) uspořádalo ve spolupráci s NÚKIB série sedmi přednášek pro seniory, které byly uspořádány napříč městy v České republice. Celá série byla zakončena konferencí v Praze. Nadace Vodafone odstartovala dlouhodobý projekt na podporu digitálního vzdělávání seniorů. Vedle toho osloví 80 seniorů, kterým daruje přístroj, připojení a kurz digitálního vzdělávání.

Témata kybernetické bezpečnosti: -

Vanda a Eda v Onl@jn světě (https://vzdelavani.nukib.cz/course/view.php?id=12#section-0***)***

Online kurz Vanda a Eda v Onlajn světě seznamuje předškoláky a žáky 1. – 2. tříd s riziky využívání digitálních technologií a internetu. Vanda a Eda si vyzkouší, jak tenká může být

hranice závislosti, že online kamarád nemusí být vždy tím, za koho se vydává, a že je nutné pečovat o svou online identitu a o to, co sdílíme.

• • •

Z uvedeného přehledu je patrné, že existuje řada velmi dobrých a promyšlených projektů a programů, které se zabývají kyberšikanou a kybernetickou bezpečností. Frekventovanějším tématem je kyberšikana.

Projekty a programy týkající se kybernetické bezpečnosti se zaměřují na kybernetické útoky pod zastřešujícím názvem Malware a také na útoky typu Phishing. Útoky Man in the Middle, DoS a DDos, útoky na IoT zařízení a úniky dat se nezabývá nikdo.

Doporučujeme tyto projekty a programy zveřejnit pro velmi dobrou inspiraci těm, kteří do budoucna budou podobné programy vymýšlet. Ti se díky tomu mohou vyhnout vymýšlení již vymyšlených a realizovaných věcí. Zároveň se dostanou ke kontaktům a lépe se tak mohou domluvit na případné spolupráci.

6. Návrhy řešení problematiky *efektivních metod podporující rozvoj jednorázového i dlouhodobého poradenství pro otázky bezpečnosti a podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí včetně vytvoření konkrétní vzdělávací podpory pro cílovou skupinu.*

Popis navrhovaných nástrojů podporující rozvoj jednorázového i dlouhodobého poradenství pro otázky bezpečnosti a podpory příležitostí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí. Popsané nástroje budou uvedeny v příloze.

- Otázky a odpovědi
- Metodika pro organizace
- Metodika pro školy a volnočasové pracovníky
- Metodika pro lektory

7. Závěr, shrnutí

Digitální technologie a digitalizace patří k oblastem, které budou nejvíce ovlivňovat naši budoucnost. Díky výkonnému hardwaru a rychlým sítím stále narůstá nejen objem elektronické komunikace mezi lidmi, ale i elektronických finančních transakcí, obchodních aktivit, záznamů o zdravotní péči nebo úředních procesech. Možností zábavy či vzdělávání je na internetu rovněž celá řada.

Ruku v ruce s těmito pozitivy jsou ovšem spojena i určitá rizika, díky kterým může člověk přijít o své finance, o svá data i o svou pověst. Proto je třeba nezapomínat na ochranu svých zařízení, programů, financí, dat i soukromí.

Mezi nejčastější negativní a rizikové jevy na internetu patří různé druhy kybernetických podvodů a krádeží, vydírání a cílené útoky na počítačové systémy. Dle dostupných prognóz se tyto kybernetické útoky budou do budoucna zvyšovat. Nejvíce ohroženou skupinou budou občané ČR, kteří mají základní znalosti a dovednosti v práci s internetem, nutně je nepotřebují k výkonu svého zaměstnání, ale využívají je ve svém soukromém životě. Dále na lidi, kteří se minimálně nebo vůbec nevěnuje své kybernetické bezpečnosti. Sem patří také děti a mládež.

Na tyto cílové skupiny je třeba cílit poradenskou činnost projektů a programů, které se tímto tématem chtějí v budoucnu cíleně zabývat. Jejich organizátoři najdou v tomto materiálu množství opor, které jim mohou usnadnit jejich práci při jejich poradenské činnost v kybernetické bezpečnosti.

8. Přílohy

A) **Soubor nejčastěji kladených otázek a odpovědí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí**

Příloha A: Otázky a odpovědi

B) **Metodika pro pracovníky organizací (školy, volnočasové instituce, knihovny, galerie, muzea aj.) poskytující poradenství rodičům, prarodičům a dětem v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a online příležitostí**

Příloha B: Kybernetická bezpečnost

C) **Mezigenerační vzdělávací program pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.**

Příloha C: Chyťme hackera

D) **Metodika pro lektory mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.**

Příloha D rozpracovaná do pokynů pro lektory

Příloha Dd Prezentace dle jednotlivých kol

Využité prameny a zdroje

- Strategie digitální gramotnosti ČR na období 2015 až 2020
- Národní úřad pro kybernetickou a informační gramotnost: https://nukib.cz/cs/
- Národní úřad pro kybernetickou a informační gramotnost: Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019
- Kyberkompas. Kyberkompas [online]. [2020]. Dostupné z: https://security.muni.cz/cyber-compass
- PortálDigi: https://portaldigi.cz/
- https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW-09Mw%3D%3D
- https://www.sagit.cz/info/sb-anotace-sb14181a
- https://www.sensen.cz
- https://zizalice.cz/produkt/mesteckokybernetov
- https://www.o2chytraskola.cz
- https://moodle.nic.cz/course/view.php?id=15
- https://www.e-bezpeci.cz
- https://www.kpbi.cz/#
- https://www.jaknainternet.cz
- https://www.bezpecnenanetu.cz
- https://www.nsmcluster.com/doc/_JCE_Koncepce.pdf
- https://www.avast.com/cz/besafeonline
- https://www.internetembezpecne.cz
- https://security.muni.cz/cybercompass
- https://vzdelavani.nukib.cz/course/view.php?id=12#section-0

Otázky a odpovědi

Soubor nejčastěji kladených otázek a odpovědí v otázkách bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí

Obsah

Co je to ten kyberprostor?

Kyberprostor je virtuální počítačový svět, přesněji elektronické médium tvořící světovou, globální počítačovou síť, která je základem online komunikace. Je to rozsáhlá počítačová síť tvořena menšími, po světě rozesetými počítačovými sítěmi, které užívají TCP/IP protokol. Ten jim umožňuje komunikaci a výměnu dat.

Jedna z hlavních vlastností struktury kyberprostoru je otevřenost širokému okruhu uživatelů v interaktivní a virtuálním prostředí. Další vlastností je anonymita, ta umožňuje v podstatě jakékoliv jednání bez zodpovědnosti.

Kyberprostor umožňuje uživatelům komunikovat,sdílet a vyměňovat si informace a nápady, hrát hry, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce, atd…virtuálním počítačovým světem v internetu tvořený daty a informacemi. Lidé zde mohou komunikovat např. pomocí emailu nebo nakupovat v internetových obchodech.

Wikipedie

Jak má rozumět pojmům kybernetická bezpečnost, kybernetická kriminalita a kyberpodvody?

Kybernetická bezpečnost je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné jeho předpokládaným uživatelům. Jedná se o celý kyberprostor.

Počátky se objevily v 80. letech, kdy se s rozmachem výpočetní techniky začaly skladovat informace právě do výpočetních systémů. Jednalo se například o evidence plateb, informace o zákaznících, armádní tajemství.

Kybernetická kriminalita představuje trestnou činnost, která zahrnuje počítač nebo síťové zařízení. Patří zde i zločiny prováděné prostřednictvím internetu, jako podvody, krádež osobních údajů a identity nebo kreditní karty. Velké množství útoků je prováděno za účelem získání peněžních prostředků.

Kyberpodvody/zločiny jsou chápány jako trestná či škodlivá jednání, která spočívají v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku a která jsou uskutečňována prostřednictvím síťových technologií.

Kdo stojí za těmito kybernetickými podvody?

Velká část kybernetických podvodů vyžaduje dobrou znalost fungování sítí a počítačových systémů. Podvodníci se proto nejčastěji rekrutují z řad tzv. hackerů. Typický hacker je velice schopný programátor, který je odborníkem na manipulace nebo úpravy počítačových systémů a sítí. Své počítačové dovednosti využívá k získání neoprávněného přístupu k cizím počítačům a sítím. Zajímá se především o citlivé informace, jako jsou hesla, údaje o platebních kartách nebo soukromé fotografie. Jedná tak pro zábavu, zisk nebo ve snaze způsobit škodu.

Týká se kybernetická kriminalita i České republiky?

V roce 2019 došlo k dalšímu nárůstu počtu kybernetických útoků proti naší zemi, z nichž některé lze označit za velmi vážné. Řada veřejných i soukromých institucí se musela vyrovnávat s obranou před těmito útoky a odstraňováním jejich následků. NÚKIB v průběhu roku řešil 78 kybernetických incidentů. Jeho pracovníci pomáhali napadeným institucím státní správy, územní samosprávy, nemocnicím i firmám s obnovováním jejich systémů, a to jak formou doporučení a metodické pomoci, tak i fyzicky přímo na místech incidentů. Úřad byl této podpory schopen jen díky týmové práci, maximálnímu úsilí a pracovnímu nasazení všech jeho zaměstnanců.

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019

Jsou u nás evidovány nějaké větší kybernetické útoky?

V prosinci 2019 došlo ke kybernetickému útoku proti systémům Nemocnice Rudolfa a Stefanie Benešov, spádové nemocnici až pro 400 000 lidí. Ransomware zašifroval data na serverech, nemocničních přístrojích a pracovních stanicích. V ordinacích nebylo možné provádět standardní ošetření, rušily se plánované operace a hospitalizovaní pacienti museli být převezeni do okolních nemocnic, včetně pacientů na jednotce intenzivní péče. Obnovení plného provozu trvalo téměř měsíc a následky útoku byly vyčísleny na 40–50 milionů korun.

Ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2019

Jaká je prognóza do budoucna?

Každý rok se budou zvyšovat počty kybernetické kriminality (blížíme se k 10 tisícům podvodů ročně).

Proč jsou prováděny kybernetické útoky?

Kybernetické útoky jsou chápány jako trestná či škodlivá jednání, jejichž podstata je v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku či jiné výhody a která jsou uskutečňována prostřednictvím síťových technologií.

Nejčastěji jsou kybernetické útoky prováděny s následujícími cíli:

- Sledování aktivit, které děláte na internetu
- Zcizení, případně i zveřejnění vašich hesel a prolomení bezpečnosti uživatelských účtů
- Zcizení financí z vašeho bankovní účtu
- Podvodné vylákání finančních prostředků
- Zpomalení nebo zablokování počítače nebo serveru
- Znemožnění využití určité internetové služby
- Zcizení idenitity, vydávání se za jinou osobu (např. na sociální síti)
- Agresivní zobrazování reklamy v zařízení
- Zneužití e-mailových účtů

- Zcizení vašich dat a dalších informací o vaší osobě či organizaci
- Rozesílání nevyžádaných informací a/nebo nebezpečných souborů vašim kontaktům
- Zablokování/zašifrování firemních systémů a požadování finančních prostředků za odblokování
- Kybernetická šikana
- Další nelegální aktivity (organizovaný zločin, šíření poplašných zpráv, zneužívání dětí, dětská pornografie)

Jaké existují kybernetické hrozby?

Kybernetické hrozby můžeme podle způsobů, jakými nás mohou ohrozit, zařadit do následujících hlavních skupin:

- Malware (velká skupina různých typů škodlivého software)
- Sociální inženýrství
- Kyberšikana
- Útoky na infrastrukturu
- Úniky dat
- Poškození zařízení

Co se může stát obyčejnému člověku, který vlastní nějaké normální digitální zařízení a přístup na internet?

Většina kybernetických útoků se týká i běžných uživatelů. Příkladem může být malware, což je zastřešující výraz pro jakýkoli typ škodlivého softwaru, jehož cílem je poškodit nebo zneužít libovolné programovatelné zařízení, službu nebo síť.

Takový škodlivý software se snaží infikovat počítač nebo mobilní zařízení. Hackeři malware používají z mnoha různých důvodů, například k získávání osobních údajů či hesel, krádežím peněz nebo k blokování přístupu do zařízení. Před malwarem se můžete chránit pomocí antimalwarového softwaru.

Většinou je šířen za účelem poskytnutí možnosti útočníkovi vzdáleně ovládat nakažené zařízení, snížit výkon systému, nakazit síť nebo v některých scénářích zablokovat přístup k datům.

Do kategorie malware řadíme především tyto skupiny škodlivého software: počítačové viry, počítačové červy, trojské koně, crimeware, špehovací software (spyware), vyděračský software (ransomware) a reklamní software (adware).

Jak se takový škodlivý software může dostat do mého počítače?

Je řada možností. Obvykle objevuje jako příloha v e-mailu, který obsahuje datovou část viru, který provádí škodlivou akci. Jakmile oběť otevře soubor, zařízení je infikováno. Škodlivým software mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento škodlivý software.

Jak zjistím, že mám nakažený počítač nebo mobil?

Škodlivý software může například extrémně zpomalit počítač vám na agresivně vyskakují reklamy, kterých se nemůžete zbavit. To je ten lepší případ. Ten horším případ se projevuje smazáním dat na disku či způsobit vyhoření hardware.

Co mám udělat, abych zamezil problémům v souvislosti s bezpečností na internetu?

Dbáme na ochranu našeho soukromí a dat a uvědomujeme si rizika kyberprostoru. Věnujeme pozornost bezpečnostním opatřením a spolehlivosti. Citlivější data chráníme dostatečně silným heslem (neodvozujeme jej od osobních údajů, pro různé přístupy volíme různá hesla) nebo jinými metodami (otisk prstu, PIN, zašifrování samotného obsahu). Své přístupové údaje nikomu nesdělujeme. Svá digitální zařízení chráníme ověřeným antivirovým programem. Uvědomuje si, že ostatní uživatelé nemusí sdílet svoji pravou totožnost (vydávání se za jiné pohlaví, nepravdivý věk apod.), a tudíž sami nesdělujeme svoje důvěrné údaje neznámým osobám nebo uživatelům na sociálních sítích. Data, o která nechceme přijít, si pravidelně zálohujeme.

Řekněte ještě několik příkladů kybernetických útoků?

- Útočník zaregistroval doménu instituce státní instituce, která připomínala doménu dotčené instituce. Pod touto doménou rozesílal podvodné emailové zprávy, ve kterých nabádal ke vstupu na podvodné stránky prostřednictvím vloženého odkaz
- Vystrašení uživatele internetu, kterému přijde e-mail, kde odesílatel je on sám. V e-mailu má výhružku, že jeho počítač je napaden a nepošle-li do 24 hodin peníze, tak budou rozeslány na všechny jeho kontakty choulostivé fotografie a videa

Kybernetická bezpečnost

Materiál přináší přehled běžných kybernetických útoků a dalších hrozeb, s nimiž se může setkat každý uživatel digitálních technologií. Účelem není podání vyčerpávajícího encyklopedického seznamu všech existujících nebezpečí, ale spíše představení obecných principů těchto hrozeb a možností obrany před nimi. Jsou zahrnuta nejčastější rizika, s nimiž se setkává při běžné činnosti většina laických uživatelů digitálních technologií. Pro lepší ilustraci jsou hlavní schémata kybernetických útoků doplněna o příběhy založené na reálných skutečnostech a případech.

Obsah

1. Úvod

Digitální technologie a digitalizace patří k oblastem, které budou nejvíce ovlivňovat naší budoucnost. Je jen malé procento lidí, které se s digitálními technologiemi aktivně nesetkalo. Využívání digitálních technologií se bude neustále zvyšovat, především díky tzv. kyberprostoru, což je zejména prostředí internetu. Zde stále narůstá objem komunikace mezi lidmi, finančních transakcí, obchodních aktivit, údajů o zdravotní péči, úředních procesů a záznamů, ale i zábavních možností a dalších dat v mnoha oblastech lidské činnosti..

Tyto činnosti budou i nadále růst, a proto je potřeba digitální dovednosti vnímat jako jednu ze základních složek funkční gramotnosti člověka. Digitálně gramotný člověk disponuje souborem dovedností univerzálně použitelných v digitálním světě. Takové dovednosti jsou označovány jako digitální kompetence.

Ten, kdo bude mít tyto digitální kompetence a bude jich využívat bude mít větší šanci na lepší uplatnění v zaměstnání i mimo něj. Zároveň také platí, že vhodným užíváním digitálních technologií může ušetřit spoustu svého času. Člověk, který bude digitálně gramotný, zvyšuje svoji konkurenceschopnost. Zároveň tím zvyšuje konkurenceschopnost jeho firma, ve které pracuje a následně zvyšuje konkurenceschopnost i celá společnost.

Internet hraje a bude hrát nezastupitelnou roli v našem každodenním životě. Na internetu a někdy i ve svých zařízeních máme velké množství dat, včetně personálních, prostřednictvím internetu provádíme většinu finančních transakcí, sdílíme zde svoje názory, umisťujeme sem naše fotky a videa, komunikujeme s dalšími…

Ruku v ruce s tímto pozitivem jsou ovšem spojeny i určitá rizika, díky kterým může přijít o své finance, o svá data i o svou pověst. Zde je třeba mít na paměti, že je třeba se věnovat ochraně svých zařízení, programů, financí, dat i soukromí.

Dbáme na ochranu našeho soukromí a dat a uvědomujeme si rizika kyberprostoru. Věnujeme pozornost bezpečnostním opatřením a spolehlivosti. Citlivější data chráníme dostatečně silným heslem (neodvozujeme jej od osobních údajů, pro různé přístupy volíme různá hesla) nebo jinými metodami (otisk prstu, PIN, zašifrování samotného obsahu). Své přístupové údaje nikomu nesdělujeme. Uvědomuje si, že ostatní uživatelé nemusí sdílet svoji pravou totožnost (vydávání se za jiné pohlaví, nepravdivý věk apod.), a tudíž sami nesdělujeme svoje důvěrné údaje neznámým osobám nebo uživatelům na sociálních sítích. Data, o která nechceme přijít, si pravidelně zálohujeme.

2. Kybernetické hrozby

Kromě mnoha přínosů a výhod je internet a celý kyberprostor zároveň ideálním prostředím pro zločince, podvodníky či jinou nebezpečnou činnost. Ta je v prostředí internetu díky podceňování online nebezpečí a rizik ze strany velké části lidí vykonávána s vidinou velkého zisku a malého rizika. Jsou však i nebezpečné činnosti, u kterých hlavním motivem útočníka není hmotný či jiný zisk, ale "pouze" zábava nebo prokázání vlastních schopností.

Kybernetické útoky jsou chápány jako trestná či škodlivá jednání, jejichž podstata je v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku či jiné výhody a která jsou uskutečňována prostřednictvím síťových technologií.

Nejčastěji jsou kybernetické útoky prováděny s následujícími cíli:

- Sledování aktivit, které děláte na internetu
- Zcizení, případně i zveřejnění vašich hesel a prolomení bezpečnosti uživatelských účtů
- Zcizení financí z vašeho bankovního účtu
- Podvodné vylákání zboží či finančních prostředků
- Zpomalení nebo zablokování počítače nebo serveru
- Znemožnění využití určité internetové služby
- Zcizení idenitity, vydávání se za jinou osobu (např. na sociální síti)
- Agresivní zobrazování reklamy v zařízení
- Zneužití e-mailových účtů
- Zcizení vašich dat a dalších informací o vaší osobě či organizaci
- Rozesílání nevyžádaných informací a/nebo nebezpečných souborů vašim kontaktům
- Zablokování/zašifrování firemních systémů a požadování finančních prostředků za odblokování
- Zničení nebo smazání datového nosiče, případně poškození dalších částí hardware
- Kybernetická šikana
- Další nelegální aktivity (organizovaný zločin, šíření poplašných zpráv, zneužívání dětí, dětská pornografie)

2.1 Typy kybernetických hrozeb

Uvedených cílů kybernetických útoků útočníci dosahují celou řadou různých technik a nástrojů. Pokud bychom je měli nějak kategorizovat, lze vytvořit následující skupiny:

- Malware (velká skupina různých typů škodlivého software)
- Sociální inženýrství
- Kyberšikana
- Útoky na infrastrukturu
- Úniky dat
- Poškození zařízení

2.2 Malware

Malware je zastřešující výraz pro jakýkoli typ škodlivého softwaru, jehož cílem je poškodit nebo zneužít libovolné programovatelné zařízení, službu nebo síť.

Takový škodlivý software se snaží infikovat počítač nebo mobilní zařízení. Hackeři malware používají z mnoha různých důvodů, například k získávání osobních údajů či hesel, krádežím peněz nebo k blokování přístupu do zařízení. Před malwarem se můžete chránit pomocí antimalwarového softwaru.

Většinou je šířen za účelem poskytnutí možnosti útočníkovi vzdáleně ovládat nakažené zařízení, snížit výkon systému, nakazit síť nebo v některých scénářích zablokovat přístup k datům.

Do kategorie malware řadíme především tyto skupiny škodlivého software: počítačové viry, počítačové červy, trojské koně, crimeware, špehovací software (spyware), vyděračský software (ransomware) a reklamní software (adware).

2.2.1. Počítačové viry

Viry jsou škodlivé kódy šířené jejich tvůrci s různými cíly. Existuje velká řada virů, účelem některých z nich je ničit, jiné naopak mají za úkol usadit se v co největším počtu počítačových systémů a tyto pak využijí k cílenému útoku. Typické pro tyto programy je schopnost šířit se mezi systémy bez nutnosti zásahu uživatele počítačového systému, jsou schopny se sami automaticky replikovat na přenosná média, připojené síťové jednotky namapované k infikovanému systému. Různé viry se mohou projevovat různě, např. od náhodného přehrávání určité melodie, přes zahlcení systému, úpravu nebo zničení dat, až po celkovou destrukci napadeného systému. Odhaduje se, že každý zhruba 300. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.

Jak se počítačový virus projevuje?

Klasický počítačový virus vyžaduje svého hostitele. Tzn. program nebo jiný spustitelný soubor, jehož spuštěním se zároveň spustí i programový kód viru. Virus se obvykle objevuje jako příloha v e-mailu, který obsahuje datovou část viru, který provádí škodlivou akci. Jakmile oběť otevře soubor, zařízení je infikováno.

Virus obsažený v souborech či programech při spuštění nebo samovolně po nějaké době začne páchat škodu. Může například extrémně zpomalit počítač, nebo v horším případě smazat data na disku či způsobit vyhoření hardware. Virem mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento virus.

Jak se ochránit před počítačovými viry?

Neměli byste pouze vědět to, že existují počítačové viry. Neméně důležité je také pochopit, proč dochází k útokům a jak se před viry bránit.

- Neměli byste navštěvovat podezřelé stránky, spouštět podezřelé aplikace a otevírat soubory, u kterých není znám původ.
- Každý počítač by měl být vybaven antivirovou ochranou (např. Avast Free Mobile Security).
- Vyhněte se stahování programů z neznámých či nelegálních (warez) zdrojů.
- Do svého zařízení nevkládejte paměťová média (např. USB externí disky) z neznámých

zdrojů.

- Neotevírejte přílohy nevyžádaných emailu nebo zprávy od neznámých kontaktů na Facebooku.
- Stahujte aplikace pouze z oficiálních obchodů. Např. aplikace pro Android v Google Play, pro Iphone v App Store, atp.
- Pravidelně provádějte ve vašem antivirovém programu kompletní kontrolu systému. Pokud se na vašem počítači objeví viry, odstraňte je.

Virů je celá řada, zde přinášíme výběr nejznámějších z nich:

2.2.2. Počítačový červ

Červ je samostatný program, který je schopen šířit sám sebe nebo své části do jiných počítačových systémů. Červi mají schopnost kopírovat se mezi počítači, obvykle pomocí zneužití nějakého druhu slabého místa zabezpečení v softwaru nebo operačním systému, a k fungování nepotřebují interakci uživatele. Počítačoví červi jsou zákeřné druhy virů, které se snaží nakazit co největší množství počítačů. Také mohou výrazně zpomalit váš počítač nebo způsobit jiné škody.

2.2.3. Trojský kůň

Trojský kůň je obvykle skrytá část programu, která vykonává činnost, se kterou by uživatel při znalosti této činnosti pravděpodobně nesouhlasil. Obvykle se totiž jedná o činnost škodlivou. Trojské koně se maskují jako neškodné aplikace, které uživatele lákají k tomu, aby si je stáhli a používali. Jakmile jsou spuštěny, mohou ukrást osobní údaje, způsobit chybu v zařízení, sledovat aktivity, odesílat spam a dokonce spustit útok.

Nejčastějším zdrojem těchto škodlivých programů bývají pochybné a neověřené zdroje různých softwarových nástrojů

2.2.4. Backdoor

Jedná se o jednu z vlastností malware typu Trojský kůň. Je to metoda, která útočníkovi umožňuje přístup k systému díky obcházení standardní autentizace, které je při běžné kontrole nezjistitelné. V podstatě zevnitř systému otevře útočníkovi “zadní vrátka”. Stejně jako trojan se nejčastěji šíří jako součást jiné aplikace, která je na první pohled nezávadná a užitečná. Díky tomu si ji uživatel instaluje do systému a autorizuje pro ni přístup k systémovým funkcím. Například v telefonu může program přistupovat k úložišti, SMS zprávám, poloze zařízení, atd. Ke stejným zdrojům pak pochopitelné má přístup i škodlivý kód.

Backdoor bývá často v softwaru zanechán úmyslně programátorem, případně to může být nějaký nástroj ladění programu, který byl omylem zanechán ve finální verzi.

2.2.5. Ransomware

Reálný příběh nemocnice v Benešově 2019

Je středa, 11. prosince 2019, dvě hodiny po půlnoci. Klid během nočního provozu Nemocnice Rudolfa a Stefanie v Benešově jen občas přeruší akutní příjem. Během zadávání dat na chirurgické ambulanci bylo zaregistrováno výrazné zpomalení počítačů, které se během

krátké doby staly zcela nefunkčními. Do rána se problém rozšířil do celé nemocniční sítě, která tak byla zcela vyřazena z provozu. Ihned po zjištění rozsahu a podstaty problému zasedá v nemocnici krizový štáb, protože je ohrožena péče o pacienty.

Do nemocniční sítě se podařilo proniknout hackerům, kteří dobře promyšleným postupem nejprve převzali kontrolu nad administrátorskými účty správců počítačové sítě, aby následně instalovali zákeřný ransomware na všechny dostupné počítače a datová úložiště. Vyděračský software začal intenzivně šifrovat všechna data. Tím se však prozradil, neboť došlo k výraznému zpomalení sítě. K šifrování je totiž potřebný obrovský výpočetní výkon. Přestože IT oddělení nemocnice ihned po zjištění problému všechny počítače odpojilo, program napáchal takové škody, že nemocnice musela řadu hodin improvizovat úplně bez svých dat. Úplné obnovení služeb trvalo několik týdnů, škody byly vyčísleny na částku kolem 60 milionů korun i přesto, že nemocnice žádné výkupné nezaplatila a obnovila postupně data a funkčnost systémů ze svých zdrojů.

Ransomware použitý k hlavnímu útoku byl identifikován jako virus typu Ryuk, který pochází z Ruska. Nebyl to ale jediný škodlivý kód použitý při tomto útoku. K zahájení stačilo otevřít podvodně zaslanou přílohu emailu, která vypadala jako faktura. Otevřením souboru došlo ke spuštění "průzkumné" části útoku zajišťované malwarem Emotet, který si už sám stáhl z internetu "posilu" v podobě viru (zde to byl virus Trickbot), který mapuje hesla uživatelů. A jakmile se viru podařilo zjistit hesla administrátorů, cesta k instalaci šifrovacího a vyděračského malware byla zcela volná…

Dopadnout pachatele podobného útoku je velmi složité, útočníci se umí velmi dobře v síti maskovat. V tomto případě však byly policejní složky úspěšné, po zhruba rok trvajícím vyšetřování a sledování byla v lednu 2021 při koordinovaném zásahu policejních složek osmi států, Europolu a Eurojustu zadržena tato hackerská skupina na Ukrajině.

Co je ransomware?

Ransomware je jedním z nejziskovějších, a tedy jedním z nejoblíbenějších typů malwaru mezi kyberzločinci. Tento speciálně upravený počítačový virus se nainstaluje do počítače oběti, zašifruje v něm soubory a poté se zaměří na oběť a požaduje výkupné (obvykle v bitcoinech), za které tato data vrátí uživateli.

Podle této činnosti se podobné vyděračské viry označují právě jako ransomware (z anglického „ransom" – výkupné) Zaplacením výkupného je podmíněno dešifrování původně zašifrovaných dat a možnost opětovného přístupu k nim. Oběť se nejčastěji infikuje tímto škodlivým softwarem při návštěvě ohrožených webových stránek nebo při stažení souboru, jehož součástí je právě ransomware.

Velmi často se ale stane, že se data neodblokují ani po zaplacení výkupného a dojde tak k dalším škodám (ztráta dat i peněz). Dobrou prevencí je být pozorný zejména v případě otevírání neohlášených příloh k emailům a mít kvalitní antivirus, který tyto hrozby dokáže zachytit. Je-li systém nakažen, nabízí se dvě základní možnosti opravy: buď operační systém přeinstalovat a přijít tak o naše data, nebo se pokusit data dešifrovat. To je však velmi složitý a ne vždy stoprocentně řešitelný úkol. Záleží i na použitém typu ransomware.

V případě dalšího konkrétního útoku se například po infiltraci počítače malwarem tento počítač následně stal součástí botnetu, přes který byl šířen tento vyděračský virus dále. Malware následně zablokoval přístup k účtu uživatele operačního systému, v tomto případě Windows a zobrazil upozornění, že počítač byl zablokován policií daného státu.

