Kapitola

[Počítačová kriminalita]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: [bit cz training s.r.o.]
Poslední úprava: [26.06.2020]

Funded by the
Erasmus+ Programme
of the European Union

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

Počítačová kriminalita

Úvod

Určitě se Vám také někdy stalo, že jste obdrželi e-mail, ve kterém Vás odesílatel žádá o změnu hesla k bankovnímu účtu, o zaplacení nějakých nedoplatků či dluhů. Takový e-mail nevypadá velmi věrohodně, není jasné, která osoba či instituce Vám jej zaslala a gramatika dost pokulhává. Většina lidí na takovýto podezřelý e-mail reaguje jen ze strachu, že něco opravdu zapomněli zaplatit a že ignorování e-mailu pro ně bude znamenat další problémy. Čeká je však nemilé překvapení. Dlužná částka byla samozřejmě podvrh a poškozená osoba teď musí navíc řešit odcizený bankovní účet. Dalším příkladem počítačové kriminality je pirátství na internetu. Internetoví piráti nelegálně zdarma užívají programy a neberou ohled na autorská práva nebo cenu, kterou za programy musí platit ostatní uživatelé.

Počítačová kriminalita je dlouhodobý problém, který je neoddělitelně spjat s online světem. Nezákonné aktivity spojené s užíváním počítače, ať už je počítač použit jako nástroj, cíl nebo prostředek k vykonání nějakého trestného činu, se řadí pod pojem počítačová kriminalita. Obecná definice počítačové kriminality zní takto: „nezákonné činy, při kterých je počítač použit jako nástroj, cíl nebo obojí" (IT Act 2000). Pod tento druh kriminality spadá široká škála trestných činů včetně těch mířených na počítačové systémy a počítačová data, padělání nebo podvody spojené s počítači, přestupky spojené s obsahem na internetu nebo autorským právem. Díky naší neustále rostoucí závislosti na počítačích a digitálním světě se technologie stávají lákavějším a snadnějším cílem pro zločince, buď jako způsob získávání informací, nebo jako prostředek k vyvolání chaosu a napáchání škod.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Nastudováním této kapitoly si osvojíte definice hlavních pojmů spojených s kriminalitou v kyberprostoru, dokážete rozeznat různé druhy a metody počítačové kriminality a jak se před nimi chránit. Dále se dozvíte, jak tyto nástrahy ohrožují děti i dospělé.

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

1. Jakou roli hraje počítačová kriminalita na internetu?

Počítačová kriminalita je pravým opakem počítačové bezpečnosti. Jedná se o široké spektrum škodlivých a nelegálních aktivit, které jedinec provádí pomocí počítače a internetu. Tato kapitola Vám pomůže lépe porozumět počítačové kriminalitě a poradí Vám, jak chránit sebe, své děti a své pracovní prostředí.

Většinu zločinů souvisejících s počítačovou kriminalitou páchají kyberzločinci nebo hackeři za účelem krádeže či vydělání peněz. Kyberzločiny páchají jak jedinci, tak organizace. Někteří zločinci pracují organizovaně, používají vyspělé technologie a metody a jsou velice technicky zdatní. Existují také zločinci, kterým nejde o peníze a kteří se dopouštějí nelegálních aktivit pouze z politických či osobních důvodů.

Co znamená pojem počítačová kriminalita? Termínem počítačová kriminalita se označují trestné činy, při kterých je počítač předmětem trestného činu, (hacking, phishing, spamming) nebo se používá jako nástroj k páchání trestného činu (dětská pornografie, zločiny z nenávisti).

Mezi projevy počítačové kriminality patří:

- E-mailové a internetové podvody
- Krádež identity (zločinec ukradne a zneužije osobní údaje jedince)
- Krádež peněz nebo údajů k platební kartě
- Krádež a následný prodej firemních dat
- Online vydírání (požadování peněz výměnou za nespáchání útoku)
- Ransomware útoky (druh online vydírání)
- Cryptojacking (nelegální těžba kryptoměny)
- Kyber-špionáž (hackeři získají přístup k firemním či vládním informacím)

Dle výše uvedených příkladů můžeme rozdělit počítačovou kriminalitu do těchto dvou největších skupin:

1. cílem trestného činu je počítač připojený do sítě; útok je mířen na důvěrnost, integritu a dostupnost sítě

2. trestný čin spáchaný za pomoci počítače připojeného do sítě a souvisejících informačních a komunikačních technologií, patří sem útoky jako např. krádeže, podvody a padělání

Následující text pojednává o trestných činech spáchaných za pomoci počítače.

Pojem počítačová kriminalita zahrnuje různé skupiny a kategorie. Druhy počítačové kriminality slouží k charakterizaci trestných činů (jako např. phishing) a jsou rozděleny do následujících kategorií. Hlavním kritériem této typologie je předmět právní ochrany. Jedná se o: „trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů"; „trestné činy související s obsahem"; a „trestné činy související s autorskými právy". Čtvrtá kategorie „trestné činy související s počítačem" se nezaměřuje na předmět právní ochrany, ale na metodu použitou ke spáchání trestného činu. To může vést k určitému překrývání mezi kategoriemi

Kategorie počítačové kriminality

Podívejme se na jednotlivé kategorie zblízka:

Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
Všechny trestné činy v této kategorii jsou zaměřeny proti jedné ze tří právních zásad důvěrnosti, integrity a dostupnosti sítě.

- Nelegální přístup (hacking, cracking)
- Nezákonné odposlouchávání (osoba na něj nemá právo)
- Nezákonné nakládání s daty (zadávání škodlivých kódů, např. virů)
- Zásahy do systému (vkládání, přenos, poškozování, mazání, znehodnocování, pozměňování nebo zadržování počítačových dat, např. viry, které zastavují nebo zpomalují počítačové systémy)

Příklad
V roce 2017 došlo k útoku WannaCry, za kterým údajně stála Severní Korea. Předmětem útoku bylo vypuštění ransomwaru, který měl za úkol uzamknout obsah na zařízení uživatele a rychle se šířit dál. WannaCry napadl 300 000 počítačů po celém světě a uživatelé byli nuceni zaplatit stovky dolarů, pokud chtěli dostat své údaje zpět.

Trestné činy související s počítačem
Do této kategorie řadíme činy spáchané za pomoci počítače. Na rozdíl od předchozí kategorie, ochrana právních zásad není u těchto trestných činů tak přísná.

- Počítačové podvody
- Padělání související s počítačem
- Phishing
- Krádež identity
- Zneužití zařízení

Příklad
Mezi lety 2013 až 2016 došlo u společnosti Yahoo k narušení dat, které vedlo k odcizení 3 miliard uživatelských účtů. U některých z těchto účtů se útočníci zmocnili soukromých informací a hesel k uživatelským účtům v jiných online službách. Většina těchto údajů je dnes k dispozici na temném webu, ať už zdarma nebo za určitou cenu.

Trestné činy související s obsahem

Tato kategorie zahrnuje:

- Erotický či pornografický materiál
- Dětskou pornografii
- Xenofobní materiál – rasismus, nenávistné projevy a obsah vyzdvihující násilí
- Urážky související s náboženskými symboly
- Hazardní a nelegální online hry
- Pomluvy a šíření nepravdivých informací
- Spam a podobné hrozby

Vývoj právních nástrojů k řešení trestných činů v této kategorii je podstatně ovlivněn národními postoji, které zohledňují kulturní a právní zásady. Co se týče nelegálního obsahu, morální a právní zásady se značně liší mezi jednotlivými společnostmi.

