Příručka kybernetické bezpečnosti

Obsah

Úvod

Právě začínáte číst teoretickou část příručky kybernetické bezpečnosti, která je určena k edukaci zaměstnanců ve vaší organizaci i všech uživatelů moderních technologií.

První část seznamuje čtenáře s problematikou škodlivých programových kódů. Je v ní stručně popsáno, jak se škodlivý kód šíří, co všechno může dokázat a co dělat pro to, aby se zabránilo zbytečným problémům.
Druhá kapitola je věnována méně zmiňovanému typu útoku - sociálnímu inženýrství. V textu jsou popsány typické způsoby a varovné příznaky podobného jednání. K dispozici jsou rovněž postupy pro případné ověřování totožnosti neznámé osoby.
Třetí kapitola varuje před podvodnými e-maily - tzv. phishingem.
Ve čtvrté části je čtenáři objasněn smysl webových certifikátů a také postup, jak kontrolovat správnost webové adresy.
Připojení k veřejné síti nemusí být bezpečné. Pátá kapitola vysvětluje proč a nabízí způsob řešení. Dále je zde zmíněná síť Eduroam.
Útočníci pro své cíle nevyužívají jen softwarové prostředky, je nutné dbát i na bezpečnost fyzickou. Tomuto tématu se věnuje pátá kapitola.
Hesla jsou klíčovým faktorem v ochraně systémů a uživatelských účtů. Šestá kapitola nabízí návod, jak volit silná hesla a jak taková hesla bezpečně ukládat.
Sedmá část je věnována problematice zálohování - jejímu významu, frekvenci a způsobu. Jsou zde rozebrány výhody a nevýhody záloh na pevná média a do cloudových úložišť. Závěrečná část radí čtenáři, jak se konkrétně zachovat ve specifických situacích, které mohou nastat a nejsou tak neobvyklé, jak by se na první pohled mohlo zdát.

Materiály nemají čtenáře zahltit nepřeberným množstvím informací, jejich smyslem je naopak snaha o zdůraznění významných bezpečnostních rizik a metod, jak hrozbám předcházet. O konkrétních postupech je šířeji pojednáno ve volně navazujících materiálech pro praktické použití.

Malware

Malware (často nesprávně virus) je souhrnný název pro škodlivý software. Účelem takových programů je poškození nebo vniknutí do počítačového systému.

Šíření malwaru

Způsobů, jak infikovat počítač, je celá řada. Mezi nejčastější způsoby infekce patří:

- otevření e-mailové přílohy (virus),
- instalace pirátských programů - malware je ukrytý v legitimním programu (trojský kůň),
- skrze díru v neaktualizovaném systému/programu - malware je schopen se šířit bez interakce s uživatelem (červ).

Schopnosti malwaru

- poškození dat - zašifrování, smazání,
- sledování - zaznamenávání stisku kláves, snímky obrazovky, historie prohlížení, krádež dat,
- zobrazování reklam,
- odkazování na jiné stránky, než které požadujeme,
- “Zotročení” počítače - systém je zahrnut do takzvaného botnetu (skupina napadených počítačů). To znamená, že počítač čeká na příkazy vlastníka botnetu, který většinou skrze tuto farmu útočí na další systémy.

Obrana proti malwaru

Malwaru je nutno se bránit několika způsoby.

Prvně je třeba udržovat operační systém včetně **všech instalovaných programů** aktualizovaný. Proto když vás systém nebo program informuje, že je k dispozici aktualizace, s aktualizací neotálejte a proveďte ji ihned.

Jako další vrstva obrany slouží antivirový program. Na trhu existuje antivirových programů zdarma (např. Avast, Avira, AVG). Vždy mějte zapnutou ochranu v reálném čase a čas od času proveďte úplný scan systému.

Brána firewall slouží k omezení provozu, který na zařízení putuje z počítačové sítě. Neumí se tedy vypořádat s viry a nedokáže zabránit před infikováním uživatele nakaženým souborem, střeží však přístup k potenciálně zranitelným systémovým prostředkům.

Jako poslední vrstvu ochrany bychom mohli brát samotného uživatele.

Poučení

- **Mějte na svém zařízení nainstalován antivirový produkt.**
- **V antiviru mějte zapnutou ochranu v reálném čase.**
- **Používejte antivirovou ochranu i na mobilech a tabletech.** V současnosti jsou oblíbeným cílem.
- **Neodkládejte aktualizace.**
- **Nevypínejte firewall.**
- **Neotevírejte přílohy od neznámých odesílatelů.**

- Nedůvěřujte přílohám e-mailů, které nejsou elektronicky podepsány. Ani PDF/Word/Excel dokumentům, prezentacím nebo archivům. **Nechte přílohy zkontrolovat antivirem.**
- **Pokud jste odkázáni na stránky, které běžně používáte, zadejte adresu do prohlížeče ručně, neklikejte na odkaz.** Některé znaky si mohou být natolik podobné, že rozdíl nepoznáte.
- **Nestahujte žádný software z podezřelých stránek** (zejména pornografických)
- **Nenavštěvujte podezřelé, podvodné a infikované stránky.**
- **Neinstalujte programy, pokud systém hlásí, že nebylo možné ověřit vydavatele.**
- **Nestahujte nelegální kopie programů.** Často bývají infikovány.
- **Nepoužívejte jednoduché přihlašovací údaje.** Malware se pomocí údajů typu admin:admin, admin:abc123 a podobných pokouší o získání přístupu.
- **Zálohujte.** V případě infekce tak můžete obnovit jinak ztracené soubory.

