Kapitola

Kybernetická bezpečnost

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: EDIT VALUE®
Poslední úprava: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

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

Kybernetická bezpečnost

Úvod

Staly jste se někdy obětí zákeřného útoku, při kterém se například někdo pokusil od Vás získat důležitý dokument nebo soukromé informace prostřednictvím odkazu v e-mailu? Pokud se vám někdy něco takového stalo, došlo k narušení Vaší kybernetické bezpečnosti.

V dnešní době je kybernetická bezpečnost velkým tématem. **Kybernetická bezpečnost zahrnuje prevenci a odhalování digitálních útoků, ochranu systémů, hardwaru i softwaru.** Souvisí také s prevencí, odhalováním, reakcí a zotavováním se z kybernetických incidentů, které mohou být zamýšlené či nikoli. Kyberútoky jsou obvykle **zaměřeny na přístup k datům/informacím, jejich změnu, krádež nebo zničení, vydírání** nebo **přerušení běžného podnikání** a kritických infrastruktur. Věděli jste, že podle nedávných studií se celkové náklady na počítačovou kriminalitu u každé společnosti pohybují kolem 12.000.000 €? Kybernetická bezpečnost tedy v současné době vyvolává debatu, která by měla zahrnovat společnost jako celek, protože každý člověk hraje důležitou roli v ochraně svých vlastních digitálních informací.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Ke kybernetickým útokům dochází čím dál tím více, což znamená, že zachování bezpečnosti softwaru, hardwaru a dat je důležitější než kdy dříve. Navzdory tomu existuje pouze málo lidí s těmito dovednostmi, takže studium základů kybernetické bezpečnosti Vám může pomoci s Vaší vlastní bezpečností na internetu.

Po dokončení této kapitoly budete znát pojem kybernetická bezpečnost a proč je kybernetická bezpečnost v dnešní době tak důležitá. V této kapitole se navíc dozvíte, co můžete udělat pro přijetí některých opatření kybernetické bezpečnosti ve Vašem každodenním životě.

Přehled výukových cílů a získaných kompetencí

V HVC_Opatření kybernetické bezpečnosti_O1 se dozvíte definici kybernetické bezpečnosti a hlavní evropské zákony týkající se tohoto tématu.

V HVC_Opatření kybernetické bezpečnosti__O2 zjistíte, co můžete dělat ohledně bezpečnosti svých hesel.

V HVC_Opatření kybernetické bezpečnosti__O3 se dozvíte, co můžete udělat pro svou ochranu během on-line nakupování.

V HVC_Opatření kybernetické bezpečnosti__04 se dozvíte o zabezpečení cloudu.

Hlavní výukové cíle	Dílčí výukové cíle
HVC_Opatření kybernetické bezpečnosti_O1: Naučíte se základní definici kybernetické bezpečnosti a hlavní zákony týkající se tohoto tématu.	DVC_Opatření kybernetické bezpečnosti_O1_O1: Umíte definovat kybernetickou bezpečnost.
HVC_Opatření kybernetické bezpečnosti_O2: Dozvíte se, co můžete udělat pro zvýšení bezpečnosti Vašeho hesla.	DVC_Opatření kybernetické bezpečnosti_O2_O1: Dokážete uvést nejčastější problémy související s heslem. DVC_Opatření kybernetické bezpečnosti_O2_O2: Umíte pojmenovat základní kroky, které zajistí bezpečnější ochranu heslem.
HVC_Opatření kybernetické bezpečnosti_O3: Budete vědět, jak se chránit při online nakupování.	DVC_Opatření kybernetické bezpečnosti_O3_O1: Znáte typy informací, které poskytujete během online nakupování. DVC_Opatření kybernetické bezpečnosti_O3_O2: Umíte vysvětlit, jak lze zlepšit chování při online nakupování.
V HVC_Opatření kybernetické bezpečnosti_O4: Dozvíte se, jak pracovat s cloudem.	DVC_Opatření kybernetické bezpečnosti_O4_O1: Umíte uvést definici pojmu „cloud computing“. DVC_Opatření kybernetické bezpečnosti__O4_O2: Umíte vyjmenovat doporučení pro používání služeb / řešení cloud computingu.