Příklad
Matthew Falder, notoricky známý pedofil (člověk, kterého sexuálně přitahují děti a nezletilí), je britský akademik s doktorátem z Univerzity v Cambridgi, který byl v roce 2017 obviněn z více než 137 trestných činů spáchaných proti 46 osobám. Tato obvinění mimo jiné zahrnovala úmyslné pobízení k znásilnění a sexuálním aktivitám s dítětem, sexuálnímu vykořisťování dětí a držení a distribuce dětské pornografie (Dennison, 2018; Vernalls a McMenemy, 2018). Své oběti vydíral a nutil je k tomu, aby na sobě a na jiných páchaly a zároveň natáčely či fotily všemožné ponižující, odporné a surové činy (např. sebepoškozování, olizování špinavého toaletního kartáče). Tyto fotografie a videa následně sdílel na hurtcore stránkách (např. Hurt 2 the Core, dnes již nefunkční), které se zaměřují na znásilňování, vraždění, sadismus a pedofilní obsah (McMenemy, 2018).

Trestné činy související s autorskými právy

Digitalizace otevřela dveře novým způsobům porušování autorských práv. Mezi nejčastější patří vzájemné vyměňování skladeb, souborů a softwarů chráněných autorskými právy prostřednictvím systémů k sdílení souborů nebo webhostingu a obcházení systému Správy digitálních práv (DRM). Podobné jednání bývá ve společnosti obecně tolerováno, přestože se stále jedná o trestné činy, nicméně lidé by měli brát v potaz následky, které pro ně z takového nelegálního chování mohou plynout.

Příklad
Nejčastějším příkladem trestných činů souvisejících s autorskými právy je užívání nelegálních kopií softwarů pro vlastní účely nebo stahování hudby a filmů z veřejně přístupných online obchodů (např. ShareRapid, MegaRapid).

1. Procvičte si znalosti

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

Cvičení ANO/NE

Související dílčí výukový cíl: DVC_Víte, jakou roli hraje počítačová kriminalita na internetu.01_01: Dokážete rozeznat rozdíly mezi jednotlivými druhy počítačové kriminality

Zadání: Veškerou hudbu a filmy uveřejněné na internetu si mohu legálně stáhnout.
Úkol: Rozhodněte, zda je uvedené tvrzení pravdivé či nikoliv:

a. ano
b. ne

2. Metody a příklady kybernetických útoků

V přecházejícím textu jsme si prohlédli 4 kategorie, do kterých dělíme počítačovou kriminalitu. Nyní se podíváme zblízka **na roli, kterou hrají počítače v počítačové kriminalitě, a na různé způsoby útoků v kyberprostoru:**

Počítače mohou hrát v trestné činnosti 4 různé role – slouží jako předmět, činitel, nástroj nebo symbol. Počítače jsou předmětem zločinu, pokud jsou narušeny nebo ukradeny. Roli činitele mají v případech, kdy jsou prostředkem ke spáchání trestného činu. Do této skupiny řadíme útoky počítačových virů nebo automatizované útoky. Další rolí počítačů v trestné činnosti je role nástroje, které umožňují zločincům vytvářet falešné informace nebo plánovat a řídit zločiny. Počítače jsou také používány jako symboly, které mají oběti oklamat.
Nejobvyklejší rolí počítačů v trestné činnosti je role činitele. Nejčastější metody užití počítače jako subjektu jsou:

- malware
- hackerství
- spam
- phishing
- DDoS útoky

Nejčastější metody útoků

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

Definice
 ***Malware*** je jednotný název pro všechny škodlivé softwary, které se šíří mezi počítači a narušují jejich činnost. Hlavním cílem malwaru je ničit obsah, např. mazat soubory a způsobovat výpadky systému, nebo krást osobní údaje.

Existuje mnoho typů malwaru, např.:

- **Počítačový virus =** může způsobit mírné změny ve fungování počítače, ale také vážnější problémy jako například poškození či poničení hardwaru, softwaru nebo souborů.
- **Počítačový červ =** program, který je schopný automaticky rozesílat kopie sebe sama na jiné počítače, aniž by k tomu potřeboval hostitele nebo zásah člověka. Počítačový červ je tedy schopen zničit celou síť, a tím pádem může být jeho dopad vážnější než u virů.
- **Trojský kůň =** druh malwaru, který se na první pohled tváří jako skutečný program. Jedná se však o podvrh, který umožňuje útočníkům nezákonný přístup k počítači. Z napadeného počítače může bez vědomí uživatele krást údaje a oklamat ho vykonáváním na první pohled rutinních úkolů, pod jejichž záminkou však doopravdy provádí skrytou neoprávněnou činnost.
- **Spyware =** software, který narušuje soukromí uživatelů shromažďováním citlivých nebo osobních údajů z napadených systémů nebo monitorováním stránek, které uživatel navštěvuje.

Definice
 Hacking ***Hacking neboli hackerství*** je proces, jehož výsledkem je narušení soukromí a získání důvěrných informací. Při tomto procesu jsou rozpoznány slabiny systému nebo mezery v síti a je zajištěn přístup k soukromým údajům. Hackování je proto také známé jako neoprávněné narušení.

Hacking nemusí být vždy vnímán jako škodlivý. V mnoha případech mají hackeři dobré úmysly a jde jim o dobrou věc. Takový druh hackingu se nazývá etický hacking a používá se např. k zabezpečení operačního systému.

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

Hackery je možno rozdělit do různých kategorií podle toho, jaké úmysly se za jejich činností skrývají, např. white hat hackeři (etický hacker), black hat hackeři (neetický hacker) a grey hat hackeři (kombinace dvou předchozích).

White Hat hackeři – Etičtí hackeři
 Jejich záměrem není poškození systému, ale odhalení slabin počítače či sítě jako součást kontroly zranitelnosti a penetračních testů systému. Etické hackování není nelegální a jedná se o jedno z náročnějších zaměstnání v IT světě. Spouska firem najímá etické hackery pro vykonávání výše zmíněných kontrol a testů.

Grey Hat hackeři
Jedná se o kombinaci black hat hackerů a white hat hackerů. Za jejich chováním se neskrývá škodolibý záměr, ale jen tak pro zábavu využívají slabin v zabezpečení počítačového systému, aniž by o tom věděl nebo s tím souhlasil jeho majitel. Jejich cílem je upozornit majitele na slabinu a získat uznání či odměnu. 

Black Hat hackeři – Crackers
 Tato skupina hackerů jedná za účelem získání neoprávněného přístupu do systému a poškození jeho provozu nebo za účelem krádeže citlivých informací. Black Hat hackování je díky svému zlomyslnému záměru vždy nelegální. Patří sem např. krádež firemních dat, narušení soukromí, poškození operačního systému, blokování síťové komunikace atd.

Definice
 ***Spam*** je nevyžádaný e-mail, který je obvykle odesílán hromadně velkému množství příjemců po celém světě. Často souvisí s farmaceutickými výrobky nebo pornografií. Spam se také používá k odesílání phishingových e-mailů nebo malwaru.

Zločin se neustále vzdaluje tradičním metodám, jako jsou násilí, drogy nebo krádeže, a začíná převládat trestná činnost na internetu. To souvisí se současným trendem online nakupování a komunikace na internetu. Oběti těchto trestných činů mohou ztratit cokoliv, co má nějakou hodnotu – bezpečí, klid, peníze nebo majetek.

Exkurz
První studie zkoumající emoční dopady počítačové kriminality ukázala, že mezi nejsilnější emoční reakce obětí patří vztek (58 %), zlost (51 %) a pocit podvedení (40 %) a v mnoha případech dokonce oběti z viní z útoku samy sebe. Pouze 3 % lidí si myslí, že se jim něco podobného nemůže stát, a skoro 80 % neočekává, že budou zločinci předvedeni před soud, což má za následek pocit bezmoci a ironickou neochotu jednat.

