

# '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 !

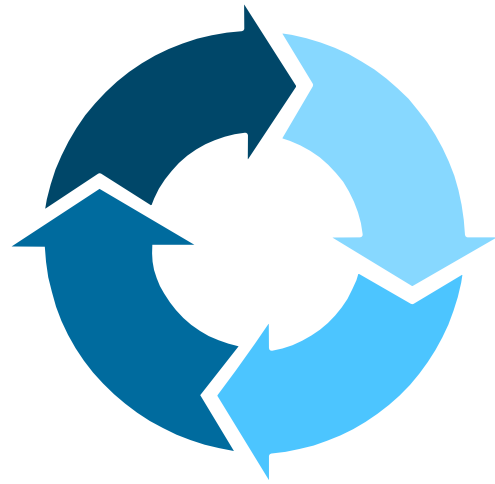


# Denken Sie an Ihre Eigene Software ...

Ist genug für die Sicherheit Ihrer Software getan/geplant?

An welchen Fakten machen Sie Ihre  
Antwort fest?

# Threat Modeling ...



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

# Threat Modeling ...



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

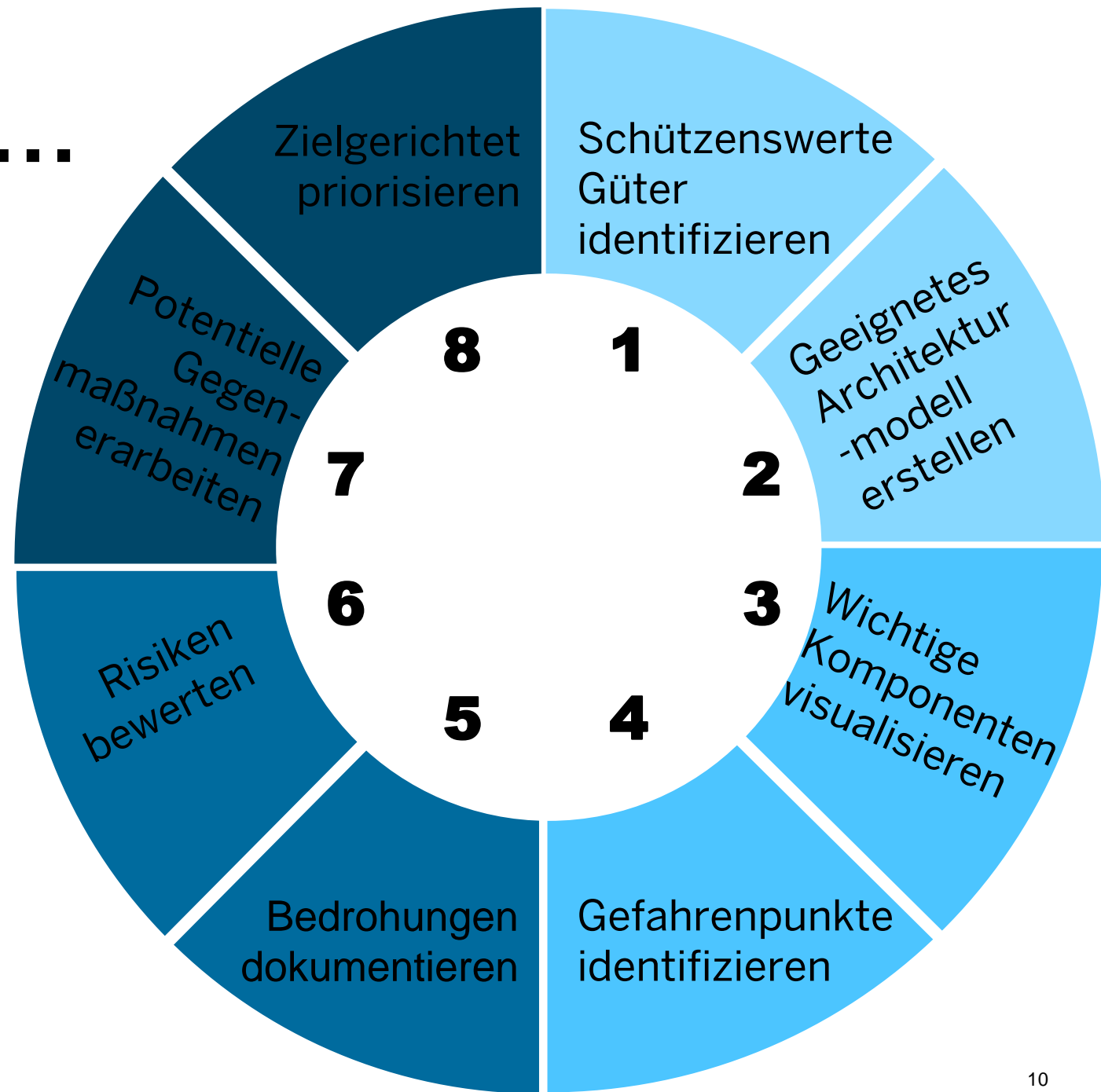
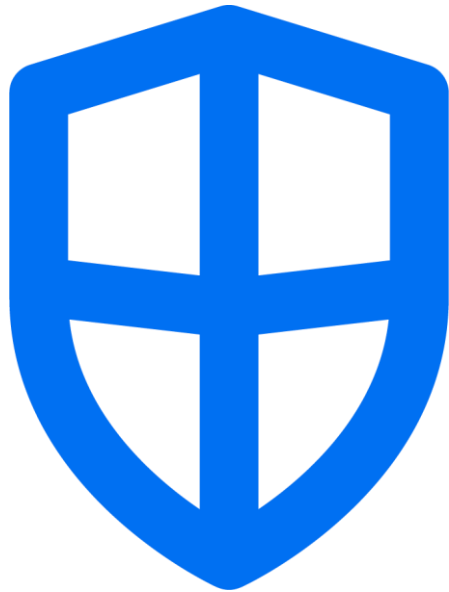


