Ishod 2 (12 bod, 30 min)

1. **(1,5) Što je autentifikacija? Kratko objasnite dvofaktorsku autentifikaciju.**

Autentifikacija je proces provjere identiteta korisnika.
2FA koristi dva različita faktora (lozinka + SMS kod)

2. **(1,5) Koji je način autentifikacije sigurniji: mobile push notifikacija ili slanje OTP koda putem SMS-a? Objasnite.**

Mobile push notifikacija je sigurnija od slanja OTP koda putem SMS-a, jer SMS može biti presretnut (SIM swap napadi).

3. **(2) Objasnite koncept risk based autentifikacije (RBA). Koji sve čimbenici se analiziraju prilikom spajanja na neku uslugu koja koristi RBA? Temeljem koje informacije će RBA blokirati pristup?**

Prilagođava provjeru identiteta na temelju rizika. Analizira se lokacija, uređaj, ponašanje korisnika. Ako se otkrije neuobičajeno ponašanje, RBA može blokirati pristup.

4. **(1) Koja je uloga sigurnosne politike? Objasnite što je bolja praksa: imati jedan dokument ili više manjih?**

Sigurnosna politika definira pravila zaštite informacija. Bolja praksa je imati više manjih dokumenata jer su lakši za ažuriranje i primjenu.

5. **(1,5) Objasnite najvažnije NIST preporuke za upravljanje lozinkama te zašto su učinkovite.**

NIST preporuke za lozinke:

- Osmišljavanje pass-fraza umjesto tradicionalnih šifru
- Koristiti dulje lozinke
- Redovito ih ažurirati samo ako postoji sumnja na kompromitaciju

Učinkovite su jer smanjuju frustraciju korisnika i povećavaju sigurnost.

6. **(1,5) Objasnite odgovornosti uprave, voditelja sigurnosti i zaposlenika u području informacijske sigurnosti.**

Uprava, voditelj sigurnosti i zaposlenici su svi odgovorni za informatičku sigurnost:

- **Uprava** - postavlja politike
- **Voditelj** - provodi mjere
- **Zaposlenici ih poštuju**

7. **(2) Zašto je važno upravljati eksternalizacijom? Pojasnite na primjeru SolarWinds napada.**

Ako se dobavljači ne nadziru, povećava se rizik od napada jer napadači često napadaju slabije zaštićene partnere.
Kod **SolarWinds napada**, napadači su kompromitirali softver jednog dobavljača i preko njega došli do tisuća organizacija.

8. **(1) Kratko objasnite najvažniju kontrolu za zaštitu prijenosnih računala.**

Najvažnija kontrola za zaštitu prijenosnih računala je enkripcija diska (npr. BitLocker) – štiti podatke ako se uređaj izgubi ili ukrade.

Dodatno

1) **Usporedite push i SMS notifikacije. Koje su prednosti i nedostatci?**

Push prednosti: enkripcija podataka (šalje se kriptirano), 2FA funkcionalnosti

Push nedostaci: phishing napadi, te pristup podacima pri fizičkoj krađi uređaja

SMS prednosti: manje ovisno o aplikacijama, ali nije potpuno otporno na malware

SMS nedostaci: phishing, nedostatak enkripcije

2) **Što je identifikacija?**

Identifikacija je proces utvrđivanja identiteta korisnika.

3) **Što je identifikacija, autentifikacija i višefaktorska autentikacija (MFA)?**

- **Identifikacija** – utvrđivanje identiteta korisnika
- **Autentikacije** – provjera identiteta korisnika i dozvola pristupa
- **MFA** - kombinacija više načina autentikacija