Definice

Phishing **-** Phishingová kampaň je hromadné rozesílání spam e-mailů nebo jiných forem komunikace. Jejím účelem je nalákat příjemce k tomu, aby udělali něco, co naruší jejich bezpečnost v soukromém životě nebo v práci. Phishingové zprávy mohou obsahovat zavirované přílohy, odkazy na škodlivé weby nebo mohou chtít od příjemce získat důvěrné informace.

Příklad
Známý phishingový incident se stal v roce 2018 během Mistrovství světa ve fotbale. Podle zpráv Inc podvod zahrnoval spam e-maily, které nabízely fanouškům zdarma cestu do Moskvy, kde se Mistrovství ve zmíněném roce konalo. Lidé, kteří rozklikli odkaz obsažený v e-mailu, přišli o své osobní údaje.

Definice
Distribuované DoS útoky (DDoS) jsou druhem útoků, při kterých se zločinci snaží zničit systémy nebo sítě. Někdy se ke spuštění DDoS útoku využívají připojená IoT (Internet of Things = Internet věcí) zařízení. DDoS útok zahltí systém velkým množstvím požadavků k připojení pomocí standardních komunikačních protokolů a tím jej znefunkční.

Příklad
Známým útokem tohoto typu je útok na webovou stránku Britské národní loterie z roku 2017. Tento útok zamezil připojení k webové stránce a mobilní aplikaci a tím zabránil občanům v hraní.

Mezi nejčastější trestné činy počítačové kriminality patří:

Předstírání identity na internetu

Jedná se o jeden z nejčastěji páchaných trestných činů na internetu. Pro tento čin je význačné využití jména, internetové domény, telefonního čísla nebo jiných údajů cizí osoby bez jejího souhlasu. Účelem je spáchání podvodu nebo způsobení újmy.

Příklad
Kláru začali na internetu obtěžovat cizí lidí poté, co někdo vytvořil pod jejím jménem příspěvek nabízející sexuální služby. Příspěvek zahrnoval osobní údaje včetně jejího telefonního čísla a adresy bydliště.

Kyberstalking

Fyzický stalking zahrnuje pronásledování, tajné pozorování, ustavičné telefonování a posílání zpráv a další způsoby, jak se přiblížit k oběti bez jejího vědomí a očekávání. Kyberstalking se liší tím, že se toto nechtěné pronásledování odehrává online – na e-mailu, sociálních sítích, v chatovacích místnostech, využitím osobních údajů dostupných na internetu a čehokoliv dalšího, co lze na internetu dohledat a co může kyberstalker použít k zprostředkování kontaktu se svou obětí.

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

Příklad
Poté, co se rozešli, začal John pronásledovat svou ex-přítelkyni za pomoci jednorázového telefonu se zapnutou GPS, který ukryl v jejím autě. Do telefonu se přihlásil na internetu, což mu umožnilo sledovat veškeré její aktivity. Dále také John volal své ex-přítelkyni více než dvěstěkrát denně.

Kyberšikana

Kyberšikana je užívání sociálních sítí k zastrašování, obtěžování, vyhrožování a shazování druhých. Obecně platí, že pokud osoba používá internet nebo jakoukoli jinou formu elektronické komunikace k ohrožování, obtěžování nebo zastrašování jiné osoby, lze toto chování považovat za trestný čin.

Příklady
Cestou ze zápasu rozešle chlapec ostatním spoluhráčům ponižující fotografii dívky, kterou potkal na kluzišti. Fotku následně přidá na Facebook odkud se šíří dál. Tři spoluhráči pošlou Pavlovi zprávy, ve kterých Pavla obviňují z prohry celého týmu a z toho, že vůbec neumí hrát. Pavel se bojí cokoliv říct trenérovi nebo rodičům, a tak raději šikanu trpí po celou hokejovou sezonu. Příští sezonu se již k hokeji nevrátí.

Jaký je rozdíl mezi kyberšikanou a kyberstalkingem?

Kyberšikana	Kyberstalking
Kyberšikana se vyznačuje neustálým kontaktem se zaměřenou osobou – jejím urážením a pomlouváním. Útočník například vytvoří na Facebooku skupinu s názvem “Nenávidím…” a pozve všechny své přátele, aby se připojili.	Kyberstalking je posedlost vyznačující se snahou dozvědět se co nejvíc informací o určité osobě bez jejího vědomí. Útočník například zjistí, kde se oběť narodila, s kým je v manželském svazku atd.

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

Krádež identity a krádež dat

Krádež identity je krádež osobních identifikačních údajů za účelem spáchání trestných činů, jako například: zřízení úvěrové linky, pronájem domu, nákup zboží nebo služeb, aukce a mzdové podvody nebo vydírání.

Krádež dat je nezákonné držení citlivých údajů jako jsou například: nešifrované informace o platebních kartách, obchodní tajemství, duševní vlastnictví, zdrojový kód, informace o zákaznících a záznamy o zaměstnancích.

Příklad
V roce 2018 byl řetězec hotelů Marriott napaden hackery a bylo odcizeno 383 milionů záznamů o hostech a přes 5 milionů čísel cestovních pasů. Ukradené údaje byly prodány na černém trhu a kdokoliv je může zneužít nebo použít k vytvoření nové identity.

Finanční kriminalita

Tento druh zahrnuje aktivity, které nečestně vytvářejí bohatství pro zapojené osoby. Jedná se o využívání důvěrných informací nebo podvodné nabývání majetku jiné osoby za účelem zajištění hmotného prospěchu. Za finanční kriminalitu se považují: podvod, praní špinavých peněz, úplatkářství, korupce a další.

Příklad
Mezi nedávné významné finanční zločiny patří například incident Enron, při kterém se energetická společnost Enron dopustila rozsáhlých podvodů a korupce. Dále například investiční skandál Bernieho Madoffa. B. Madoff dlouhou dobu předstíral, že vede úspěšnou investiční firmu, přitom kradl peníze nových klientů a dával je těm starším (tato činnost se nazývá Ponziho schéma a Madoff vedl největší takovéto schéma v celé historii). Madoff byl usvědčen z mnoha trestných činů včetně praní špinavých peněz a různých druhů podvodů.

S počítačovou kriminalitu se často můžete setkat ve Vašem okolí – například v zaměstnání. Podvod, kterého se jedinec dopouští proti společnosti, se nazývá interní podvod. Při tomto typu podvodu se pachatel dopouští činností, jejichž cílem je okrást společnost, zpronevěřit majetek nebo obejít předpisy, zákony nebo zásady společnosti. Interní podvod například zahrnuje činnosti jako úmyslné neohlášení transakcí, provádění neoprávněných transakcí a úmyslné nesprávné označování pozic.
Interní podvod lze rozdělit do dvou kategorií – zpronevěra a krádež identity. V případě zpronevěry jsou peníze odcizeny přímo ze společnosti, zatímco při krádeži identity hrají roli osobní údaje zákazníka, které zaměstnanec zneužije ve svůj prospěch. Mezi příklady interních podvodů patří:

- Krádež peněz zákazníka
- Zneužití kreditních údajů zákazníka
- Praní špinavých peněz
- Podvod při zadávání zakázek
- Krádež dat

Podvodné aktivity páchané jedinci mimo společnost se naopak nazývají externí podvody. Jedná se o krádež peněz nebo akcií osobami mimo podnik. Mezi příklady externích podvodů patří:

- Krádež identity – převzetí kontroly nad virtuální identitou jedince

- Falšování fakturačních údajů (např. pozměnění čísla účtu příjemce)
- Falšování údajů na objednávce tak, aby zboží bylo zasláno na nesprávné místo doručení
- Imitace hlasu konkrétní osoby nebo falšování jejího podpisu
- Falšování e-mailů

Za každým kybernetickým útokem se skrývá určitý **záměr**. Tyto záměry se pohybují v rozmezí od umírněných po nemilosrdné. Mezi 4 nejtypičtější patří:

- vandalismus (běžné útoky na vládní stránky)
- propaganda (šíření politických zpráv zejména prostřednictvím internetu)
- odepření přístupu (útoky např. proti ozbrojeným silám, které pro komunikaci používají počítače a satelity)
- síťové útoky na infrastrukturu (útoky na přenosové systémy energetických, plynárenských, teplárenských a ropných společností a společností v komunikační infrastruktuře, které jsou citlivé na kybernetické útoky atd.)

2. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Víte, jakou roli hraje počítačová kriminalita na internetu.01_02: Dokážete vyjmenovat metody útoků v kyberprostoru.

Zadání: Co je to Distribuovaný DoS (DDoS) útok?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

a) masové rozesílání spam e-mailů nebo jiných forem komunikace
b) druh kybernetického útoku, při kterém zločinci znefunkční systém nebo síť
c) nevyžádaný e-mail rozesílaný hromadně velkému množství příjemců po celém světě
d) zneužití bezpečnostních chyb v síti k neoprávněnému přístupu nebo použití počítačů a síťových zdrojů

Cvičení /JEDNA MOŽNOST/

Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

Zadání: Jakými aktivitami se zabývá tzv. “grey hat hacker”?

a) šířením nepravdivých informací o druhé osobě
b) krádeží osobní údaje
c) získáváním přístupu do cizího systému jen tak pro zábavu
d) finanční kriminalitou

Cvičení /JEDNA MOŽNOST/

Související dílčí výukový cíl: DVC_Víte, jakou roli hraje počítačová kriminalita na internetu.01_03: Dokážete popsat, co je to interní a externí podvod.

Zadání: Kdo se dopouští tzv. interního podvodu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

a. Interního podvodu se dopouští dodavatelé v případě, že nedodají objednané služby či zboží včas.
b. Interní podvod zahrnuje aktivity jako kybergrooming nebo kyberšikana.
c. Interního podvodu se dopouští zaměstnanci v případě provádění nepovolených finančních transakcí.
d. Interního podvodu se dopouštějí zákazníci podáním neoprávněné reklamace.

3. Důsledky počítačové kriminality

Počítače lze mimo jiné použít i k páchání trestných činů ve skutečném světě (porušení práv duševního vlastnictví, podvody s kreditními kartami, podvody s převodem peněz, pornografie atd.) a dokonce i k terorismu. Teroristé využívají informační technologie k naplánování a uskutečnění svých útoků. Takovéto chování se označuje termínem **kyberterorismus**. Mezinárodní nárůst používání IT technologií vede k zvýšení kriminality a terorismu. Díky vyspělým komunikačním technologiím lidé ani nemusejí být v jedné zemi, aby mohli společně naplánovat nějaký zločin. Zločinci a teroristé jsou schopni najít bezpečnostní mezery v systémech a provozovat svou činnost z neobvyklých míst po celém světě.

V budoucnu bude většina mezinárodních incidentů, ať už vojenských či špionážních, probíhat v kyberprostoru. Proto je na čase začít vyhodnocovat závažnost těchto hrozeb. V současné době se diskutuje o možnosti, že kyberútoky vyústí ve válečný konflikt, při kterém může dojít k ničení, újmě na zdraví, škodě na majetku nebo ztrátám na životech. Problém je v tom, že je skoro nemožné přiřadit určitý útok konkrétnímu státu. Jak již bylo zmíněno, útočník může zdánlivě připravovat útok z místa, na kterém se ve skutečnosti nemusí vůbec nacházet. Bez spolupráce mezi státy není možné skutečného útočníka odhalit.

Důsledky počítačové kriminality

Dopady počítačové kriminality mohou být velice zničující kvůli vysokému riziku ztráty dat a financí.

Pro jednotlivce
Počítačová kriminalita může mít velký dopad na jednotlivce: narušení dat, krádež identity, problémy se zařízením. Můžete se setkat s podezřelými platbami na Vašem účtu v důsledku krádeže identity, ransomware útokem, který po Vás bude požadovat vysokou finanční částku výměnou za ukradené soubory, nebo vysokými poplatky za internet nebo elektřinu kvůli cryptojackingu či botnetům. Pokud se jedná o kyberšikanu nebo sexuální obtěžování, útočníkům ani nemusí jít o peníze a následky mohou být ještě horší.

Pro podniky a vládní orgány
Pro podniky, vládní orgány nebo zdravotnické organizace jsou častými důsledky počítačové kriminality ztráta citlivých údajů, finanční zatížení a poškození dobrého jména firmy či organizace. V roce 2019 průměrný ransomware útok požadoval od malých až středně velkých podniků 5 900 dolarů výměnou za vrácení odcizených souborů či odemknutí systému. Takovýto výpadek systému stojí postižené podniky průměrně kolem 141 000 dolarů. Tyto částky se však ani zdaleka nevyrovnají těm, které se objevují při útocích na vládní orgány. Například při útoku na okres Jackson v Georgii, zločinci požadovali 400 000 dolarů za obnovu vládního IT systému a infrastruktury.

Dalším důležitým pojmem je **kybernetická válka**. Pojďme se na dva zmíněné termíny podívat zblízka:

Co je to kyberterorismus?	**Co je to kybernetická válka?**
Pojem počítačová kriminalita se často zaměňuje s kyberterorismem. Kyberterorismus vždy představuje závažnější jednání v nebo prostřednictvím kyberprostoru. Organizace NATO definuje kyberterorismus jako: "kybernetický útok, při kterém je využíván nebo zneužíván počítač či komunikační síť za účelem zničení nebo narušení, které má vyvolat strach nebo zastrašit společnost v ideologický cíl."	Kybernetická válka je využití či zacílení počítačů a sítí při válečných konfliktech. Zahrnuje jak ofenzivní, tak defenzivní operace související s kybernetickými útoky, špionáží nebo sabotérskými činy. Kybernetická válka je definována jako: "jednání jednoho státu za účelem proniknutí do počítačů či sítí druhého státu ve snaze poškodit nebo narušit jeho systém."

Příklad
Kybernetická válka včetně síťových útoků nabyla po 11. září na vážnosti. Situace po útocích z 11. září 2001 započala debatu o využití informačních a komunikačních technologií teroristy. Tuto debatu podpořilo zjištění, že pachatelé k přípravě útoků použili internet. Přestože se přímo nejednalo o kybernetické útoky, internet v jejich přípravě sehrál velkou roli. V této souvislosti byly objeveny různé způsoby využití internetu teroristickými organizacemi.

3. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Zadání: Který kybernetický útok páchaný mimo virtuální svět je nejhorší?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

c. podvod s platebními kartami
d. pornografie
e. kyberterorismus
f. krádež identity

Cvičení /VÍCE MOŽNOSTÍ/

Zadání: Jaký dopad může mít počítačová kriminalita na jednotlivce?
Úkol: Vyberte správné odpovědi – více odpovědí může být správně.

a. Krádež identity
b. ztráta práce
c. zdravotní problémy
d. ztráta dat

Cvičení /DOPLŇTE SLOVO DO ZÁVORKY/

Úkol: Doplňte správnou odpověď do závorky zadáním přesného tvaru slova bez dalších možností.

Pro_____jsou častými důsledky počítačové kriminality ztráta citlivých údajů, finanční zatížení a poškození dobrého jména.

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

4. Možnosti prevence a ochrany

Za počítačovou kriminalitu se považuje vše od krádeže peněz, krádeže osobních nebo finančních údajů po poškození či zničení důležitých firemních nebo soukromých dat. Bohužel pro nás, hackeři a jiní pachatelé jsou čím dál tím prozíravější.
Jak nejlépe ochráníte svůj počítač a své osobní údaje?
Nejlepším způsobem ochrany je prevence. Mějte na paměti těchto 5 klíčových bodů bezpečnosti na internetu: **Obezřetnost, Prevence, Ochrana, Udržení a Vytrvalost**.

