Einführung in die IT-Sicherheit

SS 23 – Grundlagen und Motivation

Inhalte der Vorlesung

- Einführung und Organisatorisches
- Grundlagen und Motivation
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Hash-Funktionen
- Digitale Signaturen
- TLS
- Verfügbarkeit
- Internetsicherheit
- Staatliche Überwachung
- IT-Sicherheits-Management

Motivation

- **IT-Sicherheit betrifft jeden!**
- Wir geben täglich unsere Daten an Dritte weiter:
  - Soziale Netzwerke
  - Krankenversicherung
  - Vereine
- Wir Benötigen eine Vielzahl an technischen Dienstleistungen:
  - Bank
  - Telekommunikation
- Unbefugte Zugriffe oder Störungen können schwerwiegende Konsequenzen haben:
  - Identitätsdiebstahl
  - Verfolgung und Diskriminierung
  - Unfähig Geld abzuheben.
  - Rettungsdienste können nicht erreicht werden.

Motivation

- Unsere physische Sicherheit hängt ebenfalls von digitalen Geräten ab:
  - Herzschrittmacher
  - Autonomes Fahren
- Angriffe auf Firmen können Auswirkungen auf die Mitarbeiter haben:
  - Kurzarbeit
  - Entlassung

Grundbegriffe

- **Security** (IT-Security, Cyber Security, Datensicherheit, IT-Sicherheit, Informationssicherheit)
  - Schutz von Daten vor Zerstörung, Abhören, Manipulation, etc.
  - Betrifft personenbezogene Daten (z.B. Mitarbeiterdaten) und Dinge (z.B. Konstruktionspläne).
- **Safety**
  - Bezieht sich auf die Verfügbarkeit von Daten und IT.
  - Systeme werden redundant entworfen: Wenn eines ausfällt, kann man mit anderen weiterarbeiten.
- Security $\neq$ Safety

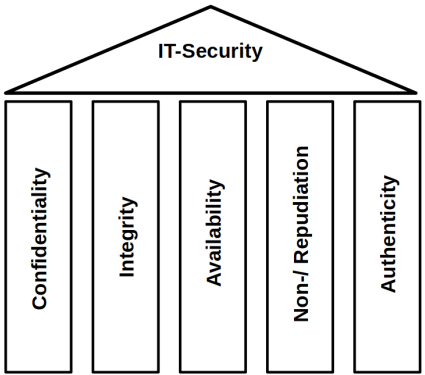
Grundbegriffe

- **Datenschutz** (privacy, data protection)
  - Schutz des Rechts auf informationelle Selbstbestimmung.
  - Hergeleitet aus `Art.2 Abs.1 GG i.V.m. Art.1 Abs.1 GG`
  - Jeder darf selbst bestimmen, wer welche Daten über ihn hat, bekommt, verarbeitet oder wann Daten gelöscht werden sollen.
  - Datenschutz ist in der DSGVO und im TKG geregelt.

Die 5 Säulen der IT-Sicherheit

Die Säulen beschreiben jeweils die Anforderungen, die in Bezug auf Sicherheit, an die Speicherung, Verarbeitung und Übermittlung von Daten gestellt werden.

- **Confidentiality** (Vertraulichkeit)
- **Integrity** (Integrität)
- **Availability** (Verfügbarkeit)
- **Non-/ Repudiation** (Nicht-/ Abstreitbarkeit)
- **Authenticity** (Authentizität)



Die 5 Säulen der IT-Sicherheit

Confidentiality

- Selbst wenn eine unberechtigte Person Zugriff zu den Daten erhält, kann diese **keine Rückschlüsse** über deren Inhalt ziehen.
- Dies kann durch die Verschlüsselung der Daten erreicht werden.
  - Hierbei wird ein Klartext p, mithilfe eines Schlüssels K_{enc} und unter Verwendung einer Verschlüsselungsfunktion enc, durch einen Geheimtext c ersetzt.
  - Der Klartext lässt sich nur durch Kenntnis eines Entschlüsselungsschlüssels k_{dec} wiederherstellen.

Die 5 Säulen der IT-Sicherheit

Integrity

- Daten können **nicht unbemerkt** manipuliert werden.
  - D.h. die Anforderung schließt nicht aus, dass ein Angreifer die Fähigkeit besitzt, unberechtigt Daten zu verfälschen.
  - Durch entsprechende Verfahren muss jedoch sichergestellt werden, dass eine Manipulation erkannt wird.
  - Dies kann u.a. durch Message Authentication Codes (MAC) oder Hash Funktionen erreicht werden.
- Nur weil die Daten vor unberechtigtem Zugriff geschützt sind (Confidentiality) ist nicht automatisch auch die Integrität gewährleistet.

