Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

BUDÚCI SLOVENSKÝ INDEX KYBERNETICKEJ BEZPEČNOSTI

JESENNÁ ITAPA, 27.11.2024

ZADANIE

Navrhnúť metodiku tvorby kľúčových indikátorov na objektívne stanovenie úrovne bezpečnosti, resp. odolnosti a pre odhadovanie trendov v kybernetickej bezpečnosti na národnej a podnikovej, resp. odvetvovej úrovni

METÓDY HODNOTENIA

Tvorba metrík na stanovenie úrovní a trendov v kybernetickej bezpečnosti

ATRIBÚTY OVPLYVŇUJÚCE STAV KYBERNETICKEJ BEZPEČNOSTI

- Rozsah implementácie bezpečnostných opatrení
- Počet a kritickosť identifikovaných / následne zaplátaných zraniteľností
- Identifikované a kvantifikované / následne ošetrené a riziká
- Počet a kritickosť nových / uzatvorených incidentov
- Čas identifikácie a riešenia incidentov (MTTI, MTTC)
- Miera súladu resp. hodnotená aplikačná prax právnych predpisov
- Testovaná miera odolnosti organizácie
- Miera vyspelosti procesov
- Certifikácia výrobkov, procesov, služieb, systémov manažérstva a osôb
- Kvalifikácia ľudských zdrojov
- Zmluvné záruky a vzťahy s tretími stranami

Rôzna váha atribútov

METÓDY VÝSKUMU V KYBERBEZPEČNOSTI

V KB je typicky používaný **empirický výskum,** t.j. zisťovanie a analýza údajov o reálne existujúcich javoch a procesoch

- potrebné je zaujať odstup od skúmaného javu, zbaviť sa subjektívnych postojov, ktoré by kontaminovali skúmané údaje

Kvantitatívny výskum

Cieľom je získať exaktné a objektívne overiteľné údaje o kybernetickej bezpečnosti

- základom je meranie (získavanie presných údajov vyjadrených numericky)
- zisťuje sa výsledný stav, rozsah, frekvencia alebo intenzita javov, ich meranie a štatistická analýza

Semikvantitatívny výskum

Cieľom je skúmať kauzálne vzťahy v kybernetickej bezpečnosti

- uprednostňuje sa reprezentatívny výber s cieľom následného zovšeobecnenia poznatkov na populáciu
- následné numerické vyjadrenie pomocou štatistických metód