Sociální inženýrství

Sociální inženýrství (též nazývané sociotechnika) je soubor metod určených k ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že útočník je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopen využít osoby, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.

Typické způsoby sociotechnického útoku

- Jsem nový zaměstnanec, jak se dělá X?
- Nemůžu se dostat do práce, můžeš mi poslat X?
- Okamžitě mi pošli X, šéf zuří.
- Můžeš mi vytisknout dokument?
- Jsem technik. Kdyby byl problém, zavolej mi na toto číslo.
- Jsem technik. Něco nefunguje, ale když mi dáš heslo, opravím to.
- Jsem technik. Nainstalujte si X, ať vám počítač funguje.
- Zkuste, jestli vám funguje X.
- Který systém/server používáte?

Varovné příznaky útoku

- neobvyklá žádost,
- ohánění se autoritou,
- zdůrazňování naléhavosti záležitosti,
- hrozba důsledky nevyhovění žádosti,
- neochota volajícího odpovídat na dotazy,
- zmiňování mnoha jmen,
- komplimenty, pochlebování nebo flirtování.

Postup pro ověřování totožnosti (od nejlepší varianty)

1. **Záruka** - Požádejte důvěryhodného pracovníka, aby se zaručil za totožnost volajícího.
2. **Nadřízený** - Kontaktujte bezprostředního nadřízeného pracovníka a požádejte ho o ověření pracovníkovy totožnosti a statutu.
3. **Bezpečný e-mail** - Požádejte o e-mail s elektronickým podpisem
4. **Osobně** - Požádejte volajícího, aby vás navštívil osobně s identifikační kartou.
5. **Zpětné volání** - Zavolejte volajícímu na číslo z oficiálního telefonního seznamu.
6. **Identifikace volajícího na displeji telefonu** - Volá z firmy? Souhlasí zobrazené jméno?

Postup pro ověřování statutu pracovníka (od nejlepší varianty)

1. **Seznam pracovníků** - Nachází se volající na seznamu pracovníků organizace?
2. **Nadřízený** - Zavolejte šéfovi volajícího na číslo uvedené v oficiálním telefonním seznamu organizace.
3. **Útvar** - Zavolejte na útvar, ve kterém volající pracuje, a zeptejte se, jestli je pracovníkem.

Postup pro ověřování potřeby informace (od nejlepší varianty)

1. **Pracovní zařazení** - Zkontrolujte v interním seznamu zaměstnanců, kteří pracovníci jsou oprávněni dostávat příslušnou informaci.
2. **Potvrzení od nadřízeného** - Kontaktujte svého nadřízeného, aby vyřízení žádosti schválil.
3. **Potvrzení od vlastníka informace nebo pověřené osoby** - Zeptejte se vlastníka informace, zda žadatel potřebuje informaci, o kterou prosí.

Kritéria pro ověřování externích osob

- **Vztah** - Zkontrolujte, jestli má firma, kterou žadatel reprezentuje, odpovídající vztah.
- **Totožnost** - Ověřte totožnost osoby a stav zaměstnání v její firmě.
- **Mlčenlivost** - Zkontrolujte, jestli osoba podepsala závazek mlčenlivosti.

Práce s PC

Zkušený sociotechnik dokáže svou oběť přesvědčit, aby na počítači či jiném zařízení provedla takové operace, které mu zajistí neomezený přístup do systému. Získává tak citlivé interní informace a znalosti výhodné k dalším fázím útoku.

Instrukce pro práci s počítačem vám může dávat

- nadřízený,
- manažer kybernetické bezpečnosti, ICT koordinátor, správce sítě.

Instrukce pro práci s PC nesouvisející s popisem vaší práce vám mohou být předány

- osobně,
- elektronicky podepsaným e-mailem,
- telefonicky (pouze pokud je identita ověřena),
- prostřednictvím dokumentace organizace,
- přes HelpDesk organizace.

Nepostupujte podle instrukcí cizího člověka nebo podle nesprávně předaných instrukcí.

Poučení

- **Sociotechnikům se hodí každá informace o osobách a interních postupech**, usnadní jim to změnu identity.
- **V případě nejasností se nebojte kontaktovat svého nadřízeného.**
- Osoba odkazující se na autoritu nemusí mluvit pravdu - **nebojte se autoritu zpochybňovat**.
- Pokud není doručený e-mail elektronicky podepsán, mohl jej poslat kdokoli. **V případě žádosti o přístup nebo užitečnou informaci je nutné identitu a požadavek ověřit**.
- **Nesdělujte nikomu žádné osobní ani vnitropodnikové informace, ledaže byste poznali hlas na opačném konci a ten by dané informace opravdu potřeboval.**
- **Znalost firemních postupů a žargonu nikoho neopravňuje k žádosti o informace** - může jít o bývalého zaměstnance či externí entitu.
- **Sociotechnici k útokům využívají zastrašování, vinu a soucit**. V takových chvílích je třeba zpozornět.
- **Bez souhlasu vedení nikdy neposílejte soubory lidem, které osobně neznáte.**
- **Jakékoli organizace uživatelské jméno lze dohledat, jeho znalost k ověření nestačí.**
- **Požadavky, které vyžadují písemnou žádost, nesmí být vyřízeny pouze na základě prosby nebo příkazu.**
- **Neotvírejte přílohu e-mailu bez elektronického podpisu.**
- **Nepostupujte podle instrukcí cizího člověka nebo podle nesprávně předaných instrukcí.**

Více v knize MITNICK, Kevin D. a William L. SIMON. Umění klamu. Gliwice: Helion, 2003. ISBN isbn:83-7361-210-6.