Die 5 Säulen der IT-Sicherheit

Availability

- Daten sind immer dann verfügbar, wenn sie benötigt werden.
- Daten können nicht verloren gehen.
- Dies muss durch entsprechende Software und Hardware sichergestellt werden.
  - Zuverlässige Software verwenden und aktuell halten, um Störungen zu vermeiden.
  - Backups + Strategie um Daten im Notfall wiederherstellen zu können.
  - Redundante Auslegung der IT-Infrastruktur.
- Verfügbarkeit ist für fast alle Unternehmen von großer Bedeutung und Erpresser machen sich dies zunutze.

Die 5 Säulen der IT-Sicherheit

Authenticity

- Daten wurden wirklich vom angegebenen Urheber erstellt und nicht von jemand anderem.
  - Digitale Signaturen (z. B. PGP, S/MIME)
- Beispiel:
  - Bank: Eine Anfrage für eine Online-Überweisung wurde tatsächlich vom Kontoinhaber gesendet.
  - E-Mail: Die E-Mail stammt wirklich vom Vorstand und nicht von einem Betrüger.

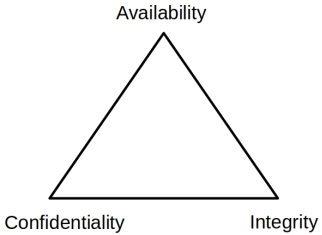
Die 5 Säulen der IT-Sicherheit

Non-/ Repudiation

- Es kann sicher festgestellt werden, um wessen Daten es sich handelt (Non-Repudiation) ...
  - z. B. können Kontoinhaber:innen nicht abstreiten, dass sie eine Online-Überweisung getätigt haben.
- ... oder es kann keine Verknüpfung zwischen der Person und den gegebenen Daten hergestellt werden (Repudiation).
  - z. B. durch Anonymisierung bei Nutzung des Internets (TOR, Tails OS).
  - z. B. durch Anonymisierung von Whistleblowern (z.B. via Secure Drop).
- Nichtabstreitbarkeit durch "Zustellungsnachweis" und "Herkunftsnachweis"
- Inkludiert die Authentizität der Parteien und Integrität der Kommunikation

Die 5 Säulen der IT-Sicherheit

Confidentiality, **I**ntegrity und **A**vailability (CIA) werden oft als die drei Kernziele der IT-Sicherheit angesehen.



Alle drei **stehen in einem stetigen Spannungsverhältnis zueinander**, d.h. sie können nicht alle gleichzeitig, vollständig erreicht werden.

Die 5 Säulen der IT-Sicherheit

- Es muss grundsätzlich, je nach Anwendungsfall, zwischen den einzelnen Zielen abgewogen werden.
- Beispiel:
  - Bei Betriebsgeheimnissen steht die Vertraulichkeit und Integrität im Vordergrund. Die Daten sollten dabei nur autorisierten Personen zugänglich sein.
  - Informationen die für die Öffentlichkeit bestimmt sind, sollten primär integer und verfügbar sein.
    - Veröffentlichung von Falschinformationen über sonst vertrauenswürdige Quellen kann das Wohlergehen von Mitbürgern gefährden.
    - Ich muss die Adresse meines Wahllokals nachschlagen können, um mein Recht wählen zu gehen, ausüben zu können.

Die 5 Säulen der IT-Sicherheit

- Viele bekannte Maßnahmen gewährleisten mehrere Schutzziele gleichzeitig.
  - MAC (Integrität und Authentizität): Eine Information die genutzt werden kann, um zu überprüfen, ob die gegebenen Daten vom angegebenen Absender stammen (Authentizität) und nicht manipuliert wurden (Integrität).
  - z.B. Poly1305

Sicherheitsrisiken

- Es gibt eine Vielzahl an Sicherheitsrisiken, denen Firmen, als auch Privatpersonen, ausgesetzt sind.
  - OSINT/ CI
  - Wirtschaftsspionage
  - Cybercrime
    - Ransomware
    - (Distributed-)Denial-of-Service
    - Fishing
  - Unsichere Software
- Durch Spionage, Sabotage und Datendiebstahl entstehen jährlich Schäden von 100 Mrd. Euro in Deutschland[1].

