malean

Herzlich Willkommen zum
7. Cyber Security Roundtable

Threat Modeling in der Praxis:
Agiles Risikomanagement für moderne Cyber Security

malean

7. CYBER SECURITY ROUNDTABLE LIECHTENSTEIN

Gastvortrag Creasoft, Mathias Fasser

Threat Modeling in der Praxis – Agiles Risikomanagement für moderne Cyber Security

Wir sind Creasoft

Individuelle Software und Beratung

Wir begleiten unsere Kunden von der Idee bis zur fertigen Software – persönlich, kompetent und zuverlässig. Software Engineering ist unsere Leidenschaft!

- Gegründet 1993
- 45 Mitarbeitende

Threat Modeling in der Praxis

«Lasst uns das Thema in einer Threat Modeling Session beleuchten.»

Heutige Agenda

1	Was ist Threat Modeling?
2	Eine kurze Threat Modeling Session
3	Was für Tools gibt es?
4	Erfahrungen aus zwei Jahren Praxis

Teil 1

Was ist Threat Modeling?

Threat Modeling ist…

… ein intuitiver **Prozess** zur Identifikation von Bedrohungen und Schwachstellen.

Mit dem Ziel, die daraus resultierenden Risiken priorisiert zu behandeln.

… ein **Framework**, welches einen modularen Baukasten mit unterschiedlichen Tools zur Verfügung stellt.

… in einen einfachen Ablauf, mit **vier aufeinander aufbauenden Schritten** aufgeteilt, wobei jeder Schritt aus einer klaren Aufgabe besteht.

… **vielseitig einsetzbar** und kann in diversen Kontexten und von unterschiedlichen Rollen eingesetzt werden.

Für wen eignet sich Threat Modeling?

«You. Everyone. Anyone who is concerned about the privacy, safety, and security of their system.»

Definition aus dem Threat Modeling Manifest

Ein Tool aus der Technik, mit dem Fokus auf Softwareentwicklung, Systeme, Netzwerke, und Infrastruktur.

Kann aber auch für die Bewertung von organisatorischen Themen (Assets, Lieferketten, Prozesse, Dienstleistungen) und zum klassischen Risikomanagement eingesetzt werden.

Ablauf

What are we working on?

Dokumentiere und visualisiere den Zustand des gewählten Themas, indem ein Modell angelegt wird.

1

What can go wrong?

Identifiziere Bedrohungen und Schwachstellen, basierend auf dem Modell aus Schritt 1.

2

What are we doing about it?

Bewerte die gefundenen Bedrohungen und Schwachstellen aus Schritt 2 und behandle die daraus abgeleiteten Risiken.

3

Have we done a good job?

Validiere die vorherigen Schritte auf Vollständigkeit, Wirksamkeit und Erfolg.

4

Teil 2

Eine kurze Threat Modeling Session

Eine kurze Threat Modeling Session

Vorbereitung

Thema: Review des User Lifecycle Management Prozesses beim KMU „XYZ“ aufgrund des kürzlich starken Personalwachstums.

Scope:
- Joiner-Mover-Leaver Prozess: Neueinstellungen, Interne Wechsel, Austritte.
- Der Mitarbeiter soll stets die richtigen, minimal notwendigen Zugriffsrechte haben.

