Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení. Ochrana proti škodlivému kódu a nežiaducemu obsahu

Pavol Dovičovič

9. december 2025

ČO HOVORÍ VYHLÁŠKA..

Bezpečnostné opatrenia (1/2)

- **Bezpečnostné opatrenia pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení podľa § 20 ods. 2 písm. o) zákona prijíma prevádzkovateľ základnej služby tak, že:**
  - priestory, v ktorých sa nachádzajú riadiace a serverové súčasti informačných a operačných technológií, majú definované pravidlá fyzickej bezpečnosti
  - je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení
  - sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu
  - sú monitorované a vizuálne zaznamenávané všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu (platí pre PKZS)
  - aktíva v zabezpečených priestoroch sú chránené pred poškodením a neoprávneným zásahom zo strany zamestnancov pracujúcich v týchto priestoroch a nepovolaných osôb

Bezpečnostné opatrenia (2/2)

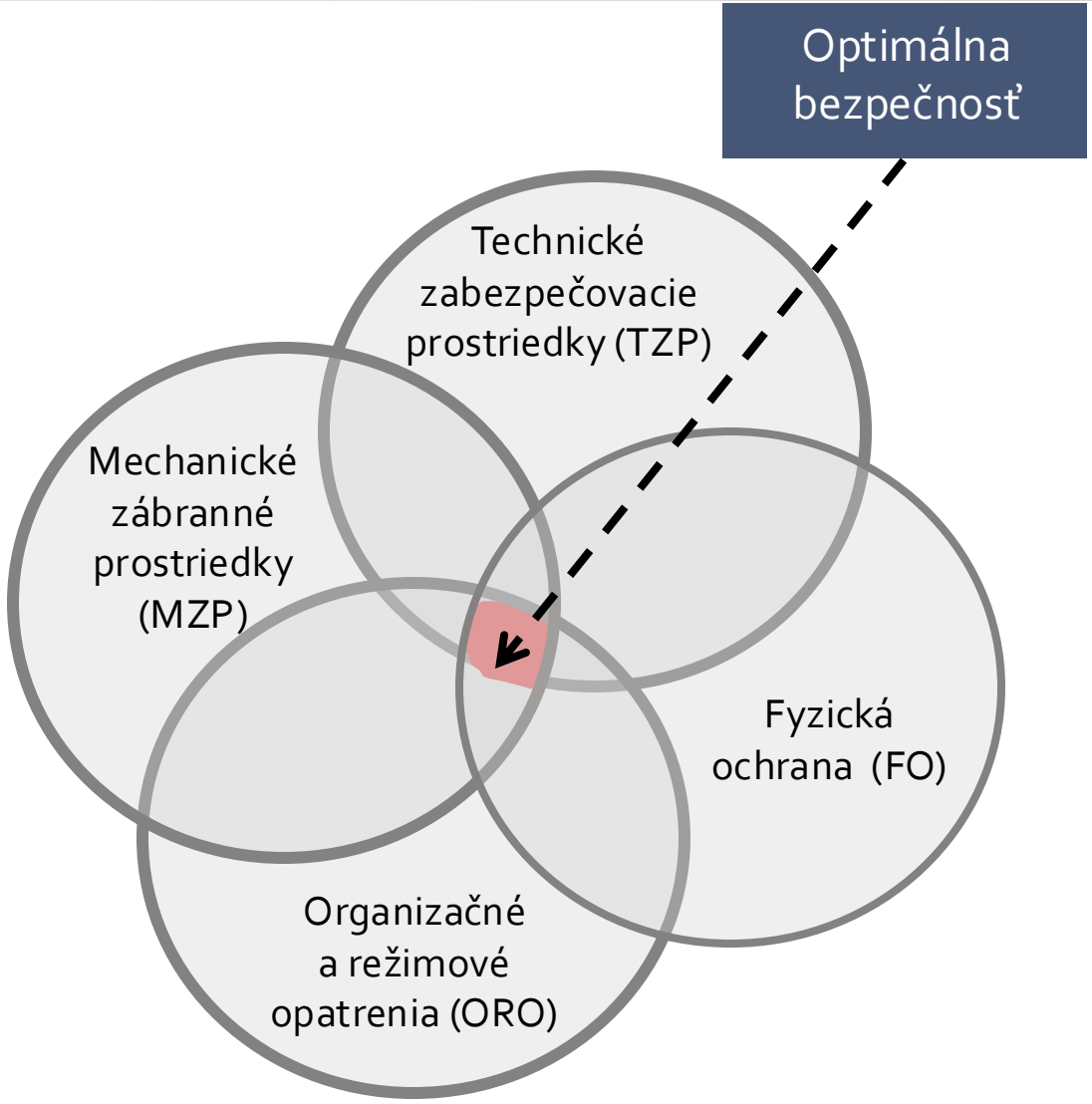
- **Bezpečnostné opatrenia pre ochranu proti škodlivému kódu a nežiaducemu obsahu podľa § 20 ods. 2 písm. l) zákona prijíma prevádzkovateľ základnej služby tak, že:**
  - je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov
  - je zaručená pravidelná aktualizácia sietí, informačných systémov a operačných technológií s cieľom zabezpečiť minimálne narušenie bežnej prevádzky
  - prístup k externým internetovým zdrojom je riadený s cieľom znížiť vystavenie škodlivému obsahu

FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ

OPTIMÁLNA FYZICKÁ BEZPEČNOSŤ

preventívne

- Mnohé hrozby sa môžu uskutočniť len vtedy, ak má nositeľ hrozby bezprostredný prístup k informačným aktívam.
- Aby organizácia zabránila neoprávnenému fyzickému prístupu k svojim aktívam, musí ich umiestniť v zabezpečených priestoroch.
- Aby znížila riziko fyzického poškodenia IKT, musí pre prevádzku IKT vytvoriť vhodné prostredie (osvetlenie, klimatizácia, vlhkosť), zabezpečiť ochranu infraštruktúry (kabeláž, ochrana pred prepätím, náhradné zdroje energie).



TYPICKÉ REŽIMOVÉ (ORGANIZAČNÉ) OPATRENIA

preventívne

- Organizačné a režimové opatrenia sú opatrenia určujúce podmienky:
  - Riadenia pohybu osôb a dopravných prostriedkov v objekte,
  - Používania mobilných telefónov, videokamier, fotoaparátov, audio záznamových zariadení,
  - Spôsobu kontroly objektu po opustení pracoviska zamestnancami,
  - Fyzického výkonu zabezpečenia objektu,
  - Manipulácie s technickými zabezpečovacími prostriedkami a podmienky ich používania,
  - Pre postup pri narušení objektu a chráneného priestoru alebo pri pokuse o narušenie objektu,
  - Pre postupy v prípade vzniku incidentu.





TECHNICKÉ ZABEZPEČOVACIE PROSTRIEDKY

- **Technické zabezpečovacie prostriedky** (TZP) slúžia na ochranu majetku a osoby pred neoprávnenými zásahmi, vrátane systémov a zariadení umožňujúcich sledovanie pohybu a prejavu osoby v objekte a jeho okolí. Tvoria systém prostriedkov na získavanie a vyhodnocovanie informácií z prostredia stráženého objektu alebo z jeho časti.
- Medzi TZP patria:
  - **EZS**: Elektrické zabezpečovacie – t. j. poplachové systémy pre detekciu a indikáciu prítomnosti, vstupu alebo pokusu o vstup narušiteľa do chránených objektov
  - **CCTV (PTV)**: Kamerová zostava v rámci uzatvoreného televízneho okruhu
  - **SKV**: Systémy na kontrolu vstupov do objektov a systémy slúžiace na elektronické preukazovanie totožnosti a oprávnenosti osôb

MECHANICKÉ ZÁBRANNÉ PROSTRIEDKY

preventívne

- **Mechanické zábranné prostriedky** sú prostriedky, ktorých účelom je sťažiť alebo celkom znemožniť násilné vniknutie nepovolanej osoby do chráneného úschovného miesta alebo úschovného objektu, prípadne zabrániť neoprávnenej manipulácií s chránenými predmetmi
- Rozdelenie MZP:
  - **bezpečnostné úschovné objekty** (synonymum: trezor) t. j. mechanické zábranné prostriedky, ktoré slúžia na bezpečnú úschovu hodnôt. Majú priestor ohraničený špeciálnou konštrukciou, ktorá zaručuje maximálne dosiahnuteľnú bezpečnosť pre vnútri uložené hodnoty pred ich zneužitím, poškodením, odcudzením alebo zničením
    - **Komorový trezor**: je bezpečnostný úschovný objekt, ktorý je pevným stavebným celkom budovy doplnený špeciálne konštrukčne riešenými trezorovými dverami
    - **Mobilný trezor** (synonymum: skriňový trezor): je bezpečnostný úschovný objekt, ktorý nie je pevným stavebným celkom budovy. Pod tento pojem zahrňujeme množstvo rôznych typov mobilných trezorov
  - stavebné prvky objektov (bezpečnostné dvere, sklá, fólie, mreže atď.)



