IT-Sicherheit
WiSe 2021/22

Grundbegriffe und Bedrohungsanalyse

Übersicht

1. Wiederholung: IT-Sicherheit als Systemeigenschaft
2. Angreifer*innen
   - Motivation und Vorgehen von Angreifer*innen
   - Vorgehen von Kriminellen und ethischen Hacker*innen
   - Fallbeispiele für Angriffe
3. Bedrohungsanalyse
   - Definition des Systems
   - Sicherheitsziele und Schutzbedarf des Systems
   - Bedrohungen gegen das System
4. Zusammenfassung

Teil 1) IT-Sicherheit als Systemeigenschaft

Sicherheitsmechanismen

- Verschlüsselung
- Netzwerkabsicherung
- Authentifizierung
- Rechtemanagement
- ….

Qualitätssicherung

- Schulung des Personals
- Regelmäßige Updates
- Hohe Software Testabdeckung
- Review der Konfigurationen
- …

Vision der LVA IT-Sicherheit

- IT-Sicherheit ist eine Systemeigenschaft
  - Je nach Tätigkeitsfeld andere Berührungspunkte
  - Schwachstellen finden und beheben benötigt Expert*innenwissen
  - Klare Kommunikation der Konsequenzen wird benötigt

- Kernkompetenz der LVA: Selbstständig neue Schwachstellen und Bedrohungen identifizieren und geeignete Maßnahmen entwickeln, implementieren und testen

Bedrohungsanalyse Grundidee

„If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." **Sun Tzu.**

- Um IT-Sicherheit angemessen zu implementieren, muss man:
  1. Potentielle Angreifer*innen kennen (Teil 2 – Angreifer*innen)
  2. Das eigene System kennen (Teil 3 – Bedrohungsanalyse)

Teil 2) Angreifer*innen

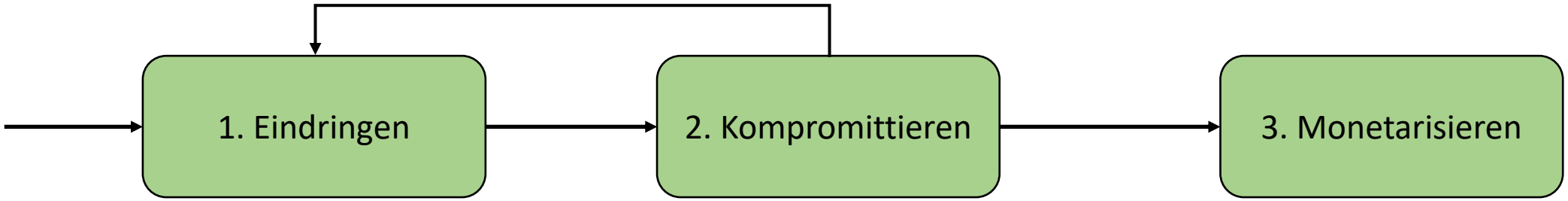
Wer kann als Angreifer*in auftreten?

Angreifer*innen, Motivationen und Vorgehen

Angreifer*in	Motivation	Vorgehen
Nutzende	Persönliche Vorteile (Features freischalten, weniger Kosten, …)	Anwendung von Tools oder Anleitungen; Anheuerung organisierter Krimineller
Mitarbeitende	Rache; Geld; Ideologie (Whistleblower)	Zugriff auf und Kompromittierung interner Systeme
Ethische Hacker*innen (White Hats, Pentester*innen)	Anerkennung; Herausforderung; Geld; Ethische Überzeugung	Identifikation von Schwachstellen; Ausnutzung unter ethischen Richtlinien
Hacktivist*innen (Grey Hats)	Anerkennung; Herausforderung; Politische oder ideologische Ziele; Vandalismus; Geld	Identifikation und Ausnutzung von Schwachstellen; Offenlegung des Eindringens
Kriminelle (Black Hats)	Geld	Identifikation und Ausnutzung von Schwachstellen; Kompromittierung des Systems; Monetarisierung
Konkurrenz	Störung; Entwendung von Technologie; Diskreditierung	Reverse-Engineering von Produkten; Anheuerung organisierter Krimineller
Staaten / Geheimdienste	Wirtschaftliche Vorteile, Destabilisierung	Kompromittierung der Infrastruktur, Komponenten oder Standards; Tarnung vor Entdeckung

Vorgehen von Kriminellen

- Viele Angriffe lassen sich in drei Phasen unterteilen:



- Oftmals wechselnde Akteure zwischen den Phasen:
  - Spezialisierte Kriminelle reichen Opfer untereinander weiter
  - Schadprogramme automatisieren Teile des Angriffs
  - Kriminelle stellen „Laien“ Werkzeuge für einzelne Phasen bereit (X-as-a-Service Modell)

Vorgehen von Kriminellen
1. Eindringen

- Kriminelle nutzen verschiedene Techniken um in ein System einzudringen:
  - **Phishing**: Fälschen einer eMail, Webseite, Fehlermeldung oder Identität am Telefon um das Opfer zu bestimmten Aktionen zu bewegen
  - **Spear Phishing:** Phishing mit einer auf das Opfer angepassten Meldung
  - **Passwort Raten:** Erraten eines einfachen oder geleakten Passwortes
  - **Physischer Zugang:** Spezielle Hardware führt beim Anschließen Schadcode aus
  - **„Hereinspazieren“:** Ausnutzen von fehlenden Sicherheitsmechanismen
  - **Exploits:** Software zum Ausnutzen einer Softwareschwachstelle des Systems

