Datensicherheit

Vorlesung 5: 12.01.2026

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

Hacken / Hacker

- die Begriffe „Hacken“ und „Hacker“ werden vielseitig eingesetzt – grundsätzlich bedeutet „Hacken“ das Ausprobieren verschiedener Lösungsansätze, bis eine passende Lösung gefunden wurde
- im Kontext von Datensicherheit bezeichnet „Hacken“ das Suchen nach Sicherheitslöchern in IT-Systemen
- ein „Hacker“ kann dabei eine Person sein, die im Auftrag eines Systembetreibers nach Sicherheitslöchern sucht (wird dann als „White-Hat“ bezeichnet) oder jemand, der/die mit kriminellem Hintergrund nach Sicherheitslöchern sucht („Black-Hat“)
- die Hacker-Aktivitäten von White-Hats werden meist auch als „Penetration Tests“ bezeichnet

Vorgehensweisen beim Hacking

- normalerweise ist das System, welches untersucht wird, eine „Black-Box“, also ein System, über das erst einmal nichts oder nur wenig bekannt ist
- als erstes wird versucht, möglichst viel über die Beschaffenheit des Systems in Erfahrung zu bringen – also z.B. welche Ports benutzt werden, welche Protokolle unterstützt werden, welche Software auf dem System installiert ist (Betriebssystem, Datenbanken, E-Mail-Server, Web-Server, ...), ...
- diese Basisinformationen werden dann genutzt, um nach bekannten Schwachstellen zu suchen – wenn solche Suchen nicht erfolgreich sind, werden verschiedene Tools eingesetzt, um gängige Probleme nacheinander auszuprobieren
- nachdem verschiedene kleiner Sicherheitslücken aufgedeckt wurden, wird versucht, diese so zu kombinieren, damit gravierendere Lücken aufgedeckt werden – dieses schrittweise Herantasten an die gravierenden Probleme, ist das eigentliche „Hacken“

Hacker-Tools

Hacken erfordert einiges an Erfahrung mit allgemeinen Programmier- und Netzwerktechniken – diverse Tools existieren, um die Arbeit zu erleichtern

- **Port-Scanner**
  - schickt Anfragen an alle Ports auf einem System und versucht zu ermitteln, welche Dienste dort laufen (z. B. https://pentest-tools.com/network-vulnerability-scanning/port-scanner-online-nmap)
- **HTTP-Client**
  - da viele Schwachstellen über die Webschnittstelle gefunden werden können, wird oft mit einem normalen Web-Browser oder einem HTTP-Proxy (z. B. *BURP*) gesucht
- **Dynamische Anwendungs-Scanner**
  - schicken gängige Angriffsmuster an eine Anwendung und bestimmen anhand der Antworten, ob eine Anwendung anfällig ist (z. B. *Nessus*)
- **weitere spezielle Programme**
  - viele weitere Tools existieren, um z. B. nach speziellen Blind-SQL-Injection-Schwachstellen zu suchen – oft müssen auch kleine Hilfsprogramm selber programmiert werden...

Hacken von Technischen Schwachstellen

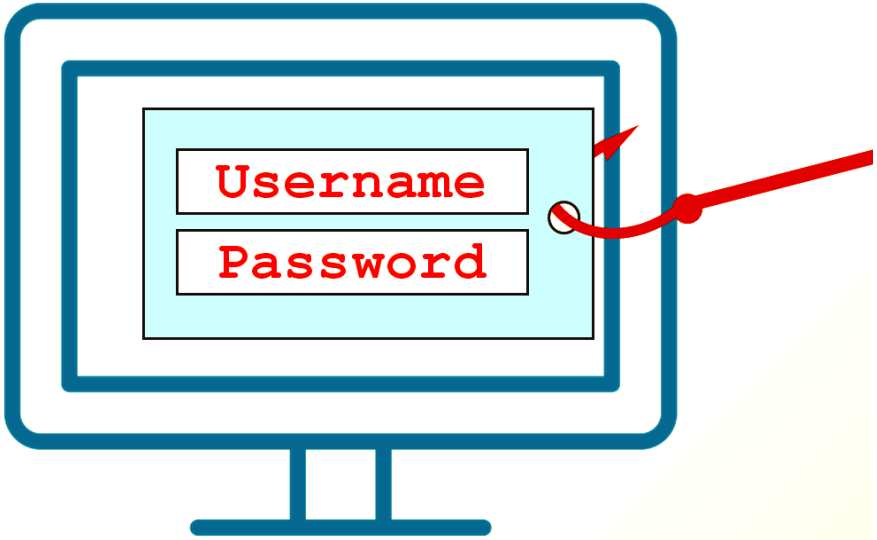
Das Hacken hat oft einen Fokus auf die technischen Schwachstellen:

- Fehler in der Software > Programmierfehler
- Fehler in der Hardware
- Architekturfehler > fehlende oder falsch konzipierte Funktionen
- Konfigurationsfehler in der Software oder Hardware

- **Problem (aus Sicht der Hacker):** Sichere Software-Entwicklungs-Methoden (Security by Design) führen dazu, dass Software-Lösungen immer weniger offensichtliche Schwachstellen haben.
- **Lösung: organisatorische Schwachstellen finden > Menschen angreifen**

Phishing

- Wortursprung: Password + Fishing
- Angeln nach Passwörtern und weiteren sensiblen Informationen im Internet.



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.

Vertrauen aufbauen

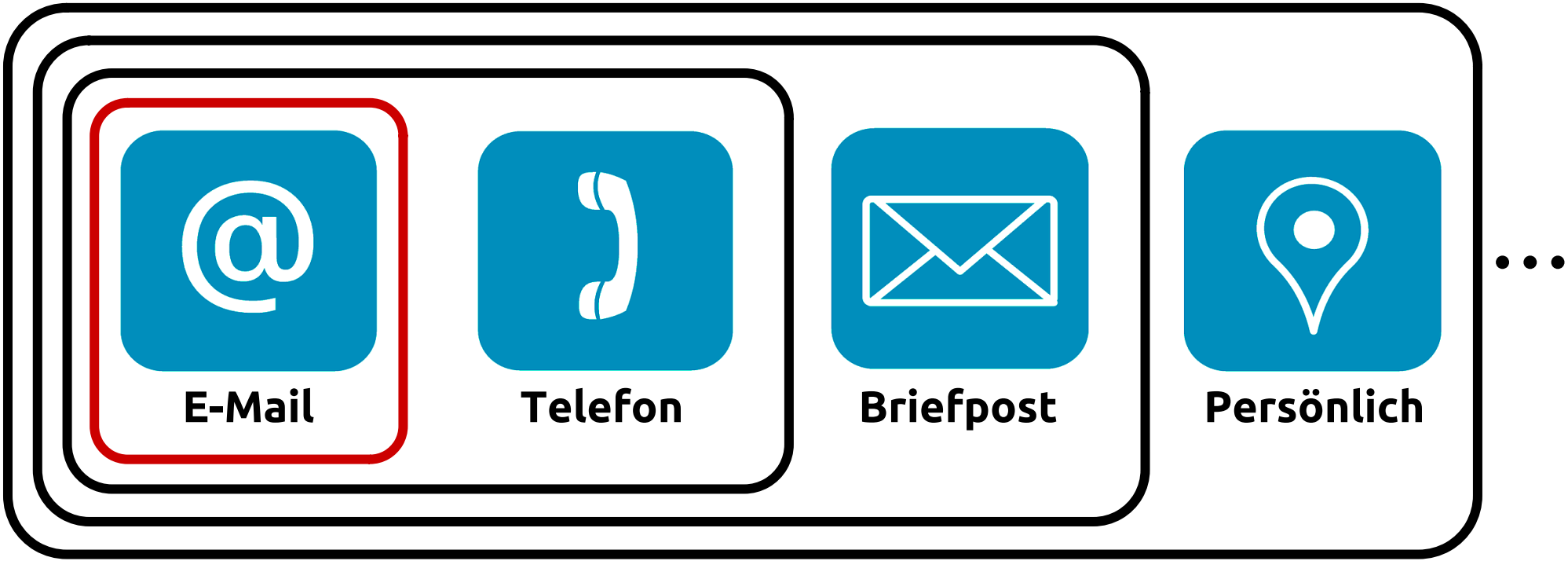
Vertrauenswürdige Instanz simulieren:

- bekannter Dienstleister (Bank/Bezahldienst, Paketdienst, Online-Shop, Social Media, …)
- Kollege / Vorgesetzter
- Kunde / Lieferant
- Behörde

Gezielt die Person ansprechen:

- persönliche Ansprache
- gezielt auf Lebensumstände eingehen (Position/Aufgabe im Unternehmen, Hobbies, familiäre Umstände, etc.)
- regionale und zeitliche Umstände berücksichtigen

Kommunikationskanäle für Phishing-Angriffe



Kombination mehrerer Kanäle auch möglich...

Phishing-Methoden

- direkte Preisgabe von Informationen
  - z. B. direkte Frage nach Informationen
- indirekte Preisgabe von Informationen
  - z. B. Vortäuschen einer vertrauenswürdigen Webseite, zum Abgreifen der Informationen
- Befolgen von Anweisungen
  - z. B. Überweisung von Geld oder Anpassung einer Kontoverbindung
- Installation von Software, die dann die Informationen ausspioniert
  - z. B. Link auf und Anhang mit Malware
- weitere Varianten…

Spear-Phishing

- Allgemeines Phishing versucht durch Angriffe, gerichtet an eine große Masse, ein paar Personen zu finden, die darauf reinfallen.
- Spear-Phishing ist ein Phishing-Angriff, der speziell auf eine gezielte Person ausgerichtet ist.
- Es werden möglichst viele Informationen über eine Person und deren Umfeld gesammelt – z. B. über Social Media – und diese Informationen werden dann genutzt, um einen sehr gezielten Angriff zu bauen.
- Diese Angriffe sind sehr zeitaufwändig, sind aber schwerer zu erkennen und somit effektiver.
- Beispiel: CEO-Fraud

Phishing-Angriffe erkennen und/oder verhindern

neben den technischen Maßnahmen, die Phishing-Angriffe erkennen und blockieren sollen, sind weitere organisatorische Maßnahmen wichtig:

- Mailinhalt analysieren
- E-Mail-Absender / -Empfänger überprüfen
- Links / URIs überprüfen
- E-Mail-Anhängen misstrauen
- über zusätzlichen Kanal die Anweisung bestätigen lassen

Phishing-Angriffe erkennen und/oder verhindern:

Mailinhalte analysieren

- Passt der Kontext der E-Mail?
- Ist der Inhalte zu gut, um wahr zu sein?
- Werde ich zu etwas aufgefordert, was ungewöhnlich ist?
- Misstrauisch sein und Fragen oder Anweisungen hinterfragen!

Phishing-Angriffe erkennen und/oder verhindern:

E-Mail-Absender / -Empfänger überprüfen

- Ist der Absender bekannt?
- Ist die E-Mail-Adresse authentisch?

  `Frank Müller <262378236@gmail.com>`
  `Informationsrecht <irecht@h-d-a.de>`

- Geht die Antwort an eine andere Adresse, als der Absender?

  `From: Informationsrecht <irecht@h-da.de>`
  `Reply To: Informationsrecht <irecht-hda@gmx.net>`

Phishing-Angriffe erkennen und/oder verhindern:

Links / URIs überprüfen

- Ist die angezeigte URI wirklich die URI, auf die verwiesen wird?
- Verweist die E-Mail zur passenden Webseite?

Phishing-Angriffe erkennen und/oder verhindern:

E-Mail-Anhängen misstrauen

- E-Mail-Anhänge können Malware enthalten.
- Das gilt nicht nur für ausführbare Programme, auch für gewisse Dokumente.
- Alle Dokumente mit Makro- oder Skript-Funktionen sind gefährlich:
  - Word-Dokumente
  - Excel-Dokumente
  - PDF-Dokumente
- E-Mail-Anhänge von unbekannten Absendern sollten niemals geöffnet werden!

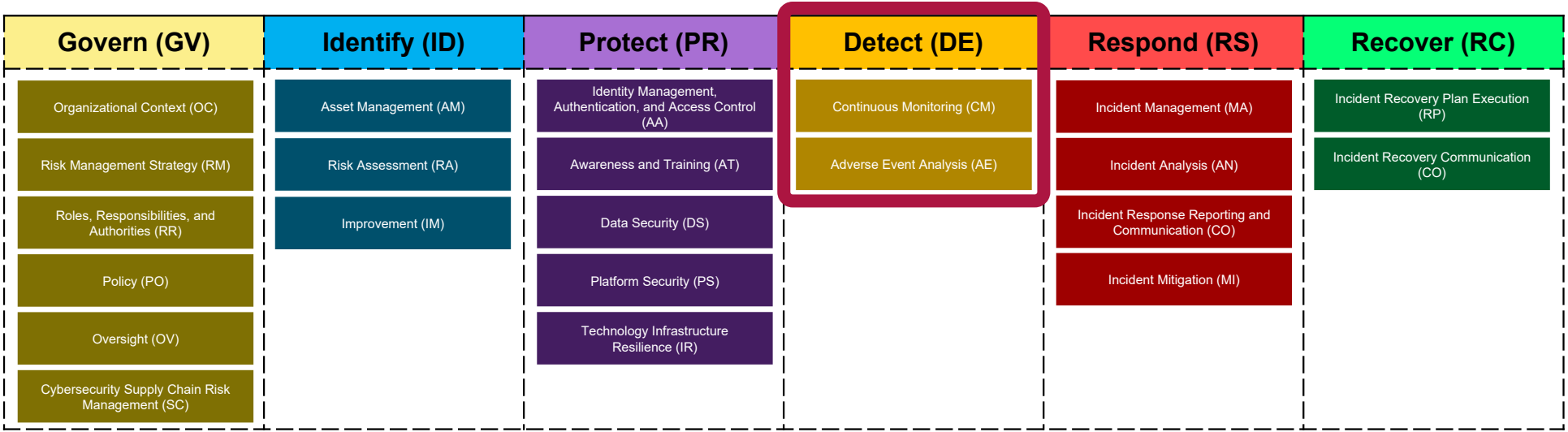
Phishing-Angriffe erkennen und/oder verhindern:

Über zusätzlichen Kanal die Anweisung bestätigen lassen

- Wenn eine sehr sensible Anfrage oder Anweisung von einem Absender kommt, dessen Authentizität nicht eindeutig bestimmt werden kann, sollte sie über einen zweiten Kommunikationskanal bestätigt werden.
- Beispiel:
  - Eine Anweisung kommt per E-Mail.
  - Den Anweisenden per Telefon anrufen und die Anweisung bestätigen lassen.

Erkennung von Hacker-Angriffen

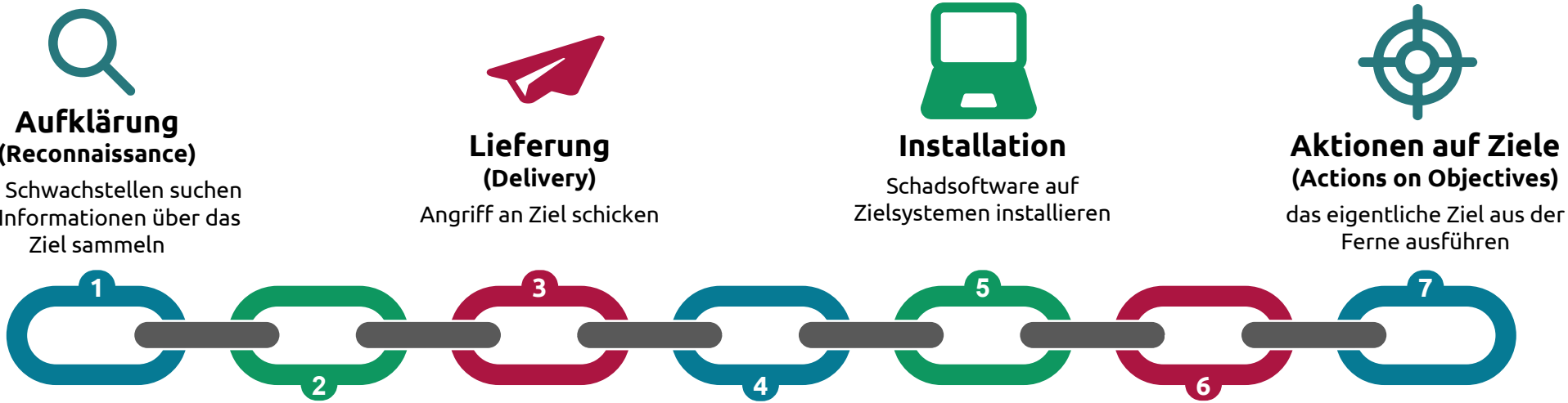
- Da es immer irgendwo in einer Organisation Systeme geben wird, die Schwachstellen oder Verwundbarkeiten aufweisen, wird es nie möglich sein, sich zu 100 % gegen erfolgreiche Angriffe zu schützen, selbst wenn der Faktor Mensch nicht beteiligt ist.
- Daher ist ein wichtiger Teil eines Cybersicherheitsprogramms die Erkennung von Hacker-Aktivitäten, was auch eine Funktion des NIST Cyber Security Framework (CSF) ist.



Indicator of Compromise (IoC)

- Ereignis oder Ereignisse, die in einem Netzwerk oder einem mit einem Netzwerk verbundenen Computersystem beobachtet werden und mit hoher Wahrscheinlichkeit auf ein bösartiges Eindringen oder auf Vorbereitungsaktivitäten für einen Angriff hinweisen
- typische IoCs:
  - ungewöhnlicher Datenverkehr, der in das und aus dem Netzwerk geht
  - unbekannte Dateien, Anwendungen und Prozesse in einem System
  - verdächtige Aktivitäten in (privilegierten) Konten
  - ungewöhnliche Aktivitäten wie Datenverkehr in Ländern, mit denen ein Unternehmen keine Geschäfte macht
  - seltsame Anmeldungen, Zugriffe und andere Netzwerkaktivitäten, die auf Sondierungs- oder Brute-Force-Angriffe hindeuten

Cyber Kill Chain



Aufklärung
(Reconnaissance)
nach Schwachstellen suchen und Informationen über das Ziel sammeln

Lieferung
(Delivery)
Angriff an Ziel schicken

Installation
Schadsoftware auf Zielsystemen installieren

Aktionen auf Ziele
(Actions on Objectives)
das eigentliche Ziel aus der Ferne ausführen

