NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

TERMINOLÓGIA V KYBERNETICKEJ BEZPEČNOSTI

Tomáš Hettych, Pavol Dovičovič

11. marec 2025

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

- **Výkon činnosti orgánu posudzovania zhody**, t.j. certifikácia
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť
- **Audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z. z.
- **Konzultačné služby** v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- **Znalecká a expertízna činnosť** podľa zákona č. 382/2004 Z. z. o znalcoch
- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií

Spolufinancovaný Európskou úniou

Terminológia v KB

TERMINOLÓGIA

- **Riadenie informačnej bezpečnosti** – Starostlivosť o bezpečnosť IT systémov a údajov v organizácii pomocou pravidiel a opatrení.
  - Príklad: Organizácia zadefinuje, kto má prístup k citlivým údajom a ako sa majú chrániť pred hackermi.

- **Kybernetická bezpečnosť** – Ochrana počítačov, sietí a dát pred útokmi hackerov, vírusmi alebo podvodmi.
  - Príklad: Používanie antivírusu a dvojfaktorového overenia na ochranu e-mailového účtu.

TERMINOLÓGIA

- **Fyzická bezpečnosť** – Opatrenia na ochranu počítačov, serverov a dátových centier pred zlodejmi, požiarom alebo výpadkom elektriny.
  - Príklad: Vstup do serverovne je možný len s riadeným prístupom.

- **Dostupnosť dát (data availability)** – Zabezpečenie, aby boli údaje vždy prístupné, keď ich potrebujeme.
  - Príklad: Cloudová služba zálohuje fotky, takže ich nestratíme ani pri poruche telefónu.

TERMINOLÓGIA

- **Integrita dát (data integrity)** – Zaručuje, že údaje sú správne a spoľahlivé.
  - Príklad: Ak si v banke pošleme peniaze na účet, systém musí zabezpečiť, že suma sa nezmení.

- **Dôvernosť dát (data confidentiality)** – Zabezpečenie, aby citlivé údaje nevideli neoprávnené osoby.
  - Príklad: Lekárska karta pacienta je prístupná len lekárom, nie všetkým zamestnancom nemocnice.

TERMINOLÓGIA

- **Klasifikácia informácií** – Rozdelenie údajov podľa dôležitosti a citlivosti.
  - Príklad: Dokumenty organizácie môžu byť označené ako „verejné“, „interné“ alebo „chránené“, resp. „prísne chránené“.

- **Aktívum** – Čokoľvek, čo má pre organizáciu hodnotu a treba to chrániť.
  - Príklad: Počítače, dáta, softvér, zamestnanci alebo osobné údaje zákazníkov.

TERMINOLÓGIA

- **Informačné aktívum** – Údaje a systémy, ktoré sú dôležité pre fungovanie organizácie.
  - Príklad: Zákaznícka databáza e-shopu s históriou objednávok.

- **Fyzické aktívum** – Hmotné veci, ktoré organizácia vlastní a používa.
  - Príklad: Notebooky zamestnancov, servery v dátovom centre alebo bezpečnostné kamery.

TERMINOLÓGIA

- **Inventár aktív** – Zoznam všetkých dôležitých vecí, ktoré organizácia vlastní.
  - Príklad: Organizácia vedie prehľad pracovných notebookov, kto ich používa a kde sa nachádzajú.

TERMINOLÓGIA

- **Riadenie rizík** – Hľadanie nebezpečenstiev, ktoré môžu ohroziť dáta a systémy, a ich riešenie.
  - Príklad: Organizácia zisťuje, aké hrozby môžu spôsobiť výpadok jej online služieb a ako ich minimalizovať.

- **Analýza rizík** – Posúdenie, ako veľmi môžu rôzne problémy uškodiť organizácii a ako im predchádzať.
  - Príklad: Banka skúma, aké veľké riziko predstavuje kybernetický útok na internetové bankovníctvo.

TERMINOLÓGIA

- **Vlastník rizika** – Osoba, ktorá je zodpovedná za rozhodovanie o tom, ako riešiť konkrétne bezpečnostné riziko.
  - Príklad: KB manažér rozhoduje, či organizácia investuje do lepšej ochrany proti phishingovým útokom.

- **Akceptovanie rizika** – Rozhodnutie, že určité nebezpečenstvo organizácia prijme, lebo jeho riešenie je príliš drahé alebo zložité.
  - Príklad: Organizácia sa rozhodne nepoistiť starý server, pretože jeho oprava je lacnejšia ako poistka.

TERMINOLÓGIA

- **Analýza dopadov (BIA)** – Hodnotenie, ako veľmi môže bezpečnostný incident ovplyvniť fungovanie organizácie.
  - Príklad: Organizácia zisťuje, koľko peňazí stratí, ak jej webová stránka prestane fungovať na 24 hodín.