Phishing

Phishing je technika, kdy se útočník snaží pomocí podvodné zprávy vylákat z uživatelů důvěrné informace jako přihlašovací údaje k účtům, PIN ke kartám atd.

```
Vážený uživateli elektronické pošty,

velikost Vaší poštovní schránky na VŠB-TU Ostrava se blíží ke svému limitu.
V tuto chvíli Vaše schránka zabírá 99,4% z dostupné kapacity.
Prosím, protřiďte si Vaši schránku. Pokud si ji neprotřídíte, nebude Vám po
zaplnění Vaší schránky doručována pošta, a to až do doby, než si ji
protřídíte a uvolníte tak místo pro nové zprávy.

V případě, že si nejste jisti, co po Vás chceme, můžete kontaktovat
oddělení Helpdesku CIT na telefonu 5666 nebo e-mailem na adrese hd@vsb.cz.
Nebo postupujte podle následujícího návodu:
https://www.sso.vsb.0l.cz/index.php?lang=cs&service=https%3A%2F%2Fidoc.vsb.c
z %2Fxwiki%2Fwiki%2Finfra%2F

Velikost Vaší poštovní schránky se řídí směrnicí rektora o elektronické
poště ze dne 15.10.2009
(https://www.vsb.cz/share/uploadedfiles/secured/smernice/SME_09_002.pdf)
a Provozním řádem elektronické pošty
(https://www.vsb.cz/share/uploadedfiles/secured/smernice/Provozni_rad_MAIL.p
df).
Maximální velikost diskového prostoru poštovní schránky je stanovena
pro zaměstnance ve výši 5000 MB, pro studenty ve výši 500 MB.

Správci poštovních serverů VŠB-TU Ostrava

VŠB-TU Ostrava
Centrum informačních technologií
```

Za účelem pročištění poštovní schránky na falešný e-mailový portál přistoupilo a zadalo své přihlašovací údaje 582 uživatelů. Naštěstí se tehdy jednalo pouze o plánovaný interní test. Útoky tohoto typu jsou však na denním pořádku. Phishing je jedna z variant sociálního inženýrství.

Nejlepší obranou proti podvodným e-mailům je selský rozum.

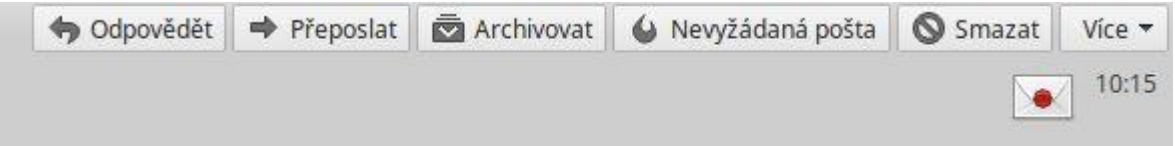
- Jak můžu mít zaplněnou schránku? Nikdy to nebylo více než z 5 %.
- Proč mě odkazuí na https://www.sso.vsb.0l.cz? Vždy to bylo https://www.sso.vsb.cz.
- Přišlo to i kolegyni? Není podivné, že se nám oběma zaplnila schránka ve stejný den?

Další běžné varovné signály:

- text obsahuje jazykové chyby,
- ve zprávě se vyskytují fráze, které odesílatel nikdy nepoužívá,
- odesílatel po mně chce něco, na co evidentně nemá nárok,
- typ přípony neodpovídá jejímu významu (faktura bývá v PDF formátu, ne archiv nebo spustitelný soubor!)

Odesílatel

Protokol pro zasílání e-mailů je bohužel navržen tak, že pole Odesílatel lze jednoduše podvrhnout. Jedinou zárukou platnosti adresy odesílatele je elektronický podpis. Platný podpis lze ve většině e-mailových klientů poznat podle ikony zapečetěné obálky.



Poučení

- **Poli Odesílatel (From) nelze důvěřovat, technicky je možné poslat e-mail jménem někoho jiného!**
- **Digitálně podepsaným e-mailům je možné důvěřovat.** U nich je matematicky zaručeno, že je pole Odesílatel (From) platné.
- Nedůvěřujte přílohám e-mailů, které nejsou elektronicky podepsány. Ani PDF/Word/Excel dokumentům, prezentacím nebo archivům. **Nechte přílohy zkontrolovat antivirem.**
- **Pokud jste odkázáni na stránky, které běžně používáte, zadejte adresu do prohlížeče ručně, neklikejte na odkaz.** Některé znaky si mohou být natolik podobné, že rozdíl nepoznáte.

Více na https://idoc.vsb.cz/xwiki/bin/view/pc/bezpecnost/phishing/.