Další příklad ransomware - WannaCry

V květnu 2017 se mnoho počítačů stalo terčem útoků ransomwarem zvaným WannaCryptor 2.0. Jde o zablokování dat, jejichž odblokování stojí peníze. K tomuto útoku došlo začátkem května 2017 a byly napadeny počítače po celém světě (až 99 zemí), V té době bylo hlavní obětí Rusko, kdy bylo napadeno až 57 % z více než 100 000 celkových útoků, včetně ruské telekomunikační firmy Megafon. Toto číslo se nakonec vyšplhalo nad 230 000. Byla také napadena zdravotní služba National Health Service ve Velké Británii, nebo telekomunikační středisko ve Španělsku zvané Telefonica. Za obnovu dat tento ransomware po firmách požadoval bitcoiny v hodnotě 300 dolarů. Ransomware změní příponu zablokovaných souborů na .WNCRY a odblokování lze uskutečnit po zaplacení částky, jinak budou soubory smazány.

Jak předcházet ztrátám dat a bránit se vydírání?

- Pravidelně zálohuji data, nejlépe alespoň na dvou odlišných místech
- Používám ochranu proti virům a škodlivému software
- Přístroje, které obsahují data, nenechávám bez dozoru a ukládám je na bezpečných místech
- Používám bezpečná hesla pro přístup k datům
- Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon)
- Instaluji pouze software z ověřených zdrojů
- Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy

2.2.6. Spyware

Spyware je program nainstalovaný ve vašem počítači nebo telefonu, obvykle bez vašeho výslovného vědomí, který zachycuje a přenáší osobní údaje nebo návyky a podrobnosti při procházení internetu jeho uživateli. Spyware umožňuje jeho uživatelům sledovat všechny formy komunikace v cíleném zařízení. Spyware je často používán organizacemi dohlížejícími na dodržování zákonů, vládními agenturami a organizacemi zabývajícími se zabezpečením informací k testování a sledování komunikace v citlivém prostředí nebo při vyšetřování. Spyware je však také k dispozici spotřebitelům, kdy osobám, které si jej pořídily, umožňuje sledovat jejich manželku, děti a zaměstnance.

Spyware je naprogramován tak, aby dokázal potají sledovat aktivitu uživatele počítače, shromažďovat tyto informace a případně je přeposílat třetím stranám. Jedná se o osobní údaje nebo historii prohlížení. Pokud nejde o záměrnou instalaci jiným uživatelem, počítač může být nechtěně nakažen spywarem i po nainstalování aplikace nebo po otevření přílohy e-mailu, hudby, filmu atd. Může se projevovat např. i přesměrováním vyhledávacích dotazů nebo vznikem neznámých ikon v hlavním panelu, na ploše či v liště prohlížeče. Odstranění se provádí antivirovým programem, nebo programem zaměřeným na odstraňování spyware. Možností je také odinstalovat podezřelé programy. Prohlížeč a antivirus je potřeba udržovat aktuální. Není dobré spouštět podezřelé aplikace, otevírat e-mailové přílohy a klikat na

Spyware je oblíbeným nástrojem hackerů, kteří jej používají ke špehování uživatelů, pro získání přístupu k vašim osobním datům, bankovním údajům nebo historii vašich online aktivit. Možné a relativně snadné je pro hackera i sledování vašeho pohybu díky GPS datům z vašeho mobilního telefonu.

Není však neobvyklé ani použití tohoto typu programu v běžně fungujících firmách či organizacích. IT oddělení dostává za úkol sledovat činnost zaměstnanců organizace např. s pomocí sledovacího softwaru instalovaného do počítače zaměstnance nebo kontrolou emailových schránek apod. Zcela běžnou činností je pak sledování polohy flotily firemních vozidel (a tudíž i řidičů) za pomoci GPS a datového přenosu. Uvedenou činností, je-li realizována bez souhlasu uživatele, však často dochází k zásahu do základních lidských práv a svobod a je zcela lhostejné, zda instalaci sledovacího software provádí externí útočník či firemní administrátor sítě.

2.2.7. Keylogger

Příběh - Jak si (ne)objednat vagón s pizzou

Jitka si občas ráda s kamarádkami přeposílá zajímavé tipy na úpravu zahrady či domu. Obrázky s krásnými dekoracemi interiéru, odkazy na krásné designové úpravy nábytku či nádob na květiny nebo videa s návody na různá domácí vylepšení. Nápady si vzájemně posílají mailem v podobě fotografií, videí či různých prezentací nebo je sdílejí přes sociální sítě. Občas při otevírání takové přílohy Jitce vyskočí na displeji chybová hláška, že soubor nejde otevřít či zobrazit, případně že je z neověřeného zdroje a mohl by být nebezpečný. Vzhledem k tomu, že zprávy přicházejí od kamarádek, Jitka je považuje za dostatečně důvěryhodné a neměla ze zpráv na obrazovce žádné obavy.

Poslední listopadovou sobotu se s manželem a dětmi rozhodli udělat doma pořádný úklid a protože to vzali opravdu zgruntu, nebyl čas na nějaké vaření. Jídlo si tedy objednali přes oblíbený rozvážkový server, do hodiny bylo doma a nikdo se nemusel v kuchyni zdržovat vařením a mytím nádobí. Večer byl celý dům krásně čistý a voňavý a celá rodina se společně spokojeně usadila na gauč ke sledování filmu.

V pondělí ráno při běžné kontrole zpráv v telefonu objevila Jitka i aktuální výpis z banky. Protože stav konta kontroluje docela často, udivilo ji, že na účtu je zhruba o dvanáct tisíc korun méně než by čekala. Při bližší kontrole zjistila, že během víkendu byly z účtu odečteny dvě sumy: 955 korun byla důvěrně známá částka útraty za dovoz sobotního oběda, ale co těch jedenáct tisíc? K Jitčinu velkému překvapení byla suma stržena stejným obchodníkem - za dovoz jídla! „Jak je to možné? Vždyť jsem přece objednávala jen čtyři porce a dezert k obědu?“

Pochopitelně nelenila a ihned se přihlásila ke svému účtu, aby zkontrolovala sobotní objednávku. Ta byla naprosto v pořádku, avšak v seznamu byla nad ní ještě jedna: byla datována do nedělního večera a podle údajů si Jitka objednala pizzu, sushi a nápoje pro třicet lidí za 11.230 korun! Objednávka byla uhrazena z její kreditní karty, jejíž číslo měla Jitka uloženo v systému rozvážkové služby. Pochopitelně se ihned spojila s kontaktní linkou obchodníka, aby nerealizovaný nákup reklamovala, ale operátorka jí sdělila, že platba byla řádně autorizována správným kódem, který patří k Jitčině kartě.

Na doporučení operátorky si okamžitě nechala zkontrolovat svůj počítač na škodlivý software a byla nepříjemně překvapena: pravděpodobně již několik týdnů má ve svém notebooku tajně instalovaný program, tzv. keylogger, který zaznamenává, co Jitka píše na klávesnici, a všechny “odposlechnuté” texty posílá na určenou adresu přes internet. Útočník ze získaných dat zjistil vstupní údaje do systému a viděl, že tam má uložené čislo své karty. Stačilo mu už jen stejným skrytým programem odposlechnout autorizační kód a mohl si na Jitčin účet nakoupit jídlo i pití na pořádnou party. Jídlo si rafinovaně nechal poslat na parkoviště v sídlišti, takže nebyla známá ani žádná adresa, kde by se mohl vyskytovat...

Keylogger je druh spyware, který (většinou tajně) zaznamenává stisky kláves. Útočník může díky keyloggeru zjistit uživatelská hesla, názvy účtu, čísla bankovních účtů, jaké stránky jsou navštěvovány nebo jakýkoliv text, který byl napsán v e-mailech nebo v jiné textové formě. Keylogger se v počítači může vyskytnout, otevřeme-li e-mailovou přílohu, klikneme na phishingový odkaz nebo jím může být nakažený nějaký software. Nakažený počítač se může chovat zpomaleně, myš se zasekává a klávesy fungují opožděně. Použití správného antiviru by mělo problém vyřešit. Jako prevenci neoprávněného užití hesel je vhodné používat dvoufázové přihlašování, kdy přihlášení k systému jedním kanálem (např. přes internetový prohlížeč) je potřeba ještě potvrdit jiným kanálem (např. zadáním kódu, který je odeslán na číslo mobilního telefonu).

Keyloggery se velmi často pojí s další kybernetickou hrozbou, kterou je krádež vašeho uživatelského účtu.

2.2.8. Rootkit

Snaží se o získání administrátorských práv k systému. Rootkity mohou přijít se staženými bezpečnostními, programy, které na první pohled vypadají neškodně. Mohou se ale také objevit formou dodatečného rozšíření programů. Rootkit se dá zjistit antivirem, který musí při provádění systémové kontroly navíc sledovat funkce DLL knihoven. Rootkit se po nalezení musí odstranit ručně.

2.2.9. Botnety

Populárním způsobem pro šíření škodlivého software a spamu je využívání e-mailů. Útočníci jako přílohy zpráv posílají soubory, které obsahují viry a jiný škodlivý software. K masovému rozesílání infikované pošty se dobře hodí tzv. botnety. Jde o síť útočníkem ovládnutých počítačů, které mají za úkol automaticky rozesílat škodlivý software na různé e-mailové adresy současně. Botnety jsou většinou ovládány z jednoho centrálního počítače. Nakaženým zařízením, která jsou takto využívána, se také říká zombie. Mezi známé botnety patří například Necurs a Satori.

Kromě rozesílání spamu a šíření malware mohou útočníci váš počítač zapojený do botnetu použít i jako přímý nástroj výdělku. Známým příkladem je zneužití cizích počítačů k těžbě kryptoměny Bitcoin. V tomto případě se každý útočníkem ovládnutý počítač částí svého výpočetního výkonu podílel na složitých výpočtech vedoucích k získání kryptoměny.

Botnety jsou obecně založeny na využívání velkého množství softwarových robotů (tzv. „bots“). Tyto boty pracují v samostatném režimu mimo IT kontrolu napadeného prostředí. Nad tímto cíleně infikovaným počítačem do určité míry převzala neoprávněně kontrolu třetí osoba, a to bez vědomí oprávněných uživatelů. Takto infikované systémy slouží nejčastěji jako základna pro anonymní připojování útočníka k internetu, k zasílání škodlivých programů, uskutečňování útoků na další cíle, realizace DDosS útoků, k šíření spamu, krádežím identit či jiným kybernetickým útokům. Jakákoliv manipulace s těmito infikovanými počítači nebo počítačovými systémy nebo využívání takovýchto počítačů, či počítačových systémů bez souhlasu oprávněné osoby je porušením čl. 11 LZPS („Každý má právo vlastnit majetek. Vlastnické právo všech vlastníků má stejný zákonný obsah a ochranu.“), a to nehledě na to, v jaké podobě bude s těmito počítači či systémy manipulováno

Botnet Necurs

Jedná se o rozsáhlý botnet, který je určen pro šíření malware přes e-mailové přílohy. Během jeho existence bylo zaznamenáno nespočet incidentů tohoto botnetu. Nejnovější incident

UTB ve Zlíně, Fakulta aplikované informatiky, však nastal koncem března roku 2018. Během jediného dne rozeslal kolem sto tisíc e-mailů, které se chovaly jako objednávky s přílohou. Uživatelé tak otevřeli tuto přílohu a byli nakaženi trojským koněm zvaným Quant Loader, který je schopen do počítače vložit ransomware a vymáhat peníze, nebo ukrást citlivá hesla.

Botnet Satori

Nejnovější verze tohoto botnetu se od ostatních botnetů liší tím, že jeho hlavním cílem jsou zařízení, na kterých se těží kryptoměna zvaná Ethereum. Satori napadne tato zařízení a přepíše cílovou adresu, na kterou je vytěžená částka poslána. Útočí na zařízení, na kterém je nainstalován program pro těžbu, zvaný Claymore.

2.2.10. Spam

Spam je nevyžádané sdělení šířené internetem v podobě e-mailu, zprávy na sociální síti, článku na určitém webovém serveru. Nevyžádané zprávy obtěžují uživatele a zahlcují informační prostor. Za škodlivé považujeme zejména programy pro rozesílání nevyžádaných zpráv, avšak hrozba může přijít i uvnitř samotné zprávy v podobě přílohy infikované některým druhem malware, případně může být zpráva prostředkem phishingového útoku, atp.

Příběh - spam

Karel je fanouškem historických vozidel. Pravidelně jezdí na historické srazy a doma má pěknou sbírku starých motoristických suvenýrů. Poslední dva roky hodně šetřil, aby si mohl pořídit pěkného veterána i domů. Zaregistroval se na fanouškovských fórech, sleduje internetové bazary a skupiny a úplně nejraději sleduje videa o opravách starých vozů.

Z oblíbeného diskuzního serveru přišla Karlovi jednoho dne zpráva, že došlo k napadení jejich databázového serveru a pravděpodobně k úniku dat. Zástupce serveru se uživatelům omlouval a doporučil neprodlenou změnu přístupových údajů ke službě. Karel to podle doporučení serveru provedl a fórum mohl bez problému používat dál. Během několika dnů však do jeho emailové schránky začalo přicházet velké množství reklam na zboží, o které se nikdy nezajímal.

Spamboty

Nevyžádané zprávy jsou většinou rozesílány či publikovány automaticky specializovanými programy, tzv. spamboty. Spambot umí i automaticky vyplnit přihlašovací nebo registrační formuláře, aby bylo možné distribuovat spam jménem určitého uživatelského účtu. Často jsou k rozesílání spamu zneužívány počítače nebo uživatelské účty napadené hackery. Pokud se vám něco takového stane, obvykle spam začne chodit vašim kontaktům přímo z vašeho účtu.

Emailové adresy, na které je spam odesílán, jsou uloženy ve velkých databázích spammerů. Do nich se dostávají různým způsobem. Nejčastěji to je za pomoci automatického sběru emailových adres z webových stránek, adresy spammerům však často poskytují sami uživatelé, když vymění svoji adresu za přístup k nějakému benefitu (ebook či video zdarma, atd.). Výjimečné nejsou ani záměrné krádeže databází adres hackery, protože funkční adresy potenciálních zákazníků jsou pro mnoho obchodníků velmi cenné a ukradené adresy se tak dají dobře zpeněžit.

Jak zatočit se spamem?

- Při registraci do nové služby pozorně čtu podmínky zpracování a použití mých dat.

Není-li to nezbytné, nepovoluji použití pro marketingové účely

- Klikání na neznámé odkazy v příchozí poště často způsobí, že se moje adresa dostane do dalších seznamů pro posílání spamu
- Ve vašem mailboxu spam důsledně označuji
- Pro účely jednorázových a méně důležitých registrací mám zvláštní emailovou adresu. Odlehčím tím své hlavní schránce
- Je-li v nevyžádané poště možnost odhlášení (zrušení zasílání), využiji ho.
- Pokud spamovým filtrem prochází určitý druh nevyžádaných zpráv, přidám jejich odesílatele na blacklist filtru
- Pokud běžné a očekávané zprávy končí ve spamovém koši, upravuji whitelist spamového filtru

2.2.11. Adware

Programy adwaru nabízí uživatelům nechtěné reklamy, a když provedete nějakou akci, obvykle zobrazí blikající reklamy nebo automaticky otevíraná okna. Programy adwaru jsou často nainstalovány výměnou za jinou službu, například za oprávnění používat program nebo nějaký doplněk, aniž byste za něj museli platit.

Tyto bezplatné programy se snaží vydělat peníze zobrazováním reklam. Reklamy jsou z velké části otravné a neškodné, ale počítač mohou i zpomalovat. Existuje i adware, který může být nebezpečný, neboť může sledovat historii prohlížení nebo osobní informace. Jestli je napaden náš systém adwarem poznáme tak, že se nám samovolně spouští nová okna s reklamními bannery, případně se domovská stránka prohlížeče bez našeho vědomí přesměruje na nějakou stránku, kde můžeme utrácet peníze. Před adwarem se dá bránit tak, že udržujeme aktualizovaný veškerý software (operační systém, prohlížeče, antivirové programy atd.). Existuje však i specializovaný anti-adware software.

Vyskakovací okna s inzercí obtěžují každého uživatele, nejsou však sama o sobě nebezpečná. Nebezpečné však mohou být internetové stránky, na které vedou odkazy z takové inzerce. Velmi často jsou zdrojem dalšího škodlivého software.

2.2.12. Neautorizované změny prohlížečů

Příběh - nebezpečné doplňky v prohlížeči

Jirka se učí na kytaru a rozhodl se nacvičit oblíbenou píseň z videoklipu světoznámé rockové skupiny. Aby mohl během víkendu trénovat i na chatě, kde není možnost připojení k internetu, hledal způsob, jak nahrávku dostat z Youtube videa do svého telefonu. Na internetovém fóru dostal tip na doplněk do internetového prohlížeče, který umí video se zvukem stáhnout do offline podoby. Jakmile bylo video uložené v počítači, zkopírování do telefonu už byla otázka chvilky.

Když se v neděli večer vrátil domů, spustil počítač, protože potřeboval objednat na eshopu nové struny. Při otevření prohlížeče očekával úvodní stránku svého oblíbeného vyhledávače, místo toho se však objevila neznámá stránka plná reklam na podivné webové stránky. Po každém zadání internetové adresy navíc přes hlavní okno prohlížeče vyskakovala stále další a další okénka s reklamou a nabídkami výhodných nákupů.

Jiří si za pomoci kamaráda a internetových zdrojů nakonec s problémem poradil. Rozšíření prohlížeče, které podivné chování programu způsobilo, snadno odstranil, avšak pátrání po příčinách a opětovné nastavení prohlížeče stálo Jirku pěkných pár hodin času.

Nebezpečí v prohlížeči

Jak již název kapitoly napovídá, některá rozšíření prohlížeče nebo speciálně upravené webové skripty mohou provádět neautorizované změny v prohlížeči bez vědomí uživatele. Prográmek změní důležitá nastavení webového prohlížeče a tím způsobí, že se váš počítač nebude chovat podle vašich představ. Mnohdy vás rovnou navádí na weby se závadným nebo nebezpečným obsahem (viry, pornografie…) Tyto typy útoků řadíme rovněž do skupiny adware, avšak cílem útočníka a prostředkem nevyžádané reklamy jsou výhradně internetové prohlížeče.

Obrana proti tomu je relativně snadná, uživatel by však měl být pozorný a opatrný. Určitě není příliš bezpečné stahovat neověřené doplňky do prohlížečů nebo ignorovat varovná hlášení prohlížeče či antiviru o potenciálním nebezpečí navštívené stránky. Samotná změna nastavení prohlížeče záškodníkem tolik nebezpečná není, avšak weby na podstrčených odkazech mohou skrývat nebezpečí mnohem větší. Vždy je proto dobrým pomocníkem i kvalitní ochrana počítače před škodlivým softwarem v podobě antivirového programu.

2.2.13. Ochrana proti malwaru

Hrozeb v podobě škodlivého software je tedy celá řada. Standardní ochranu proti malware představuje antivirový software, který slouží k vyhledávání a identifikaci škodlivých kódů a následně jejich smazání nebo zabránění napadení systému. Antivirový program je potřeba udržovat v nejaktuálnější verzi, aby dokázal objevit i nejnovější hrozby. To samé platí i pro systém na mobilním telefonu (Android, iOS), protože hrozí, že ve starších verzích systému byly nalezeny bezpečnostní díry, které otevírají útočníkům možnosti, jak zařízení ovládnout

Pravidla ochrany v kostce:

- Aktuální antivirová ochrana
- Korektně nastavený firewall
- Legální software
- Základní digitální gramotnost uživatele
- Pravidelné bezpečnostní aktualizace systému

2.3 Sociální inženýrství

Jedná se o způsob manipulace lidí za účelem provedení požadované akce nebo získání určité informace. Sociální inženýrství využívá k získávání informací slabosti lidského faktoru. Především lidské neopatrnosti, slabosti, neodpovědnosti a hlouposti. Principem této techniky je snaha útočníka vylákat peníze nebo citlivé informace včetně např. hesel k účtům prostřednictvím telefonu, mailu nebo osobního kontaktu, infikovaného flash disku atp. Využívá mimo jiné i lidské zvědavosti, například rozmístěním cd/dvd nosičů s různými „zajímavými“ popisky jako např. Platy managementu.

2.3.1. Phishing

Příběh - phishing

Pan Karel seděl u svého počítače, sledoval zábavná videa na Youtube a dobře se u nich bavil. Najednou uslyšel cinknutí ohlašující nový e-mail. Karel zastavil video a podíval se, kdo že mu to píše. Podle známého designu poznal, že je to zpráva od jeho banky s požadavkem na zaslání uživatelského jména a hesla:

Od: Tvoje Banka

service@tvojebanka.info

Datum: 15.9.2018 14:35

Předmět: Re

Vážený kliente,

V souladu s přechodem na nový systém péče o zákazníky budeme aktivovat nový systém, který výrazně zlepší vaší komunikaci s naší bankou a práci s vaším účtem.

Naším cílem je individuální přístup ke každému zákazníkovi, kdy každému nastavujeme jeho účet specificky podle požadavků klienta, viz naše oznámení před týdnem. K tomu však potřebujeme vaší součinnost:

Běžte prosím na tuto stránku: www.tvojebanka.info a tam klikněte vlevo dole na tlačítko „Kontrola údajů“

Karel okamžitě kliknul na odkaz jeho banky. Okamžitě se objevila webová stránka jeho banky, kterou tak důvěrně znal. Kliknul na doporučené tlačítko a vše vyplnil podle údajů.

Zkontrolujte si své údaje

Zkontrolujte číslo svého bankovního účtu a rovněž zkontrolujte heslo. V případě chybného čísla jej upravte a pošlete zpět.

Děkujeme vám za důvěru

Číslo Vašeho účtu:

Vaše heslo:

Za půl hodiny mu přišla na jeho mobil zpráva, kde se dočetl, že z jeho bankovního účtu bylo vybráno 30 tisíc korun, což byl jeho denní maximální výběr. Okamžitě si otevřel svůj elektronický účet a zjistil, že z něj opravdu odešlo 30 tisíc korun.

Nečekal a volal do své banky. Po krátkém rozhovoru se dozvěděl, že právě podlehl tzv. phishingovému útoku, kdy dal přístup ke svému bankovnímu účtu neznámým podvodníkům.

V současné době, kdy banky již vesměs používají vícefázové ověřování plateb, by takto jednoduchý útok již nebyl možný, nicméně uvedený příběh je typickou ukázkou phishingu, jedné z často používaných technik v počítačovém sociálním inženýrství. Phishingový útok začíná nejčastěji zasláním vhodně formulované zprávy poškozenému. Zpráva na první pohled nevzbuzuje u uživatele žádné podezření o možném podvodu. Součástí takové zprávy bývá zpravidla odkaz na zdánlivě důvěryhodnou stránku, odkaz bývá většinou doprovázen informací, že je potřebné vykonat nějaký jednoduchý, ale důležitý úkon (např. bezpečnostní aktualizace, potvrzení identity uživatele, atd.)

Otevřená webová stránka se následně tváří jako její originální ověřená předloha, svým vzhledem a funkčností je obvykle celkem zdařilou napodobeninou. Stránka se tváří, že je jejím prostřednictvím možné možné realizovat platební styk, vstupovat na zabezpečená

konta, taková konta spravovat apod. Uživatel stránce důvěřuje a do známých polí zadá požadované údaje. Data vložená uživatelem jsou však automaticky odesílána útočníkovi. Útočník tímto způsobem může získat například identifikační údaje uživatelů internetových bankovních služeb. Hlavním cílem útoků je přístup k jednotlivým bankovním účtům uživatelů napadených systémů, uživatelským datům v napadených službách nebo také k citlivým osobním informacím. Velmi snadno zneužitelné údaje získané touto činností jsou i údaje o platebních kartách, s jejichž pomocí je poté v prostředí internetu možné realizovat platby apod.

Ačkoli se o phishingu mluví nejčastěji ve spojení s bankovními aplikacemi (účty, platební karty), není nikterak výjimečný např. útok zaměřený na získání e-mailových hesel či důvěrných osobních údajů.

Ochrana před phishingem

- Nejen phishingu, ale i dalším útokům z oblasti sociálního inženýrství se lze bránit zejména neustálým vzděláváním sama sebe, získáním všeobecného přehledu.
- Protože se jedná o nelegální činnost, existuje pochopitelně legislativa, která ji postihuje. Zločinci však zákony obvykle příliš nerespektují, proto je vhodné být dobře informovaným a trénovaným uživatelem.
- Vzhledem k tomu, že se jedná o soubor klamavých technik, které míří spíše na uživatele jako takového, nikoliv na počítače nebo mobilní telefony, nelze se prakticky bránit technologickým zabezpečením. Antivirový program by mohl pomoci v případě trojského koně, ale na podvržené formuláře na webu bohužel nestačí.
- V reálném světě důvěřujte, ale prověřujte. Ve světě kybernetickém spíše nedůvěřujte!
- Ignorujte veškeré nabídky z nevyžádané pošty (spamu).
- Nikdy neklikejte na žádné odkazy z nevyžádané pošty (spamu).
- Internetové prohlížeče dnes disponují funkcí upozornění na potenciálně nebezpečné odkazy. Poučený uživatel sleduje, kam míří odkazy, na které kliká a v případě jakékoliv nesrovnalosti (např. chybějící či přebývající písmenko v internetové adrese banky) své údaje nikam nezadává.
- Své osobní údaje, heslo nebo bankovní údaje nevyplňujte na vám neznámých webových stránkách a neposílejte je emailem nebo instant messengery.

2.3.2. Pharming

Pharming je sofistikovanější formou phishingu. Útočník se naboural do DNS (Domain Name System) dané stránky a kohokoliv, kdo tuto stránku navštíví, automaticky přesměruje na stránku podvodnou. Útok začíná ve chvíli, kdy uživatel zadá do svého internetového prohlížeče doménové jméno svého finančního ústavu. Následně nedojde k přesměrování na příslušnou IP adresu originálního serveru, ale na adresu podvrženou. Webové stránky provozované na této podvržené adrese poměrně věrně kopírují originální stránky. Uživatel následně zadá přihlašovací údaje, které získá útočník.

Vzhledem k tomu, že podvržená stránka vypadá tak, jak uživatel očekává (např. jako internetové bankovnictví), je i pro zkušenější uživatele velmi obtížné tento typ útoku odhalit.

2.3.3. Scareware

Příběh - scareware: Jak jsem dostal výhružný e-mail sám od sebe

Na začátku pracovního dne se obvykle dívám do e-mailů, jestli tam není něco důležitého, co bych měl okamžitě řešit. A ejhle – e-mail Platba na základě 283; smlouvy. Kouknu na odesílatele a je tam můj vlastní e-mail. Přemýšlím, co je to za nesmysl, že píšu sám sobě. To už se začítám do textu v e-mailu, resp. ve spamu, který mě zřejmě má vyděsit a přimět k zaplacení cca 30000 Kč:

> *„Ahoj! Všiml sis, že jsem ti tento email poslal z tvého účtu? Přesně tak, znamená to, že mám k tvému zařízení plný přístup. Sleduji tě už několik posledních měsíců. Chceš vědět, jak? No, z erotické webové stránky, kterou jsi navštívil, byl tvůj systém infikován malwarem. Možná se v takových věcech neorientuješ, takže se ti to pokusím vysvětlit. Úplný přístup k tvému počítači a jakémukoliv jinému zařízení jsem získal díky viru trojského koně. To jinými slovy znamená, že tě můžu kdykoliv po aktivování kamery a mikrofonu prostřednictvím tvého monitoru sledovat a ty si toho ani nevšimneš. A stejně tak jsem získal i přístup k tvému seznamu kontaktů a veškeré korespondenci. Možná se teď sám sebe ptáš: „Jak se to ale možný, když mám na svém počítači aktivován antivir? Jak to, že jsem nedostal žádný upozornění?“. Odpověď je jednoduchá – můj malware využívá ovladače, ve kterých každé čtyři hodiny aktualizuji podpisy, takže je naprosto nezjistitelný a tvůj antivir o něm vůbec neví. Aktuálně mám k dispozici video, na kterém v levé části obrazovky masturbuješ, zatímco v její pravé části se přehrává klip, který při tom sleduješ. A chceš vědět, co všechno s ním můžu udělat? Jediným kliknutím myši ho můžu rozeslat na všechny tvé stránky sociálních sítí a všem tvým emailovým kontaktům. Zároveň můžu i zveřejnit přístupové údaje kšveškeré tvé emailové korespondenci a messengerům, které vššoučasnosti používáš. Pokud tomu chceš zabránit, stačí na moji bitcoinovou adresu převést částku 1200 EURO (pokud nemáš ponětí, jak to udělat, zadej do svého prohlížeče snadný dotaz: “Koupit bitcoiny”). Moje bitcoinová adresa (BTC Wallet) je: 1778RYiKxW5kCFLH7BPbKEJ2zce83adFf2 Ihned po potvrzení platby video smažu a je hotovo. Nikdy víc už o mně neuslyšíš. Na dokončení transakce máš 2 dny (48 hodin). Po otevření tohoto emailu, mi dojde oznámení a časový odpočet začne tikat. Jakýkoliv pokus o podání stížnosti je zbytečný, protože tento email, stejně jako moji bitcoinovou adresu, nelze zpětně vysledovat. Na svém systému pracuju, jak nejdéle to jen jde, a chybám nedávám sebemenší prostor. Pokud jakýmkoliv způsobem zjistím, že jsi tuhle zprávu komukoliv ukázal, výše uvedené video okamžitě zveřejním“.*

Nejprve si vyhledávám informace o podobných podvodných e-mailech. Dozvídám se, že tyto falešné e-maily jsou v současné době běžnou záležitostí a dělat s nimi nic moc nejde. Důležité ale zachovat zdravý rozum. Ve většině případů podobné výhružky ve spamu neznamenají vůbec nic. Výjimkou jsou případy, kdy útočník do vašeho počítače skutečně pronikl a nějaké vaše kompromitující materiály doopravdy má – v tom případě si ale buďte jisti, že by vám rovnou poslal nějakou ukázku, což není tento případ. Rozhodně bychom neměli platit nějaké peníze za podvodníkovo mlčení. Je to jen útočníkova léčka - taková zkouška, jaké máme digitální vědomosti a jestli se na to nachytáme. Je samozřejmě vhodné pravidelně kontrolovat zabezpečení vašeho počítače proti virům a dalšímu nežádoucímu softwaru.