1.Kybernetická bezpečnost - definice a právní předpisy

Ochrana osobních údajů a kybernetická bezpečnost se stávají podstatnými hodnotami pro společnost. Z tohoto důvodu prošly v poslední době tyto dvě oblasti významným právním vývojem a nyní jsou v rámci EU více konsolidovány. Odstranění hrozeb a kybernetických útoků je však téměř nemožné, takže zavedení opatření kybernetické bezpečnosti a posílení jejích schopností je zcela nutné. Nicméně zavádění účinných opatření v oblasti kybernetické bezpečnosti je dnes obzvláště náročné, protože elektronických zařízení je v současnosti více než lidí a hackeři jsou stále inovativnější. V dnešním propojeném světě jsou pokročilá opatření týkající se kybernetické bezpečnosti výhodná pro každého. Na individuální úrovni může kybernetický útok vyústit ve vše od krádeže identity, přes pokusy o vydírání až po ztrátu důležitých dat.

Ale co přesně je myšleno pojmem „kybernetická bezpečnost“?

Definice
Kybernetická bezpečnost je postup obrany **počítačů, serverů, mobilních zařízení, elektronických systémů, programů, sítí a dat před škodlivými útoky, poškozením nebo neoprávněným přístupem.** Neexistuje žádná standardní, zejména všeobecně přijímaná definice kybernetické bezpečnosti. Jinými slovy, kybernetická bezpečnost souvisí se všemi ochrannými opatřeními a opatřeními přijatými na obranu informačních systémů a jejich používání před neoprávněným přístupem, útoky a poškozením a k zajištění důvěrnosti, integrity a dostupnosti dat.

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

1.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O1_O1:

Zadání: Co znamená kybernetická bezpečnost?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Kybernetická bezpečnost zahrnuje obranu hardwaru a softwaru.
- Kybernetické útoky přibývají a každý je nyní vůči těmto typům incidentů citlivější.
- Mezi účinná opatření v oblasti kybernetické bezpečnosti patří uplatnění několika opatření.
- Školení v oblasti kybernetické bezpečnosti by mělo být zajištěno co nejdříve, z důvodu potřeby zavedení několika důležitých opatření.

2.Kybernetická bezpečnost – zabezpečení heslem

Dokážete určit nejjednodušší způsob, jak může kyberzločinec získat přístup k Vašemu bankovnímu účtu, sociálním sítím, e-mailům a dalším soukromým údajům? **Je jím nedostatečně silné heslo.** Ve skutečnosti je většina hesel rozluštěna během „mrknutí oka“. Podle Nacional Cyber Security Centre bylo pět nejčastějších hesel v roce 2019 „123456“, „123456789“, „qwerty“, „heslo“ a „1111111“. Takže, pokud máte některá z těchto hesel nebo hesla jim podobná, podívejte se prosím na příklad níže.

Příklad

Množství času na rozluštění hesla

123456	0,29 ms
potato	1,37 ms
Potato	3,28 s
P0tat0	1h 23m.27s 0.10ms
P0tat0!	1 měsíc, 3 týdny, 5 dní a 21h 54min, 40s 8ms
IAtE27P0taT0s!	47623938 tisícitelí, 8 století, 73 let and 8 měsíců

