Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

SECURITY
Risikomanagement

May 10, 2024

Marc Stöttinger

More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk.

Bruce Schneier

MOTIVATION RISKOMANAGEMENT

→ **Bisher:** Aufsetzen eines ISMS und Durchführen des PDCA Zyklus zum strukturierten Behandeln von IT-Sicherheit

→ **Beispiel:** Kernprozess "Notenpflege in COMPASS"
- → Plan: Identifikation und Priorisierung der IT-Sicherheitsmaßnahmen
- → Do: Implementierung des Backup Systems
- → Check: Verifikation der Backup Lösung
- → Act: Implementierung der ISMS Verbesserungen

MOTIVATION RISKOMANAGEMENT

→ **Bisher:** Aufsetzen eines ISMS und Durchführen des PDCA Zyklus zum strukturierten Behandeln von IT-Sicherheit

→ **Beispiel:** Kernprozess "Notenpflege in COMPASS"

- → Plan: Identifikation und Priorisierung der IT-Sicherheitsmaßnahmen
- → Do: Implementierung des Backup Systems
- → Check: Verifikation der Backup Lösung
- → Act: Implementierung der ISMS Verbesserungen

Prio	Maßnahme
?	Backupsystem
?	Schulung
?	Multi-Faktor Authentifizierung

MOTIVATION RISKOMANAGEMENT

→ **Bisher:** Aufsetzen eines ISMS und Durchführen des PDCA Zyklus zum strukturierten Behandeln von IT-Sicherheit

→ **Beispiel:** Kernprozess "Notenpflege in COMPASS"
- → Plan: Identifikation und Priorisierung der IT-Sicherheitsmaßnahmen
- → Do: Implementierung des Backup Systems
- → Check: Verifikation der Backup Lösung
- → Act: Implementierung der ISMS Verbesserungen

→ **Heute:**
- → Inhalt: Identifikation und Priorisierung von Maßnahmen im Plan Schritt

Prio	Maßnahme
?	Backupsystem
?	Schulung
?	Multi-Faktor Authentifizierung

WIRTSCHAFTLICHKEIT VON IT-SICHERHEIT

- → Einsatz von IT-Systemen soll den Profit erhöhen, indem z.B.
  - → Geschäftsprozesse optimiert und Kosten reduziert werden
  - → der Umsatz gesteigert wird

Folie basiert auf der Veröffentlichung: Norbert Pohlmann: Wirtschaftlichkeit von Cyber-Sicherheit

WIRTSCHAFTLICHKEIT VON IT-SICHERHEIT

- → Einsatz von IT-Systemen soll den Profit erhöhen, indem z.B.
  - → Geschäftsprozesse optimiert und Kosten reduziert werden
  - → der Umsatz gesteigert wird

- → IT-Sicherheitsmaßnahmen reduzieren typischerweise weder Kosten noch steigern sie den Umsatz

Folie basiert auf der Veröffentlichung: Norbert Pohlmann: Wirtschaftlichkeit von Cyber-Sicherheit

WIRTSCHAFTLICHKEIT VON IT-SICHERHEIT

- Einsatz von IT-Systemen soll den Profit erhöhen, indem z.B.
  - Geschäftsprozesse optimiert und Kosten reduziert werden
  - der Umsatz gesteigert wird

- IT-Sicherheitsmaßnahmen reduzieren typischerweise weder Kosten noch steigern sie den Umsatz

- IT-Sicherheit verhindert Schäden, die mit gewisser Eintrittswahrscheinlichkeit anfallen

Folie basiert auf der Veröffentlichung: Norbert Pohlmann: Wirtschaftlichkeit von Cyber-Sicherheit

WIRTSCHAFTLICHKEIT VON IT-SICHERHEIT

- → Einsatz von IT-Systemen soll den Profit erhöhen, indem z.B.
  - → Geschäftsprozesse optimiert und Kosten reduziert werden
  - → der Umsatz gesteigert wird

- → IT-Sicherheitsmaßnahmen reduzieren typischerweise weder Kosten noch steigern sie den Umsatz

- → IT-Sicherheit verhindert Schäden, die mit gewisser Eintrittswahrscheinlichkeit anfallen

- → Benötigt wird also eine Wirtschaftlichkeitsbetrachtung von IT-Sicherheit, die potentielle Schäden ihrer Eintrittswahrscheinlichkeit gegenüberstellt

Folie basiert auf der Veröffentlichung: Norbert Pohlmann: Wirtschaftlichkeit von Cyber-Sicherheit

RISIKOMANAGEMENT AM BEISPIEL VERSICHERUNGEN

Verschiedene Versicherungsmodelle für Fahrzeuge

→ Haftpflicht

Quelle: https://www.check24.de/kfz-versicherung/automarken/bmw/1er/

RISIKOMANAGEMENT AM BEISPIEL VERSICHERUNGEN

Verschiedene Versicherungsmodelle für Fahrzeuge

- → Haftpflicht
- → Teilkaskoversicherung

Quelle: https://www.check24.de/kfz-versicherung/automarken/bmw/1er/

RISIKOMANAGEMENT AM BEISPIEL VERSICHERUNGEN

Verschiedene Versicherungsmodelle für Fahrzeuge

- → Haftpflicht
- → Teilkaskoversicherung
- → Vollkaskoversicherung

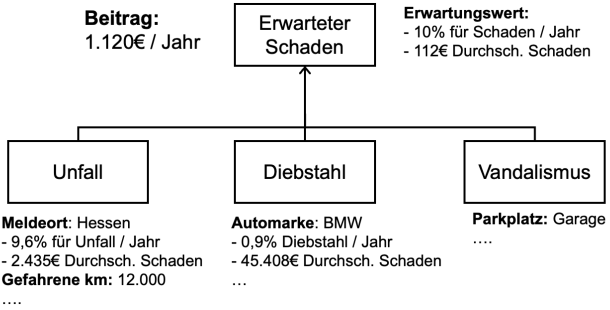
Quelle: https://www.check24.de/kfz-versicherung/automarken/bmw/1er/

RISIKOMANAGEMENT AM BEISPIEL VERSICHERUNGEN

Verschiedene Versicherungsmodelle für Fahrzeuge

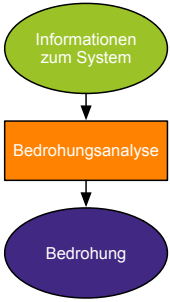
- → Haftpflicht
- → Teilkaskoversicherung
- → Vollkaskoversicherung

Quelle: https://www.check24.de/kfz-versicherung/automarken/bmw/1er/



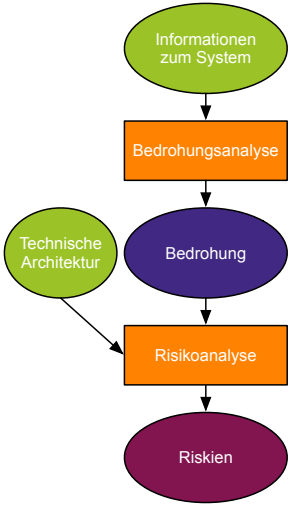
BEDROHUNGS- UND RISIKOANALYSE (TARA)

- → Eine **Bedrohungen** ist ein Umstand, der zu einem Schaden führen könnte
  - → Beispiel: Passwort raten
- → Eine **Gefährdung** ist eine Bedrohung, die konkret eine Schwachstelle ausnutzt
  - → Beispiel: Angreifer rät schwaches Passwort



BEDROHUNGS- UND RISIKOANALYSE (TARA)

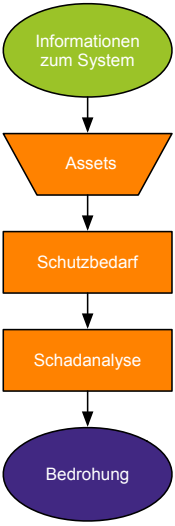
- → Eine **Bedrohungen** ist ein Umstand, der zu einem Schaden führen könnte
  - → Beispiel: Passwort raten
- → Eine **Gefährdung** ist eine Bedrohung, die konkret eine Schwachstelle ausnutzt
  - → Beispiel: Angreifer rät schwaches Passwort
- → Ein **Risiko** ist die Kombination aus dem Ausmaß des Schadens einer Bedrohung und deren Eintrittswahrscheinlichkeit
- → Die **Bedrohungs- und Risikoanalyse** (auch **T**hreat **A**nalysis and **R**isk **A**ssessment, TARA) ist ein strukturierter Vorgang, um Risiken zu identifizieren und priorisieren



BEDROHUNGSANALYSE

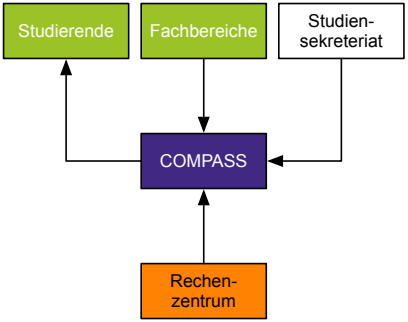
- Eine **Bedrohungsanalyse** als ein strukturierter Prozess, um potentielle Bedrohungen möglichst vollständig zu identifizieren

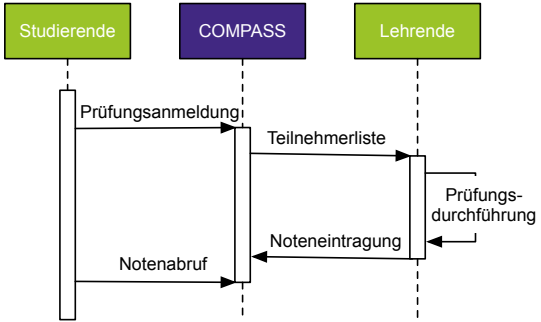
- Vorgehen bei der Bedrohungsanalyse:
  - Welche Vermögenswerte (**Assets**) sind am System beteiligt
  - Welchen **Schutzbedarf** haben die Assets?
  - Wie hoch ist der **Schaden** bei Verlust des Schutzbedarfs?
  - Was sind abstrakte **Bedrohungen**?



TECHNISCHE VORRAUSETZUNG - KERNPROZESS LEHRE UND PRÜFUNG

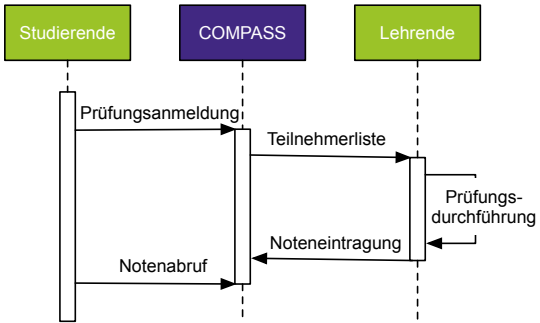
- Kernprozess Lehre und Prüfungen mit Use-Cases
  - Studierende melden sich zu einer Prüfung an
  - Lehrende tragen Noten ein
  - Studierende rufen Noten ab





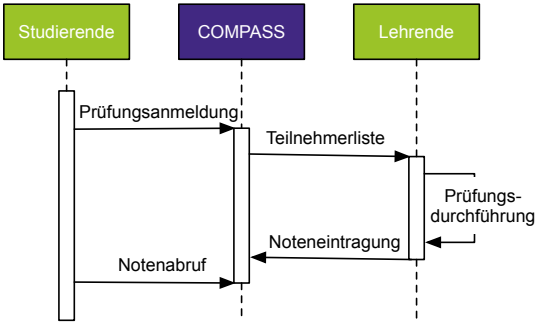
ASSEST IDENTIFIZIEREN

- → **Assets:** Etwas von (ideellem) Wert für die Teilnehmenden
- → Use-Cases für Lehre und Prüfung
  - → Prüfungsanmeldung
  - → Notenmanagement



ASSEST IDENTIFIZIEREN

- → **Assets:** Etwas von (ideellem) Wert für die Teilnehmenden
- → Use-Cases für Lehre und Prüfung
  - → Prüfungsanmeldung
  - → Notenmanagement
- → Assets für Lehre und Prüfung
  - → Noten (Daten)
  - → Prüfungsanmeldungen (Daten)
  - → COMPASS Funktionen (System)



SCHUTZBEDARFS- UND SCHADENSANALYSE

- → Der Schutzbedarf liefert eine Unterteilung für mögliche Schäden an Assets
  - → Unterteilung anhand ausgewählter Sicherheitsziele (z.B. CIA, CIAA, STRIDE, ...)

