Bezpečnostný manažment

Skúška 2025

1. Ako definujeme kybernetickú bezpečnosť a prečo je dôležitá?

Kybernetická bezpečnosť je súbor princípov, procesov, technológií a opatrení na ochranu systémov, sietí, dát a infraštruktúr pred neautorizovaným prístupom. Je dôležitá vďaka rozsiahlej digitalizácii služieb, rastu internetových hrozieb a prenikaniu IT do každodenného života. Zahŕňa mechanizmy autentifikácie a autorizácie.

Hrozba je potenciálna udalosť, ktorá môže spôsobiť ujmu.

Zraniteľnosť je slabé miesto, ktoré môže byť zneužité.

Riziko vyjadruje pravdepodobnosť a dopad incidentu.

2. Aké sú tri piliere modelu CIA a čo znamenajú?

- **Dôvernosť** zabezpečuje, aby k informáciám pristupovali iba oprávnené osoby.
- **Integrita** chráni úplnosť a správnosť informácií.
- **Dostupnosť** garantuje, že služby a dáta sú k dispozícii.

- Manažér musí vyvažovať tieto atribúty podľa povahy aktív a potrieb prevádzky.

3. Ako sa vyvíjala kybernetická bezpečnosť a regulácie?

Zameranie sa posunulo od ochrany mainframov k vrstvovej obrane a reakcii na internetové hrozby. Po roku 2000 pribudli APT, DDoS, ransomware a útoky na ICS (Incident Command System).

Na Slovensku sú aktuálne kľúčové:

- zákon č. 69/2018 Z. z., GDPR,
- zákon č. 95/2019 Z. z. o ITVS,
- vyhláška č. 179/2020 Z. z. Súčasťou sú NBÚ a SK-CERT.

4. Aké sú hlavné úlohy manažéra kybernetickej bezpečnosti?

- Plánuje, implementuje a hodnotí bezpečnostné opatrenia.
- Vedie bezpečnostné tímy a zodpovedá za analýzu rizík.
- Zabezpečuje súlad s legislatívou, tvorbu politík a bezpečnostnej dokumentácie.
- Koordinuje komunikáciu s IT, auditmi, dodávateľmi a štátnymi orgánmi.
- Zabezpečuje monitoring incidentov a školenia zamestnancov.

5. Ktoré dokumenty musí manažér pravidelne aktualizovať?

- Bezpečnostnú politiku, smernice a postupy vrátane plánov reakcie na incidenty.
- Evidenciu a správu prístupových práv s pravidelnými revíziami.
- Analýzu rizík, bezpečnostný projekt a súvisiacu dokumentáciu.
- Záznamy o incidentoch, auditoch a školeniach.
- Plány kontinuity a havarijnej obnovy s priebežným testovaním.

6. Aké sú hlavné zákony kybernetickej bezpečnosti na Slovensku?

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti transponuje NIS2.
- Zákon č. 95/2019 Z. z. o ITVS riadi informatizáciu verejnej správy.
- Vyhláška č. 179/2020 Z. z. kategorizuje systémy a stanovuje bezpečnostné opatrenia.

7. Čo je ISO/IEC 27001 a aké sú jej hlavné požiadavky?

- ISO/IEC 27001 je globálny štandard ISMS. Definuje požiadavky na zavedenie, prevádzku, monitorovanie a neustále zlepšovanie.
- Organizácia musí identifikovať riziká, stanoviť ciele a implementovať opatrenia.
- Vyžaduje audit, hodnotenie efektivity a ročné revízie vedením.
- Je základom pre certifikáciu a súlad s GDPR.

8. Aké sú povinnosti organizácií spadajúcich pod reguláciu KB podľa legislatívy?

- Systematická identifikácia a riadenie rizík s dokumentáciou.
- Implementácia technických a organizačných opatrení.
- Bezodkladné hlásenie incidentov NBÚ a SK-CERT.
- Pravidelné školenia zamestnancov a budovanie bezpečnostnej kultúry.
- Pravidelné audity a vyhodnocovanie súladu s predpismi.

9. Kto vykonáva dohľad a aké sankcie hrozia?

- NBÚ je hlavným regulátorom, vykonáva inšpekcie a vydáva opatrenia.
- MIRRI SR dohliada na ITVS vo verejnej správe.
- Úrad ochrany osobných údajov sankcionuje porušenia GDPR.

