ZÁSADY BEZPEČNÉHO VYUŽÍVÁNÍ KYBERPROSTORU

Přednášející: Jiří Fišer

Zimní semestr 2023/2024

Podklady: NÚKIB

MVŠO MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB)

Ústřední správní orgán

- pro kybernetickou bezpečnost, ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.
- Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo.
- Vznikl 1. srpna 2017.
- https://www.nukib.cz/
- Věnuje se i širší veřejnosti: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

- OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.
- CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.

  Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.
- ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM (klávesová zkratka win + l). Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovnictví.
- AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
  Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.
- POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

- NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.

  Pro uchování přihlašovacích údajů používám šifrovaného správce hesel:

Funkce správců hesel:

- Generování silných hesel
- Ukládání hesel v šifrovaném formátu
- Automatické vyplňování hesel
- Synchronizace hesel mezi různými zařízeními

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

- NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.

  Pro uchování přihlašovacích údajů používám šifrovaného správce hesel:

Správce hesel

•Výhody:
- Zlepšená bezpečnost
- Ušetření času
- Zjednodušení správy hesel

•Nevýhody:
- Ztráta přístupu k hlavnímu heslu
- Útoky na správce hesel

Hesla uložená v prohlížeči

Výhody:
- Pohodlné
- Přizpůsobené prohlížeče

Nevýhody:
- Horší bezpečnost
- Ztráta přístupu k prohlížeči
- Útoky na prohlížeče

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

- ZAPÍNÁM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
  Pro útočníka představují potenciální cestu do zařízení.
- POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM TZV. VPN (Virtual Private Network)
  neboli virtuální soukromou síť, která zabezpečí mou komunikaci na potenciálně nebezpečné síti.
- ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
  Tak budou v případě ztráty nebo odcizení nečitelná.
- PRAVIDELNĚ ZÁLOHUJI DATA. Využít mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

- DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ. Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.
- PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS. Https protokol poznáme podle zámečku v adresním řádku:
- DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM. Je-li to technicky možné, zkontroluji, že odkaz nevede na podezřelou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.
- VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU. Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku apod.

BEZPEČNÝ POHYB V KYBERSVĚTĚ
JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

- K INFORMACÍM NA INTERNETU PŘISTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ. Při práci s informacemi mohu využít rady, které sepsala iniciativa ZVOLSI.INFO ve svém Surfařově průvodci internetem.
- NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MÉ RODINĚ, PŘÁTELÍCH NEBO SPOLUPRACOVNÍCÍCH. Data narození, náboženské vyznání nebo fotografie mohou být zneužity.
- INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMISŤUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM. Nikdy nevím, kdy může být takový materiál zneužit.
- PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY. Mohu se zeptat přátel nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěsím a zavolám zpátky na telefonní číslo z oficiálního seznamu.

BEZPEČNÝ POHYB V KYBERSVĚTĚ
JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

- NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
  V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.
- JAK PHISHING POZNÁM? “Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí.” Podvodník používá obecná oslovení typu „Vážený pane/í“ bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřele vyhlížející odkazy typu https://www.xbamka.cz.
- V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLNÝ. Vše, co na sebe prozradím, může být zneužito.

BEZPEČNÝ POHYB V KYBERSVĚTĚ
JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

- NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ. Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.
- RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNÉHO. Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.
- PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
  Útočníci rádi pracují s časovou tísní - teď je třeba něco vykonat, napravit, sdělit. Klid!
  Škoda z prodlení bývá menší než důsledky neuvážených činů.

BEZPEČNÝ POHYB V KYBERSVĚTĚ
JAK ZABEZPEČÍM SVÉ ONLINE ÚČTY?

- U SILNÉHO HESLA ZADÁVÁM ALESPOŇ 12 ZNAKŮ A VÍCE. Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.
- PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO. To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.
- NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SÍLY HESLA. Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.
- NESDÍLÍM PRIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚCTŮM A SLUŽBÁM. V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.

BEZPEČNÝ POHYB V KYBERSVĚTĚ
JAK ZABEZPEČÍM SVÉ ONLINE ÚČTY?

- U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI. Příkladem může být elektronické bankovnictví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, nechám si potvrzovací SMS zaslat na jiné zařízení.
- ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO Administrátorský účet používám pouze pro správu systému.
- NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu "příjmení třídní učitelky z páté třídy" nebo “nejmenší planeta sluneční soustavy”. Podobné informace jsou dohledatelné z veřejných zdrojů. Je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna“ zvolím odpověď „N9qy$_@?9b7G&_tp“.

RIZIKA KYBERNETICKÉHO PROSTORU
TRACKING COOKIES

Co je to?

- Malé soubory, které webové stránky ukládají do vašeho prohlížeče.
- Tyto soubory mohou být použity k sledování vašich aktivit na webových stránkách:
  - Například co prohlížíte,
  - jaké produkty si prohlížíte
  - nebo jak často navštěvujete webové stránky.

RIZIKA KYBERNETICKÉHO PROSTORU
TRACKING COOKIES

Možná nebezpečí

- Zneužití osobních údajů (poloha, zájmy nebo nákupní zvyklosti): Tyto údaje mohou být použity k cílení reklamy nebo k profilování uživatelů.
- Ztráta soukromí: Uživatelé a jejich aktivity na webových stránkách mohou být sledovány a zaznamenávány.
- Útoky na bezpečnost: Získání přístupu k osobním údajům uživatelů nebo k zavlečení malware.

DOMÁCÍ ZAŘÍZENÍ
IOT (INTERNET OF THINGS)

Co to je?

- Síť fyzických zařízení, která jsou připojena k internetu a mohou komunikovat mezi sebou a s dalšími systémy.
- Tato zařízení mohou být vybavena senzory, které shromažďují data o svém okolí, a mohou být ovládána na dálku.

Příklady zařízení IoT:

- Inteligentní domácí spotřebiče, jako jsou termostaty, osvětlení a zabezpečovací systémy
- Inteligentní dopravní systémy, jako jsou chytré semafory a kamery
- Inteligentní zdravotnické systémy, jako jsou zdravotnické senzory a monitorovací zařízení

DOMÁCÍ ZAŘÍZENÍ
VZTAH IOT A KYBERBEZPEČNOSTI

- Internet věcí představuje nové výzvy pro kyberbezpečnost.
- Tato zařízení jsou často méně zabezpečená než tradiční počítače a jsou náchylnější k útokům.

Hlavní hrozby IoT

- Únik dat: Útočníci mohou získat přístup k citlivým datům, jako jsou osobní údaje nebo obchodní tajemství.
- Útoky typu denial-of-service: Útočníci mohou způsobit, že zařízení IoT přestanou fungovat, což může mít vážné následky, například v případě dopravních systémů nebo zdravotnických zařízení.
- Útoky typu malware: Útočníci mohou nainstalovat malware na zařízení IoT, který může způsobit poškození zařízení nebo krást data.

DOMÁCÍ ZAŘÍZENÍ
VZTAH IOT A KYBERBEZPEČNOSTI

Jak se chránit?

- Aktualizovat software (firmware): Aktualizace software často obsahují opravy bezpečnostních chyb.
- Používat firewally a antivirový software (např. v rámci domácí sítě)
- Buďte opatrní s tím, co připojujete k internetu: Než připojíte nové zařízení IoT k internetu, ujistěte se, že je bezpečné.