Datensicherheit

Vorlesung 7: 26.01.2026

Wintersemester 2025/2026 h_da

Heiko Weber, Lehrbeauftragter

Teil 2: Datensicherheit
Themenübersicht der Vorlesung

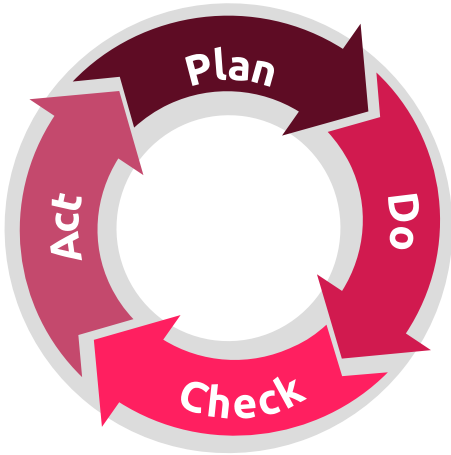
1. Einführung / Grundlagen / Authentifizierung & Autorisierung
2. Kryptografie / Verschlüsselung & Signaturen / Vertrauen / Blockchain
3. Softwaresicherheit / Schadsoftware
4. Evaluation / Netzwerksicherheit / TLS / PGP & S/MIME / Firewalls & Netzwerksegmentierung
5. Hacking / Phishing / Einführung in den Datenschutz / Anonymität / Darknet
6. Datenschutzgesetze / Technische & Organisatorische Maßnahmen
7. **Organisationssicherheit / Managementsysteme / Zusammenfassung**

Organisationssicherheit

- um die IT-Systeme einer Organisation den Bedürfnissen entsprechend zu schützen, muss eine systematische Vorgehensweise entwickelt werden, um
  - Sicherheitsmaßnahmen umzusetzen, die dem Bedarf der Organisation entsprechen
  - IT-Systeme auf den neuesten Sicherheitsstand zu halten (Updates + Patches einspielen)
  - IT-Systeme auf Bedrohungen zu überwachen
  - Personen für das Thema Sicherheit zu sensibilisieren
  - die Effektivität der umgesetzten Maßnahmen zu kontrollieren
  - neue Maßnahmen einzuführen, wenn neue Risiken identifiziert werden

> Informations-Sicherheits-Management-System (ISMS)

Informations-Sicherheits-Management-System (ISMS)



Standards:

- ISO/IEC 27001 (international)
- BSI IT-Grundschutz (speziell für Behörden und Organisationen in Deutschland)
- NIST SP 800-53 (speziell für Behörden in USA)
- TISAX (speziell für Automobil-Zulieferer)

Informationssicherheits-Risiko-Management

- **Risiko-Identifizierung**
  - um Informationssicherheits-Risiken zu managen, müssen Prozesse zur Identifizierung relevanter Risiken eingerichtet werden
  - gängige Methoden: Bedrohungsmodellierung, Bestandsanalyse, Audits, Expertenbefragungen, ...
- **Risiko-Bewertung**
  - die identifizierten Risiken müssen bewertet werden, um den Risikograd zu bestimmen
  - in der Regel wird das Risiko als Wahrscheinlichkeit des Auftretens und als Auswirkung des Auftretens ausgedrückt (PI Score / Probability-Impact Score)
  - die Risikobewertung umfasst auch die Bewertung der Wirksamkeit der eingeführten Maßnahmen zur Risikominderung und die Bestimmung des Restrisikos, das nach vollständiger Umsetzung der Maßnahmen verbleibt
- **Risiko-Behandlung**
  - nachdem das Risiko bewertet wurde, muss entschieden werden, wie mit dem Risiko umgegangen werden soll
  - übliche Behandlungsoptionen: Reduzierung, Vermeidung, Teilung, Akzeptanz

Informationssicherheits-Vorfall-Management

- auch die besten Schutzmaßnahmen können keinen 100% Schutz bieten
- wenn es zu einem Datenschutz- oder Informationssicherheits-Vorfall kommt, müssen klare Prozesse existieren, wie damit umgegangen wird

- Melde-Wege müssen festgelegt sein
- Verantwortlichkeiten müssen klar geregelt sein (wer kümmert sich um was, wenn es zu einer Datenpanne gekommen ist)
- Kommunikationsprozesse müssen klar geregelt sein
  - zum Beispiel zum Verantwortlichen, zur Datenschutzaufsichtsbehörde und zu den Betroffenen im Rahmen von Datenschutzvorfällen

Datenschutz-Management-System (DMS)

- DSGVO macht es zwingend erforderlich systematische Datenschutz-Maßnahmen zu verwalten
- Datenschutz-Management-System soll sicherstellen, dass Rollen- und Verantwortlichkeiten klar geregelt sind und die erforderlichen Datenschutz-Maßnahmen dokumentiert und kontrolliert werden
  - Dokumentierte Prozesse (z. B. für Wahrung der Betroffenenrechte)
  - Verzeichnis von Verarbeitungstätigkeiten
  - Datenschutz-Audits
  - Risikobewertung, Datenschutzfolgeabschätzung, Transfer Impact Assessment, …
- Standards:
  - ISO/IEC 27701
  - NIST Privacy Framework

Anforderungen für weitere Daten-Management-Systeme

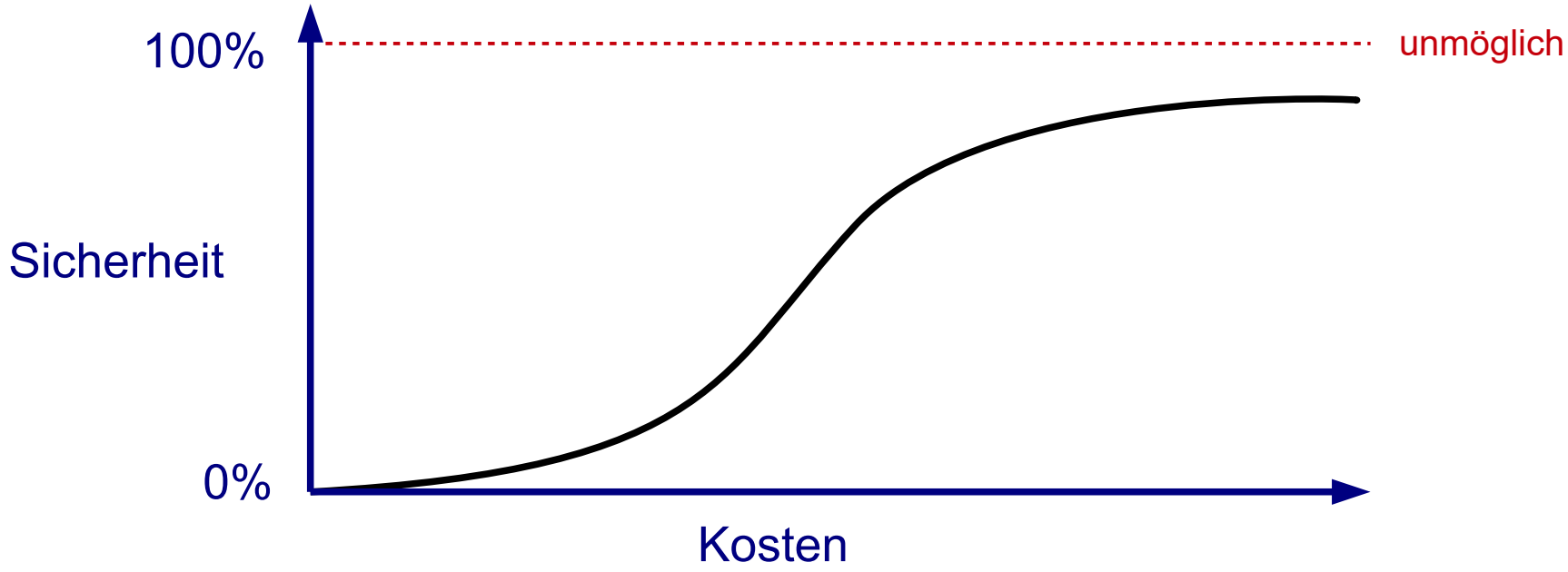
- neue Technologien und regulatorische Anforderungen erfordern, dass die bestehenden Management-Systeme erweitert werden oder ggf. weitere eingeführt werden
- neue EU-Gesetze, die das erforderlich machen sind z.B.
  - NIS2-Richtlinie (mit nationalen Umsetzungs-Gesetzen)
  - AI Act
  - Data Act
  - Cyber Resilience Act

Datensicherheit

Zusammenfassung der wichtigsten Themen

Wie sicher können IT-Systeme sein?

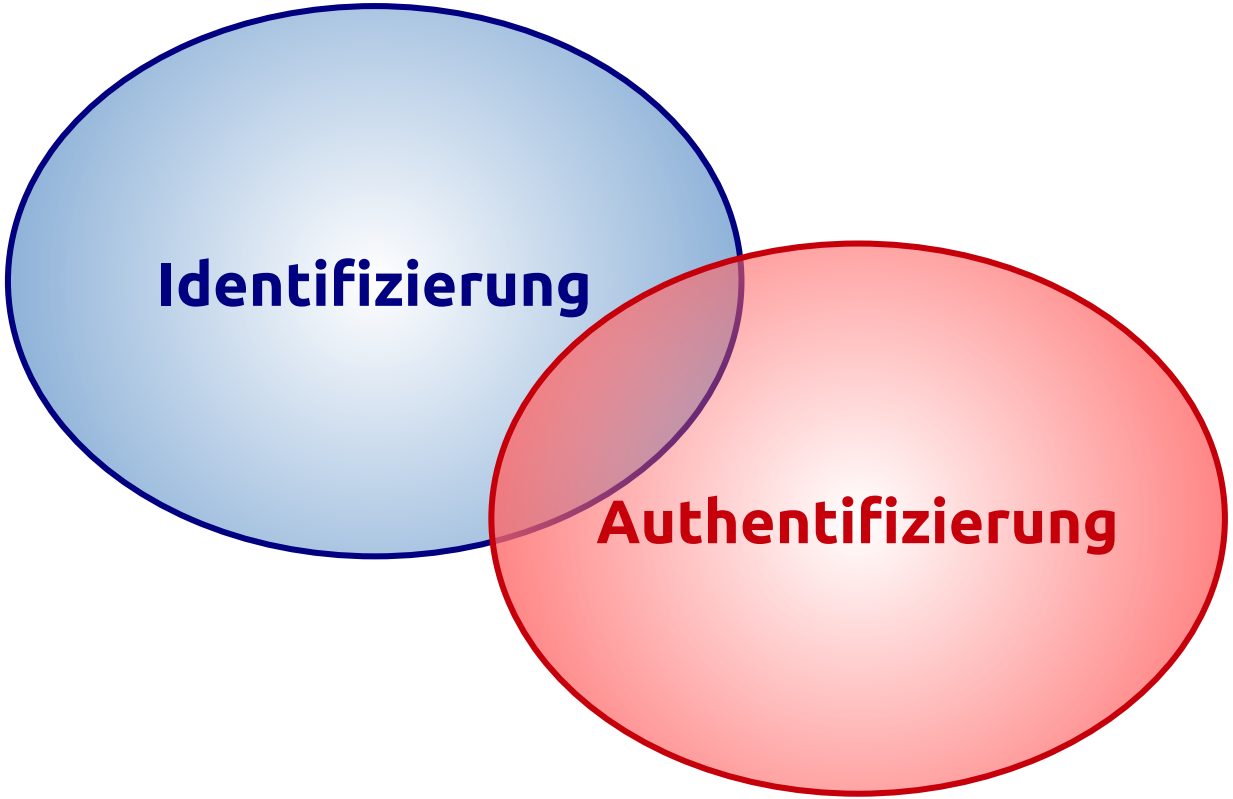
- 100% Sicherheit ist unmöglich
- Sicherheit ist immer eine Abwägung zwischen Risiken und Aufwand bzw. Benutzbarkeit



Schutzziele der Datensicherheit

Vertraulichkeit		Daten dürfen nur von Berechtigten **gelesen** werden
Verfügbarkeit		Daten müssen für Berechtigte **zugänglich** sein
Integrität		Daten dürfen nur von Berechtigten **erstellt**, **verändert** und **gelöscht** werden
Authentizität		Daten sind vom **angegebenem Ursprung**
Nichtabstreitbarkeit		Inhalte von Daten sind so **beabsichtigt**, wie angegeben

Methoden zur Identifizierung und Authentifizierung



Häufige Probleme bei Passwörtern

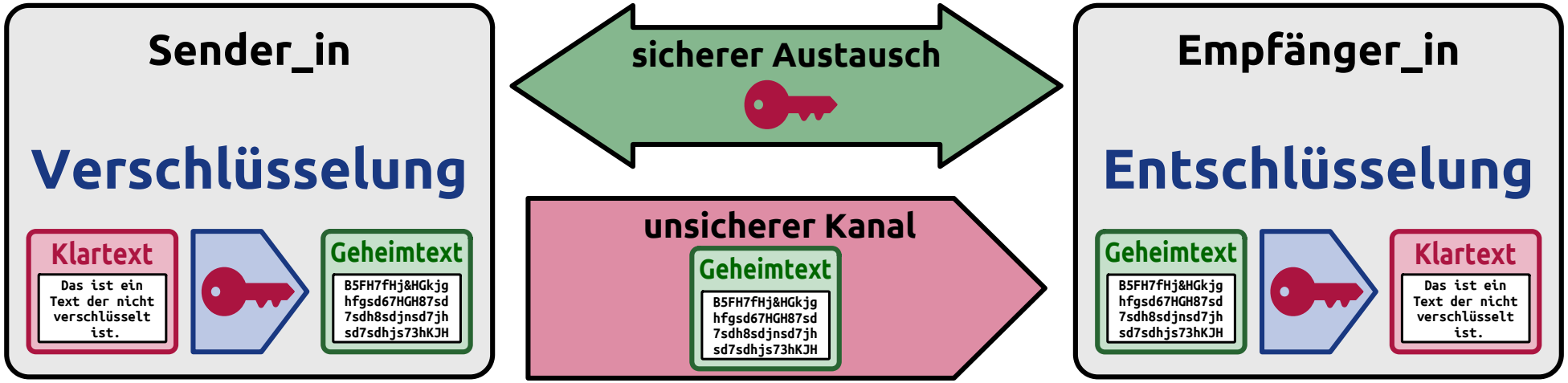
- schwache Passwortregeln
- schlechte Passworterneuerungsverfahren
- schlechter Schutz gegen Brute-Force-Angriffe
- unveränderbare Passwörter
- unsichere Speicherung der Passwörter
- unsicherer Transport der Passwörter

Sichere Passwörter

- leicht für einen Menschen zu merken
- schwer für eine angreifende Person zu raten
- möglichst lang

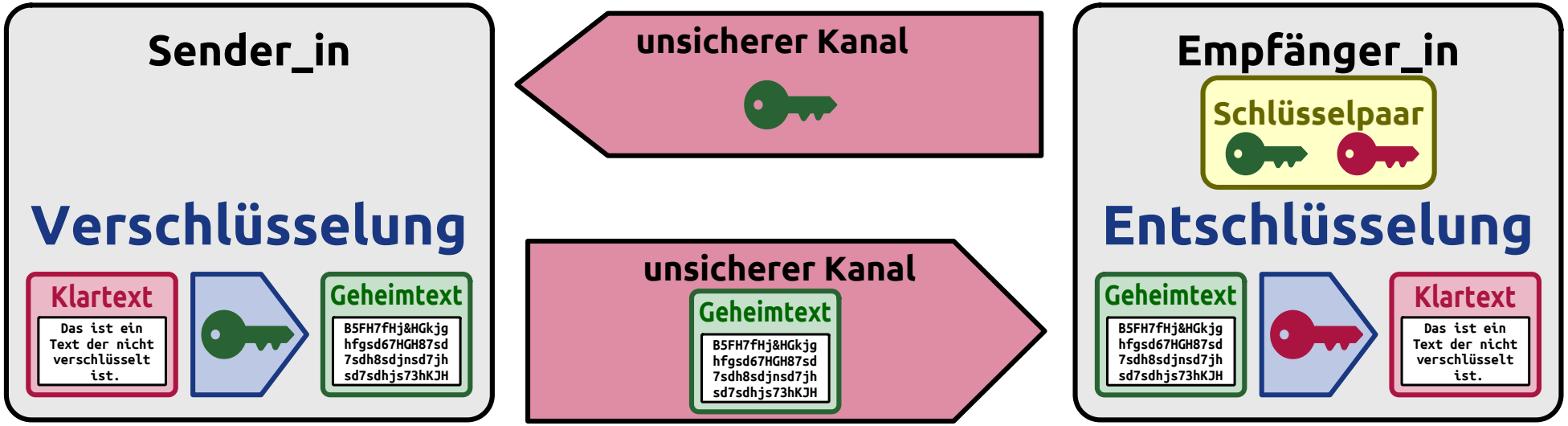
- schwer zu merken und leicht für einen Computer zu erraten:
  `g7X4D3b5`
- leicht zu merken und schwer für einen Computer zu erraten:
  `montagsHOLEichMIReineLAUGENBRETZELamBAHNHOF_:-)`