- → Für jede Kombination aus (Sicherheitsziel x Asset) sollte der mögliche Schaden mittels Schadensnormen (z.B. HEAVENS Standard) abgeschätzt werden

[HEAVENS] Bewertung	Beschreibung
Keine	Keine Verluste
Niedrige	Geringe Verluste
Mittel	Tolerlierbare Verluste
Hoch	Substantielle Verluste
Kritisch	Verluste bedrohen Existenz

SCHUTZBEDARFS- UND SCHADENSANALYSE

- → Der Schutzbedarf liefert eine Unterteilung für mögliche Schäden an Assets
  - → Unterteilung anhand ausgewählter Sicherheitsziele (z.B. CIA, CIAA, STRIDE, ...)

- → Für jede Kombination aus (Sicherheitsziel x Asset) sollte der mögliche Schaden mittels Schadensnormen (z.B. HEAVENS Standard) abgeschätzt werden

- → Beispiel: Verfügbarkeit der Noten
  - → Studierenden könnten das Studium nicht abschließen
  - → Imageschaden (Rückgang der Studierendenzahlen)
  - → Schaden = Mittel

[HEAVENS] Bewertung	Beschreibung
Keine	Keine Verluste
Niedrige	Geringe Verluste
Mittel	Tolerlierbare Verluste
Hoch	Substantielle Verluste
Kritisch	Verluste bedrohen Existenz

BEDROHUNGSANALYSE COMPASS ERGEBNIS FÜR ASSET NOTEN

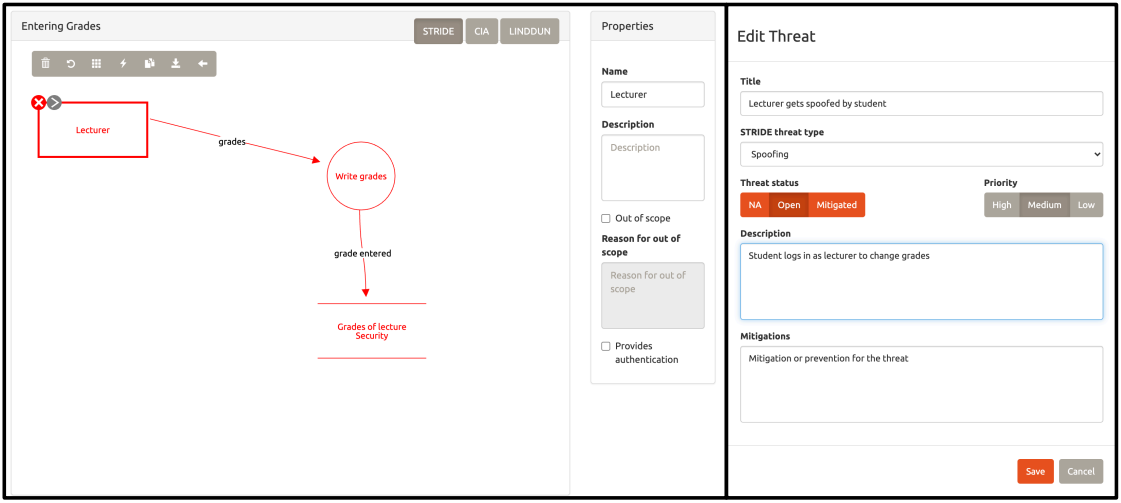
Asset	Sicherheitsziel	Bedrohung	Schaden	Begründung
Noten	Vertraulichkeit	Veröffentlichung der Noten	Hoch	DSGVO Strafzahlungen, Imageschaden
	Integrität	Verfälschung der Noten	Mittel	Klagen durch Studierende, Studierende könnten Studium nicht abschließen, Imageschaden
	Authentizität	Note zu Modul nicht korrekt zugeordnet	Niedrig	Verfälschung des Notendurchschnitts für Studierende
	Verfügbarkeit	Noten nicht mehr verfügbar	Mittel	Studierende können Studium nicht abschließen, Imageschaden
	Autorisierung	Unbefugter Zugriff auf Noten	Hoch	(Verweis auf Vertraulichkeit und Integrität)
	Nicht-Abstreitbarkeit	Leugnung einer Prüfungsleistung	Niedrig	Verbesserung der Note, Studierende nicht exmatrikulierbar

STRIDE: METHODIK

Nutzt die Schutzzielspezifischen Bedrohung und ordnet abstrakt dies einem Basiselement einer Datenfluss-Architektur zu. Die sogenannte **Stride-per-Element** Methode. Somit können Systeme abstrakt modelliert und analysiert werden.

STRIDE Typ	Datentransfer	Speicher	Prozess	Actor
Spoofing			x	x
Tampering	x	x	x	
Repudiation	x		x	x
Information Disclosure	x	x	x	
Denial of Service	x	x	x	
Evaluation of Privlages	x	x	x	

STRIDE: BEISPIEL

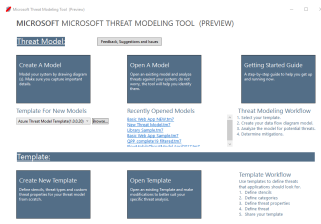


STRIDE: WERKZEUG

Das **Threat Modeling Tool** und **Threat-Dragon Tools** könnenzur Erstellung von Bedrohungsmodellen für die Bedrohungsanalyse genutzt werden.

- → Modellierung des Systems per Datenflussgraph
- → Bedrohungsanalyse mittels Stride-per-Element Ansatz
- → Tools sind lizenzfrei verfügbar:
  - → Threat Modeling Tool (nur für Windows) **[Download]**
  - → Threat-Dragon (für Windows, Linux, Mac) **[Download]**

Quelle: https://owasp.org/www-project-threat-dragon/



Quelle: https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool-getting-started

BEDROHUNGSMODELL - DREAD

Das DREAD Modell wird genutzt, um potentielle Bedrohungen besser zu Kategorisierung und zu bewerten. Dabei wird die Bedrohungen nach folgenden Kriterien bewertet:

→ **D**amage (Schaden):
Wie schwer ist der versuchte Schaden durch den Angriff?

BEDROHUNGSMODELL - DREAD

Das DREAD Modell wird genutzt, um potentielle Bedrohungen besser zu Kategorisierung und zu bewerten. Dabei wird die Bedrohungen nach folgenden Kriterien bewertet:

- → **D**amage (Schaden):
  Wie schwer ist der versuchte Schaden durch den Angriff?
- → **R**eproducibility (Reproduzierbarkeit):
  Wie leicht lässt sich der Angriff reproduzieren/anwenden/wiederholen?

