'Threat Modeling’: IT-Sicherheitsanforderungen möglichst früh identifizieren und richtig priorisieren

Axel Fasse, SAP SE
October 25, 2023

Public

Denken Sie an Ihre Eigene Software ...

Ist genug für die Sicherheit Ihrer Software getan/geplant?

Denken Sie an Ihre Eigene Software ...

Ist genug für die Sicherheit Ihrer Software getan/geplant?

JA !

Denken Sie an Ihre Eigene Software ...

Ist genug für die Sicherheit Ihrer Software getan/geplant?

Nein !

Denken Sie an Ihre Eigene Software …

Ist genug für die Sicherheit Ihrer Software getan/geplant?

Fällt mir schwer !

Denken Sie an Ihre Eigene Software ...

Ist genug für die Sicherheit Ihrer Software getan/geplant?

An welchen Fakten machen Sie Ihre Antwort fest?

Threat Modeling ...

Praxis

Beispiel

Einführung

- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

Threat Modeling ...

Praxis

Beispiel

Einführung

- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

Threat Modeling ...

- ist **eine strukturierte Methode zum Identifizieren von Bedrohungen** und **daraus abgeleiteten Sicherheitsanforderungen** im Kontext bestimmter Angriffsszenarien.
- wird **initial während der „Design Time“** der Architektur der Anwendung durchgeführt.
- **ermöglicht** eine **Priorisierung der sicherheitsbezogenen Anforderungen** und ein **nachvollziehbares Risikomanagement**.
- ist auch bei agilem Vorgehen nutzbar.

Schritt für Schritt …

Praxis

Beispiel

Einführung

Threat Modeling ...

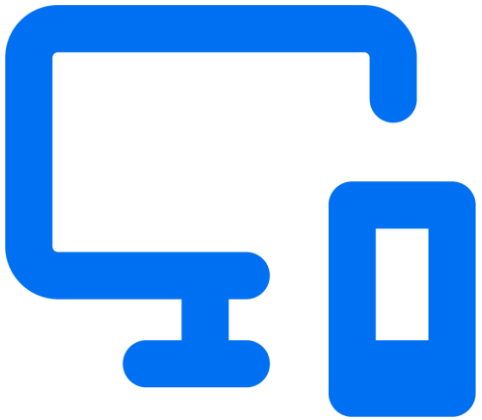
Praxis

Beispiel

Einführung

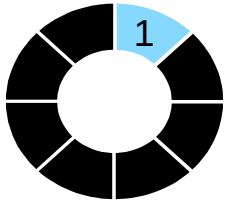
- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

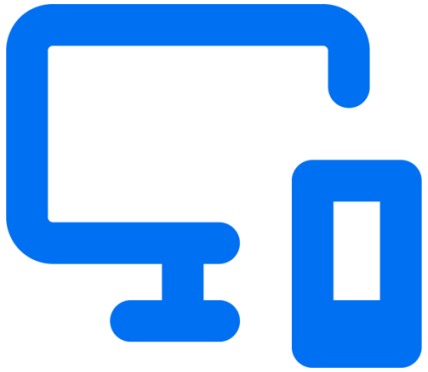
Beispiel - mobiles Kundenstammblatt



- Ein Kundenstammblatt soll dem Außendienst den unmittelbaren Zugriff auf Informationen über einen Kunden mit dessen wichtigsten Eckdaten und aktuellen Aktivitäten ermöglichen.
- Das Kundestammblatt soll auch offline auf mobilen Endgeräten verfügbar sein.

Mögliche schützenswerte Güter

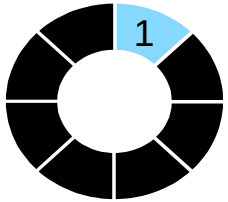


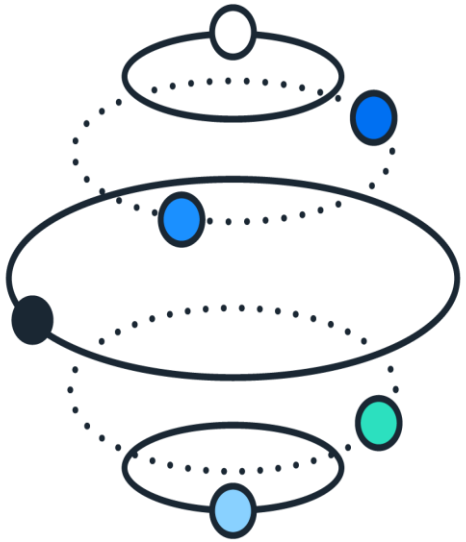


- Daten im Backend
- Mobile Daten, Kundenstammblatt
- Verfügbarkeit des Services
- CPU Last des Servers: BitCoin Mining
- ...

ACHTUNG: Angreife und Verteidiger können durchaus unterschiedliche Auffassung darüber haben, was schützenswert oder eine interessante Beute ist!