Symmetrische Verschlüsselung



1. über eine sichere Methode wird der geheime Schlüssel ausgetauscht
2. mit dem geheimen Schlüssel wird verschlüsselt
3. über den unsicheren Kanal wird der Geheimtext verschickt
4. mit dem gleichen geheimen Schlüssel wird entschlüsselt

Asymmetrische Verschlüsselung (Public Key)



1. Empfänger_in hat ein Schlüsselpaar (öffentlicher und privater Schlüssel)
2. über einen unsicheren Kanal wird der öffentliche Schlüssel publik gemacht
3. mit dem öffentlichen Schlüssel wird verschlüsselt
4. über den unsicheren Kanal wird der Geheimtext verschickt
5. mit dem geheimen Schlüssel wird entschlüsselt

Hybride Verschlüsselungsverfahren

- asymmetrische Verschlüsselungsverfahren sind wesentlich langsamer als symmetrische
- **Ziel**
  - Vorteile von symmetrischer und asymmetrischer Verschlüsselung kombinieren
- **hybrider Ansatz**
  - symmetrischer Schlüssel mit asymmetrischem Verfahren verschlüsselt
  - Daten mit symmetrischen Verfahren verschlüsselt
- wird zum Beispiel bei PGP und S/MIME für E-Mail-Verschlüsselung verwendet

Asymmetrische Verschlüsselung (Public Key)

Schlüsselpaar

Öffentlicher Schlüssel

Privater Schlüssel

Verschlüsselung mit öffentlichem Schlüssel
Entschlüsselung mit privatem Schlüssel

FOLGENDES GEHT AUCH!
Verschlüsselung mit privatem Schlüssel
Entschlüsselung mit öffentlichem Schlüssel

Prinzip hinter Digitalen Signaturen

Schutzziele der Datensicherheit – Technische Maßnahmen

Terminologie

- **Schwachstelle** (Weakness)
  ein Software-Fehlertyp, der in gewissen Situationen zu einer Verwundbarkeit der Software führen kann

- **Verwundbarkeit** (Vulnerability)
  das Auftreten einer oder mehrerer Schwachstellen in einer Software, in der diese Schwachstelle genutzt werden kann, um ein Fehlverhalten hervorzurufen

- **Offenlegung** (Exposure)
  das Auftreten einer oder mehrerer Schwachstellen in einer Software, die Informationen oder Funktionen offenlegen, die einen Angriff auf ein System erleichtern

- **Auswirkung** (Impact)
  das Ergebnis, welches eine erfolgreich ausgenutzte Verwundbarkeit in einer Software haben kann

Anwendungs-Eingabe und -Ausgabe

Welche Software ist sicher und welche ist unsicher?

Eigentlich gibt es nur Software, von der bekannt ist, dass sie unsicher ist und solche, von der noch nicht bekannt ist, ob sie unsicher ist.