- Exploits für deren Softwareschwachstelle noch kein Patch existiert werden als **Zero-Day** Exploits (bzw. **Zero-Day** Schwachstelle) bezeichnet

Vorgehen von Kriminellen
2. Kompromittieren

- Kompromittieren geschieht manuell oder automatisiert via Malware (**Mal**icious Soft**ware**)

- Verfeinerung der Klassifikation von Malware je nach Vorgehen:
  - **Ransomware**: Fordert Lösegeld unter Bedrohung von Nutzenden (z.B. Löschen von Daten, …)
  - **Spyware**: Späht Informationen über Geräte, Netzwerk oder Nutzer*innen aus
  - **Trojaner**: Lädt weitere Malware nach oder erlaubt Angreifer*innen Zugriff
  - **Viren**: Modifiziert Programme um sich eigenständig weiterzuverbreiten
  - **Würmer**: Kopiert sich selbst um sich eigenständig weiterzuverbreiten
  - **Adware / Cryptominer**: Zeigt unerwünschte Werbung oder „mined“ Crypto Währung

- Moderne Malware lässt sich nicht eindeutig klassifizieren (Beispiel Emotet später)

- **Advanced Persistent Threats** (APTs) bezeichnen zielgerichtete und manuelle Angriffe, bei denen sich Angreifer*innen tarnen um über längere Zeit im zu System bleiben

Vorgehen von Kriminellen
3. Monetarisieren

- Angriffe können auf verschiedene Weisen monetarisiert werden:
  - **Verkauf geheimer Daten** (Geistiges Eigentum, Accounts, Adressen, …)
  - **Erpressung via:**
    - Veröffentlichung von Daten (Tegut Kundendaten, ...)
    - Löschung kritischer Daten oder Zerstörung von Systemen
    - Störung eines Dienstes (Denial of Service - DoS)
  - **Diebstahl** von Kontodaten und Überweisung des Geldes
  - **Missbrauch der Infrastruktur** des Opfers für weitere Dienste (Crypto Mining, DoS)

- Manche Kriminelle monetarisieren Dienste für Angriffe:
  - Bereitstellen von **Angriffsframeworks** zum Bau von Malware (Angriff-as-a-Service Modell)
  - Bereitstellen infizierter Rechner (**BotNets**) für Dienste wie Distributed DoS (DDoS), Spam, …

Wert von Daten im Darknet [PRIV]

- **Darknet:** Auf dem Internet aufsetzende Netzwerke, die zugangsgeschützt und anonymisiert sind und für illegale Zwecke genutzt werden

Account / Daten / Dienst	Kosten (in $)
eMail Adressen (380k Österreich)	10
Kreditkartedaten (1x)	25 – 240
Crypto Währung Account (1x)	300 – 810
Facebook Account (1x)	65
Gmail Account (1x)	80
Instagram Account (1x)	45
Instagram 1000 Follower	5
eBay Account mit gutem Feedback (1000+ Feedback)	1,000
Französischer Pass (1x)	4,000
Denial of Service Angriff (10-50k Anfragen für 24 Stunden)	50

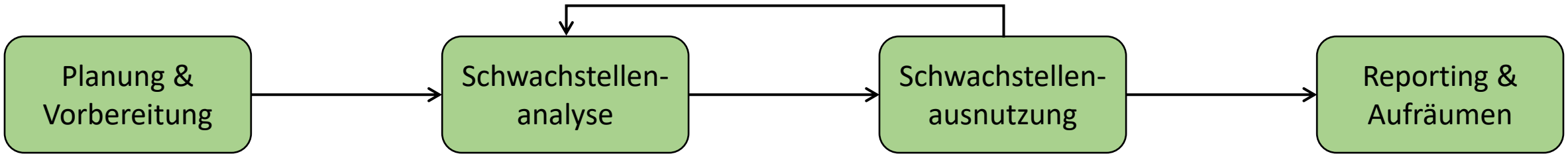
Wert von Schwachstellen [BB]

- **Bug Bounty:** Belohnung für das Finden und Melden von anerkannten Schwachstellen via Responsible Disclosure. Höhe hängt von potentiellem Schaden der Schwachstelle ab.
- **Responsible Disclosure:** Betroffenes Unternehmen wird über Schwachstelle informiert und dem Unternehmen wird Zeit (z.B. 90 Tage) zum Beheben gegeben bevor die Schwachstelle veröffentlicht wird
- **Full Disclosure:** Die Schwachstelle wird ohne eingespielten Fix veröffentlicht

Firma	Bug Bounty Minimum (in $)	Bug Bounty Maximum (in $)
Intel	500	30,000
Yahoo	-	15,000
Paypal	50	10,000
Cisco	100	2,500
Twitter	140	15,000
Apple	-	200,000
Facebook	500	-
Google	300	31,1337
Microsoft	15,000	250,000
GitHub	200	10,000

Penetration Testing

- Simulation eines realen Angriffs durch ethische Hacker*innen. Phasen:



Klärung von Details:
- Ziele des Angriffs
- Angriffsoberfläche
- Erlaubte Tools
- Weitere Informationen
- Dauer der Tests
- Rechtliche Absicherung

Vorbereitung des Angriffs:
- Evaluierung der Informationen (öffentlich, durch Ausnutzung erhalten oder vorab kommuniziert) auf Schwachstellen

Durchführung des Angriffs:
- Ausnutzen der Schwachstellen
- Identifikation von weiteren Informationen
- Prüfen ob das Ziel des Angriffs erreichbar ist

Abschluss des Auftrags:
- Kommunikation der Schwachstellen
- Vorschlag von Maßnahmen
- Löschen der erhaltenen Informationen

Ablauf eines Angriffs

- Fallbeispiele für Ablauf eines Angriffs gegen
  1. Privatperson via Phishing durch Kriminelle
  2. Unternehmensnetzwerk via Malware durch Kriminelle
  3. Fahrzeug via Sicherheitsanalyse durch Ethische Hacker

Fallbeispiel 1 – Privatperson Phishing

1. Privatperson bekommt Warnung beim Surfen

2. Person ruft Nummer an und wird erhält Anleitung um Remote Desktop Software herunterzuladen

3. Angreifer*in übernimmt Steuerung und installiert Schadcode und/oder bringt Opfer dazu eine Zahlung zu veranlassen

- **Resultat**: Infizierter Rechner wurde neu aufgesetzt und Passwörter mussten geändert werden

Fallbeispiel 2 – Unternehmen Malware (Emotet) bei Heise [HEISE]

1. Mitarbeiter öffnet Word Datei eines*r Geschäftspartners*in und bestätigt gefälschte Makro Meldung

2. Word Makro lädt Emotet nach, welcher Rechner und Heise Netzwerk befällt
   - eMails und Kennwörter im Rechner werden ausgelesen
   - Automatische Infektion weiterer Systeme im Netz über Passwort raten
   - Exploits für bekannte Schwachstellen werden angewendet

3. Antiviren Software schlägt an, Admin loggt sich im befallenen Rechner ein
   - Evtl. wurde hierbei ein Admin Passwort ausgespäht (Unklar)

4. Emotet verbreitet sich mittels Domänen Admin Account auf weitere Rechner

5. Admins registrieren verdächtige Verbindungen nach außen und kappen Internet Verbindung
   - Ansonsten: Angreifer*in analysiert System, entwendet Daten, macht System unbrauchbar und erpresst Lösegeld

- **Resultat:** Infizierte Rechner wurden außer Betrieb genommen und das Netzwerk wurde neu aufgesetzt

Fallbeispiel 3 – Jeep Cherokee Hack [FCA]

1. Sicherheitsforscher analysieren Multimedia System und WLAN Interface:
   - Schwachstellen existieren um wahlfreie Befehle auf dem Multimedia System auszuführen
   - Schwachstellen können via GSM ausgenutzt werden
   - Ca. 300.000 anfällige Jeeps werden via GSM identifiziert

2. Sie identifizieren weitere Sicherheitslücken um wahlfreie Nachrichten im Fahrzeugnetzwerk zu senden
   - Fahrzeugnetzwerk enthält: Bremsen, Lenkung, Türsteuerung, …
   - Senden von Nachrichten an Fahrzeugnetzwerk ist möglich via GSM

3. Sie demonstrieren den Angriff via Remote Hack mit Reporter am Steuer

- **Resultat:** FCA musste für 1.4 Millionen Dollar Fahrzeuge zurückrufen und updaten.