Tyto body jsou obsaženy v následujících krocích:

1. Vyhněte se sdělování svých osobních údajů na internetu a v e-mailech.
2. Pečlivě zvažte přidávání fotografií na internet – kdokoli je může kdykoli použít v jiném kontextu
3. Nastavte si silná hesla

4. Užívejte a pravidelně aktualizujte antivirové programy
5. Neposílejte číslo a heslo Vaší kreditní karty přes e-mail
6. Hlídejte, jaké webové stránky Vaše děti navštěvují
7. Zálohujte si svá data a předejděte tak jejich ztrátě při napadení virem
8. Používejte bezpečnostní program, který Vám umožní spravovat soubory cookie
9. Pravidelně aktualizujte software a operační systém
10. Nikdy neotevírejte přílohy ve spam e-mailech
11. Neklikejte na odkazy ve spam e-mailech nebo na nedůvěryhodné stránky
12. Kontaktujte přímo společnost ohledně podezřelých požadavků
13. Dohlížejte na své bankovní výpisy
14. Dávejte si pozor na to, jaké stránky navštěvujete

Jak rozpoznat bezpečné stránky?

Tyto 3 níže uvedené tipy Vás zbaví nejistoty a naučí Vás, jak zaručeně rozpoznat, zda je stránka důvěryhodná či nikoli. Nejprve se naučíte pár jednoduchých vizuálních kontrol, které Vám na první pohled poskytnou užitečné informace. Dále se dozvíte, jaké existují bezpečností nástroje, které byste na webových stránkách měli mít a které Vám poskytnou informace a navedou Vás. Nakonec Vás naučíme, jak provést důkladný průzkum, pokud si s nějakou stránkou stále nejste jisti. Tak se do toho pusťme, ať znovu můžete bez obav surfovat po internetu.

1 - Vizuální kontrola bezpečnosti webových stránek

- Překontrolujte URL adresu — Začneme s nejjednodušším tipem. Nejsnazší je se ujistit, že URL adresa nevypadá podezřele. Předtím, než nějaký odkaz rozkliknete, najeďte na něj myší a v levém dolním rohu zkontrolujte, zda vše vypadá v pořádku. Hlavní zásadou phishingových útoků je vypadat co nejvěrohodněji. Na první pohled se URL adresa nemusí zdát falešná, při bližším prozkoumání však můžete odhalit, že místo "l" je zapsaná "1" nebo místo ".com" končí adresa ".net". Naučte se každou adresu zkontrolovat, než ji rozkliknete nebo než na ní začnete zadávat osobní údaje jako jsou uživatelské jméno a heslo.
- Zkontrolujte, zda adresa obsahuje https — Zkratka http, kterou vidíte na začátku každé URL adresy, znamená Hypertext Transfer Protocol (česky protokol pro přenos hypertextových dokumentů) a slouží ke komunikaci s WWW servery. Je to velmi užitečný nástroj, který je však snadno napadnutelný hackery. Pokud se na konci vyskytuje navíc "S" (https) a vedle URL se ukazuje obrázek visacího zámku, můžete se být jisti, že je webová stránka zabezpečená. Takové stránky jsou zašifrované a mají ověřený SSL certifikát, který zaručuje bezpečné spojení mezi webovou stránkou a prohlížečem. Pokud nemůžete pomocí https ověřit, že je stránka bezpečná, vyvarujte se zadávání osobních údajů.

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

Pamatujte si: zločinci na internetu udělají cokoliv, aby Vás přinutili uvěřit, že se jedná o poctivou stránku. Přestože jsou https stránky bezpečnější, může se stát, že se ocitnete na nějaké, která je provozována podvodníky. Pokud Vám i přes vizuální kontrolu stránka připadá podezřelá, využijte nějaký z níže uvedených bezpečnostních nástrojů a prověřte ji:

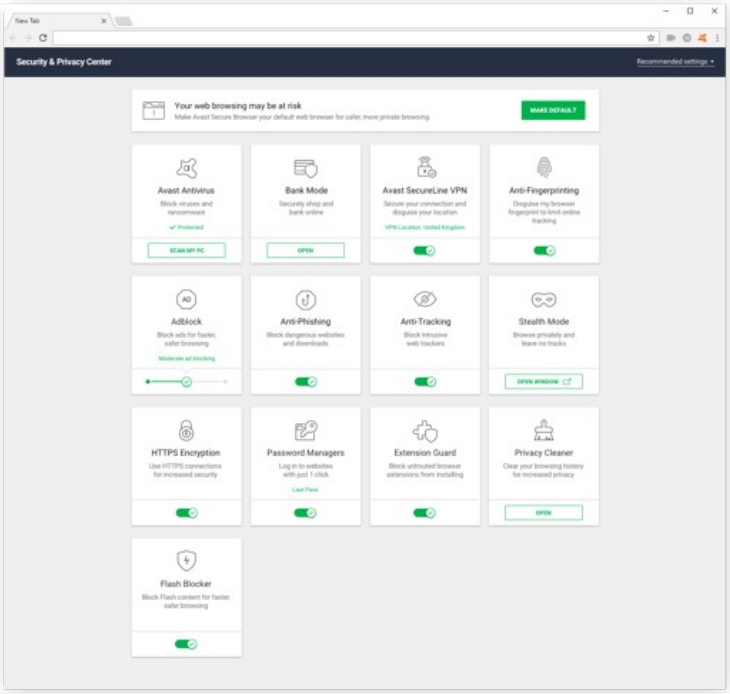
2 - Bezpečnostní nástroje

- Využijte nástroje prohlížeče — První nástroje, se kterými byste se měli seznámit, jsou bezpečnostní nástroje prohlížeče. Prohlédněte si nastavení soukromí a zabezpečení. Je pravděpodobné, že se Vám výchozí nastavení bude zdát zběžnější, než byste chtěli. Ručně si upravte nastavení podle toho, jak Vám vyhovuje. Zablokujte vyskakovací okna, vypněte automatické stahování a zabraňte webovým stránkám ve sledování Vašich aktivit. Upravitelné možnosti se liší podle toho, jaký prohlížeč používáte.

- Proveďte online bezpečností kontrolu stránek — Existuje několik kontrolních nástrojů, ze kterých můžete vybírat. Doporučujeme nestranný VirusTotal. Tyto online nástroje používají antivirové skenery a další způsoby kontroly bezpečnosti stránek. Jednoduše vložíte URL adresu stránky, kterou chcete zkontrolovat, do vyhledávače Vámi zvoleného kontrolního nástroje a ten Vám obratem oznámí výsledek. Níže příklad s VirusTotal - zadejte URL adresu a VirusTotal vyhodnotí, zda je stránka podezřelá či nikoliv.

- Nainstalujte si webové bezpečností nástroje — Chcete-li získat úplnou důvěru v bezpečnost webových stránek, ochraňte se pomocí špičkových bezpečnostních programů (např. Avast Free Antivirus, McAfee, AVG). Pokud používáte soukromou síť, můžete také využít výhody ochrany soukromí na webu.

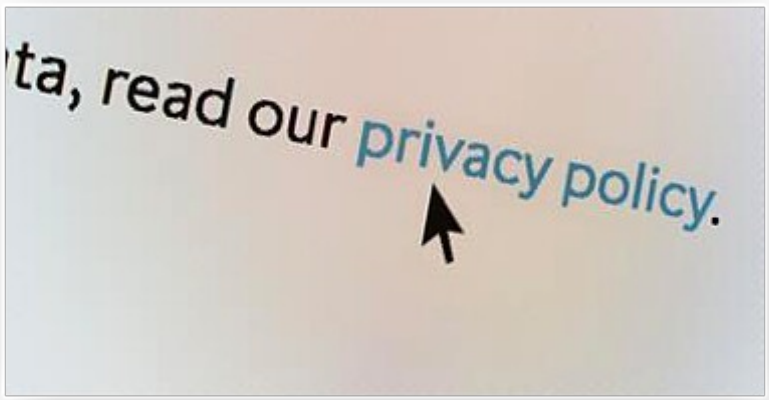
.



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

3 - Rychlý průzkum bezpečnosti na webu

- Prověřte stránku pomocí kontaktních údajů — Pokud jste podstoupili všechny výše zmíněné kroky a stále si nejste jisti, najděte na stránce odkaz "Kontakt" a obraťte se na provozovatele. Podle toho jak a jestli Vám vůbec odpoví poznáte, zda je možné stránce věřit či nikoliv.
- Zkontrolujte, zda má Váš antivirus Anti-Phishing certifikát — Ne všechny antivirové programy se tímto certifikátem pyšní. Nezávislé testovací laboratoře testují anti-phishingovou ochranu antivirových programů. Jednou takovou laboratoří je například AV-Comparatives. Testují, jak dobrou mají antiviry ochranu před phishingovými URL adresami (které se snaží získat Vaše osobní údaje) a zda dokáží rozpoznat falešný poplach od skutečných hrozeb v online bankovnictví.
- Zkontrolujte, zda má adresa URL zásady ochrany osobních údajů — Tohle by neměl být žádný velký oříšek. Pokud na stránce nejsou uvedeny zásady ochrany osobních údajů, měl by to pro Vás být velký vykřičník, že stránce nejspíš nelze důvěřovat.



- Dohledejte vlastníka domény pomocí WHOIS — Dále máte možnost dohledat vlastníka konkrétní domény pomocí veřejně dostupných záznamů na WHOIS. Prostřednictvím tohoto vyhledávání se dozvíte vše o doméně včetně toho, kdo a kdy ji zaregistroval.

<u>Reakce podniků na počítačovou kriminalitu</u>

Pokud jde o podniky, nejlepší ochranou proti počítačové kriminalitě je mít připravený solidní reakční plán. Plánování často nestačí — měli byste mít k dispozici bezpečnostní personál a nástroje k jeho provedení. Reakční plán podle SANS struktury zahrnuje tyto body:

- Příprava — stanovte si své zásady zabezpečení, rozpoznejte typy kritických bezpečnostních incidentů, připravte si komunikační plán a zaznamenávejte funkce, odpovědnosti a procesy každého incidentu. Sestavte reakční CSIRT tým (Computer security incident response team = Skupina pro reakci na počítačové bezpečnostní události), naberte do něj členy a zaškolte je.

- Identifikace — používejte bezpečnostní nástroje k přesné detekci neobvyklého chování v síťovém provozu, koncových bodech, aplikacích nebo uživatelských účtech a rychle shromažďujte důkazy, které Vám pomohou najít správné řešení incidentu.
- Zamezení šíření — izolujte zasažené systémy, očistěte je a postupně je přiveďte zpět online
- Vyhubení od kořene — identifikujte zdroj incidentu a udělejte vše pro to, abyste zabránili jeho opakování. Opravte slabiny, poškozená bezpečnostní opatření, která pomohly útočníkům proniknout do systému, a vyčistěte všechny koncové body od malwaru.
- Obnova — nahoďte zpět produkční systémy a zabraňte dalším podobným útokům. Otestujte, že všechno běží tak, jak má.
- Ponaučení — do dvou týdnů po incidentu si s týmem projděte jednotlivé body reakčního plánu, podívejte se, co se povedlo a co ne a pokuste se plán vylepšit.

Evropská unie se snaží pro boj s počítačovou kriminalitou využívat celou řadu prostředků. Rada Evropské unie v roce 2005 přijala strategii EU pro boj proti terorismu s cílem bojovat proti terorismu na celosvětové úrovni a zvýšit bezpečnost Evropy. Tato strategie spočívá na čtyřech pilířích: prevence, ochrana, pronásledování, reakce.

V rámci boje proti počítačové kriminalitě a jejího výkonu na různých úrovních, EU zavedla následující legislativní opatření:

- 2001 – **Rámcové rozhodnutí o potírání podvodů a padělání** definuje podvodné chování, které musí státy EU považovat za trestné činy.
- 2002 – **Směrnice o soukromí a elektronických komunikacích** definuje předpisy týkající se elektronických komunikací v EU s cílem zvýšit soukromí jednotlivců a subjektů.
- 2011 – **Směrnice o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii** se zabývá novým vývojem v online světě, jako je například grooming (pachatelé vystupují jako děti, aby nalákali nezletilé osoby k sexuálnímu zneužívání).
- 2013 – **Směrnice o útocích na informační systémy** usiluje o boj proti rozsáhlým kybernetickým útokům s cílem posílit národní zákony o počítačové kriminalitě a zavést přísnější trestní postihy.

Mezinárodně aktivní organizace se snaží přispět k boji proti počítačové kriminalitě. Dvě hlavní organizace působící na území EU jsou:

HYPERLINK "https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3" European Cybercrime Centre—(“Evropské středisko pro počítačovou kriminalitu”) - EC3 pomáhá členským státům v jejich úsilí o nabourání a narušení sítí počítačového zločinu a ve vývoji nástrojů a poskytování školení-na totot téma ~~EC3 assists member states in their efforts~~

The European Union Agency for Cybersecurity – ENISA (“Evropská agentura pro bezpečnost sítí a informací”) pracuje na poskytování rad, řešení a zlepšování možností kybernetické bezpečnosti. Odborné středisko vyhledává pro členské státy a orgány EU rady ohledně bezpečnosti sítí a informací.

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

4. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

Zadání: Co je to Anti-Phishing certifikát

a) test anti-phishingové ochrany antivirových programů
b) kontrola, zda má webová stránky zásady ochrany osobních údajů
c) ověření, zda je webová stránka nebo odkaz bezpečný
d) ověření skutečného majitele webové stránky

Cvičení ANO/NE

Úkol: Rozhodněte, zda je uvedené tvrzení pravdivé či nikoliv:

Zadání: Stránky, které mají na konci zkratky http navíc "S" a vedle URL obrázek visacího zámku, jsou bezpečnější.

a) Ano
b) Ne

5. Dopady počítačové kriminality na Váš život

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

Internet může být nebezpečným místem jak pro děti, tak pro dospělé. To platí obzvlášť v dnešní digitální době, kdy internet, a hlavně sociální sítě, jako například Facebook nebo Instagram, hrají v našich životech velkou roli. Ochrana na internetu vyžaduje dobré znalosti hrozeb a pokročilé IT schopnosti – jako rodič musíte znát všechna možná nebezpečí a vědět, jak před nimi chránit sebe, a hlavně své děti.