# Threat Modeling ...

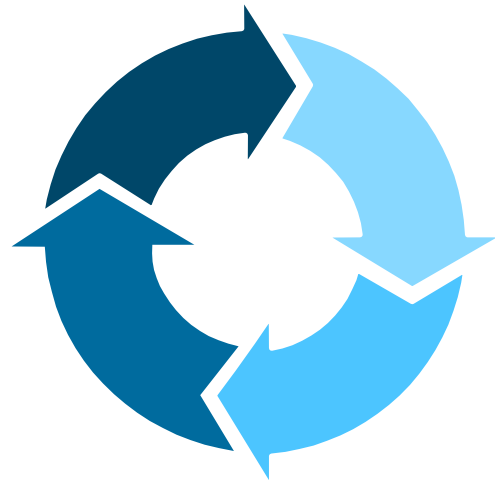


- ist eine strukturierte Methode zum Identifizieren von Bedrohungen und daraus abgeleiteten Sicherheitsanforderungen im Kontext bestimmter Angriffsszenarien.
- wird initial während der „Design Time“ der Architektur der Anwendung durchgeführt.
- ermöglicht eine Priorisierung der sicherheitsbezogenen Anforderungen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

# Schritt für Schritt ...

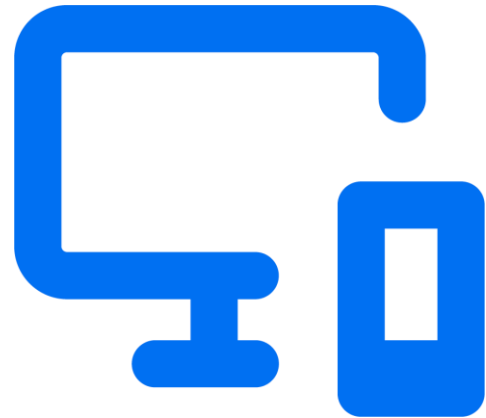
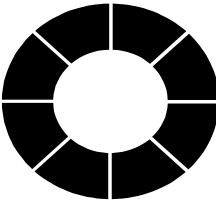


