Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden

Datenschutz Informationssicherheit Datensicherheit

Datenschutz vs Datensicherheit

Datenschutz Datensicherheit

Datenschutz vs Datensicherheit

Datenschutz Schutz von Personen Datensicherheit Schutz von Daten

Datenschutz

Datenschutz -Schutz von Personen

- ☐ Rechtlich/organisatorisches Thema
- ☐ Schutz von personenbezogenen Daten
- ☐ Schutz des allgemeinen Persönlichkeitsrechtes
- ☐ Stichworte: Datenschutz-Grundverordnung DSGVO und Bundesdatenschutz-Gesetz BDSG

Schutzziele der Informationssicherheit

CIA

Schutzziele der Informationssicherheit

Schutz von Informationen vor

- unbefugtem Zugriff
- Manipulation
- Verlust.

Umfasst verschiedene

- Maßnahmen und Konzepte,
- um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Grundprinzipien (CIA)

1. Vertraulichkeit (Confidentiality)
2. Integrität (Integrity)
3. Verfügbarkeit (Availability)

Grundprinzipien (CIA)

1. Vertraulichkeit (Confidentiality)

Nur autorisierte Personen dürfen auf Informationen zugreifen.

Maßnahmen: Verschlüsselung, Zugriffskontrollen, VPNs

2. Integrität (Integrity)

Informationen dürfen nicht unbemerkt verändert oder manipuliert werden.

Maßnahmen: Hashing, digitale Signaturen, Prüfmechanismen

3. Verfügbarkeit (Availability)

Informationen müssen für berechtigte Nutzer jederzeit zugänglich sein.

Maßnahmen: Backups, Redundanz, DDoSSchutz

Gefahren für Informationssicherheit

Hackerangriffe

- z. B. Phishing, Malware, Ransomware, Viren

Menschliche Fehler

- z. B. schwache Passwörter, versehentliches Löschen

Technische Fehler

- z. B. Hardware-Ausfälle, Software-Bugs

Naturkatastrophen

- z. B. Feuer, Überschwemmung

Datensicherheit

Schutz vor

Gewährleistung von

- [ ] Unbefugter Zugriff Dritter,
- [ ] Manipulation,
- [ ] Verlust der Daten
- [ ] Vertraulichkeit,

- Integrität,
- Verfügbarkeit von Daten

Datenschutz vs Datensicherheit vs Informationssicherheit

Datenschutz Schutz von Personen

- Regelwerk • Rechtlich/organisatorisches Thema
- Schutz von personenbezogenen Daten
- Schutz des allgemeinen Persönlichkeitsrechtes
- Stichworte: Datenschutz-Grundverordnung DSVGO und Bundesdatenschutz-Gesetz BDSG

Datensicherheit Schutz von Daten

- Maßnahmen • Technisches Thema
- Sichere Verarbeitung von Daten
- Schutz vor : Unbefugter Zugriff Dritter, Manipulation, Verlust der Daten
- Gewährleistung von: Vertraulichkeit, Integrität, Verfügbarkeit von Daten

Informationssicherheit

- Grundprinzipien
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Datenschutz

'Du darfst diese Daten nur unter bestimmten Bedingungen nutzen'

Datensicherheit

'Wenn du sie nutzt, musst du sie schützen'

Schutzziele

'Was bedeutet schützen'

Datensicherheit

Aspekt: Schutz vor Verlust von Daten

Datensicherung

Prozess des Sicherns von Daten

Ziel

- Daten im Falle des Verlusts wiederherstellen können

Redundanz

- Daten werden mehrfach erstellt
- Begriffe: Sicherungskopie/ Backup

Speicherung der Kopien

- Online vs offline
- Unterschiedliche Medien

Räumliche Trennung von Backup und Daten

Ziel: Datensicherheit/ Ausfallsicherheit erhöhen

Georedundanz

Offsite-Backup

- Backup an einem anderen Standort

Onsite-Backup

- Backup am gleichen Standort

Räumliche Entfernung von der EDV-Anlage

Räumliche Entfernung von der EDV-Anlage

Räumliche Entfernung von der EDV-Anlage

Lokal (gleicher Standort)

Vorteile:

- Sehr schnell verfügbar
- Einfach umzusetzen

Nachteile:

- Kein Schutz bei Brand, Wasser, Diebstahl
- Beide Daten können gleichzeitig verloren gehen

Standortnah (gleiches Gebäude / Gelände)

Vorteile:

- Etwas mehr Sicherheit als lokal · Schneller Zugriff bleibt erhalten

Nachteile:

- Risiken wie Feuer oder Stromausfall betreffen oft trotzdem alles

Remote / Cloud

Vorteile:

- Automatisierbar
- Geografisch weit entfernt
- Oft redundant gespeichert

Nachteile:

- Abhängigkeit vom Internet
- Laufende Kosten
- Datenschutz beachten

Offsite bzw AirGapped Backup (physisch getrennt)

Vorteile:

- Sehr hoher Schutz vor Hackerangriffen und Ransomware
- Kann nicht übers Netzwerk kompromittiert werden
- Schutz vor lokalen Katastrophen

Nachteile:

- Manuelles Handling nötig
- Organisation aufwendig
- Wiederherstellung langsamer

Räumliche Entfernung von der EDV-Anlage: Sicherheitsniveau

Sicherheits- niveau	Typisch	Schützt vor	Schützt nicht vor / Risiken	Besonderheiten / Beispiel
Lokal gespeicherte Backups (z. B. USB-Platte am selben PC)	• versehentlichem Löschen • einfachen Softwarefehlern	• Hardwaredefekt (wenn beide betroffen sind) • Diebstahl / Brand / Wasser • Ransomware	Nur Minimallösung, kein echtes Sicherheitskonzept	Niedrig
Standortnahes Backup (z. B. NAS im selben Gebäude)	• einzelnen Geräteausfällen	• größere Schäden (Feuer, Stromausfall) • Angriffe im Netzwerk	NAS von Synology im Serverraum	Mittel

Sicherheits- niveau	Typisch	Schützt vor	Schützt nicht vor / Risiken	Besonderheiten / Beispiel
Remote/ Cloud-Backups	• lokale Katastrophen • Hardwareausfälle	• Ransomware (bei erreichbaren Backups) • Fehlkonfiguration • Internetabhängigkeit	Microsoft Azure oder Amazon Web Services	Hoch
Offsite + Air-Gap	• Ransomware • gezielten Angriffen • Manipulation von Backups	-	physisch getrenntes Backup Beispiel: Cloud + externe Platte im Safe	Sehr hoch
3-2-1-Regel (3 Kopien, 2 Medien, 1 offsite)	• nahezu allen realistischen Ausfallszenarien	-	Ergänzt durch: Air-Gap, Verschlüsselung, Wiederherstellungstests	Maximal (Best Practice)

Backup Varianten, Methoden und Strategien

Prozess der Sicherung

Wie werden die Daten gesichert

Wie werden die Ressourcen eingesetzt

- Speicherkapazität
- Dauer der Datensicherung
- Dauer der Wiederherstellung

Prozess: Backup-Varianten

Speicherabbild- Sicherung	Ein Abbild des gesamten Systems wird erstellt Vorteil: Nur 1 Datei Nachteil: Zeitaufwand + hoher Speicheraufwand
Komplett-/ Vollsicherung	Alle Daten werden gesichert
Komplett-/ Vollsicherung	Nachteil: Zeitaufwand + hoher Speicheraufwand
Differenzielles Backup	Jeden Tag: Änderungen seit Vollsicherung

Inkrementelles Backup

Tag 1 nach Vollsicherung: Änderungen seit Vollsicherung

Später: Änderungen seit letztem Backup

Allgemein: Änderungen seit letztem Backup

Backup Methoden

Differenziell

Step 1: Vollsicherung

Differenziell

Backups werden Tag für Tag größer

- Mit jeder Teilsicherung werden die vorherigen Daten erneut mit gespeichert

Vorteil

- Deutlich schneller als Vollsicherung

Nachteil

- Dateien, die nach Vollsicherung nur einmal geändert werden, werden jedesmal wieder gesichert
- Alle Änderungen seit dem letzten vollständigen Backup werden gesichert
- Benötigt mehr Speicherplatz

Wiederherstellung

- Aus Vollbackup und 1 Datei des entsprechenden Tages

Inkrementell

Unterschied

- mit jeder Teilsicherung werden nur die Daten gesichert, die seit der letzten Sicherung (egal, ob Voll- oder Teilsicherung) erstellt oder verändert wurden

Verknüpfung

- einzelne Datensätze sind miteinander verknüpft

Vorteil

- geringer Speicherbedarf
- gehen schnell

Nachteil

- Wiederherstellung aus Vollsicherung und allen nachfolgenden inkrementellen Sicherungen wird komplexer

Änderungsverfolgung

Change Detection

Verfahren

Verfahren	Fachbegriff
Archivbit nutzen	Archive Bit Tracking
Zeitstempel vergleichen	Timestamp-based Change Detection
Prüfsummen vergleichen	Checksum-based Detection
Dateisystem protokolliert Änderungen	Journal-based Change Detection

Archiv-Bit

Dateimerkmal von Windows um zu markieren, ob eine Datei seit der letzten Sicherung verändert wurde.

