

Osvětové materiály kybernetické bezpečnosti

#SecFest2021

Materiály na ZČU

- Dostupné na <https://bezpecnost.zcu.cz>
- Více info SecFest 2020 <https://secfest.zcu.cz/SecFest2020/>
- Výborný nápad z doby předcovidové
- Dnes forma nevhodná - připraveno na prezenční školení



1/10 **B E Z P E Č N O S T** **BEZPEČNOST.ZCU.CZ** **fondrozvoje cesnet**

Základní principy a motivace

Internet je jen dalším prostředím v reálném světě. A stejně jako v reálném světě se v něm pohybují lidé dobří i zlí. A jelikož se ve světě Internetu často přidává předpoda kyber, můžeme se u těch zlých setkat s pojmy jako kyberpodvodník nebo kyberkriminalník.

Proti těmto kyberkriminalníkům je nutné se bránit a tato série vzdělávacích materiálů by čtenáři měla ukázat, že základy kyberbezpečnosti zvládne každý.

DORRÝ PENÍ JA JSEM KYBERKRYMINÁLNIK.
KRADÍ VAŠE HESLA, POSÍLÁ SPAMY, HOŘKY A VYDRÁM.

MÉ ČALÉŠNÉ JMÉNO JE EMANUEL HRÍZA A BYDLÍM NĚKDE NA INTERNETU.
NIC MI NENÍ SVATÉ, BUDU VÁM LHÁT A SPOLEHAT NA VAŠI DŮVĚŘIVOST.

JSEM PROFESIONÁLNÍ ZLOUPÍN. MOŽE PRÁCE MNE BAVIT A OBČAS JE LUKRATIVNÍ.
VE VOLNÉM ČASE MNE BAVÍ A OBČAS JE LUKRATIVNÍ.

VE VOLNÉM ČASE MNE BAVÍ A OBČAS JE LUKRATIVNÍ.
VE VOLNÉM ČASE MNE BAVÍ A OBČAS JE LUKRATIVNÍ.

Základní principy

Kybersvět je založen na informacích, kterým často říkáme data, a kyberbezpečnost má za úkol zajistit dostupnost, důvěrnost a integritu těchto dat.

- **Dostupnost** - data mám k dispozici, kdykoli je potřebuji
- **Důvěrnost** - data dostane jen ten, komu patří nebo kdo má na ně nárok
- **Integrita** - data jsou nezměněna a nepoškozena

Stejně jako v běžném životě, tak i při ochraně dat platí princip nejslabšího článku a využívá se víceúrovňová obrana. Oba pojmy si nyní vysvětlíme.

Princip nejslabšího článku

Název vychází ze známého faktu, že řetěz je tak pevný, jak je pevný jeho nejslabší článek. Ten se přetrhne jako první a jeho funkce je tím porušena. Stejně tak si kyberútočník může vybrat cestu, jakou se vydá k cíli a vybírá si často tu nejsnadnější.

Vicestupňová obrana

Útočník často potřebuje rychle uspět a jít tzv. o dům dál. Pokud mu ale v jeho činnosti bráníme několika překážkami, které musí postupně překonávat, jeho činnost mu zkomplikujeme a útočník to buď předčasně vzdá, nebo narazí na takovou překážku, kterou již nebude schopen překonat.

Stejně k obraně přistupovali i architekti středověkých hradů, kdy nepoužívali jen hradby, ale třeba i vodní příkop.

V IT můžeme víceúrovňovou obranu demonstrovat na možnostech zabránění spuštění viru z přílohy v e-mailové zprávě:

- Antivirová kontrola na poštovním serveru odstraňuje zavirované přílohy
- Poučený uživatel pochybnou přílohu vůbec neotevře
- Antivirový program běžící na počítači blokuje pokusy o spuštění viru

Pokud alespoň jedno z výše uvedených opatření zabere, nesplní virus svůj úkol infikovat cílový počítač.

Cena za bezpečnost

Každé opatření něco stojí a cenu za bezpečnost je třeba srovnat s tím, jakou hodnotu opatření chrání.

Prevence

Vždy je lepší problémům předcházet, než je řešit. Vhodnými preventivními opatřeními jsme schopni snížit pravděpodobnost výskytu problému nebo snížovat jeho dopad.

