

CIA

oder die 3 1/2 Säulen der IT-Sicherheit

Michael Schommer
Herrenberg Digital
21.03.2018

Abgrenzung

Datenschutz:

Schutz personenbezogener Daten vor Missbrauch, eher rechtlicher Rahmen

IT-Sicherheit:

Schutz von IT-Systemen vor Einbruch, Missbrauch, Beschädigung etc.

eher technische, prozessurale Maßnahmen

IT Security Controls

Welche IT Security Controls kennen Sie?

CIA

Confidentiality
Integrity
Availability
Authenticity

CIA: Schutzziele

Vertraulichkeit

Integrität

Verfügbarkeit

Authentizität

(+ Nichtabstreitbarkeit, Privatsphäre...)

C - Vertraulichkeit

Daten sind nur für befugte
Benutzer zugänglich

C - Vertraulichkeit

Mögliche Security Controls:

Zutrittskontrolle zum RZ

Zugangskontrolle: Login, Berechtigungen

Verschlüsselung

...

I - Integrität

**Daten können nicht unbefugt
verändert werden**

(oft auch: Alle Änderungen müssen lückenlos nachvollziehbar sein)

I - Integrität

Mögliche Security Controls:

Prüfsummen

Message Digests (MD5, SHA etc.), HMAC

Digitale Signaturen

Blockchain

...

NICHT: Verschlüsselung.

Oder doch?

Nein.

Exkurs: Verschlüsselung vs. Integrität

Klartext “IIIII” → verschlüsselt “%l0m.F2YxH&”

Chiffre “%l0m.F2YxH&” → entschlüsselt “IIIII”

Verändertes Chiffre “%l0m.**E**2YxH&” entschlüsselt zu “IIII1I”

Für Menschen erkennbar... vielleicht.

Für Algorithmen eher nicht.

Also: Auch verschlüsselte Daten können verändert werden –
vielleicht sogar, ohne dass es auffällt.

Verschlüsselung hilft also nicht zur Integritätssicherung!

A - Verfügbarkeit

IT-Systeme stehen im geplanten
Rahmen zur Verfügung

A - Verfügbarkeit

Mögliche Security Controls:

Zutrittskontrolle zum RZ

Server-Cluster

Ausweich-RZ

RAID

Cloud

...

A - Authentizität

Der Ursprung eines Datums kann zweifelsfrei festgestellt werden

A - Authentizität

Mögliche Security Controls:

Digitale Signaturen

Zugangskontrolle: Login, Berechtigungen

...

Done.