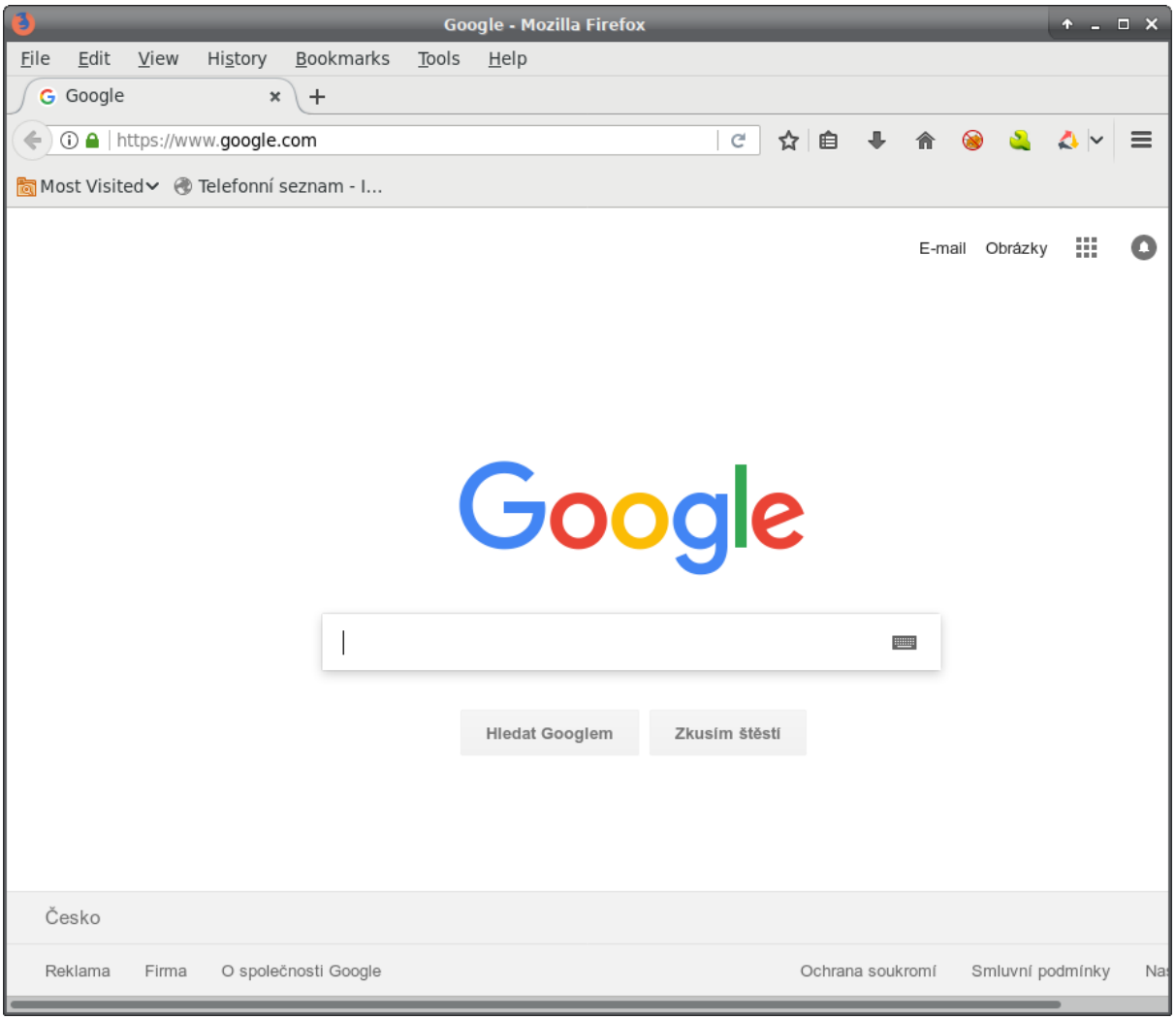
Přístup na webové stránky

Pro zkušeného útočníka není problém vytvořit falešné webové stránky a pomocí sociálního inženýrství či phishingu přimět uživatele, aby je navštívil. Útočník tak může získat citlivé údaje různého charakteru (přihlašovací údaje, číslo kreditní karty atd.) Z tohoto důvodu je většina stránek zabezpečena certifikáty.

Webové certifikáty

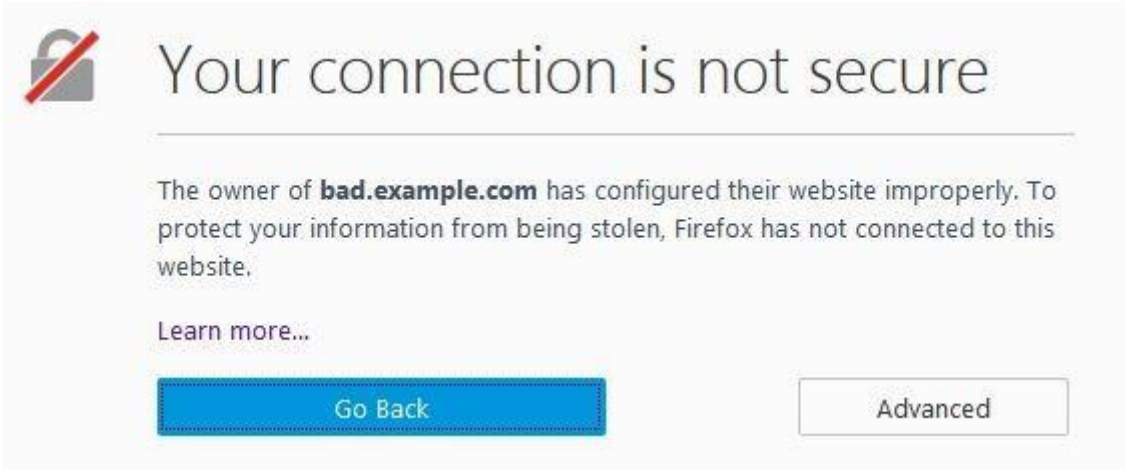
Z formálního pohledu je certifikát *veřejný šifrovací klíč digitálně podepsaný důvěryhodnou třetí stranou (certifikační autoritou)*. V praxi to znamená, že data odesílaná na konkrétní webové stránky prakticky nelze odposlouchávat.

Stránky s certifikátem mají na začátku adresy text *https://* a obvykle mají vedle adresního panelu zelenou ikonu zámku.



Problémy s webovými certifikáty

Prohlížeč Vás na podezřelé certifikáty upozorní:



Nejčastěji se můžete setkat s těmito příčinami problému:

SEC_ERROR_EXPIRED_CERTIFICATE - Certifikát vypršel, je neplatný. Počkejte, až správce webu problém opraví.

SEC_ERROR_UNKNOWN_ISSUER - Certifikát nebyl potvrzen důvěryhodnou certifikační autoritou, stránka je podvržená! **Nevstupovat** .

SSL_ERROR_BAD_CERT_DOMAIN - Certifikát je platný, ale pro jinou stránku. Buď se jedná o chybu správce nebo je stránka podvržená! **Nevstupovat** .

Formát URL adresy

I podvodná stránka může být opatřena certifikátem. proto je nezbytné ověřovat, že skutečně pracujete na požadované stránce. Jak to provést?

Jako příklad použijme https: //sapweb. vsb. cz/ irj/portal

Z adresy poznáme, že:

1. je navštívena přes protokol https: //, tedy zabezpečeným způsobem,
2. jedná se o českou (cz) doménu,
3. konkrétně vsb .cz, která je přidělena VŠB,
4. správci domény vsb.cz vytvořili subdoménu sapweb ,
5. konkrétní obsah stránky je (zjednodušeně řečeno) umístěn v souboru /irj/portal . To už není příliš podstatné, z předchozích bodů víme, že stránka spadá pod VŠB.

Je třeba zdůraznit, že doména (část mezi definicí protokolu a prvním následujícím lomítkem) vzniká zprava doleva a podstatný je tedy její konec! Adresa hackers.vsb.cz by tedy *spadala* pod VŠB, vsb.hackers.cz *nikoliv* !

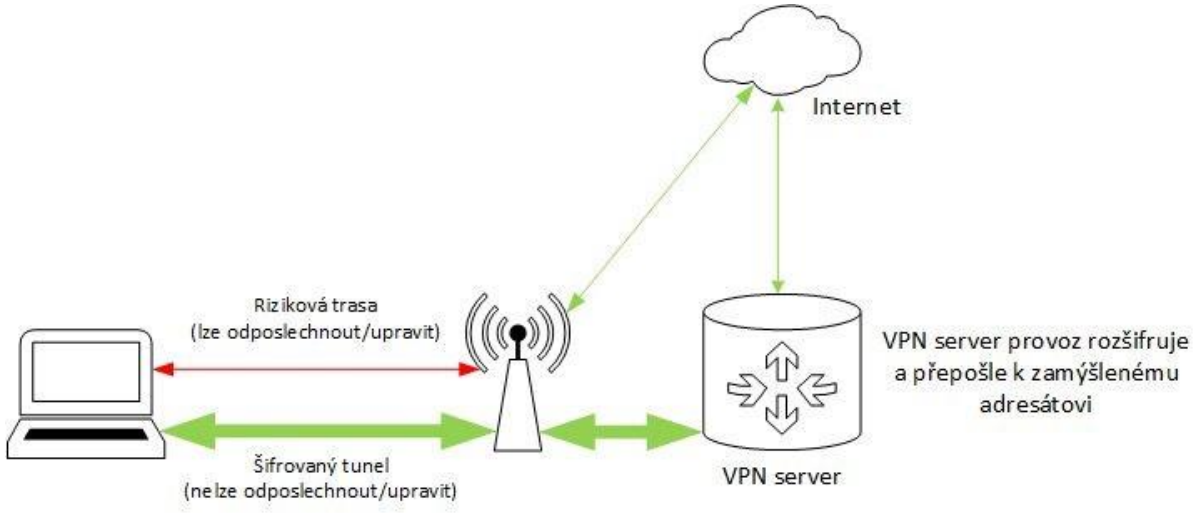
Poučení

- **Nikdy nezadávejte citlivé údaje na nesprávně zabezpečené nebo nezabezpečené stránky!**
- **Neignorujte upozornění prohlížeče na problém se zabezpečením!**
- **Kontrolujte, zda jste skutečně navštívili správnou stránku.**

Veřejná Wi-Fi

Málokdo si uvědomuje, že uživatele připojené k veřejné Wi-Fi síti lze relativně snadno odposlechnout. Ve špatně zabezpečené síti je dokonce útočník schopen veškerý provoz přesměrovat přes své zařízení a takový provoz upravit (vložení malwaru apod.). Provoz také často upravuje samotný provozovatel sítě, kdy se nejčastěji jedná o přidávání reklam při prohlížení webu, či sledování celkové aktivity uživatele.

