Kapitola

Kybernetická bezpečnost

Projekt: B-SAFE
~~Number~~Číslo: 2018-1CZ01-KA204-048148
~~Name of author~~Jméno autora: EDIT VALUE®
~~Last processing date~~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

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

V dnešní době je kKybernetická bezpečnost velkým problémemtématem. Kybernetická bezpečnost zahrnuje prevenci a odhalování digitálních útoků, ochranu systémů, hardwaru ia softwaru. Souvisí také s prevencí, odhalováním, reakcí a zotavováním se z incidentů kybernetickékybernetických incidentů bezpečnosti, které mohou být zamýšlenéy či nikoli. Kyberútoky jsou obvykle zaměřeny na přístup k datům/informacím, jejich změnu, krádež nebo zničení, vydírání peněz nebo přerušení běžnéhoých podnikáníů a kritických infrastruktur. Věděli jste, že podle nedávných studií se celkové náklady na kyberkriminalitu počítačovou kriminalitu u každé společnosti pohybují kolem 12.000.000 €? Kybernetická bezpečnost je tedy současnou debatouv současné době vyvolává debatu, která musí zahrnovatby 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

Kybernetické útoky se dějí čím dál častějiKe kybernetickým útokům dochází čím dál tím více, což znamená, že zachování bezpečnosti softwaru, hardwaru a dat je důležitější než kdy dříve. Navzdory tomu existuje nedostatek pouze málo lidí s těmito dovednostmi, takže studium, jak začít s kybernetickou bezpečností základů kybernetické bezpečnosti; Vvám může pomoci s Vvaší vlastní bezpečností na internetu.

Po seznámení s touto obsahovou jednotkoudokončení této kapitoly se seznámíte s pojmem budete znát pojem kybernetická bezpečnost a proč je kybernetická bezpečnost v dnešní době tak důležitá. V této obsahové jednotcekapitole se navíc budete vědětdozvíte, co můžete udělat pro přijetí některých opatření kybernetické bezpečnosti vve Vvašem každodenním životě.

Přehled výukových cílů a získaných kompetencí

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

V LOHVC_Opatření kybernetické bezpečnosti_Kyberbezpečnostní opatření_O2 budete vědětzjistíte, co můžete dělat ohledně bezpečnosti svých hesel.

V LOHVC_Opatření kybernetické bezpečnosti_Kyberbezpečnostní opatření_O3 budete vědětse dozvíte, co můžete udělat pro svou ochranu během on-line nakupování.

V LOHVC_Opatření kybernetické bezpečnosti_Kyberbezpečnostní opatření_04 se dozvíte o zabezpečení cloudu.

Hlavní výukové cíle	Dílčí výukové cíle
LOHVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O1: Naučíte se základní definici kybernetické bezpečnosti a hlavní zákony týkající se tohoto tématu.	FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O1_O1: Umíte uvést definici kybernetické bezpečnostidefinovat kybernetickou bezpečnost.
LOHVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O2: Budete vědětDozvíte se, co můžete udělat s pro zvýšení bezpečnostíí Vvašeho hesla.	FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O2_O1: Umíte vysvětlitDokážete uvést nejčastější problémy související s s heslem. FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O2_O2: Umíte pojmenovat základní kroky, které zajistí bezpečnou bezpečnější ochranu heslema.
LOHVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O3: Budete vědět, jak se chránit při online nakupováním.	FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O3_O1: Znáte typy informací, které uvádíte poskytujete během online nakupování. FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O3_O2: Umíte vysvětlit, jak lze zlepšit chování při online nakupování.
V LOHVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O4: Dozvíte se, jak pracovat s cloudem.	FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O4_O1: Umíte uvést definici pojmu „cloud computing“. FODVC_Kyberbezpečnostní opatřeníOpatření kybernetické bezpečnosti_O4_O2: Umíte uvést vyjmenovat doporučení, co byste měli dělat při pro používání služeb / řešení cloud computingu.

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

1.~~Buduj znalosti —~~ Kybernetická bezpečnost - definice a právní předpisy

Ochrana osobních údajů a k~~K~~ybernetická bezpečnost se stávají podstatnými~~j významem~~ hodnotami pro společnost. Z tohoto důvodu~~ v poslední době~~ ~~-~~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 ~~použití~~ zavedení opatření kybernetické bezpečnosti a posílení jejích schopností ~~kybernetické bezpečnosti~~ je ~~povinné~~zcela nutné. Nicméně z~~Z~~avádění účinných opatření v oblasti kybernetické bezpečnosti je dnes obzvláště náročné, protože elektronických zařízení je v ~~současné době~~současnosti více než lidí~~,~~ a hackeři jsou stále inovativnější. V dnešním propojeném světě jsou pokročilá opatření týkající se kybernetické bezpečnosti výhodná pro každého. ~~každý těží z pokročilých opatření kybernetické bezpečnosti.~~ Na individuální úrovni může kybernetický útok vyústit ve vše~~,~~ od krádeže identity, přes pokusy o vydírání až po ztrátu důležitých dat.