6 největších hrozeb, kterým děti na internetu čelí:

- Kyberšikana
- Nechtěné stažení malwaru
- Kybergrooming
- Phishing
- Sdílení osobních údajů
- ”Přátelé” v chatovacích místnostech

Nicméně, děti nejsou jedinou skupinou, která se může na internetu setkat s nebezpečím. Počítačová kriminalita je široký pojem a existuje mnoho způsobů, jak se s ní můžete setkat i Vy. Kybernetičtí zločinci útočí na lidskou nevědomost, neznalost a pohodlí, což může způsobit ztrátu identity nebo peněz. Na co by si lidé měli dávat pozor? Zločinci vědomě při plánování svých útoků zneužívají slabin a chování lidí, jako například:

- ochotu věřit druhým
- náznak naléhavosti nebo důležitosti zprávy
- náznaky věrohodnosti nebo autority zprávy či jedince (branding totožný s oficiálním brandingem firmy nebo jednotlivce, který má vyvolat důvěru)
- strach ze situací, které mohou vyvolat stres či úzkost
- příhodnost (nejjednodušší rozhodnutí nemusí být to nejbezpečnější)
- tendence lidí sdílet příliš mnoho osobní údajů na internetu (hlavně na sociálních sítích jako Facebook, Twitter, LinkedIn)
- neznalost nových technologií
- podcenění situace, ve které se jedinec ocitl

Pokud bude jedinec pokračovat ve výše zmíněném chování, vystavuje se většímu riziku kybernetické krádeže. Kybernetická krádež je trestný čin, při kterém se zločinec zmocní osobních či finančních údajů za použití počítače. Kybernetičtí zloději jsou sofistikovaní a dokáží proniknout přes bezpečnostní opatření.
Prvním krokem pro pachatele je získání totožnosti cizího počítače. Toho nejčastěji dosáhne krádeží elektronických dat (hesel, přístupových dat atd.), obvykle pomocí neoprávněného kopírování (skimming), podvodným phishingem nebo hackováním. Celý tento proces se nazývá krádež identity. Druhým krokem je zneužití ukradené identity. Hlavním cílem je většinou nabytí majetku, v některých případech jde zločincům pouze o ublížení či pošpinění jména oběti, například vydáváním se za oběť na sociálních sítích jako je Facebook.

Ochrana není složitá – je důležité řídit se těmito jednoduchými pravidly:

1. kontrolujte své účty

2. nakupujte na zabezpečených webových stránkách – pokud se vedle zkratky “https” nachází zelený visací zámek, můžete si být jisti, že jste na bezpečném webu
3. dávejte si pozor při otevírání nedůvěryhodných e-mailů

Jak počítačová kriminalita ovlivňuje jednotlivce, firmy a celou společnost

Počítačová kriminalita má přímý a značný vliv na pracovní místa, inovace, hospodářský růst a investice. Krádež IP adres navíc tvoří nejméně 25 % výdajů na počítačovou kriminalitu a představuje zvýšené riziko pro vojenské technologie. Dvěma obtížně měřitelnými oblastmi počítačové kriminality jsou krádež IP adres a ztráta příležitostí.

Nejzřejmějším dopadem je krádež – jednotlivci a podniky mohou kvůli počítačové kriminalitě utrpět **značnou finanční ztrátu.** Podstatná může také být ztráta zakázek v případě DoS útoku na velké korporace, který způsobí nedostupnost dané služby.

Moderní technologie nám podstatně zjednodušují život, zároveň nás však vystavují rizikům. Proto by **měla být počítačová bezpečnost nejvyšší prioritou, která výrazně ovlivňuje náš každodenní a pracovní život**. Porušení zabezpečení může být pro firmy a jejich zaměstnance a klienty katastrofální.

Škody způsobené kybernetickými útoky a krádežemi se mohou přesunout z původního cíle na ekonomicky propojené firmy, a tím zvětšit hospodářské škody. Firmy sdílejí stejné počítačové chyby a slabiny, což znamená, že všechny čelí stejným kybernetickým hrozbám.

Trestná činnost postihuje každého a v budoucnu bude počítačová kriminalita (a počítačová bezpečnost) ovlivňovat společnost čím dál víc. Nikdo není v bezpečí – počítačová kriminalita představuje hrozbu jak pro bohaté, tak pro chudé lidi:

- pro kohokoliv s mobilním telefonem v kapse
- pro kohokoliv s bankovním účtem
- pro kohokoliv, kdo si do počítače ukládá důležité soubory

- pro každého, jehož jméno je uvedeno v databázi přímého marketingu

Počítačová kriminalita není problém budoucnosti. Jedná se o současný problém, s kterým se lidé potýkají dennodenně. Počítačoví zloději se zaměřují na krádeže peněz a identity. S Vaší identitou si může pachatel vzít půjčku, získat úvěr, zadlužit Vás, a nakonec beze stopy zmizet. Může trvat roky, než získáte svou identitu zpět. Počítačový vir dokáže zničit soubory a ztracená databáze zapříčinit nechtěné obchodní hovory.

Počítačová bezpečnost je důležitá pro celkovou národní bezpečnost

- Existují státní tajemství, která musí zůstat utajena
- Osobní bezpečnost našich vůdců je velmi důležitá.
- Databáze otisků prstů a databáze Odboru vnitřních věcí musí být zabezpečeny.
- Teroristé nesmí být schopni obchodovat s důležitými národními a mezinárodními databázemi obsahujícími citlivé osobní údaje.

Národní bezpečnost však nemůže potlačovat naši osobní svobodu, o kterou jsme tak usilovně bojovali:

- Klíčová je naše svoboda slova
- Svoboda tisku vede lidi k zodpovědnosti
- Soukromí zajišťuje demokracii
- Svoboda surfování po internetu bez sledování

5. Procvičte si znalosti

Cvičení /JEDNA MOŽNOST/

Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

Zadání: Kdo může být ovlivněn počítačovou kriminalitou?

a. každý, kdo používá mobilní telefon, online účty nebo bankovní účty
b. pouze děti
c. pouze firmy
d. pouze veřejné instituce

Cvičení /JEDNA MOŽNOST/

Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

Zadání: Co je to kybernetická krádež?

a. posedlost určitou osobou ve snaze zjistit o ní co nejvíc informací
b. využívání nebo zneužívání počítače nebo komunikační sítě za účelem zničení nebo způsobení rozruchu, které mají vyvolat strach nebo zastrašit společnost k nějaké ideologii
c. pomlouvání nebo urážení nějaké osoby
d. odcizení finančních nebo osobních údajů za použití počítače

CVIČENÍ ANO/NE

Úkol: Rozhodněte, zda je uvedené tvrzení pravdivé či nikoliv.

Zadání: Kyberbetická bezpečnost není důležitá pro národní bezpečnost.

a) Ano
b) Ne

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

Zdroje

Zdroj: http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
Zdroj: https://study.com/academy/lesson/finance-crime-definition-comparisons-examples.html
Zdroj: https://www.avast.com/c-cybercrime
Zdroj: NATO science for peace and security series, 2008
Zdroj: CLARKE, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233
Zdroj: CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html.
For an overview, see: Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; Gercke, Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007
Zdroj: EU counter-terrorism strategy
Zdroj: https://www.avast.com/c-website-safety-check-guide
Zdroj: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Zdroj: https://www.enisa.europa.eu/
Zdroj: https://arxiv.org/pdf/1811.06624.pdf

Zapamatujte si

Shrnutí

Používání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je v současnosti trendem. Neexistuje téměř žádná oblast lidské činnosti, ve které se nepoužívají informační nebo komunikační technologie.

Naneštěstí, technický pokrok přináší více možností pro zločince. Zločin může být páchán mnoha způsoby, mezi nejčastější počítačové trestné činy patří:

- **Malware** – jednotný název pro všechny škodlivé softwary, které se šíří mezi počítači a narušují jejich práci.
- **Hacking** – proces, jehož výsledkem je narušení soukromí a získání důvěrných informací.
- **Spam** – nevyžádaný e-mail, který je obvykle odesílán hromadně velkému množství příjemců po celém světě.
- **Phishing** – hromadné rozesílání spam e-mailů nebo jiných forem komunikace. Jejím účelem je nalákat příjemce k tomu, aby udělali něco, co naruší jejich bezpečnost v soukromém životě nebo v práci.
- **Distribuovaný DoS útok (DDoS)** – zahltí systém velkým množstvím požadavků k připojení a tím ho znefunkční

Hacking nemusí být vždy vnímán jako škodlivý. V mnoha případech mají hackeři dobré úmysly a jde jim o dobrou věc. Takový druh hackingu se nazývá etický hacking a používá se např. k zabezpečení operačního systému.