OCHRANA PROTI ŠKODLIVÉMU KÓDU A NEŽIADUCEMU OBSAHU

Hrozbový kontext a východiská ochrany

- **Primárny iniciačný vektor incidentov** - škodlivý kód a obsah sú najčastejším spôsobom prieniku do prostredia.
- **E-mail, web, používateľská interakcia** - väčšina útokov začína klikom, otvorením prílohy alebo spustením súboru.
- **Ľudský faktor zosilňuje dopad** - správne fungujúce technické opatrenia nezabránia všetkým chybám používateľov.
- **Kontinuálna ochrana, nie jednorazové riešenie** - ochrana musí bežať nepretržite a reagovať na meniace sa hrozby.
- **Dôraz na merateľnú účinnosť kontrol** - nestačí nástroj vlastniť, je nutné overovať, že funguje.

Rozšírená definícia škodlivého kódu a nežiadúceho obsahu

- **Škodlivý kód**
  - **Klasický malware**
    Vírusy, trójske kone a ransomvér s priamym vplyvom na systémy.
  - **Fileless a skriptové útoky**
    Zneužívajú legitímne funkcie operačného systému.
  - **Makrá a embedded objekty**
    Častý spôsob skrytého spustenia škodlivého kódu.

- **Nežiaduci obsah**
  - **Phishing a podvodné weby**
    Cielené na získanie prístupov alebo údajov.
  - **C2 infraštruktúra a drop zóny**
    Riadiace servery a miesta šírenia škodlivého kódu.
  - **Obsah porušujúci bezpečnostné politiky**
    Aj bez technického exploitnutia môže predstavovať riziko.

Technické kontrolné mechanizmy (defence-in-depth)

- **Endpoint ochrana** - detekcia správania, exploitov a neoprávnených aktivít.
- **Behaviorálne a heuristické mechanizmy –** reagujú aj na neznáme alebo upravené hrozby.
- **E-mailová ochrana** - analýza príloh, URL a reputácie odosielateľa.
- **Web a DNS filtering** - blokovanie známych a rizikových domén ešte pred pripojením.
- **Centrálna viditeľnosť a korelácia** - umožňuje rýchlu reakciu a kontextové vyhodnotenie udalostí.

Procesy, pravidlá a riadenie výnimiek

- **Jasné pravidlá pre prácu so súbormi a obsahom** - používatelia musia vedieť, čo je povolené a čo nie.
- **Formalizované schvaľovanie výnimiek** - každá výnimka má dôvod, časové obmedzenie a vlastníka.
- **Väzba na incident response procesy** - detekcia musí automaticky spustiť ďalšie kroky riadenia incidentu.
- **Forenzná pripravenosť** - logy a záznamy musia byť použiteľné ako dôkaz.
- **Auditovateľnosť opatrení** - organizácia vie spätne preukázať, čo sa detegovalo a blokovalo.

Overovanie účinnosti a zodpovednosti

- **Priebežné testovanie kontrol** - simulácie a testy overujú reálnu funkčnosť ochrany.
- **Bezpečnostné metriky a trendy** - sleduje sa vývoj, nie len jednorazové čísla.
- **Monitoring výnimiek a konfigurácií** - výnimky sú častým miestom zlyhania ochrany.
- **Jasne definované zodpovednosti** - každý nástroj a proces má svojho vlastníka.
- **Ochrana ako riadený proces, nie produkt** - ide o neustály cyklus zlepšovania, nie o hotové riešenie.

Záver - Integrovaný pohľad na ochranu (IT, obsah, fyzický priestor)

- **Kybernetická a fyzická bezpečnosť tvoria jeden bezpečnostný systém**
  Narušenie fyzického prostredia môže viesť k rovnakým dopadom ako technický útok.
- **Fyzický prístup = potenciálny kybernetický incident**
  Neoprávnený prístup k zariadeniu, sieti alebo médiám obchádza logické kontroly.
- **Zariadenia, médiá a infraštruktúra pod kontrolou**
  Ochrana serverov, pracovných staníc, sieťových prvkov a záložných médií je nevyhnutná.
- **Prevencia zavlečenia škodlivého kódu mimo sieťových kanálov**
  USB zariadenia, externý HW alebo servisné zásahy sú reálnym vektorom útoku.
- **Riadený prístup, evidencia a zodpovednosti**
  Každý prístup – fyzický aj logický – má byť autorizovaný, evidovaný a spätne dohľadateľný.
- **Konzistentný prístup naprieč všetkými vrstvami ochrany**
  Technické, organizačné aj fyzické opatrenia musia byť zosúladené a pravidelne overované.
- **Bezpečnosť ako end-to-end proces**
  Od priestoru, cez používateľa až po dáta – bez „slabých článkov" medzi nimi.

NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.