Teil 3) Bedrohungsanalyse

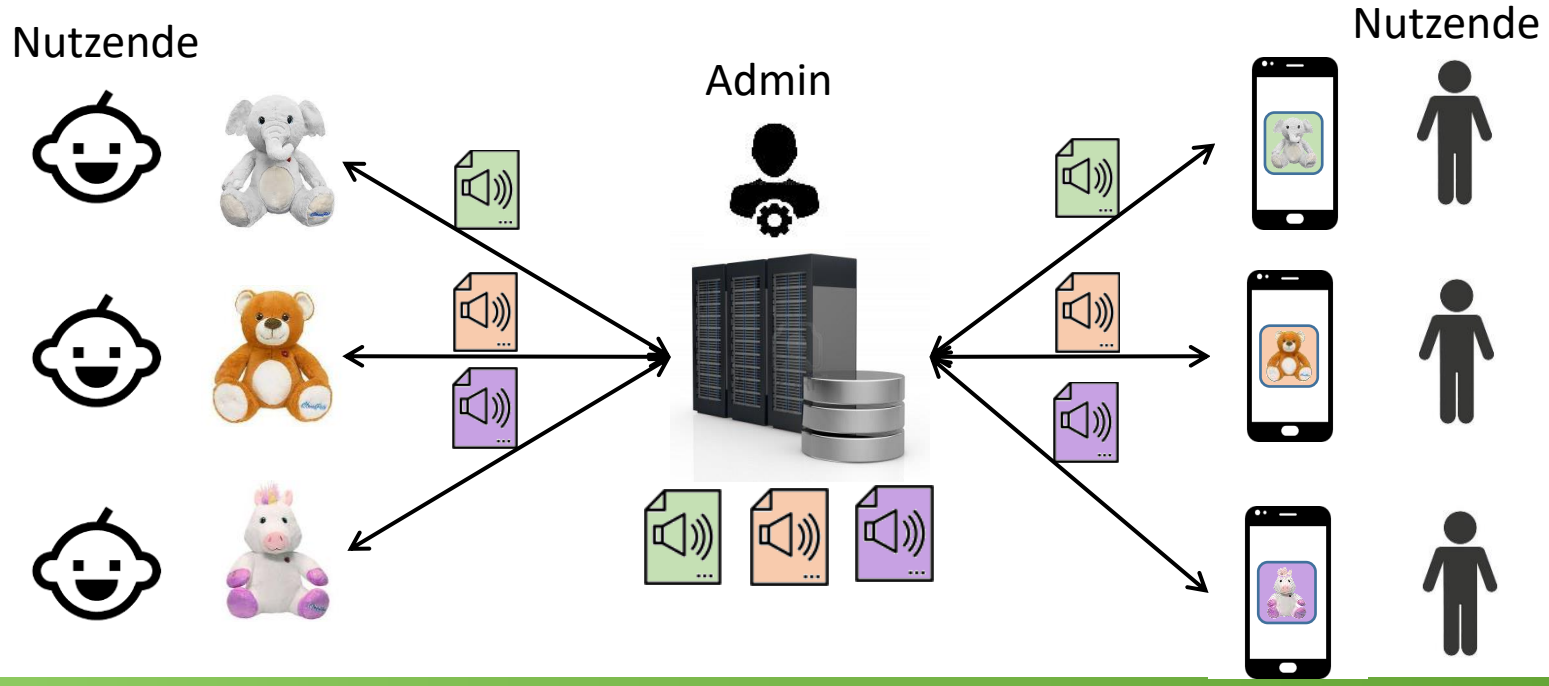
Wie würden Sie beim Absichern eines Systems vorgehen?

Anwendung von IT-Sicherheit

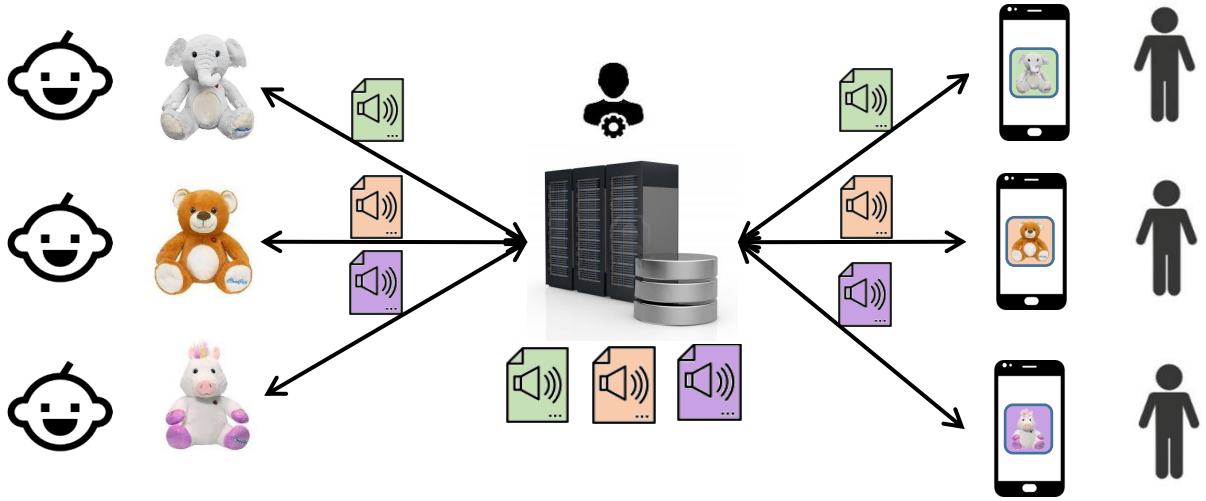
- IT-Sicherheit ist eine Systemeigenschaft
- Die relevanten Bedrohungen und Maßnahmen hängen vom System ab
- Angewendete Maßnahmen müssen auf das System zugeschnitten werden
  - Gefilterte Kommunikation, Rechtevergabe für Nutzende, …
- Es gibt keine Einheitslösung die überall angewendet werden kann
- **Aber:** Wie entwickelt man eine angepasste Sicherheitslösung?

Beispielsystem CyberPets (1/2)

- **CyberPets Use-Cases** [PET]:
  1. Audiodaten sollen zwischen Spielzeug und App übertragen werden
  2. Audiodaten sollen gespeichert werden um sie später erneut abzurufen