BEDROHUNGSMODELL - DREAD

Das DREAD Modell wird genutzt, um potentielle Bedrohungen besser zu Kategorisierung und zu bewerten. Dabei wird die Bedrohungen nach folgenden Kriterien bewertet:

- → **D**amage (Schaden):
  Wie schwer ist der versuchte Schaden durch den Angriff?
- → **R**eproducibility (Reproduzierbarkeit):
  Wie leicht lässt sich der Angriff reproduzieren/anwenden/wiederholen?
- → **E**xploitability (Ausnutzbarkeit):
  Wie schwer ist es, den Angriff durchzuführen?

BEDROHUNGSMODELL - DREAD

Das DREAD Modell wird genutzt, um potentielle Bedrohungen besser zu Kategorisierung und zu bewerten. Dabei wird die Bedrohungen nach folgenden Kriterien bewertet:

- → **D**amage (Schaden):
  Wie schwer ist der versuchte Schaden durch den Angriff?
- → **R**eproducibility (Reproduzierbarkeit):
  Wie leicht lässt sich der Angriff reproduzieren/anwenden/wiederholen?
- → **E**xploitability (Ausnutzbarkeit):
  Wie schwer ist es, den Angriff durchzuführen?
- → **A**ffected users (Betroffene):
  Wie viele Personen/Systeme/Komponenten sind vom Angriff betroffen?

BEDROHUNGSMODELL - DREAD

Das DREAD Modell wird genutzt, um potentielle Bedrohungen besser zu Kategorisierung und zu bewerten. Dabei wird die Bedrohungen nach folgenden Kriterien bewertet:

- → **D**amage (Schaden):
  Wie schwer ist der versuchte Schaden durch den Angriff?
- → **R**eproducibility (Reproduzierbarkeit):
  Wie leicht lässt sich der Angriff reproduzieren/anwenden/wiederholen?
- → **E**xploitability (Ausnutzbarkeit):
  Wie schwer ist es, den Angriff durchzuführen?
- → **A**ffected users (Betroffene):
  Wie viele Personen/Systeme/Komponenten sind vom Angriff betroffen?
- → **D**iscoverability (Auffindbarkeit):
  Wie einfach kann die Angriffsprozedur gefunden werden?

BEWERTUNGSBEISPIEL - DREAD

Bewertung	Gering	Mittel	Hoch
Damage: Schaden	Verarbeitung unbedeutender Information ist möglich	Verbreitung relevanter Informationen ist möglich	Sicherheitslücke untergraben und vollständige Bescheinigungen erlangt
Reproducibility: Reproduzierbarkeit	Nur mit Kenntnis der Sicherheitslücke schwer reproduzierbar	Angriff kann innerhalb eines bestimmten Zeitfensters reproduziert werden	Angriff kann jederzeit reproduziert werden.
Exploitability: Ausnutzbarkeit	Nur Experten mit Fachwissen können den Angriff durchführen	Erfahrene Programmierer können den Angriff ausführen	Programmieranfänger kann den Angriff in kurzer zeit durchführen.
Affected users: Betroffene	Ein sehr geringer Prozentsatz von Benutzern ist betroffen	Einzelne sind betroffen; keine Standardkonfiguration	Alle Benutzer sind betroffen; Standardkonfiguration
Discoverability: Auffindbarkeit	Der Fehler ist unbekannt und es ist unwahrscheinlich, dass Benutzer das Schadenspotential erkennen.	Die Sicherheitslücke befindet sich in einem selten verwendeten Teil des Produkts. Die bösartige Verwendbarkeit ist nur mit einigem Aufwand erkennbar.	Angriff wird über öffentlich zugängliche Medien erklärt. Die Sicherheitslücke findet sich in einer viel verwendeten Funktion und ist leicht wahrnehmbar.

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN (1/2)

Ermittlung der Eintrittswahrscheinlichkeit am Beispiel der Versicherungen und von COMPASS

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN (1/2)

Ermittlung der Eintrittswahrscheinlichkeit am Beispiel der Versicherungen und von COMPASS

→ **Beispiel Versicherungen**
Unfall

- → Rückschluss aus empirischen Datenmengen (Unfälle / Jahr)
- → Unfallsituationen vergleichbar
- → Unfall wird (meist) nicht durch Menschen beabsichtigt

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN (1/2)

Ermittlung der Eintrittswahrscheinlichkeit am Beispiel der Versicherungen und von COMPASS

→ **Beispiel Versicherungen**
Unfall

- → Rückschluss aus empirischen Datenmengen (Unfälle / Jahr)
- → Unfallsituationen vergleichbar
- → Unfall wird (meist) nicht durch Menschen beabsichtigt

→ **IT-Sicherheit**
Verfügbarkeit der Noten

- → Datenmengen recht klein bis sogar individuell
- → Situation sehr individuell (wer hat Zugriff, wo wird gehostet, ...)
- → Angreifer beabsichtigt Schaden

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN (2/2)

Alternative: Modellierung der Eintrittswahrscheinlichkeit durch Voraussetzungen für einen erfolgreichen Angriff (z.B. aus [HEAVENS])

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN (2/2)

Alternative: Modellierung der Eintrittswahrscheinlichkeit durch Voraussetzungen für einen erfolgreichen Angriff (z.B. aus [HEAVENS])

[HEAVENS] Faktoren	Kritisch(3)	Hoch(2)	Mittel(1)	Niedrig(0)
Zugriffsmöglichkeiten	Internet	Lokales Netzwerk	Systemzugriff	Physischer Zugriff
Expertise	Laie	Kompetent	Experte	Mehrere Experten
Wissen über das Ziel	Öffentlich	Branchenspezifisch	Unternehmensspezifisch	Geheim
Benötigte Geräte	Standard	Spezialisierte Geräte	Speziell Produzierte Geräte	Mehrere Speziell Produzierte Geräte

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN – BEISPIELE

- **Beispiel A:** Phishing eines Passwortes
  - Angreifer identifiziert Opfer via HSRM Homepage
  - Angreifer baut Login-Seite nach und sendet sie an Opfer

Faktor	Phising
Zugriffs-möglichkeiten	Internet (3)
Expertise	Laie (3)
Wissen über das Ziel	Öffentlich (3)
Benötigte Geräte	Standard (3)
Summe	**12**

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN – BEISPIELE

- **Beispiel A:** Phishing eines Passwortes
  - Angreifer identifiziert Opfer via HSRM Homepage
  - Angreifer baut Login-Seite nach und sendet sie an Opfer