# Threat Modeling ...



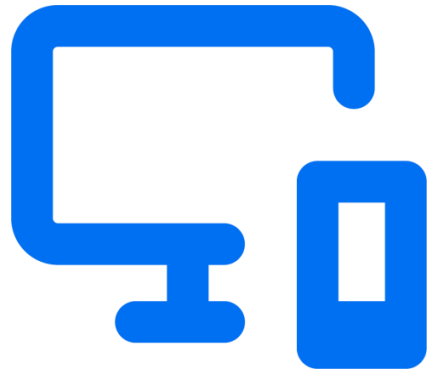
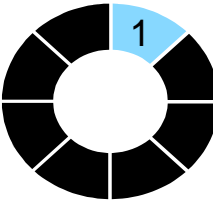
- eine Einführung
- ein konkretes, einfaches Beispiel
- einige Erkenntnisse aus der Praxis
- Ihre Fragen, Erfahrungen & Meinungen

# 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.

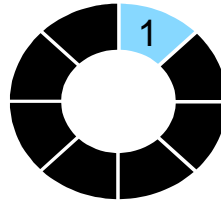
# Mögliche schützenswerte Güter



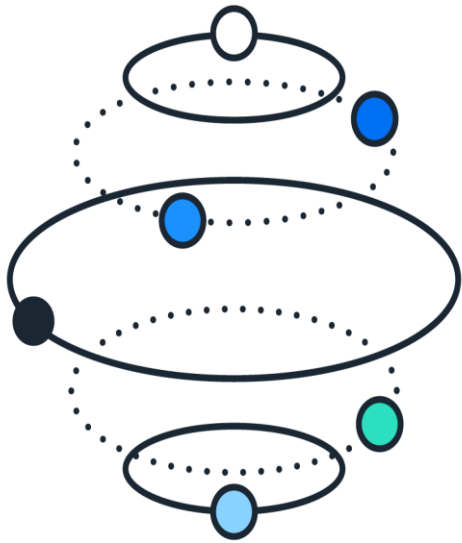
- Daten im Backend
- Mobile Daten, Kundenstammblatt
- Verfügbarkeit des Services
- CPU Last des Servers: BitCoin Mining
- ...

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

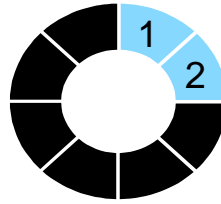
# Beispiel - mobiles Kundenstammblatt



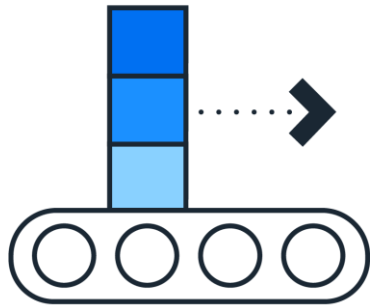
- Daten im Backend und Smartphone
  - Confidentiality = Vertraulichkeit
  - Integrity = Korrektheit
  - Availability = Verfügbarkeit



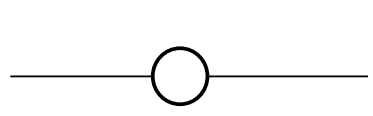


# Architekturmodell

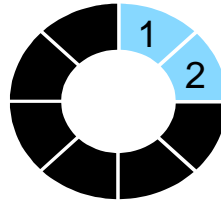


- Gezielt vereinfacht
- Modelliert mit „Fundamental Modeling Concepts“ (FMC)
- Kennzeichnung von „Trust Boundaries“