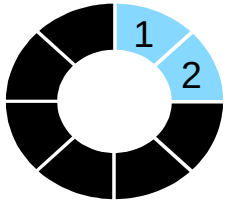
Beispiel - mobiles Kundenstammblatt

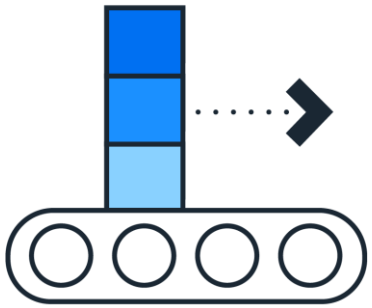




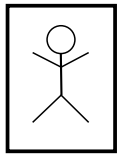
- Daten im Backend und Smartphone
  - Confidentiality = Vertraulichkeit
  - Integrity = Korrektheit
  - Availability = Verfügbarkeit

Architekturmodell



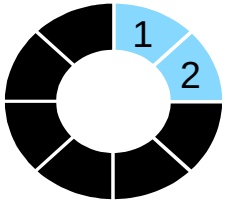


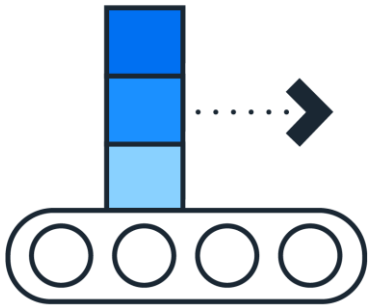
- Gezielt vereinfacht
- Modelliert mit „Fundamental Modeling Concepts“ (FMC)
- Kennzeichnung von „Trust Boundaries“

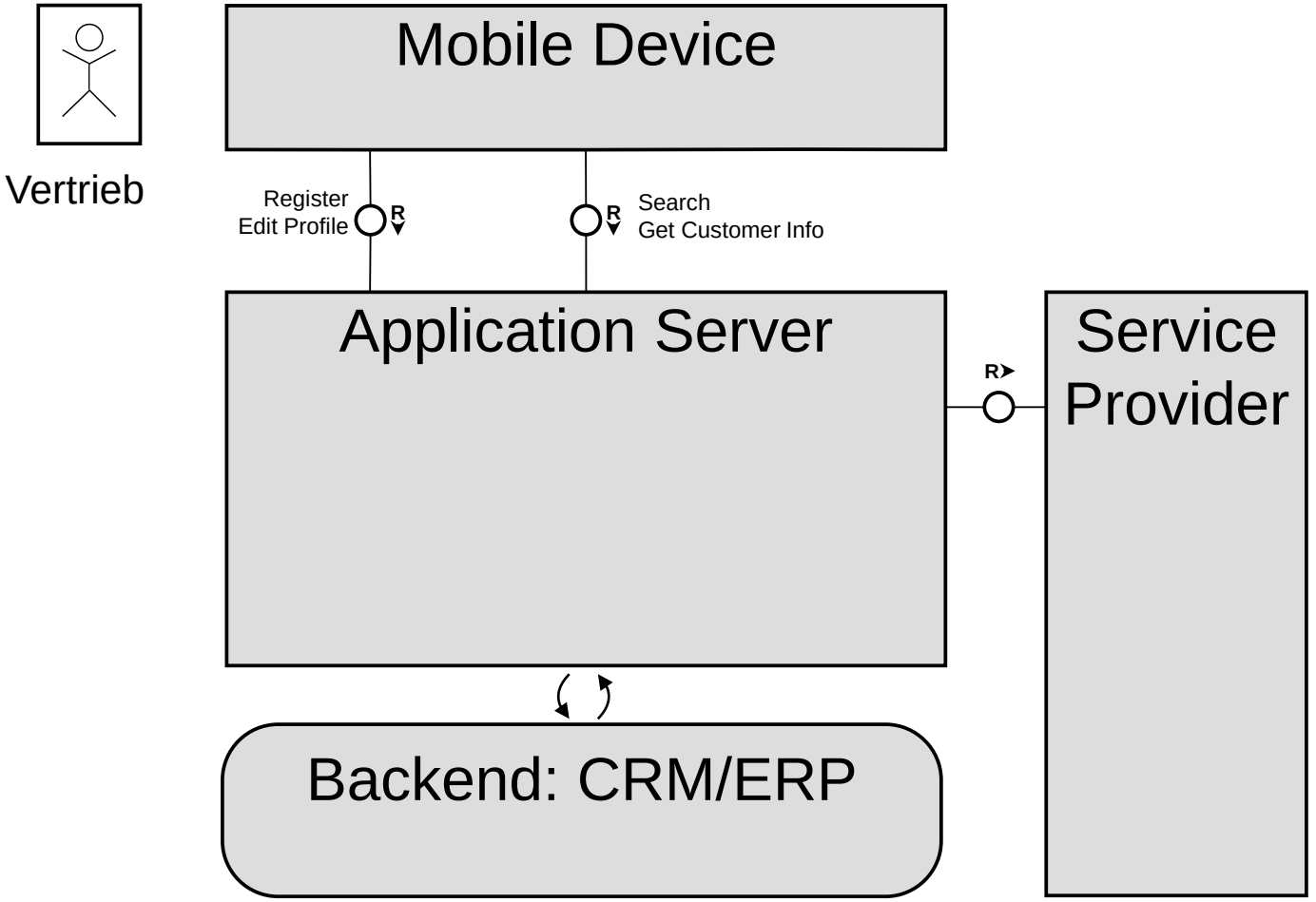
Agent 	**Agenten** verarbeiten Information, nutzen Speicher, kommunizieren über Kanäle
Storage	**Speicher** enthalten Informationen, auf die Agenten zugreifen
	**Kanäle** werden von Agenten genutzt um Informationen zu transportieren