Já jsem povolal rodinu k troše digitální osvěty - přečetl jim e-mail a vysvětlil jim, že se jedná

o podvodný útok a co je jeho cílem. Vysvětlil jsem jim, že tito podvodníci náhodně vybírají adresy odesílatele z emailových adres, které najdou na internetu a já měl prostě to „štěstí". Adresu odesílatele může útočník při troše technických znalostí skutečně podvrhnout. Dětem jsem zdůraznil, aby si dávaly pozor na to, když je někdo mailem žádá o peníze nebo o poskytnutí různých důvěrných údajů jako je číslo kreditní karty nebo uživatelské jméno pro určitou bankovní službu. Nevím, jak moc to zabralo, protože od té doby dostávám dotazy spíše na to, jestli už jsem internetová hvězda a slib, že video se mnou všichni rozhodně lajknou.

Zároveň jsem napsal tento článek s tímto upozorněním na podvodné e-maily s vírou v to, že se na ně už nikdo nenachytá a přesune je rovnou do spamu.

Podobné útoky řadíme mezi tzv. scareware – mají uživatele vyděsit a přimět ho k nějaké akci, ze které útočník profituje. První část se tomuto podvodníčkovi zčásti podařila i v mém případě, jazyková nedokonalost zprávy a další podezřelé údaje byly však dostatečným varováním a věřím, že by byly i pro vás.

Útok, nebo chcete-li pokus o podvod z našeho příběhu je příkladem scareware. Kyberzločinci obětem vnutí, že jejich počítače nebo chytré telefony byly nakaženy, aby je přesvědčili k zakoupení falešné aplikace nebo zaplacení určité částky. Při typickém napadení z oblasti scareware se vám může při procházení webu zobrazit výstražná zpráva s varováním, že váš počítač je infikován nebo že se v něm vyskytl virus. Scareware však nemusí mít nutně jen softwarovou podobu. K vyvolání strachu a paniky uživatele často stačí (tak jako v našem příběhu) vhodně formulovaný email s více či méně věrohodnou informací, že počítač uživatele byl napaden. Útočník ve zprávě vyhrožuje např. zveřejněním kompromitujících či jinak citlivých informací o uživateli atp.

2.3.4. Kombinované útoky

Útoky za pomoci technik sociálního inženýrství lze velmi přesně zacílit na konkrétní osoby. Velmi častou obětí útoků jsou majitelé účtů na službách s placeným obsahem. K útokům je využito více různých technik, např. phishing v kombinaci s keyloggerem distribuovaným v nevyžádané poště.

2.3.4.1 Krádež uživatelského účtu

Příběh - ukradené hry

Patnáctiletý Radek je vášnivým sportovcem a velmi dobře hraje na klavír. Hodně volného času ale také tráví hraním počítačových her. Kromě oblíbeného fotbalu si na počítači s kamarády rád zahraje i nějakou týmovou strategickou střílečku. Většinu her si nakoupil přes distribuční platformu Steam. Nákupy i instalace přes Steam jsou jednoduché a všechno může Radek ovládat z jednoho prostředí. Hraní mu většinou sponzorují rodiče a občas dostane od někoho dalšího jako dárek poukázku na nákup nové hry nebo nějakých vylepšení.

Tipy na nové hry i různé herní triky studuje s kamarády na Youtube nebo na herních fórech a registroval se i k odběru řady hráčských newsletterů, které mu chodí do emailové schránky. Často jsou doprovázeny přílohami s různými návodnými texty či obrázky.

V létě ale tolik času u počítače netráví. Během posledních letních prázdnin byl na fotbalovém soustředění a pak s rodiči na deset dnů v Alpách. Po obědě na horské chatě Radek rychle kontroloval zprávy na svém telefonu. Po několika rychlých odpovědích chatujícím kamarádům narazil v emailové schránce na něco, co ho zarazilo: zpráva z podpory Steamu, že právě nakoupil za 30 dolarů nové funkce do hry Dota.

“To přece není možné, vždyť jsem nakupoval naposledy někdy v květnu a teď v létě jsem už tři týdny ani nehrál?” diví se Radek. Večer, když se vrátili do penzionu, se Radek zkusil z tátova notebooku přihlásit do Steamu. Ani na třetí pokus heslo, které si naprosto bezpečně pamatoval, neprošlo…

Radkovi někdo na Steamu odcizil uživatelský účet. Děje se to tak, že útočník nějakým způsobem zjistí uživatelské jméno a heslo. Získat uživatelské jméno je celkem snadné - obvykle jej používáte na herním fóru nebo je viditelné při multiplayer hraní. Heslo při těchto útocích nejčastěji útočník zjistí z nějaké hacknuté databáze nebo za pomoci keyloggeru ve vašem počítači. Další možností je zaútočit přímo na váš emailový účet - pokud se tam útočník dostane, většinou pak snadno získá přístup ke všem službám, které jsou k mailu navázané a nemají vícefázové ověření přístupu.

Jak ochránit svůj účet před hackery?

- Používám bezpečná, tzv. silná hesla (“JednaDve34pet” je mnohem bezpečnější než “12345”
- Přístupové údaje k účtům bezpečně ukládám, případně i šifruji
- Používám antivirovou ochranu svých zařízení
- Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon)
- Instaluji pouze software z ověřených zdrojů
- Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy
- Neprodleně reaguji na jakékoliv známky napadení účtu (změním heslo, dočasně umožním přístup jen z jednoho zařízení, atd.)

2.3.4.2 Odcizený účet jako nástroj phishingu

Přístup k cizímu účtu však může poškodit nejen samotnou oběť, ale i další její kontakty. Pokud je útočník důsledný a vytrvalý, může odcizený účet použít k dalším phishingovým či jiným útokům.

S pomocí souběžného útoku na uživatelské účty přátel oběti na sociálních sítích dokonce může útočník prolomit i vícefaktorové ověřování přístupu, například v kombinaci heslo+SMS ověření:

Příběh - nákup na cizí účet

Předpokládejme, že máme dva kamarády - Honzu a Martina. Útočníkovi se podaří nabourat se do Honzova účtu na eshopu a rozhodne se, že nakoupí zboží na Honzův účet. Honza má svoji platební kartu v účtu uloženou, eshop však má zabezpečené platby a kromě platební karty ověřuje nákup ještě zasláním verifikačního kódu k platbě. Problém je, jak zjistit verifikační SMS kód, aniž by Honza pojal nějaké podezření. Jak to udělat? Útočník si na pomoc vezme Martina. Tedy ve skutečnosti ukradený Martinův účet na sociální síti.

To se tak Honza večer chystá ke spánku a zničehonic pípne mobil. V Messengeru vidí zprávu od Martina a mezi SMS je další nepřečtená zpráva. Martin píše, že prý omylem při registraci zadal Honzovo telefonní číslo a potřeboval by přeposlat registrační kód, který by před chvílí měl přijít do mobilu. Martin je dobrý kamarád, takže Honza moc dlouho nepřemýšlí a kód z esemesky Martinovi přeposílá. Útočník tím pádem dokončuje platbu a vyzvedává zboží z eshopu. Honza škodu zjistí až za pár dnů při kontrole výpisu ze svého účtu

“Kamarád” Martin byl tedy ve skutečnosti maskovaný útočník, který se Martinovi naboural do Facebookového účtu. Protože měl k dispozici Honzův přístup k účtu, k převodu peněz mu stačilo provést druhé ověření přes textovou zprávu. Z identity Honzova dobrého přítele tedy útočník odeslal prosbu o přeposlání verifikačního kódu, a protože Honza “Martinovi” vyhověl, útočník dostal správný verifikační kód a peníze putovalyl tam, kam potřeboval.

Že by se ve vašem případě něco takového nemohlo stát? Možná u vás ne, ale pokud má útočník dostatečně velkou zásobu obětí, u kterých je schopen se k údajům dostat, je téměř jisté, že bude úspěšný.

Jak se podobným útokům bránit?

V každém případě je potřeba důležité služby chránit vícefaktorovým ověřováním, tj. kombinací hesla s dalším kanálem, jako je SMS, biometrické údaje, atd. A nikdy nepřeposíláme žádná hesla a verifikační kódy, aniž bychom si tuto operaci opět neověřili jiným kanálem, nejlépe osobně nebo alespoň telefonicky.

2.3.5. Scam

Typ podvodu, kdy se útočník obvykle emotivními a zdánlivě důvěryhodnými zprávami (nejčastěji emaily) snaží vybudovat důvěru oběti. Obětem jsou nabízeny peníze, neobvyklé zážitky, získání skvělého životního partnera, zázračný lék, atd. Běžný scénář je takový, že pro daný benefit je potřeba nejprve zaplatit nějaký (administrativní, manipulační…) poplatek ve výši zlomku hodnoty nabízeného zisku. V okamžiku úhrady poplatku buď komunikace útočníka končí nebo se “náhle a nečekaně” vyskytnou problémy, kvůli kterým je potřeba uhradit ještě něco dalšího, případně se celý proces nekonečně prodlužuje. Ve všech případech akce končí v neprospěch oběti.

U nás jsou z oblasti scamu asi nejznámějším případem tzv. Nigerijské dopisy. Je jich celá řada, mohou vypadat např. takto:

> *Omlouváme se za tento způsob, jak vás kontaktovat. Jmenuji se Patricia Zorzutti. Mám francouzskou národnost. Ale v současné době jsem v Beninu ze zdravotních důvodů, trpím vážným onemocněním, které mě odsoudí k jisté smrti, je to rakovina hrdla a mám částku 43.000 eur, kterou bych rád dal někomu důvěryhodnému a čestnému, aby se dobře používal. Vlastním společnost, která dováží červený olej do Francie, a před 6 lety jsem ztratil manžela, hodně se mě to dotklo a dosud jsem se nemohl znovu oženit, nemáme žádné děti. Chci darovat tuto částku před svou smrtí….*

Již na prvním odstavci takového dopisu vás může zaujmout např. zvláštní jazyk, kterým je psán - jedná se o automatický překlad (většinou z angličtiny), proto zdánlivý pisatel zmatečně přechází z mužského rodu do ženského atd. Dopisy bývají jinak docela čtivé a emotivní, ale zamysleli jste se nad tím, proč tolik peněz nabízí pisatel právě vám? Ano, je to proto, že chce vzbudit váš zájem a důvěru a čeká, kdo mu na tuhle vějičku naskočí...

Další informace o tomto typu podvodu lze najít např. na Hoax.cz: (https://www.hoax.cz/scam419/co-je-to-scam-419)

2.3.6. Podvodné nákupy na internetu - prodávejte bezpečně

Příběh

Jirka dostal k narozeninám nový notebook a protože ten starý byl stále funkční, rozhodl se, že jej prodá na internetu. Sestavil proto inzerát, který vystavil na několika online bazarech. Cenu trochu nadsadil, řekl si, že zlevnit může kdykoli. Prvních pár dnů se nic nedělo, až asi za týden mu blikla v chatu zpráva:

"Dobrý den, máte ještě ten notebook? Měl bych zájem."

Jirka zrovna dělal práci do školy, ale vidina rychlého prodeje jeho soustředění rychle převedla jinam. Odepsal, že není problém a že přístroj je připraven k předání.

"Potřeboval bych to mít zítra ráno u sebe, zvládnete mi počítač odeslat ještě dnes? Vaši cenu respektuji a zaplatím přes banku okamžitě, když mi pošlete číslo účtu", pokračoval zájemce v konverzaci.

Myšlenky na školu byly definitivně pryč, Jirka vylovil z paměti číslo a hned ho poslal do konverzace. Z druhé strany přišlo rychlé "OK" a asi za dvě minuty chat cinká znovu:

"Tak je to hotové, peníze odeslány. Pošlu pro počítač kurýra, do hodiny je u vás. Mohu požádat o adresu? Potvrzení z banky pošlu další zprávou."

Jiří bleskově vypsal adresu domů a mrknul do rohu, kde stála krabice se starým notebookem: "To je panečku rychlost," pomyslel si když mu na displeji blikla další zpráva, tentokrát i s přílohou:

"Tady je to potvrzení z banky, peníze máte do rána na účtu. Kurýr už je na cestě k vám."

Po rozkliknutí se na displeji objevil strohý oficiální formulář Potvrzení o platbě, kde stálo, že banka potvrzuje, že z účtu 123456789/5678 vedeného na majitele Davida Eliáše. bylo převedeno 4500 CZK na účet 45454545/5566, což je číslo Jirkovy banky. Jiří se spokojeně usmál a odlomil si kousek čokolády, která ležela na stole. Za pár desítek minut zastavila před domem bílá dodávka a Jiří předal šoférovi balíček. Krátkou zprávou kupujícímu, který měl svůj profil označen jako Dave Strong ještě poděkoval za rychlý obchod.

Už nějakou dobu se chystal si pořídit nová luxusní herní sluchátka a peníze za notebook se mu teď budou docela hodit. Za dva dny večer tedy usedl k eshopu a vybraný kousek naklikal do košíku. Uvědomil si, že by měl ještě zkontrolovat, zda už platba za notebook dorazila. Pustil tedy internetové bankovnictví. Zůstatek byl však stejný jako před týdnem, platba od Dave Stronga. nikde. Zkusíme mu napsat? OK, ale co to? Uživatel neexistuje?

Platba nedorazila ani v dalších dnech a bylo jasné, že se Jiří stal obětí internetového podvodníka. Při důkladné kontrole potvrzení z banky zjistil, že číslo účtu na potvrzení je smyšlené a celé potvrzení je jen obyčejný textový dokument bez elektronického podpisu banky. Takže podvrh. Vzhledem k tomu, že Jiří nevěděl o podvodníkovi vůbec nic a nebyl schopen ani blíže identifikovat šoféra s dodávkou, šance na dohledání podvodně vylákaného notebooku je prakticky nulová.

Pravidla bezpečného prodeje

- U nakupujících, které neznám, se snažím zjistit věrohodné reference
- Zboží popíšu co nejpřesněji, aby bylo naprosto zřejmé, co prodávám
- Při prodeji bazarového zboží je nejbezpečnější osobní předání na veřejném místě,

případně zaslání zboží po platbě předem

- Platbu dobírkou, případně po obdržení zboží akceptuji jen u ověřených nakupujících
- Obrázek nebo jiný dokument obsahující jakékoli potvrzení o platbě není věrohodný, pokud neobsahuje elektronický podpis (certifikát) toho, kdo potvrzení vystavuje.
- Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží)
- Není-li to nezbytné, nevodím neznámé zájemce až k sobě do bytu. Věc lze předat venku či na veřejném místě

2.3.7. Podvody při prodeji zboží - jak nenaletět při nákupu

Příběh

Michalovi se pomalu, ale jistě blížily jeho patnácté narozeniny. "To je významný mezník v životě každého mladého člověka" prohovořil otec při nedělním obědě. "A takový mezník je třeba orámovat nějakým darem, který se významně zapíše do Tvého života synu" pokračoval otec. "Co by sis přál, abys pocítil změnu života? zeptal se otec. Michal se dlouho nerozmýšlel a rychle odpověděl: "Iphone, jednoznačně Iphone, většina ve třídě ho má." "To přece není argument", odpověděl otec, na kterém bylo vidět, že ho přání zaskočilo. Nechtěl brát své slovo zpět a tak řekl: "Napiš mi na A4, jaký je takový rozdíl mezi Iphone a jiným mobilem, že ho tak potřebuješ". Brzy Michal přinesl zpracovaný úkol. Na papíše A4 bylo velkými Písmeny napsáno: "JE TO PROSTĚ IPHONE". Otec se zprvu chtěl rozčilovat, ale pak si uvědomil, že v té větě je vše, co po synovi vyžadoval. Rozhodl se dostát svému slibu.

Na Internetu našel iPhony, které se pohybovaly okolo dvanácti tisíc, což bylo nad maximem, které chtěl do mobilu investovat. To si zakázal dívat se na poslední novinky, které byly násobně vyšší. Pak si dal vybraný mobil do porovnávačů cen. Našel levnější ceny u použitých nebo zánovních iPhonů. Chtěl však synovi koupit k patnáctinám mobil nový a tak pokračoval v hledání nejlevnějšího eshopu. Pak ho našel. Obchod s výprodejem těchto mobilů s cenou pod šest tisíc., Obchod se jich zbavoval, protože chtěl prodávat jen ty nejmodernější typy. Otec nezaváhal ani vteřinu a okamžitě ho koupil, především z toho důvodu, že na skladě byly poslední dva, navíc v požadovné barvě.

Narozeniny se blížily a otec spokojený se svými obchodními dovednostmi čas od času vypustil poznámku, která naznačovala, že se má Michal na co těšit. Uplynul týden a mobil nepřišel. Nepřišel ani další týden. To už do narozenin zbývaly necelé dva týdny. Otec volal do eshopu několikrát denně. Nikdo nebral telefony. Začal se tedy o eshop zajímat více. Zjistil, že nesídlí v České republice, ale v zahraničí. V referencích, které na obchod našel, si přečetl, že jedná o podvodný obchod, který nabízí levné mobily, avšak je nikdy neodeslal. Takových referencí tam bylo desítky. Otec byl ten den velmi zatrpklý. Ještě zkusil párkrát zavolat, napsal i e-mail, podíval do diskuzí na možnosti postupu, volal na úřady. Výsledkem bylo, že v den narozenin šel do klasické prodejny, kde koupil iPhone za téměř třináct tisíc korun.

Triky podvodníků

Internet je největší světové tržiště. Lze na něm koupit cokoli - luxusní a kvalitní zboží i levné a nefunkční cetky. Můžete i naletět úplně a za své peníze nedostat vůbec nic. Vytvořit elektronický obchod, který bude vypadat, že je plný krásného zboží, není nic složitého. Náklady jsou zanedbatelné. Pro podvodníka je tedy velmi snadné vytvořit lákavou "výkladní skříň",

přes kterou se bude snažit vylákat z vás peníze. Vy si objednáte pěkný telefon, zaplatíte a od té doby o obchodu neuslyšíte. A jste bez peněz.

To však není jediný způsob, jak přijít o peníze. Jsou i obchody, které zboží skutečně posílají, avšak kvalita toho, co dostanete domů, je o moc horší než to, co obchod inzeroval. Pak nezbývá než reklamovat a to je často velmi dlouhá anabáze. Mnoho podvodníků dopředu spoléhá na to, že u levnějších položek zákazník reklamovat nebude a se ztrátou se prostě smíří.

Rozpoznat podvod na první pohled není úplně snadné. Existuje však několik způsobů, jak zvýšit pravděpodobnost, že vámi vybraný obchod vám skutečně doručí to, co potřebujete. Obchodník, který kromě eshopu provozuje i velkou síť kamenných obchodů, nebude pravděpodobně patřit k nejlevnějším, ale dá vám vyšší jistotu, že na druhé straně nestojí anonymní podvodník. Navíc budete mít jednodušší i případnou reklamaci vadného zboží. Nejcennějším nástrojem jsou však dnes asi sdílené zkušenosti uživatelů. Pokud jsou řádově stovky či tisíce jiných lidí s nákupem spokojeny, pravděpodobně budete spokojeni i vy. U referencí není dobré spoléhat na jeden zdroj, ale pokud například zkombinujete čtení recenzí v nákupních srovnávačích (Heureka.cz, Zbozi.cz) s průzkumem zkušeností na sociálních sítích, získáte o obchodu celkem dobrý obrázek

Pravidla bezpečného nákupu

- U prodejců, které neznám, se snažím zjistit věrohodné reference.
- Informace o prodejci ověřuji z více nezávislých zdrojů (Má kamenné obchody? Jaké jsou reference na srovnávačích? Co říkají sociální sítě? A co články v médiích?).
- Pokud nakupuji, za zboží předem platím jen v případě ověřených prodejců.
- Před nákupem se snažím o zboží i podmínkách prodeje zjistit maximum (recenze zboží jinde než u prodejce, nezávislé testy, záruční a reklamační podmínky…).
- Platební údaje k bankovní kartě ukládám odděleně a používám je jen u ověřených prodejců.
- Platební údaje nenechávám uložené ve svém účtu u obchodníka.
- Online platby provádím pouze ze zařízení, o kterém vím, že je bezpečné.
- Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží).

2.3.8. Hoax

Příběh

Minulý týden Jitka ve své doručené poště nalezla následující zprávu:

> *Od: mojebanka@bankovnivarovani.com*
> *Pro: klienti@bankovnivarovani.com*
> *Předmět: Víte, jak používat svůj PIN?*
> *Vážení klienti,*
> *přímo od bankovní komise jsme dostali oficiální informaci, kterou s vámi musíme ihned sdílet:*
> *V případě, že jste napadeni a ocitnete se v situaci, kdy musíte pod nátlakem*

vybrat peníze z bankovního automatu na požádání/přinucení násilníkem, zadejte svůj PIN opačně:

to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli.

Prosíme, přepošlete toto co nejvíce lidem.

Jitce se informace příliš nezdála a proto zavolala do svojí banky a sdělila operátorovi informace z mailu. Dozvěděla se, že se jedná o hoax, zpráva je zcela smyšlená a nemá žádný reálný základ. Nejlepším řešením je zprávu smazat a dále se jí nezabývat.

Hoax je nepravdivá zpráva nebo informace, která se tváří jako ověřený fakt. Obvykle jde o senzační či zdánlivě velmi důležitou zprávu, která se šíří internetem jako lavina. Uživatelé, kteří této informaci uvěří a jednají v souladu s ní, mohou být svým jednáním poškozeni. Často jsou hoaxy šířeny s cílem ovlivnit chování či názory určité skupiny uživatelů internetu.

Jak rozpoznávat a vypořádat se s hoaxy?

- Zajímám se o to, co se děje kolem a tudíž mám přehled, co ve skutečnosti platí a co ne.
- Nesdílím neověřené informace.
- Pokud mne někdo vybízí ke sdílení informace, kterou mám pouze od něho, informaci si nejprve ověřím z více různých spolehlivých zdrojů.
- Pokud někdo vědomě šíří nepravdivou informaci, která by mohla způsobit nějaké škody, jedná se o trestný čin. Takové jednání neprodleně hlásím PČR.
- Zprávy čtu pozorně a přemýšlím nad jejich obsahem. Rozvíjím své kritické myšlení.
- Pokud někdo z mého okolí šíří hoax, upozorním jej na to.

2.4 Kyberšikana

Příběh

Daniel je IT pracovník v malé fabrice na okresním městě. Celý den ve firmě řeší problémy spolupracovníků s jejich počítači, připojuje tiskárny, spravuje síť, vysvětluje jak se připojit k internetu nebo jak funguje optická myš. Ve volném čase rád zajde s přáteli na šipky nebo na kolo.

Před několika lety, když ho opakující se dotazy kolegů v práci dohánělyk šílenství, začal vybíjet svou frustraci trollingem. Tu napsal vulgární anekdotu na křesťanském fóru, jindy sdílel na kutilském webu nesmyslné video, například jak lze na kapotě usmažit vajíčko. Nejčastěji navštěvoval fórum IT-help.cz. Uživatelé tam totiž psali tytéž dotazy, se kterými pomáhal kolegům ve fabrice. Narozdíl od práce, ale na fóru mohl Daniel říct, co si o problému skutečně myslí, jindy se danému uživateli vysmíval nebo místo odpovědi zkopíroval kuchařský recept..

Nikdy si nepřipustil, že to co dělá, je špatné, a že ne všichni uživatelé mají stejnou výchozí pozici jako on sám.

Jednoho dne šel Daniel hrát šipky se svým kamarádem Františkem. Ten ač má už hodně přes 70 let ho v šipkách pravidelně poráží. Tento večer ale není ve své kůži. Po chvilce naléhání se svěří, že má trable v digitálním světě. Kvůli svému věku moc neovládá počítač, ale

styděl se požádat kohokoliv ze svého okolí o pomoc. Začal proto sám s pomocí fóra IT-help.cz. Bohužel často narazil místo rady na posmívání nebo nesmyslné řešení. Nechápal, proč někteří na dotazy reagují takto. Obzvlášť posměšky, od některých jiných uživatelů, ho bolely. Přemýšlí proto, že notebook, který dostal od dětí jako dárek, prodá.

Teprve nyní si Daniel uvědomuje, kdo také může sedět na druhé straně obrazovky. Velmi se stydí. Nabízí Františkovi, že k němu domů ještě tento týden zajde a základy práce s počítačem mu naživo ukáže. Vysvětluje mu také, kdo jsou to trollové a že nejlepší obranou proti nim je ignorovat je. Ve Františkově věku je přece obdivuhodné, že se pouští do neznámých vod digitálního světa. Sám Daniel navíc začíná přemýšlet o tom, jak naloží s volným časem, který tak nesmyslně věnoval trollení…

Kyberšikana (kybernetická – počítačová šikana, angl. cyberbullying) je druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) k ublížení druhému (vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.) Trolling z našeho příběhu je pouze jednou z forem kyberšikany. Mezi ty další řadíme např. kybergrooming (zneužívání dětí), kyberstalking (pronásledování), atp.

Oproti útokům z kategorie sociálního inženýrství není primárním cílem kyberšikany prospěch útočníka, nýbrž poškození oběti.

Jak se bránit kyberšikaně?

- Na sociálních sítích důkladně zvažuji, pro koho bude viditelný mnou publikovaný obsah a toto nastavení pravidelně kontroluji.
- Nepublikuji veřejně žádné informace, které by mohly být snadno zneužity (např. intimní fotografie nebo soukromá videa).
- Pokud někdo publikuje obsah, který mne zesměšňuje, mohu požádat provozovatele služby o smazání či nahlásit závadnost příspěvku.
- V případě, že je předpoklad, že obsah, který mne poškozuje, naplňuje charakter přestupku nebo trestného činu, příspěvek hlásím rovnou Policii ČR - nežádám o smazání, neboť se jedná o důkazní materiál.
- Vzdělávám se a získávám přehled o možných hrozbách i o možnostech, jak získat pomoc.
- Cítím-li se ohrožen, neváhám kontaktovat někoho, kdo mi může pomoci (rodič, učitel, trenér, policie, linka důvěry…).
- V diskuzi či jiné komunikaci, ve které jsem napadán, nepokračuji, zvláště hrubé jednání hlásím provozovateli služby.

2.5 Útoky na úrovni infrastruktury

Předchozí útoky vesměs vyžadovaly určitou interakci uživatele a mířily do uživatelských zařízení či přímo na osobu, data či peníze konkrétního uživatele. Existují však i útoky na komunikační kanály či prvky vyšší infrastruktury, které útočník může ovládnout bez toho, aby napadl koncového uživatele. Pro útočníka má takový útok v případě úspěchu mnohem vyšší užitek, neboť může operovat s daty velkého množství uživatelů naráz.

2.5.1. Sniffing

O sniffingu hovoříme v případě, kdy se jedná o zachytávání dat, nelegální odposlech či záznam telekomunikačního provozu sítě. Sniffing je metodou, která zachytává data (volné packety) procházející sítí prostřednictvím tzv. snifferu. Tento sniffer slouží k monitorování a prohlížení si cizí komunikace. Často u síťových spojení dochází k nešifrované komunikaci a díky tomu je sniffing reálnou hrozbou. Takto sniffovaný provoz umožňuje „číst“ soukromá data vysílaná a přijímaná v rámci sítě. Takovou činnost můžeme označit jako nelegální odposlech či záznam telekomunikačního provozu. Mimo „hackerů“ mohou sniffing využít i administrátoři či bezpečnostní experti v rámci podnikových sítí, kdy na základě “odposlechu” síťového provozu umějí identifikovat případné hrozby (nežádoucí provoz v síti v důsledku přítomnosti spyware či jiného nebezpečného software).

Laikovi se princip odposlechu pomocí sniffingu může zdát shodný s fungováním spyware. Zásadním rozdílem je to, že případě sniffingu útočník (či obecně ten, kdo chce obsah komunikace zachytit) nepotřebuje do uživatelova systému nic instalovat. Odposlech probíhá v síti na trase, kterou musí datové pakety absolvovat při cestě od jednoho uživatele ke druhému.

2.5.2. Man in the Middle

Principem útoku Man in the Middle je to, že se útočník dostane do digitální cesty (komunikačního kanálu) mezi dvěma účastníky komunikace. Útočník tento kanál může přerušit a přijímat zprávy od obou stran, měnit jejich obsah a vysílat je dále k protistraně. Oběma stranám komunikace se útočník jeví jako správná protistrana. Při nezabezpečené komunikaci stačí účastníkovi data číst. Pokud obě strany používají šifrování, přítomnost útočníka v komunikačním řetězci mu umožňuje zaměnit šifrovací klíče účastníků za klíče vlastní a útočník tak může komunikaci dešifrovat, pozměnit a opět zašifrovat a poslat dál.