D.h. es gibt Software, von der aus Erfahrung gesagt werden kann, dass sie laut den bisher bekannten Informationen relativ sicher ist. Absolut sichere Software gibt es nicht.

Viren

- selbstreproduzierend
- keine eigenständige Software – benötigen einen Wirt (beispielsweise eine übliche Anwendungssoftware)
- Wirtssoftware muss ausgeführt werden zum Aktivieren des Virus
- Funktionsweise:
  1. Start des infizierten Programms (Wirtssoftware): Aktivierung des Virus
  2. Virus infiziert selbständig andere Programme
  3. Virus aktiviert Schadensfunktion

Würmer

- spezielle Art von Viren
- selbstreproduzierend
- selbstständige Software – kein Wirt benötigt
- Verbreitung: aktiv
  z. B. durch Versenden von E-Mails an Mitglieder der Adressliste oder automatischem Zugriff auf weitere System über Netzwerkverbindungen
- muss ausgeführt werden zum Aktivieren des Wurms

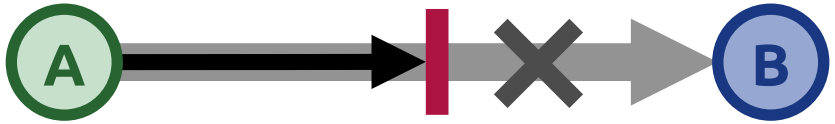
Trojanische Pferde

- auch teilweise als „Trojaner“ bezeichnet (wobei es ja eigentlich eher „Griechen“ heißen müsste – das Pferd enthielt ja Griechen, die die Trojaner angegriffen haben)
- Schadsoftware, die vom Benutzer unbemerkt Aktionen auf dessen Computer ausführt - zu diesen Aktionen gehören u. a.:
  - Löschen von Daten
  - Sperren von Daten
  - Modifizieren von Daten
  - Auslesen/Kopieren von Daten
  - Beeinträchtigen der Funktionalität von Computern oder Computernetzwerken

Denial of Service (DoS)

- Unterbrechung der Netzwerkverbindung
- Schutzziel **Verfügbarkeit** verletzt

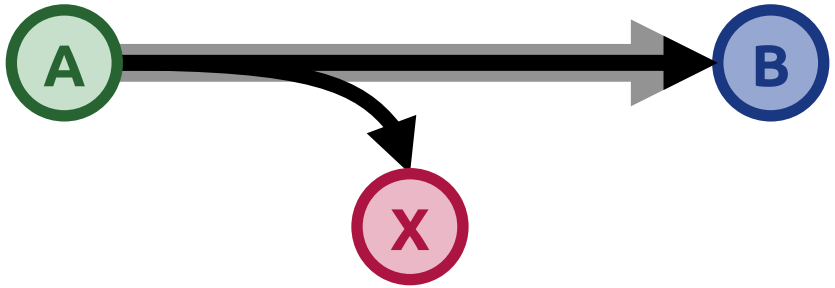
- Knoten A kann mit Knoten B nicht mehr kommunizieren



Sniffing

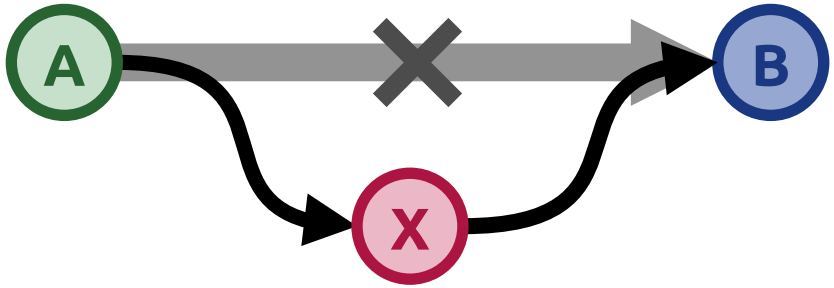
- Abhören
- Schutzziel **Vertraulichkeit** verletzt

- Daten die von Knoten A zu Knoten B gesendet werden, hört der Angreifer X mit



Man in the Middle (MitM)