Bewaffnung
(Weaponization)
Angriff erstellen

Ausnutzung
(Exploit)
Angriff ausführen

```
0101010101010
1011110101010
0001010101010
```

Befehlen & Kontrollieren
(Command & Control)
Kommunikationskanal zum Kontrollieren der Zielsysteme aus der Ferne erstellen

Detektions- und Reaktionslösungen

- **Endpoint Detection and Response (EDR)**
  - überwacht kontinuierlich die Endpunkten (Clients und Server) auf verdächtige Aktivitäten
  - sammelt, korreliert und analysiert Daten von den Endpunkten
  - generiert nach Prioritäten geordnete Warnungen
  - kann in einigen Fällen automatisch auf IoCs reagieren, um eine Bedrohung einzudämmen und zu beseitigen, bevor sie sich ausbreiten kann (z. B. Isolierung des Endpunkts vom Netzwerk)
- **Network Detection and Response (NDR)**
  - gleiche Funktionalität wie EDR, aber Überwachung der Netzwerkkommunikation (Verkehrsflüsse und Daten)

- Beide bieten eine Kombination von Funktionen, die auch als Intrusion Detection System (IDS) und Intrusion Prevention System (IPS) bezeichnet werden.

Security Information and Event Management (SIEM)

- Sammeln von Ereignissen aus verschiedenen Quellen im gesamten Unternehmen (bzw. Netzwerk) und Erstellen von aggregierten Triggern für diese Ereignisse
- typischerweise kombiniert mit einer Datenbank, um die Ereignisse über einen längeren Zeitraum zu speichern und zu analysieren

- Vorteile des Betriebs eines SIEM:
  - potenzielle Bedrohungen in einer einzigen Ansicht
  - Erkennung von und Reaktion auf Bedrohungen in Echtzeit
  - transparente Überwachung von Benutzern, Anwendungen und Geräten

Datenschutz?

personenbezogene Daten

spezielle Daten

= Daten schützen

technische & organisatorische Maßnahmen

spezielle Sicherheitsmaßnahmen

= Datensicherheit

Verfahren, die personenbezogene Daten verarbeiten

Verfahren, die spezielle Daten verarbeiten

= IT-Sicherheit

Datenschutz

- grob gesehen ist Datenschutz:
  - Schutz vor missbräuchlicher Verarbeitung personenbezogener Daten
  - Schutz des Rechts auf informationelle Selbstbestimmung
  - Schutz des Persönlichkeitsrechts bei der Datenverarbeitung
  - Schutz der Privatsphäre
- das Recht eines Individuums, selbst zu entscheiden, welche personenbezogenen Daten von Externen einsehbar sind und benutzt werden dürfen
- in Zeiten der zunehmenden Datenverarbeitung durch Computersysteme, wird es immer schwerer, dieses Recht einzufordern und die Umsetzung zu überprüfen
- zudem werden die meisten Menschen immer unsensibler und geben ihre personenbezogenen Daten oft freiwillig preis, ohne zu wissen, was damit passiert
- technischer Datenschutz ist ein Teil der Datensicherheit

Was macht personenbezogene Daten so schutzwürdig?

„Recht auf informationelle Selbstbestimmung“

Allgemeines Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG + Art. 1 Abs. 1 GG

Art. 8 der EU-Grundrechte-Charta:

„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“

Was sind personenbezogene Daten?

Artikel 4 Satz 1 Nr. 1 DSGVO:

„personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Beispiele für personenbezogene Daten

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Rollen, Titel, Tätigkeitsbeschreibung
- Kontonummer, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalnr., Personalausweisnr., Sozialversicherungsnr.
- Werturteile wie zum Beispiel Zeugnisse
- IP-Adressen von Endgeräten

Grundsätze für die Verarbeitung personenbezogener Daten

Wahrung der Betroffenenrechte

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

Bisherige Schutzziele für Datensicherheit

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Nichtabstreitbarkeit

Genügen diese Schutzziele auch für den Datenschutz?

Wie werden die Rechte der Betroffenen sichergestellt?

Datensicherheit – Datenschutz

	allgemeine Datensicherheit	Datenschutz
schützt	Daten, Hardware, Systeme, Software	natürliche Personen
Gefahr	Verlust, Zerstörung, Unterbrechung, Missbrauch	Verletzung von Persönlichkeits-rechten

Schutzziele für Datenschutz

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

Neue Schutzziele für Datenschutz

Betroffenenrechte

- **Transparenz**
  - personenbezogene Verfahren sollen mit zumutbarem Aufwand von den Betroffenen nachvollzogen, überprüft und bewertet werden können
- **Intervenierbarkeit**
  - personenbezogene Verfahren benötigen Maßnahmen, damit sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen

Kaptitel III DSGVO

Transparenz

- Betroffene müssen die sie betreffenden Verfahren kennen
- Anlegen von Verfahrensverzeichnissen
- Nachvollziehbarkeit durchgeführter Verfahren
- Information der Betroffenen bei Einwilligung
- Auskunftsrecht der Betroffenen
- Benachrichtigungspflicht bei fehlender Direkterhebung
- besondere Informationspflichten (z. B. bei Videoüberwachung, unrechtmäßige Kenntnis von Daten durch Dritte, ...)

Intervenierbarkeit

- Widerruf einer Einwilligung
- Widerspruch gegen Datenverarbeitung
- Berichtigung von personenbezogenen Daten
- Löschung von personenbezogenen Daten

Schutzziele für Datensicherheit und Datenschutz

- **Vertraulichkeit**
  - **Verdecktheit**
  - **Nichtverkettbarkeit**
- **Integrität**
- **Verfügbarkeit**
  - **Findbarkeit**
- **Authentizität**
- **Nichtabstreitbarkeit**
- **Transparenz**
- **Intervenierbarkeit**

Neue Schutzziele für Datenschutz

- **Verdecktheit (Unentdecktheit)**
  - gesicherter Nichtzugriff auf die Information, ob vertraulicher Nachrichteninhalt überhaupt existent ist
- **Nichtverkettbarkeit**
  - einzelne personenbezogene Daten sollen nicht miteinander verknüpft werden können, so dass ein umfangreiches Profil einer Person erstellt werden kann
- **Findbarkeit**
  - gesicherter Zugriff innerhalb einer festgelegten Zeit selbst auf vertraulichen Nachrichteninhalt

Schutzmaßnahmen für Transparenz

- **auf Datenebene:**
  Protokollierung der Datenverarbeitung
- **auf Systemebene:**
  Dokumentation der eingesetzten Systeme und ihrer Konfiguration und Dokumentation von Veränderungen und administrativen Eingriffen
- **bei Prozessen:**
  Dokumentation der Verfahren selbst und der Prozesse, mit denen Änderungen bewirkt werden

Schutzmaßnahmen für Nichtverkettbarkeit

- **auf Datenebene:**
  Anonymisierung, Pseudonymisierung oder Nicht-Erhebung identifizierter Daten
- **auf Systemebene:**
  Einrichtung entsprechender Zugriffsrechte oder Verarbeitung auf unterschiedlichen Systemen
- **bei Prozessen:**
  keine Erhebung nicht erforderlicher Daten bzw. Löschung der Daten unmittelbar nach Zweckerreichung