Jedním z nejčastějších problémů je skutečnost, že jsou hesla obecně snadno uhodnutelná. Mnoho lidí si myslí, že krátké heslo se spoustou různých typů znaků je bezpečné, ale ve skutečnosti je jediný způsob, jak zajistit skutečně bezpečné heslo, vytvořit heslo, které se skládá **alespoň ze 14 poměrně nahodilých znaků**. Navíc, jak vidíte, **čím složitější je vaše heslo, tím obtížnější je ho uhodnout**. Silné heslo je kombinace písmen (velkých a malých), čísel a symbolů. Dobrý způsob, jak nikdy nezapomenout své jedinečné heslo, je zvolit větu místo slov, smíchat ji s alfanumerickými znaky a většina webových stránek dokonce umožňuje použít mezery mezi slovy! Při vytváření nových účtů a digitálních profilů je však třeba vzít v úvahu více aspektů, které plně maximalizují vaši kybernetickou bezpečnost a ochranu.
Níže můžete pozorovat velmi časté příklady co „Dělat“ a „Nedělat“ v souvislosti s hesly . Pokud budete postupovat podle těchto „zlatých pravidel“, budou vaše hesla pro hackery téměř nerozluštitelná.

Nedělat: **Pro každý účet použijte stejné heslo.**

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

Dělat: Vytvořte jedinečná hesla k jednotlivým účtům a profilům.

Všichni víme, že dnes téměř každá webová stránka vyžaduje založení uživatelského účtu a téměř každý z nás používá stejná hesla pro různé účty. Lidé však často zapomínají, že tyto účty obsahují jejich identifikační nebo finanční údaje, které mohou být ukradeny nebo zkompromitovány, a použitím pouze jednoho hesla se stávají snadným cílem kybernetických útoků.

Nedělat: Uložte si hesla do jiného zdroje.
Dělat: Zapamatujte si svá hesla a na svých účtech si nastavte bezpečnostní otázky.

Jedním ze snadných a častých způsobů, jak svá hesla nezapomenout, je ukládat je do tabulky, na pevný disk nebo do osobních poznámek. **Snažte se si svá hesla zapamatovat!** Můžete také na svých účtech preventivně nastavit bezpečnostní otázky. Místo běžných otázek typu „Jaké je jméno Vaší matky?“ nebo „Odkud jste?“ používejte otázky, na které můžete odpovědět jen vy.

Nedělat: Sdílejte svá hesla s ostatními.
Dělat: Zachovejte mlčenlivost o svých heslech.

Hned po použití stejného hesla pro každý Váš účet je další častou chybou to, že lidé sdílejí svá hesla s ostatními prostřednictvím e-mailu, textových zpráv nebo sociálních médií.
Aby byla Vaše hesla v bezpečí, **musíte je pravidelně měnit**. Nezapomínejte, že někde na světě existuje hacker, který se neustále snaží ukrást hesla uživatelů, a čím více času má, tím vyšší je riziko jeho úspěchu.

Nedělat: Zvolte silné heslo a držte se ho.
Dělat: Měňte hesla každé tři měsíce.

Většina prohlížečů a aplikací umožňuje uživatelům uložit přihlašovací údaje, aby je nemuseli vkládat pokaždé, když se chtějí přihlásit. Přestože je to velmi pohodlné, mějte na paměti, že pokud ztratíte zařízení a cizímu člověku se podaří prolomit heslo, získá přístup ke všem těmto informacím.

Nedělat: Použijte jeden ověřovací faktor.
Dělat: Přidejte dvoufázové ověření pro každý digitální účet.

Pokud na svých digitálních účtech **použijete dvoufázové ověření,** přidáváte další vrstvu zabezpečení. Když se někdo přihlásí k Vašemu účtu z jiné oblasti, zařízení nebo prohlížeče, obdržíte **heslo**, které je třeba pro povolení přihlášení zadat. Kromě toho dalším typem dvoufázové autentizace je **otisk prstu, hlasový záznam nebo kód odeslaný** do Vašeho telefonu. Spousta lidí si myslí, že tímto ověřením pouze ztrácejí čas, ale pokud máte vážné obavy o své soukromí, měli byste pro své digitální účty použít, pokud možno, dvoufázové ověření. Pokud tuto možnost nemáte, měli byste postupovat podle doporučení, která byla zmíněna výše.

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

2.Procvičte si znalosti

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O2_O1:

Zadání: **Která z následujících možností je správná?**
Úkol: Vyberte správné možnosti podle zásady více správných odpovědí: Pouze jedna odpověď je pravdivá.