Ochrana před útokem

Ochranou je šifrovaná komunikace s výměnou klíčů jiným ověřeným a bezpečným kanálem (např. telefonem nebo prostřednictvím certifikační autority)

2.5.3. Útoky typu DoS a DDos

Denial of service (DoS) je útok na internetovou službu s cílem tuto službu znepřistupnit ostatním uživatelům. Útok službu znefunkční nejčastěji prostřednictvím velkého množství požadavků, případně využitím nějaké chyby v systému služby. Uvedená napadení neumožní získat nad službou kontrolu, avšak odstaví ji z provozu. DDoS je zkratkou pro tzv. distributed denial of service typ útoku, kdy se pro zahlcení cílové služby používá velké množství počítačů rozmístěných v internetu.

Útokům typu DoS jsou z důvodu nekorektně vedeného střetu názorů často vystaveny významné servery vládních organizací či politických stran, avšak výjimkou nejsou ani útoky na weby komerčních subjektů, eshopy, atd.

Občas dochází k paradoxní situaci, kdy si poškozený subjekt podobný útok sám vyvolá. Často například dochází ke zhroucení eshopů v průběhu výprodejových či slevových akcí. Nabídka prodejce je pro zákazníky natolik lákavá, že kapacita serveru nestihne odbavit všechny zájemce a systém pod množstvím požadavků zkolabuje. Dalším příkladem byl kolaps čerstvě spuštěného webu Ministerstva dopravy edalnice.cz pro nákup elektronických dálničních známek. Web nebyl před svým startem řádně otestován a pouze několik minut po spuštění v prosinci 2020 pod náporem uživatelských požadavků přestal fungovat.

Ochrana před útokem

Před těmito útoky se uživatel služby chránit nemůže, uživatel není přímou obětí útoku. Ochrana je nutná na straně poskytovatele či provozovatele služby. Spočívá ve správném nastavení serverů, firewallů a důkladném monitoringu síťového provozu.

2.5.4. SQL Injection

Útoky tohoto typu míří na servery, které pracují s SQL databázemi. Útočník využívá chyb v programovém kódu (nejčastěji webové stránky) a snaží se serveru podstrčit programový kód, který mu v případě úspěchu dá možnost ze serveru získat jinak nepřístupné informace, případně server zcela ovládnout. Vložení závadného kódu bývá překvapivě jednoduché: útočníci používají např. vyhledávací nebo registrační formulářová pole webů.

Ochrana před útokem

Útoku se lze bránit kvalitním ošetřením programového kódu serverové aplikace proti vložení nežádoucího kódu.

2.5.5. Útoky na IoT zařízení

Útoky využívají obvykle slabší zabezpečení jednoduchých přístrojů napojených na internet. Často je k napadení využit botnet, napadené zařízení se pak může stát jeho součástí, ačkoli jinak funguje navenek normálně. V jiných případech naopak mohou útočníci naráz velký počet přístrojů znefunkčnít.

Velmi diskutovaným tématem současnosti je hrozba útoků na inteligentní systémy řízení dopravních prostředků. Potenciální průnik útočníka například do řídícího systému automobilu a převzetí kontroly nad vozidlem může mít fatální následky.

Ochrana před útokem

Užitečné je pravidelně aktualizovat firmware chytrých zařízení a ztížit tak útočníkovi jeho snahu. Velmi snadno se lze dostat např. do zařízení, ve kterém necháte výchozí heslo z výroby.

2.6 Úniky dat

Data jsou obvykle to nejcennější, co uživatelé a firmy ve svých počítačích a dalších digitálních zařízeních mají. Proto také k jejich získání směřuje největší množství kybernetických útoků. Oblíbeným cílem jsou údaje o uživatelích či klientech, jejich hesla a osobní data, ale pochopitelně také další zpeněžitelné informace, jako např. firemní know-how, strategické dokumenty a další informace.

Ochrana před útokem

Principem ochrany před únikem dat je dodržení pravidel ochrany před všemi typy kybernetických hrozeb.

2.7 Poškození nebo zničení části počítačového systému

K útokům prostřednictvím virů nebo sociálního inženýrství je na straně útočníka potřebná obvykle slušná znalost programování, technologií či psychologie. K tomu, abyste přišli o svá data, bohužel často stačí podstatně méně. Ztráta notebooku, ke kterému nemáte zálohu, či poškození vašeho zařízení požárem nebo vadnou nabíječkou dokážou napáchat stejné, ba mnohdy i větší škody než hackeři, kteří mají zájem o vaše data.

Kromě nahodilých technických závad se ve světě techniky občas vyskytnou i závady uměle vyvolané. Neboli existují útočníci, které nezajímají data, ale chtějí poškodit vaše zařízení.

2.7.1. USB killer

Příběh - USB killer

Tak jako téměř každý den si i tohle dopoledne Jitka užívala se svým malým synkem Radimem na dětském hřišti. Byl teplý začátek září a hřiště skoro plné. Děti vesele skotačily a maminky probíraly zážitky z prázdninových cest. Jitka se pomalu chystala s Radimem k odchodu, když chlapec radostně přiběhl: „Maminko, podívej, co jsem našel!“ Držel v ruce malou barevnou tyčinku a radostně s ní mával nad hlavou. Jitka se nejprve trochu lekla, že její dítko někomu sebralo oblíbenou hračku, ale při bližším ohledání zjistila, že tohle hračka určitě nebude. „Ráďo, myslím, že jsi našel něco, co někdo ztratil. Zkusíme zjistit, komu to patří.” Barevná tyčinka byla totiž ve skutečnosti USB flashdisk v docela pěkném pouzdře z měkkého plastu.

Dotazování na ztrátu v okolí hřiště se nesetkalo s odezvou, Jitka se tedy rozhodla, že zjistí, co na nalezeném datovém médiu je a podle toho zkusí dohledat majitele. Doma tedy po obědě otevřela notebook a po startu systému vsunula flashdisk do konektoru a spustila prohlížeč souborů. Chvilku se nic nedělo, ale pak najednou počítač problikl, zhasl a zcela ztichnul. Jitka hned zkusila opětovný start, nic. „Asi se vybila baterie.“ Připojila tedy napájecí zdroj a stiskla znovu zapínací tlačítko. Stále bez odezvy. Počítač byl relativně nový, po chvilce zkoušení proto rezignovala a zavolala prodejci s popisem problému.

Notebook putoval do opravy a už za dva dny bylo jasno. Počítač byl na odpis a diagnóza? Jitce zničil počítač ten krásně barevný USB disk!

Co je USB killer?

Zdánlivý disk nebyl ve skutečnosti paměťové médium, ale tzv. USB killer - zařízení, které po připojení k počítači dokáže po několika sekundách vygenerovat tak silný elektrický výboj, že dokáže zničit obvody na základní desce počítače, případně i další jeho komponenty. Princip je poměrně jednoduchý, obvod s kondenzátory se postupně nabije z USB konektoru a po dosažení určité úrovně se veškerá energie v podobě vysokonapěťového pulzu vrátí přes datové piny do počítače. Účinek je bleskový a většinou fatální. Nezbývá než výměna všech poškozených komponent. Existuje i USB killer softwarový - na flashdisku je malware, který dokáže rychle smazat nebo nevratně poškodit datové struktury na pevném disku počítače.

Obrana před takovými hrozbami je jediná - USB disky neznámého původu nikdy ke svému počítači nepřipojovat.

2.7.2. Jak se bránit poškození mého digitálního zařízení?

- Nikdy ke svému počítači nepřipojuji USB disky či jiná paměťová média neznámého původu.
- Nepoužívám nabíječky či zdroje s poškozeným krytem nebo izolací.

- Používám ochranné kryty a pouzdra.
- Pokud nemám elektrické zásuvky s přepěťovou ochranou, při bouřce nebo delší nečinnosti odpojuji zařízení od elektrické sítě.
- Používám jen takové elektrické příslušenství, které má homologaci pro použití v naší rozvodné síti s napětím v zásuvce 230 V a kmitočtem 50 Hz. Příslušenství určené pro jiné země nemusí správně fungovat nebo jejich použití může být nebezpečné.
- Digitální techniku ukládám vždy na bezpečné místo, kde nehrozí poškození vodou, nárazem či vysokou teplotou. V případě rychlého přechodu ze zimy do tepla dochází v přístroji ke kondenzaci, která je nebezpečná pro elektrické obvody. Před spuštěním je vhodné nechat zařízení přizpůsobit teplotě okolního prostředí.
- Zařízení s baterií, které delší dobu nepoužívám, občas nechám dobít. Baterie se pomalým tempem sama vybíjí a při dosažení velmi nízké úrovně nabití se podstatně zvyšuje opotřebení baterie a možnost její poruchy.

2.8 Obecné zásady zajištění bezpečnosti systémů

Jak se bránit

V prvé řadě je potřeba ke všemu přistupovat rozumně a nespěchat. Není doporučeno ukládat uložená hesla, kódy, pin, názvy účtů v počítači. Před opuštěním počítače je žádoucí se odhlásit z jakýchkoliv aplikací a stránek. Instalací kvalitního antiviru se dá zamezit možným útokům zvenku, neboť je schopný zadržet příchozí viry a jiný škodlivý program. Při interakci s jinými lidmi je potřeba jednat ostražitě a využívat pouze důvěryhodné stránky. Neměly by se navštěvovat pochybné stránky, které mohou být nakaženy virem - tyto stránky se většinou dají poznat z uvedeného odkazu. Před návštěvou stránky je možno odkaz zadat například do google a zjistit o této stránce více informací.

2.8.1. Kategorie kybernetické bezpečnosti

Kybernetickou bezpečností je nutné se zabývat na několika úrovních:

a) **Personální bezpečnost** – Jedná se o všechny osoby, které se systémem pracují. Největší podíl na bezpečnostních nehodách mají právě lidé. Neznalost, nezaškolení, bezohlednost a neprovádění kontroly zaměstnanců může vést k chybám vzniklých v systému, proto je potřeba zvolit kvalifikované pracovníky.

b) **Fyzická bezpečnost** – Jde o ochranu všech fyzických věcí firmy. Může se jednat o vybavení jako jsou servery, počítače, suroviny, hotové výrobky, polotovary, nářadí, dokumenty, ale i lidi. Všechny tyto objekty se mohou stát obětí přírodních katastrof, požárů, nebo útoků lidí.

c) **Logická bezpečnost** – Firmy při své činnosti využívají různé typy software. Ať už jde o operační systémy, tak různé databáze, kancelářský software. Pro bezpečný chod firmy by měly být tyto software přístupné jen určitým zaměstnancům. Například správa sítě bude povolena technikovi, který se o tuto síť stará. Operační systém a kancelářský software bude přístupný například sekretářkám. Proto je potřeba zřídit přístup pro jednotlivé osoby.

d) **Komunikační bezpečnost** – Ochrana při přenášení informací přes síť. Můžeme se stát cílem odposlouchávání nebo přetížení.

e) **Organizační bezpečnost** – Bezpečnost se zřizuje pomocí stanovení odpovědnosti

osob a skupin v organizaci, nebo společenství. Zřizují se bezpečnostní standardy, Každý zaměstnanec má tím pádem své povinnosti a nezasahuje do práce ostatních.

2.8.2. Nastavení bezpečnosti uvnitř systémů

Z pohledu řešení bezpečnosti systémů pak můžeme použít např. následující rozdělení dle nastavení restrikcí pro uživatele:

a) **Promiskuitní** – Jde o systémy, které nemají žádné zákazy. V praxi se tenhle typ systému nedoporučuje.

b) **Paranoidní** – V systému je vše zakázáno. Používá se jen tam, kde nám nezbývá nic jiného, u věcí, které se těžce udržují.

c) **Přísný** – Povolení se udává na základě whitelistů (bílý list), kde jsou uvedeny výjimky, ke kterým můžeme přistupovat.

d) **Povolný** – Povolení se udává na základě blacklistů (černý list), kde jsou uvedeny výjimky, ke kterým přistupovat nemůžeme.

Měli bychom si být vědomi, že i přes všechna provedená zabezpečení vždy existuje riziko narušení. Žádný systém není stoprocentně dokonalý a může se stát terčem útoku.

3. Slovník

Kyberprostor

Virtuální počítačový svět, přesněji elektronické médium tvořící světovou, globální počítačovou síť, která je základem online komunikace. Je to rozsáhlá počítačová síť tvořena menšími, po světě rozesetými počítačovými sítěmi, které užívají TCP/IP protokol. Ten jim umožňuje komunikaci a výměnu dat.

Jedna z hlavních vlastností struktury kyberprostoru je otevřenost širokému okruhu uživatelů v interaktivní a virtuálním prostředí. Další vlastností je anonymita, ta umožňuje v podstatě jakékoliv jednání bez zodpovědnosti.

Kyberprostor umožňuje uživatelům komunikovat,sdílet a vyměňovat si informace a nápady, hrát hry, účastnit se diskuzí na sociálních fórech, provádět obchodní transakce, atd…virtuálním počítačovým světem v internetu tvořený daty a informacemi. Lidé zde mohou komunikovat např. pomocí emailu nebo nakupovat v internetových obchodech.

Kybernetická bezpečnost

Odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné jeho předpokládaným uživatelům. Jedná se o celý kyberprostor.

Počátky se objevily v 80. letech, kdy se s rozmachem výpočetní techniky začaly skladovat informace právě do výpočetních systémů. Jednalo se například o evidence plateb, informace o zákaznících, armádní tajemství.

Kybernetická kriminalita

Představuje trestnou činnost, která zahrnuje počítač nebo síťové zařízení. Patří zde i zločiny prováděné prostřednictvím internetu, jako podvody, krádež osobních údajů a identity nebo kreditní karty. Velké množství útoků je prováděno za účelem získání peněžních prostředků.

Kyberpodvody / zločiny

Jsou chápány jako trestná či škodlivá jednání, která spočívají v získávání informací nebo v manipulaci s nimi za účelem dosažení zisku a která jsou uskutečňována prostřednictvím síťových technologií.

Hacker

Jedná se obvykle o velice schopného programátora, který je odborníkem na úpravy počítačových systémů a sítí. Využívá své počítačové dovednosti k získání neoprávněného přístupu k cizím počítačům a sítím. Zajímá se především o citlivé informace, jako jsou hesla, údaje o platebních kartách nebo například soukromé fotografie. Jedná tak obvykle pro zábavu, zisk nebo ve snaze způsobit škodu.

Existují ovšem i “hodní” hackeři - Zejména velké firmy si najímají tyto specialisty, aby jim prověřili odolnost jejich systémů proti útokům a případným únikům dat.

E-mail (email)

Elektronická pošta je způsob výměny zpráv mezi uživateli, kteří využívají služeb tzv. e-mailových serverů. Ty každému majiteli e-mailové adresy nabízejí přijímání, přeposílání, doručování a ukládání zpráv. Dále posílání dat do určité velikosti, přes e-mail probíhá často také notifikace. Jedná se o nejdéle trvající online způsob komunikace.

Fake news (junk/pseudo news)

Falešné nevyžádané zprávy úmyslně dezinformující uživatele tradičních zpravodajských médií (noviny, TV a radio vysílání) nebo sociálních médií.

Firewall

V počítačových systémech je firewall síťový bezpečnostní systém, který sleduje a řídí příchozí i odchozí síťový provoz mezi dvěma sítěmi podle předem definovaných bezpečnostních pravidel.

Hoax

Nepravdivá zpráva nebo informace, která se tváří jako ověřený fakt. Obvykle jde o senzační zprávu, která se šíří internetem jako lavina. Uživatelé, kteří této informaci uvěří a jednají v souladu s ní, mohou být svým jednáním poškozeni.

HTTP, HTTPS

Hypertext Transfer Protocol je internetový protokol, pomocí kterého komunikuje prohlížeč s webovým serverem (www). HTTPS (security) je rozšíření protokolu HTTP, kdy se pro komunikaci používá šifrování, aby nebylo možné přenášená data odchytávat a zneužít.

Kyberšikana

Jakýkoliv projev chování, jehož záměrem je ublížit, ponížit, zastrašit nebo ohrozit druhého pomocí digitálních nástrojů (telefon, počítač,...). Například zneužití cizího účtu, natáčení citlivých videí a jejich zveřejnění na síti, vytvoření zesměšňující webové stránky, …

Login

Proces přihlášení k účtu v počítači, na web…

Phishing (fišing)

Podvodná technika využívaná na internetu k vylákání citlivých údajů (heslo, přihlašovací jméno, číslo platební karty,…). Obvykle formou oficiálně vypadajícího e-mailu nebo SMS. Mezi rozpoznávací znaky patří naléhavý tón, chyby v textu, podezřelá doména nebo neočekávanost zprávy.

Spam

Nevyžádané sdělení šířené internetem v podobě e-mailu, zprávy na sociální síti, článku na určitém webovém serveru.

4. Literatura a zdroje

- Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- 2020. Dostupné z: https://en.wikipedia.org/
- Wikipedie, otevřená encyklopedie [online]. [2020]. Dostupné z: https://cs.wikipedia.org/
- Hacker - kdo to je a jak před ním ochránit vaše PC. Avast.com [online]. [2020]. Dostupné z: https://www.avast.com/cs-cz/c-hacker
- What Are Cyber Threats and What to Do About Them. Preyproject.com [online]. [2020]. Dostupné z: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect--you-what-to-do-about-them/
- Top 10 Most Common Types of Cyber Attacks. Netwrix blog [online]. [2020]. Dostupné z: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
- Ukliknutí ‚stálo' nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy. Lidovky.cz [online]. [2020]. Dostupné z: https://www.lidovky.cz/domov/uklik-nuti-stalo-nemocnici-v-benesove-40-milionu-kyberutok-zacal-kliknutim-na-prilohu.A200115_201359_ln_domov_vlh
- Národní úřad pro kybernetickou a informační bezpečnost [online]. [2020]. Dostupné z: https://www.nukib.cz/
- Kyberkompas. Kyberkompas [online]. [2020]. Dostupné z: https://security.muni.cz/cyber-compass

Chyťme hackera

Program Chyťme hackera je mezigenerační vzdělávací program pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.

Obsah

Úvod

Digitální technologie a digitalizace patří k oblastem, které budou nejvíce ovlivňovat naši budoucnost. Díky výkonnému hardwaru a rychlým sítím stále narůstá nejen objem elektronické komunikace mezi lidmi, ale i elektronických finančních transakcí, obchodních aktivit, záznamů o zdravotní péči nebo úředních procesech. Možností zábavy či vzdělávání je na internetu rovněž celá řada.

Ruku v ruce s těmito pozitivy jsou ovšem spojena i určitá rizika, díky kterým může člověk přijít o své finance, o svá data i o svou pověst. Proto je třeba nezapomínat na ochranu svých zařízení, programů, financí, dat i soukromí.

Mezi nejčastější negativní a rizikové jevy na internetu patří různé druhy podvodů a krádeží, šikana, zneužívání lidí včetně dětí, vydírání a cílené útoky na počítačové systémy.

Záměr programu

Cílem programu Chyťme hackera je posílit povědomí žáků a studentů o kybernetických hrozbách na Internetu. Program chce ukázat, že tyto hrozby začínají být součástí našich životů a počty napadených se každoročně zvyšují. Pokud se nebude každý z nás umět bránit, může se stát, že terčem napadení budeme my a nastanou nám díky tomu výrazné problémy. Abychom však se však mohli účinně bránit, musíme s obrannými mechanismy být v dostatečné míře seznámeni.

Zároveň chce program poukázat na to, že kybernetické podvody jsou protizákonné. Oproti tomu chce vysvětlit, že dodržování zákonů a pravidel je ve standardní demokracii normální.

Cíle programu

- Zajímavou, atraktivní a interaktivní formou seznámit maximální počet žáků a studentů s problematikou kybernetických hrozeb
- Zvýšit povědomí o kybernetické bezpečnosti
- Seznámit žáky a studenty s nejčastějšími kybernetickými hrozbami.
- Seznámit je, jak se kybernetickým hrozbám bránit
- Seznamovat je s významem digitálních technologií
- Ukazovat možnosti využití digitálních technologií v běžném životě
- V maximální míře realizovat program Chyťme hackera za pomoci digitálních technologií
- Motivovat žáky a studenty k tomu, aby o jednotlivých hrozbách informovali své rodiče a prarodiče

Varianty programu

- Kooperativní hra
- Postupová soutěž družstev (třídní kolo, školní kolo …)

Materiál je zpracován jako kooperativní program, kde účastníci společně bojují proti hackerovi, který chce podniknout proti škole opakovaný kybernetický útok. Účastníci společně prochází pěti koly programu, ve kterých postupně získávají vědomosti a dovednosti, aby se dokázali ubránit kybernetickému útoku a v posledním kole napomoci k tomu, aby byl podvodník odsouzen.

Obsah programu Chyťme hackera

Tento program přibližuje dospívající populaci problematiku kybernetických hrozeb poutavou a kooperativní formou. Ukazuje na problém zvyšujících se kybernetických útoků. Tím u nich rozvíjí povědomí o této problematice.

Program je kombinací hry a prožitku, týkajícího se kybernetických hrozeb. Účastníci se na začátku dozvídají o možnosti kybernetického útoku, který se týká přímo jich. Společně pak pátrají po útočníkovi (hackerovi), procházejí řadou úkolů, kde se seznamují s danou problematikou, aby na konci usvědčili hackera z trestného činu. Program chce ukázat účastníkům nástrahy kybernetického prostředí a také jak se jim účelně bránit Nebude to však dělat instruktivní formou, ale tak, aby na to účastníci přišli sami.

Hlavní hrozby při pohybu v internetu a jejich možné následky

Zcizení, případně i zveřejnění vašich uživatelských hesel

Prolomení bezpečnosti uživatelského účtu nabízí možnost převzetí kontroly nad službou. Ten kdo zná vaše heslo, může službu používat vašim jménem stejně jako vy. Například může sledovat filmy, za které jste zaplatili.

Někdy ovšem útočník nejde po penězích, ale může velmi snadno váš účet použít k tomu, aby vás veřejně zesměšnil, zostudil či vám způsobil jiné problémy. Třeba tak, že vašim jménem publikuje na internetu choulostivé fotografie nebo bude neslušně vystupovat v nějaké diskuzi.

Hesla lze zcizit různými způsoby, ty nejčastější jsou dva: Buď útočník pronikne do databáze poskytovatele služby, odkud si všechna hesla naráz zkopíruje, nebo je sbírá po jednom přímo od uživatelů. Vhodnou technikou je tzv. phishing, kdy nic netušící uživatel zadává heslo do podvrženého formuláře, který vypadá jako jeho oblíbená stránka pro email, bankovnictví, atd.

Sledování aktivit, které děláte na internetu

Obvykle sledování probíhá za pomoci záškodníkem instalovaného software. Takový program bez vašeho vědomí odesílá data o tom, co právě na počítači nebo telefonu děláte. Tato data lze poté využít k vydírání, zasílání nevyžádané reklamy, v některých případech je lze i dobře prodat někomu dalšímu.

Zcizení financí z vašeho bankovní účtu

Moderní elektronické bankovnictví je obvykle zabezpečeno nejméně dvěma nezávislými kanály (např. po zadání hesla musíte ještě použít autorizaci přes SMS nebo nějakým biometrickým údajem). To však neznamená, že si s takovým zabezpečením útočník neporadí. Časté jsou například falešné platební příkazy, které se tváří jako platba za vaše pojištění nebo telekomunikační služby. Faktura vypadá úplně stejně jako ta, na kterou jste zvyklí, avšak číslo účtu patří útočníkovi.

Jiný útok na vaše finance může vypadat tak, že se vám přes sociální síť ozve kamarád, že by potřeboval přeposlat nějakou zprávu z vašeho telefonu. Ve skutečnosti se však jedná o útočníka skrytého pod falešnou identitou a v přeposílané zprávě je autorizační kód pro převod financí z vašeho účtu.

Podvodné vylákání finančních prostředků

Oblíbeným trikem podvodníků byly v minulosti dopisy, které vám s radostí oznamovaly, že jste zdědili velké peníze někde daleko v Africe. Abyste se k dědictví dostali, stačí zaplatit drobný poplatek notáři na určený účet. Že je notář vymyšlený a číslo účtu patří útočníkovi, dnes již pravděpodobně většina uživatelů dokáže odhalit. Jsou však mnohem rafinovanější postupy. Pokud se útočník naboural do účtu některého z vašich přátel, může vás velmi snadno jeho jménem požádat o nějakou finanční výpomoc. Pokud si žádost neověříte (nejlépe osobně), buďte si jisti, že své peníze už nejspíš nikdy neuvidíte.

Zneužití vašeho počítače záškodníkem

Pokud útočník získá kontrolu nad vaším počítačem nebo telefonem, vůbec o tom nemusíte vědět. Přitom z vašeho počítače mohou odcházet nevyžádané emaily na stovky dalších adres nebo se na vašem disku může nacházet nelegálně vytvořený a sdílený obsah jako jsou autorsky chráněná díla nebo dětská pornografie.

Případně lze váš počítač využít jako součást velké sítě tzv. „botů“ k cílenému útoku na další systémy. Takové útoky většinou cílí na odstavení určité služby nebo celého serveru. Jsou prováděny tak, že velké množství botů pošle v jeden okamžik stejný požadavek na službu a ta nápor nevydrží. V lepším případě přestane reagovat, v tom horším se zcela zhroutí.

Vydírání

V takových případech vás obvykle útočník tlačí do kouta tím, že zná nějaké vaše choulostivé údaje nebo dokonce má kontrolu nad vašimi daty. Často takový útok probíhá prostřednictvím ransomware, což je speciální typ počítačového viru, který vaše data zašifruje tak, že je umí rozklíčovat pouze útočník. Ten pochopitelně požaduje výkupné. Není ale vůbec neobvyklé, že po zaplacení výkupného data obnovena nejsou a vy zůstanete bez peněz i bez dat.

Obsah programu Chyťme hackera

1. kolo: Digitální svět

První kolo je zaměřeno na digitální technologie jako takové. Cílem je ukázat důležitost digitálních technologií a jejich význam pro každodenní život. Vysvětlit, že význam digitálních technologií bude neustále růst a bude pronikat do dalších oblastí lidského konání.

Princip:

Je připraveno 10 popisů různých technologických novinek (trendů). Družstva mají za úkol rozhodnout, zda novinka již existuje nebo ne.

Příklady:

Lidé si zvykli na placení kartou, i když pro řadu z nich se jedná už o přežitou záležitost, protože platí chytrým mobilem. Někteří dokonce hodinkami nebo náramkem. Jsou tací, kteří platí čipem, který mají zabudovaný pod kůží. A teď naše otázka: Je možné platit očima? Přijdete do obchodu, kouknete do platebního terminálu a je zaplaceno?

Ano - *V současné době je ve světě možné platit pouhým pohledem do skeneru oční čočky*

Teď se půjdeme podívat na hřbitovy. Na některých už jsou k vidění digitální náhrobky, kde je stačí naskenovat kód do mobilu, a můžete si listovat profilem zemřelého. Tím to ale nekončí, někde jsou už k mání digitální hřbitovy, kam nemusíte vůbec fyzicky chodit. Stačí si v pohodlí domova pustit počítač a navštívit virtuální hrob nebožtíka, kde jsou informace o zemřelém, jeho fotografie a videa. Některé virtuální hřbitovy dokonce nabízí, vedle koho (slavného) může nebožtík spočinout.

Existují virtuální hřbitovy? **Ne.**

2. kolo: Pasti, pasti pastičky

Druhé kolo rozvíjí dovednosti účastníků ve skládaní šestiúhelníků s využitím prostorové představivosti. Cílem je vysvětlit účastníkům, že v souvislosti s rozvojem digitálních technologií bude neustále růst nutnost umět se bránit tzv. kybernetickým útokům. Seznámit účastníky s důležitostí antivirových programů pro bezpečnost našich digitálních zařízení.

Princip:

Účastníci dostanou přístup do on-line hry Hexeto. Úkolem účastníků bude klást do počítače pasti na kybernetické podvodníky. Pasti jsou šestiúhleníky se šesti barvami, které budou účastníci skládat do jednoho kompletního celku. A to ale tak, aby se k sobě složilo co nejvíce barevných stran. Čím více barevných stran k sobě složí, tím více zamezí útokům podvodníků a také – tím více bodů dostanou.

3. kolo: Hackerova zbraň

Třetí kolo ukazuje důležitost informací při ochraně před kybernetickými útoky. Příkladem může být stažení neznámého programu do počítače nebo mobilu bez zjištění (např. pomocí recenzí), zda stažení programu nemůže nějakým způsobem ohrozit můj PC nebo mobil.

Princip:

Po místnosti (budově) je umístěno 10 QR kódů. Na základě těchto indicií budou družstva hledat název hackerovy zbraně.

Příklad:

- Počítač
- Covid
- Fred
- Film Hostitel
- Lebka v počítači
- TV program
- Vyděšený obličej
- Teploměr
- Zpěvák Cohen
- Kopie

4. kolo: Kybernetické hrozby

Cílem je seznámit účastníky s možnými kybernetickými hrozbami, které se jich mohou týkat. Zároveň je seznámit s cíli kybernetických útoků (vylákání finančních prostředků, zcizení identity, vydávání se za jinou osobu, zablokování počítače, zneužití emailových účtů…).

Družstva, vytvořená v předchozím kole, pokračují ve stejném složení i v tomto kole. Je připraveno 10 různých kybernetických hrozeb. Jednotlivá družstva si losem vyberou jednu kybernetickou hrozbu. Jeho úkolem je napsat 5 možností, jak se této hrozbě bránit.

Příklad:

S klukama dnes ve škole nic moc nebylo. Seděli o přestávkách v lavicích, v ruce mobily a pařili nějakou novou hru. Karel nahlédl přes rameno jednoho z nich a hra se mu hned zalíbila. Dal si její název do vyhledávače a z první možné nabídky si ni stáhl. Doma jí hrál snad celý večer. Byla to pecka.