- Opakované nedostatky vedú k reputačným stratám.
- Sankcie zahŕňajú finančné pokuty až do stoviek tisíc eur za závažné porušenia.

10. Ako sa líšia CISO, CSIRT a DPO v rolách?

- **CISO** vedie strategické riadenie bezpečnosti. Spolupracuje s NBÚ a MIRRI SR.
- **CSIRT** rieši incidenty a forenzne analýzy.
- **DPO** dohliada na súlad s GDPR.

- Každá rola má definované kompetencie.

11. Aká je úloha CISO v organizácii?

- CISO je zodpovedný za strategické riadenie informačnej bezpečnosti v celej organizácii.
- Tvorí bezpečnostnú politiku, riadi riziká a koordinuje tímy.
- Komunikuje s vedením, NBÚ a ďalšími orgánmi dohľadu.
- Zodpovedá za súlad so zákonmi a normami ISO.
- Je kľúčovým styčným bodom pri vážnych incidentoch.

12. Ako má vyzerať štruktúra bezpečnostných tímov?

- Jasne definované roly: **CISO, bezpečnostní analytici, incident response tím** a **administrátori**.
- **Analytici** monitorujú logy a hrozby. Incident response rieši incidenty a robí forenznú analýzu.
- **Administrátori** implementujú technické opatrenia.

- Všetky roly sú zdokumentované s kompetenciami a kontaktnými údajmi.

13. Čo je bezpečnostná politika a čo musí obsahovať?

- Bezpečnostná politika je hlavný dokument definujúci ciele, princípy a pravidlá ochrany.
- Obsahuje rozsah platnosti, základné princípy CIA a úroveň ochrany.
- Presne vymedzuje zodpovednosti, roly a kompetencie.
- Obsahuje pravidlá správania, správy hesiel a hlásenia incidentov.
- Musí byť pravidelne revidovaná.

14. Ako súvisia bezpečnostná politika a smernice?

- Politika je nadradený rámec, smernice rozpracúvajú detaily. Typické smernice: politika riadenia prístupov, zálohovania, ochrany údajov. Rozpracúvajú technické a procesné detaily. Musia byť v súlade so zákonom a normami ISO. Aktualizujú sa pri zmenách technológií alebo legislatívy.

15. Prečo je externá spolupráca dôležitá?

CSIRT a SK-CERT poskytujú koordináciu pri incidentoch a zdieľanie informácií. Dodávatelia ovplyvňujú bezpečnosť cez spravované služby. Spolupráca s vysokými školami prináša aktuálne poznatky. Externí experti realizujú penetračné testy a audity. Sieť partnerstiev zvyšuje odolnosť a schopnosť reagovať.

16. Čo je informačný systém a aké sú jeho prvky?

- Informačný systém je organizovaný súbor ľudí, procesov, dát a technológií.
- Zahŕňa aplikačný softvér, databázy, infraštruktúru a komunikačné siete.
- Súčasťou sú procesy spracovania informácií a riadenia prístupov.
- Ľudský faktor je kľúčový.

- Bezpečnostné opatrenia musia zohľadniť všetky vrstvy.

17. Aké sú princípy prevádzky sietí a bezpečnosť?

- **Sieťové modely** (OSI, TCP/IP) popisujú vrstvy komunikácie.
- **Protokoly** (TCP, UDP, HTTP, DNS) definujú pravidlá prenosu.

- Správne adresovanie a segmentácia znižujú šírenie incidentov.
- Bezpečnostné opatrenia musia byť na viacerých vrstvách.
- Znalosť sieťových princípov je nutná pre návrh architektúry.

18. Akú úlohu zohráva firewall v bezpečnosti?

- Firewall je základné hraničné zariadenie filtrujúce sieťovú komunikáciu.
- Môže byť paketový filter, stavový firewall alebo aplikačný proxy.
- Umožňuje definovať povolený a zakázaný prenos medzi zónami.
- Jeho účinnosť závisí od správne navrhnutej politiky.
- Je prvou líniou obrany, ale musí byť doplnený IDS/IPS.

19. V čom sa líšia IDS a IPS?

- **IDS** (Intrusion Detection System) monitoruje prevádzku a upozorňuje. Vytvára reporty, ale aktívne neblokuje.
- **IPS** (Intrusion Prevention System) je v ceste komunikácie a blokuje. Znižuje riziko, ale pri zlej konfigurácii môže spôsobiť výpadky.