- Doporučuje se zvolit jednoduché heslo, které si dobře zapamatujete.
- Některá unikátní hesla jsou odvozena od Vašeho jména, jména člena rodiny nebo jména domácího mazlíčka.
- Čím více znaků a symbolů hesla obsahují, tím méně je obtížné je uhodnout.
- **Silné heslo obsahuje kombinaci velkých a malých písmen, symbolů a čísel a je dlouhé nejméně osm znaků.**

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O2_O2:

Zadání: **Jaká jsou některá pravidla pro ochranu Vašich digitálních účtů před kybernetickými útoky?**
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Použijte stejné heslo na více webech / účtech.
- **Pravidelně měňte hesla.**
- Uložte přihlašovací údaje do prohlížeče nebo aplikace konkrétního počítače.
- **Otisk prstu, hlasový záznam nebo PIN kód jsou dobrou volbou pro dvoufázové ověřování.**
- **Při vytváření nového hesla se vyhněte slovům, která se nacházejí ve slovníku, zájmenům, uživatelským jménům a dalším předem definovaným pojmům, stejně jako běžně používaným heslům.**

3.Online nakupování

Jak jsme se již dozvěděli, kybernetická bezpečnost zlepšuje spojení mezi lidmi a uplatňuje postupy, jejichž cílem je chránit informace před škodlivými útoky. V roce 2019 byl elektronický trh odpovědný za tržby kolem 3,5 bilionu dolarů a nyní se očekává, že do roku 2021 dosáhne 4,9 bilionů dolarů. Kromě toho 21,8 % celosvětové populace nakupuje on-line a značky jsou stále aktivnější na sociálních sítích, což znamená, že se více spojují s lidmi prostřednictvím různých on-line kanálů.
V dnešní době stále více lidí upřednostňuje online nakupování před konvenčními způsoby. Některé z těchto výhod souvisí s pohodlím, možností srovnání cen, komfortem a dostupností. Když nakupujete online, musíte si obvykle vytvořit účet. V důsledku toho jste povinni poskytnout některé ze svých soukromých údajů, například „jméno“, „adresu“, „telefonní číslo“, „e-mail“ a způsob platby. Vzhledem k tomu, že je vše na internetu sledováno a z obrovského množství elektronického obchodování a interakcí na sociálních sítích vzniká velké množství dat, je opravdu důležité předem dobře vědět o možných důsledcích těchto jednání.

Pokud se chcete při online nakupování vyhnout internetovým podvodům, budete muset učinit několik opatření. Níže naleznete několik návrhů:

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

Zjistěte, s kým máte co do činění

Přečtěte si recenze a zjistěte, zda ostatní spotřebitelé měli s webem pozitivní nebo negativní zkušenosti. Ujistěte se, že je web zabezpečen.

Kontrolujte své finanční účty

Pravidelně si kontrolujte své výpisy a ujistěte se, že se na nich vyskytují pouze platby, kterých jste si vědomi.

Platba kreditní nebo debetní kartou

Kreditní karty jsou obecně jednou z nejbezpečnějších variant, protože umožňují kupujícímu požádat emitenta o úvěr, pokud produkt není dodán nebo není tím, co bylo objednáno. Zvažte použití virtuální jednorázové kreditní karty. Virtuální kreditní karty jsou kreditní karty, které umožňují provádět transakce na hlavním účtu kreditní karty bez použití nebo odkrytí jeho čísla. K vytvoření tohoto typu kreditních karet můžete například použít Capital One.

Podívejte se na zásady ochrany osobních údajů

Zásady ochrany osobních údajů popisují, jak jsou vaše osobní údaje shromažďovány, používány a sdíleny při návštěvě nebo nákupu v online obchodě. Měli byste si přečíst zásady ochrany osobních údajů a zjistit, zda souhlasíte s ochranou osobních údajů společnosti.