Fundamental Modeling Concepts (FMC) Homepage: http://www.fmc-Modeling.org

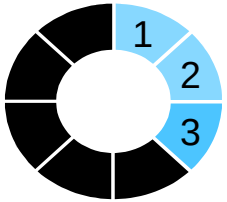
Geeignetes Architekturmodell







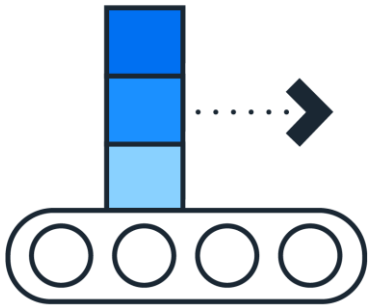
Wichtige Komponenten visualisieren

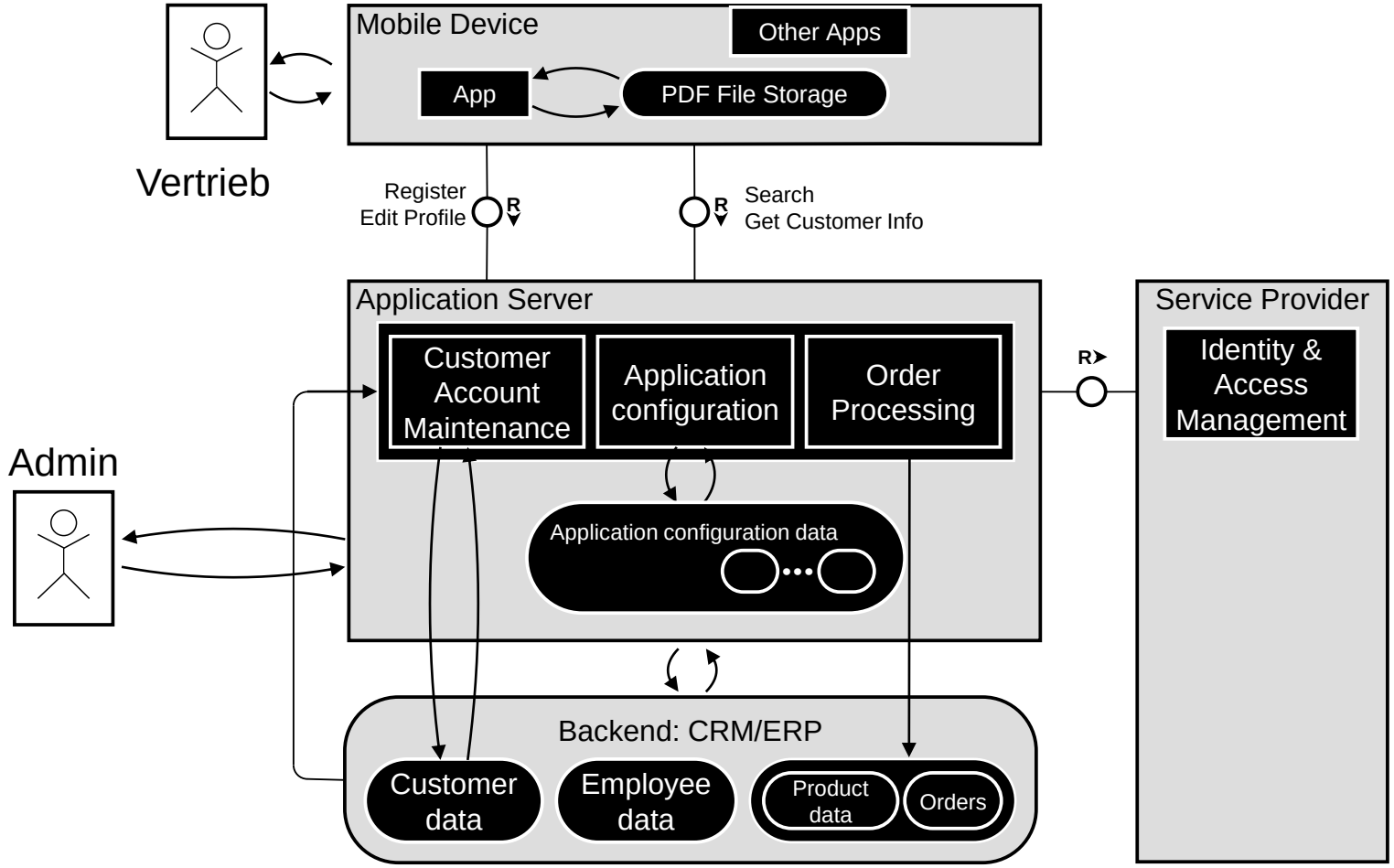


Praxis

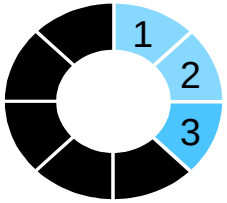
Beispiel

Einführung





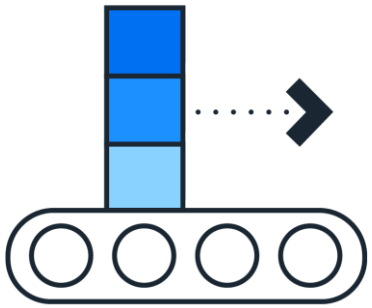
Vertrauenszonen visualisieren

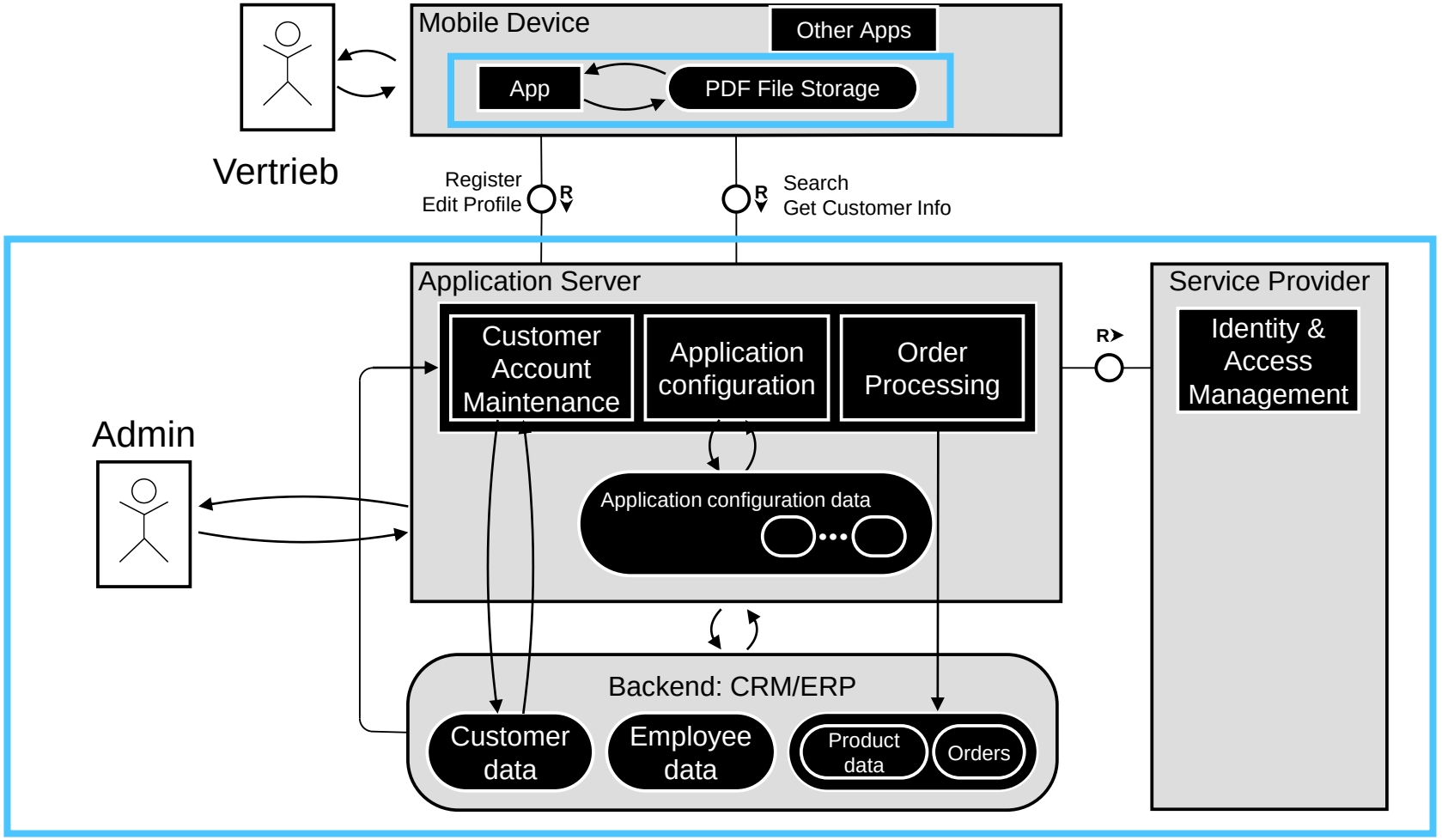


Praxis

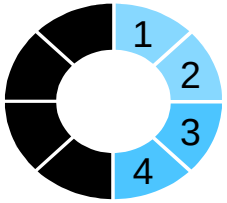
Beispiel

Einführung





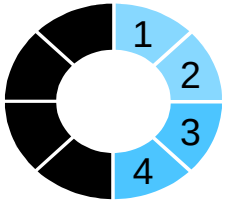
Gefahrenpunkte identifizieren



Methodenvielfalt

- Offen
  - Brainstorming
  - Worst Case Szenario
- Geführt
  - OWASP Top 10, STRIDE …
  - Firmenspezifische Checkliste: gesammelte Erfahrung

Was ist „OWASP Top 10“?



Praxis

Beispiel

Einführung

Top 10 Web Application Security Risks

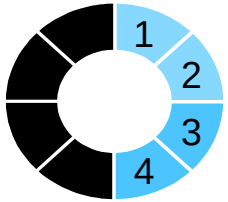
There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.