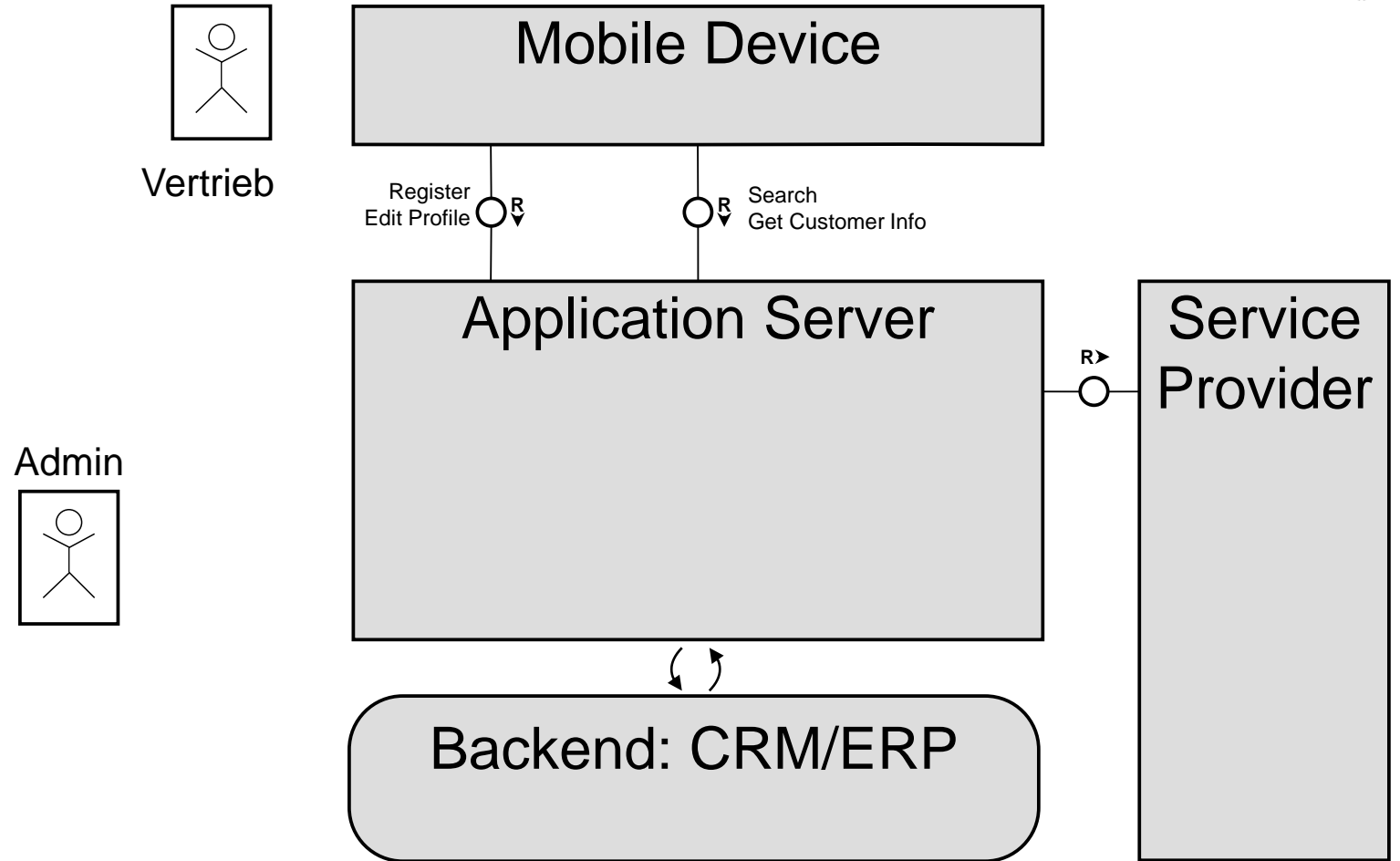
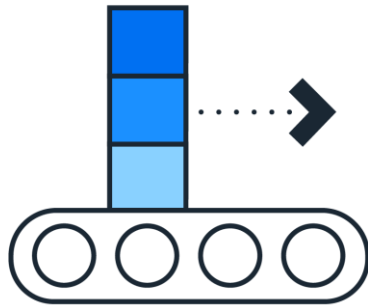


|  |  |
|--|--|
|   | <b>Agenten</b> verarbeiten Information, nutzen Speicher, kommunizieren über Kanäle |
|  | <b>Speicher</b> enthalten Informationen, auf die Agenten zugreifen                 |
|  | <b>Kanäle</b> werden von Agenten genutzt um Informationen zu transportieren        |

