Øvelse 28 - CIA modellen

Information

CIA modellen er central i arbejdet med informationssikkerhed. Hvor modellen stammer fra er der uenighed om, men modellen er simpel og kan bruges mange steder i arbejdet med sikkerhed.

På dansk er modellen oversat til FIT, men det er mest udbredt at anvende den engelske betegnelse.

C står for **C**onfidentiality (Fortrolighed) I står for **I**tegrity (Itegritet) A står for **A**vailability (Tilgængelighed)

Formålet med denne øvelse er at blive bekendt med CIA modellen.

Instruktioner

Øvelsen skal laves som gruppe/team

1. Læs om CIA modellen i bogen "IT-Sikkerhed i praksis, en introduktion" kapitel 2.
2. Vælg **et** af følgende scenarier som i vil vurdere i forhold til CIA:
    - En password manager (software)
    - En lægeklinik (virksomhed)
    - Dine data på computere og cloud (...)
    - Energileverandør (kritisk infrastruktur)
3. Vurder, prioitér scenariet i forhold til CIA modellen. Noter og begrund jeres valg og overvejelser.
4. Hvilke(n) type hacker angreb vil være mest aktuelt at tage forholdsregler imod? (DDos, ransomware, etc.)
5. Hvilke forholdsregler kan i tage for at opretholde CIA i jeres scenarie (kryptering, adgangskontrol, hashing, logging etc.)
6. Hver gruppe fremlægger det de er kommet frem til og alle giver feedback.

Løsning

1. Valgt: **En lægeklinik (virksomhed)**

2. Vurdering:
    - Confidentiality (Fortrolighed)
        - Journaler om personer
        - Følsomme personoplysninger (cpr, adresse, m.m.)
        - GDPR
    - Integrity (Integritet)
        - Det vigtigt, at dataen i f.eks. jorunaler ikke ændres.
    - Availability (Tilgængelighed)
        - Dataen skal være tilgængelig, når den bliver efterspurgt.
3. Forholdsregler mod hackerangreb
    - Eftersom Availability (Tilgængelighed) i CIA modellen siger, at dataen skal være tilgængelig skal der sikres mod DDoS.
    - Der skal også sikres mod ransomware, da der er mange personfølsomme oplysninger, som behandles.
    - Der skal også trænes mod phishing m.m.
4. Opretholdelse af CIA
    - Der skal tages hånd om dem alle.

Vurdering af vores besvarelse og bedre opsat af chatten.

3. Vurder og prioriter scenariet i forhold til CIA

CIA-komponent	Vurdering	Begrundelse / Eksempler
Confidentiality (Fortrolighed)	Højeste prioritet	Journaler og patientoplysninger (CPR, adresse, helbredsoplysninger) er ekstremt følsomme. GDPR kræver, at de beskyttes. Brud kan have juridiske og etiske konsekvenser.
Integritet (Integritet)	Næsthøjeste	Journaler skal være korrekte. Fejl eller ændringer i data kan føre til forkert behandling af patienter. Audit logs og versionskontrol er vigtige.
Availability (Tilgængelighed)	Tredje prioritet	Data skal være tilgængelige for læger og patienter, men midlertidigt nedbrud er mindre kritisk end tab af fortrolighed eller integritet. Backup-systemer og redundans sikrer dette.

4. Hvilke typer hackerangreb er mest relevante?

Angrebstype	Relevans for lægeklinik	Påvirker CIA
Ransomware	Krypterer data og kræver løsesum	**Availability & Confidentiality**
Phishing	Kan stjæle login og adgang til patientdata	**Confidentiality**
DDoS	Gør systemet utilgængeligt	**Availability**
Insider-trusler	Utilsigtet eller ondsindet læk af oplysninger	**Confidentiality**

5. Forholdsregler for at opretholde CIA

CIA-komponent	Forholdsregler
Confidentiality	Kryptering af data i hvile og under overførsel, stærk adgangskontrol, to-faktor autentifikation, sikker håndtering af CPR og andre følsomme oplysninger.
Integrity	Hashing af journaler, versionskontrol, audit logs for ændringer, backup af data.
Availability	Redundante systemer, regelmæssige backups, DDoS-beskyttelse, nødprocedurer og plan for systemnedbrud.

2026-02-19 12:04:53