2017	2021
A01:2017-Injection	A01:2021-Broken Access Control
A02:2017-Broken Authentication	A02:2021-Cryptographic Failures
A03:2017-Sensitive Data Exposure	A03:2021-Injection
A04:2017-XML External Entities (XXE)	(New) A04:2021-Insecure Design
A05:2017-Broken Access Control	A05:2021-Security Misconfiguration
A06:2017-Security Misconfiguration	A06:2021-Vulnerable and Outdated Components
A07:2017-Cross-Site Scripting (XSS)	A07:2021-Identification and Authentication Failures
A08:2017-Insecure Deserialization	(New) A08:2021-Software and Data Integrity Failures
A09:2017-Using Components with Known Vulnerabilities	A09:2021-Security Logging and Monitoring Failures*
A10:2017-Insufficient Logging & Monitoring	(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://owasp.org/www-project-top-ten/

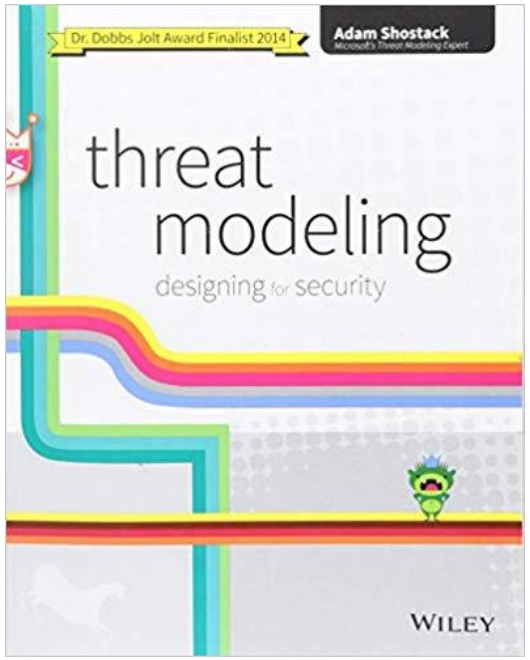
Was ist STRIDE?



Praxis

Beispiel

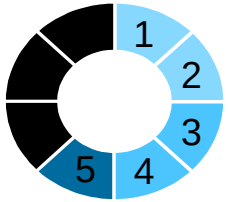
Einführung

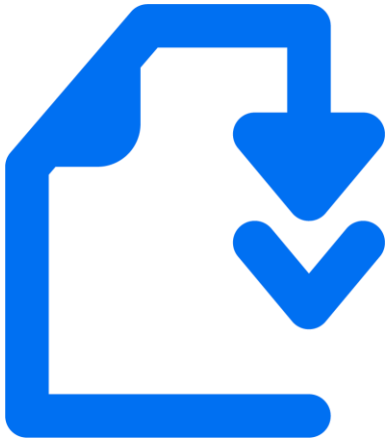


- Spoofing
  - Authentizität - Vorgeben, etwas oder jemand anderes als Sie selbst zu sein
- Tampering
  - Integrität - Etwas auf Festplatte, Netzwerk, Speicher oder an anderer Stelle ändern
- Repudiation
  - Nicht-Abstreitbarkeit - Behauptung, dass Sie nichts getan haben oder nicht verantwortlich waren
- Information Disclosure
  - Vertraulichkeit - Bereitstellung von Informationen für nicht Berechtigte
- Denial of Service
  - Verfügbarkeit – Überlastung von Ressourcen die für die Serviceerbringung erforderlich sind
- Elevation of Priviledges
  - Erweiterung der Berechtigungen – Erlaubt etwas zu tun, wozu eigentlich im jeweiligen Kontext keine Berechtigung vorgesehen ist

Threat Modeling: Designing for Security
Adam Shostack: https://www.wiley.com/en-us/Threat+Modeling%3A+Designing+for+Security-p-9781118810057

Bedrohungen dokumentieren





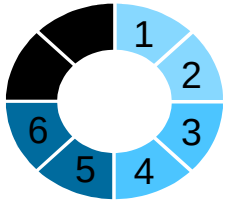
Beschreibung: Externer Zugriff (Vertrieb) sollen über Verfahren *x*, interner Zugriff (Admin, DevOps) über Verfahren *y* erfolgen. Anhand des genutzten Verfahrens *x* oder *y* werden auch die Berechtigungen vorsortiert.

Konkrete Bedrohung: Eine fehlerhafte Zuordnung des Verfahrens gefährdet die Vertraulichkeit und Integrität der Daten.