# Geeignetes Architekturmodell

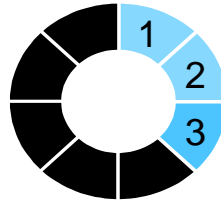


Praxis  
Beispiel  
Einführung

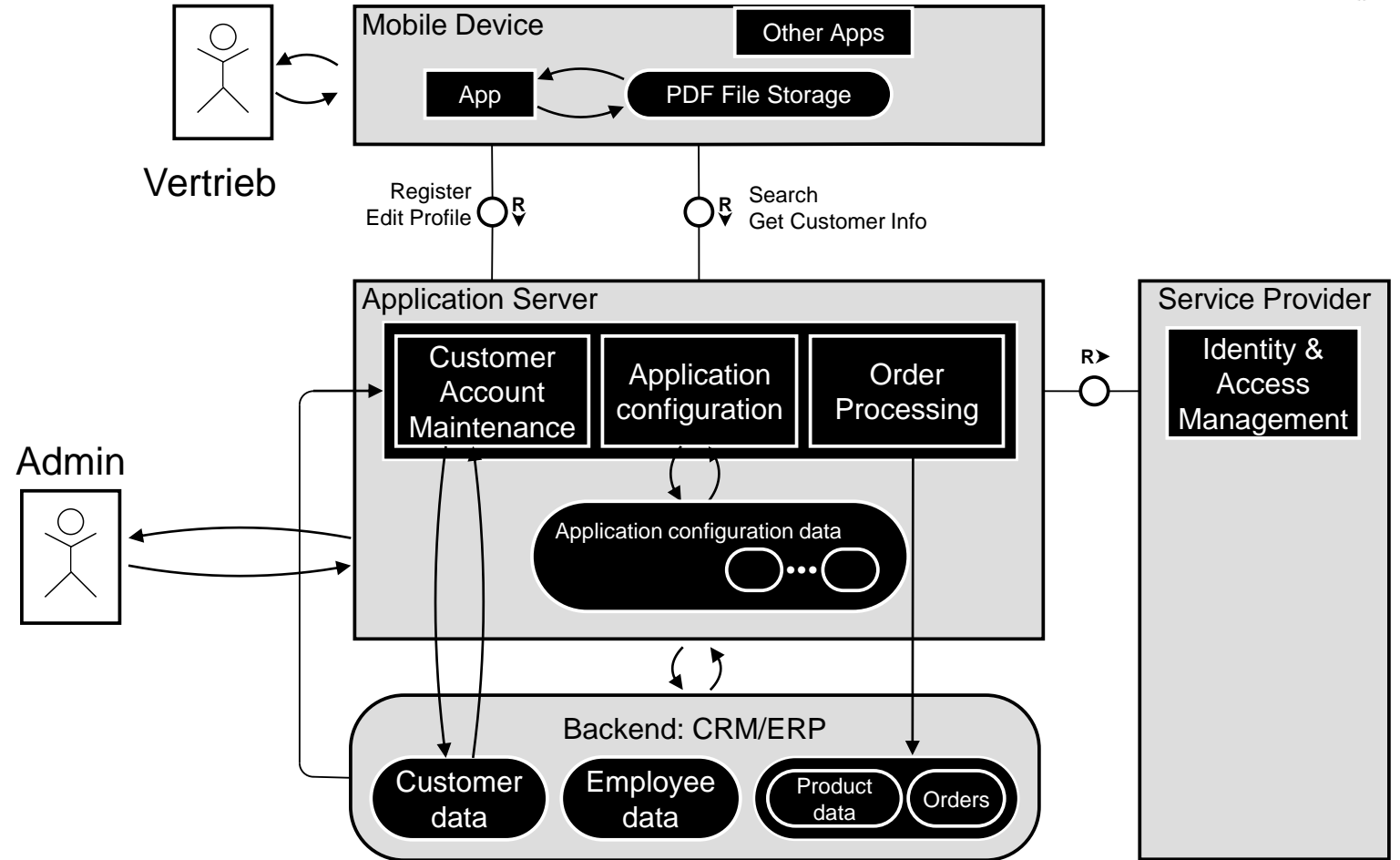
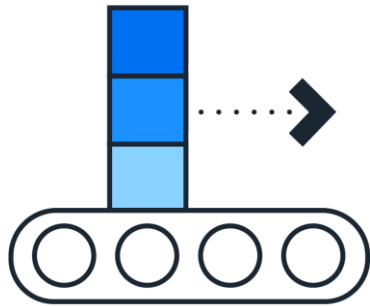