ZDROJE ÚDAJOV PRE VÝSKUM

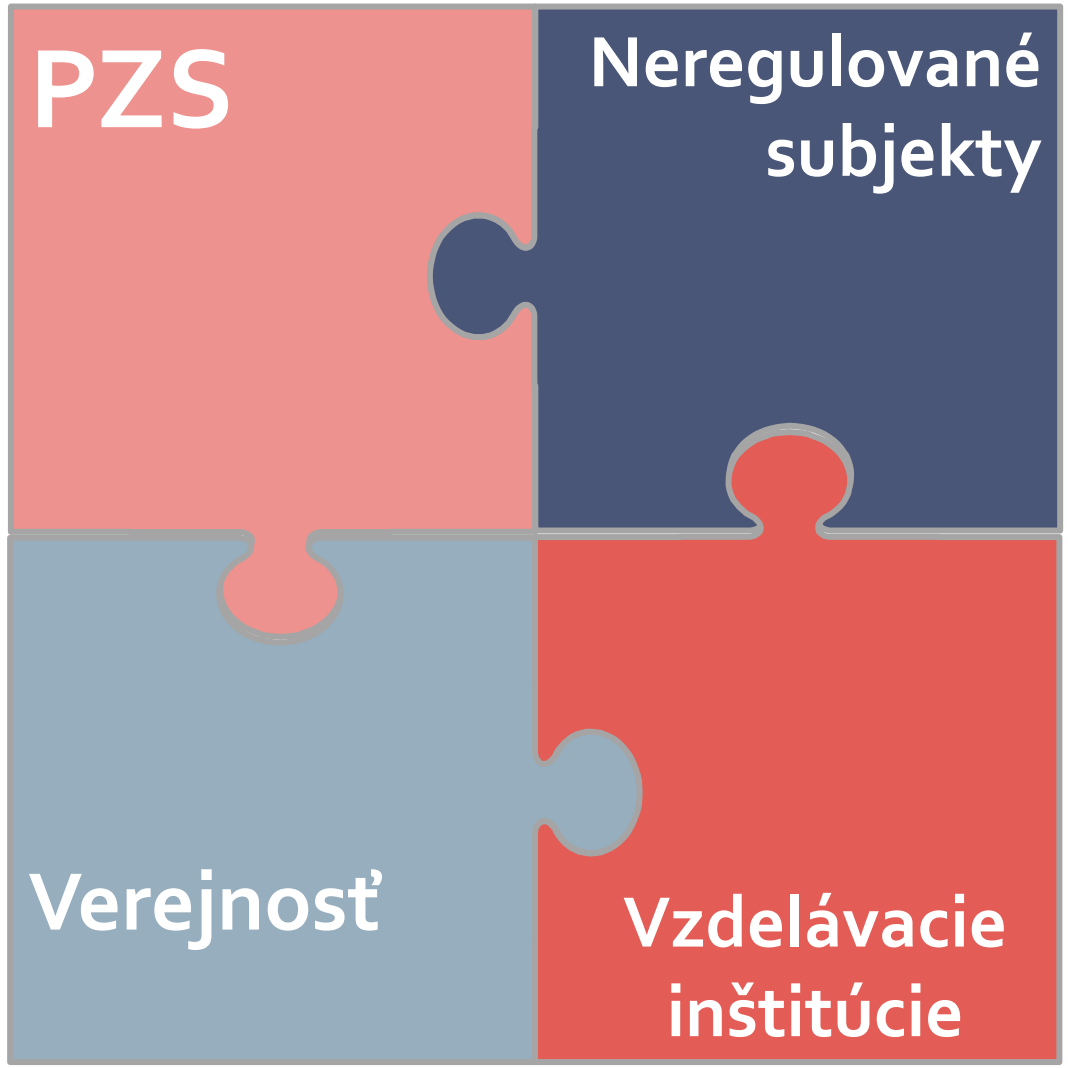
Tvorba metrík na stanovenie úrovní a trendov v kybernetickej bezpečnosti

VÝSKUMNÉ SUBJEKTY

Anonymizované dáta
o počte auditných zistení zo
záverečných správ auditu podľa
§ 29 zákona č. 69/2018 Z.z.
o kybernetickej bezpečnosti

Anonymizované dáta
z formulárov samohodnotenia
doručených Úradu podľa
§ 34a zákona č. 69/2018 Z.z.
o kybernetickej bezpečnosti

Výsledky prieskumov
vypracovaných podľa
štandardov Slovenskej
Asociácie Výskumných Agentúr,
prostredníctvom agentúry AKO



Výsledky prieskumov
vypracovaných podľa
štandardov Slovenskej
Asociácie Výskumných Agentúr,
prostredníctvom agentúry AKO

Priame prieskumy na základe
memoránd
o spolupráci s VŠ

TYPY ATRIBÚTOV VÝSKUMNÝCH DÁT

Technické aspekty – najmä existencia a plnenie technických opatrení, zraniteľnosti, riziká, incidenty,

Organizačné aspekty – najmä vyspelosť procesov, organizačné usporiadania, existencia a plnenie organizačných opatrení, spôsobilosť na operatívne činnosti

Kvalifikácia - overované zručnosti, merané vedomosti, akreditácie študijných odborov, certifikácie osôb

Kapacita a vyspelosť - dostupné ľudské zdroje, dostupná technológia, vyspelosť opatrení a procesov

Komunikácia - transparentnosť, vyspelosť internej a externej komunikácie

Kooperácia - zapojenie do národných a medzinárodných štruktúr

Vyspelosť - konzistentnosť legislatívneho procesu, prehľadnosť regulácie, riadenie súladu, manažérska kontrola, audit