Out-of-Scope: Rekrutierung, Screening, technische Details

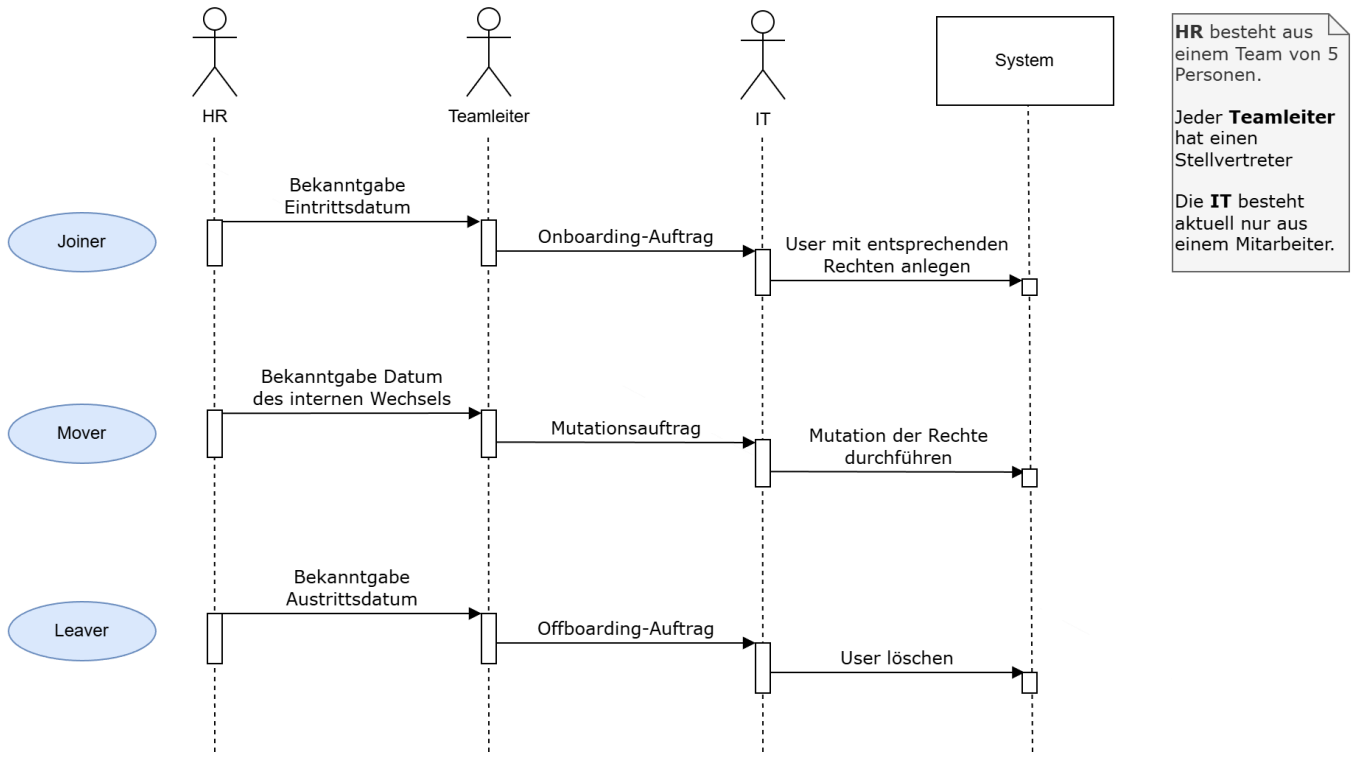
Ziele: Allfällige Bedrohungen und Schwachstellen in den Joiner-Mover-Leaver Prozessen identifizieren, priorisieren und geeignete Massnahmen definieren.

Teilnehmer: Expertenteam (HR, Teamleitung, IT) + Moderator

Schritt 1: What are we working on?

Dokumentiere und visualisiere den Zustand des gewählten Themas, indem ein Modell angelegt wird.