Mezi nejčastěji páchané zločiny v kyberprostoru patří:

- **Předstírání identity na internetu** – využití jména, internetové domény, telefonního čísla nebo jiných údajů cizí osoby bez jejího souhlasu.

- **Kyberstalking** – posedlost vyznačující se snahou zjistit co nejvíc informací o určité osobě bez jejího vědomí.
- **Kyberšikana** – pomlouvání nebo urážení jiné osoby.
- **Krádež identity** – krádež osobních identifikačních údajů za účelem spáchání trestných činů.
- **Krádež dat** – nezákonné držení citlivých údajů jako jsou například nešifrované informace o platebních kartách
- **Finanční zločiny** – peněžní podvod, praní špinavých peněz, úplatkářství, korupce a další.

Počítačová kriminalita může mít devastující následky jako např. poškození dobrého jména, ztráta dat nebo finanční dopady na:

- Děti
- Dospělé
- Firmy
- Státy/vlády

Počítačová kriminalita může mít nejen finanční, ale i nečestné dopady na jednotlivce nebo firmy. Pro podniky, vládní orgány nebo zdravotnické organizace jsou časté ztráty citlivých údajů, finanční zatížení a poškození dobrého jména organizace či firmy.
Velkým plánovaným útokům se říká kyberterorismus nebo dokonce kybernetická válka.
Kyberterorismus představuje závažnější jednání v nebo prostřednictvím kyberprostoru. Jedná se o kybernetické útoky, při kterých je využíván nebo zneužíván počítač či komunikační síť za účelem zničení nebo narušení, které má vyvolat strach nebo zastrašit společnost v ideologický cíl.
Kybernetická válka je využití či zacílení počítačů pro válečné účely. Zahrnuje jak ofenzivní, tak defenzivní operace související s kybernetickými útoky, špionáží nebo sabotérskými činy.

Důležitým nástrojem v boji proti počítačové kriminalitě je prevence a ponaučení. Počítačová gramotnost je důležitým prvkem při prevenci zneužívání informačních a komunikačních technologií. Zaškolit bychom měli nejen děti, ale i dospělé a firmy a připravit je na nebezpečí, které na ně čeká v kyberprostoru, a pokusit se jim poskytnout potřebné znalosti pro bezpečné používání informačních technologií.

Nejlepším způsobem ochrany je prevence. Mějte na paměti těchto 5 klíčových bodů bezpečnosti na internetu: **Obezřetnost, Prevence, Ochrana, Udržení a Vytrvalost.**

Tyto body jsou obsaženy v následujících krocích:

1. Vyhněte se sdělování svých osobních údajů na internetu a v e-mailech.
2. Pečlivě zvažte přidávání fotografií na internet – kdokoliv je může kdykoliv použít v jiném kontextu
3. Nastavte si silná hesla
4. Užívejte a pravidelně aktualizujte antivirové programy
5. Neposílejte číslo a heslo Vaší kreditní karty přes e-mail
6. Hlídejte, jaké webové stránky Vaše děti navštěvují
7. Zálohujte si svá data a předejděte tak jejich ztrátě při napadení virem
8. Používejte bezpečnostní program, který Vám umožní spravovat soubory cookie
9. Pravidelně aktualizujte software a operační systém
10. Nikdy neotevírejte přílohy ve spam e-mailech
11. Neklikejte na odkazy ve spam e-mailech nebo na nedůvěryhodné stránky
12. Kontaktujte přímo společnost ohledně podezřelých požadavků
13. Dohlížejte na bankovní výpisy

14. Dávejte si pozor na to, jaké stránky navštěvujete

Jak rozpoznat bezpečné stránky?

1 - Vizuální kontrola bezpečnosti webových stránek.
2 - Bezpečnostní nástroje
3 - Rychlý průzkum bezpečnosti na webu

Internet se jen hemží phishingovými podvody. Žádná značka není v bezpečí před padělaním a každý uživatel se může stát terčem zločinců. Více než kdy předtím musíme převzít odpovědnost za naši bezpečnost na internetu. Řiďte se výše uvedenými tipy a buďte obezřetní. Poskytli jsme Vám všechny potřebné informace ohledně počítačové kriminality a jak se před ní chránit, **Vaším největším ochráncem jste však Vy sami.**

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

Správné odpovědi

Zadání: Veškerou hudbu a filmy uveřejněné na internetu si mohu legálně stáhnout.
Úkol: Rozhodněte, zda je uvedené tvrzení pravdivé či nikoliv:

a. ano
b. ne

Zadání: Co je to Distribuovaný DoS (DDoS) útok?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

e) masové rozesílání spam e-mailů nebo jiných forem komunikace
f) druh kybernetického útoku, při kterém zločinci znefunkční systém nebo síť
g) nevyžádaný e-mail rozesílaný hromadně velkému množství příjemců po celém světě
h) zneužití bezpečnostních chyb v síti k neoprávněnému přístupu nebo použití počítačů a síťových zdrojů

Zadání: Jakými aktivitami se zabývá tzv. "grey hat hacker"?
e) šířením nepravdivých informací o druhé osobě
f) krádeží osobní údaje
g) získáváním přístupu do cizího systému jen tak pro zábavu
h) finanční kriminalitou

Zadání: Kdo se dopouští tzv. interního podvodu?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

e. Interního podvodu se dopouští dodavatelé v případě, že nedodají objednané služby či zboží včas.
f. Interní podvod zahrnuje aktivity jako kybergrooming nebo kyberšikana.
g. Interního podvodu se dopouští zaměstnanci v případě provádění nepovolených finančních transakcí.
h. Interního podvodu se dopouštějí zákazníci podáním neoprávněné reklamace.

Zadání: Který kybernetický útok páchaný mimo virtuální svět je nejhorší?
Úkol: Vyberte správné odpovědi – pouze jedna odpověď je správná.

g. podvod s platebními kartami
h. pornografie
i. kyberterorismus
j. krádež identity

Zadání: Jaký dopad může mít počítačová kriminalita na jednotlivce?
Úkol: Vyberte správné odpovědi – více odpovědí může být správně.

e. Krádež identity
f. ztráta práce
g. zdravotní problémy
h. ztráta dat

Úkol: Doplňte správnou odpověď do závorky zadáním přesného tvaru slova bez dalších možností.

Pro_____jsou častými důsledky počítačové kriminality ztráta citlivých údajů, finanční zatížení a poškození dobrého jména.

Podniky, firmy, společnosti, instituce, korporace, úřady, vlády

Zadání: Co je to Anti-Phishing certifikát
e) **test anti-phishingové ochrany antivirových programů**
f) kontrola, zda má webová stránky zásady ochrany osobních údajů
g) ověření, zda je webová stránka nebo odkaz bezpečný
h) ověření skutečného majitele webové stránky

Zadání: Stránky, které mají na konci zkratky http navíc "S" a vedle URL obrázek visacího zámku, jsou bezpečnější.
c) Ano
d) Ne

Zadání: Kdo může být ovlivněn počítačovou kriminalitou?
a. každý, kdo používá mobilní telefon, online účty nebo bankovní účty
b. pouze děti
c. pouze firmy
d. pouze veřejné instituce

Zadání: Co je to kybernetická krádež?
a. posedlost určitou osobou ve snaze zjistit o ní co nejvíc informací
b. využívání nebo zneužívání počítače nebo komunikační sítě za účelem zničení nebo způsobení rozruchu, které mají vyvolat strach nebo zastrašit společnost k nějaké ideologii
c. pomlouvání nebo urážení nějaké osoby
d. odcizení finančních nebo osobních údajů za použití počítače

Zadání: Kyberbetická bezpečnost není důležitá pro národní bezpečnost.
a) Ano
b) Ne