Zdarma vždy nepředstavuje výhodu

Spořiče obrazovky nebo virtuální karty, které jsou nabízeny zdarma, by mohly přenášet nebezpečné viry. Udržujte svůj antivirový a antispywarový software spolu s vaším firewallem aktualizovaný.

Neposílejte e-mailem své finanční informace

Legitimní společnosti od Vás nepožadují finanční informace prostřednictvím e-mailu nebo vyskakovacího okna.

3.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O3_O1:

Zadání: **Jaké informace byste při nakupování na internetu nikdy neměli uvádět?**
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Číslo občanského průkazu.**
- **Bezpečnostní kód kreditní karty.**
- **Číslo debetní karty.**
- **Číslo bankovního účtu.**
- Emailová adresa.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O3_O2:

Zadání: **Ze seznamu vyberte, které chování při online nakupování Vám pomůže nestát se obětí kybernetického zločinu.**
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Před poskytnutím údajů o kreditní kartě je třeba věnovat dostatek času průzkumu webových stránek.**
- **Nakupujte z webu, který používá šifrování.**
- **Než si něco objednáte, přečtěte si zásady reklamace a další podmínky a zásady ochrany osobních údajů webu.**
- Plaťte debetní kartou, hotovostí nebo bankovním převodem.
- Pro ochranu důvěrnosti použijte „hotspot“.

4.Cloud Computing

Dávno jsou pryč doby, kdy jste své soubory ukládali na kompaktní disk nebo na USB klíč, vždy s velkou obavou, že je nakonec ztratíte a nikdy je už nenajdete. V dnešní době můžete mít díky cloud computingu přístup ke svým souborům z jakéhokoli počítače a v podstatě jsou teď cloudová řešení stále více používaná po celém světě při každodenních činnostech.
S některými typy cloudových řešení jste neustále v kontaktu, například při kontrole své e-mailové schránky nebo při používání telefonu ke kontrole dopravní situace. Díky **cloudovým řešením jsou Vaše data uložena u poskytovatele a jsou dostupná přes internet.**
Proto se v této souvislosti nabízí otázka, zda jsou naše data v cloudu v bezpečí a nehrozí jim žádné riziko? Z tohoto důvodu je důležité vědět více o konceptu cloud computingu.

Definice
Cloud computing lze definovat jako **dodání IT zdrojů na vyžádání** - jako je například úložiště, výpočetní výkon nebo kapacita pro sdílení dat - přes internet prostřednictvím hostingu na vzdálených serverech. Jinými slovy, cloud computing znamená ukládání a přístup k datům a programům přes internet namísto prostřednictvím pevného disku Vašeho počítače. Mezi zdroje patří nástroje a aplikace, jako jsou úložiště dat, servery, databáze, sítě a software. Cloudová řešení jsou velmi populární volbou pro lidi a podniky z mnoha důvodů, včetně úspor nákladů, zvýšené produktivity, rychlosti a efektivity, výkonu a zabezpečení.

Cloud, big data a digitalizace průmyslu jsou doprovázeny nárůstem potenciálních zranitelných míst, která pomáhají jedincům se špatnými úmysly lépe se zaměřit na větší množství obětí. Rozmanitost typů útoků a jejich rostoucí sofistikovanost znesnadňují udržení tempa vývoje zabezpečení. Z tohoto důvodu je důležité **zavést některá denní preventivní opatření, aby se zabránilo krádeži, úniku a / nebo vymazání důležitých informací.**
Podívejte se na stručné shrnutí některých opatření, která můžete použít ke zlepšení zabezpečení cloud computingu.