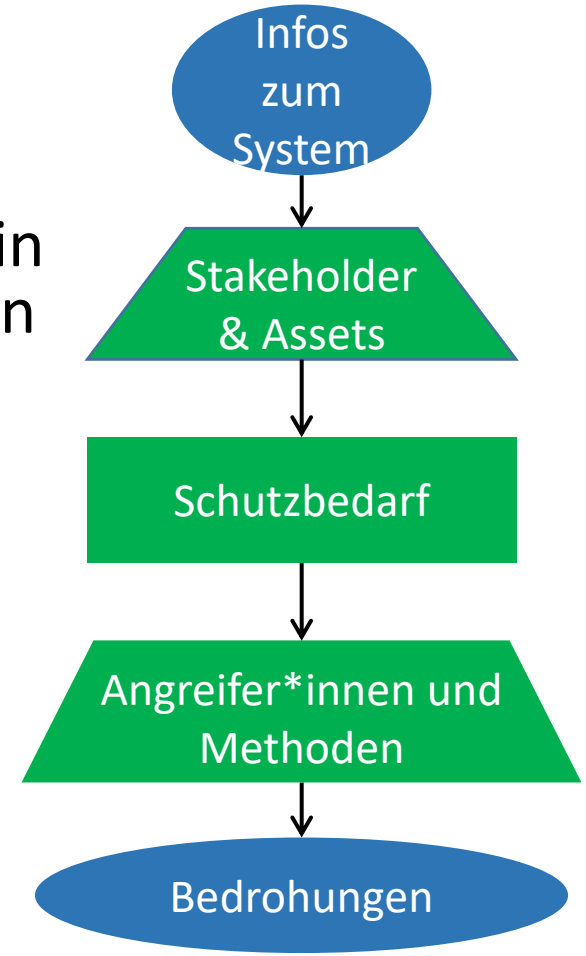
Beispielsystem CyberPets (2/2)



- **Frage:** Was sind relevante Bedrohungen für das CyberPets System?
  1. Wer ist Angreifer*in?
  2. Was ist die Methode?
  3. Was ist das Ziel?

Bedrohungsanalyse

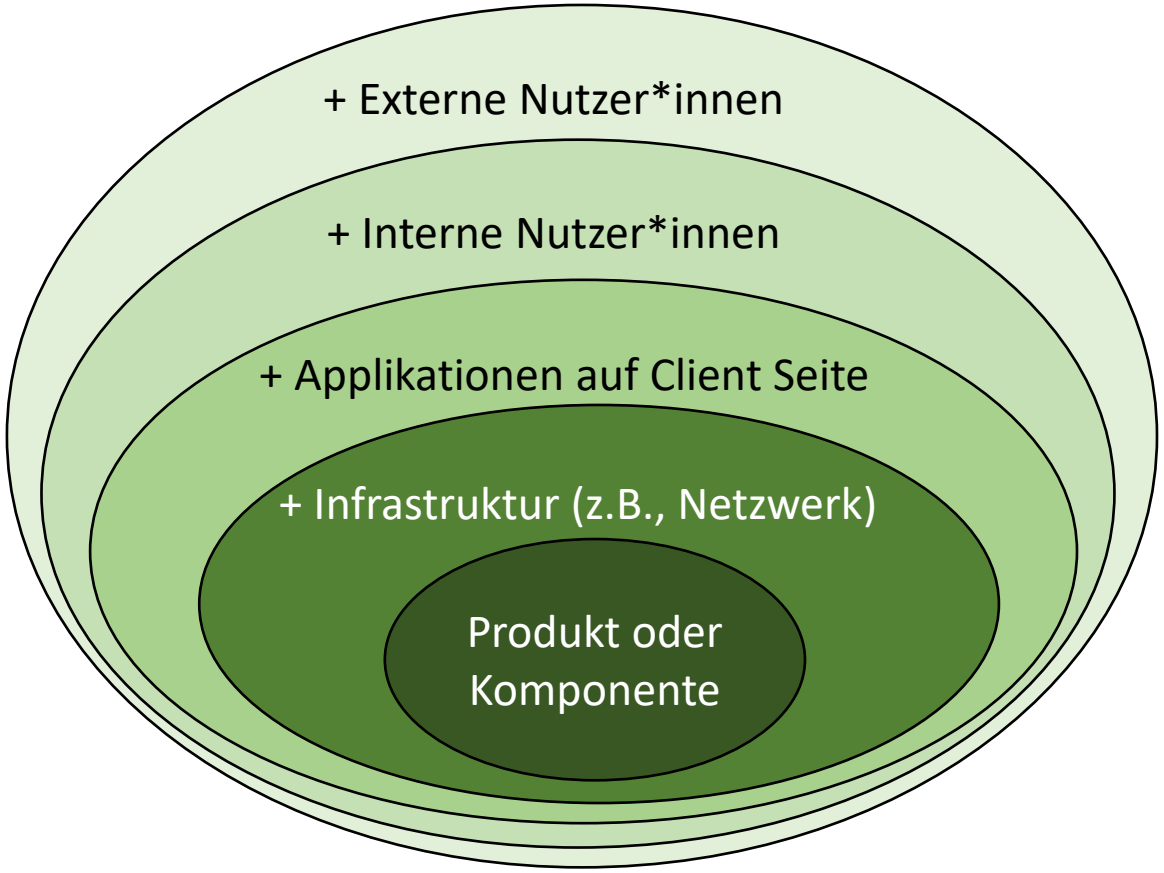
- Problem: Wurden alle relevanten Bedrohungen berücksichtigt?
- **Bedrohungsanalyse** als ein strukturierter Prozess um Vertrauen in die Vollständigkeit der identifizierten Bedrohungen zu bekommen
- Vorgehen bei der Bedrohungsanalyse:
  1. Identifikation des **relevanten Systems**
  2. Welche Parteien (**Stakeholder**) sind mit welchen Vermögenswerten (**Assets**) am System beteiligt
  3. Welchen **Schutzbedarf** haben die Assets?
  4. **Wer** hat **welches Interesse** daran den Schutzbedarf **mit welchen Methoden** zu brechen?