[1] bit20.

Sicherheitsrisiken: OSINT/CI

- **O**pen **S**ource **I**ntelligence (OSINT): Sammeln von Informationen über Unternehmen und Personen durch (halb-)offene Informationsquellen.
  - Websites
  - Newsletter
  - Soziale Netzwerke
  - Internetforen
  - Ungesicherte Schnittstellen (APIs)
- **C**ompetitive **I**ntelligence (CI): Sammeln von Informationen über Konkurrenzunternehmen.
  - Kann als ein Spezialfall von OSINT angesehen werden.
  - Viele Unternehmen haben CI Abteilungen.

Sicherheitsrisiken: OSINT/CI

- Mögliche Auswirkungen:
  - Identitätsdiebstahl
  - Phishing/ Social Engineering: Je mehr Informationen vorliegen, desto effektiver können Phishingangriffe durchgeführt werden.
  - Account Zugriffe: z.B. unter Verwendung von Nutzername, E-Mails, persönlichen Informationen, ...
  - Bekanntwerden von Firmengeheimnissen.
  - Abwerben von wichtigem Personal.

Sicherheitsrisiken: Cybercrime

Hohe wirtschaftliche Schäden u.a. durch:

- **Ransomware**: Verschlüsselung und ggf. Exfiltration von Daten mit dem Versprechen diese nach dem Zahlen eines Lösegelds (engl. Ransom) wieder zu entschlüsseln.
  - Ohne Backups sind Firmen den Tätern ausgeliefert.
  - Angreifer sind nicht vertrauenswürdig (Double-Extortion-Ransomware-Attack): Opfer werden doppelt erpresst, d.h. sie sollen ein Lösegeld zur Entschlüsselung der Daten zahlen und ein zweites damit die Daten von den Angreifern nicht veröffentlicht werden.
- **(D)DOS**:
  - Störung der Verfügbarkeit eines Unternehmens.
  - z.B. durch Überlastung der Infrastruktur.

Sicherheitsrisiken: Cybercrime

- **Phishing**
  - Kriminelle versuchen ihr Opfer zu einer bestimmten Tat zu bewegen.
    - Herausgabe sensibler Informationen.
    - Überweisen von Geld.
    - Anschluss eines USB Rubber Ducky an einen Computer der mit dem Firmennetzwerk verbunden ist.
    - Herunterladen und Installation von Schadsoftware.
  - Angreifer können dabei eine Reihe an Medien nutzen.
    - E-Mail
    - SMS (smishing)
    - Telefon
  - Angreifer nutzen die Schwächen des Menschen zu ihrem Vorteil.
    - Betonung der Dringlichkeit.
    - Zu gut um wahr zu sein.

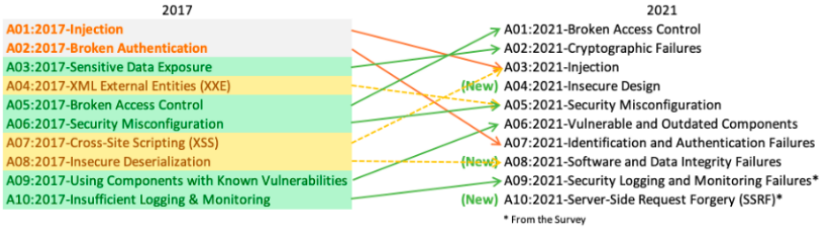
Sicherheitsrisiken: Unsichere Software

- Die Entwicklung von Software ist komplex.
  - Anwendungen müssen Daten von nicht vertrauenswürdigen Quellen verarbeiten[2].
  - Anwendungen nutzen oft eine Vielzahl an Dependencies mit potenziellen Schwachstellen[3].
  - Unaufmerksamkeiten in der Verwendung von Low Level Sprachen (C, C++) können ein Einfallstor für Schadcode darstellen (Shellcode-Injection, ROP, JOP, ...).
- Ein unsicheres Design kann ebenfalls einen Einfluss auf die Sicherheit von Software haben.
  - HTTP wurde mit Fokus auf Funktionalität jedoch nicht auf Sicherheit entwickelt.
  - An insecure design cannot be fixed by a perfect implementation[4].

[2] OWAa.
[3] Sta.
[4] OWAb.