Použití vícefaktorové autentizace	Tradiční kombinace uživatelského jména a hesla často nestačí k ochraně uživatelských účtů před hackery a ukradené přihlašovací údaje jsou jedním z hlavních způsobů, jak hackeři získají přístup k Vašim datům / informacím. Z tohoto důvodu musíte použít nejen **silná hesla**, ale také **vícefaktorovou autentizaci** - známou také jako dvoufázové ověřování - abyste zajistili, že se do Vašich cloudových aplikací bude moci přihlásit a získat přístup k citlivým datům pouze autorizovaný personál. Vícefaktorová autentizace je jedním z nejúčinnějších způsobů, jak zabránit hackerům v přístupu k Vašim cloudovým aplikacím. Mezi příklady patří heslo

	kombinované s kódem zaslaným prostřednictvím SMS nebo s číslem vygenerovaným aplikací. Je také důležité, abyste se nezapomínali odhlásit a nikdy neukládali své přihlašovací údaje na webech nebo v aplikacích.
Spravujte svůj uživatelský přístup a vylepšete zabezpečení cloud computingu	Většina lidí nepotřebuje přístup ke všem informacím, ke každé aplikaci nebo ke každému souboru. Proto **nastavení správných úrovní autorizace** zajišťuje, že každý uživatel může pouze prohlížet nebo manipulovat s určitými aplikacemi nebo daty / informacemi. Pokud má někdo povolen přístup ke všemu a nechá se nachytat phishingovým e-mailem a neúmyslně poskytne své přihlašovací údaje, hacker má poté velmi snadno přístup ke všem informacím.
Monitorujte, zaznamenávejte a analyzujte aktivity uživatelů pomocí automatizovaných řešení pro detekci vetřelců	**Monitorování a analýza uživatelských aktivit v reálném čase** Vám mohou pomoci zaznamenat případné nesrovnalosti, které se odchylují od běžných vzorců chování uživatelů. Tyto neobvyklé činnosti by mohly naznačovat narušení Vašeho systému, takže jejich včasné zachycení může zastavit hackery v jejich postupech a umožnit Vám opravit bezpečnostní problémy dříve, než se něco pokazí. V dnešní době najdete mnoho řešení pro automatizované monitorování a správu sítí 24/7 a přechod na pokročilá řešení kybernetické bezpečnosti. Protože každý podnik / osoba má různé potřeby pro různé úrovně kybernetické bezpečnosti, nezapomeňte před provedením velké investice do zabezpečení získat posouzení možných rizik od třetí nezávislé strany.
Anti-phishingové školení	Hackeři mohou získat přístup k zabezpečeným informacím odcizením důležitých údajů pomocí některých technik, jako je phishing, IP spoofing a špionáž na sociálních médiích. Z tohoto důvodu mějte na paměti, že například **phishingové školení** by mělo být nepřetržitým procesem, který musí být řízen někým v rámci organizace, aby mohl být efektivní.
Zálohujte soubory v různých cloudových účtech	Bez ohledu na velikost, odvětví, region nebo lidi je zajištění dostupnosti dat prioritou pro každého. Navíc ztráta dat / informací v důsledku lidské chyby je velmi vysoké riziko, takže neukládejte všechna důležitá data na jedno místo. Ať už chráníte a přistupujete k souborům na svém osobním notebooku nebo jste poskytovatelem služeb odpovědným za firemní portfolio (a jeho rostoucí množství dat), cloudové aplikace jsou v moderním digitálním světě zásadním nástrojem. Proto je velmi důležité najít **více než jedno řešení zálohování mezi cloudy**, abyste zajistili, že kopie dat, které vytváříte, ukládáte a sdílíte, jsou na bezpečném místě.

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

4. Procvičte si znalosti

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: FO_Opatření kybernetické bezpečnosti_O4_O1

Zadání: **Pokud jde o cloud computing, které tvrzení je pravdivé?**
Úkol: Vyberte správné možnosti podle zásady více správných odpovědí: Pouze jedna odpověď je pravdivá.