Identifikation des Systems [SECENG]

- Je nach Standpunkt kann Umfang und Definition von System variieren

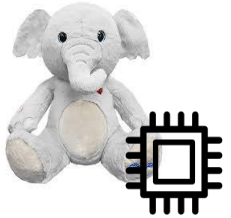
- Eine falsche Definition des Systems kann führen zu:
  - Nicht betrachteten Angriffen (zu enge Definition)
  - Falschen Annahmen und Unbenutzbarkeit (zu weite Definition)



Bedrohungsanalyse CyberPets
CyberPets System

- CyberPets: Betreibt Server und Service. Verantwortet:
  - Absicherung gegen interne und externe Nutzer*innen
  - Absicherung Infrastruktur (Server, Netzwerk, …)
  - Kommunikation der Sicherheitsmaßnahmen an Supplier
  - Sichere Konfiguration Spielzeug/App/Server

- Supplier A: Baut Spielzeug mit IoT Lösung. Verantwortet:
  - Korrekte funktionale Umsetzung des Spielzeugs

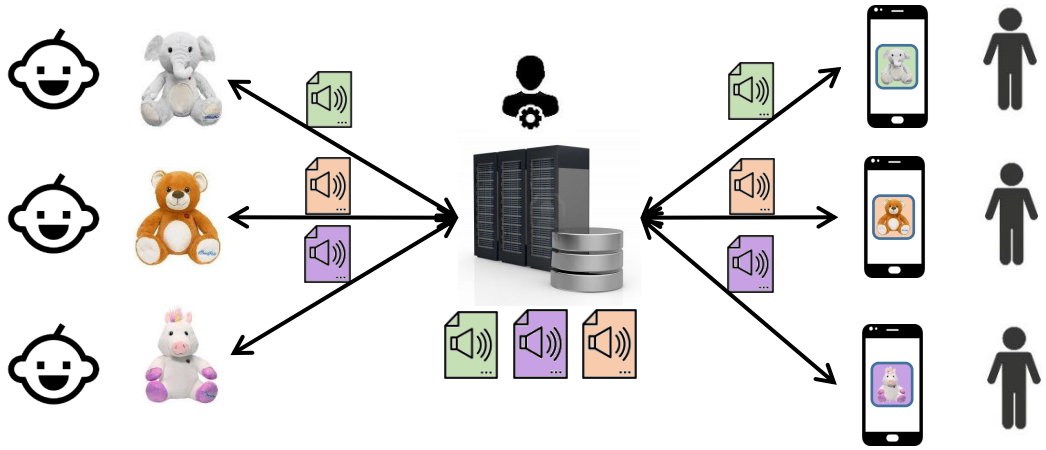


- Supplier B: Entwickelt App. Verantwortet:
  - Korrekte funktionale Umsetzung der App
  - Sicherheit in Infrastruktur Smartphone

Bedrohungsanalyse CyberPets
Stakeholder und Assets

- **Stakeholder:** Eine am System beteiligte Partei mit eigenen Interessen:
  - Kinder und Eltern (K&E)
  - Unternehmen
  - Admins

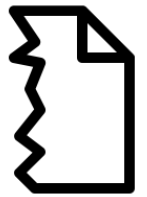
- **Asset:** Etwas von (ideellem) Wert für einen Stakeholder:
  - Audiodateien (K&E)
  - Infrastruktur (Unternehmen)



Sicherheitsziele (1/3) [Z. BSI]

1. **Vertraulichkeit**: Schutz vor unbefugter Preisgabe von Informationen.
   - Bedrohung Beispiel: Veröffentlichung kompromittierender Daten

2. **Integrität**: Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
   - Bedrohung Beispiel: Ändern der eigenen Note in horstl



3. **Authentizität**: Kommunikationspartner*in ist tatsächlich diejenige Person, die sie vorgibt zu sein bzw. die Informationen wurden tatsächlich von der angegebenen Quelle erstellt
   - Bedrohung Beispiel: Senden einer eMail unter anderem Namen

Sicherheitsziele (2/3) [Z. BSI]

4. **Verfügbarkeit**: Sicherstellung der vorgesehenen Nutzbarkeit eines IT-Systems
   - Bedrohung Beispiel: Stören der Webex Verbindungen

5. **Autorisierung**: Freischaltung der eingeräumten Rechte für eine erfolgreich authentifizierte Person
   - Bedrohung Beispiel: Freischalten von kostenpflichtigen Features in Software

6. **Verbindlichkeit**: Empfangen/Senden einer Nachricht oder Durchführen einer Handlung kann nicht abgestritten werden.
   - Bedrohung Beispiel: Beschuldigen des autonomen Fahrsystems für Unfall