Školení uživatelů je efektivní forma prevence, protože uživatel často bývá tím slabým článkem v řetězu opatření.

Řešení problémů

I při sebelepší prevenci může k problémům dojít a musíme být jednak připraveni, ale hlavně se musíme z problému poučit, aby dopady případného dalšího výskytu byly již zanedbatelné nebo žádné.

Jsem leták ke školení IT bezpečnosti uživatelů síť ZČU. Školení má 10 témat. Má, ostatní letáky, brožury a prezentace najdete na <https://bezpecnost.zcu.cz>.


Naši almu mater je Západočeská univerzita v Plzni a na svět jsme přišli také díky podpoře Fondu rozvoje CESNET, z.s.p.o.

Materiály jejichž základem byly materiály ZČU

- Dostupné na <https://bezpecnost.czu.cz/cs/r-14478-nase-cinnost/r-16977-bezpecnostni-desatero>
- Přepřacováno do webové prezentace + informační listy

ZÁKLADNÍ PRINCIPY A MOTIVACE

Internet je jen dalším prostředím v reálném světě. A stejně jako v reálném světě se v něm pohybují **lidé dobří i zlí**. A jelikož se ve světě Internetu často přidává předpona kyber, můžeme se u těch zlých setkat s pojmy jako kyberpodvodník nebo kyberkriminálník

1 
B E Z P E Č N O S T N Í
D E S A T E R O

Příklad principu nejslabšího článku v IT

Plán útočnicka na získání důvěrné informace v informačním systému, ke kterému má uživatel přístup:

- **Získání informace** od uživatele manipulativním dotazem.
- **Získání hesla** uživatele pomocí phishingu.
- **Přečtení informace** z opuštěného počítače, kde je uživatel přihlášen.
- **Ovládnutí** („hacknutí“) informačního systému.

Útočnickovi by k získání informace stačila realizace libovolného z výše naznačených plánů.

Prevence v IT

Ransomware je škodlivý kód šířený různými způsoby (emailem, přenosnými úložišti). Po jeho spuštění dochází k zašifrování, a tedy k znečitelnění souborů. Po zašifrování se zpravidla následně zobrazí informační stránka s pokyny k zaplacení výkupného. Proti tomuto typu útoku se můžeme bránit:

- **Zálohováním** – při zašifrování souborů je obnovíme ze zálohy (snížení dopadu).
- **Technickými prostředky** – zabraňují spuštění škodlivého kódu (snížení pravděpodobnosti výskytu).
- **Pojištěním** – uhradíme výkupné z pojistného plnění (přenesení odpovědnosti).

Uvedená opatření lze samozřejmě kombinovat.

Řešení problémů

I při sebelepší prevenci může čas od času k problémům dojít a **je potřeba být připraven**. Zachovejte klid, nezatajujte informace, spolupracujte. Kontaktujte někoho, kdo Vám dokáže pomoci. Může to být Váš kamarád, kolega, lokální IT správce nebo Helpdesk ČZU.

 Česká zemědělská univerzita v Praze
Odbor bezpečnosti

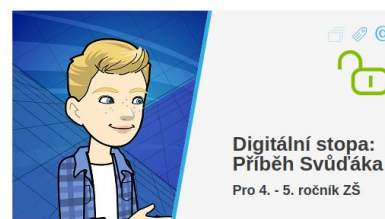
<https://bezpecnost.czu.cz>

Vznik osvětových materiálů

- Touha předat zkušenosti a vylepšit svět
- Čím více poučených uživatelů, tím méně práce pro ajťáky - řešení následků útoků
- Z pohledu vzdělávaného
 - Získání konkurenční výhody
 - Štěstí přeje připraveným
- Vliv lockdownů a covidu:
 - IT pracovníci na homeoffice = ušetřený čas
 - Administrativní pracovníci na homeoffice = větší riziko v nekontrolovaném prostředí
 - Větší riziko vyvolaným strachem z nákazy a zneužívání kyberzločinci = snadnější podlehnoutí útokům