TERMINOLÓGIA

- **Hrozba** – Čokoľvek, čo môže spôsobiť škodu na IT systémoch alebo dátach.
  - Príklad: Hacker sa pokúša prelomiť heslá zamestnancov.

- **Zraniteľnosť** – Slabé miesto v systéme, ktoré môže byť zneužité.
  - Príklad: Starý softvér bez aktualizácií obsahuje chybu, ktorú môžu hackeri využiť na prístup do systému.

TERMINOLÓGIA

- **Udalosť** – Akýkoľvek neobvyklý jav v systéme, ktorý môže (ale nemusí) byť nebezpečný.
  - Príklad: Zamestnanec sa pokúša prihlásiť do informačného systému organizácie z neznámeho zariadenia.
- **Incident** – Bezpečnostná udalosť, ktorá spôsobila problém.
  - Príklad: Hacker ukradne heslá zamestnancov a získa prístup k údajom organizácie.
- **Dopad** – Následky bezpečnostného problému.
  - Príklad: Po kybernetickom útoku organizácia stratí citlivé údaje klientov a poškodí si reputáciu.

TERMINOLÓGIA

- **Cieľový bod obnovy (RPO)** – Koľko starých dát môže organizácia stratiť pri obnove po výpadku.
  - Príklad: Ak je RPO nastavené na 1 hodinu, znamená to, že pri obnove systému môžu chýbať maximálne posledné 60 minút uložených dát.

- **Cieľový čas obnovy (RTO)** – Ako rýchlo sa musí organizácia zotaviť po incidente a začať poskytovať služby na prijateľnej úrovni.
  - Príklad: Ak organizácia stanoví RTO na 4 hodiny, musí do 4 hodín po výpadku znovu sprevádzkovať všetky dôležité služby.

TERMINOLÓGIA

- **Dodávateľ** – Firma alebo osoba, ktorá poskytuje IT služby alebo technológie.
  - Príklad: Spoločnosť, ktorá zabezpečuje cloudové úložisko pre organizáciu.

TERMINOLÓGIA

- **Riadenie kontinuity činností** – Plánovanie toho, ako bude organizácia fungovať aj v prípade problémov (krízy).
  - Príklad: Organizácia má plán, čo robiť a ako postupovať v prípade, ak dôjde k výpadku elektriny alebo kybernetickému útoku.

- **BCP/DRP** – BCP (Business Continuity Plan) pomáha organizácii pokračovať v činnosti aj pri problémoch (kríze), DRP (Disaster Recovery Plan) sa zameriava na obnovu IT systémov.
  - Príklad: Organizácia má plán na rýchlu obnovu dát po výpadku serverov.

TERMINOLÓGIA

- **Prevádzkový monitoring** – Sledovanie výkonu a funkčnosti IT systémov.
  - Príklad: IT oddelenie kontroluje, či servery bežia bez výpadkov a s požadovanými parametrami, ako sú napríklad zaťaženie systému, dostupná pamäť a podobne.

- **Bezpečnostný monitoring** – Neustále sledovanie možných kybernetických hrozieb.
  - Príklad: Systém upozorní bezpečnostný tím v prípade, keď niekto skúša opakovane nesprávne heslo.

TERMINOLÓGIA

- **Riadenie prístupov** – Určenie, kto má prístup k akým systémom a údajom.
  - Príklad: Účtovník nemôže otvárať súbory IT oddelenia.

- **Riadenie zmien** – Plánovanie a bezpečná implementácia zmien v IT systémoch.
  - Príklad: Pred aktualizáciou softvéru sa otestuje, či aktualizácia nespôsobí chyby.

TERMINOLÓGIA

- **Šifrovanie** – Ochrana dát tak, aby ich bez správneho kľúča nebolo možné prečítať.
  - Príklad: Správy v aplikácii WhatsApp sú zašifrované, takže ich nikto cudzí nevidí.

- **Digitálny podpis** – Overenie pravosti dokumentu alebo e-mailu.
  - Príklad: Elektronický podpis na faktúre zaručuje, že ju poslala správna firma.

TERMINOLÓGIA

- **Technické opatrenia** – Ochranné prvky ako firewally, antivírusy a šifrovanie.
  - Príklad: Používanie bezpečnostného softvéru na ochranu pred vírusmi.
- **Organizačné opatrenia** – Pravidlá a školenia na zvýšenie bezpečnosti.
  - Príklad: Zamestnanci musia pravidelne meniť heslá.
- **Audit** – Kontrola súladu s požiadavkami legislatívy.
  - Príklad: Certifikovaný audítor preverí, či organizácia spĺňa požiadavky platnej legislatívy.

ZÁVER

- Ďakujeme Vám za Váš čas a pozornosť
- Nasledujúci webinár na tému: „Organizácia a riadenie informačnej a kybernetickej bezpečnosti, Personálna bezpečnosť, ľudské zdroje a vzdelávanie“ bude 2. apríla 2025.

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.