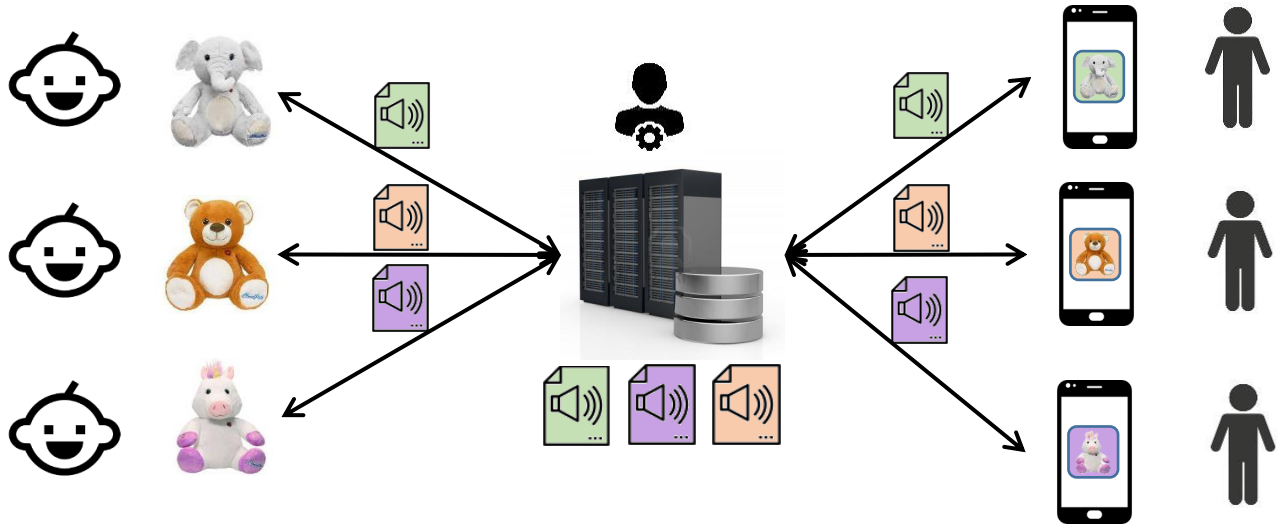
Sicherheitsziele (3/3)

- **Sicherheitsziele** konkretisieren den abstrakten Begriff Sicherheit

Sicherheitsziel	Sicherheitsziel Englisch	Bedrohung	Bedrohung Englisch
Vertraulichkeit	Confidentiality	Veröffentlichung von Informationen	Information Disclosure
Integrität	Integrity	Manipulation	Tampering
Authentizität	Authenticity	Fälschen	Spoofing
Verfügbarkeit	Availability	Störung des Betriebs	Denial-of-Service
Autorisierung	Authorization	Erhöhung von Rechten	Elevation of Privileges
Verbindlichkeit	Non-Repudiation	Abstreiten von Aktionen	Repudiation

- Verschiedene gängige Kombinationen von Sicherheitszielen:
  - **CIA: C**onfidentiality, **I**ntegrity, **A**vailability
  - **CIAA:** CIA + **A**uthenticity
  - **STRIDE**: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privileges

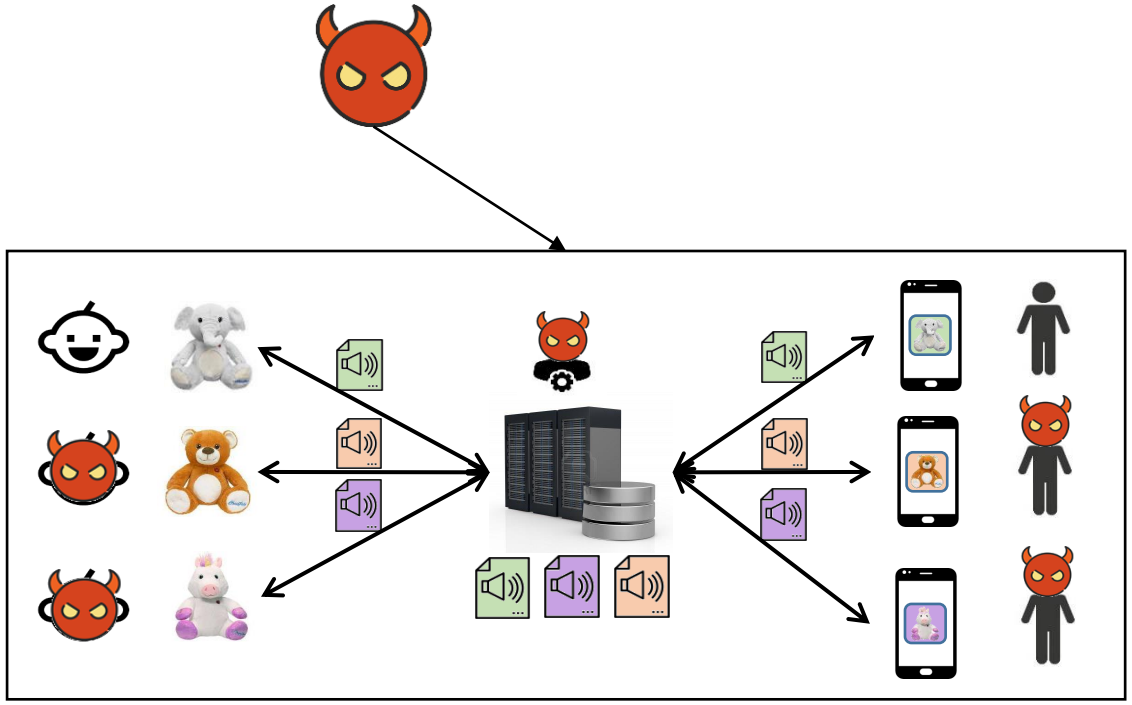
Bedrohungsanalyse CyberPets
CyberPets Schutzbedarf