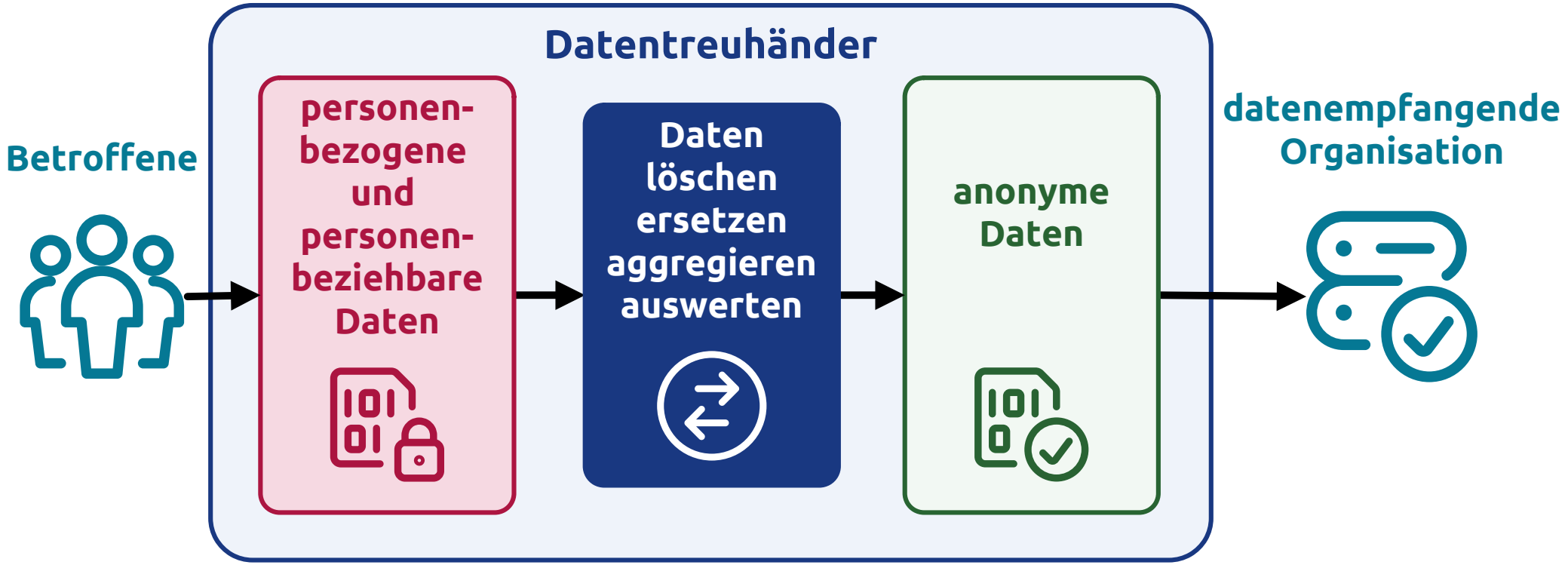
Anonymisierung und Pseudonymisierung

- **Anonymisierung**
  - Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können
- **Pseudonymisierung**
  - Ersetzung der Identifikationsmerkmale, so dass sie einer Person nicht mehr zugeordnet werden können, aber einzelne Datensätze einer Person immer noch zur gleichen Person zugehörig zu erkennen sind
  - dann wichtig, wenn mehrfach Daten erhoben werden und diese einer konkreten Instanz zugeordnet werden sollen, aber die eigentliche Person anonym bleiben soll (z. B. in Umfragen, die in mehreren Etappen erfolgen)
  - erfolgt meist über die Abbildung auf einen Schlüssel und das Abbildungsverfahren wird geheim gehalten

Vertrauen und Pseudonymisierung

- Eine vollständige Anonymisierung von Daten ist in vielen Fällen nicht möglich – zumindest dann nicht, wenn auch spezielle Auswertungen der Daten erfolgen sollen.
- In der Datenschutz-Grundverordnung kommt das Wort „Anonymisierung“ auch nur im Erwägungsgrund 26 vor und in den eigentlichen Artikeln wird nur von „Pseudonymisierung“ als Maßnahme gesprochen. Laut Ansicht einiger Datenschützer wurde das gezielt so formuliert, weil das Ziel der vollständigen Anonymisierung die Verarbeitung von personenbezogenen Daten letztendlich unmöglich machen würde.
- Für Pseudonymisierung wird oft eine dritte vertrauenswürdige Instanz eingeschaltet, die sicherstellt, dass die datenempfangende Organisation die Zuordnung von Daten zu Personen nicht kennt.
- Diese dritte vertrauenswürdige Instanz wird auch als **Datentreuhänder** bezeichnet.
- Der Datentreuhänder stellt dem Betroffenen gegenüber sicher, dass die auf ihn beziehbaren Daten nur anonymisiert weitergegeben werden.

Datentreuhänder



Anonymität im Internet

- da Personen bei der Nutzung des Internets an verschiedenen Stellen Informationen hinterlassen und diese digital erfasst werden, wird es immer leichter, umfangreiche Erhebungen von personenbezogenen Daten durchzuführen
- da die Dienste im Internet in unterschiedlichen Ländern gehosted sind, treffen unterschiedliche oder gar keine Datenschutzgesetze zu, so dass sich die Personen eigentlich selbst schützen müssen, um den Datenschutz zu sichern
- fortgeschrittene Verfahren, die Verhaltensmustererkennung (Tippverhalten, Clickverhalten, Webseiten-Interessen) einsetzen, ermöglichen es Internetdiensten auch Personen zu erkennen, die sich gar nicht freiwillig identifiziert haben
- es wird immer schwieriger, anonym im Internet unterwegs zu sein...

