Trei întrebări. Trei obiective.

Reține C • I • D: Confidențialitate • Integritate • Disponibilitate

C CONFIDENȚIALITATE

Cine poate vedea?

Doar persoanele autorizate au acces la informații.

EXEMPLU: Un elev vede doar notele la care are drept de acces.

SECRET

Criptare + drepturi de acces

I INTEGRITATE

Datele sunt corecte?

Datele nu sunt modificate neautorizat; sistemele funcționează corect.

EXEMPLU: O notă nu poate fi schimbată de un elev.

CORECT

Drepturi de modificare + jurnale

D DISPONIBILITATE

Pot folosi serviciul?

Serviciile sunt utilizabile atunci când este nevoie de ele.

EXEMPLU: Catalogul online răspunde când este accesat.

ACCESIBIL

Monitorizare + copii de siguranță

Același incident poate afecta C + I + D. O singură măsură nu este suficientă.

PROTECȚIA FUNCȚIONEAZĂ ÎN STRATURI

PREVII
Acces minim, actualizări

→

DETECTEZI
IDS, monitorizare, jurnale

→

RĂSPUNZI
Raportezi și limitezi incidentul

→

RECUPEREZI
Restaurezi din copii verificate

4 OBICEIURI UTILE

- Parole lungi și unice
- MFA: mai mult decât parola
- Actualizează programele
- Verifică mesajele suspecte

Cum arată un atac?

Întreabă-te: ce este afectat - secretul informației, corectitudinea ei sau accesul la serviciu?

CONFIDENȚIALITATE

Divulgare neglijentă
Date trimise accidental altcuiva.

Interceptare
Informații citite în timpul transmiterii.

Acumulare de informații
Detalii publice combinate pentru a deduce informații private.

PROTECȚIE

Criptează. Controlează accesul. Verifică destinatarul.

INTEGRITATE

Atac la autentificare
Atacatorul se dă drept alt utilizator.

Furtul sesiunii
Preia o sesiune deja autentificată.

Atac de protocol
Exploatează slăbiciuni ale protocolului.

Manipulare socială
Păcălește o persoană să ofere acces.

Acces neglijent
Ex.: firewall dezactivat sau configurat greșit.

Abuz de privilegii
Folosește drepturile în scop nepermis.

Backdoor
O cale ascunsă de acces la sistem.

DISPONIBILITATE

Interferențe și inundare
Bruiaj sau prea multe cereri: serviciul nu mai răspunde.

Supresia jurnalizării
Ascunde evenimentele sau îngreunează analiza jurnalelor.

Date neașteptate
Date pe care aplicația nu le tratează corect pot provoca blocarea.

PROTECȚIE

Filtrează traficul. Aplică actualizări. Pregătește recuperarea.

Gruparea este orientativă: de exemplu, furtul unei sesiuni poate compromite și confidențialitatea.

VERIFICĂ-TE ÎN 30 DE SECUNDE

1. Cineva citește notele fără drept.
2. Cineva schimbă o notă fără drept.
3. Catalogul nu mai răspunde.

Răspunsuri: 1 → C 2 → I 3 → D

REGULA DE AUR: acces doar cât este necesar + mai multe niveluri de protecție + utilizatori instruiți.

Securitatea reduce riscul. Tehnologia, oamenii și procedurile trebuie să funcționeze împreună.