Beispiele:

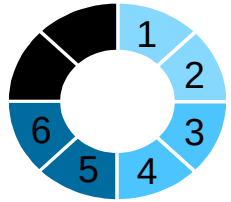
- Admin mit x und y
- Vertrieb mit x und y

Risiken bewerten



- Komplexität ~~Wahrscheinlichkeit~~ des Angriffs
- Potentielle Auswirkungen

Risiken bewerten

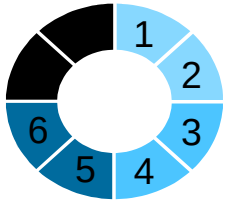


potentielle Auswirkung

	sehr komplex	komplex	aufwendig	einfach
kritisch	hoch	hoch	kritisch	kritisch
hoch	mittel	mittel	hoch	kritisch
moderat	niedrig	mittel	mittel	hoch
gering	niedrig	niedrig	mittel	mittel

Komplexität des Angriffs

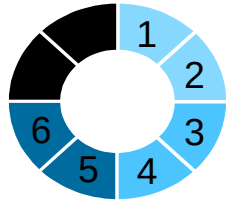
Risiken bewerten

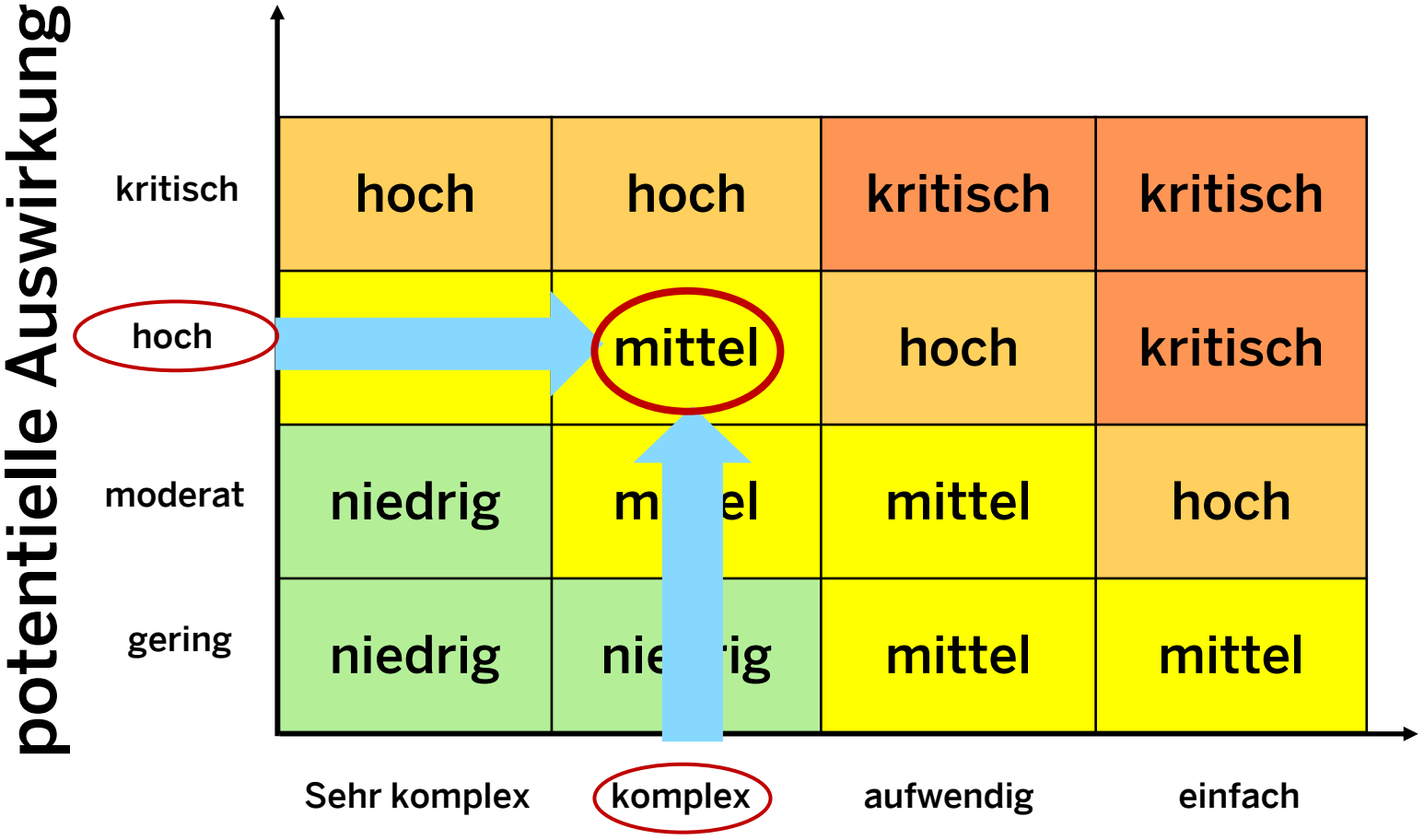


Gefahrenpunkt „Zugriff“:

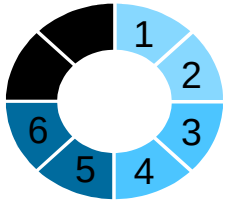
- Komplexitätsgrad des Angriffs: komplex
  - Voraussetzung: Legitimierter Zugriff als Nutzer
  - Spezielles IT-KnowHow / Hacker mit Erfahrung
  - **Angriffspfad:** Fehlerhafte Konfiguration für Administratoren (zufällig oder absichtlich)
- Potentielle Auswirkung: hoch
  - Vertraulichkeit der Daten
  - Integrität der Daten