- Často sa používajú kombinované riešenia.

20. Prečo je správa systémov a riadenie konfigurácií kritické?

- Nesprávne konfigurácie sú príčinou zraniteľností.
- Správa systémov zahŕňa inštaláciu, patch management, monitoring a zálohovanie.
- Riadenie konfigurácií eviduje nastavenia a umožňuje kontrolované zmeny.
- Automatizačné nástroje znižujú chyby a zvyšujú konzistenciu.
- Audit konfigurácií pomáha odhaliť slabiny.

21. Čo je riadenie rizík podľa ISO 31000?

- ISO 31000 je systematický proces identifikácie, analýzy, hodnotenia a ošetrenia rizík. Uplatňuje sa na všetky úrovne riadenia.
- V kybernetickej bezpečnosti prioritizuje investície podľa skutočného dopadu. Zvyšuje spoľahlivosť, odolnosť a dôveryhodnosť. Vyžaduje pravidelné revízie a komunikáciu so zainteresovanými stranami.

22. Aké sú hlavné fázy riadenia rizík?

- **Kontext** - ciele, prostredie a kritériá.
- **Identifikácia** aktív, hrozieb a zraniteľností.
- **Analýza** posudzuje pravdepodobnosť a dopad.
- **Hodnotenie** určuje priority.
- **Ošetrenie** zahŕňa výber opatrení.

23. Ako sa identifikujú aktíva, hrozby a zraniteľnosti?

- **Aktívom** je čokoľvek, čo má pre organizáciu hodnotu a je potrebné chrániť. Evidujú sa priradením vlastníka.
- **Hrozby** sa delia na úmyselné (útoky) a neúmyselné (chyby).
- **Zraniteľnosti** sú slabiny v technike a procesoch.

- Používajú sa katalógy hrozieb a databázy (CVE).

24. Ako sa hodnotí riziko v praxi?

- Pravdepodobnosť sa hodnotí na škále 1--5 od veľmi nízkej po veľmi vysokú.
- Dopad sa rovnako hodnotí podľa finančných a právnych následkov.

- Riziko sa vyjadruje kombináciou pravdepodobnosti a dopadu.

- Výsledné hodnoty sa triedia do kategórií: nízke, stredné, vysoké. Matice rizík vychádzajú napr. z ISO 31000.

25. Uveďte stratégie ošetrenia rizík

- **Vylúčenie** -- ukončenie činnosti.
- **Redukcia** -- technické opatrenia a školenia.
- **Prenos** -- poistenie a SLA.
- **Akceptácia** -- pri nízkej úrovni.

- Výber stratégie musí byť zdokumentovaný a schválený vedením.

26. Ako sa vyberajú bezpečnostné opatrenia?

- Výber vychádza z priorít rizík a legislatívy. Zohľadňuje sa ISO/IEC 27001, odporúčania NBÚ.
- Manažér porovnáva alternatívy podľa nákladov a prínosov.
- Opatrenia musia byť primerané a auditovateľné.
- Výsledok sa premieta do bezpečnostného projektu.

27. Praktické uplatnenie modelu CIA v riadení rizík

- Pri každom aktíve sa hodnotí, či je kritickejšia dôvernosť, integrita alebo dostupnosť.

- Pre **dôvernosť**: riadenie prístupu, šifrovanie.
- Pre **integritu**: kontroly zmien, digitálne podpisy.
- Pre **dostupnosť**: redundancia, zálohy, BCP.

- Kombinácia určuje konkrétne opatrenia.

28. Ako sa zisťuje súlad opatrení?

- Porovnáva sa reziduálne riziko s akceptačnými kritériami.
- Využívajú sa audity, testy, penetračné testovanie.
- Sledujú sa incidenty a zistenia z kontrol.

- Ak je riziko príliš vysoké, navrhujú sa dodatočné opatrenia. Výsledky sa dokumentujú v správach o stave bezpečnosti.

29. Čo je technické bezpečnostné opatrenie?

- Technické opatrenie je kontrola realizovaná cez IT prostriedky.
- Patria sem:
  - firewally, IDS/IPS, antivírusy, šifrovanie.
  - Segmentácia sietí, hardening systémov, viacfaktorová autentifikácia.