Těmto problémům se lze relativně snadno bránit použitím VPN. Při jejím použití se na zařízení vytvoří šifrovaný tunel do důvěryhodné sítě a veškerý provoz směřuje přes něj. Šifrování pomocí matematických funkcí zaručí, že s provozem nikdo nemanipuloval a že provoz není čitelný nikomu jinému než zamýšlenému adresátovi.



Pozor na poskytovatele VPN, kteří služby poskytují zdarma. Tito poskytovatelé často také s provozem manipulují, nebo ho sledují. Při vybírání poskytovatele si vždy ověřte, že je důvěryhodný.

EDUROAM

Pro bezpečné připojení je potřeba nakonfigurovat připojení do sítě EDUROAM.

Při konfiguraci postupujte přesně podle návodu a nevynechávejte žádné kroky. Pro bezpečné připojení je nezbytné ověřovat identitu serverů pomocí certifikátu. V opačném případě se vystavujete riziku, že se přihlásíte na počítač útočníka, který si vytvořil síť se stejným názvem (tzv. evil twin attack). Takový útočník může kromě manipulace/odposlechu provozu také získat vaše heslo. Reálný útok zaměřený na sběr hesel byl například v roce 2016 proveden na VŠE v Praze.

Konfiguraci sítě EDUROAM nemusíte provádět ručně. Lze si vše zjednodušit stažením automatického konfigurátoru z https://cat.eduroam.org /.

Poučení

- **Pokud se připojujete k nedůvěryhodné Wi-Fi síti, síti bez zabezpečení (open) nebo se zabezpečením typu WEP či WPA, využijte důvěryhodnou (např. školní) službu VPN.**
- **Na domácí Wi-Fi si nastavte zabezpečení WPA2 personal (osobní, též PSK) s dostatečně složitým heslem.**
- **Heslo k domácí Wi-Fi nesdělujte nedůvěryhodným osobám.**
- **Heslo k domácí Wi-Fi často měňte.**
- **Při konfiguraci sítě EDUROAM dodržte všechny kroky a žádný nevynechávejte.**

Fyzická bezpečnost

V předchozích kapitolách bylo řečeno, že útočník může získat přístup k systému prostřednictvím softwarových prostředků (malware). Existuje však další hrozba, která mnohdy nevyžaduje pokročilé znalosti IT technologií - hrozba fyzická. V následujících bodech jsou představena některá rizika, která hrozí při nesprávném nakládání s aktivy.

Rizika

- Osoba, která získala přístup k zapnutému počítači s přihlášeným uživatelem, může pod cizí identitou provádět cokoliv.
- Osoba, která získala přístup k vypnutému počítači s nešifrovanými disky, získává přístup ke všem souborům, často i k těm smazaným. Mimo jiné se jedná o stažené soubory, vytvořené dokumenty, e-maily, uložená hesla.
- Osoba, která získala přístup k volně položenému flashdisku, získává přístup ke všem souborům na flashdisku, často i k těm již smazaným.
- Osoba, která získala přístup k hardwarovým prostředkům podle výše uvedených odstavců, může do systému nasadit malware, který bude útočníkovi poskytovat trvalý přístup do systému a dále sledovat veškerou aktivitu legitimního uživatele včetně stisku kláves, odposlouchávání zvuku a snímání všeho, co lze vidět na monitoru a z webkamery. I vypnutá webkamera může být softwarovými způsoby útočníkem zapnuta.
- Osoba, která získala přístup k cizí identifikační kartě, se může za svou oběť vydávat - získává přístup do chráněných prostor, využije kredit k nákupu apod. Kartu lze naklonovat, jednou získaný přístup ústí v přístup trvalý.
- Heslo na papírku na stole, na monitoru nebo pod klávesnicí, heslo sdělené kolegovi nebo IT podpoře je zbytečné heslo, již neslouží k ochraně.
- Dokumenty s citlivými údaji ležící na stole si může přečíst (případně vyfotit) kdokoli.
- Vyhozené dokumenty s citlivými údaji se dostávají do rukou dalších osob. Této metodě průniku se říká *dumpster diving*.

Poučení

- **Šifrujte disky.** Jen tak se při získání plného fyzického přístupu znemožní získání dat.
- **Při opuštění pracovní stanice si zamykejte obrazovku** (Windows: +L).
- **Hlídejte svá přenosná paměťová média.**
- **Nikomu nedávejte svou identifikační kartu.** Mimo nezbytné situace ani občanský průkaz, řidičský průkaz nebo kreditní kartu.
- **Nenechávejte citlivé dokumenty ležet na stole.**
- **Při nepřítomnosti si zamykejte kancelář.**
- **Nepotřebné dokumenty s citlivými údaji skartujte.** Skartování na proužky *nestačí* .
- **Pořiďte si posuvné kryty na webovou kameru.** Kameru pak odkryjte pouze při používání.