Risiken bewerten





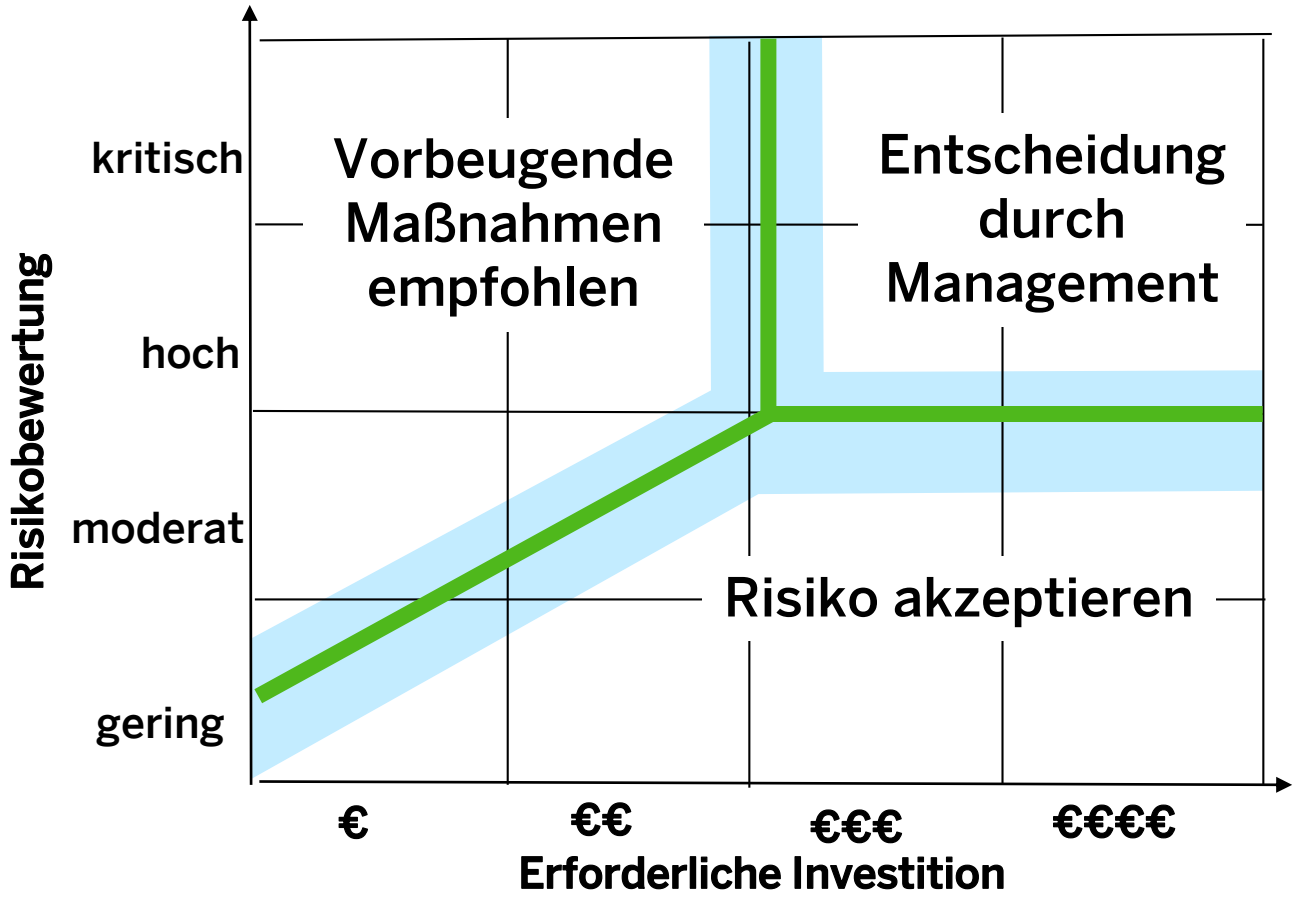
Risiken bewerten



Praxis

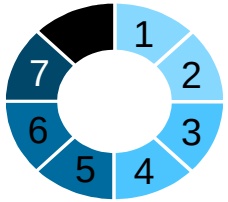
Beispiel

Einführung



ACHTUNG: Zusätzlich dazu sollten rechtliche Anforderungen zum Datenschutz oder sonstige rechtliche Rahmenbedingungen (HIPAA, NIS-2, GDPR, ...) sollten bei der Risikobetrachtung gegebenenfalls gesondert beachtet werden

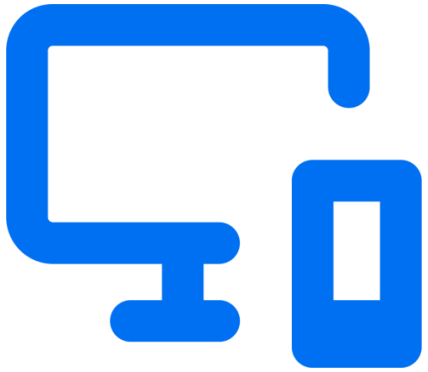
Mögliche schützenswerte Güter



Praxis

Beispiel

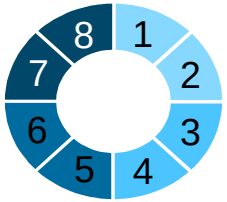
Einführung



Gefahrenpunkt „Zugriff“:

- Mögliche Gegenmaßnahmen
  - Separate Programme zur Prüfung der Konfiguration: Health Checks & Controls
  - Automatisierte Überwachung dieser „Health Checks & Controls“ im Betrieb
  - Manipulationssichere Protokollierung aller Konfigurationsänderungen der Zugriffskontrollsysteme
  - Festlegung von TOM‘s (Technischen und Organisatorischen Maßnahmen)