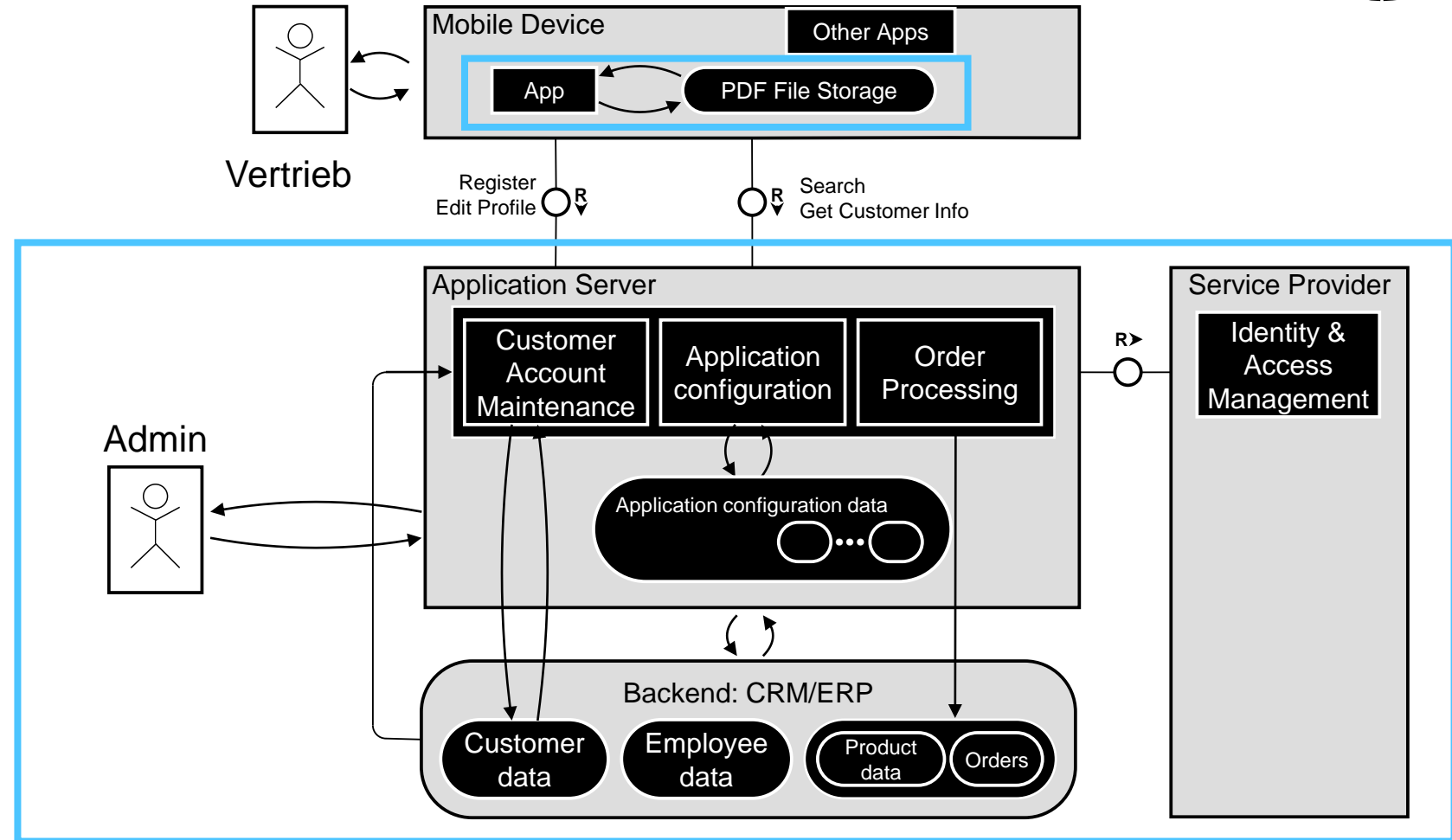
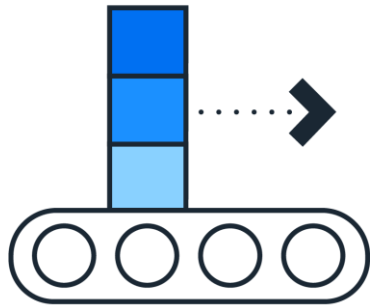
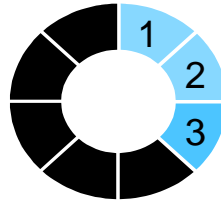
# Wichtige Komponenten visualisieren