Es hilft Backup-Programmen zu entscheiden, welche Dateien gesichert werden müssen.

Archiv-Bit

Archiv-Bit

Vollbackup

- sichert alle Daten
- Danach Archivbit wieder auf 0

Inkrementelles Backup

- Sichert nur Daten mit Archivbit = 1
- Danach: Archivbit wieder auf 0
- Folge: Jedes inkrementelle Backup hat nur Änderungen seit letztem Backup

Differenzielles Backup

- Sichert nur Daten mir Archivbit = 1
- Danach: Archivbit wird NICHT auf 0 gesetzt
- Folge: Alle Änderungen seit letztem Vollbackup bleiben markiert

Archiv-Bit

PowerShell

```
- Get-Item "C:\Test\datei.txt" | Select-Object Name, Attributes · (Get-Item "C:\Test\datei.txt").Attributes += "Archive"
```

- (Get-Item "C:\Test\datei.txt").Attributes -= "Archive"

CMD

- attrib C:\Test\datei.txt · attrib -A C:\Test\datei.txt · attrib +A C:\Test\datei.txt

Zeitstempel

Linux

- mtime → Inhalt geändert
- ctime → Metadaten/Rechte geändert
- atime → Zugriff auf Datei

Beispiel

- ls -l
- stat datei

Windows

- (Get-Item "C:\Test\datei.txt").LastWriteTime

Prüfsummen/ Hashes/ Hashwerte

Windows

```
- Get-FileHash C:\Test\datei.txt · Get-FileHash C:\Test\datei.txt -Algorithm MD5
```

Dateien vergleichen

- $hash1 = (Get-FileHash C:\Test\a.txt).Hash · $hash2 = (Get-FileHash C:\Test\b.txt).Hash · · $hash1 -eq $hash2

Prüfsummen/ Hashes/ Hashwerte

Linux

- sha256sum datei.txt
- md5sum datei.txt
- sha256sum a.txt b.txt

Beispiel

```
- hash1=$(sha256sum a.txt) · hash2=$(sha256sum a.txt) · [ "$hash1" = "$hash2" ] && echo "gleich" || echo "ungleich"
```

Funktion schreiben in Datei ~/.bashrc

```
sha256cmp() { hash1=$(sha256sum "$1" | cut -d' ' -f1) hash2=$(sha256sum "$2" | cut -d' ' -f1) [ "$hash1" = "$hash2" ] && echo "gleich" || echo "ungleich" }
```

Backup-Strategien

Backup-Strategien

3-2-1 Backup Regel

Großvater-Vater-Sohn

First in, First out (Fifo)

Backup-Strategien: 3-2-1 Backup Regel

Exemplare

Bewahre mindestens 3 Kopien Deiner Unternehmensdaten auf

Die goldene3-2-1-1-0Backup-Regel

Datensicherung auf 2 verschiedenen Medien Mindestens eine Kopie an einem externen Ort speichern

Backup-Strategien: Großvater-Vater-Sohn

TAG: Sohn

- Tägliche Sicherung (inkrementell/ differenziell)
- 4 bis 5 Bänder

WOCHE: Vater

- Am Ende jeder Woche
- Vollständiges Backup
- Löschung aller vorangegangenen Backups

MONAT: Großvater

- Nach 4 Wochen:

- Neues Vollständiges Backup
- Löschung der vier wöchentlichen Sicherungen

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Fifo

neue oder geänderte Dateien überschreiben die ältesten

Bsp: 14 Tage Backup

an Tag 15 wird Backup von Tag 1 überschrieben

Recovery Point Objective

Wie lange dürfen die neuesten Backups maximal zurückliegen?

Beispiel:

- RPO = 1 Tag : Wenn heute die Platte ausfällt, sind maximal Daten von gestern weg
- RPO = 1 Stunde : Wenn heute ein Fehler passiert, sind maximal die letzten 60 Minuten Arbeit weg
- RPO = 1 Woche : Datenverlust von bis zu 7 Tagen

RPO bestimmt, wie oft Backup gemacht wird

- RPO 1 Tag → täglich backupen
- RPO 1 Stunde → stündlich backupen
- RPO 1 Woche → wöchentlich backupen

Quellen

- Dokument: Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden
- ID: 136

Revision #2
Created 19 May 2026 15:40:12 by Admin
Updated 19 May 2026 15:53:52 by Admin