Osvětové materiály NÚKIB

- Dostupné na <https://osveta.nukib.cz>
- Rozdělené podle cílových skupin
 - Základy KB pro každého
 - Ředitelé škol
 - Pedagogové
 - 1. - 3. ročník ZŠ
 - 4. - 5. ročník ZŠ
 - 5. - 7. ročník ZŠ
 - 8. - 9. ročník ZŠ
 - 1. a 2. ročník SŠ
- Různé formy
 - textové
 - videokurzy



Osvětové materiály NÚKIB - Jsem netvor, tvor, který žije na netu

- Dostupné na <https://osveta.nukib.cz/course/view.php?id=108>
- 6 témat
- Forma mluvený videokurz
- Vhodné pro většinu mladých lidí, kteří jsou zvyklí na youtubery a moc nečtou

Videozóna pro žáky

Objevuj svět kybernetické bezpečnosti s Lukefrym a zjisti, proč se hackeři mohou zaměřit i na tebe! 🤖

Listovat
postupně

Přehled témat



Osvětové materiály MUNI - Kyberkompas

- Dostupné na <https://security.muni.cz/cybercompass>
- 6 oblastí, obecně použitelné 3 (ostatní jsou specifické pro MUNI)
- Forma webové prezentace
 - vizuálně hezky zpracované
 - čtivé



Jak vytvořit z maličkostí účinnou obranu?

Hranice mezi vaším online a offline světem se stírá: tak proč volit pro zabezpečení dvojitý metr? Je na čase dopřát všem digitálním zařízením adekvátní péči. Antiviry, zálohování, šifrování, zamykání a zavírání obrazovek probereme srozumitelně hned v první lekci.

ZABEZPEČENÍ ZAŘÍZENÍ



Využíváte všechny výhody, které MUNI nabízí?

Masarykova univerzita poskytuje členům univerzity služby, za které by si jinak nemálo připlatili. Ve čtvrté lekci objevíte vychytávky Eduroamu, naučíte se bezpečně připojit i z kavárny, poslat opravdu soukromou zprávu nebo třeba chytře nasdílet výzkumná data.

BEZPEČNÁ KOMUNIKACE



Jak dobře jsou střeženy vaše cennosti?

Jsou to právě hesla, za kterými se skrývají vaše (online) identity, cennosti a informace. Ve druhé lekci se naučíte vytvořit frázové heslo (nejsilnější, a přece nejsnazší na zapamatování), objevíte praktičnost správce hesel a zjistíte, jak se chovat k heslům tak, aby zůstala jen vaše.

HESLA



Jak si poradit s bezpečnostním incidentem?

Útoky v digitálním světě nabývají čím dál větší rozmanitosti a promyšlenosti – neváhejte nahlásit sebemenší podezření či nesrovnalost. V páté lekci zjistíte, komu se ozvat, když se něco (možná) stalo a kdo konkrétně vám poradí na MUNI. Uživatel nemusí být nejslabším článkem řetězu!

HLÁŠENÍ INCIDENTŮ



Jak se nenechat ošálit v kyberprostoru?

Člověk je omylný a je to naprosto v pořádku. V kyberprostoru se ale jedná o charakteristiku nejčastěji využívanou útočníky. Jak se ubránit manipulativním technikám tzv. sociálního inženýrství, jak spravovat digitální stopu a jak si snadno zašifrovat data, najdete ve třetí lekci.

SEBEOBRANA



Neloučíme se: tady totiž cesta nekončí

Je náročné začít přemýšlet o mnoha věcech úplně jinak. Pojdte si na závěr připomenout, co všechno jste se dozvěděli – a nechte se překvapit rozšiřujícími multimediálními materiály. Lekce je vhodná jako tahák, ke kterému se vrátíte, jakmile si v budoucnu nebudete něčím rychle jisti.

KYBERTAHÁK

Osvětové materiály MUNI+ZČU - Kyber21

- Dostupné na <https://webcentrum.muni.cz/crp-kyber21> - bude lepší doména
- Projekt financovaný MŠMT, nyní dokončovaný,
- 5 oblastí
- Témata zpracována v textové formě + kurz v e-learning Moodle
- Bude k dispozici i v anglické verzi

Proč
kyberbezpečnost?

Bezpečné heslo

Bezpečná
komunikace

Sociální
inženýrství

Ochrana zařízení

Děkuji za pozornost