Ale co přesně ~~máme na mysli pod~~ 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~~,~~ ~~aby byla zajištěna~~ zajištění důvěrnosti, integrity~~a~~ a dostupnosti dat.

1.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: ~~FO~~DVC_ ~~Kyberbezpečnostní opatření~~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 ~~uplatnit~~ zavedení několika důležitých ~~kroků~~opatření.

2.~~Buduj znalosti —~~ Kybernetická bezpečnost – zabezpečení heslem

~~Znáte —~~ Dokážete určit nejjednodušší způsob, jak může kyberzločinec získat přístup ~~k vaší bance~~k Vašemu bankovnímu účtu, sociálním ~~médiím~~sítím, e-mailům a dalším soukromým údajům? Je jím~~to~~ nedostatečně silné heslo. Ve skutečnosti ~~bude~~ je většina hesel rozluštěna během „mrknutí oka“.

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

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 and 21h 54min, 40s 8ms
IAtE27P0taT0s!	47623938 tisícitelí, 8 století, 73 let and 8 měsíců

Jedním z nejčastějších problémů s hesly je tenje skutečnost, že jsou hesla obecně snadno uhodnutelná. Mnoho lidí si myslí, že krátké heslo se spoustou různých typů znaků je bezpečné, když ale ve skutečnosti je realita taková, že jediný způsob, jak zajistit skutečně bezpečné heslo, je udělat vytvořit heslo, které se skládá alespoň ze 14 poměrně nahodilých znaků dlouhých a poněkud svévolných. Navíc, jak vidíte, čím složitější je vaše heslo, tím obtížnější je ho uhodnout. Silné heslo je kombinace písmen (velkých a malých písmen), 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 „Co Dělat“ a „Neědělat“- v souvislosti s hesly týkající se hesel. Pokud budete postupovat podle těchto „zlatých pravidel“, budou vaše hesla pro hackeryrům téměř nerozluštitelná.

Nedělat:I Pro každý účet použijte stejné heslo.
Dělat: Vytvořte jedinečná hesla k jedinečným jednotlivým účtům a profilům.

Všichni víme, že dnes téměř každá webová stránka vyžaduje účet založení uživatelského účtu a téměř každý z nás používá stejná hesla pro různé účty. Lidé však často zapomínají, že tyto účty obsahují jejich identitu identifikační nebo finanční informaceúdaje, které mohou být ukradeny nebo zkompromitovány, a použitím pouze jednoho hesla se stávajíáte 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 si svá hesla nezapomenoutčasto pamatovat, 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 na svých účtech. Místo kladení běžných otázek typu „Jaké je jméno Vaší matky?“ nebo „Odkud jstei?“ používejte otázky, na které můžete odpovědět jen vy.

Nedělat: Sdílejte svá hesla s ostatními.

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

Dělat: Zachovejte mlčenlivost o svých heslech.

Hned po použití stejného hesla pro každý V~~v~~áš účet je , ~~–~~další častou chybou toje, že lidé sdílejí svá hesla s ostatními prostřednictvím e-mailu, textových zpráv nebo sociálních médií.
Aby byla V~~v~~aše 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 m~~á~~ají, tím vyšší je riziko jehojich ~~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: Použ~~í~~ijte jeden ověřovací faktor.
Dělat: Přid~~ejte~~at dvoufázové~~aktorové~~ ověření pro každý digitální účet.

Pokud na svých digitálních účtech použijete ~~dvoufaktorové~~ dvoufázové ověření, přidáváte , ~~toto ověření představuje~~ další vrstvu zabezpečení. Když se někdo přihlásí k V~~v~~ašemu účtu z jiné~~ho umístění~~ oblasti, zařízení nebo prohlížeče, obdržíte heslo, které je třeba pro povolení přihlášení zadat. Kromě toho dalším typem ~~dvoufaktorové~~ dvoufázové autentizace je otisk prstu, hlasový ~~otisk~~ záznam nebo kód odeslaný do V~~v~~ašeho telefonu. ~~Mnoho~~ Spousta lidí si myslí, že ~~je to časově náročné~~tímto ověřením pouze ztrácejí čas, ale pokud máte vážné obavy o své soukromí, měli byste pro své digitální účty použít, pokud možno, ~~dvoufaktorovou autentizaci~~dvoufázové ověření~~, pokud je tato volba možná~~. Pokud tuto možnost nemáte ~~možnost použít dvoufaktorové ověřování~~, měli byste postupovat podle doporučení, která byla zmíněna ~~dříve~~výše.