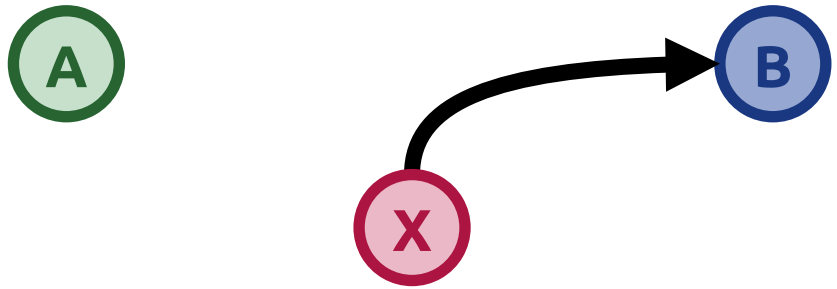
- Abfangen und Modifizieren
- Daten die von Knoten A zu Knoten B gesendet werden, fängt der Angreifer X ab, verändert sie und schickt sie an den Knoten B weiter (meistens so, dass Knoten B denkt, dass die Daten von Knoten A kommen)
- Schutzziel **Integrität** verletzt – zusätzlich Vertraulichkeit und Authentizität verletzt



Spoofing

- Erzeugen
- Schutzziel **Authentizität** verletzt

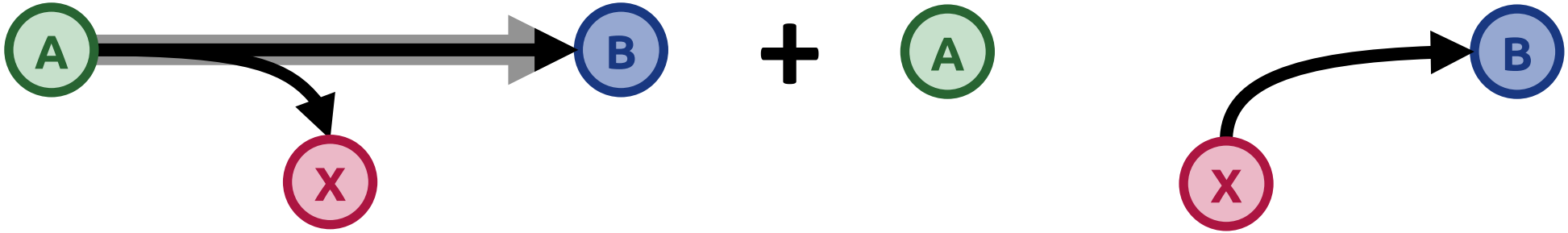
- Angreifer X schickt Daten an Knoten B und täuscht vor, dass die Daten von Knoten A kommen würden