V dalších dnech se jeho mobil začal chovat velmi podivně. Výrazně se zpomal a to tak, že v něm nemohl hrát žádnou ze svých oblíbených her, ani se učit. Navíc mu tam každou minutu naskakovalo plno reklam a to i s velmi nevhodným obsahem. Nešlo se jich zbavit. Karel nedělal prakticky nic jiného, než kliknutím ukončoval reklamy.

Svěřil se svým problémem klukům a dozvěděl se, že si stáhl do svého mobilu počítačový virus, protože si hru stáhnul z neoficiálního obchodu. Odinstaloval hru, ale problémy nepřestaly. Co dělat?

Viry jsou škodlivé kódy šířené jejich tvůrci s různými cíli. Existuje velká řada virů, účelem některých z nich je ničit, jiné naopak mají za úkol usadit se v co největším počtu počítačových systémů a tyto pak využijí k cílenému útoku. Různé viry se mohou projevovat různě, např. od náhodného přehrávání určité melodie, přes zahlcení systému, úpravu nebo zničení dat, až po celkovou destrukci napadeného systému. Odhaduje se, že každý zhruba 300. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.

Virus obsažený v souborech či programech při spuštění nebo samovolně po nějaké době začne páchat škodu. Může například extrémně zpomalit počítač, nebo v horším případě smazat data na disku či způsobit vyhoření hardware. Virem mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento virus.

5. kolo: Zákon a trest

Cílem je posilovat právní povědomí dětí a mládeže a vysvětlovat, že porušování zákonů a pravidel není ve standardní demokracii normální. To se týká i kybernetických podvodů.

Princip:

Organizátor rozdá družstvům přístup do on-line hry Klikačka, kde bude připraveno 10 otázek z oblasti zákonů se čtyřmi odpověďmi A-B-C-D. Družstva postupně odpovídají na otázky tak, že vybírají správnou odpověď.

Pokud neví, mohou otázku přeskočit. Na každou odpověď si mohou vsadit 0 – 4 body. Pokud odpoví správně, získají tolik bodů, kolik vsadili. Odpoví-li špatně, ztrácí tolik bodů, kolik vsadili, a pokračují další otázkou.

Příklad:

Marek se chtěl vyhnout zkoušení z fyziky, a tak zatelefonoval řediteli školy a oznámil, že je ve škole ukryta bomba. Z legrace pak ještě telefonoval na nádraží a městský úřad a také oznámil hrozící bombový útok. Policie jej vypátrala a zjistila, že ještě nedovršil 15 let. Bude mít pro Marka nějaké následky, že spáchal čin jinak trestný?

a) Ano, soud pro mládež může učinit opatření potřebná k jeho nápravě.

b) Ne, ještě není trestně odpovědný.

c) Ano, bude odejmut rodičům a ti budou odsouzeni za zanedbání výchovy s trestní sazbou skutku spáchaného Markem.

d) Ne, pouze bude pokárán policií.

Trestní zákon spojuje trestní odpovědnost člověka až s dovršením věku 15 let. Dopustí-li se dítě mladší než patnáct let činu jinak trestného, může soud pro mládež učinit “opatření” potřebná k jeho nápravě, kterými jsou dohled probačního úředníka, zařazení do vhodného výchovného programu a ochranná výchova dle §§ 89 a 93 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, v platném znění.

Jiří získal pomocí internetu předpremiérový titul nového dosud neuvedeného filmu. Tento film dále kopíruje a pro své kamarády a známé. Jedná se o protiprávní skutek?

a) Ano, protože titul byl získán nelegální cestou a šíří jej dále.

b) Ano, protože není povoleno z internetu cokoli kopírovat.

c) Ne, protože za kopie filmu nepožaduje peníze.

d) Ne, protože nepořádá domácí projekci.

Filmy patří mezi díla chráněná autorským zákonem. Za porušení těchto práv se zakládá občanskoprávní i trestněprávní odpovědnost. V občanskoprávním řízení mu může být uloženo, aby se protiprávního jednání zdržel, závadný stav napravil a vydal bezdůvodné obohacení, a to podle § 40 odst. 3 aut. zák. a poskytnul přiměřené zadostiučinění, a to i finanční. Podle závažnosti a rozsahu porušení autorských práv se dopouští přestupku nebo může jít až o trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 268 trestního zákona.

Chyťme hackera

Metodika pro lektory

Metodika pro lektory mezigeneračního vzdělávacího programu pro oblast bezpečnosti a rizik spojených s používáním digitálních technologií a využíváním online příležitostí určený pro presenční použití ve školách, volnočasových institucích apod.

Obsah

Záměr programu

Cílem programu Chyťme hackera je posílit povědomí žáků a studentů o kybernetických hrozbách na Internetu. Program chce ukázat, že tyto hrozby začínají být součástí našich životů a počty napadených se každoročně zvyšují. Pokud se nebude každý z nás umět bránit, může se stát, že terčem napadení budeme my a nastanou nám díky tomu výrazné problémy. Abychom však se však mohli účinně bránit, musíme s obrannými mechanismy být v dostatečné míře seznámeni.

Zároveň chce program poukázat na to, že kybernetické podvody jsou protizákonné. Oproti tomu chce vysvětlit, že dodržování zákonů a pravidel je ve standardní demokracii normální.

Cíle programu

- Zajímavou, atraktivní a interaktivní formou seznámit maximální počet žáků a studentů s problematikou kybernetických hrozeb
- Zvýšit povědomí o kybernetické bezpečnosti
- Seznámit žáky a studenty s nejčastějšími kybernetickými hrozbami
- Seznámit je, jak se kybernetickým hrozbám bránit
- Seznamovat je s významem digitálních technologií
- Ukazovat možnosti využití digitálních technologií v běžném životě
- V maximální míře realizovat program Digitální svět za pomoci digitálních technologií
- Motivovat žáky a studenty k tomu, aby o jednotlivých hrozbách informovali své rodiče a prarodiče

Obsah programu Chyťme hackera

Tento program přibližuje dospívající populaci problematiku kybernetických hrozeb poutavou a kooperativní formou. Ukazuje na problém stále častějších kybernetických útoků a dalších kybernetických hrozeb. Tím u nich rozvíjí povědomí o této problematice.

Program je kombinací hry a prožitku, týkajícího se kybernetických hrozeb. Účastníci se na začátku dozvídají o možnosti kybernetického útoku, který se týká přímo jich. Společně pak pátrají po útočníkovi (hackerovi), procházejí řadou úkolů, kde se seznamují s danou problematikou, aby na konci usvědčili hackera z trestného činu. Program chce ukázat účastníkům nástrahy kybernetického prostředí a také jak se jim účelně bránit Nebude to však dělat instruktivní formou, ale tak, aby na to účastníci přišli sami.

1. kolo: Digitální svět

Ukázat důležitost digitálních technologií a jejich význam pro každodenní život. Vysvětlit, že význam digitálních technologií bude neustále růst a bude pronikat do dalších oblastí lidského konání.

Prokázání vědomosti z digitálního světa pro boj s hackerem.

Vědomostní část, rozhodování, spolupráce

2. kolo: Pasti, pasti, pastičky

Vysvětlit možnosti ochrany proti kybernetickým hrozbám. Seznámit účastníky s důležitostí antivirů pro bezpečnost našich digitálních zařízení.

Kladení pastí hackerovi.

Prostorová představivost, rozvoj dovednosti, rychlost, taktika.

3. kolo: Hackerova zbraň

Zapojit všechny členy družstva do vzájemné spolupráce. Rozvoj týmového ducha – na boj s kybernetickými zločinci se podílí řada institucí a musí být mezi nimi souhra a spolupráce.

Na základě indicií účastníci pátrají po zbrani, kterou proti nim hacker použije.

Rozhodování týmu, spolupráce, rychlost, taktika

4. kolo: Kybernetické hrozby

Seznámit s možnými kybernetickými hrozbami, které se mohou účastníků týkat. Hledání obrany proti nim. Účastníci ví, jakou hrozbu hacker použije. Nyní hledají proti ní účinnou ochranu.

Prezentace, přesvědčování a obhajování vlastních názorů.

5. kolo: Zákon a trest

Zvýšení povědomí o tom, že dopouštět se porušování zákonů a pravidel není normální.

Prokázání vědomosti z oblasti zákonů ČR.

Hacker porušil zákony ČR a bude odsouzen.

Vědomostní část, rozhodování, spolupráce

Průběh programu

Úvodem

Na začátku organizátor sdělí, že vedení instituce (školy), ve které program probíhá, byla napadena hackerským útokem.

Škola dostala e-mail ze svého e-mailového účtu. Hacker tvrdí, že se naboural do informačního systému školy. Ta obdržela od hackera tento e-mail:

„Nazdárek! Všimli jste si, že jsem vám tento email poslal z vašeho účtu? Přesně tak, znamená to, že mám plný přístup k vašemu informačnímu systému, ovládám vaši wifi, všechny počítače, notebooky, tablety a mobily ve škole. Sleduji vás už několik posledních měsíců. Chcete vědět, jak? No, z vaší nezabezpečené webové stránky, kterou jsem infikoval malwarem. Teď můžu po aktivování kamery a mikrofonu prostřednictvím monitoru sledovat kdykoliv a kohokoliv ve škole a nikdo si toho nevšimne. A stejně tak jsem získal i přístup k seznamu kontaktů a veškeré korespondenci, fotkám, videím u všech ve škole. Můj malware využívá ovladače, ve kterých každé čtyři hodiny aktualizuji podpisy, takže je naprosto nezjistitelný a antiviry ve vašich zařízeních o něm vůbec neví. Teď zpracovávám fotky a videa ze všech mobilních telefonů, která se nikdy neměla dostat na světlo světa.

A chcete vědět, co všechno s ním můžu udělat? Jediným kliknutím myši je můžu rozeslat na všechny stránky sociálních sítí všech lidí ze školy a také jejich emailovým kontaktům. Zároveň zveřejním veškeré informace o všech žácích ve škole i všechny jejich hesla k sociálním sítím a nejen k nim. Tím se dopustíte trestného činu, za který budete odsouzeni, protože to uděláte VY.

Pokud tomu chcete zabránit, stačí na moji bitcoinovou adresu převést částku 4000 EURO (pokud nemáte ponětí, jak to udělat, zadejte do svého prohlížeče snadný dotaz: “Koupit bitcoiny”). Moje bitcoinová adresa (BTC Wallet) je: 1778RYiKxW5kCFLH7BPbKEJ2zce83adFf2 Ihned po potvrzení platby vše, co jsem postahovat, smažu a je hotovo. Nikdy víc už o mně neuslyšíte. Na dokončení transakce máte 2 dny (48 hodin). Po otevření tohoto emailu, mi dojde oznámení a časový odpočet začne tikat. Jakýkoliv pokus o podání stížnosti je zbytečný, protože tento email, stejně jako moji bitcoinovou adresu, nelze zpětně vysledovat. Na svém systému pracuju 10 let a chybám nedávám sebemenší prostor.

48 hodin začalo běžet!!!!

Poznámka: Možností je poslat účastníkům tento e-mail, aby program byl ještě reálnější.

Vedení školy za pomoci pedagogického sboru a dalších odborníků zjistilo, že škola byla napadena kybernetickým útokem, což je jinými slovy pokus o podvod. Ke kybernetickému útoku byl využit nástroj, který se jmenuje SCAREWARE. Kyberzločinci / hackeři obětem vnutí, že jejich počítače nebo chytré telefony byly nakaženy, aby je přesvědčili k zakoupení falešné aplikace nebo zaplacení určité částky. Při typickém napadení SCAREWARE se vám může při procházení webu zobrazit výstražná zpráva s varováním, že váš počítač je infi-

kován nebo že se v něm vyskytl virus. Scareware však nemusí mít nutně jen softwarovou podobu. K vyvolání strachu a paniky uživatele často stačí (tak jako v případě naší školy) vhodně formulovaný e-mail s více či méně věrohodnou informací, že počítač uživatele byl napaden. Útočník ve zprávě vyhrožuje např. zveřejněním kompromitujících či jinak citlivých informací o uživateli atp.

Řešení

Tento e-mail byl na první pohled nevěrohodný. Vedení školy se rozhodlo s podvodníkem nekomunikovat a celý případ předat policii ČR.

Blíží se další kybernetický útok

Dle názoru přizvaných odborníků dojde v brzké době další kybernetický útok, pravděpodobně s větší účinností, který se dotkne všech žáků a studentů ve škole.

Vedení školy požaduje pomoc všech tříd. Máme dvě hodiny na to, abychom vypátrali, jakou kybernetickou hrozbu chce použít, hackera porazili a dokázali mu, že porušuje zákony ČR.

Hacker je ve filmech kladný týpek, který se dokáže dostat k zásadním informacím vlády, které vedou k dopadení zločince, který chce zničit celou naší planetu. V reálném životě je pravda to, že se jedná velice schopného programátora, který je odborníkem na manipulace nebo úpravy počítačových systémů a sítí. Nehoní zločince, ale zločincem je sám, kdy využívá své počítačové dovednosti k získání neoprávněného přístupu k cizím počítačům a sítím. Zajímá se především o citlivé informace, jako jsou hesla, údaje o platebních kartách nebo soukromé fotografie. Jedná tak pro zábavu, zisk nebo ve snaze způsobit škodu.

Jak na to půjdeme

Čeká nás pět úkolů, abychom společně chytli hackera, aby nemohl provést další útok. V prvním a ve druhém kole budeme muset získat dohromady 10 klíčů, které nás ve 3. kole přivedou k 10 indiciím, na základě kterých se dozvíme, jakou zbraň proti nám hacker při svém útoku chce použít. Ve čtvrtém kole budeme klást hackerovi pasti. Doufejme, že na ně skočí. V pátém kole mu dokážeme že porušil zákony ČR.

Pojďme a chyťme hackera!

Doba trvání: Program se dá stihnout za 2 hodiny.

Lepší varianta je rozdělit program do více lekcí a zařadit do běžné výuky. Program lze doplnit o úkoly mezi lekcemi, například mohou trénovat on-line hry. Příkladem může být postupné zařazování jednotlivých kol do hodin.

Nejde o soutěž, protože jde o nás všechny, všech se to může týkat. Jde o spolupráci a společný cíl.

---

1. kolo: Digitální svět

Legenda

Abychom společně mohli porazit hackera, musíme se trochu vyznat v digitálních technologiích a vědět, jaké jsou noviny a kam se v tomto směru ubírá svět.

Cíl

První kolo je zaměřeno na digitální technologie jako takové. Cílem je ukázat důležitost digitálních technologií a jejich význam pro každodenní život. Vysvětlit, že význam digitálních technologií bude neustále růst a bude pronikat do dalších oblastí lidského konání.

Doporučujeme pročíst tytu články k tématu na PortálDigi.cz: https://portaldigi.cz/?s=trendy

Princip prvního kola

Je připraveno 10 popisů různých technologických novinek (trendů). Družstva mají za úkol rozhodnout, zda novinka již existuje nebo ne.

Příklady

Lidé si zvykli na placení kartou, i když pro řadu z nich se jedná už o přežitou záležitost, protože platí chytrým mobilem. Někteří dokonce hodinkami nebo náramkem. Jsou tací, kteří platí čipem, který mají zabudovaný pod kůží. A teď naše otázka: Je možné platit očima? Přijdete do obchodu, kouknete do platebního terminálu a je zaplaceno?

Ano - V současné době je ve světě možné platit pouhým pohledem do skeneru oční čočky

Teď se půjdeme podívat na hřbitovy. Na některých už jsou k vidění digitální náhrobky, kde jen stačí naskenovat kód do mobilu, a můžete si listovat profilem zemřelého. Tím to ale nekončí, někde jsou už k mání digitální hřbitovy, kam nemusíte vůbec fyzicky chodit. Stačí si v pohodlí domova pustit počítač a navštívit virtuální hrob nebožtíka, kde jsou informace o zemřelém, jeho fotografie a videa. Některé virtuální hřbitovy dokonce nabízí, vedle koho (slavného) může nebožtík spočinout.

Existují virtuální hřbitovy? Ano

Hodnocení

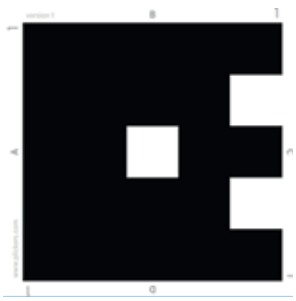
Každý účastník odpovídá sám za sebe, ale zároveň přispívá k úspěšnosti všech zúčastněných. Cílem je, aby v pěti otázkách odpověděla většina účastníků správně, tj. více než 50% účastníků. Pokud neodpovědí účastníci většinově na nějakou otázku správně, dostanou další otázku, maximálně však 10. Za každou správně zodpovězenou otázku dostanou ve 3. kole jednu informaci, která povede ke zjištění jaký nástroj (zbraň) chce hacker použít.

Hodnotící kritéria

Hodnotí se správnost odpovědi v časovém limitu

Způsob hodnocení

Každý účastník dostane papírovou kartu s QR kódem, která vhodným otočením vyjadřuje odpověď Ano nebo Ne. Organizátor přečte otázku a promítne ji na plátno. Účastníci mají 15 sekund na odpověď. Na dané znamení zvednou kartičku a porotce chytrým mobilem naskenuje všechny kartičky najednou a má okamžité výsledky.



Doporučená digitální aplikace: Plickers

Aplikace Plickers je velmi jednoduchá z hlediska správy i obsluhy. Nejprve si v internetové aplikaci organizátor programu připraví otázky a mobilem naskenuje odpovědí z karet a má okamžitě výsledky.

Odkaz: https://www.plickers.com

Délka soutěžního kola: 10 – 15 minut

Pomůcky

- 10 otázek přípravených v aplikaci Plickers
- Počítač s otázkami, dataprojektor, plátno
- Chytrý telefon s aplikací Plickers
- Počítač, tablet pro každého účastníka
- Hlasovací karty s QR kódy
- 5 obrázků klíčů

Maximální počet získaných klíčů: **5**

---

2. kolo: Pasti, pasti pastičky

Legenda

Prvních pět klíčů máme z prvního kola, kde jsme osvědčili naší orientaci v novinkách digitálních technologiích. Druhé kolo bude zaměřeno na dovednosti. Budeme klást pasti na kyberenetické podvodníky. Samozřejmě, že vše proběhne formou hry.

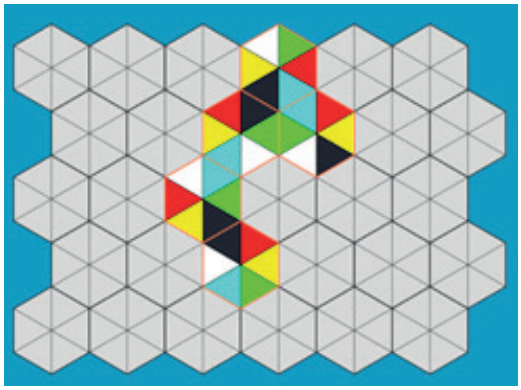
Cíl

Druhé kolo rozvíjí dovednosti účastníků ve skládaní šestiúhelníků s využitím prostorové představivosti. Cílem je vysvětlit účastníkům, že v souvislosti s rozvojem digitálních technologií bude neustále růst nutnost umět se bránit kybernetickým hrozbám. Seznámit účastníky s důležitostí antivirových programů pro bezpečnost našich digitálních zařízení.

Doporučujeme články k antivirům: https://www.antivirovecentrum.cz/antiviry.aspx

Princip druhého kola

Organizátor rozdá účastníkům přístup do on-line hry Hexeto. Úkolem účastníků bude klást do počítače pasti na kybernetické podvodníky. Pasti jsou šestiúhleníky se šesti barvami, které budou účastníci skládat do jednoho kompletního celku. A to ale tak, aby se k sobě složilo co nejvíce barevných stran. Čím více barevných stran k sobě složí, tím více zamezí útokům podvodníků a také – tím více bodů dostanou.



Hodnocení

Každý účastník hraje sám za sebe, ale zároveň přispívá k úspěšnosti všech zúčastněných. Cílem je v pěti minutách získat celkem 3,5 bodu. Druhým cílem je, aby 3,5 bodu a více získalo alespoň 50% účastníků. Pokud to bude jen 10%, získají účastníci jen jeden klíč, který povede v dalším kole k nalezení zbraně hackera. Za každé dalších 10% to bude vždy jeden klíč navíc (20% = 2 klíče, 3 = 3, 4 = 4, 5 = 5). Maximálně mohou získat v tomto kole 5 klíčů. Dohromady za první dvě kola 10 klíčů.

Hodnotící kritéria

Hodnotí se počet získaných bodů v časovém limitu

Bodování

Správně přiložená barva: + 0,2 body

Nesprávně přiložená barva: - 0,1 bodu

Doporučená on-line hra: Hexeto

HEXETO je skládačka složená z pravidelných šestiúhelníků. Do této skládačky se vkládají barvami k sobě jednotlivé šetiúhelníky rozdělené třemi úhlopříčkami na šest dílků.

Odkaz: https://www.projektrubikon.cz/rol/hexetonazkousku.html

Délka soutěžního kola: 5 minut

Pomůcky

- On-line hra Hexeto
- Počítač, tablet pro každého účastníka
- 5 obrázků klíčů

---

3. kolo: Hackerova zbraň

Legenda

V předchozích kolech získali účastníci 10 klíčů (možná i méně). Každý klíč je cesta k jedné indicii, podle které je možné identifikovat hackerovu zbraň. Pokud hráči najdou hackerovu zbraň, je jednodušší najít možnosti, jak se jeho útoku bránit. V našem případě účastníci dostávají pro další kolo sadu nápověd.

Boj s kybernetickými podvodníky je týmová práce, na které se podílí mnoho složek. Záměrem je zapojit všechny účastníky do vzájemné spolupráce. Z tohoto důvodu jsou účastníci tentokráte rozděleni do družstev, například pomocí aplikace Flipiti.

Cíl

Ukázat důležitost informací při ochraně před kybernetickými hrozbami. Příkladem může být stažení neznámého programu do počítače nebo mobilu bez zjištění (např. pomocí recenzí), zda stažení programu nemůže nějakým způsobem ohrozit můj PC nebo mobil.

Doporučujeme pročíst přílohu B.

Princip třetího kola

Po místnosti (budově) je umístěno 15 QR kódů. Indicie budou na tolika QR kódech, kolik získali účastníci v předchozích kolech klíčů, maximálně 10 podle toho, kolik získají účastníci indicií. Dalších 5 budou tzv. zdržovačky (Hackerův škleb), které není nutné zařazovat. Na základě těchto indicií budou družstva hledat název hackerovy zbraně.

Příklad

- Počítač
- Covid
- Fred
- Film Hostitel
- Lebka v počítači
- TV program
- Vyděšený obličej
- Teploměr
- Zpěvák Cohen
- Kopie

Průběh

Organizátor rozdělí účastníky do družstev cca po 5 účastnících, například pomocí programu Flippity. Družstva hledají QR kódy a pomocí foťáku v mobilu nebo aplikace QR scanner je naskenují. V mobilu se jim objeví indicie, ze kterých budou skládat název nástroje, který chce hacker použít k útoku. Až si budou jistí správnou odpovědí, napíšou ji na papír a odevzdají organizátorovi. Pokud neodpoví dobře, dostanou sankci 3 minuty a mohou pokračovat dále.

Druhou možností je, že družstva se musí domluvit na jednom výsledku a ten odevzdat. V tomto případě družstva 10 minut hledají výsledek a 5 minut se na něm domlouvají.

Hodnocení

Odpoví-li minimálně 50% družstev správně a je dodržen časový limit (počet družstev x 15 minut) získávají účastníci sadu nápověd pro další kolo.

Hodnotící kritéria

Hodnotí se správnost odpovědi v časovém limitu

Doporučená digitální aplikace: Flippity

Aplikace Flippity umožňuje snadnou tvorbu interaktivních online cvičení, která lze využít jak ve výuce, tak v tomto programu. Zároveň je možné pomocí jednoho kliknutí účastníky rozdělit do skupin nebo družstev. Jen je nutné je do Flippity předtím zadat.

Doporučená digitální aplikace: QR Scanner

QR Scanner je skener pro čtení QR / čárových kódů. Účastníci namíří mobilem na QR kód, který chtějí oskenovat, aplikace jej oskenuje a zobrazí, co se pod QR kódem skrývá.

Odkaz: https://play.google.com/store/apps/details?id=com.gamma.scan&hl=cs&gl=US

Délka soutěžního kola: 15 minut

Pomůcky

- Alespoň jeden chytrý mobilní telefon do každého družstva
- Karty s QR kódy
- Program Flippity na rozdělení do družstev
- Aplikace QR scanner pro hledání indicií
- Papíry a tužky na poznámky

---

4. kolo: Kybernetické hrozby

Legenda

V předchozím kole pátrali účastníci po zbrani, kterou chce podvodník proti škole použít. Pokud ji uhádli, pak dostávají v tomto kole sadu nápovědu, které jim ulehčí práci v hledání obrany proti hackerskému útoku.

Cíl

Seznámit účastníky s možnými kybernetickými hrozbami, které se jich mohou týkat. Zároveň je seznámit s cíli kybernetických útoků (vylákání finančních prostředků, zcizení identity, vydávání se za jinou osobu, zablokování počítače, zneužití emailových účtů…).

Doporučujeme pročíst přílohu B, část kybernetické hrozby.

Princip čtvrtého kola

Družstva, vytvořená v předchozím kole, pokračují ve stejném složení i v tomto kole. Je připraveno 10 různých kybernetických hrozeb. Jednotlivá družstva si losem vyberou jednu kybernetickou hrozbu. Jeho úkolem je napsat 5 možností, jak se této hrozbě bránit.

Průběh

Každé družstvo si vylosuje jinou kybernetickou hrozbu, to znamená text s popisem hrozby a tím, jak se hrozba projevuje). Pokud v předchozím kole účastníci identifikovali hackerovu zbraň, dostávají seznam možných řešení, které jim mohou napomoci v hledání správného řešení. Pak mají 10 minut na vymyšlení, nebo výběr řešení obrany proti této hrozbě.

Po 10 minutách bude prezentovat své návrhy ostatním. Pokud budou tři návrhy správné, jsou úspěšní. Poté organizátor shrne všechny možnost ochrany proti této hrozbě.

Seznam kybernetických hrozeb:

1. Počítačové viry
2. Poškození nebo zničení hardware
3. Phishing
4. Podvodné nákupy na internetu
5. Podvody při prodeji zboží
6. Vydírání
7. Krádež uživatelského účtu

8. Spam
9. Hoax
10. Zneužití osobních dat

Příklad: Počítačové viry

S klukama dnes ve škole nic moc nebylo. Seděli o přestávkách v lavicích, v ruce mobily a pařili nějakou novou hru. Karel nahlédl přes rameno jednoho z nich a hra se mu hned zalíbila. Dal si její název do vyhledávače a z první možné nabídky si ji stáhl. Doma hrál snad celý večer. Byla to pecka.

V dalších dnech se jeho mobil začal chovat velmi podivně. Výrazně se zpomal a to tak, že v něm nemohl hrát žádnou ze svých oblíbených her, ani se učit. Navíc mu tam každou minutu naskakovalo plno reklam a to i s velmi nevhodným obsahem. Nešlo se jich zbavit. Karel nedělal prakticky nic jiného, než kliknutím ukončoval reklamy.

Svěřil se svým problémem klukům a dozvěděl se, že si stáhl do svého mobilu počítačový virus, protože si hru stáhnul z neoficiálního obchodu. Odinstaloval hru, ale problémy nepřestaly. Co dělat?

Viry jsou škodlivé kódy šířené jejich tvůrci s různými cíli. Existuje velká řada virů, účelem některých z nich je ničit, jiné naopak mají za úkol usadit se v co největším počtu počítačových systémů a tyto pak využijí k cílenému útoku. Různé viry se mohou projevovat různě, např. od náhodného přehrávání určité melodie, přes zahlcení systému, úpravu nebo zničení dat, až po celkovou destrukci napadeného systému. Odhaduje se, že každý zhruba 300. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.

Virus obsažený v souborech či programech při spuštění nebo samovolně po nějaké době začne páchat škodu. Může například extrémně zpomalit počítač, nebo v horším případě smazat data na disku či způsobit vyhoření hardware. Virem mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento virus.

Správné odpovědi

- Neměli byste navštěvovat podezřelé stránky, spouštět podezřelé aplikace a otevírat soubory, u kterých není znám původ.
- Každý počítač by měl být vybaven antivirovou ochranou (např. Avast Free Mobile Security).
- Vyhněte se stahování programů z neznámých či nelegálních (warez) zdrojů.
- Do svého zařízení nevkládejte paměťová média (např. USB externí disky) z neznámých zdrojů
- Neotevírejte přílohy nevyžádaných emailu nebo zprávy od neznámých kontaktů na Facebooku.
- Stahujte Android aplikace pouze z oficiálního obchodu Google a aplikace pro iOS u Apple store.
- Pravidelně provádějte ve vašem antivirovém programu kompletní kontrolu systému. Pokud se na vašem počítači objeví viry, odstraňte je.

Hodnocení

Družstva prezentují maximálně 5 námětů, kde alespoň 3 musí být správné.

Odpoví-li minimálně 50% družstev správně, zabránili hackerovi napadnout školu.

Účastníci tak splnili první hlavní úkol a je třeba jim pogratulovat.

Hodnotící kritéria:
Hodnotí se správnost odpovědí. Družstva musí mít minimálně 3 odpovědi správné.