Asset	Vertraulichkeit	Integrität	Authentizität	Verfügbarkeit	Autorisierung	Verbindlichkeit
Audiodaten	Ja (K&E)	Ja (K&E)	Ja (K&E)	Ja (K&E)	Nein	Ja (U)
Infrastruktur	Nein	Ja (U)	Nein	Ja (U)	Ja (U)	Nein

Bedrohungsanalyse CyberPets
Angreifer*innen und Zugriffspotential

Angreifer*in	Zugriffspotential
Externe Angreifer*in	Zugriff via öffentlichen Kanälen
Nutzende	Zugriff auf eigene Audiodaten sowie Smartphone und Spielzeug
Admins	Tiefer administrativer Zugriff auf Infrastruktur



Bedrohungsanalyse CyberPets

Hochschule Fulda
University of Applied Sciences

Asset	Schutzziel	Angreifer*in	Bedrohungen
Audiodaten	**Vertraulichkeit / Integrität / Authentizität / Autorisierung**	Externe Angreifer*in	Schwachstellen in der öffentlich erreichbaren Infrastruktur suchen um Audiodaten zu lesen / ändern / fälschen
		Nutzende	Zugriff auf Audiodaten anderer Nutzender via bestehender Schnittstellen auf dem Smartphone und dem Spielzeug
		Admins	Rechte ausnutzen um Audiodaten auszulesen / zu ändern / zu fälschen; Infrastruktur ändern
	Verfügbarkeit	Externe Angreifer*in	DoS gegen öffentlich erreichbares System
		Nutzende	Hohe Last auf die Infrastruktur via bestehender Schnittstellen erzeugen
		Admins	System herunterfahren; kritische Komponenten stoppen
	Verbindlichkeit	Nutzende	Kompromittierende Audiodatei auf eigenem Account platzieren. Unternehmen anklagen
		Admins	Kompromittierende Audiodatei auf Account platzieren und Unternehmen bzw. Nutzende anklagen

Weiteres Vorgehen… (Später in LVA)

- **Bisher:** Bedrohung auf nicht-technischem Level
  - Grund: Priorität sollte auf Überblick der Bedrohungen gegen das Systems liegen bevor technisch ins Detail gegangen wird
  - Allerdings sind die abstrakten Bedrohungen wenig hilfreich für technische Expert*innen

- **Nächste Schritte (Im Rahmen der LVA):**
  - Tieferes technisches Verständnis der Bedrohungen
  - Identifikation und Evaluierung konkreter technischer Angriffe
  - Design und Evaluierung von Gegenmaßnahmen
  - Entscheidung über Umgang mit Bedrohung (sog. Risikomanagement)

Kritik an Bedrohungsanalyse

Negativ

- Modellierung ist nicht trivial und subjektiv
- Ergebnisse manchmal realitätsfern
- Läuft oft auf Reverse-Engineering der Standardmaßnahmen hinaus
- Zeitaufwändig und wenig Benefit für Expert*innen mit Erfahrung in IT-Sicherheit

Positiv

- Bietet Grundlage zur Diskussion und einheitlichem Verständnis
- Hilft Personen die das System nicht kennen
- Ableitung schafft Verständnis gegenüber Management
- Wird anerkannt bei rechtlichen Vorgaben für IT-Sicherheitsmaßnahmen

Zusammenfassung

- Um IT-Sicherheit angemessen zu realisieren müssen bekannt sein:
  - **potentielle Angreifer*innen,** deren Motivationen und technisches Vorgehen
  - Der Umfang und Schutzbedarf des **eigenen Systems**

- **Sicherheitsziele:** Vertraulichkeit**,** Integrität, Authentizität, Verfügbarkeit, Autorisierung, Verbindlichkeit

- Die **Bedrohungsanalyse** liefert abstrakte Bedrohungen gegen das jeweilige System

- **Ausblick:** Technische Angriffe und Sicherheitsmechanismen für die jeweiligen Bereiche (angefangen mit Kryptographie)

Referenzen

[BSI]: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html

[PRIV]: Preise von Daten im Darknet: https://www.privacyaffairs.com/dark-web-price-index-2021/

[HEISE]: https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html

[FCA]: Jeep Cherokee Hack: http://www.illmatics.com/Remote%20Car%20Hacking.pdf

[PET]: Unverschlüsselte Datenübertragung von Kinderspielzeug: https://www.heise.de/security/meldung/Cloudpets-2-2-Millionen-Sprachdateien-von-Kinderspielzeug-offen-im-Netz-3637923.html

[BB]: BugBounty Höhe verschiedener Firmen: https://www.guru99.com/bug-bounty-programs.html

[SECENG]: R. Andersson: Security Engineering. 2te Auflage von 2008 online verfügbar: https://www.cl.cam.ac.uk/~rja14/book.htm