2.Procvičte si znalosti

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: ~~FO~~DVC_~~Kyberbezpečnostní opatření~~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: ~~FO~~DVC_ ~~Kyberbezpečnostní opatření~~Opatření kybernetické bezpečnosti_O2_O2:

Zadání: Jaká jsou některá pravidla ~~pro~~na ochranu V~~v~~ašich 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 ~~otisk~~ záznam nebo PIN kód jsou dobrou volbou pro dvoufázové~~aktorové~~ ověřování.
- Při vytváření nového hesla se vyhněte slovům, která se nacházejí ve slovníku, zájmenům~~ech~~, uživatelském~~ch~~ jménům~~ech~~ a dalším~~ch~~ předem definovaném~~ch~~ pojmům~~ech~~, stejně jako běžně používaným heslům.

3.~~Buduj znalosti —~~Online nakupování

Jak jsme se ~~-již viděli~~dozvěděli, kybernetická bezpečnost ~~vyvíjí~~ 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 ~~médiích~~, 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~~m~~ 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 ~~co je na internetu je sledováno~~na internetu je sledováno~~, není překvapením, že všechna data, která vyplývají~~ a z obrovského množství elektronického obchodování a interakcí na sociálních ~~médiích~~ sítích ~~vyplývá~~vzniká velké množství dat, ~~znamenají, že~~ je opravdu důležité ~~dopředu~~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:

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 ~~vystavení~~ odkrytí jeho čísla ~~hlavního účtu kreditní karty~~. K vytvoření tohoto typu kreditních karet můžete například použít Capital One.

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 ~~odrážejí poplatky~~se na nich vyskytují pouze platby, které jste ~~provedli~~si vědomi.

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.

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

Zdarma vždy nepředstavuje výhodu

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

Neposílejte e-mailem své finanční informace

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

3.Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: ~~FO~~DVC_~~Kyberbezpečnostní opatření~~Opatření kybernetické bezpečnosti_O3_O1:

Zadání: Jaké ~~jsou některé~~ informace~~, které~~ 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: ~~FO~~DVC_~~Kyberbezpečnostní opatření~~Opatření kybernetické bezpečnosti_O3_O2:

Zadání: Ze seznamu vyberte~~, správnou reakci, abyste se nestali obětí počítačové kriminality~~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 ~~má~~ používá šifrování.
- Než si něco objednáte, přečtěte si zásady reklamace a další podmínky a zásady ochrany osobních údajů webu.
- Platte debetní kartou, hotovostí nebo bankovním převodem.
- ~~-~~Pro ochranu důvěrnosti použijte „hotspot“.

4.~~Buduj znalosti —~~Cloud Computing

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

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.
~~Long gone are the days that you saved your files on a compact disc or even a pen drive, always with the dreadful feeling that you would eventually misplace those to never be found again. Nowadays, you can access your files on any computer and, in fact, currently cloud solutions are becoming more and more used worldwide on day-to-day activities.~~
~~You are constantly interacting with some type of cloud solutions when you are checking your email or while you are using your phone to check traffic conditions. With **cloud solutions your data is stored with a provider and accessed over the internet**.~~
~~Hence the question arising in this context is whether our data is safe and secured in the cloud? Because of that, it is important to know more about the concept of cloud computing.~~

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 computing** can be defined by the **delivery of on-demand IT resources** - such as storage, computing power or data-sharing capacity - over the internet, through hosting on remote servers.~~
~~In other words, cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive. These resources include tools and applications like data storage, servers, databases, networking and software. Cloud solutions are a very popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance and security.~~

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.
~~The cloud, big data and the digitalization of industry is accompanied by a growth in the exposure of vulnerabilities, enabling malicious people to target even more victims. The variety of attack types and their growing sophistication make it genuinely difficult to keep pace. Because of that, it is important to **implement some daily precautions in order to avoid theft, leakage and/or deletion of important information.**~~
~~Please see a brief summary of some measures that you can use in order to improve cloud computing security.~~

	Tradiční kombinace uživatelského jména a hesla často nestačí k ochraně

~~Use a multi-factor authentication~~ Použití vícefaktorové autentizace	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 V~~v~~ašim cloudovým aplikacím. Mezi příklady patří heslo kombinované s kódem zaslaným prostřednictvím SMS nebo s číslem vygenerovaným aplikací. Je také důležité, abyste se nezapomínali odhlásit~~vždy pamatovali na odhlášení~~ a nikdy neukládali své přihlašovací údaje na webech nebo v aplikacích. ~~The tradicional username and passwords combination is often insufficient to protect user accounts from hackers and stolen credentials is one the main ways hackers get access to your data/information.~~ ~~Because of that, you have to use not only **strong passwords** but also a **multi-factor authentication** - also known as two factor authentication - to ensure that only authorized personnel can log in your cloud apps and access that sensitive data.~~ ~~A multi-factor is one the most effective ways of keeping hackers from accessing your cloud applications. Some examples of multi-factor authentication are a password combined with a code sent over SMS or a number generated by an app.~~ ~~It is also important that you always remember to log out and never save your credentials.~~
~~Manage your user access to improve cloud computing security~~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. ~~Most people don't need access to every piece of information, every application or every file. Therefore, **seeting proper levels of authorization** ensures that each people can only view or manipulate the applications or data/information.~~ ~~If someone has access to everything and gets tricked by a phishing email and inadvertently provides their log in information, the hacker has access to all the information very easily.~~
Monitorujte, zaznamenávejte a	**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