Délka soutěžního kola: 25 minut

Pomůcky:
- 10 popisů kybernetických hrozeb
- Sada nápověd pro každé družstvo
- Psací potřeby
- Papír
- Případná vizualizace.
  A3 s krátkým popisem kybernetické hrozby a možností nalepit pod to vybrané možnosti ochrany proti této hrozbě.

---

5. kolo Zákon a trest

Legenda
Závěrečné kolo se týká znalosti zákonů a pravidel. Legislativa České republiky říká, že kybernetické podvody jsou trestnými činy a jejich pachatelé musí být odsouzeni. V tomto kole je třeba prokázat takové vědomosti ze zákonů, aby mohl být podvodník odsouzen.

Cíl
Cílem je posilovat právní povědomí dětí a mládeže a vysvětlovat, že porušování zákonů a pravidel není ve standardní demokracii normální. To se týká i kybernetických podvodů.

Princip pátého kola
Organizátor rozdá družstvům přístup do on-line hry Klikačka, kde bude připraveno 10 otázek z oblasti zákonů se čtyřmi odpověďmi A-B-C-D. Družstva postupně odpovídají na otázky tak, že vybírají správnou odpověď.

Pokud neví, mohou otázku přeskočit. Na každou odpověď si mohou vsadit 0 – 4 body. Pokud odpoví správně, získají tolik bodů, kolik vsadili. Odpoví-li špatně, ztrácí tolik bodů, kolik vsadili, a pokračují další otázkou.

Příklad
Marek se chtěl vyhnout zkoušení z fyziky, a tak zatelefonoval řediteli školy a oznámil, že je ve škole ukryta bomba. Z legrace pak ještě telefonoval na nádraží a městský úřad a také oznámil hrozící bombový útok. Policie jej vypátrala a zjistila, že ještě nedovršil 15 let. Bude mít pro Marka nějaké následky, že spáchal čin jinak trestný?

a) Ano, soud pro mládež může učinit opatření potřebná k jeho nápravě.

b) Ne, ještě není trestně odpovědný.

c) *Ano, bude odejmut rodičům a ti budou odsouzeni za zanedbání výchovy s trestní sazbou skutku spáchaného Markem.*

d) *Ne, pouze bude pokárán policií.*

Trestní zákon spojuje trestní odpovědnost člověka až s dovršením věku 15 let. Dopustí-li se dítě mladší než patnáct let činu jinak trestného, může soud pro mládež učinit "opatření" potřebná k jeho nápravě, kterými jsou dohled probačního úředníka, zařazení do vhodného výchovného programu a ochranná výchova dle §§ 89 a 93 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, v platném znění.

Hodnocení

Všechna družstva odpovídají sama za sebe, ale zároveň přispívají k úspěšnosti všech zúčastněných. Cílem, aby 50% družstev získalo 10 bodů během 10 minut.

Hodnotící kritéria

Hodnotí se správnost odpovědí v časovém limitu

Doporučená on-line hra: Klikačka on-line

Klikačka je on-line vědomostní hra o zákonech. Několik set otázek prověří vědomosti žáků z oblasti práva a zákonů. Hra tak pomáhá zvyšovat jejich právní vědomí. Organizátor okamžitě vidí výsledky žáků a studentů.

Chcete-li si Klikačku on-line vyzkoušet, zde máte přístupy:

Adresa: projektrubikon.cz/klikacka

Login: Účastník 1 (až Účastník 40)

Heslo: U1 (až U40)

Více informací: http://www.projektrubikon.info/cz/vyukove-url-klikacka0.html

V případě zájmu kontaktujte vlastníky k bezplatnému využívání

Poznámka: Toto kolo se dá sehrát bez pomoci Klikačky on-line stejným způsobem jako první kolo. Je to ale v tomto případě časově náročnější.

Délka soutěžního kola: 10 minut

Pomůcky:

- On-line hra: Sázecí Klikačka
- Počítač pro každé družstvo a organizátora

Scénář programu Chyťme hackera

Program je koncipován jako kooperativní program, kde účastníci společně bojují proti hackerovi, který chce podniknout proti škole opakovaný kybernetický útok. Účastníci společně prochází pěti koly programu, ve kterých postupně získávají vědomosti a dovednosti, aby se dokázali ubránit kybernetickému útoku a v posledním kole napomoci k tomu, aby byl podvodník odsouzen.

	Program	Pomůcky	Čas
1.	***Přivítání účastníků*** Přečtení dopisu a následná diskuze, ve které bude stručně vysvětleno, kdo je to hacker a co je to hackerský útok a co může způsobit. **Otázka:** Kdo už měl napadený počítač nebo tablet Zároveň účastníkům sdělíme, že hacker plánuje další útok, který musíme společně odrazit.	• Tabule – bodování jednotlivých kol = MY a Hacker • E-mail od hackera • Aplikace Plikers • Hlasovací karty s QR kódy pro každého účastníka	12
2.	***Jak porazit hackera*** Čeká nás pět úkolů, abychom společně chytli hackera, aby nemohl provést další útok. V prvním a ve druhém kole budeme muset získat dohromady 10 klíčů, které nás ve 3. kole přivedou k 10 indiciím, na základě kterých se dozvíme, jakou zbraň proti nám hacker při svém útoku chce použit. Ve čtvrtém kole budeme klást hackerovi pasti. Doufejme, že na ně skočí. V pátém kole mu dokážeme že porušil zákony ČR.		3
3.	***1. Kolo Digitální Svět*** Cílem tohoto kola je získat 5 klíčů. Před začátkem prvního kola se může organizátor rozpovídat o digitálních trendech, případně ukázat nějaké zajímavé aplikace, například na principu umělé inteligence (Google Assistant, Navigace…) **Průběh 1. kola:** 5 – 10 otázek s odpověďmi Ano – Ne Za každou správně zodpovězenou otázku více než 50% účastníky dostávají jeden klíč, maximálně 5.	• 10 otázek přípravených v aplikaci Plickers • Počítač s otázkami, data-projektor, plátno • Chytrý telefon s aplikací Plickers • Počítač, tablet pro každého účastníka • Hlasovací karty s QR kódy • 5 obrázků klíčů	20

	Program	Pomůcky	Čas
4.	***2. kolo Pasti, pasti pastičky*** Cílem tohoto kola je získat dalších 5 klíčů. Vysvětlení důležitosti antivirových programů Průběh 2. kola: On-line hra Hexeto Základ je získat 3,5 bodu. Pokud získá 3,5 bodu 1 družstvo, dostanou účastníci 1 klíč. (2 družstva 2 klíče, 3=3, 4=4,5 a více 5 klíčů).	• Hlasovací karty s QR kódy • On-line hra Hexeto • Počítač, tablet pro každého účastníka • 5 obrázků klíčů	15 10 hra
5.	***3. kolo Hackerova zbraň*** Cílem je identifikovat hackerovu zbraň, kterou chce použít v dalším útoku. Na začátku organizátor vysvětlí účastníkům, kdo je to hacker, co je to kybernetická hrozba (Hackerova zbraň) a kybernetický útok. Rozdělení účastníků do družstev (cca 5 členů), například pomocí programu Flipity Organizátoři dopředu poschovávají v prostoru karty s QR kódy podle získaných klíčů. ***Průběh 2. kola*** Družstva hledají QR kódy, které jim ukazují indicie. Podle nich určují hackerovu zbraň. 50% a více pozná správně hackerovu zbraň = splněný úkol. Za to dostávají družstva v dalším kole sadu nápověd	• Alespoň jeden mobilní telefon do každého družstva • Karty s QR kódy • Program Flipity na rozdělení do družstev • Aplikace QR scanner pro hledání indicií • Papíry a tužky na poznámky	20 15 hra

	Program	Pomůcky	Čas
6.	***Kybernetické hrozby*** Cílem je najít možnosti, jak se bránit útoku hackera, který se na nás chystá. Už víme, co na nás hacker chystá, ale musíme být připraveni na vícero možností. Zde je organizátor přečte a velmi stručně naznačí, o co jde. Každé družstvo si vylosuje jednu hrozbu. K tomu dostanou sadu nápověd. Pokud v předchozím kole neuspěli – nezískávají nic. Organizátor na příkladu počítačového viru vysvětlí, co mají družstva dělat. ***Průběh 4. kola: Kybernetické hrozby*** Úkolem družstva je napsat 5 možností, jak se této hrozbě bránit, 3 návrhy z toho musí být správně. Pokud to zvládne 50% družstev – poráží hackera.	• 10 popisů kybernetických hrozeb • Sada nápověd pro každé družstvo • Psací potřeby • Papír • Případná vizualizace. A3 s krátkým popisem kybernetické hrozby a možností nalepit pod to vybrané možnosti ochrany proti této hrozbě	25 15 hra
7.	***Zákon a trest*** V tomto kole je třeba prokázat takové vědomosti ze zákonů, aby mohl být podvodník odsouzen. Organizátor zdůrazňuje, že kybernetické podvody jsou trestnými činy a jejich pachatelé musí být odsouzeni. V tomto kole je třeba prokázat takové vědomosti ze zákonů, aby mohl být podvodník odsouzen. ***Průběh 4. kola: Kybernetické hrozby*** V Klikačce je připraveno 10 otázek se čtyřmi odpověďmi A-B-C-D. Družstva postupně odpovídají na otázky, tak že vybírají správnou odpověď. Účastníci vítězí, pokud 50% družstev získá 10 bodů během 10 minut.	• On-line hra: Sázecí Klikačka • Počítač pro každé družstvo a organizátory	15 10 hra

	Program	Pomůcky	Čas
8.	***Závěr*** Shrnutí – porazili jsme hackera. Co je důležité pro každého z nás – 5 vět z průběhu programu, nebo každý řekne jednu věc. Poděkování a gratulace		10

Pokud budete využívat aplikaci **Plikers** je možné do programu zařadit řadu iniciačních otázek:

- Zajímáš se o digitální Novinky?
- Máš ve svém mobilu nějaký antivirový program?
- Navrhuješ variantu A-B-C-D?
- Už jsi dostal nějaký e-mail od hackera?

Pomůcky a podklady k realizaci programu

Otázky pro 1. kolo: Digitální svět

1. Platba očima

Lidé si zvykli na placení kartou, i když pro řadu z nich se jedná už o přežitou záležitost, protože platí chytrým mobilem. Někteří dokonce hodinkami nebo náramkem. Jsou tací, kteří platí čipem, který mají zabudovaný pod kůží.

Otázka: Je možné platit očima? Přijdete do obchodu, kouknete do platebního terminálu a je zaplaceno?

Odpověď: Ano - *V současné době je ve světě možné platit pouhým pohledem do skeneru oční čočky*

Zdroj: https://payeye.com/en/

2. Virtuální hřbitovy

Teď se půjdeme podívat na hřbitovy. Na některých už jsou k vidění digitální náhrobky, kde je stačí naskenovat kód do mobilu, a můžete si listovat profilem zemřelého. Tím to ale nekončí, někde jsou už k mání digitální hřbitovy, kam nemusíte vůbec fyzicky chodit. Stačí si v pohodlí domova pustit počítač a navštívit virtuální hrob nebožtíka, kde jsou informace o zemřelém, jeho fotografie a videa. Některé virtuální hřbitovy dokonce nabízí, vedle koho (slavného) může nebožtík spočinout.

Otázka: Existují na internetu virtuální hřbitovy?

Odpověď: Ano - *Existují online služby, kde lze vytvořit profil zemřelého se vzpomínkou. Virtuální hřbitovy existují lidské i zvířecí.*

Zdroj: https://virtualgrave.eu/, https://www.joincake.com/blog/virtual-cemetery/

3. Autobusy bez řidičů

Technologický vývoj jde rychle dopředu i v oblasti dopravy. Začala éra elektromobilů a umělé inteligence. Vyspělé počítačové systémy umějí auto nejen rozjet a udržet na silnici, ale jsou schopné i číst dopravní značení a řídit se jím. Jednotlivá počítačem řízená vozidla spolu vzájemně komunikují a jsou tak schopná stoprocentně předcházet dopravním nehodám. Z důvodu vyšší bezpečnosti a spolehlivosti již některé země preferují hromadné dopravní prostředky bez obsluhy. Auta či autobusy s pasažéry řízené výhradně počítačem proto již docela často najdeme v rušných ulicích měst Japonska či USA.

Otázka: Jezdí v některé zemi na světě v běžném silničním provozu vozidla bez lidské obsluhy?

Odpověď: Ne. *Asistenční systémy jsou sice ve vozidlech běžné, ale řízení ještě dlouhou dobu zůstane na člověku. Lidské zásahy jsou nezbytné i u provozu s vysokým stupněm automatizace. V současné době se nepředpokládá běžný legální provoz autonomních vozidel před rokem 2050.*

Zdroj: https://www.auto.cz/autonomni-auta-za-rohem-nebo-je-to-vsechno-jinak-134619, https://cs.wikipedia.org/wiki/Autonomn%C3%AD_vozidlo

4. Virtuální asistent

Každý z nás, kdo vlastní chytrý telefon si může pořídit tzv. virtuálního asistententa, což je umělá inteligence zabudovaná v našem chytrém mobilu. Ta nám odpovídá na naše otázky, poskytuje řadu různých doporučení, zavolá konkrétnímu člověku, pošle mu SMS, dokáženas navigovat na určené místo nebo pomůže s organizací každodenních úkolů. To vše za pomoci hlasových pokynů.

Otázka: Dokážou virtuální asistenti udělat všechny tyto věci?

Odpověď: Ano

Zapněte například svůj mobil s Androjdem. Položte otázku, například: "Jaké je dnes počasí a mobil vám hlasem odpoví.

5. Virtuální psycholožka

Není žádnou novinkou, že virtuální realita přináší mnoho zábavy a poučení. Stačí si nasadit virtuální brýle a můžete se podívat na historická místa, před pěti sty lety, nebo si můžete udělat prohlídku uvnitř lidského těla.

Virtuální realita dnes proniká do zdravotnictví. Nasadíte si brýle a před vámi se objeví sympatická dáma, která vám pokládá řada otázek na tělo. Je to virtuální psycholožka, která s vámi dělá první vyšetření. Pokládá otázky, vyhodnocuje otázky a systém zároveň vyhodnocuje, jak se chová vaše tělo. Na konci doporučí další postup - co má v následujících dnech dělat, doporučí běžné léky, nebo diagnostické vyšetření od skutečného psychologa.

Otázka: *Využívají některé psychologické ordinace k prvnímu vyšetření virtuálního psychologa?*

Odpověď: Ne

6. Pozemek na měsíci

Pomalu se blíží ta doba, kdy bude běžné cestovat na jiné planety. A nejenom cestovat, ale i bydlet tam. Už dnes si můžete koupit pozemek na planetách sluneční soustavy. K tomu slouží Lunární ambasáda (Lunar Embassy) - společnost, která podle práva Kalifornie vlastní pomocí licencovaných ambasád pozemky na tělesech sluneční soustavy a nabízí je k prodeji.

Otázka: *Můžete si koupit pozemek na planetách sluneční soustavy?*

Odpověď: Ano*, můžete. Dokonce cca 8 tisíc občanů ČR již vlastní nějakou část sluneční soustavy.*

7. Lety do vesmíru

Kathleen Rubins si NASA vybrala v roce 2009. Rubins dokončila svůj první vesmírný let na Expedici 48/49, kde strávila 115 dní ve vesmíru a provedla dva výstupy do vesmíru. Při druhém měla za úkol vyzkoušet, zda se pomocí chytrého telefonu dokáže spojit s posádkou rakety, která byl den od její vesmírné stanice. Z pěti pokusů se tři vydařily a Kathleen si minutu pokecala v kolegy v raketě.

Otázka: *Podařilo se Kathleen Rubins pomocí mobilu promluvit s jinou vesmírnou posádkou.*

Odpověď: Ne

8. Bezpečnostní kamery

V řadě špionážních filmů jsou lidé minitorováni chytrými špionážními kamerami. Na monitorech jsou lidé pak vidět s cedulkou u hlavy, kde jsou vypsány veškeré informace o daném člověku: Jméno, věk, povolání, kde pracuje, jaké má nemoci, zda platí daně, jak často je na sociálních sítích, kam chodí do restaurace…

Dnes už toto není jen ve filmu. Tyto bezpečnostní kamery jsou vyvinuty a dokonce je v některých lokalitách využívají k identifikaci svých občanů.

Otázka: *Jsou tekovéto bezpečnostní kamery využívány k identifikaci lidí?*

Odpověď: Ano. *Na ulicích v Číně přibývá kamer. Vláda je chce používat hlavně k rozpoznávání obličejů a následné lepší identifikaci jednotlivých obyvatel. každému občanovi Číny chce přidělovat určitý kredit na základě jeho chování.*

Více zde: https://tech.instory.cz/893-cina-ma-ve-mestech-site-kamer-pro-rozpoznavani-tvari-dokazi-identifikovat-cloveka-behem-vteriny.html

9. Drony s lidskou posádkou

Na drony, kteří dokážou natáčet video z výšky, na ty jsme si už celkem zvykli a můžeme si je koupit. Víte ale, že už existuje dron, který dokáže přepravit člověka. Přístroj vypadá jako malá helikoptéra. Na rozdíl od ní má ale čtyři dvojité vrtule. Ty se točí rovnoběžně se zemí, jako je tomu u ostatních dronů.

Elektřinou poháněný dron vydrží létat 23 minut. Do kabiny se vejde dospělý člověk společně s malým příručním zavazadlem. Dron unese „náklad“ o hmotnosti 100 kilogramů. Cestující zadá do systému plán letu, pak stačí už pouze stisknout tlačítko „vzlétnout“ na tabletu. Let se poté ukončuje tlačítkem „přistát“.

Otázka: *Je takovýto dron již v prodeji?*

Odpověď: Ano: *Čínská společnost Ehang jej prodává za dvě stě až tři sta tisíc dolarů.*

Více zde: https://21stoleti.cz/2016/01/12/prvni-dron-s-lidskou-posadkou/

10. GPS technologie

Prostřednictvím technologie GPS lze lokalizovat jakékoliv místo na zemském povrchu. V kombinaci s dalšími bezdrátovými sítěmi (WiFi internet, mobilní GSM sítě, mýtné systémy na silnicích…) tahle technologie umožňuje efektivní sledování majetku (auta, kola, zvířata) i osob. Nevýhodou je, že díky tomu nyní vždy někdo ví, kde přesně se pohybujete. To je však daní za technologický pokrok.

Otázka: *Je pravda, že díky moderním technologiím si v současné době mohou bezpečnostní složky či zločinci kdykoliv zjistit vaši polohu bez ohledu na to, co právě děláte?*

Odpověď: Ne - *Všechny používané technologie pro lokalizaci mají své limity a jejich použití není neomezené. Konkrétní osobu, která v sobě ani u sebe nemá žádné elektronické identifikační nebo lokalizační zařízení (čip, mobilní telefon, vozidlo s lokalizačním zařízením, atd.) žádným vzdáleným způsobem lokalizovat není možné. Možnost lokalizace většiny zařízení znemožníte odpojením od zdroje energie. Naprosto spolehlivým řešením je pak odstínění, obvykle pomocí kovové obálky, případně velmi silné vrstvy jiného materiálu. Např. v jeskyních lokalizace možná není z důvodu neprůchodnosti signálu přes silnou vrstvu horniny. Ve filmech často vídaná lokalizace zločinců pomocí termovize neumožňuje identifikaci konkrétní osoby. Lze pouze omezeně zjistit přítomnost nějaké osoby, ale nikoli její identitu.*

11. Chytrý záchod

Lékaři a vývojáři z americké Stanfordovy univerzity vymysleli chytrý záchod, který pomocí zabudované technologie dokáže vyhodnotit vzorek moči a stolice. Zároveň dokáže sejmout otisky prstů a odlišit podobu konečníku. Výsledky pak odešle do systému, kde jsou následně vyhodnoceny. Závažné onemocnění aplikace rozpozná tak, že je ve stolici či moči nepatrné množství krve, anebo podle jejich struktury a barvy. Svého majitele pak může včas upozornit na závažné nemoci, jako je rakovina tlustého střeva, selhání ledvin, ale i méně závažné záněty močových cest.

Otázka: *Dokážou toto všechno chytré záchody*

Odpověď: Ano, *dokážou*

Více zde: https://magazin.aktualne.cz/kuriozity/americti-medici-predstavili-chytry-zachod--rozpozna-nemoc-i-c/r~f24aa632797a11eaa7deac1f6b220ee8/

12. Pes zpívá operu

Už jsme si zvykli na filmy plné digitálních triků a iluzí. Počítačová grafika je leckdy k nerozeznání od reality. Ovšem kouzla se dají dělat nejen s obrazem. V nahrávacích studiích je dnes běžné, že písničky chtějí nahrávat i lidé, kteří vůbec neumějí zpívat. Prostě přijdou do studia, odrecitují text a přítomný hudebník jejich hlas pouhým hraním na klávesy nebo klikáním myší upraví do požadované melodie. Podobná kouzla jdou dělat s jakýmkoliv jiným zvukem, členem kapely na nové nahrávce může tak být klidně váš pes, zubní kartáček nebo pračka.

Otázka: *Je možné za pomoci klávesového nástroje udělat z mluveného slova či jiných zvuků melodii?*

Odpověď: Ano - *např. program Auto Tune umožňuje přes MIDI rozhraní připojit digitální klaviaturu, pomocí které lze přesně naladit jakýkoliv zvuk vstupující do programu*

Zdroj: https://www.antarestech.com/

13. Digitální trenér

Elektronika a digitální technologie jsou dnes nedílnou součástí přípravy sportovců, a to nejen profesionálů. Chytré hodinky v kombinaci s mobilem umí monitorovat vaši tepovou frekvenci, rychlost pohybu, zaznamenávat trasy i ukládat všechny naměřené údaje. Dokonce si můžete s jejich pomocí realizovat vlastní tréninkový plán, který vám připravil živý profesionální trenér. Velmi často se však stává, že vám tenhle digitální "asistent trenéra" říká, že byste měli běžet pomaleji, ačkoli máte stále sil na rozdávání. Protože rychlejším tempem více natrénujete, informace z digitálního zařízení berete jen jako informativní a trénujete raději podle svého pocitu.

Otázka: *Je pravda, že pokud budete dle doporučení trenéra a digitálních tréninkových pomůcek trénovat méně a pomaleji, než na co se zrovna cítíte, budou vaše sportovní výkony naopak lepší?*

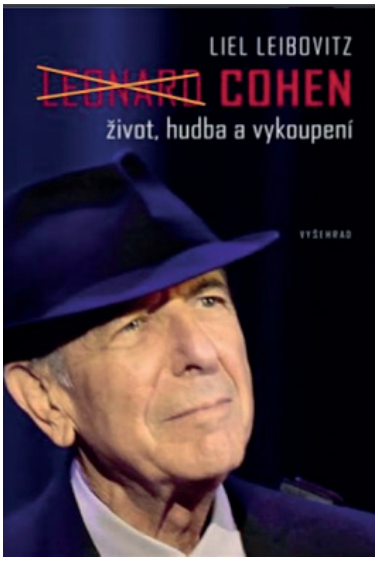
Odpověď: Ano - *ve sportu úplně neplatí, že čím více trénujete, tím budete silnější a rychlejší. Platí, že nejlepší je ten, kdo trénuje nejlépe. A podle vědeckých poznatků je nejefektivnější trénink takový, který optimálně střídá zátěž a regeneraci. Takže kdo trénuje pouze formou co nejvyšší zátěže, nikdy nebude tak dobrý jako ten, kdo nechává tělo správně odpočívat, a to například i formou hodně lehkých tréninkových jednotek. Proto například běžci nebo*

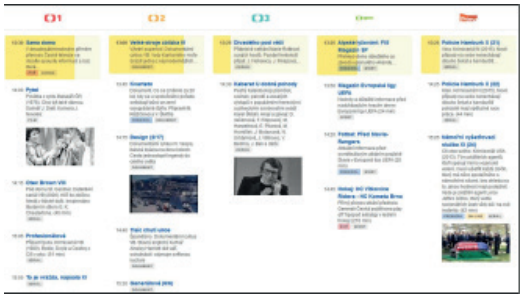
cyklisté mají dlouhé tréninky ve výletním tempu, kdy si spolu mohou bez problému povídat a nejsou vůbec zadýchaní.

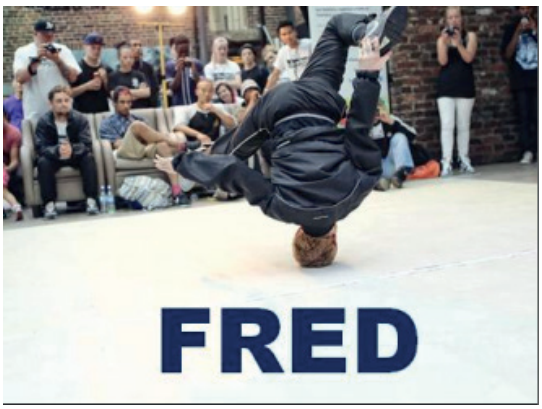
Zdroj: např. https://www.fsps.muni.cz/emuni/data/reader/book-5/14.html

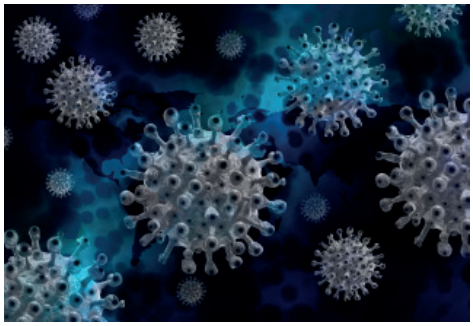
Indicie pro 3. kolo: Hackerova zbraň

Správný výsledek: Počítačový vir (virus)









Úkoly pro 4. kolo: Kybernitické hrozby

1. Počítačové viry

Náš příběh

S klukama dnes ve škole nic moc nebylo. Seděli o přestávkách v lavicích, v ruce mobily a pařili nějakou novou hru. Karel nahlédl přes rameno jednoho z nich a hra se mu hned zalíbila. Dal si její název do vyhledávače a z první možné nabídky si ji stáhl. Doma hrál snad celý večer. Byla to pecka.

V dalších dnech se jeho mobil začal chovat velmi podivně. Výrazně se zpomalil a to tak, že v něm nemohl hrát žádnou ze svých oblíbených her, ani se učit. Navíc mu tam každou minutu naskakovalo plno reklam a to i s velmi nevhodným obsahem. Nešlo se jich zbavit. Karel nedělal prakticky nic jiného, než kliknutím ukončoval reklamy.

Svěřil se svým problémem klukům a dozvěděl se, že si stáhl do svého mobilu počítačový virus, protože si hru stáhnul z neoficiálního obchodu. Odinstaloval hru, ale problémy nepřestaly. Co dělat?

O počítačových virech

Viry jsou škodlivé kódy šířené jejich tvůrci s různými cíli. Existuje velká řada virů, účelem některých z nich je ničit, jiné naopak mají za úkol usadit se v co největším počtu počítačových systémů a tyto pak využijí k cílenému útoku. Různé viry se mohou projevovat různě, např. od náhodného přehrávání určité melodie, přes zahlcení systému, úpravu nebo zničení dat, až po celkovou destrukci napadeného systému. Odhaduje se, že každý zhruba 300. zaslaný email v celosvětovém měřítku obsahuje alespoň jeden počítačový vir.

Virus obsažený v souborech či programech při spuštění nebo samovolně po nějaké době začne páchat škodu. Může například extrémně zpomalit počítač, nebo v horším případě smazat data na disku či způsobit vyhoření hardware. Virem mohou být infikovány e-maily, webové stránky, aplikace či soubory, které když se stáhnou, s sebou přinesou právě tento virus.

Úkol: Napište 5 možností, jak se bránit počítačovým virům.

Jak se bránit - Správné odpovědi

1. Neměli byste navštěvovat podezřelé stránky, spouštět podezřelé aplikace a otevírat soubory, u kterých není znám původ.
2. Každý počítač by měl být vybaven antivirovou ochranou (např. Avast Free Mobile Security).
3. Vyhněte se stahování programů z neznámých či nelegálních (warez) zdrojů.
4. Do svého zařízení nevkládejte paměťová média (např. USB externí disky) z neznámých zdrojů.
5. Neotevírejte přílohy nevyžádaných emailu nebo zprávy od neznámých kontaktů na Facebooku.
6. Stahujte Android aplikace pouze z oficiálního obchodu Google a aplikace pro iOS u Apple store.
7. Pravidelně provádějte ve vašem antivirovém programu kompletní kontrolu systému. Pokud se na vašem počítači objeví viry, odstraňte je.

2. Poškození nebo zničení hardware

Náš příběh

Tak jako téměř každý den si i tohle dopoledne Jitka užívala se svým malým synkem Radimem na dětském hřišti. Byl teplý začátek září a hřiště skoro plné. Děti vesele skotačily a maminky probíraly zážitky z prázdninových cest. Jitka se pomalu chystala s Radimem k odchodu, když chlapec radostně přiběhl: „Maminko, podívej, co jsem našel!“ Držel v ruce malou barevnou tyčinku a radostně s ní mával nad hlavou. Jitka se nejprve trochu lekla, že její dítko někomu sebralo oblíbenou hračku, ale při bližším ohledání zjistila, že tohle hračka určitě nebude. „Ráďo, myslím, že jsi našel něco, co někdo ztratil. Zkusíme zjistit, komu to patří.” Barevná tyčinka byla totiž ve skutečnosti USB flashdisk v docela pěkném pouzdře z měkkého plastu.