Tool: Sequenzdiagramm

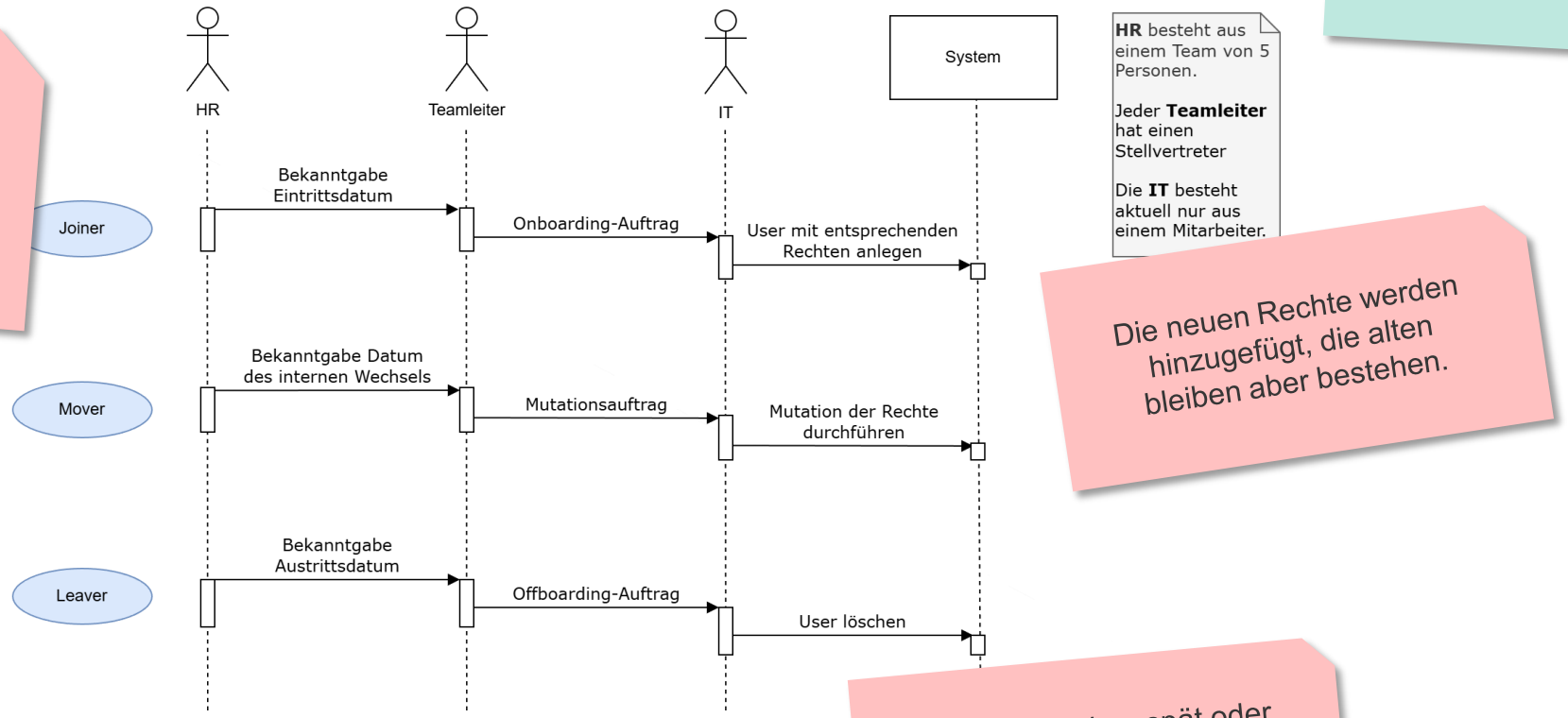


Schritt 2: What can go wrong?

Identifiziere Bedrohungen und Schwachstellen, basierend auf dem Modell aus Schritt 1.

Tool: Brainstorming

Jemand gibt sich als Teamleiter aus und lässt unrechtmässig einen neuen User mit privilegierten Rechten anlegen.



HR besteht aus einem Team von 5 Personen.

Jeder **Teamleiter** hat einen Stellvertreter

Die **IT** besteht aktuell nur aus einem Mitarbeiter.

Die neuen Rechte werden hinzugefügt, die alten bleiben aber bestehen.

Der User wird zu spät oder gar nicht gelöscht.

Schritt 3: What are we doing about it?

Bewerte die gefundenen Bedrohungen und Schwachstellen aus Schritt 2 und behandle die daraus abgeleiteten Risiken.

Tool: Eintrittswahrscheinlichkeit und Schadenspotenzial

	Risiko	*EW	*SP	*RB	Massnahmentyp ELIMINATE, MITIGATE, TRANSFER, ACCEPT	Massnahme(n)	Status READY, IN PROGRESS, IN REVIEW, DONE		
1	Jemand gibt sich als Teamleiter aus und lässt unrechtmässig einen neuen User mit privilegierten Rechten anlegen.	Niedrig (1)	Hoch (3)	3	ELIMINATE	• Die IT holt sich vor dem Ausführen der Änderungen im System nochmals persönlich die Bestätigung von HR und Teamleiter ein.			
2	Die neuen Rechte werden hinzugefügt, die alten bleiben aber bestehen.	Mittel (2)	Mittel (2)	4	MITIGATE	• Stellvertreter aufbauen und Vieraugenprinzip einführen • Regelmässige Reviews einführen			
3	Der User wird zu spät oder gar nicht gelöscht.	Mittel (2)	Mittel (2)	4	MITIGATE	• Die IT informiert das HR nach ausgeführter Aktion. Das HR fragt nach, falls die Meldung ausbleibt. • Regelmässige Reviews einführen			
4									

- *EW = Eintrittswahrscheinlichkeit (1 = niedrig, 2 = mittel, 3 = hoch)
- *SP = Schadenspotenzial (1 = niedrig, 2 = mittel, 3 = hoch)
- *RB = Risikobewertung (EW x SP)

Schritt 4: Have we done a good job?