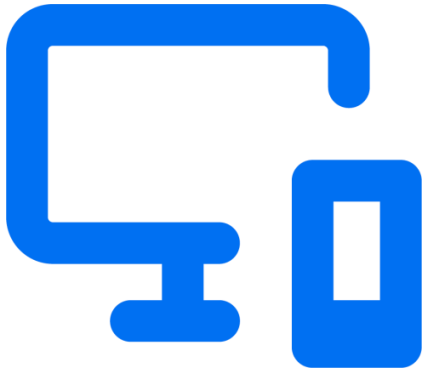
Mögliche schützenswerte Güter



Praxis

Beispiel

Einführung



Gefahrenpunkt „Zugriff“:

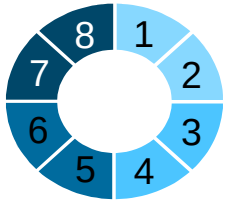
- Mögliche Gegenmaßnahmen

€€
- Separate Programme zur Prüfung der Konfiguration: Health Checks & Controls

€
- Automatisierte Überwachung dieser „Health Checks & Controls“ im Betrieb

€
- Manipulationssichere Protokollierung aller Konfigurationsänderungen der Zugriffskontrollsysteme
- Festlegung von TOM‘s (Technischen und Organisatorischen Maßnahmen)

Ergebnisse eines Threat Modeling



- Identifizierte Gefahrenpunkte
- Sicherheitsanforderungen im Backlog
- Vorschläge für gezielte Testen
- Ansatzpunkte für effizientes Code-Audit
- Erhöhte Fachkompetenz im Team

➔ **TM-Workshop ist kein Audit!**

Threat Modeling ...

Praxis

Beispiel

Einführung

- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

Bedrohungen weit denken …

- Angriff über Dienstleister
- Angriff über Software Supply Chain
- Innentäter
- Missbrauch als Mining Platform (Apps)
- Änderung in der Nutzung
- …

Bedrohungen weit denken …

Praxis

Beispiel

Einführung

Missing Link: Die MOVEit-Sicherheitslücke – eine Zwischenbilanz

Selbst wer die Software nicht verwendet, kann ein Opfer sein. Schätzungen gehen bisher von rund 68 Millionen Personen aus, deren Daten abgeflossen sind.

Lesezeit: 12 Min. In Pocket speichern 82

(Bild: Sergey Nivens/Shutterstock.com)

https://www.heise.de/hintergrund/Die-MOVEit-Sicherheitsluecke-eine-Zwischenbilanz-9318038.html

Bedrohungen weit denken …

Analysiert: Lego Mindstorms für Cyber-Angriffe missbraucht

Hintergrund 18.01.2016 17:43 Uhr - Imanuel von Cube

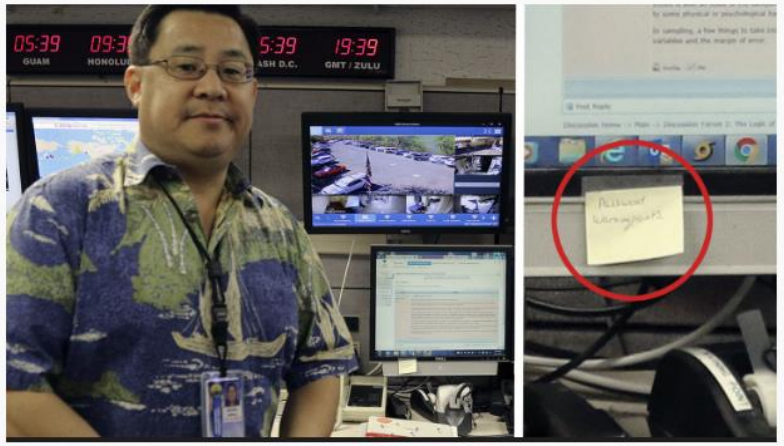
In einer deutschen Forschungseinrichtung arbeiten auch Lego-Roboter im Dienste der Wissenschaft. Eines Tages entwickelten diese jedoch ein gefährliches Eigenleben.

https://www.heise.de/security/artikel/Analysiert-Lego-Mindstorms-fuer-Cyber-Angriffe-missbraucht-3055305.html

Bedrohungen weit denken …

SICHERHEITSLÜCKE

Raketenalarm auf Hawaii: Passwort für Warnsystem stand monatelang im Internet



https://www.stern.de/digital/computer/raketenalarm-auf-hawaii--passwort-stand-monatelang-im-internet-7824260.html

Akzeptierte Riskiken: „assume the breach“...

- Akzeptierte Risiken mit einem Kontrollverfahren absichern.
- Indikatoren für die Kompromittierung eines Systems/Services suchen oder künstlich einbauen.

Threat Modeling ...

Praxis

Beispiel

Einführung

- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

… Fragen & Meinungen & Feedback

Vielen Dank

Contact information:

Axel Fasse
axel.fasse@sap.com

SAP folgen auf

www.sap.com/germany/contactsap

THE BEST RUN SAP®

Follow us

www.sap.com/contactsap

THE BEST RUN SAP®