- **Beispiel B:** USB-Stick mit Trojaner an COMPASS Server anschließen
  - Angreifer verschafft sich Zugang zum Serverraum
  - Angreifer schließt bösartigen USB Stick an, der einen Trojaner installiert

Faktor	Phising
Zugriffs-möglichkeiten	Internet (3)
Expertise	Laie (3)
Wissen über das Ziel	Öffentlich (3)
Benötigte Geräte	Standard (3)
Summe	**12**

EINTRITTSWAHRSCHEINLICHKEITEN VON ANGRIFFEN – BEISPIELE

- → **Beispiel A:** Phishing eines Passwortes
  - → Angreifer identifiziert Opfer via HSRM Homepage
  - → Angreifer baut Login-Seite nach und sendet sie an Opfer
- → **Beispiel B:** USB-Stick mit Trojaner an COMPASS Server anschließen
  - → Angreifer verschafft sich Zugang zum Serverraum
  - → Angreifer schließt bösartigen USB Stick an, der einen Trojaner installiert

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

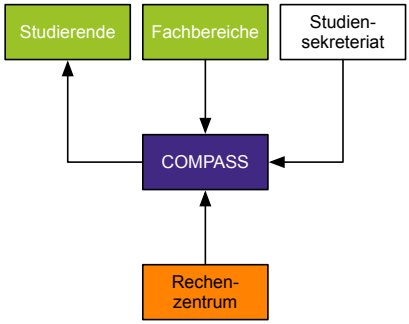
BEISPIEL NOTENPFLEGE VIA COMPASS

- → Die Risikoanalyse setzt Kenntnisse technischer Details voraus
  - → Umso mehr Details bekannt sind, desto besser die Abschätzung
  - → Technisches Verständnis entwickelt sich über die ISMS Zyklen

BEISPIEL NOTENPFLEGE VIA COMPASS

- → Die Risikoanalyse setzt Kenntnisse technischer Details voraus
  - → Umso mehr Details bekannt sind, desto besser die Abschätzung
  - → Technisches Verständnis entwickelt sich über die ISMS Zyklen

- → **Technische Details zu COMPASS**
  - → Die COMPASS Webseite authentifiziert alle User nur via Passwort
  - → Auf dem COMPASS Server existiert ein ssh Zugang für Administratoren
  - → Der Serverraum ist mit einem Gebäudeschlüssel zugänglich



ANGRIFFSBÄUME ZUR ABSCHÄTZUNG DER EINTRITTSWAHRSCHEINLICHKEIT

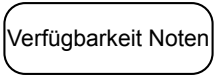
- → Unterschiedlicher Detailgrad der Informationen in der Risikoanalyse
  - → Abstrakte Bedrohung: Verlust der Verfügbarkeit der Noten
  - → Konkrete Angriffe: Phishing oder Anschluss bösartiger Hardware

ANGRIFFSBÄUME ZUR ABSCHÄTZUNG DER EINTRITTSWAHRSCHEINLICHKEIT

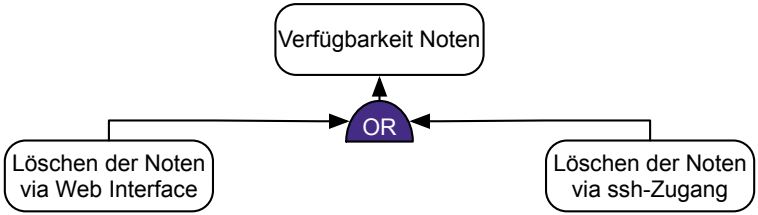
- Unterschiedlicher Detailgrad der Informationen in der Risikoanalyse
  - Abstrakte Bedrohung: Verlust der Verfügbarkeit der Noten
  - Konkrete Angriffe: Phishing oder Anschluss bösartiger Hardware

- Methode zum Verknüpfen der Informationen: **Angriffsbäume**
  - Abstrakte Bedrohungen als Wurzelknoten
  - Konkrete und abschätzbare Angriffe als Blätter
  - Knoten als logische Unterteilung möglicher Angriffe
  - Knoten werden mittels logischer Verknüpfungen (AND oder OR) verbunden

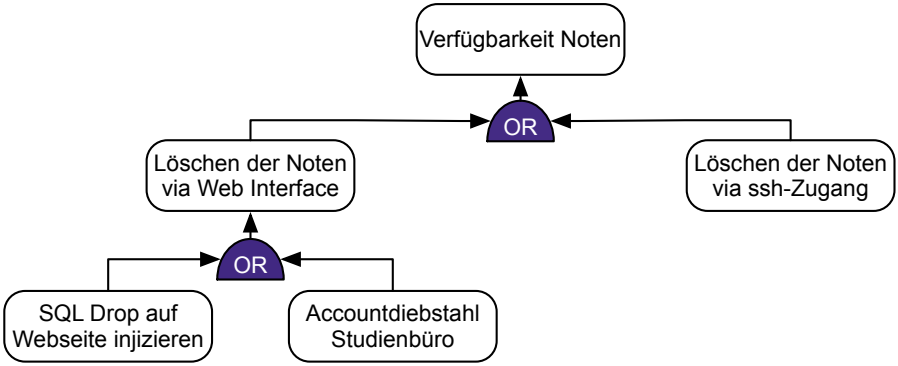
VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



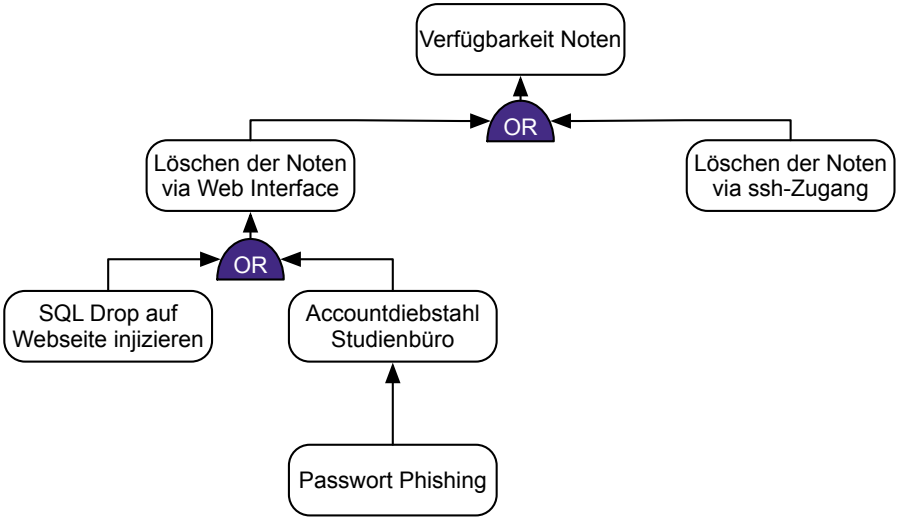
VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