- Technické opatrenia musia byť podporené procesmi a monitoringom. Ich účinnosť závisí od aktuálnosti a konfigurácie.

30. Čo je organizačné bezpečnostné opatrenie?

- Organizačné opatrenie je pravidlo, proces alebo zodpovednosť upravujúca správanie ľudí.
- Príklady: bezpečnostná politika, smernice, proces riadenia incidentov.
- Systém školení, segregácia povinností, schvaľovacie postupy.

Vytvárajú rámec pre konzistentné fungovanie technických opatrení.

31. Ako plánuje manažér bezpečnostné projekty?

- Plánovanie vychádza z analýzy rizík a legislatívnych povinností.
- Prioritu majú projekty chrániacu najkritickejšie aktíva.
- Plány musia mať jasné ciele, rozsah, harmonogram a rozpočet.
- Manažér definuje zodpovednosti a komunikačné kanály.

Dôležitá je väzba na stratégiu organizácie.

32. Čo znamená návrh a výber mechanizmov?

- Výber konkrétnych technológií a procesov na naplnenie cieľov.
- Posudzuje sa kompatibilita, náklady, škálovateľnosť.
- Zohľadňujú sa odporúčania noriem ISO a NBÚ.
- Porovnávajú sa riešenia rôznych dodávateľov.
- Výsledok sa premieta do architektonických návrhov.

33. Rozdiel medzi technickými a organizačnými opatreniami

- **Technické opatrenia** sú realizované cez IT prostriedky (firewally, šifrovanie).
- **Organizačné opatrenia** sú smernice, procesy a školenia. Ú

- spešná implementácia vyžaduje koordináciu oboch typov.
- Technické bez procesov vedú k chaosu.
- Procesy bez techniky k formálnemu, nie reálnemu zabezpečeniu.

34. Čo znamená zavádzanie a optimalizácia opatrení?

- Zavádzanie zahŕňa inštaláciu, konfiguráciu, testovanie a nasadenie.
- Optimalizácia znamená dolaďovanie podľa reálnych incidentov.

Využívajú sa pilotné projekty a fázy rollout-u. Manažér musí sledovať dopad na výkon a bezpečnosť.

Cieľom je rovnováha medzi bezpečnosťou a komfortom.

35. Ako sa hodnotí efektivita opatrení?

- Využívajú sa ukazovatele: počet incidentov, čas reakcie, počet zablokovaných útokov.
- Porovnávajú sa stavy pred a po zavedení opatrení.
- Sledujú sa náklady na incidenty.
- Dôležité sú zistenia z auditov, penetračných testov.
- Na základe hodnotenia sa opatrenia upravujú.

36. Čo je bezpečnostný incident?

- Incident je akákoľvek udalosť, ktorá ohrozuje dôvernosť, integritu alebo dostupnosť aktív.
- Môže ísť o útok zvonka, vnútorné zlyhanie, únik údajov.
- Bez formálneho procesu vzniká chaos a vysoké škody.
- Proces umožňuje rýchlu detekciu a eskaláciu.
- Je požadovaný legislatívou a normami ISO/IEC.

37. Základné kroky detekcie a nahlasovania incidentu

- Detekcia prostredníctvom monitoringu, SIEM, IDS/IPS alebo hlásení.
- Posúdenie závažnosti a kategorizácia.
- Formálne zaznamenanie v ticketovom systéme.
- Spustenie komunikačných postupov.
- Pri vybraných kategóriách hlásenie NBÚ, SK-CERT a ďalším inštitúciám.

38. Činnosti pri vyšetrovaní incidentu

- Zber dôkazov z logov, sieťovej prevádzky, systémov.
- Analýza rozsahu, vektorov útoku a dotknutých aktív.
- Dokumentovanie časovej osi a prijatých opatrení.
- Zachovanie forenznej hodnoty dôkazov.
- Výstupom je správa s odporúčaniami na zlepšenie.

39. Komunikácia s NBÚ, SK-CERT a tretími stranami

- Organizácia musí poznať kategórie incidentov, ktoré je povinná hlásiť.
- Hlásenia v stanovenej forme a lehotách.
- SK-CERT poskytuje metodickú podporu a koordináciu.
- Pri incidentoch u dodávateľov postup podľa SLA.

- Transparentná komunikácia chráni reputáciu.