Sicherheitsrisiken: Unsichere Software

Das **O**pen **W**eb **A**pplication **S**ecurity **P**roject (OWASP) veröffentlicht in regelmäßigen Abständen eine Liste der häufigsten Schwachstellen.



Sicherheitsrisiken: Unsichere Software

A01:2021 Broken Access Control

- Access Control setzt von einer Anwendung definierte Zugriffsregeln durch, sodass Nutzer nur in einem für sie vorgegebenen Rahmen operieren können.
- Prinzipien:
  - **Authentication**: Ich beweise, dass ich die angegebene Person bin (Username + Password, YubiKey, ...).
  - **Authorization**: Die Anwendung überprüft, ob ich berechtigt bin eine Aktion auszuführen, z.B. durch Nutzerrollen (User, Guest, Admin, ...).
- Schwachstellen:
  - Autorisierung wird nicht korrekt oder gar nicht überprüft (Violation of the principle of least privilige).
  - API ohne Zugriffskontrolle
- Auswirkungen: Unberechtigter Zugriff, Modifikation und Zerstörung von Daten.

Sicherheitsrisiken: Unsichere Software

A02:2021 Cryptographic Failures

- Die meisten Anwendungen hängen in irgend einer Form von sicheren kryptographischen Algorithmen und Protokollen ab. Sollten diese Schwachstellen besitzen, so wirkt sich dies auch auf die Anwendung selber aus.
- Schwachstellen:
  - Sensible Daten wie z.B. Passwörter werden im Klartext übertragen (HTTP, SMTP, FTP).
  - Nutzung von alten oder schwachen kryptographischen Algorithmen und Protokollen (DES, iClass).
  - Nutzung von wenigen vordefinierten Schlüsseln auf einer Vielzahl von Geräten.
  - Nutzung von (Pseudo-)Zufallszahlengeneratoren die nicht kryptographisch sicher sind.
- Auswirkungen:
  - u.a. Unberechtigter Zugriff, Manipulation von Informationen.

Sicherheitsrisiken: Unsichere Software

A03:2021 Injection

- Bei Injection-Angriffen gelingt es dem Angreifer Daten (Untrusted Data) an eine Anwendung zu übergeben, die dort einen vom Entwickler unbeabsichtigten Vorgang auslösen.
- Schwachstellen:
  - Vom Nutzer bereitgestellte Daten werden nicht korrekt validiert oder gefiltert.
  - Vom Nutzer bereitgestellte Daten werden direkt in Datenbank-Queries verwendet.
- Auswirkungen:
  - SQL Injection: Indirekter Zugriff auf die Datenbank, z.B. über die Suchfunktion einer Webseite.
  - Cross-Site-Scriptig (XSS): Einschleusen von (JS-)Schadcode, der von anderen Nutzern, beim Besuchen der Webseite, heruntergeladen und ausgeführt wird.

Sicherheitsrisiken: Unsichere Software

A04:2021 Insecure Design

- Schwachstellen können aufgrund eines fehlerhaften Anwendungs-/ Protokolldesigns entstehen.
- An insecure design cannot be fixed by a perfect implementation [OWAb].
- Mögliche Maßnahmen:
  - Erstellung eines Threadmodells für kritische Bereiche (Authentisierung von Nutzern, ...).
    - Beschreibung des Systems, welches modelliert wird (what are we working on?).
    - Potenzielle Risiken für das System (what can go wrong?).
    - Maßnahmen die ergriffen werden können, um die Gefahr zu minimieren (what are we goint to do about it?).
    - Validierung des Modells, Gefahren und Maßnahmen (did we do a good enough job?).
  - Ausrollen von Unit- und Integrationstests.

Sicherheitsrisiken: Unsichere Software

A05:2021 Security Misconfiguration

- Ein für sich sicheres Design und korrekte Implementierung können durch falsche Konfiguration eine Anwendung trotzdem unsicher machen.
- Schwachstellen:
  - Die verwendete Software ist Out of Date oder es sind für diese Angriffe bekannt.
  - Standard Accounts und deren Passwörter werden verwendet.
  - Unnötige Funktionen werden bereitgestellt.
    - Offene Ports die eigentlich nicht verwendet werden.
  - Ein Server sendet keine Security Headers oder Direktiven.
    - HTTP Strict Transport Security (HSTS) – Erzwingen der Kommunikation via HTTPS.
    - Content Security Policy (CSP) – Whitelisting von Quellen für z.B. JS.