Validiere die vorherigen Schritte auf Vollständigkeit, Wirksamkeit und Erfolg.

- Findet zeitversetzt statt
- Lassen wir heute ausfallen ☺

Teil 3

Was für Tools gibt es?

Tools

What are we working on?

Tools zur Dokumentation und Visualisierung des Zustands

1

What can go wrong?

Tools zur Identifikation von Bedrohungen und Schwachstellen

2

What are we doing about it?

Tools zur Bewertung von Risiken

3

Have we done a good job?

4

Tools / Schritt 1: What are we working on?

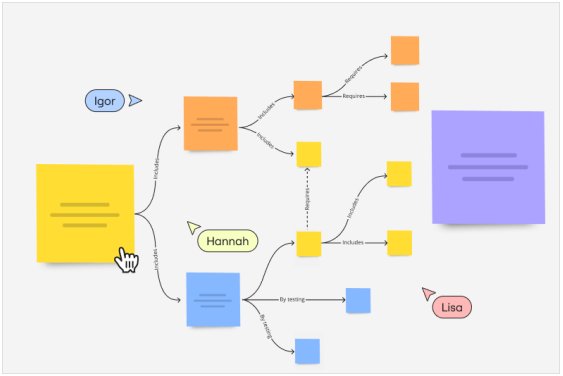
Tools zur Dokumentation und Visualisierung des Zustands

Allgemein

- Mindmap
- Skizze

Infrastruktur

- Netzwerkdiagramm



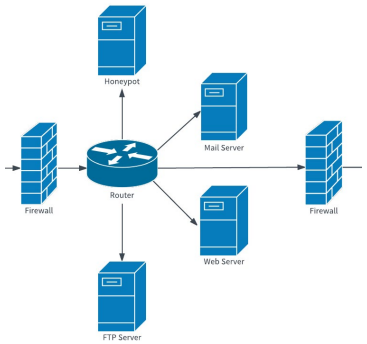
https://miro.com/mind-map/

Softwareentwicklung

- Architekturdiagramm
- Sequenzdiagramm
- Data Flow Diagramm

Organisatorisch

- Darstellung von Assets, Lieferketten, Prozessen, Dienstleistungen
- Risikoliste



https://www.lucidchart.com/

Tools / Schritt 2: What can go wrong?

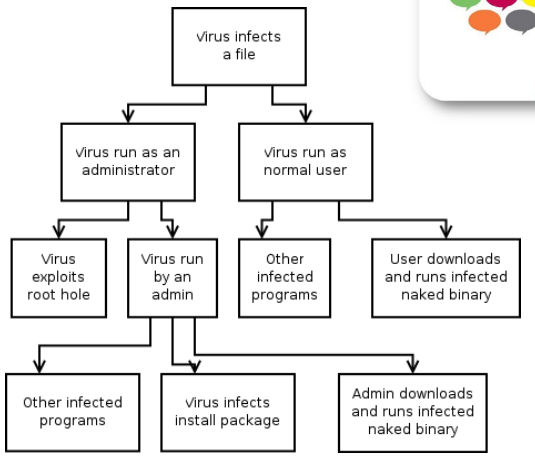
Tools zur Identifikation von Bedrohungen und Schwachstellen

- Brainstorming
- STRIDE
- Attack Trees
- «Elevation of Privilege» Kartenspiel

https://shostack.org/games/elevation-of-privilege

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

https://www.sei.cmu.edu/blog/threat-modeling-12-available-methods/

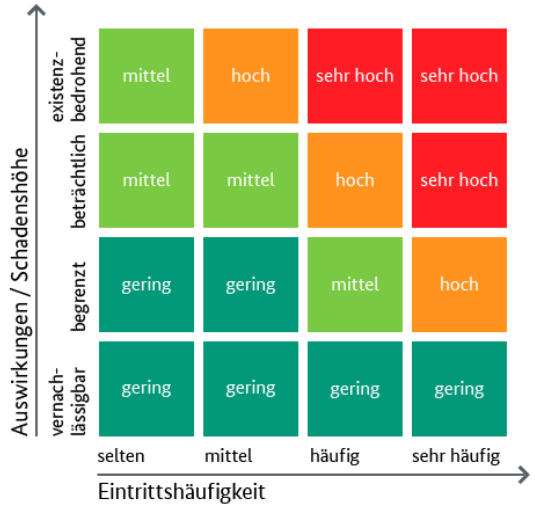


https://en.wikipedia.org/wiki/Attack_tree

Tools / Schritt 3: What are we doing about it?

