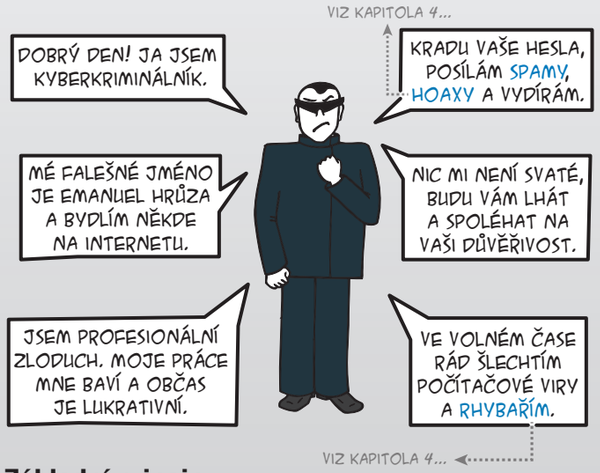
Základní principy a motivace

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.

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



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 vícestupňová 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.

Pokud mu chce obránce dosažení cíle zabránit, musí současně chránit všechny cesty. Jednotlivými články řetězu v případě kyberbezpečnosti jsou technická opatření jako například antivirové programy, firewally nebo samotní uživatelé.

Právě uživatelé bývají často nejslabšími články a jsou přirozeně cílem kyberútočníků. Kyberútočník má řadu možností, jak na uživatele zaútočit. Pokud se mu útok nepodaří u jednoho uživatele nebo jednou možností, zkusí jinou možnost nebo útok na jiného uživatele.

Vícestupňová obrana

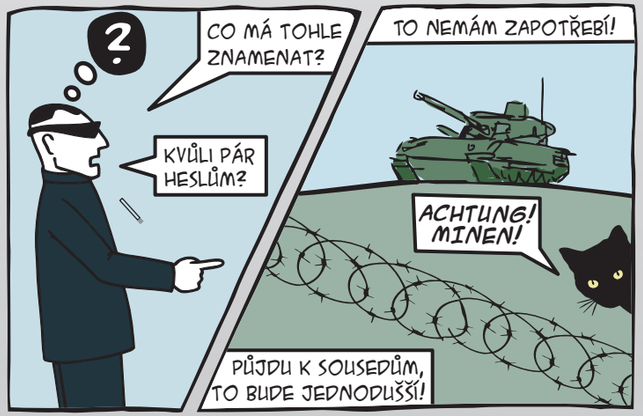
Útočník často potřebuje rychle uspět a jít tzv. o dům dál. Pokud mu ale v jeho činnosti bráníme několika překážkami, které musí postupně překonávat, jeho činnost mu zkomplikujeme a útočník to buď předčasně vzdá, nebo narazí na takovou překážku, kterou již nebude schopen překonat.

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

V IT můžeme vícestupňovou 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 snižovat 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 sítě ZČU. Školení má 10 témat. Mě, ostatní letáky, brožury a prezentace najdete na https://bezpecnost.zcu.cz.

Naší almou mater je Západočeská univerzita v Plzni a na svět jsme přišly také díky podpoře Fondu rozvoje CESNET, z.s.p.o.