Sicherheitsrisiken: Unsichere Software

A06:2021 Vulnerable and Outdated Components

- Alle Komponenten einer Anwendung sollten aktuell gehalten und auf Schwachstellen überprüft werden.
- Schwachstellen:
  - Die Software besitzt Schwachstellen, wird nicht mehr unterstützt oder ist veraltet.
  - Updates und Fixes werden nach Bekanntwerden von Schwachstellen zu spät oder gar nicht druchgeführt.
  - Entwickler testen nicht die Kompatibilität von aktualisierten Komponenten (breaking changes).
  - Die Komponenten sind inkorrekt konfiguriert (siehe A05).
- Auswirkungen:
  - z.B. Zugriff auf einen Server via einer PHP Reverse Shell, die durch ein veraltetes Word Press Plugin, mit Sicherheitsschwachstelle, hochgeladen werden konnte.

Sicherheitsrisiken: Unsichere Software

A07:2021 Identifcation and Authentication Failures

- Das Überprüfen der Identität eines Nutzers, die Authentisierung und das Session Management sind wichtiger Bestandteil vieler (Web-)qAnwendungen.
- Schwachstellen:
  - Anwendung erlaubt die Durchführung automatisierter Angriffe (z.B. Credential Stuffing).
    - Fehlermeldungen werden nicht generisch gehalten.
    - Beliebig viele Versuche sind zugelassen.
  - Verwendung von schwachen Passwörtern.
  - Speicherung von Passwörtern im Klartext oder Verwendung von schwacher Verschlüsselung oder schwachen Key Derivation Funktions (KDF).

Sicherheitsrisiken: Unsichere Software

A08:2021 Software and Data Integrity Failures

- Die Verwendung von Software, Daten und Updates ohne Überprüfung derer Integrität ermöglicht es, z.B. über einen automatisierten Update-Prozess, eine sichere Anwendung in einen unsicheren Zustand zu überführen.
- Vorkehrungen:
  - Verwendung digitaler Signaturen und MACs um verifizieren zu können, dass die Daten vom angegebenen Absender stammen und nicht manipuliert wurden.
  - Ausschließliche Verwendung von vertrauenswürdigen Repositories (apt, npm, Maven, ...).
  - Review Prozess bei Konfigurations- und Codeänderungen.

Sicherheitsrisiken: Unsichere Software

A09:2021 Security Logging and Monitoring Failures

- Ohne Logging und Monitoring können Sicherheitsvorfälle nicht registriert und korrekt adressiert werden.
- Je mehr über einen Vorfall bekannt ist, desto besser kann ähnlichen Vorfällen in Zukunft vorgebeugt werden.
- Logging kann weiterhin Forensikern bei der Ermittlung unterstützen:
  - Loggen von Logins, fehlgeschlagenen Logins, und besonders schützenswerten Transaktionen.
  - Die Log-Nachrichten müssen aussagekräftig sein.
  - Die Logs müssen (automatisiert) beobachtet werden um "ungewöhnliche" Aktivitäten registrieren zu können.
  - Prozesse bei Eintreten eines Vorfalls müssen klar festgelegt werden (Incident Response Plan).

Sicherheitsrisiken: Unsichere Software

A10:2021 Server-Side Request Forgery (SSRF)

- SSRF erlaubt einem Angreifer einen Server dazu zu bringen, HTTP Anfragen an beliebige Domänen zu senden (Angreifer → Request → Server → Request → Resource).
  - z.B. Zugriff, mittels eines anfälligen Servers, auf eine Redis Datenbank die eigentlich nicht nach außen zugänglich ist.
- Vorkehrungen:
  - Separieren von Remote Resource Access Funktionalität in ein separates Netzwerk.
  - Erzwingen von "Deny by Default" Firewall Policies.
  - Vertraute niemals Daten von Anwendern.

Citations

[bit20] bitkom. *Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt*. bitkom, 2020.

[OWAa] OWASP. *Deserialization of untrusted data*. URL: https://owasp.org/www-community/vulnerabilities/Deserialization_of_untrusted_data. (accessed: 26.05.2022).

[OWAb] OWASP. *OWASP Top 10 - 2021*. URL: https://owasp.org/Top10/. (accessed: 26.05.2022).

[Sta] Stanford. *Log4Shell Vulnerability: What You Need to Know*. URL: https://uit.stanford.edu/news/log4shell-vulnerability-what-you-need-know. (accessed: 26.05.2022).