- V Platform as a Service (PaaS) platí společnost za služby jako je ukládání, vytváření sítí a virtualizace.
- Infrastruktura jako služba (IaaS) je model cloud computingu, ve kterém poskytovatel třetí strany dodává hardwarové a softwarové nástroje.
- **Software as a Service (SaaS) je model licencování a dodávání softwaru, ve kterém je software licencován na základě předplatného a je centrálně hostován.**
- Při používání cloudových počítačů musí uživatelé a společnosti spravovat fyzické servery.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: DVC_Opatření kybernetické bezpečnosti_O4_O2

Zadání: **Které chování Vám pomůže nestát se obětí kybernetického zločinu?**
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Ukládejte informace, jako jsou adresy, telefonní čísla, bankovní údaje atd. do různých cloudů.**
- **Vytvořte jedinečné heslo pouze pro cloudovou službu.**
- Při používání cloudových řešení není důležité mít antivirový program.
- Kvůli praktičnosti se doporučuje ukládat přihlašovací údaje do příslušné aplikace.

Zdroje

Alexandra, Susan (April 04, 2019). 10 Tips for Keeping Your Personal Data Safe on Social Media. Retrieved from https://securitytoday.com/Articles/2019/04/04/10-Tips-for-Keeping-Your-Personal-Data-Safe-on-Social-Media.aspx?Page=2

Cucu, Paul (December 21, 2016). 17 Underused Online Shopping Security Tips. Retrieved from https://heimdalsecurity.com/blog/online-shopping-security-tips/

European Commission (March 2019). Briefing Paper: Challenges to effective EU cybersecurity policy, Briefing paper. European Court of Auditors.

Federal Trade Comission (n.d.). 9 Online Shopping Tips. Retrieved from https://www.yumpu.com/en/document/read/4010016/nine-online-shopping-tips-federal-trade-commission

Kapiswe, Subham (April 23, 2019). NCSC Reveals List Of World's Most Hacked Passwords. .Retrieved from https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#cite_note-NCSCList-15

Kapersky (n.d.). Safer Online Shopping. Retrieved from https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping

National Cybersecurity Alliance (n.d.). Online Safety Basics: Online Shopping. Retrieved from https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

Acronis (n.d.). Case study: The Benefits of Cloud-to-Cloud Backup Solutions from Acronis. Retrieved from https://www.acronis.com/en-us/articles/cloud-to-cloud-backup/

D'Silva, Frank (June 15, 2020). 6 Tips for Improving Cloud Computing Security. Retrieved from https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security

Zapamatujte si

Doba internetu nám dala superschopnost být všudypřítomní. Internet zmenšil vzdálenosti mezi lidmi, podniky a místy. Umožnil lidem být pouhým kliknutím kdekoli a s kýmkoli. Jak jste měli možnost v této kapitole zjistit, za **online soukromí a bezpečnost osobních údajů nesou společnou odpovědnost všechny strany:** vláda, vývojáři softwaru, poskytovatelé cloudových služeb, společnosti i koncoví uživatelé.
Se zavedením GDPR získávají koncoví uživatelé důvěru v zabezpečení svých dat, protože cílem tohoto nařízení je chránit soukromí lidí na internetu. Existuje však mnoho způsobů chování, které si koncoví uživatelé musí osvojit, aby mohli dobře hrát svou roli v kybernetické bezpečnosti. Toto chování je společné pro všechny aktivity na internetu - od sociálních médií po cloud - a běžně se označuje jako „zlatá pravidla internetu".
První pravidlo se opírá o hesla: **mějte jedinečná a silná hesla s dvoufázovým ověřením** při přihlašování a **měňte je každé tři měsíce**. Druhé pravidlo se týká soukromých informací: **neukládejte ani nesdílejte citlivé informace přes internet**, zejména při nakupování na internetu; navíc, pokud máte soukromá data uložená v cloudu, ujistěte se, že **neshromažďujete všechny své informace pouze do jednoho cloudu!**
Třetí pravidlo se týká chytrého brouzdání na internetu: **neukládejte své přihlašovací údaje** do žádného prohlížeče, webu nebo aplikace a odhlaste se pokaždé, když opustíte web. Stejně tak **neklikejte na žádný pochybný odkaz** ani nezadávejte své informace na nezabezpečených webech.
Na závěr je důležité si uvědomit, že jde i o Vaše data, která by mohla být ohrožena kyberútoky, a proto je nutné abyste plnily svou roli při ochraně a zabezpečení dat na internetu.