Tools zur Bewertung von Risiken

- Risikomatrix
  - Eintrittswahrscheinlichkeit und Schadenspotenzial
- DREAD / DREAD-D
  - Damage, Reproducibility, Exploitability, Affected users, Discoverability



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_07/Lektion_7_07_node.html

Teil 4

Erfahrungen aus zwei Jahren Praxis

Vorteile

- «Lasst uns das Thema in einer Threat Modeling Session beleuchten.» **Risikomanagement wird gelebt** und ist keine Pflichtübung.
- Erschafft einen kreativen Raum mit Workshop Charakter → **Bessere Ergebnisse**
- **Strukturiertes Vorgehen, aber trotzdem viel Freiraum**
- **Flexibel**: Verschiedene Tools für verschiedene Anwendungsbereiche
- **Schafft Transparenz** und dokumentiert den Weg und die Gedanken zum Ergebnis
- Ein Tool, aber mehrere Einsatzgebiete und Anwendungsfälle → **weniger Schulungen**

Einsatzgebiete bei Creasoft

Grundsätzlich immer dann, wenn situativ Bedarf besteht:

- Als Teil unseres DevSecOps Prozesses in der Softwareentwicklung
  - In der Planungs- und Designphase von neuen Projekten
  - Bei der Entwicklung und Weiterentwicklung von Features
- Zur Bewertung von Assets, Lieferketten, Prozessen, Dienstleistungen, IT-Infrastruktur und der physischen Sicherheit.

Oder iterativ im Kontext des ISO 27001 Risikomanagements.

Lessons Learned

- Gute **Vorbereitung** und einen erfahrenen **Moderator** ist essenziell.
- Die Risiken müssen so beschrieben sein,
  dass alle Teilnehmer **das Gleiche darunter verstehen**.
- Jede Session basiert auf dem Ergebnis der vorherigen.
  Nachbearbeitung und Vorbereitung durch den Moderator ist essenziell.
- Mit unterschiedlichen Tools experimentieren.
- Ignoriere keine Bedrohungen (aber behandle sie evtl. in einer separaten Session).

Empfehlung

Lektüre zum Thema

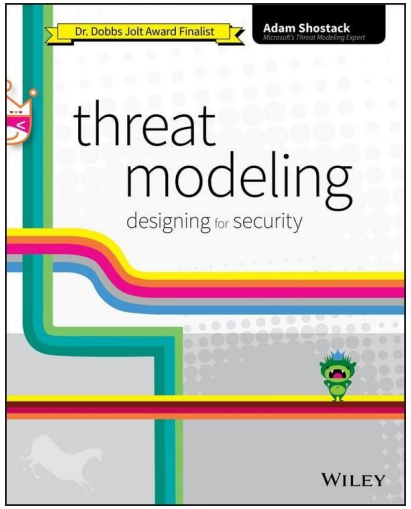
Lesenswertes: Threat Modeling

- https://www.threatmodelingmanifesto.org/
- https://www.threatmodelingmanifesto.org/capabilities/
- https://owasp.org/www-project-threat-modeling/
- https://shostack.org/games/elevation-of-privilege
  (Elevation of Privilege Kartenspiel)
- Buch “Threat Modeling - Designing for Security”
  (Autor: Adam Shostack)

THREAT MODELING MANIFESTO

https://www.threatmodelingmanifesto.org/

https://shostack.org/games/elevation-of-privilege



https://www.orellfuessli.ch/shop/home/artikeldetails/A1030759935

Herzlichen Dank fürs Zuhören!

Gibt es Fragen?

Herzlichen Dank für eure Aufmerksamkeit!

Save the Date

25. Juni 2026

8. Cyber Security Roundtable

Bis bald!

Wir freuen uns darauf, euch beim nächsten Roundtable wiederzusehen und gemeinsam weitere spannende Themen zu erkunden.