

Kybernetická bezpečnost podniku

Referát z předmětu Informatika II

Vypracoval: Kateřina Sedláčková

Datum: 06.03.2025

Obor: Podniková ekonomie

Specializace: Management výroby

**OBSAH**

[**1.** **Úvod** 2](#_Toc192264108)

[**2.** **Historie pojmu** 2](#_Toc192264109)

[**3.** **Opatření pro minimalizaci útoku na podnik** 3](#_Toc192264110)

[**4. Organizační opatření** 3](#_Toc192264111)

[**5. Závěr** 4](#_Toc192264112)

# **Úvod**

Obsah obrázku elektronika, obvod, Elektronické inženýrství, snímek obrazovky

Popis byl vytvořen automatickyKybernetická bezpečnost, dále jen „Kyberbezpečnost“ je poměrně rozsáhlý pojem, který lze popsat jako soubor nástrojů, technologií, technik, činností, zásad a procesů, jejichž úkolem je prevence, ochrana a související správa zabezpečení počítačových systémů a technologií nejen organizací ale i jednotlivců.

Toto téma je také součástí legislativy, která upravuje některé jeho prvky.

Obrázek Ilustrační foto

# **Historie pojmu**

Pojem „Kyberbezpečnost“ byl založen na základě prvních kybernetických útoků již v 80. letech 20. století. Tyto útoky byly vedeny na samostatné jednotlivé osobní počítače a probíhaly převážně pomocí virů, které měly za úkol omezení jejich funkčnosti.

Doba, kdy se internet začal používat jako celosvětová počítačová síť, byla velkým posunem v této oblasti. Většina tehdejších počítačů v této síti byla nechráněna a dovolila tak velmi snadno získat přístup zvenčí.

V dnešní době je již běžné, že počítače již při jejich koupi obsahují základní ochranné programy a tím spotřebitel získává alespoň nějakou formu zabezpečení svých dat.

# **Opatření pro minimalizaci útoku na podnik**

Pro bezpečný chod jakékoliv organizace je potřeba učinit několik opatření, která mohou minimalizovat možnosti útoku.

Náš podnik již několika útokům čelil, proto se snažíme maximálně zabezpečit naše data a předcházet dalším útokům pomocí několika nástrojů a opatření.

Několik z nich si nyní přiblížíme:

* **Firewall a antivirový systém** **–** Tyto dva nástroje pomáhají identifikovat hrozby, které se nám do systému mohou dostat. Firewall kontroluje požadavky, které zařízení z internetu přijímá a antivirový program dohlíží, zda v zařízení není žádný známý škodlivý soubor.
* **Politika hesel –** Směrnice, která definuje zaměstnancům, jak mají pracovat s hesly. Obsahuje například: požadavky pro tvorbu hesla(délka, znaky,…), expirace hesel, mazání hesel, pokuty a sankce za nedodržení politiky hesel
* **Pravidelné aktualizace systémů**
* **Pravidelné zálohování –** zálohování dat je klíčovou součástí ochrany, protože i po případné ztrátě dat po útoku, má stále podnik možnost se zpět ke svým datům dostat. Zálohu je doporučeno dělat hned několikrát. Konkrétně u nás v podniku máme nastaveno zálohování na třech místech a to jak v místě, tak také na cloudovém uložišti

# **4. Organizační opatření**

Všechna opatření se nemusejí týkat přímo sítě (a práci s ní) jako takové. Dalším krokem, který může vylepšovat kvalitu zabezpečení, je například pravidelné školení zaměstnanců, což může rozšířit obzory třeba starším generacím pracujících ve firmách, pro které může být práce s výpočetní technikou poněkud komplikovaná. Školení jim pak pomůže nejen pochopit zabezpečení firemních dat ale může se jim hodit i v osobním životě.

Nesmíme zapomenout ani na řízení přístupů. Ve zkratce – Ne každý, musí vědět vše. Podnik rozdělí příslušné role oprávnění svým zaměstnancům a tím zajistí, že se důležitá data dostanou pouze k uživatelům, kteří tato data opravdu potřebují vidět a tím sníží riziko případného úniku dat.

# **5. Závěr**

Z vlastní zkušenosti mohu říct, že zabezpečení podniku z hlediska kybernetiky je velmi důležité a je potřeba, aby na něm pracovalo nejen oddělení IT ale i každý zaměstnanec podniku, který může být potenciální hrozbou, pokud nebude dodržovat stanovená pravidla.

V našem podniku velmi pomohlo důkladné proškolení všech zaměstnanců, protože podle statistik, které naše IT oddělení vede, došlo od té doby k rapidnímu snížení potenciálních hrozeb.

Troufám si tedy říct, že naše ochranné mechanismy jsou nastaveny dobře a podnik je tak velmi dobře chráněn před kybernetickými útoky.

# **6. Zdroje**

<https://is.ambis.cz/th/nqwp7/BP_Kourkova_Katerina.pdf>

<https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberbezpecnost>

konzultace s IT oddělením našeho podniku

Použité obrázky:

<https://gaudeamus.cz/fakulty/detail-fakulty/facultyHash:0174f7ab9e3323106b9b3fdb0b14516e>

Obr. 1 - <https://skrivanek.cz/cz/blog/kyberneticka-bezpecnost-data/>