Dotazování na ztrátu v okolí hřiště se nesetkalo s odezvou, Jitka se tedy rozhodla, že zjistí, co na nalezeném datovém médiu je a podle toho zkusí dohledat majitele. Doma tedy po obědě otevřela notebook a po startu systému vsunula flashdisk do konektoru a spustila prohlížeč souborů. Chvilku se nic nedělo, ale pak najednou počítač problikl, zhasl a zcela ztichnul. Jitka hned zkusila opětovný start, nic. „Asi se vybila baterie.“ Připojila tedy napájecí zdroj a stiskla znovu zapínací tlačítko. Stále bez odezvy. Počítač byl relativně nový, po chvilce zkoušení proto rezignovala a zavolala prodejci s popisem problému.

Notebook putoval do opravy a už za dva dny bylo jasno. Počítač byl na odpis a diagnóza? Jitce zničil počítač ten krásně barevný USB disk!

USB killer

Zdánlivý disk nebyl ve skutečnosti paměťové médium, ale tzv. USB killer - zařízení, které po připojení k počítači dokáže po několika sekundách vygenerovat tak silný elektrický výboj, že zničí obvody na základní desce počítače i další jeho komponenty. Princip je poměrně jednoduchý, zařízení se postupně nabije z USB konektoru a po dosažení určité úrovně nabití se veškerá energie v podobě vysokonapěťového pulzu vrátí naráz přes datové piny do počítače. Účinek je bleskový a pro počítač většinou smrtící. Nezbývá než výměna všech poškozených komponent. Existuje i USB killer softwarový - na flashdisku je virus, který dokáže rychle smazat nebo nevratně poškodit datové struktury na pevném disku počítače.

Úkol: Napište 5 možností, jak se bránit poškození vašeho zařízení

Jak se bránit - Správné odpovědi

1. Nikdy ke svému počítači nepřipojuji USB disky či jiná paměťová média neznámého původu.
2. Nepoužívám nabíječky či zdroje s poškozeným krytem nebo izolací.
3. Používám ochranné kryty a pouzdra.
4. Pokud nemám elektrické zásuvky s přepěťovou ochranou, při bouřce nebo delší nečinnosti odpojuji zařízení od elektrické sítě.
5. Používám jen takové elektrické příslušenství, které má homologaci pro použití v naší rozvodné síti s napětím v zásuvce 230 V a kmitočtem 50 Hz. Příslušenství určené pro jiné země nemusí správně fungovat nebo jejich použití může být nebezpečné.
6. Digitální techniku ukládám vždy na bezpečné místo, kde nehrozí poškození vodou, nárazem či vysokou teplotou. V případě rychlého přechodu ze zimy do tepla dochází v přístroji ke kondenzaci, která je nebezpečná pro elektrické obvody. Před spuštěním je vhodné nechat zařízení přizpůsobit teplotě okolního prostředí.

7. Zařízení s baterií, které delší dobu nepoužívám, občas nechám dobít. Baterie se pomalým tempem sama vybíjí a při dosažení velmi nízké úrovně nabití se podstatně zvyšuje opotřebení baterie a možnost její poruchy.

---

3. Phishing

Náš příběh

Aplikace NEJLEPŠÍ PŘEVODNÍK MĚN ZDARMA!

Na jaře roku 2020 se na Google Play objevila velmi chytrá a užitečná vychytávka pro všechny uživatele Androidu, kteří často přepočítávají měny různých států podle směnných kurzů. Aplikace byla od počátku velmi dobře hodnocena a brzy dosáhla desetitisícových počtů stažení. Uživatelé při jejím používání nešetřili chválou a vůbec netušili, že si instalací pozvali k sobě domů záškodníka.

Během instalace si aplikace vyžádala oprávnění přistupovat k uživatelským datům. To je v těchto případech docela obvyklé a nikomu se to nezdálo nebezpečné. V prvních několika týdnech aplikace fungovala zcela normálně, při dosažení určitého počtu uživatelů však začala provádět zvláštní věci: během přístupu do bankovnictví dokázala číst přístupové údaje uživatele a ty odesílat vzdálenému útočníkovi. Po zjištění tohoto chování Google neprodleně aplikaci ze svého obchodu Play odstranil.

Uvedený příběh je zcela reálný, o odhalení phishingového útoku za pomoci nebezpečné aplikace se skrytým tzv. trojským koněm se postarala česká antivirová společnost Avast.

O phishingu

Principem phishingu (česky se mu někdy říká “rhybaření”) je to, že útočník nasadí návnadu a čeká, kdo se chytí. V tomto případě byl škodlivý kód umístěn do aplikace, která nabízela velmi žádanou službu a byla umístěna v největším světovém aplikačním obchodu. Tato aplikace posloužila jako udička s návnadou na oběti útoku. Neaktivita viru v počátku distribuce byla zcela záměrná - útočník vyčkával na kladné reakce uživatelů a očekával výrazný růst počtu napadených uživatelů. Aktivitu viru spustil až v okamžiku, kdy počty instalací pro něho byly příznivé a dal se očekávat snadný a bohatý “úlovek” v podobě velkého množství získaných osobních dat.

Autoři phishingových útoků spoléhají na to, že pro uživatele jsou některé věci obzvlášť lákavé a snadno tedy vyvolají jejich akci. Jsou to např. programy nebo hry zdarma, výhra v loterii, snadné zabezpečení počítače, odvrácení hrozby, atd. Pokud uživatelům útočník nastraží past v podobě infikovaného programu nebo falešného formuláře pro změnu hesla, je velká pravděpodobnost, že se na léčku někdo chytí.

Phishing a další triky hackerů, které jsou založeny na záměrném vyvolání určité reakce uživatelů, řadíme do kategorie tzv. sociálního inženýrství. Manipulují vybrané osoby za účelem získání informace, kterou by osoba jinak nesdělila. Uvedou oběť do situace, kdy se domnívá, že ví, co dělá, ale ve skutečnosti její činnost řídí útočník. Jinými slovy: není třeba prolamovat hesla speciálními programy, když jej oběť sama dobrovolně sdělí. V našem případě se uživatelé domnívali, že zadávají své údaje do systému svojí banky.

Úkol: Napište 5 možností, jak čelit phishingu

Jak se bránit - Správné odpovědi

1. Phishingu stejně jako dalším technikám sociálního inženýrství se lze bránit zejména neustálým vzděláváním sama sebe, získáním všeobecného přehledu o fungování internetu.
2. Vzhledem k tomu, že se jedná o soubor klamavých technik, které míří spíše na uživatele jako takového, nikoliv na počítače nebo mobilní telefony, nelze se prakticky bránit technologickým zabezpečením. Antivirový program by mohl pomoci v případě trojského koně, ale na podvržené formuláře na webu bohužel nestačí.
3. V reálném světě důvěřujte, ale prověřujte. Ve světě kybernetickém spíše nedůvěřujte!
4. Málokteré nabídky věcí či služeb "Zdarma" jsou doopravdy poskytnuty zcela nezištně. Ve skutečnosti musíte výměnou poskytnout nějaká svá osobní data (email, věk, adresa…) nebo musíte koukat na reklamy. Někdy to děláte vědomě, v horších případech si data bez vašeho vědomí zjistí skrytý špionský software.
5. Ignorujte veškeré nabídky z nevyžádané pošty (spamu).
6. Nikdy neklikejte na žádné odkazy z nevyžádané pošty (spamu).
7. Čtěte údaje v řádku s adresou webu. Je-li adresa podezřelá (vypadá jinak než jste zvyklí), stránku raději opusťte a nezadávejte na ní žádná data.
8. Své osobní údaje, heslo nebo bankovní údaje nevyplňujte na neznámých webových stránkách a neposílejte je emailem nebo instant messengery.

---

4. Podvodné nákupy na internetu

Náš příběh

Jirka se rozhodl prodat na internetu svůj starší notebook. Sestavil proto inzerát, který vystavil na několika online bazarech. Asi za týden mu blikla v chatu zpráva:

"Dobrý den, máte ještě ten notebook? Měl bych zájem."

Jirka zrovna dělal práci do školy, ale vidina rychlého prodeje jeho soustředění rychle převedla jinam. Odepsal, že není problém a že přístroj je připraven k předání.

"Potřeboval bych to mít zítra ráno u sebe, zvládnete mi počítač odeslat ještě dnes? Vaši cenu respektuji a zaplatím přes banku okamžitě, když mi pošlete číslo účtu", pokračoval zájemce v konverzaci.

Myšlenky na školu byly definitivně pryč, Jirka vylovil z paměti číslo a hned ho poslal do konverzace. Z druhé strany přišlo rychlé "OK" a asi za dvě minuty chat cinká znovu:

"Tak je to hotové, peníze odeslány. Pošlu pro počítač kurýra, do hodiny je u vás. Mohu požádat o adresu? Potvrzení z banky pošlu další zprávou."

Jiří bleskově vypsal adresu domů a mrknul do rohu, kde stála krabice se starým notebookem: "To je panečku rychlost," pomyslel si když mu na displeji blikla další zpráva, tentokrát i s přílohou:

"Tady je to potvrzení z banky, peníze máte do rána na účtu. Kurýr už je na cestě k vám."

Po rozkliknutí se na displeji objevil strohý oficiální formulář Potvrzení o platbě, kde stálo, že banka potvrzuje, že z účtu 123456789/5678 vedeného na majitele Davida Eliáše bylo převedeno 4500 CZK na účet 45454545/5566, což je číslo Jirkovy banky. Jiří se spokojeně usmál a odlomil si kousek čokolády, která ležela na stole. Za půl hodiny zastavila před domem

bílá dodávka a Jiří předal šoférovi balíček. Krátkou zprávou kupujícímu, který měl svůj profil označen jako Dave Strong ještě poděkoval za rychlý obchod.

Druhý den ráno Jirka spustil internetové bankovnictví. Zůstatek byl však stejný jako před týdnem, platba od Dave Stronga. nikde. Zkusíme mu napsat? OK, ale co to? Uživatel neexistuje?

Platba nedorazila ani v dalších dnech a bylo jasné, že se Jiří stal obětí internetového podvodníka. Při důkladné kontrole potvrzení z banky zjistil, že číslo účtu na potvrzení je smyšlené a celé potvrzení je jen obyčejný textový dokument bez elektronického podpisu banky. Takže podvrh. Vzhledem k tomu, že Jiří nevěděl o podvodníkovi vůbec nic a nebyl schopen ani blíže identifikovat šoféra s dodávkou, šance na dohledání podvodně vylákaného notebooku je prakticky nulová.

Falešné platby

Podvodníci mají při obchodování na internetu mnohem více prostoru pro různé triky než je tomu při běžném obchodování "z ruky do ruky". V kyberprostoru lze daleko snáze skrýt svou identitu. Téměř nikdy si nemůžete být jisti, že člověk, se kterým jste v kontaktu, je ve skutečnosti tím, za koho se vydává. Profilová fotka mladé maminky s dítětem může klidně patřit protřelému zlodějíčkovi v důchodu nebo naopak.

Pokud něco prodáváte, mezi nejčastější podvodné techniky nakupujících patří fiktivní platby a padělané dokumenty. Podvodník si získá vaši důvěru tím, že skvěle spolupracuje a komunikuje. Nabízí rychlou platbu předem a zaslání různých druhů potvrzení o převodu z banky. Při bližším zkoumání však zjistíte, že potvrzení jsou kopií obrazovky, tj. obrázkem. A obrázek nevznikl v bance, nýbrž v počítači rafinovaného podvodníka. Využil skutečný screen z bankovnictví a v něm pozměnil platební údaje tak, abyste si mysleli, že vám peníze skutečně poslal. Avšak platba na váš účet nikdy nedorazí. Pokud po obdržení takového potvrzení zboží odešlete, můžete se rozloučit s ním i s penězi. Podvodníka nejspíš nenajdete, neboť nemáte ani adresu. Rafinovanější podvodníci totiž posílají pro zboží "svého kurýra", přičemž tím kurýrem často bývají oni sami, aniž byste to tušili.

V posledních letech to mají podvodníci trochu složitější, neboť banky velmi zrychlily převody peněz a mnoho prodávajících raději počká na fyzický převod částky než by posílali cokoliv naslepo.

Úkol: Napište 5 pravidel bezpečného nákupu na internetu.

Pravidla bezpečného prodeje

1. U nakupujících, které neznám, se snažím zjistit věrohodné reference.
2. Zboží popíšu co nejpřesněji, aby bylo naprosto zřejmé, co prodávám.
3. Při prodeji bazarového zboží je nejbezpečnější osobní předání na veřejném místě, případně zaslání zboží po platbě předem.
4. Platbu dobírkou, případně po obdržení zboží akceptuji jen u ověřených nakupujících.
5. Obrázek nebo jiný dokument obsahující jakékoli potvrzení o platbě není věrohodný, pokud neobsahuje elektronický podpis (certifikát) toho, kdo potvrzení vystavuje.
6. Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží).

7. Není-li to nezbytné, nevodím neznámé zájemce až k sobě do bytu. Věc lze předat venku či na veřejném místě

---

5. Podvody při prodeji zboží

Náš příběh

Michalovi se pomalu, ale jistě blížily jeho patnácté narozeniny. "To je významný mezník v životě každého mladého člověka" prohovořil otec při nedělním obědě. "A takový mezník je třeba orámovat nějakým darem, který se významně zapíše do Tvého života synu" pokračoval otec. "Co by sis přál, abys pocítil změnu života? zeptal se otec. Michal se dlouho nerozmýšlel a rychle odpověděl: "iPhone, jednoznačně iPhone, většina ve třídě ho má." "To přece není argument", odpověděl otec, na kterém bylo vidět, že ho přání zaskočilo. Nechtěl brát své slovo zpět a tak řekl: "Napiš mi na A4, jaký je takový rozdíl mezi iPhone a jiným mobilem, že ho tak potřebuješ". Brzy Michal přinesl zpracovaný úkol. Na papíše A4 bylo velkými Písmeny napsáno: "JE TO PROSTĚ IPHONE". Otec se zprvu chtěl rozčilovat, ale pak si uvědomil, že v té větě je vše, co po synovi vyžadoval. Rozhodl se dostát svému slibu.

Na Internetu našel iPhony, které se pohybovaly okolo dvanácti tisíc, což bylo nad maximem, které chtěl do mobilu investovat. To si zakázal dívat se na poslední novinky, které byly násobně vyšší. Pak si dal vybraný mobil do porovnávačů cen. Našel levnější ceny u použitých nebo zánovních iPhonů. Chtěl však synovi koupit k patnáctinám mobil nový a tak pokračoval v hledání nejlevnějšího eshopu. Pak ho našel. Obchod s výprodejem těchto mobilů s cenou pod šest tisíc., Obchod se jich zbavoval, protože chtěl prodávat jen ty nejmodernější typy. Otec nezaváhal ani vteřinu a okamžitě ho koupil, především z toho důvodu, že na skladě byly poslední dva, navíc v požadovné barvě.

Narozeniny se blížily a otec spokojený se svými obchodními dovednostmi čas od času vypustil poznámku, která naznačovala, že se má Michal na co těšit. Uplynul týden a mobil nepřišel. Nepřišel ani další týden. To už do narozenin zbývaly necelé dva týdny. Otec volal do eshopu několikrát denně. Nikdo nebral telefony. Začal se tedy o eshop zajímat více. Zjistil, že nesídlí v České republice, ale v zahraničí. V referencích, které na obchod našel, si přečetl, že jedná o podvodný obchod, který nabízí levné mobily, avšak je nikdy neodeslal. Takových referencí tam bylo desítky. Otec byl ten den velmi zatrpklý. Ještě zkusil párkrát zavolat, napsal i e-mail, podíval do diskuzí na možnosti postupu, volal na úřady. Výsledkem bylo, že v den narozenin šel do klasické prodejny, kde koupil iPhone za téměř třináct tisíc korun.

Triky podvodníků

Internet je největší světové tržiště. Lze na něm koupit cokoli - luxusní a kvalitní zboží i levné a nefunkční cetky. Můžete i naletět úplně a za své peníze nedostat vůbec nic. Vytvořit elektronický obchod, který bude vypadat, že je plný krásného zboží, není nic složitého. Náklady jsou zanedbatelné. Pro podvodníka je tedy velmi snadné vytvořit lákavou "výkladní skříň", přes kterou se bude snažit vylákat z vás peníze. Vy si objednáte pěkný telefon, zaplatíte a od té doby o obchodu neuslyšíte. A jste bez peněz.

To však není jediný způsob, jak přijít o peníze. Jsou i obchody, které zboží skutečně posílají, avšak kvalita toho, co dostanete domů, je o moc horší než to, co obchod inzeroval. Pak nezbývá než reklamovat a to je často velmi dlouhá anabáze. Mnoho podvodníků dopředu spoléhá na to, že u levnějších položek zákazník reklamovat nebude a se ztrátou se prostě smíří.

Úkol: Napište 5 možností, jak se bránit podvodům při prodeji zboží na interentu.

Pravidla bezpečného nákupu

1. U prodejců, které neznám, se snažím zjistit věrohodné reference.
2. Informace o prodejci ověřuji z více nezávislých zdrojů (Má kamenné obchody? Jaké jsou reference na srovnávačích? Co říkají sociální sítě? A co články v médiích?).
3. Pokud nakupuji, za zboží předem platím jen v případě ověřených prodejců.
4. Před nákupem se snažím o zboží i podmínkách prodeje zjistit maximum (recenze zboží jinde než u prodejce, nezávislé testy, záruční a reklamační podmínky…).
5. Platební údaje k bankovní kartě ukládám odděleně a používám je jen u ověřených prodejců.
6. Platební údaje nenechávám uložené ve svém účtu u obchodníka.
7. Online platby provádím pouze ze zařízení, o kterém vím, že je bezpečné.
8. Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží).

---

6. Vydírání

Náš příběh

Je středa, 11. prosince 2019, dvě hodiny po půlnoci. Klid během nočního provozu Nemocnice Rudolfa a Stefanie v Benešově jen občas přeruší akutní příjem. Během zadávání dat na chirurgické ambulanci bylo zaregistrováno výrazné zpomalení počítačů, které se během krátké doby staly zcela nefunkčními. Do rána se problém rozšířil do celé nemocniční sítě, která tak byla zcela vyřazena z provozu. Ihned po zjištění rozsahu a podstaty problému zasedá v nemocnici krizový štáb, protože je ohrožena péče o pacienty.

Do nemocniční sítě se podařilo proniknout hackerům, kteří dobře promyšleným postupem nejprve převzali kontrolu nad administrátorskými účty správců počítačové sítě, aby následně instalovali zákeřný ransomware na všechny dostupné počítače a datová úložiště. Vyděračský software začal intenzivně šifrovat všechna data. Tím se však prozradil, neboť došlo k výraznému zpomalení sítě. K šifrování je totiž potřebný obrovský výpočetní výkon. Přestože IT oddělení nemocnice ihned po zjištění problému všechny počítače odpojilo, program napáchal takové škody, že nemocnice musela řadu hodin improvizovat úplně bez svých dat. Úplné obnovení služeb trvalo několik týdnů, škody byly vyčísleny na částku kolem 60 milionů korun i přesto, že nemocnice žádné výkupné nezaplatila a obnovila postupně data a funkčnost systémů ze svých zdrojů.

Ransomware

Ransomware je jedním z nejziskovějších, a tedy jedním z nejoblíbenějších typů malwaru mezi kyberzločinci. Tento speciálně upravený počítačový virus se nainstaluje do počítače oběti, zašifruje v něm soubory a poté se zaměří na oběť a požaduje výkupné (obvykle v bitcoinech), za které tato data vrátí uživateli.

Podle této činnosti se podobné vyděračské viry označují právě jako ransomware (z anglického „ransom“ – výkupné) Zaplacením výkupného je podmíněno dešifrování původně zašifrovaných dat a možnost opětovného přístupu k nim. Oběť se nejčastěji infikuje tímto škodlivým softwarem při návštěvě ohrožených webových stránek nebo při stažení souboru, jehož

součástí je právě ransomware.

Velmi často se ale stane, že se data neodblokují ani po zaplacení výkupného a dojde tak k dalším škodám (ztráta dat i peněz). Je-li systém nakažen, nabízí se dvě základní možnosti opravy: buď operační systém přeinstalovat a přijít tak o naše data, nebo se pokusit data dešifrovat. To je však velmi složitý a ne vždy stoprocentně řešitelný úkol.

Úkol: Napište 5 možností, jak se bránit vydírání.

Jak předcházet ztrátám dat a bránit se vydírání?

1. Pravidelně zálohuji data, nejlépe alespoň na dvou odlišných místech.
2. Používám ochranu proti virům a škodlivému software.
3. Přístroje, které obsahují data, nenechávám bez dozoru a ukládám je na bezpečných místech.
4. Používám bezpečná hesla pro přístup k datům.
5. Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon).
6. Instaluji pouze software z ověřených zdrojů.
7. Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy.

---

7. Krádež uživatelského účtu

Náš příběh

Patnáctiletý Radek je vášnivým sportovcem a velmi dobře hraje na klavír. Hodně volného času ale také tráví hraním počítačových her. Kromě oblíbeného fotbalu si na počítači s kamarády rád zahraje i nějakou týmovou strategickou střílečku. Většinu her si nakoupil přes distribuční platformu Steam. Nákupy i instalace přes Steam jsou jednoduché a všechno může Radek ovládat z jednoho prostředí. Hraní mu většinou sponzorují rodiče a občas dostane od někoho dalšího jako dárek poukázku na nákup nové hry nebo nějakých vylepšení.

Tipy na nové hry i různé herní triky studuje s kamarády na Youtube nebo na herních fórech a registroval se i k odběru řady hráčských newsletterů, které mu chodí do emailové schránky. Často jsou doprovázeny přílohami s různými návodnými texty či obrázky.

V létě ale tolik času u počítače netráví. Během posledních letních prázdnin byl na fotbalovém soustředění a pak s rodiči na deset dnů v Alpách. Po obědě na horské chatě Radek rychle kontroloval zprávy na svém telefonu. Po několika rychlých odpovědích chatujícím kamarádům narazil v emailové schránce na něco, co ho zarazilo: zpráva z podpory Steamu, že právě nakoupil za 30 dolarů nové funkce do hry Dota.

“To přece není možné, vždyť jsem nakupoval naposledy někdy v květnu a teď v létě jsem už tři týdny ani nehrál?” diví se Radek. Večer, když se vrátili do penzionu, se Radek zkusil z tátova notebooku přihlásit do Steamu. Ani na třetí pokus heslo, které si naprosto bezpečně pamatoval, neprošlo…

Jak lze ukrást váš účet?

Radkovi někdo na Steamu odcizil uživatelský účet. Děje se to tak, že útočník nějakým způsobem zjistí uživatelské jméno a heslo. Získat uživatelské jméno je celkem snadné -

obvykle jej používáte na herním fóru nebo je viditelné při multiplayer hraní. Heslo při těchto útocích nejčastěji útočník zjistí z nějaké hacknuté databáze nebo za pomoci keyloggeru ve vašem počítači. Další možností je zaútočit přímo na váš emailový účet - pokud se tam útočník dostane, většinou pak snadno získá přístup ke všem službám, které jsou k mailu navázané a nemají vícefázové ověření přístupu.

Úkol: Napište 5 možností, jak se bránit vydírání.

Jak ochránit svůj účet před hackery?

1. Používám bezpečná, tzv. silná hesla (“JednaDve34pet” je mnohem bezpečnější než “12345”.
2. Přístupové údaje k účtům bezpečně ukládám, případně i šifruji.
3. Používám antivirovou ochranu svých zařízení.
4. Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon).
5. Instaluji pouze software z ověřených zdrojů.
6. Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy.
7. Neprodleně reaguji na jakékoliv známky napadení účtu (změním heslo, dočasně umožním přístup jen z jednoho zařízení, atd.).

---

8. Spam

Náš příběh

Karel je fanouškem historických vozidel. Pravidelně jezdí na historické srazy a doma má pěknou sbírku starých motoristických suvenýrů. Poslední dva roky hodně šetřil, aby si mohl pořídit pěkného veterána i domů. Zaregistroval se na fanouškovských fórech, sleduje internetové bazary a skupiny a úplně nejraději sleduje videa o opravách starých vozů.

Z oblíbeného diskuzního serveru přišla Karlovi jednoho dne zpráva, že došlo k napadení jejich databázového serveru a pravděpodobně k úniku dat. Zástupce serveru se uživatelům omlouval a doporučil neprodlenou změnu přístupových údajů ke službě. Karel to podle doporučení serveru provedl a fórum mohl bez problému používat dál. Během několika dnů však do jeho emailové schránky začalo přicházet velké množství reklam na zboží, o které se nikdy nezajímal.

Co je Spam?

Spam je nevyžádané sdělení šířené internetem v podobě e-mailu, zprávy na sociální síti, článku na určitém webovém serveru. Zprávy jsou většinou rozesílány či publikovány automaticky specializovanými programy, tzv. spamboty. Spambot umí i automaticky vyplnit přihlašovací nebo registrační formuláře, aby bylo možné distribuovat spam jménem určitého uživatelského účtu. Často jsou k rozesílání spamu zneužívány počítače nebo uživatelské účty napadené hackery. Pokud se vám něco takového stane, obvykle spam začne chodit vašim kontaktům přímo z vašeho účtu.

Emailové adresy, na které je spam odesílán, jsou uloženy ve velkých databázích spammerů. Do nich se dostávají různým způsobem. Nejčastěji to je za pomoci automatického sběru emailových adres z webových stránek, adresy spammerům však často poskytují sami uživatelé, když vymění svoji adresu za přístup k nějakému benefitu (ebook či video zdarma,

atd.). Výjimečné nejsou ani záměrné krádeže databází adres hackery, protože funkční adresy potenciálních zákazníků jsou pro mnoho obchodníků velmi cenné a ukradené adresy se tak dají dobře zpeněžit.

Úkol: Napište 5 možností, jak se bránit spamu.

Jak zatočit se spamem?

1. Při registraci do nové služby pozorně čtu podmínky zpracování a použití mých dat. Není-li to nezbytné, nepovoluji použití pro marketingové účely.
2. Klikání na neznámé odkazy v příchozí poště často způsobí, že se vaše adresa dostane do dalších seznamů pro posílání spamu.
3. Ve vašem mailboxu spam důsledně označujte.
4. Pro účely jednorázových a méně důležitých registrací si založte zvláštní emailovou adresu. Odlehčíte tím své hlavní schránce.
5. Je-li v nevyžádané poště možnost odhlášení (zrušení zasílání), využijte ji.
6. Pokud spamovým filtrem prochází určitý druh nevyžádaných zpráv, upravte blacklist filtru.
7. Pokud běžné a očekávané zprávy končí ve spamovém koši, upravte whitelist spamového filtru.

---

9. Hoax

Náš příběh

Minulý týden Jitka ve své doručené poště nalezla následující zprávu:

> *Od: mojebanka@bankovnivarovani.com*
> *Pro: klienti@bankovnivarovani.com*
> *Předmět: Víte, jak používat svůj PIN?*
>
> *Vážení klienti,*
>
> *přímo od bankovní komise jsme dostali oficiální informaci, kterou s vámi musíme ihned sdílet:*
>
> *V případě, že jste napadeni a ocitnete se v situaci, kdy musíte pod nátlakem vybrat peníze z bankovního automatu na požádání/přinucení násilníkem, zadejte svůj PIN opačně:*
>
> *to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli.*
>
> *Prosíme, přepošlete toto co nejvíce lidem.*

Jitce se informace příliš nezdála a proto zavolala do svojí banky a sdělila operátorovi informace z mailu. Dozvěděla se, že se jedná o hoax, zpráva je zcela smyšlená a nemá žádný reálný základ.

Co je Hoax?

Hoax je nepravdivá zpráva nebo informace, která se tváří jako ověřený fakt. Obvykle jde o senzační či zdánlivě velmi důležitou zprávu, která se šíří internetem jako lavina. Uživatelé, kteří této informaci uvěří a jednají v souladu s ní, mohou být svým jednáním poškozeni. Pokud zpráva neohrožuje nikoho dalšího, nejlepším řešením je zprávu smazat a dále se jí nezabývat.

Úkol: Napište 5 možností, jak se vypořádat s hoaxy.

Jak rozpoznávat a vypořádat se s hoaxy?

1. Zajímám se o to, co se děje kolem a tudíž mám přehled, co ve skutečnosti platí a co ne.
2. Nesdílím neověřené informace.
3. Umím s pomocí internetu, případně dalších zdrojů (rodič, učitel, odborník) zjistit, který zdroj lze považovat za důvěryhodný.
4. Pokud mne někdo vybízí ke sdílení informace, kterou mám pouze od něho, informaci si nejprve ověřím z více různých spolehlivých zdrojů (např. Hoax.cz, Manipulatori.cz, ověřené zpravodajské servery).
5. Pokud někdo vědomě šíří nepravdivou informaci, která by mohla způsobit nějaké škody, jedná se o trestný čin. Takové jednání neprodleně hlásím Policii ČR.
6. Zprávy čtu pozorně a přemýšlím nad jejich obsahem. Rozvíjím své kritické myšlení.
7. Pokud někdo z mého okolí šíří hoax, upozorním jej na to.

---

10. Zneužití osobních dat

Náš příběh

Karel pravidelně zásobuje na sociálních sítích své přátele humornými komentáři k běžným denním úkonům. Získal si díky tomu i značný počet sledujících osob mimo okruh svých osobních přátel.

Předloni se s rodinou přestěhoval do velkého domu na polosamotě v krásné podhorské oblasti. Dům postupně opravil a jelikož je aktivní hudebník, zařídil si tam i dobře vybavenou zkušebnu. Samozřejmě nezapomněl o každé etapě přestavby důkladně informovat své internetové přátele.

V létě se s manželkou rozhodli vzít děti k moři. Při odjezdu na letiště stihl Karel vyfotit hromadu kufrů před domem a se vzkazem "Teď o mně chvíli neuslyšíte, ale za dva týdny jsem zpět ;-)" poslal fotku na všechny své osobní síťové profily.