Práce s hesly

To, jak si hesla tvoříme a jak s nimi zacházíme, má obrovský dopad na naši bezpečnost. Nejdříve si řekneme, jak prolamování hesel probíhá, abyste mohli pochopit, z čeho vzešla doporučení, která budeme předkládat.

Jak může uniknout heslo

- **Chyba na webovém serveru**. Útočník tak získá databázi uživatelských jmen a hesel. Pokud užíváte všude heslo stejné, jsou tím de-facto prolomeny všechny vaše účty. Dopady takového úniku můžeme minimalizovat tím, že pro každou službu budeme používat jiné heslo.

- **Útoky hrubou silou, slovníkové útoky**. Útočník zkouší za pomocí speciálního algoritmu heslo uhádnout. Útok může probíhat pomocí slovníku, kde jsou již uniklá hesla, nebo vyzkoušením všech možných kombinací písmen a čísel. Jako obrana proti tomuto útoku je volit nepredikovatelná a dlouhá hesla. Odolnost hesel vůči útoku hrubou silou můžete vidět v tabulce.
- **Phishingový útok, sociální inženýrství**. Útočník vás zmanipuluje, abyste mu heslo sami řekli. Více o sociálním inženýrství se můžete dozvědět v samostatné kapitole.
- **Pomocí šmírovacího malwaru**. Více o malwaru a jak se mu bránit se lze dozvědět v samostatné kapitole.

	8 znaků	**12 znaků**	**15 znaků**	**Příklad**
malá/velká písmena	35 minut	8 let	2 miliony let	pepicekk
písmena	2 dny	377 tisíc let	53 miliard let	pEpiceKk
písmena + číslice	1 rok	3 miliony let	742 miliard let	pE8ic0Kk1
písmena + číslice + speciální znaky	46 let	459 milionů let	381 trilionů let	pE8*c0Kk!

Tab.: Demonstrace exponenciálního nárůstu doby uhádnutí hesla pomocí útoku hrubou silou

Sílu vlastního hesla je možné ověřit na stránkách https://howsecureismypassword.net/ nebo https://password.kaspersky.com/. Je vhodné *nezadávat* přesné heslo, ale heslo podobné. Stránka https://haveibeenpwned.com/ nabízí ověření, zda někdy nebyl prolomen účet s danou e-mailovou adresou.

Tvorba hesel

V předchozím textu jsme zmínili, že je dobré tvořit dlouhá hesla s co nejbohatší znakovou sadou. Problém však můžeme mít při jeho zapamatování. Pokud si chceme vytvořit silné heslo a zároveň si ho pamatovat, tak si můžeme například vymyslet nesmyslnou větu, kterou bude snadné si zapamatovat. Můžeme použít například: “V sámošce u Janka mi spadla Tatranka.” Takové heslo není prolomitelné slovníkovým útokem. Proti útokům hrubou silou je chráněno svou délkou i použitou znakovou sadou (malá/velká písmena, speciální znaky).

Ukládání hesel

Jedno z doporučení je nepoužívat stejné heslo na více službách. Jak si ale pamatovat všechna hesla, když máme dejme tomu 100 účtů? Dnes oblíbené a doporučované řešení je použití tzv. klíčenek (správců hesel). Z pohledu uživatele to vypadá tak, že si pamatuje jen jedno silné heslo do klíčenky. Ostatní hesla má uložena v ní a vůbec si je nemusí pamatovat.

Výhody klíčenek jsou následující:

- Stačí si pamatovat jedno heslo.
- Soubor s hesly je šifrovaný (nikdo nepovolaný si hesla nepřečte).
- Klíčenky obsahují generátory hesel, takže je nemusíte vymýšlet.
- Hesla nikdy nezapomenete. V klíčence zůstávají, dokud je nesmažete.

Mezi nevýhody klíčenek bychom mohli zařadit:

- Klíčenky je nutné **ZÁLOHOVAT** (viz. kapitola o zálohování).
- Při zapomenutí hlavního hesla ztrácíte přístup ke všem údajům v klíčence.

Mezi nejznámější klíčenky patří například KeePass (zdarma) nebo LastPass.

Poučení

- **Volte dostatečně dlouhá a neuhodnutelná hesla.**
- **Vyhněte se heslům admin, abc123, 12345, qwertz a podobným.** Ta útočníci zkoušejí nejdříve.
- **Nepoužívejte osobní údaje či jejich kombinaci jako heslo, útočníci tohoto fenoménu využívají.** Tyto údaje lze snadno dohledat. Jedná se zejména o jméno, login, telefonní číslo, datum narození, osobní údaje partnerů/dětí, jméno psa, číslo domu, přezdívka.
- **Nevolte jednoduchá (slovníková) hesla s tím, že nahradíte písmena za čísla** (např. nereknu -> n3r3knu). Algoritmy na prolamování hesel tato nahrazení zkouší.
- **Heslo nikomu nesdělujte.**
- **Heslo si nepište na papír.**
- **Nepoužívejte stejné heslo pro více služeb.**
- **Nesdělujte heslo IT zaměstnancům, nepotřebují ho.**
- **Jednou za čas svá hesla vyměňte.**
- **Nepřihlašujte se na cizím zařízení.** Hesla můžou být odchycena.
- **Nezadávejte citlivé údaje na nesprávně zabezpečené nebo nezabezpečené stránky.**

Zálohování

Lidé mnohdy začínají zálohovat až poté, kdy přijdou o cenná data. Může se jednat například o ztrátu rodinných fotografií za posledních 10 let (uživatel nezálohuje vůbec) nebo o ztrátu práce, na které zaměstnanec týden pracoval (nedostatečná frekvence zálohování). Abyste podobné problémy nemuseli řešit, musíte si zvolit vhodnou taktiku zálohování souborů.

