Zabezpečení počítače

V kybernetickém světě veškeré dění probíhá mnohem rychleji než v běžném lidském životě. Zabezpečení počítačů musí být založeno tedy na stejně rychlých technických prostředcích. Bránit musíme také krádeži nebo neoprávněnému přístupu.

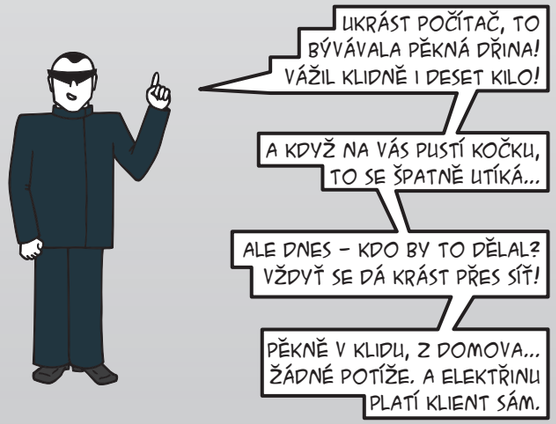
Fyzický přístup k zařízení

Při zabezpečení počítačů i jiných elektronických zařízení je nutnou podmínkou omezení fyzického přístupu k nim. Zabrání se tak:

- zneužití zařízení
- krádeži zařízení
- odebrání nebo přidání nějakých součástí

Zařízení připojené do sítě

V dnešní době jsou téměř všechna zařízení připojena k Intenetu a je tedy potřeba chránit zařízení i z pohledu zneužití po síti.



Automatické aktualizace operačního systému

Operační systém, stejně jako jakákoli jiná aplikace, může obsahovat chyby a některé mohou být obzvlášť závažné a zneužitelné. Výrobci operačních systémů proto na zjištěné chyby reagují vydáváním oprav, které distrubuují do zařízení pomocí aktualizací.

Aby zařízení dostalo opravu co nejdříve, je vhodné používat automatické aktualizace operačního systému. V takovém případě si zařízení v pravidelných intervalech zjišťuje, zda je pro něj připravena nějaká aktualizace a případně ji stáhne a nainstaluje.

Automatické aktualizace používaných aplikací

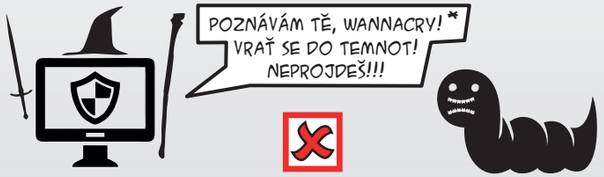
Aplikace, nainstalované v operačním systému, jako kancelářské balíčky, aplikace pro správu pošty a mnohé jiné specializované, trpí úplně stejnými problémy jako operační systémy. Mohou tedy také obsahovat chyby a je třeba je pravidelně aktualizovat.

Aplikace pro zabezpečení zařízení

Tyto aplikace se typicky slučují do jedné velké nazvané *Zabezpečení koncových zařízení* (Endpoint Security).

Antivirový program

Neustále monitoruje, co zařízení dělá, hlídá a zabraňuje spuštění škodlivého kódu. Je velmi důležité pravidelně aktualizovat databázi antivirového programu, aby dokázal efektivně čelit nejnovějším hrozbám.



*VYDĚRAČSKÝ VIRUS Z ROKU 2017 TYPU "ČERV"

Firewall

Filtruje síťový provoz podle nastavených pravidel. Do zařízení se nesmí dostat žádný nepovolený tok dat ze sítě a naopak, do sítě nesmí zařízení nic nepovoleného ani samo posílat.

*PORT VZDÁLENÉ PLOCHY VE WINDOWS

Bezpečná návštěva webu

Aktivně kontroluje a prověřuje stránky, na které se webový prohlížeč snaží dostat, a chrání před navštívením falešných webových stránek.

Oddělení admin a uživatelských účtů

Aplikace, které spustí uživatel, nemohou číst nebo měnit data, která mu nepatří, tedy například systémová. Naopak administrátor nastavuje operační systém, a má tak z principu možnost systémová data měnit. Proto pokud není potřeba měnit nastavení systému, je bezpečnější pracovat pod uživatelským účtem.

Správce zařízení

Správce zařízení je odborník, který se o zařízení stará a aplikuje v něm bezpečnostní doporučení. Každé zařízení by mělo mít svého správce.

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.