Upravljanje sigurnošću

Voditelj sigurnosti informacijskog sustava – CISO

- osoba koja razumije sigurnost i ne bavi se operativnim detaljima
- pri vrhu organizacijske strukture - jedna od zahtjevnijih zadaća CISO-a je komunikacija s Upravom

- Voditelj sigurnosti zadužen je za cjelokupnu sigurnost (fizičku, informacijsku, prijevare

Faza 1 (1990-te – 2000)

- uvjerenje da informacije u tvrtki nisu nikome interesantne
- ograničena sigurnost, naglasak na lozinkama i kontroli pristupa

Faza 2 (2000 – 2004)

- Pojava legislative za zaštitu privatnosti i podataka
- Prvi put se zahtijevalo da postoji netko zadužen za sigurnost

Faza 3 (2004 – 2008)

- Problem s ispunjavanjem regulative
- CISO orijentiran na rizike, naglasak na „mekim vještinama", još uvijek dio IT-ja

Faza 4 (2008 – 2016)

- Sigurnost svjesna prijetnji, društvene mreže, mobilni uređaji, računarstvo u oblaku
- CISO treba marketing, politiku, tehnologiju

Faza 5 (2016 – 2020-te)

- Privatnost dobija na značenju (GDPR), „outsource", dobavni lanac
- CISO svjestan privatnosti i podataka

<u>SVRHA CISO-a</u>

- Nadzire i koordinira aktivnosti vezane uz sigurnost informacijskog sustava.
- Inicira primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava.
- Ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

Zadaće CISO-a

- Izrada internih akata
- Provjera provođenja internih akata
- Upravljanje rizicima – temeljni alat u radu
- Upravljanje incidentima – postupak bi trebao biti definiran aktima
- Edukacija i osvještavanje
- Izvješćivanje uprave i nadzornog odbora
- Rad s vanjskim suradnicima
- Analiza sigurnosnih potreba
- Sudjelovanje u bitnim aktivnostima planiranja poslovanja i klasifikacije informacija
- Sudjelovanje u razvoju i održavanju IT-a
- definira način upravljanja sistemskih i operativnim zapisima (logovima)

Problemi (i izazovi) s kojima se CISO susreće

- Vrlo dinamična okolina koju je teško pratiti
- Evaluacija rizika raznih tehnologija
- Koordiniranje aktivnosti s organizacijskom jedinicom informacijske tehnologije i unutarnjom revizijom
- Operativni i strateški poslovi

Kompetencije CISO-a

- Upravljačke vještine
- Poslovne vještine
- Stalno usavršavanje
- „Soft skills”
- Vještine i znanja iz sigurnosti informacijskih sustava
- Planiranje oporavka od katastrofičnih događaja
- Sposobnost istraživanja sigurnosnih incidenata

Interni akti

Temeljni akt je **Politika sigurnosti informacijskog sustava**

krovni dokument koji definira što za informacijski sustav znači da je siguran

temelj za ostale akte

Vrste internih akata:

1. Politika
2. Pravilnik
3. Procedura

Sadržaj politike

- Pregled – o čemu je politika
- Svrha – zašto je politika potrebna
- Obuhvat – što sve politika obuhvaća
- Kome je namijenjena – tko je sve obvezan djelovati temeljem politike
- Politika – Temeljni dio dokumenta koji navodi što treba biti učinjeno
- Definicije – Pojmovi koji se upotrebljavaju u politici
- Verzioniranje – Vođenje evidencija o promjenama

Nadzor sigurnosti

Sigurnosno operativni centar - centralizirana funkcija unutar organizacije koja korištenjem ljudi, procesa i tehnologije kontinuirano prati i poboljšava sigurnosno stanje organizacije te sprečava, detektira, analizira i odgovara na sigurnosne incidente

Nadzor rada CISO-a

- Sprečavanje potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja

Tu dužnost obavljaju: unutarnja i vanjska revizija, osoba/funkcija nadređena voditelju sigurnosti - CEO, CIO, CSO