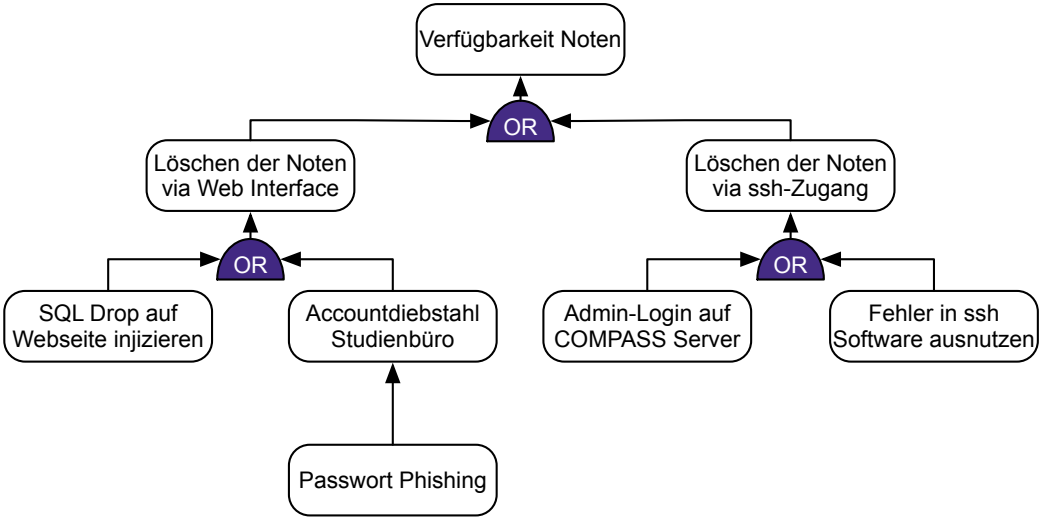
VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



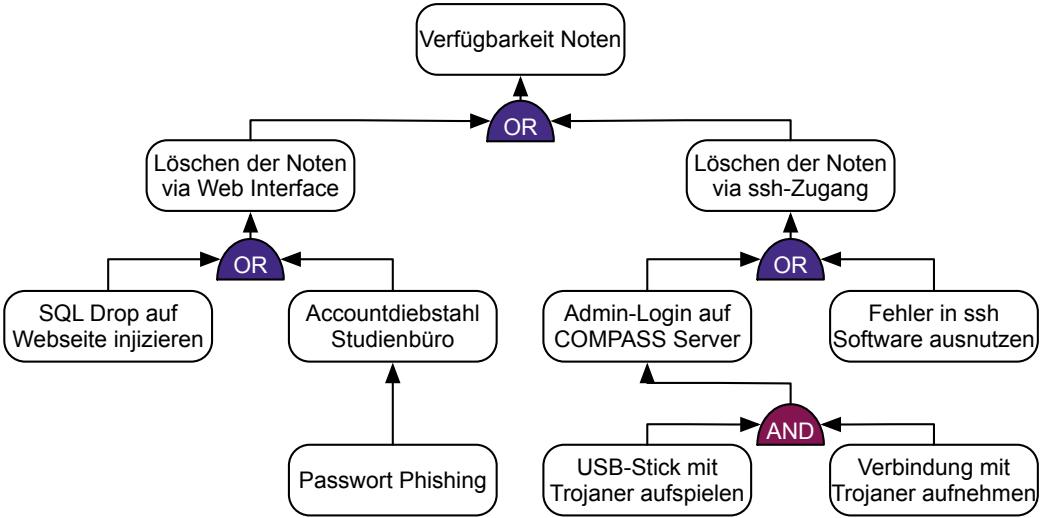
VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



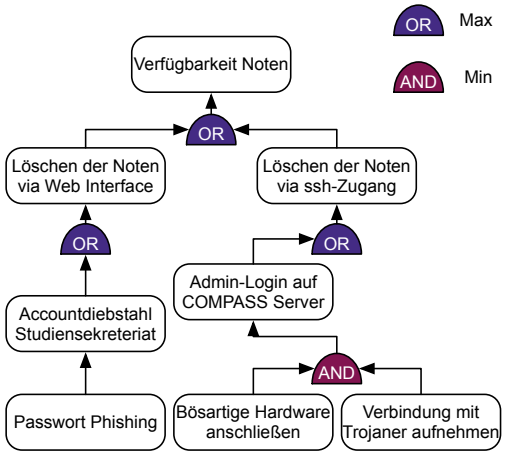
VERFEINERUNG DER BEDROHUNGEN VIA EINES ANGRIFFSBAUMS



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

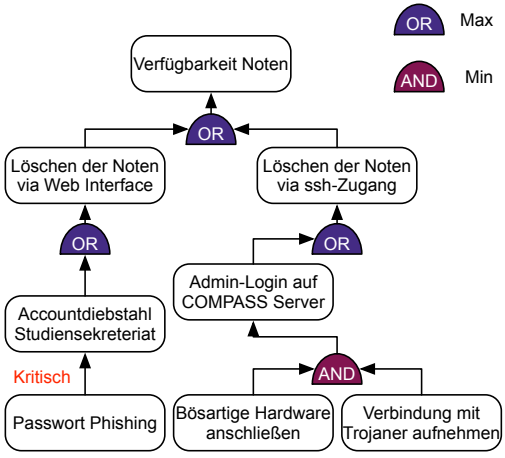
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

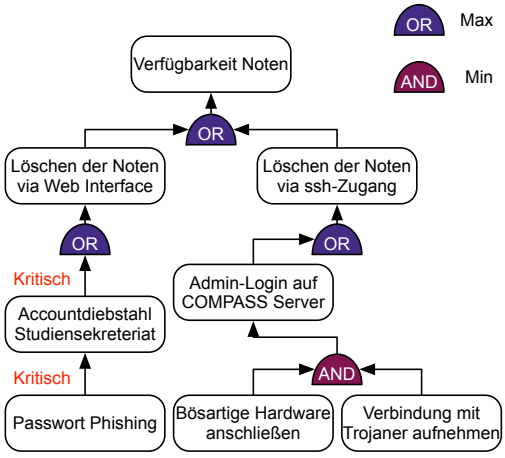
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

