

Inleiding tot CIA

- Wat is CIA?
- • Het CIA-trio staat voor:
 - - Confidentiality (Vertrouwelijkheid)
 - - Integrity (Integriteit)
 - - Availability (Beschikbaarheid)
- • Deze principes vormen de basis voor informatiebeveiliging.



Confidentiality

(Vertrouwelijkheid)

Definitie:

-
- Verzekeren dat alleen geautoriseerde gebruikers toegang hebben tot gevoelige informatie.
-

Belang:

-
- Bescherming van persoonlijke en gevoelige gegevens.
-

Voorbeelden:

-
- Encryptie
-
- Authenticatie (wachtwoorden, biometrie)
-
- Toegangscontroles

Integrity

(Integriteit)

Definitie:

-
- Waarborgen dat informatie accuraat en onveranderd blijft, tenzij geautoriseerde veranderingen plaatsvinden.
-

Belang:

-
- Vertrouwen in de juistheid van gegevens.
-

Voorbeelden:

-
- Hashing
-
- Digitale handtekeningen
-
- Versiebeheer
-

Availability

(Beschikbaarheid)

Definitie:

-
- Zorgen dat informatie en systemen toegankelijk zijn wanneer nodig.
-

Belang:

-
- Voorkomen van systeemuitval of gegevensverlies.
-

Voorbeelden:

-
- Redundantie (back-ups)
-
- Load balancing
-
- Bescherming tegen DDoS-aanvallen
-

Waarom zijn de CIA- principes belangrijk?

Impact op organisaties:

- Gegevensdiefstal (verlies van vertrouwelijkheid)
- Gegevensvervalsing (schending van integriteit)
- Downtime en systeemstoringen (verlies van beschikbaarheid)

Balans tussen de CIA-principes



Evenwicht bewaren:



- Niet elk principe is even belangrijk in elke situatie.



- Voorbeeld: Hogere vertrouwelijkheid kan de beschikbaarheid verminderen.

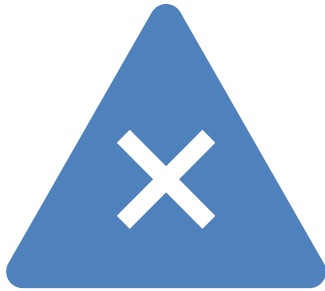
Voorbeelden uit de praktijk

- Case study 1: Hack van een overheidsinstantie (verlies van vertrouwelijkheid)

- Case study 2: Corruptie van databasebestanden (verlies van integriteit)

- Case study 3: Systeemstoring door een cyberaanval (verlies van beschikbaarheid)

Conclusie



- CIA-principes zijn de hoekstenen van informatiebeveiliging.



- Elke organisatie moet deze principes toepassen om beveiliging te waarborgen.

Bedankt voor je
aandacht! Zijn
er nog vragen?