Anonymes Surfen

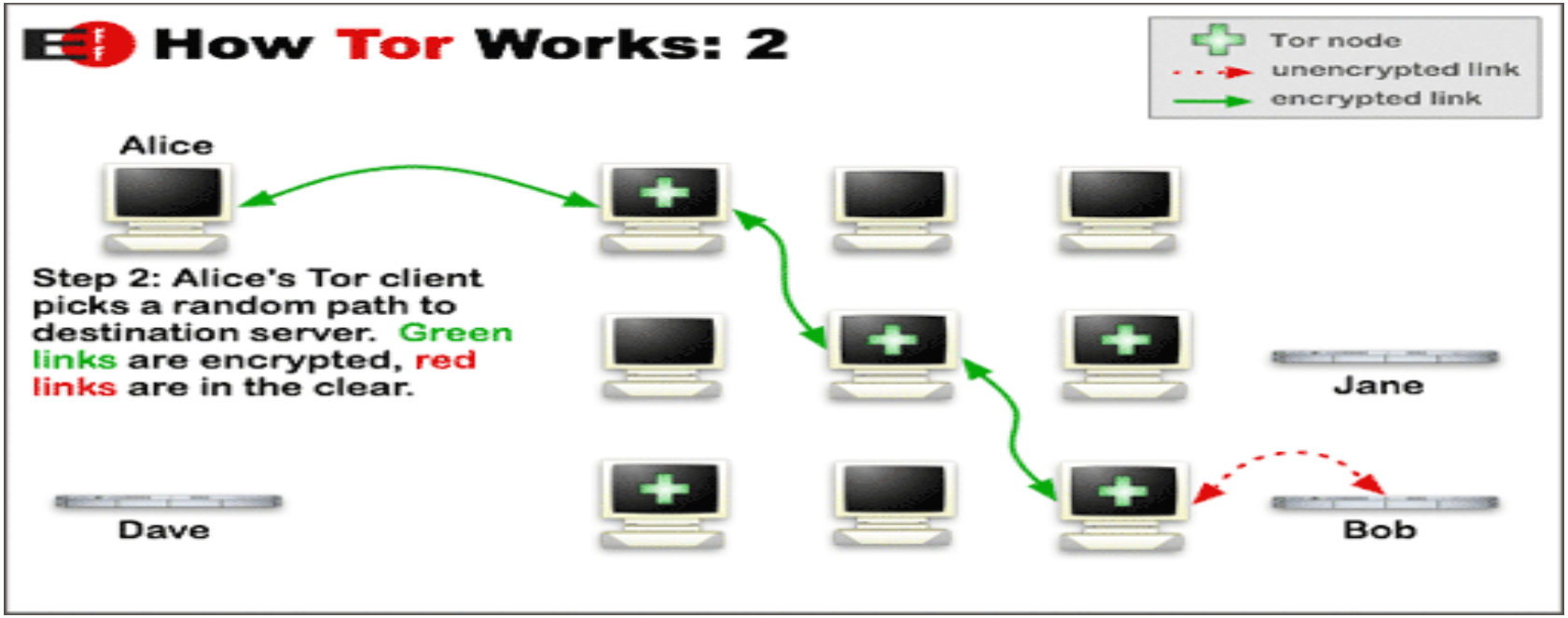
- wie anonym ist das Surfen im Internet?
- Informationen im HTTP-Header bei einer HTTP-Anfrage:

```
Host: www.irecht.h-da.de
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=[...]
Cookie: fe_typo_user=fc15e472d8ba74f17aa6e67b77bcaf8c
Connection: keep-alive
Cache-Control: max-age=0
```

- zusätzlich ist im TCP/IP-Header die Absender-IP-Adresse enthalten
- wenn von zuhause über einen festen Internetanschluss oder mobil mit Handyvertrag gesurft wird, ist es alles andere als anonym

The Onion Router - TOR

- https://www.torproject.org/
- ermöglicht anonyme Verbindungen zu Diensten im Internet
- keine direkte Verbindung, sondern durch mehrere Knoten des TOR-Netzwerks



Anonymes kommunizieren im Internet

- z. B. anonym Feedback geben
- geht per normaler E-Mail nicht, weil eine E-Mail typischerweise genau einer Person zugeordnet werden kann
- Webformulare zur Kommunikation auf Webseiten, in Kombination mit TOR, wären eine anonyme Option
- es gibt auch spezielle **Remailer-Dienste**, die eine E-Mail empfangen, aus dieser E-Mail die Absende-Adresse löschen und sie dann an die Empfangs-Adresse weiterleiten, so dass der Remailer nur noch als Absende-Adresse zu sehen ist und nicht die Ursprungs-Absende-Adresse
- zudem gibt es Online-Angebote, mit denen Einmal-E-Mail-Adressen erstellt werden können, die genau für eine E-Mail-Nachricht gültig sind
- echte anonyme Kommunikation geht typischerweise nur in eine Richtung, weil die Absende-Adresse ja unbekannt sein soll

Tracking

- Zuordnen und Wiedererkennen von Entitäten (Personen, Computer, Organisationen)

- Zwecke des Trackings:
  - Werbung
  - Benutzerfreundlichkeit
  - Überwachung

- Technische Umsetzung über:
  - IP-Adressen
  - Cookies oder Web Storage (siehe Vorlesung 5 IT- und Medientechnik)
  - Nutzerverhalten (z. B. Mausbewegung, Tastenanschlagmuster, Suchbegriffe, ...)

Weitere Infos zu Datenschutz und Informationsfreiheit

- **Chaos Computer Club**
  - https://www.ccc.de
- **Digitalcourage e.V.**
  - https://digitalcourage.de/
- **Gesellschaft für Datenschutz und Datensicherheit**
  - https://www.gdd.de
- **Der Hessische Beauftragte für Datenschutz und Informationsfreiheit**
  - https://datenschutz.hessen.de/
- **Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**
  - https://www.bfdi.bund.de/