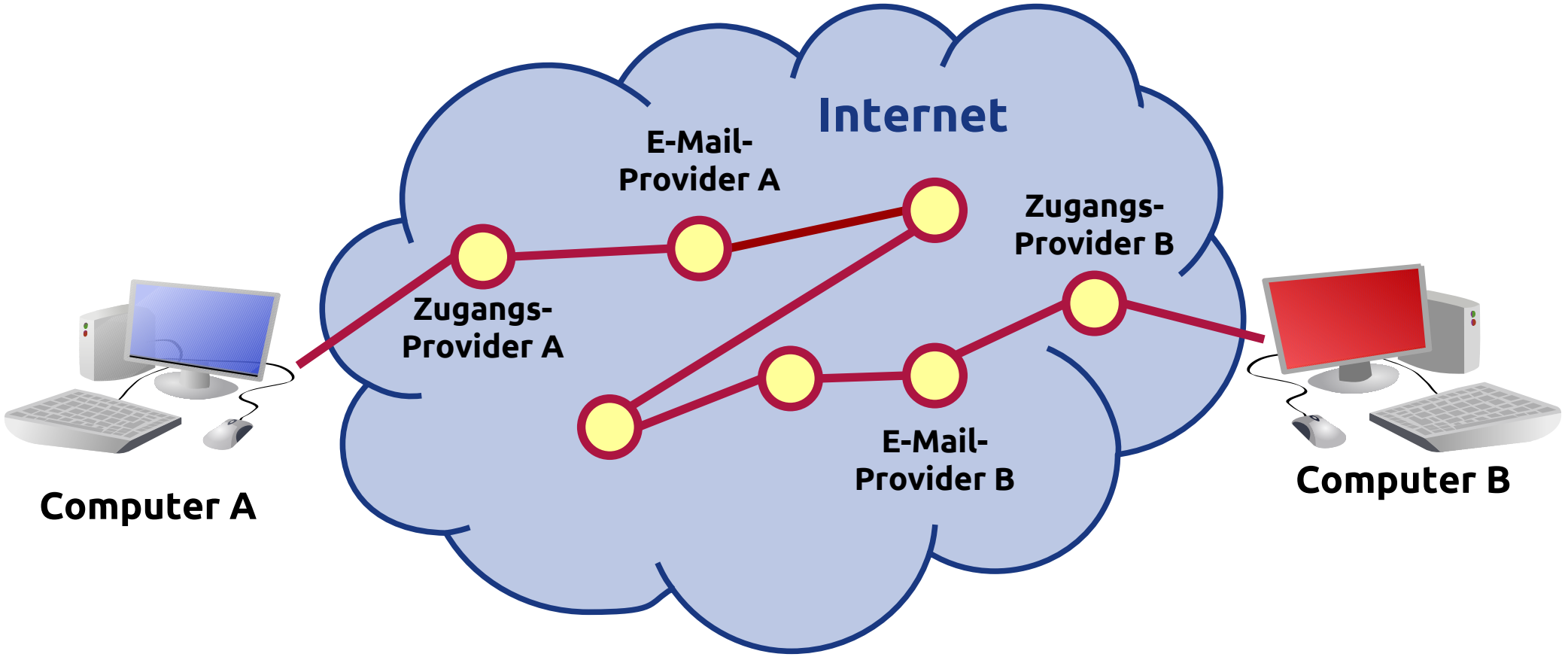
Replay

- Datenmithören und erneut senden
- Schutzziel **Authentizität** verletzt

- Daten die von Knoten A zu Knoten B gesendet werden, hört der Angreifer X mit und sendet sie zu einem späteren Zeitpunkt erneut



Computer-Kommunikation für E-Mails



Was ist Phishing?

- **Angriff auf das Sicherheitsbewusstsein von Menschen** und nicht auf die Sicherheit von IT-Systemen.

  Annahme: Menschen machen Fehler und sind leichter zu überlisten, als technische Sicherheitssysteme.

- Nutzt **Social-Engineering-Maßnahmen zur Manipulation von Menschen**, mit dem Ziel, dass sie sensible Informationen preisgeben oder falsche Aktionen tätigen in dem Glauben, dass sie korrekt seien.
- **Vertrauen aufbauen** oder eine vertrauenswürdige Instanz simulieren und dann die Informationen abgreifen oder Anweisung geben.

Schutzziele für Datenschutz

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Nichtabstreitbarkeit
- Transparenz
- Intervenierbarkeit

Art. 32 Abs. 1 DSGVO: Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Grundsätze für die Verarbeitung personenbezogener Daten

- Rechtmäßigkeit
- Fairness und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- **Vertraulichkeit, Integrität, Verfügbarkeit**
- Rechenschaftspflicht

TOMs gemäß DSGVO

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Zutrittskontrolle zu Verarbeitungsbereichen
- Zugangskontrolle zu Datenverarbeitungssystemen
- Zugriffskontrolle auf besondere Bereiche von Datenverarbeitungssystemen
- Trennung der Verarbeitung für unterschiedliche Zwecke
- Pseudonymisierung
- Verschlüsselung

Integrität (Art. 32 Abs. 1 lit. b DSGVO)
- Eingabekontrolle
- Weitergabekontrolle

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)
- Verfügbarkeitskontrolle
- Belastbarkeit

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs und organisatorische Maßnahmen zur Gewährleistung der Sicherheit (Art. 32 Abs. 1 lit. d DSGVO)
- Datenschutz-Management
- Incident-Response-Management
- Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle

Privacy by Default

(Datenschutz durch datenschutzfreundliche Voreinstellungen)

Artikel 25 Abs. 2 DSGVO:

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.