analyzujte aktivity uživatelů pomocí automatizovaných řešení pro detekci vetřelcůMonitor, log and analyze user activities with automated solutions to detect intruders	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 / lidéosoba mámají různé potřeby pro různé úrovně kybernetické bezpečnosti, nezapomeňte proto před provedením velké investice do zabezpečení získat posouzení možných rizik od třetí nezávislé strany.názor třetí nezávislé strany pro posouzení rizik. **Real-time monitoring and analysis of user activities** can help you notice eventual irregularities that deviate from normal behaviours/patterns. These unusual activities could indicate a breach in your system so catching them early on can stop hackers in their tracks and allow you to fix security issues before things go wrong. You can find many solutions for automated 24/7 networking monitoring and management and moving up to advanced cybersecurity solutions. Because every business/people has different needs for different levels of cybersecurity be sure to get a third part for risk assessment before making a big investment.
Anti-phishing trainingAnti-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. Hackers can gain access to secure information by stealing credentials through some techniques such as phishing, spoofing websites and social media spying. Because of that, keep in mind that, for instance, **phishing training** should be a continuous process that needs to be managed by someone withing the organization in oder to make it effective.
Zálohujte soubory v různých cloudových účtech Back up files in different cloud accounts	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. Regardless of scale, industry, region and/or people, ensuring data availability is a priority for everyone. In addtion, losing data/information due to human

	~~error is very high so don't put all your important data in one place.~~ ~~Whether you're protecting and accessing the files on your personal laptop or you're a managed service provider responsible for a portfolio of business (and their growing amounts of data), cloud apps are essential in the modern digital world.~~ ~~Therefore, it is crucial to find more than one cloud-to-cloud backup solution to ensure a copy of the data you create, store and share in a safe location.~~

4. Procvičte si znalosti

Cvičení JEDNA MOŽNOST

Související dílčí výukový cíl: FO_~~Kyberbezpečnostní opatření~~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. ~~Číslo bankovního účtu~~
- 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: ~~FO~~DVC_~~Kyberbezpečnostní opatření~~Opatření kybernetické bezpečnosti_O4_O2~~:~~

Zadání: ~~Ze seznamu prosím vyberte správnou reakci~~K~~,~~ ~~k~~které chování Vám pomůže nestát se obětí kybernetického zločinu?~~.tak abyste se nestali obětí kyberkriminality.~~
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 ~~všudypřítomnosti~~být všudypřítomní. Internet zmenšil vzdálenosti~~Zúžil mezery~~ mezi lidmi, podniky a místy. Umožnil lidem být pouhým kliknutím kdekoli a s kýmkoli ~~a to pouhým kliknutím~~. Jak jste měli možnost v této kapitole zjistit,~~li~~ ~~v celé této obsahové jednotce,~~ za online soukromí a bezpečnost osobních údajů nesou společnou odpovědnost všechny strany: vláda, vývojáři softwaru, poskytovatelé cloudových služeb, společnosti ~~i~~a koncoví uživatelé.
Se zavedením GDPR získávají koncoví uživatelé důvěru v zabezpečení svých dat~~Zavedením GDPR získávají koncoví uživatelé důvěru ve svou ochranu údajů~~, 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: mějteít jedinečná a silná hesla s ~~dvoufaktorovým~~ dvoufázovým ověřením při přihlašování a měňteit 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 soukromáé ~~informace~~ data uloženáé v cloudu, ujistěte se, že neshromažďujete všechny své informace pouze do jednoho cloudu!
Třetím pravidloem ~~je procvičováníse~~ týká chytrého ~~procházeníbrouzdání~~ 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.~~Celkově musíte uznatNa závěr berte v potaz fakt~~, ~~že jsou to~~ Vvaše údaje, které by nakonec mohly být ohroženy kyberútokyy, a v ~~důsledku tohoproto jste zodpovědní za to musíte zajistit, že budete dodržovat svou část~~ pravidel ~~ochrany soukromí a zabezpečení dat na internetu.~~

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

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

Správné odpovědi

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.

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.

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.

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.

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.
- Platťte debetní kartou, hotovostí nebo bankovním převodem.
- Pro ochranu důvěrnosti použijte „hotspot".

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.

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.