DOSTUPNÉ ATRIBÚTY PRE TVORBU INDEXU KB

- **Zraniteľnosti**
  (Common Vulnerability Scoring System - CVSS)
- **Hrozby**
  (katalógy hrozieb, atribúcia)
- **Riziká**
  (Key Risk Indicators - KRI)
- **Incidenty**
  (Indicators of Compromise – IOCs, počty, straty, objemy, reakčný čas)
- **Miera súladu**
  (počet auditných zistení a vývoj uzatvorených odporúčaní, implementácia práva)
- **Vyspelosť**
  (vyspelosť opatrení a procesov, CMMI 0-5)
- **Certifikácia**
  (počet certifikovaných produktov, osôb, systémov manažérstva)
- **Kvalifikácia**
  (výsledky testovania znalostí a zručností)
- **Verejná mienka**
  (výsledky prieskumov, pri zachovaní štatistickej významnosti vzoriek)

METÓDY INTERPRETÁCIE VÝSLEDKOV

Tvorba metrík na stanovenie úrovní a trendov v kybernetickej bezpečnosti

CIEĽOVÝ PARAMETER: SPÔSOBILOSŤ

- Aby sa dosiahla požadovaná vyspelosť ochrany informačných aktív a aby mohli byť splnené ciele stanovené v bezpečnostných požiadavkách, organizácie musia **zaručiť určité spôsobilosti** v oblasti informačnej a kybernetickej bezpečnosti

- „**Spôsobilosť**“ (z angl.: „capability“) je osobitná schopnosť, ktorú môže organizácia vlastniť alebo vykonávať s cieľom dosiahnuť konkrétny účel

VPLYV ATRIBÚTOV NA SPÔSOBILOSTI

1. **Spôsobilosti NARASTAJÚCE NÁRASTOM kvantity, alebo kvality určitého meraného atribútu**

   - Napr. prísnejšie stanovené bezpečnostné ciele, širší rozsah implementovaných opatrení, vyšší počet zdrojov bezpečnostne relevantných informácií pripojených do bezpečnostného monitoringu, prísnejšia úroveň regulácie, širšie pokrytie chránenej infraštruktúry

2. **Spôsobilosti NARASTAJÚCE POKLESOM meranej hodnoty atribútu**

   - Napr. úroveň identifikovaných rizík, počet zraniteľností, počet nových incidentov

3. **Spôsobilosti KLESAJÚCE NÁRASTOM kvantity meraných atribútov**

   - Napr. vyšší počet domén, vyšší počet sieťových segmentov, vyšší počet koncových bodov, vyšší počet zraniteľných zariadení.

4. **Spôsobilosti KLESAJÚCE POKLESOM kvality meraných atribútov**

   - Napr. počet kvalifikovaných profesionálov, nižší počet absolventov vzdelávania, nižší počet obsadených pracovných miest, horšie výsledky hodnotenia znalostí, atď.

ZÁVER

- Vrcholový manažment organicky vníma, že kybernetická bezpečnosť **nie je subjektívny POCIT bezpečia, ale objektívny a merateľný STAV** hrozieb a rizík

- Doktrína Data-driven decision-making je definovaná ako **používanie faktov, metrík a údajov na usmerňovanie strategických rozhodnutí**, ktoré sú v súlade s cieľmi, zámermi a iniciatívami organizácie

- Pri riadení informačnej a kybernetickej bezpečnosti by malo byť nutné **pristupovať k rozhodovaniu na základe empirického výskumu,** t. j. zisťovania a analýzy údajov o reálne existujúcich javoch a procesoch

- Manažérstvo je aj (alebo najmä) o riadení ľudských zdrojov, preto výskumnou otázkou je, **či kvantitatívne štatistické metódy sú efektívne použiteľné na zabránenie subjektívnej kontaminácie** skúmaných javov v kybernetickej bezpečnosti

- Budeme tiež vychádzať z hypotéz, že **návrh metriky musí kategorizovať atribúty štatistických súborov do rôznych tried** a že jednotlivé **hodnotiace kategórie majú rôzne váhy**, podľa typu hodnotenej entity

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