40. Čo je post-incident analýza?

- Spätné hodnotenie incidentu s cieľom poučiť sa.
- Obsahuje **príčiny**, **priebeh** a **dopady**.
- Hodnotí účinnosť detekcie a reakcie.
- Navrhuje úpravy politík, postupov a konfigurácií.
- Podklad pre aktualizáciu analýzy rizík a dokumentácie.

41. Prečo je personálna bezpečnosť kľúčová?

- Väčšina incidentov súvisí s ľudským faktorom.
- Zamestnanci majú prístup k systémom a údajom.
- Ich správanie ovplyvňuje úroveň rizika.
- Personálna bezpečnosť znižuje insider hrozby a ľudské chyby.
- Je požadovaná legislatívou a normami ISO/IEC.

42. Pravidlá pre zamestnancov a tretie strany

- Jasné definovanie zodpovedností a oprávnení.
- Podpis vyhlásení o mlčanlivosti a bezpečnostných pravidiel.
- Povinnosť hlásiť incidenty a podozrivé správanie.
- U dodávateľov: bezpečnostné klauzuly v zmluvách.
- Pravidlá pravidelne komunikovať a aktualizovať.

43. Čo znamená selektívny prístup?

Princíp: každý má iba oprávnenia potrebné na prácu (least privilege).

- Prístupy podľa rolí (RBAC) a pravidelné revízie.
- Segmentácia systémov a oddelenie prostredí.
- Pri odchode zmena oprávnení okamžite.
- Správne nastavenie obmedzuje dopad kompromitovaného účtu.

44. Ako majú vyzerať školenia a povedomie?

- Pravidelné, povinné a prispôsobené typom používateľov.
- Aktualizácia podľa nových hrozieb a legislatívy.
- Kombinácia e-learning, workshopy, phishingové simulácie.

- Praktickosť -- reálne útoky, bezpečná práca s e-mailom.
- Výsledky evidovať ako dôkaz súladu.

45. Ako prebieha kontrola a revízia prístupov?

- Pravidelne porovnávajú prístupy s aktuálnou pozíciou.
- Vlastníci systémov potvrdzujú potrebu účtov.
- Rušenie neaktívnych a nadbytočných účtov.
- Kontrola administrátorských účtov a prístupov tretích strán.
- Výsledky dokumentovať pre audity.

46. Rozdiel medzi interným a externým auditom

- **Interný audit** vykonávajú pracovníci organizácie, zameraný na zlepšovanie.
  - Interný overuje súlad s internými politikami.

- **Externý audit** realizuje nezávislá tretia strana (certifikačný orgán).
  - Externý posudzuje splnenie noriem a zákonov. Výstupom: zistenia a akčné plány.

47. Prečo je dôležitá správa bezpečnostnej dokumentácie a hodnotenie súladu (compliance)?

- Dokumentácia preukazuje splnenie zákona a noriem.
- Bez nej ťažko obhájiť rozhodnutia pri kontrolách.
- Hodnotenie súladu identifikuje medzery.
- Umožňuje plánovať nápravné opatrenia.
- Posilňuje dôveru partnerov a regulátorov.

48. Čo je BCP a DRP?

- **BCP** (Business Continuity Plan) definuje, ako organizácia udrží kritické procesy pri narušení.
- **DRP** (Disaster Recovery Plan) sa zameriava na obnovu IT služieb.

- BCP vychádza z analýzy dopadov a stanovuje RTO a RPO.
- DRP obsahuje technické scenáre obnovy. Oba sa pravidelne testujú.

49. Úloha kryptografie a PKI v ochrane dát

- Kryptografia zabezpečuje dôvernosť, integritu a autentickosť.
- Symetrické šifrovanie pre veľké objemy. Asymetrické pre kľúče a podpisy.

- PKI poskytuje rámec certifikátov a dôveryhodnosti. Základ pre HTTPS, VPN, e-podpis.

Manažér musí riešiť správu certifikátov a kľúčov.

50. Nové hrozby a trendy: AI, IoT, NIS2

- **AI** - sofistikovanejšie útoky aj lepšia obrana.
- **IoT** - rozsiahla útočná plocha.
- **NIS2** - rozšírené povinnosti a požiadavky. Potreba kontinuálneho vzdelávania.

Budúcnosť bude viac regulovaná a prepojená.

Veľa šťastia na skúške!