Dovolená probíhala podle plánu až do devátého dne. Ráno Karlovi volal soused, že byl dle domluvy nakrmit jeho králíky a našel Karlův dům otevřený. V obýváku chyběla veškerá elektronika a co hůř, hudební zkušebna byla úplně prázdná....

Při vyšetřování policie zjistila, že se Karlův dům stal terčem nájezdu organizované skupiny zlodějů, která si na sociálních sítích tipovala své oběti. Když viděli fotky pěkně vybaveného domu a zjistili, že v něm čtrnáct dnů nikdo nebude, nemohli si takovou příležitost nechat ujít.

Co lze s mými osobními daty dělat?

Zjednodušeně řečeno, pokud má o vás útočník dostatek informací, může s vámi udělat

téměř cokoliv. Extrémním případem je úplné odcizení identity, kdy se někdo další za vás vydává a vaším jménem koná. Může prodat váš dům, půjčit si na vaše jméno peníze, atd. Pokud zloděj ví, že máte doma hezké věci a dozví se, že váš dům není vůbec střežen, je to pro něj snadná kořist. Kdo se dostane k vašemu elektronickému podpisu nebo podpisovému vzoru, může místo vás podepisovat smlouvy či jiné dokumenty.

Jiný druh zneužití je kompromitace či možné vydírání vaší osoby na základě úniku vašich intimních fotografií. Nezáleží přitom, zda se jedná o fotky z domácí koupelny nebo nějakého bujarého večírku, obojí je možné zneužít.

Jak se bránit zneužití osobních dat

1. Na internetu nesdílím žádné důvěrné údaje o své osobě ani o druhých.
2. Vždy zvažuji míru rizika zveřejnění informace. Vysoce rizikové zdaleka nejsou jen fotografie osobních dokladů. Mnoho problémů mohou způsobit i fotky dokumentující dobré majetkové poměry, místo bydliště, moje pravidelné zvyky, atd.
3. Sdílení fotek a videozáznamů, které mi dnes přijdou zábavné, mi v budoucnu mohou uškodit např. při nástupu do zaměstnání. Při jejich sdílení je dobré myslet dopředu.
4. V sociálních sítích používám nastavení soukromí. Nezpřístupňuji všechno všem.
5. Pokud je někde na internetu o mně zveřejněno něco, co by mne mohlo poškodit, požádám správce služby o smazání této informace.
6. Udržuji v bezpečí a nikomu nesděluji přístupové údaje ke všem službám, které na internetu používám.
7. Používám antivirový software a pravidelně aktualizuji zabezpečení svého počítače nebo mobilu.
8. Pokud opouštím na delší dobu byt, je vhodné pověřit spolehlivou osobu, aby na něj dohlédla. Naopak není úplně nejlepší hlásit celému světu, že byt zůstane opuštěný.

SADA NÁPOVĚD

1. Čtěte údaje v řádku s adresou webu. Je-li adresa podezřelá (vypadá jinak než jste zvyklí), stránku raději opusťte a nezadávejte na ní žádná data.
2. Digitální techniku ukládám vždy na bezpečné místo, kde nehrozí poškození vodou, nárazem či vysokou teplotou. V případě rychlého přechodu ze zimy do tepla dochází v přístroji ke kondenzaci, která je nebezpečná pro elektrické obvody. Před spuštěním je vhodné nechat zařízení přizpůsobit teplotě okolního prostředí.
3. Do svého zařízení nevkládejte paměťová média (např. USB externí disky) z neznámých zdrojů.
4. Ignorujte veškeré nabídky z nevyžádané pošty (spamu).
5. Informace o prodejci ověřuji z více nezávislých zdrojů (Má kamenné obchody? Jaké jsou reference na srovnávačích? Co říkají sociální sítě? A co články v médiích?).
6. Instaluji pouze software z ověřených zdrojů.
7. Instaluji pouze software z ověřených zdrojů.
8. Je-li v nevyžádané poště možnost odhlášení (zrušení zasílání), využijte ji
9. Každý počítač by měl být vybaven antivirovou ochranou (např. Avast Free Mobile Security).
10. Klikání na neznámé odkazy v příchozí poště často způsobí, že se vaše adresa dostane do dalších seznamů pro posílání spamu.

11. Málokteré nabídky věcí či služeb “Zdarma” jsou doopravdy poskytnuty zcela nezištně. Ve skutečnosti musíte výměnou poskytnout nějaká svá osobní data (email, věk, adresa…) nebo musíte koukat na reklamy. Někdy to děláte vědomě, v horších případech si data bez vašeho vědomí zjistí skrytý špionský software.
12. Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží).
13. Mám-li o protistraně jakékoli pochybnosti, je lepší obchod neuskutečnit, byť by se zdál sebevýhodnější. Mohu vyzvat protistranu, aby pochybnosti rozptýlila (např. osobní předání zboží).
14. Na internetu nesdílím žádné důvěrné údaje o své osobě ani o druhých.
15. Neměli byste navštěvovat podezřelé stránky, spouštět podezřelé aplikace a otevírat soubory, u kterých není znám původ.
16. Není-li to nezbytné, nevodím neznámé zájemce až k sobě do bytu. Věc lze předat venku či na veřejném místě.
17. Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy.
18. Neotevírám neočekávané přílohy emailů ani neznámé či podezřelé odkazy.
19. Neotevírejte přílohy nevyžádaných emailu nebo zprávy od neznámých kontaktů na Facebooku.
20. Nepoužívám nabíječky či zdroje s poškozeným krytem nebo izolací.
21. Neprodleně reaguji na jakékoliv známky napadení účtu (změním heslo, dočasně umožním přístup jen z jednoho zařízení, atd.).
22. Nesdílím neověřené informace.
23. Nikdy ke svému počítači nepřipojuji USB disky či jiná paměťová média neznámého původu.
24. Nikdy neklikejte na žádné odkazy z nevyžádané pošty (spamu).
25. Obrázek nebo jiný dokument obsahující jakékoli potvrzení o platbě není věrohodný, pokud neobsahuje elektronický podpis (certifikát) toho, kdo potvrzení vystavuje.
26. Online platby provádím pouze ze zařízení, o kterém vím, že je bezpečné.
27. Platbu dobírkou, případně po obdržení zboží akceptuji jen u ověřených nakupujících.
28. Platební údaje k bankovní kartě ukládám odděleně a používám je jen u ověřených prodejců.
29. Platební údaje nenechávám uložené ve svém účtu u obchodníka.
30. Pokud běžné a očekávané zprávy končí ve spamovém koši, upravte whitelist spamového filtru.
31. Pokud je někde na internetu o mně zveřejněno něco, co by mne mohlo poškodit, požádám správce služby o smazání této informace.
32. Pokud mne někdo vybízí ke sdílení informace, kterou mám pouze od něho, informaci si nejprve ověřím z více různých spolehlivých zdrojů (např. Hoax.cz, Manipulatori.cz, ověřené zpravodajské servery).
33. Pokud nakupuji, za zboží předem platím jen v případě ověřených prodejců.
34. Pokud někdo vědomě šíří nepravdivou informaci, která by mohla způsobit nějaké škody, jedná se o trestný čin. Takové jednání neprodleně hlásím Policii ČR.
35. Pokud někdo z mého okolí šíří nepravdivé zprávy, upozorním jej na to.
36. Pokud nemám elektrické zásuvky s přepěťovou ochranou, při bouřce nebo delší nečin-

nosti odpojuji zařízení od elektrické sítě.

37. Pokud opouštím na delší dobu byt, je vhodné pověřit spolehlivou osobu, aby na něj dohlédla. Naopak není úplně nejlepší hlásit celému světu, že byt zůstane opuštěný.
38. Pokud spamovým filtrem prochází určitý druh nevyžádaných zpráv, upravte blacklist filtru.
39. Používám antivirovou ochranu svých zařízení.
40. Používám antivirový software a pravidelně aktualizuji zabezpečení svého počítače nebo mobilu.
41. Používám bezpečná hesla pro přístup k datům.
42. Používám bezpečná, tzv. silná hesla (“JednaDve34pet” je mnohem bezpečnější než “12345”.
43. Používám jen takové elektrické příslušenství, které má homologaci pro použití v naší rozvodné síti s napětím v zásuvce 230 V a kmitočtem 50 Hz. Příslušenství určené pro jiné země nemusí správně fungovat nebo jejich použití může být nebezpečné.
44. Používám ochranné kryty a pouzdra.
45. Používám ochranu proti virům a škodlivému software.
46. Pravidelně provádějte ve vašem antivirovém programu kompletní kontrolu systému. Pokud se na vašem počítači objeví viry, odstraňte je.
47. Pravidelně zálohuji data, nejlépe alespoň na dvou odlišných místech.
48. Pro účely jednorázových a méně důležitých registrací si založte zvláštní emailovou adresu. Odlehčíte tím své hlavní schránce.
49. Před nákupem se snažím o zboží i podmínkách prodeje zjistit maximum (recenze zboží jinde než u prodejce, nezávislé testy, záruční a reklamační podmínky…).
50. Při prodeji bazarového zboží je nejbezpečnější osobní předání na veřejném místě, případně zaslání zboží po platbě předem.
51. Při registraci do nové služby pozorně čtu podmínky zpracování a použití mých dat. Není-li to nezbytné, nepovoluji použití pro marketingové účely.
52. Přístroje, které obsahují data, nenechávám bez dozoru a ukládám je na bezpečných místech.
53. Přístupové údaje k účtům bezpečně ukládám, případně i šifruji.
54. Sdílení fotek a videozáznamů, které mi dnes přijdou zábavné, mi v budoucnu mohou uškodit např. při nástupu do zaměstnání. Při jejich sdílení je dobré myslet dopředu.
55. Snažím zjistit věrohodné reference.
56. Stahujte Android aplikace pouze z oficiálního obchodu Google a aplikace pro iOS u Apple store.
57. Své osobní údaje, heslo nebo bankovní údaje nevyplňujte na neznámých webových stránkách a neposílejte je emailem nebo instant messengery.
58. Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon).
59. Tam, kde v případě prolomení nebo zcizení účtu hrozí větší škody, používám vícefázové ověření přístupu (např. heslo + kód zaslaný na telefon).
60. Udržuji v bezpečí a nikomu nesděluji přístupové údaje ke všem službám, které na internetu používám.
61. Umím s pomocí internetu, případně dalších zdrojů (rodič, učitel, odborník) zjistit, který zdroj lze považovat za důvěryhodný.

62. V sociálních sítích používám nastavení soukromí. Nezpřístupňuji všechno všem.
63. V reálném světě důvěřujte, ale prověřujte. Ve světě kybernetickém spíše nedůvěřujte!
64. V tomto případě se lze bránit zejména neustálým vzděláváním sama sebe, získáním všeobecného přehledu o fungování internetu.
65. Ve vašem mailboxu spam důsledně označujte.
66. Vyhněte se stahování programů z neznámých či nelegálních (warez) zdrojů.
67. Vzhledem k tomu, že se jedná o soubor klamavých technik, které míří spíše na uživatele jako takového, nikoliv na počítače nebo mobilní telefony, nelze se prakticky bránit technologickým zabezpečením. Antivirový program by mohl pomoci v případě trojského koně, ale na podvržené formuláře na webu bohužel nestačí.
68. Vždy zvažuji míru rizika zveřejnění informace. Vysoce rizikové zdaleka nejsou jen fotografie osobních dokladů. Mnoho problémů mohou způsobit i fotky dokumentující dobré majetkové poměry, místo bydliště, moje pravidelné zvyky, atd.
69. Zajímám se o to, co se děje kolem a tudíž mám přehled, co ve skutečnosti platí a co ne.
70. Zařízení s baterií, které delší dobu nepoužívám, občas nechám dobít. Baterie se pomalým tempem sama vybíjí a při dosažení velmi nízké úrovně nabití se podstatně zvyšuje opotřebení baterie a možnost její poruchy.
71. Zboží popíšu co nejpřesněji, aby bylo naprosto zřejmé, co prodávám.
72. Zprávy čtu pozorně a přemýšlím nad jejich obsahem. Rozvíjím své kritické myšlení.

Otázky pro 5. kolo: Zákon a trest

1. Petr dosáhl osmnácti a půl roku věku a právě dostal řidičský průkaz. Otec mu nechtěl půjčit auto, které si vždycky přál řídit, protože bylo plně vybaveno chytrými digitálními technologiemi. Petr si tedy sám vzal klíče a jel se projet. Policie ho přistihla a zjistila, že nemá technický průkaz. Petr se nakonec přiznal, že si auto vypůjčil bez dovolení. Dopustil se trestného činu?

a. **Ano. Bez dovolení užíval cizí věc.**

b. Ne. Auto patří jeho rodině.

c. Ano. Neměl technický průkaz.

d. Ne. Měl více než 18 let.

Podle § 207 zákona č. 40/2009 Sb., trestní zákoník, se ten, kdo se zmocní cizího motorového vozidla s úmyslem užívat jej, dopouští trestného činu. V tomto případě Petr nebyl vlastníkem automobilu. Jízda bez technického průkazu je posuzována jako přestupek. Dosažení osmnácti let je naopak podmínkou pro řízení automobilu.

2. Kolik let má mladistvý pachatel?

a. Dítě, které nedovršilo v době spáchání trestného činu 15 let.

b. Má víc než 18 let a nedovršil v době spáchání trestného činu 21 let.

c. **Má víc než 15 let a nedovršil v době spáchání trestného činu 18 let.**

d. Dítě, které nedovršilo v době spáchání trestného činu 12 let.

Zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže v platném znění, § 2, písm. c) : Mladistvým je ten, kdo v době spáchání provinění dovršil patnáctý rok a nepřekročil osmnáctý rok svého věku.

3. Sedmnáctiletý Patrik spáchal krádež a mimo jiné mu byla uložena ochranná výchova. Co to znamená?

a. Je povinen setrvávat ve školním zařízení i mimo vyučování, nejdéle však do převzetí chlapce některým z rodičů.

b. **Je jedním z ochranných opatření, jejichž účelem je kladně ovlivnit duševní, mravní a sociální vývoj mladistvého a chránit společnost před páchaním provinění mladistvými.**

c. Patrik je povinen se každý den hlásit v určitou dobu na policejní stanici.

d. Určený sociální pracovník navštěvuje pravidelně jeho rodinu a kontroluje, zda rodiče nezanedbávají jeho výchovu.

Zákon č.218/2003 Sb., o soudnictví ve věcech mládeže v platném znění dává možnost uložit mladistvému ochrannou výchovu, mimo jiných i v případě, kdy o výchovu mladistvého není řádně postaráno, dosavadní výchova byla zanedbána, prostředí, ve kterém mladistvý žije, neposkytuje záruku náležité výchovy. Ochranná výchova se vykonává ve výchovných zařízeních. § 22 zákona č. 218/2003 Sb.

4. Nelegální používání softwaru

a. **může být trestným činem**

b. není trestné

c. nepodléhá žádnému zákonu ČR

d. je pouze přestupkem

Používání nelegálně získaného softwaru může být kvalifikováno jako trestný čin podle § 270 trestního zákona č.40/2009 Sb.

Zákon o právu autorském … č. 121/2000 § 2 odst. 1 říká: „Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické…“

Počítačové programy vám nepatří. Stáváte se pouze oprávněným uživatelem po získání (např. zakoupení) licence. Licence zaručuje právo programy používat, nemůžete však instalovat kopie na jiné počítače nebo software poskytovat kamarádům.

5. Ota ukradl ve specializovaném obchodě mobil. Byl přistižen prodavačem. Prodavač jej zadržel a nutil jej setrvat v prodejně do příchodu policie. Jednal prodavač správně?

a. **Ano, osobní svobodu osoby podezřelé ze spáchání trestného činu může omezit každý, pokud je to nutné k zjištění jeho totožnosti, k zamezení útěku nebo k zjištění důkazu. Je však povinen předat ihned tuto osobu policejnímu orgánu.**

b. Ne. Není to trestný čin.

c. Pokud se Ota přiznal, měl jej propustit.

d. Ano. Přistihl jej při páchání trestného činu.

Podle § 76 odst.2 tr.řádu osobní svobodu osoby, která byla přistižena při trestném činu, nebo bezprostředně po té smí omezit, pokud je to nutné k zjištění totožnosti, zamezení útěku, nebo k zajištění důkazů. Je však povinen předat tuto osobu ihned policejnímu orgánu.

6. Student vysoké školy z Říčan si chtěl přivydělat. Zhotovoval kopie softwaru a prostřednictvím inzerce je nabízel k prodeji. Odhadněte, jaký by mu mohl být uložen trest?

a. Pokuta podle zákona o přestupcích ve výši 5 000,-- Kč.

b. trest obecně prospěšných prací

c. trest odnětí svobody v délce trvání 7 let a zabavení počítače odsouzeného

d. **Trest odnětí svobody v délce trvání 2 let a propadnutím věci nebo jiné majetkové hodnoty.**

§ 268 trestního zákona č. 40/2009: neoprávněné šíření softwaru je trestným činem a může být takový člověk odsouzen podle výše škody, kterou způsobí.

7. Zdena přeložila z angličtiny do češtiny texty písní zpěvačky Pink. Nyní chce toto své dílo zveřejnit na internetu. Má na to právo?

a. Ano, je autorkou překladu, tak s ním může nakládat podle svého uvážení.

b. Ne, správně by měla mít svolení autorky již před tím, než začne texty překládat, a k jejich uveřejnění také.

c. Ano, pokud překlad nebude zpeněžovat, nepotřebuje svolení autorky originálních textů.

d. **Pouze se souhlasem autorky původních textů.**

Překladem nejsou práva autora díla přeloženého (původního) nijak dotčena, pouze k nově vzniklému překladu bude mít práva jak autor díla původního, tak i překladatel. Zdena tedy může svůj překlad užít (tj. včetně zveřejnění na internetu) jen se svolením autora díla původního. Pokud by chtěla překlad užít třetí osoba, musela by získat svolení jak od autorky díla původního, tak od Zdeny.

8. Jiří získal pomocí internetu předpremiérový titul nového dosud neuvedeného filmu. Tento film dále kopíruje a pro své kamarády a známé. Jedná se o protiprávní skutek?

a. Ano, protože není povoleno z internetu cokoli kopírovat.

b. **Ano, protože titul byl získán nelegální cestou a šíří jej dále.**

c. Ne, protože za kopie filmu nepožaduje peníze.

d. Ne, protože nepořádá domácí projekci.

Filmy patří mezi díla chráněná autorským zákonem. Za porušení těchto práv se zakládá občanskoprávní i trestněprávní odpovědnost. V občanskoprávním řízení mu může být uloženo, aby se protiprávního jednání zdržel, závadný stav napravil a vydal bezdůvodné obohacení, a to podle § 40 odst. 3 aut. zák. a poskytnul přiměřené zadostiučinění, a to i finanční. Podle závažnosti a rozsahu porušení autorských práv se dopouští přestupku nebo může jít až o trestný čin porušování autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 268 trestního zákona.

9. Marek se chtěl vyhnout zkoušení z fyziky, a tak zatelefonoval řediteli školy a oznámil, že je ve škole ukryta bomba. Z legrace pak ještě telefonoval na nádraží a městský úřad a také oznámil hrozící bombový útok. Policie jej vypátrala a zjistila, že ještě nedovršil 15 let. Bude mít pro Marka nějaké následky, že spáchal čin jinak trestný?

a. **Ano, soud pro mládež může učinit opatření potřebná k jeho nápravě.**

b. Ne, ještě není trestně odpovědný.

c. Ano, bude odejmut rodičům a ti budou odsouzeni za zanedbání výchovy s trestní sazbou skutku spáchaného Markem.

d. Ne, pouze bude pokárán policií.

Trestní zákon spojuje trestní odpovědnost člověka až s dovršením věku 15 let. Dopustí-li se dítě mladší než patnáct let činu jinak trestného, může soud pro mládež učinit "opatření"

potřebná k jeho nápravě, kterými jsou dohled probačního úředníka, zařazení do vhodného výchovného programu a ochranná výchova dle §§ 89 a 93 zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže, v platném znění.

10. Co to je kyberšikana?

a. Ponižování slabších žáků, které se ve škole rozrostlo do většiny tříd.

b. **Druh útoku na jiné jedince pomocí elektronických prostředků jako je mobil, e-mail, internet, sociální síť, atd.**

c. Způsob blokování mailových zpráv od odesílatelů, se kterými si nechceme mailovat.

d. Veškerá šikana ve škole.

Je to druh útoku na jiné lidi pomocí elektronických prostředků jako je mobil, e-mail, internet, sociální síť (např. Facebook), atd. Od běžné šikany se liší tím, že je často anonymní, útok může přijít kdykoliv a její dopad je podstatně větší.

11. Pavlovi se stala nepříjemná věc: někdo mu ukradl heslo k emailovému účtu a začal jeho jménem rozesílat maily. Co by měl udělat?

a. Rozeslat svým známým zprávu to tom, že někdo za něho posílá zprávy.

b. **Změnit heslo.**

c. Nahlásit útok správci mailových serverů.

d. Změnit správce serveru.

Ano, je potřeba co nejdříve změnit heslo. Útočník to obvykle nemůže udělat, protože je to zajištěno tak, že server vám povolí změnit heslo jen po zpětném potvrzení záložním mailem, zodpovězením kontrolních otázek nebo SMSkou.

12. Alena byla hezká dívka, a proto se ráda předváděla na Instagramu. Když jejich dům zloději vykradli, policie ji pak označila za osobu, která přispěla svým neopatrným chováním k vykradení. Jak se to mohlo stát?

a. Její kamarádky věděly, kde bydlí.

b. **Na Instagramu zveřejňovala obrázky, podle kterých si zloději vytipovali dům rodičů a také zjistili, kdy tam nikdo nebyl.**

c. Byla spolčena se zloději.

d. Zvala své kamarádky do domu.

Na Instagramu zveřejňovala obrázky, podle kterých si zloději vytipovali dům rodičů a také zjistili, kdy tam nikdo nebyl. Je potřeba zkontrolovat si, zda nezveřejňuji důvěrné informace, jako je např. obrázek svého bydliště, název ulice, atd.

13. Rodiče se rozhodli, že zřídí Věrce bankovní účet pro mladé. Asi po měsíci Věře přišel mail s logem její banky, ve kterém ji žádali o kontrolu jejích údajů. Věra je poctivě vyplnila včetně všech údajů z kreditní karty. Když druhý den chtěla v knihkupectví platit kartou, zjistila, že na ní nemá žádné peníze. Co se jí stalo?

a. **Došlo k phishingu.**
b. Došlo k rapingu.
c. Došlo k pollingu.
d. Došlo k valorizaci

Phishing (někdy převáděno do češtiny jako rybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. Pamatujte: nikdy nesdělujte své bankovní údaje.

14. Alena večer dokončila úkoly, zkoukla školní web, napsala e-mail týkající se účasti na taneční soutěži. Pak projížděla Instagram a Facebook. Najednou ji přišla zpráva. Nějaký muž ji nabídl přátelství a chtěl s ní debatovat. Souhlasila a byla velmi překvapená a začala mít obavy proto, že o ní tento cizí muž věděl spoustu informací: kde bydlí, do jaké školy chodí atd. Nevěděla, jak je mohl získal. Kde si o ní neznámý muž získat takové informace?

a. Z telefonního seznamu.
b. **Z Instagramu a Facebooku.**
c. Ze školního webu.útok
d. Z mailové korespondence

Z Instagramu a Facebooku. Alena byla na nich velmi aktivní. Z fotek a z Facebooku se dá získat spousta informací, aniž by si to dotyčný uvědomoval. Proto si dávejte pozor na to, co zveřejňujete. Neměla by se z toho dát vyčíst adresa, majetkové poměry vaší rodiny, atd.

15. Občas většina z nás dostane tzv. nevyžádanou reklamu, která je šířená internetem v podobě e-mailu, zprávy na sociální síti, článku na určitém webovém serveru. Proč je nevyžádaná reklama, která se objevuje při surfování na internetu nebezpečná?

a. Za takovou reklamu platíme.
b. **Některé takové reklamy mohou v sobě skrývat viry.**
c. Mohou zjistit naši identitu.
d. Mohou vypnout monitor.

Některé takové reklamy mohou v sobě skrývat viry. Některá vyskakovací okna nebo falešná tlačítka „stáhnout“ nás mohou navést na škodlivé stránky či přímo stáhnout škodlivý software.

16. Olda chtěl na svůj Instagram nahrát novou fotku, ale nemohl se přihlásit. Poté od kamaráda zjistil, že jeho Instagramový účet se změnil: všechny fotky zmizely, jméno bylo změněno a jediný post (příspěvek) odkazoval na škodlivou stránku. Co může Olda udělat?

a. Najde dotyčnou osobu, která mu ukradla účet.
b. Kontaktuje Národní centrum kybernetické bezpečnosti.
c. **Může požádat o obnovu hesla u Instagramové podpory.**
d. Pokusí se účet ukradnout zpět.

Oldovi ukradl účet neznámý útočník. Tento útok se nazývá account hijacking. Pomocí tohoto útoku převezme útočník plnou kontrolu vašeho účtu a získá tím vaše sledující, kterým může posílat podvodnou reklamu. Olda musí Instagramu prokázat svou identitu a může požádat o vrácení stránek do původního stavu.

17. Proč je dobré mít jiné heslo na mail a např. na Facebook?

a. Abychom si zlepšili paměť.
b. Aby nám Facebook neviděl na maily.
c. Mail potřebuje jiný formát hesla.
d. **Pokud nám útočník ukradne Facebookový účet, můžeme si ho pomocí mailu obnovit.**

Pokud nám útočník ukradne Facebookový účet, můžeme si ho pomocí mailu obnovit. Kdybychom používali všude stejné heslo, může nám útočník zamezit jakýkoliv pokus o obnovení přístupu k účtům (Facebook, Google, Instagram).

18. Chytrý vysavač

Rodinka Novákových si pořídila chytrý vysavač. Byli z něj úplně nadšení. V mobilu měli plány jejich domu, kde chytrý vysavač geniálně vysával veškerou špínu. Jednoho dne Novákovým někdo vykradl byt. Zloděj se po domě pohyboval velice jistě, ukradl dokonce i chytrý vysavač. Policie konstatovala, že získal mapy domu z chytrého vysavače.

a. Ne, není
b. Pouze v případě, že by vysavač mapy vyluxoval a zloději by je našli v popelnici
c. **Chytrý vysavač se v případě jeho prolomení se stává doslova špionážní jednotkou**
d. Není, mapy získali zloději naskenování domu Novákových

Některé vysavače mají k dispozici vyšší výkon než chytré mobilní telefony. Vždy záleží, stejně jako u všech ostatních zařízení, na konkrétním typu a produktu. Obecně však platí, že bezpečnost chytrého vysavače je možné prolomit mnoha způsoby. Díky tomu se nenápadný vysavač promění doslova ve špionážní jednotku, která například dokáže zaslat hackerovi přesné mapy místností, ve kterých se pohybuje. I taková kauza už tady byla.

19. Chytrá panenka

Rodiče koupili své dcerce Evičce roztomilou panenku Mílu. Míla patřila mezi tzv. chytré panenky, která byla vybavena Wi-Fi, bluetooth, mikrofonem a schopností mluvit s Evičkou skrze vestavěný reproduktor. Evička byla se svojí panenkou všechen čas.

Po nějaké době si rodiče všimli, že když nebyli v dosahu, tak panenka dává Evičce úkoly, které jejich dcerka plnila, například zjišťovala, kam rodiče ukládají peníze, kde má maminka šperky, jaké mají mobily…

Je možné, aby panenka byla takto naprogramovaná?

a. Ano, je, jedná se o bezpečnostní funkci povinnou pro výrobce chytrých hraček
b. **Ano, je, panenka byla hacknutá a ovládána hackerem**
c. Pokud je v panence umělá inteligence, tak ano
d. Evička mluvila za panenku a rodiče to nepoznali

O tom, že chytrá zařízení jsou při slabém zabezpečení skutečnými mistry špionáže, svědčí i příběhy chytrých hraček. Právě hračky jsou podle různých průzkumů zabezpečeny z výroby jenom velmi slabě. Představte si, že s vámi začne mluvit váš oblíbený plyšák nebo panenka, chce se s vámi kamarádit, anebo vám postupně začne diktovat, co a jak máte udělat.

20. Legrácka

Kamil byl 17ti letý student průmyslovky a známý vtipálek, který když mohl, tak někomu něco vyvedl. Vyznal se dobře v digitálních technologiích a tyto dva koníčky dokázal pospojovat. Jednou si o Milana půjčil jeho Notebook a věděl, že ve správě hesel najde jeho hesla na různé stránky. Nemýlil se, byly tam. Kamil tak Milanovi změnil řadu nastavení a nejen to, objednal mu placené služby, včetně nového tarifu v mobilu. Nějakou dobu se pak bavil nad tím, jak je Milan zmatený ze zpráv, informací a věcí, které mu přicházejí. Jakmile jednoho dne přišel do třídy otec Milana spolu s policií a začalo vyšetřování Milanovi škody, která přesahovala 10500 korun.

Čeho se Kamil dopustil?

a. Trestného činu
b. **Přestupku**
c. Ničeho, ještě mu není 18 let
d. Ničeho, není zde úmysl poškodit druhou osobu

Kamil se dopustil přestupku podle Zákona 251/2016 o přestupcích, protože úmyslně neoprávněně užíval cizí věc. Jelikož ale způsobil školu nikoliv malou, kdy hodnota škody přesahovala částku 10000,- Kč, od které je čin kvalifikován jako trestný čin.