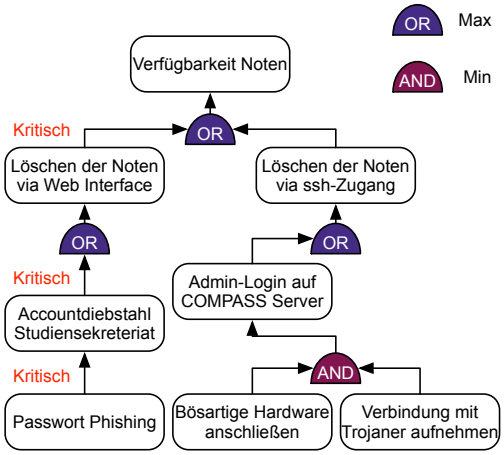
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

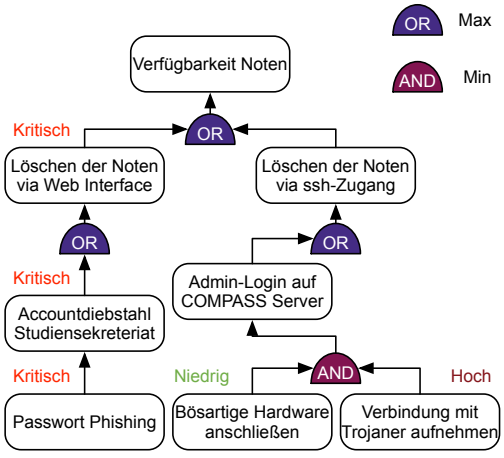
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

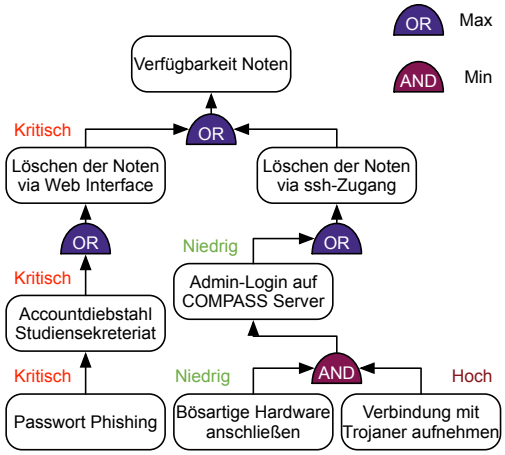
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

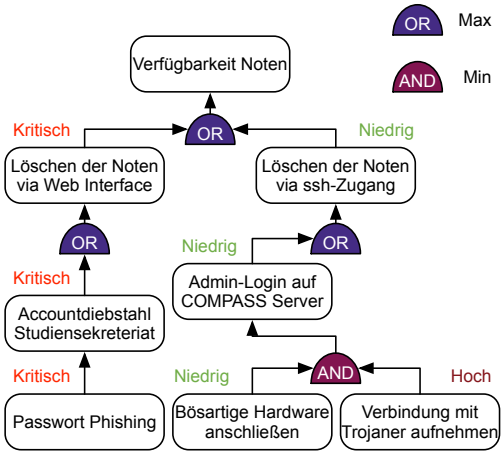
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

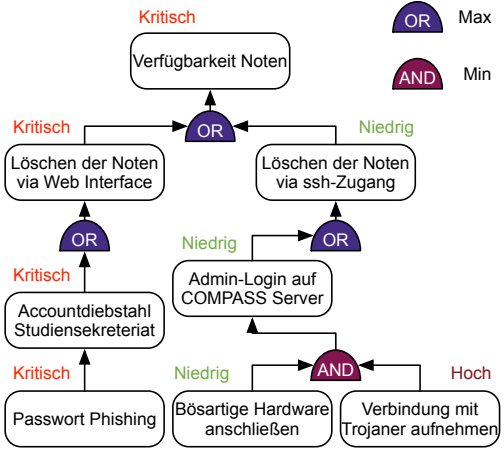
Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



PROPAGIEREN DER EINTRITTSWAHRSCHEINLICHKEIT

Faktor	Phising	USB-Stick mit Trojaner
Zugriffs-möglichkeiten	Internet (3)	Physisch (0)
Expertise	Laie (3)	Kompetent (2)
Wissen über das Ziel	Öffentlich (3)	Unternehmensspez. (1)
Benötigte Geräte	Standard (3)	Spezialisiert (2)
Summe	**12**	**5**

Wert	0-2	3-5	6-8	9-10	11-12
Bewertung	Keine	Niedrig	Mittel	Hoch	Kritisch



BERECHNUNG DES GESAMTRISIKOS

→ Schaden und Eintrittswahrscheinlichkeit werden zum Risiko kombiniert

→ **Risiko**: Verluste der Verfügbarkeit der Noten ist **Hoch**
  → Schaden: Mittel
  → Eintrittswahrscheinlichkeit: Kritisch

Risiko

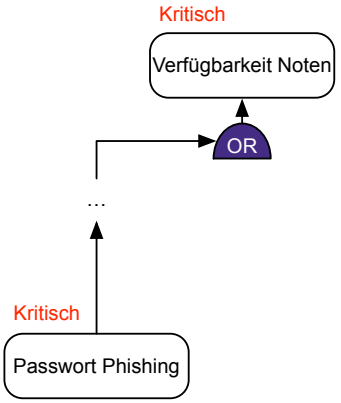
Eintrittswahrscheinlichkeit		Klein	Niedrig	Mittel	Hoch	Kritisch
Schaden	Klein	Klein	Klein	Klein	Klein	Niedrig
	Niedrig	Klein	Niedrig	Niedrig	Niedrig	Mittel
	Mittel	Klein	Niedrig	Mittel	Mittel	Hoch
	Hoch	Klein	Niedrig	Mittel	Hoch	Hoch
	Kritisch	Niedrig	Mittel	Hoch	Hoch	Kritisch

ZIEL DER RISIKOBEHANDLUNG

Die Bedrohungs- und Risikoanalyse liefert eine Liste an Risiken zusammen mit detaillierten Angriffsbäumen

