ORGANIZÁCIA A RIADENIE INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI, PERSONÁLNA BEZPEČNOSŤ, ĽUDSKÉ ZDROJE A VZDELÁVANIE

BEZPEČNOSŤ NIE JE LEN O IT – JE O ĽUĎOCH, PROCESOCH A ZODPOVEDNOSTI

Kybernetická bezpečnosť sa často chápe ako technická téma, no v skutočnosti je to **systém riadenia** – podobne ako účtovníctvo, kvalita či bezpečnosť pri práci. Nejde len o to, mať antivírus alebo firewall. Ide o **nastavenie pravidiel, procesov a zodpovedností,** ktoré udržia vašu firmu funkčnú aj vtedy, keď sa stane incident.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ako má vyzerať organizácia kybernetickej bezpečnosti vo firme

Každá firma, aj menšia, by mala mať **základnú štruktúru riadenia bezpečnosti** – nemusí ísť o zložité procesy, ale o jasne stanovené úlohy a zodpovednosti. Odporúča sa mať definované minimálne tieto roly:

- **Manažér kybernetickej bezpečnosti** – osoba, ktorá dohliada na celkový stav kybernetickej bezpečnosti.

  Príklad: MKB riadi vyšetrovanie kybernetického incidentu.

- **Správca IT** – zodpovedá za technické opatrenia (antivírus, firewall, zálohy, aktualizácie).
  Príklad: externý IT dodávateľ, ktorý zabezpečuje správu serverov a počítačov.

- **Používatelia** – každý zamestnanec má svoju úlohu pri ochrane dát a informačných aktív.
  Príklad: neotvára podozrivé e-maily, dodržiava zásady pre silné heslá a nahlási podozrivé správy.

- **Biznis vlastník –** zodpovedá za správne nastavenie a prácu konkrétnej časti organizácie. To znamená: Strategické smerovanie, financovanie a dosahovanie cieľov služby či produktu. Určuje priority, schvaľuje kľúčové rozhodnutia, zodpovedá za riadenie rizík vo svojej oblasti a zabezpečuje, aby výsledky prinášali biznis hodnotu.

Okrem zodpovedností by mal byť vytvorený aj **minimálny súbor pravidiel (interné smernice alebo politika kybernetickej bezpečnosti)**, kde sú uvedené zásady, ktoré sú aplikované v rámci organizácie, ako sú napríklad:

- ako sa majú správať používatelia,
- aké softvérové vybavenie sa smie a nesmie inštalovať,
- ako sa pracuje s prenosnými médiami a údajmi,
- kto rieši bezpečnostné incidenty.

Takýto dokument nemusí mať desiatky strán – dôležité je, aby bol **zrozumiteľný, aktuálny a známy všetkým**.

Personálna bezpečnosť – ľudia sú najväčšou zraniteľnosťou aj ochranou

Väčšina kybernetických útokov sa začína **ľudskou chybou**. Nie preto, že by ľudia nechceli byť opatrní, ale preto, že nie vždy chápu, aké následky môže mať obyčajné kliknutie na e-mail alebo zdieľanie informácie.

Preto je personálna bezpečnosť o troch základných zásadách:

1. **Vstupné preškolenie zamestnancov**

   Pred prijatím zamestnancov, ktorí budú mať prístup k informačným aktívam, je dôležité vstupné preškolenie v oblasti kybernetickej bezpečnosti a ich oboznámenie sa s internými procesmi a s bezpečnostnou dokumentáciou.

2. **Zmluvná zodpovednosť a zvyšovanie bezpečnostného povedomia**

   Každý zamestnanec by mal mať v pracovnej zmluve alebo v interných pravidlách jasne uvedené, **čo je jeho povinnosťou pri ochrane údajov** a zúčastňovať sa na vzdelávacích aktivitách.

3. **Kultúra dôvery, nie strachu**

   Ak zamestnanec urobí chybu, je lepšie, aby ju **nahlásil okamžite**, než aby sa ju snažil skryť. Dôležité je vytvoriť prostredie, kde sa o bezpečnosti dá otvorene hovoriť.

Vzdelávanie a budovanie povedomia

Najlepšia ochrana je **informovaný človek**. Technológie síce pomáhajú, ale **ľudia rozhodujú** – na čo kliknú, kam údaje zadajú, ako reagujú na podozrivé e-maily.

Na dosiahnutie tohto cieľa sú často krát vhodné jednoduché formy vzdelávania:

- **Krátke školenia alebo workshopy** ako rozpoznať phishing, deepfake videá alebo falošné správy, informovanie o najnovších trendoch vo vývoji hrozieb, cielených na používateľov,
- **Interné testy** – napríklad fiktívny phishing e-mail, aby sa preverila pozornosť a reakcie zamestnancov.
- **Letáky, plagáty, pripomienky na nástenke** – jednoduché vizuálne tipy, ako sa správať bezpečne.

Vzdelávanie by nemalo byť jednorazové. Kybernetické hrozby sa rýchlo menia a preto je dôležité **bezpečnostné povedomie neustále zvyšovať**.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Praktické odporúčania pre malé a stredné firmy

Aby bola kybernetická bezpečnosť riadená a nie len „riešená, keď sa niečo stane", odporúča sa zaviesť kroky a procesy, ktoré aj v prípade, ak nie ste poskytovateľ základnej služby (PZS), významných spôsobom prispejú k zvýšeniu úrovne kybernetickej bezpečnosti:

- Vypracovať **politiku kybernetickej bezpečnosti** (jednoduchý dokument so zásadami).
- Vykonať **analýzu rizík** a následne ich **riadiť**.
- Vymenovať **zodpovednú osobu** za kybernetickú bezpečnosť.
- Zaviesť **pravidelné školenia**.
- Nastaviť **zálohovanie a obnovu dát**.
- Viesť **prehľad aktív**.
- Zaviesť **silné heslá a viacfaktorové overenie (MFA)**.
- Pravidelne **aktualizovať softvér**.

Tieto jednoduché opatrenia sú základom funkčného systému riadenia kybernetickej bezpečnosti – aj bez zložitých certifikácií.

Záver

Organizácia a riadenie kybernetickej bezpečnosti presahuje rámec dokumentácie – je to **súčasť každodennej firemnej práce**. Jasne definované pravidlá, zodpovednosti a systematické vzdelávanie zamestnancov sú základom efektívneho zvládania incidentov.

Bezpečnosť nie je konečný stav a cieľ, ktorý chceme dosiahnuť, ale trvalý proces neustáleho zlepšovania.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti