

CIA

Schutzziele der Datensicherheit

Schutzziel	Praktisches Beispiel	Passende Schutzmaßnahme
Vertraulichkeit	Eine Person ohne Berechtigung könnte Personalakten lesen.	Die Akten nur für die Personalabteilung per Berechtigung freigeben.
Integrität	Ein Rechnungsbetrag wird unbemerkt verändert.	Änderungen protokollieren und nur berechtigten Personen das Bearbeiten erlauben.
Verfügbarkeit	Der Dateiserver fällt aus und Mitarbeitende können nicht auf ihre Dokumente zugreifen.	Einen Ersatzserver bereitstellen, der bei einem Ausfall übernimmt.

Technische und organisatorische Maßnahmen (TOMs)

Maßnahme	Praktisches Beispiel: Was soll verhindert werden?	Eine passende Maßnahme
Zutrittskontrolle	Eine fremde Person betritt den Serverraum.	Serverraum mit einer elektronischen Schließanlage sichern.
Zugangskontrolle	Jemand meldet sich mit einem gestohlenen Passwort am Firmennetz an.	Anmeldung mit einem zweiten Faktor absichern.
Zugriffskontrolle	Ein Mitarbeiter ist angemeldet, liest aber Personalakten, die er für seine Arbeit nicht benötigt.	Leserechte nur der Personalabteilung zuweisen.
Weitergabekontrolle	Eine Datei mit Kundendaten wird während der Übertragung von Unbefugten mitgelesen.	Datei über eine verschlüsselte Verbindung übertragen.
Eingabekontrolle	Ein Datensatz wird geändert und später ist unklar, wer die Änderung vorgenommen hat.	Änderungen mit Benutzerkennung und Zeitpunkt protokollieren.
Auftragskontrolle	Ein externer Dienstleister nutzt Kundendaten für eigene Zwecke.	Die Verarbeitung durch einen Auftragsverarbeitungsvertrag und dokumentierte Weisungen festlegen.
Verfügbarkeitskontrolle	Nach einem Festplattenausfall fehlen wichtige Dateien.	Regelmäßige Backups erstellen und ihre Wiederherstellung testen.
Trennung von Daten	Daten verschiedener Kunden oder Verarbeitungszwecke werden vermischt.	Getrennte Datenbereiche mit passend eingerichteten Berechtigungen verwenden.

Merke: *Zutritt* betrifft Räume, *Zugang* die Anmeldung am System und *Zugriff* die Berechtigung auf bestimmte Daten. Verfügbarkeit bedeutet, dass Systeme wie vorgesehen nutzbar sind; eine

ausnahmslos jederzeitige Verfügbarkeit ist damit nicht gemeint.

CIA-Schutzziele - Beispiele für Server, Serverraum und Haus

Bereich	Schutzziel	Praktisches Beispiel	Schutzmaßnahme
Server	Vertraulichkeit	Unbefugte könnten Kundendaten auf dem Server lesen.	Zugriffsrechte auf berechnigte Benutzer beschränken.
Server	Integrität	Jemand verändert unbemerkt Einträge in einer Datenbank.	Änderungen protokollieren und Schreibrechte begrenzen.
Server	Verfügbarkeit	Eine defekte Festplatte legt den Serverdienst lahm.	Redundante Festplatten einsetzen.
Serverraum	Vertraulichkeit	Ein Besucher könnte an einem offenen Serverschrank Daten von Datenträgern entnehmen.	Serverschränke abschließen.
Serverraum	Integrität	Jemand steckt Netzkabel um und verändert dadurch die Verbindungen.	Zutritt zum Serverraum auf Berechnigte beschränken.
Serverraum	Verfügbarkeit	Die Klimaanlage fällt aus; Server überhitzen und schalten sich ab.	Temperatur überwachen und bei Überhitzung alarmieren.
Haus/Gebäude	Vertraulichkeit	Eine fremde Person betritt ein Büro und liest vertrauliche Unterlagen.	Gebäudezutritt mit Schlüsselkarten kontrollieren.
Haus/Gebäude	Integrität	Jemand verändert unbefugt die Einstellungen der zentralen Stromversorgung.	Technikräume abschließen.
Haus/Gebäude	Verfügbarkeit	Ein Stromausfall im Gebäude unterbricht sämtliche IT-Dienste.	Eine unterbrechungsfreie Stromversorgung (USV) einsetzen.

TOMs einfach erklärt

Maßnahme	Merksatz	Beispiel
Zutrittskontrolle	Wer darf in den Raum?	Nur Personen mit Schlüsselkarte kommen in den Serverraum.
Zugangskontrolle	Wer darf sich am System anmelden?	Ein Benutzer meldet sich mit Passwort und zweitem Faktor an.
Zugriffskontrolle	Welche Daten darf ein angemeldeter Benutzer sehen oder ändern?	Nur die Personalabteilung darf Gehaltsdaten öffnen.

Maßnahme	Merksatz	Beispiel
Weitergabekontrolle	Wie werden Daten bei der Übermittlung geschützt?	Kundendaten werden über eine verschlüsselte Verbindung versendet.
Eingabekontrolle	Wer hat welche Daten geändert?	Ein Protokoll zeigt, wer einen Datensatz wann bearbeitet hat.
Auftragskontrolle	Was darf ein externer Dienstleister mit den Daten tun?	Ein Cloud-Anbieter verarbeitet Kundendaten nur nach dokumentierten Weisungen.
Verfügbarkeitskontrolle	Sind die Daten bei Bedarf nutzbar?	Nach einem Festplattenausfall werden Daten aus einem Backup wiederhergestellt.
Trennung von Daten	Welche Daten müssen getrennt bleiben?	Kundendaten verschiedener Unternehmen liegen in getrennten Bereichen.

Die ersten drei sind besonders wichtig: Zutritt = ins Gebäude oder in den Raum. Zugang = ins IT-System. Zugriff = an bestimmte Daten.

TOM	IT-Beispiel	Maßnahme
Zutrittskontrolle	Jemand könnte einen Server im Serverraum direkt bedienen oder eine Festplatte mitnehmen.	Serverraum mit Schlüsselkarte sichern.
Zugangskontrolle	Jemand versucht, sich am NAS anzumelden.	Anmeldung mit Passwort und zweitem Faktor absichern.
Zugriffskontrolle	Ein angemeldeter Mitarbeiter versucht, den Ordner „Personal“ zu öffnen.	Ordnerberechtigung nur für die Personalabteilung vergeben.
Weitergabekontrolle	Eine Datei wird vom Laptop zum Firmenserver übertragen.	Übertragung per verschlüsseltem VPN schützen.
Eingabekontrolle	Ein Benutzer ändert einen Kundendatensatz in einer Anwendung.	Benutzer, Zeitpunkt und Änderung im Audit-Log protokollieren.
Auftragskontrolle	Ein externer Cloud-Anbieter speichert Kundendaten für die Firma.	Per Auftragsverarbeitungsvertrag und dokumentierten Weisungen festlegen, was er mit den Daten tun darf.
Verfügbarkeitskontrolle	Das NAS fällt aus und Dateien sind nicht mehr erreichbar.	Regelmäßige Backups erstellen und die Wiederherstellung testen.
Trennung von Daten	Eine Anwendung verwaltet Daten von Firma A und Firma B.	Daten beider Firmen in getrennten Bereichen mit eigenen Zugriffsrechten speichern.