→ **Fokus der Risikobehandlung:** Die am höchsten priorisierten Risiken sinnvoll adressieren

Bedrohung	Bewertung
Noten nicht abrufbar	**Hoch**
Veröffentlichung der Noten	Hoch
Unbefugter Zugriff auf Noten	Hoch
Verfälschung der Noten	Mittel



MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

1. **Mitigieren:** Mechanismen implementieren, um die Eintrittswahrscheinlichkeit und somit das Risiko zu reduzieren (z.B.: Zwei-Faktor Authentifizierung)

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

1. **Mitigieren:** Mechanismen implementieren, um die Eintrittswahrscheinlichkeit und somit das Risiko zu reduzieren (z.B.: Zwei-Faktor Authentifizierung)
2. **Vermeiden:** Schwachstelle entfernen; Funktion nicht umsetzen, Daten oder Zugang entfernen (z.B. Admin Zugang zum COMPASS Server nicht aus dem Internet erreichbar)

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

1. **Mitigieren:** Mechanismen implementieren, um die Eintrittswahrscheinlichkeit und somit das Risiko zu reduzieren (z.B.: Zwei-Faktor Authentifizierung)
2. **Vermeiden:** Schwachstelle entfernen; Funktion nicht umsetzen, Daten oder Zugang entfernen (z.B. Admin Zugang zum COMPASS Server nicht aus dem Internet erreichbar)
3. **Transferieren:** Risiko auf eine andere Instanz übertragen; Schaden durch Verträge abdecken (z.B. Versicherung für Ransomware oder Weitergabe des Risikos an Zulieferer)

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

1. **Mitigieren:** Mechanismen implementieren, um die Eintrittswahrscheinlichkeit und somit das Risiko zu reduzieren (z.B.: Zwei-Faktor Authentifizierung)
2. **Vermeiden:** Schwachstelle entfernen; Funktion nicht umsetzen, Daten oder Zugang entfernen (z.B. Admin Zugang zum COMPASS Server nicht aus dem Internet erreichbar)
3. **Transferieren:** Risiko auf eine andere Instanz übertragen; Schaden durch Verträge abdecken (z.B. Versicherung für Ransomware oder Weitergabe des Risikos an Zulieferer)
4. **Akzeptieren:** Keine Aktionen durchführen (z.B. sinnvoll bei niedrigem Risiko)

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Es gibt verschiedene Möglichkeiten mit einem Risiko umzugehen

1. **Mitigieren:** Mechanismen implementieren, um die Eintrittswahrscheinlichkeit und somit das Risiko zu reduzieren (z.B.: Zwei-Faktor Authentifizierung)
2. **Vermeiden:** Schwachstelle entfernen; Funktion nicht umsetzen, Daten oder Zugang entfernen (z.B. Admin Zugang zum COMPASS Server nicht aus dem Internet erreichbar)
3. **Transferieren:** Risiko auf eine andere Instanz übertragen; Schaden durch Verträge abdecken (z.B. Versicherung für Ransomware oder Weitergabe des Risikos an Zulieferer)
4. **Akzeptieren:** Keine Aktionen durchführen (z.B. sinnvoll bei niedrigem Risiko)

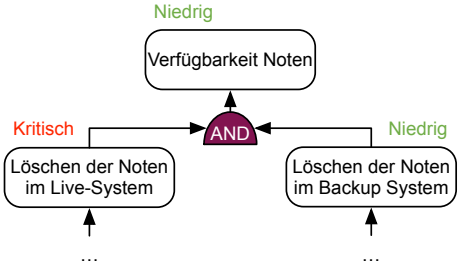
→ Entscheidung über Umgang mit Risiko muss von Person mit entsprechender Befugnis getroffen werden

MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

→ Verschiedene Möglichkeiten im Beispiel Verfügbarkeit der Noten

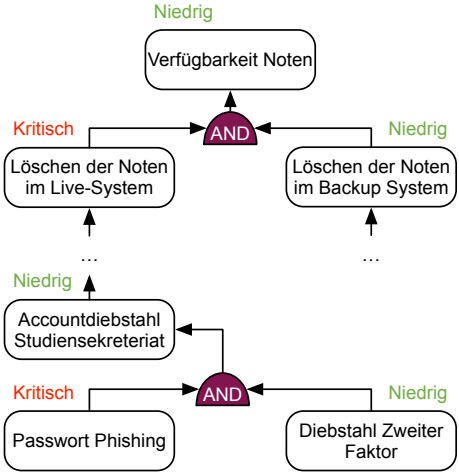
MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

- → Verschiedene Möglichkeiten im Beispiel Verfügbarkeit der Noten
  - → Implementierung eines Backup Systems



MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

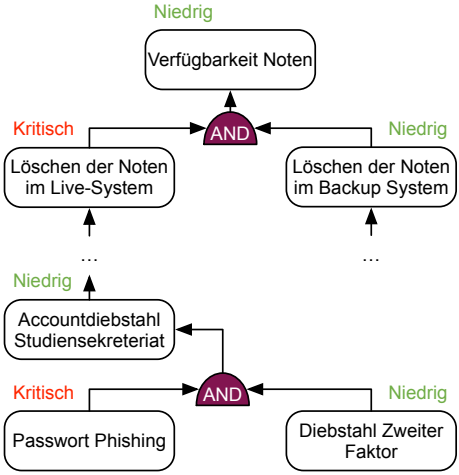
- → Verschiedene Möglichkeiten im Beispiel Verfügbarkeit der Noten
  - → Implementierung eines Backup Systems
  - → Implementierung einer 2-Faktor Authentifizierung (z.B. Smartphone)



MÖGLICHKEITEN ZUR RISIKOBEHANDLUNG

- → Verschiedene Möglichkeiten im Beispiel Verfügbarkeit der Noten
  - → Implementierung eines Backup Systems
  - → Implementierung einer 2-Faktor Authentifizierung (z.B. Smartphone)

- → Entscheidung zu Maßnahmen hängt u.a. von Umsetzbarkeit, Effektivität und Kosten ab



ZUSAMMENFASSUNG

- → Probleme bei der Wirtschaftlichkeitsbetrachtung von IT-Sicherheit
- → Bedrohungsanalyse mit STRIDE und DREAD
- → Bedrohungs- und Risikoanalyse an einem konkreten Beispiel durchführen
- → Verfeinerung der Risikoanalyse durch Angriffsbäume
- → Möglichkeiten der Risikobehandlung