Ztrátu dat může způsobit

- porucha pevného disku,
- napadení počítače ransomwarem (soubory se při napadení zašifrují a útočník za jejich zpřístupnění požaduje výkupné - i desetitisíce korun),
- chyba uživatele.

Jak často zálohovat?

Zde záleží čistě na vašem úsudku. resp. zálohuji data tak často, aby mě to při případné ztrátě nemrzelo, data jsem obnovil a pokračoval jako by se nic nestalo. U zvlášť cenných dat klidně několikrát denně.

Kde zálohovat?

Na výběr je více možností. Využít lze například externí pevné disky nebo tzv. cloudové služby (Google Drive, OneDrive, DropBox apod.), které při instalaci speciálního programu umožňují zálohování v reálném čase.

Výhody zálohy na externí pevný disk

- Vysoká kapacita úložiště.
- Pokud je PC napaden ransomwarem a není k němu disk připojen, záloha není dotčena. Při použití pevného disku na zálohy ho tedy **vždy** po provedení zálohy **odpojte**!

Nevýhody zálohy na externí pevný disk

- Disky jsou náchylné k poškození.
- Možnost získání přístupu k datům, pokud je disk odcizen a není šifrovaný. Je vhodné jej fyzicky zabezpečit proti krádeži.
- Zálohovat musíte manuálně.

Výhody zálohy na cloud

- Data mohou být zálohována v reálném čase.
- Přístup k datům máte z více zařízení. Lze využít i jako nástroj pro synchronizaci.

Nevýhody zálohy na cloud

- Nutné být připojen k internetu.
- Pokud se zálohuje v reálném čase a počítač napadne ransomware, tak jsou zašifrovány i vaše zálohy. Někteří poskytovatelé však umožňují detekci takového útoku a obnovu dat, takže byste data ztratit neměli. O této možnosti byste se před výběrem řešení měli informovat.
- Data se ukládají na servery cizí společnosti.
- Nelze zaručit, že poskytovatel cloudového úložiště nebude data prohlížet/přeprodávat.

Ideální je oba způsoby zálohy kombinovat.

Co přesně je cloud?

Cloud lze chápat jako poskytování služeb či programů pomocí internetu. Z hlediska bezpečnosti je třeba si uvědomit, že běh těchto služeb je zajištěn na infrastruktuře jejího poskytovatele a tam jsou také uložena data. Řada lidí proto ráda používá frázi: “Cloud je pouze cizí počítač.”

Je dobré si uvědomit, že soubory citlivé povahy by se do cloudu (na cizí počítač) ukládat neměly a když ano, tak v zašifrované formě. Výjimku může tvořit cloud poskytovaný zaměstnavatelem.

Poučení

- **Využívejte pro méně citlivá data cloudová úložiště.**
- **Citlivá data v čitelné podobě neukládejte na cloudová úložiště.**
- **Pravidelně provádějte fyzickou zálohu vašich dat.**

Životní situace

Zadal jsem přihlašovací údaje do phishingové stránky

1. Neprodleně si změňte heslo.
2. Přepošlete e-mail na adresu manažera kybernetické bezpečnosti nebo správce sítě, kde incident zpracuje bezpečnostní tým a prověří, zda se nenachytal i někdo další. Připište informaci o tom, že byl váš účet kompromitován a heslo jste si změnili.
3. Pokud prozrazené heslo používáte i na jiných službách, je nutné toto heslo změnit všude, kde ho používáte.

Přišel mi phishingový e-mail

1. Na e-mail nereagujte a neklikejte na odkazy v něm obsažené.
2. Zprávu přepošlete svému bezpečnostnímu týmu.

Mám zavirovaný počítač

1. Proveďte úplný scan antivirovým programem.
2. Všechny nalezené hrozby nechte odstranit.
3. Stáhněte si druhý antivirový scanner (např. online scanner firmy Eset nebo Kaspersky).
4. Proveďte scan druhým antivirem a všechny hrozby odstraňte.

Pokud si na odstranění malwaru netroufáte nebo se vám to nedaří, kontaktujte svého manažera kybernetické bezpečnosti nebo správce sítě.

Ztratil jsem pracovní notebook/telefon

V případě, že jste ztratil/a takové zařízení a nebylo šifrováno, tak proveďte následující kroky:

- Změňte si všechna hesla ke službám, které jste na zařízení používali.
- Pokud používáte stejná hesla i jinde, tak si je změňte také.
- Pokud byla na disku citlivá data, nahlaste tuto skutečnost vašemu nadřízenému.

Kontaktujte bezpečnostní tým svého zaměstnavatele

- pokud došlo, nebo máte dojem, že došlo k úniku dat,
- pokud máte dojem, že byl na vás proveden cílený útok,
- pokud jste způsobili bezpečnostní incident.

Pokud jste způsobili bezpečnostní incident, nebojte se ho nahlásit.