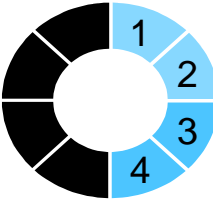
Praxis  
Beispiel  
Einführung



# Vertrauenszonen visualisieren



# Gefahrenpunkte identifizieren

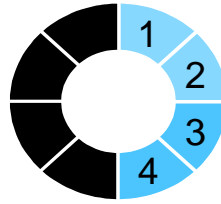


## Methodenvielfalt

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



# Was ist „OWASP Top 10“?



## Top 10 Web Application Security Risks

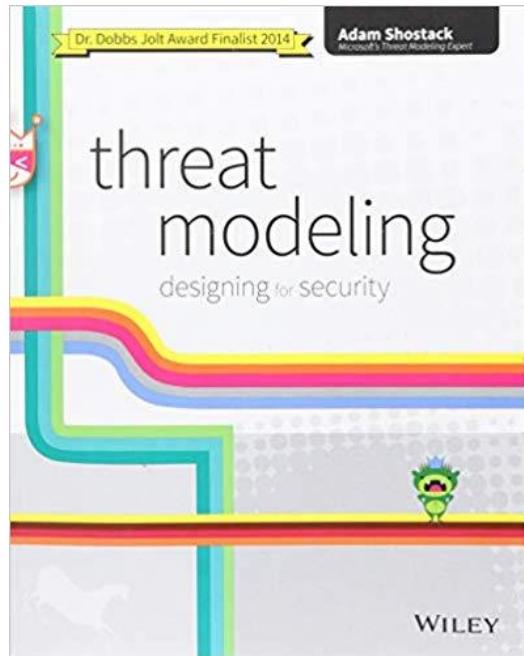
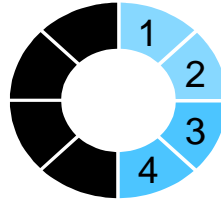
There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



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

\* From the Survey

# Was ist STRIDE?

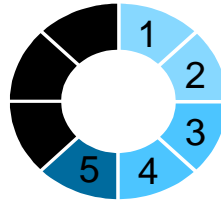


- **S**poofing
  - Authentizität - Vorgeben, etwas oder jemand anderes als Sie selbst zu sein
- **T**ampering
  - Integrität - Etwas auf Festplatte, Netzwerk, Speicher oder an anderer Stelle ändern
- **R**epudiation
  - Nicht-Abstreitbarkeit - Behauptung, dass Sie nichts getan haben oder nicht verantwortlich waren
- **I**nformation Disclosure
  - Vertraulichkeit - Bereitstellung von Informationen für nicht Berechtigte
- **D**enial of Service
  - Verfügbarkeit – Überlastung von Ressourcen die für die Serviceerbringung erforderlich sind
- **E**levation 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



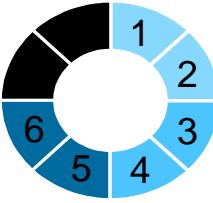
**Beschreibung:** Externer Zugriff (Vertrieb) sollen über Verfahren  $x$ , interner Zugriff (Admin, DevOps) über Verfahren  $y$  erfolgen. Anhand des genutzten Verfahrens  $x$  oder  $y$  werden auch die Berechtigungen vorsortiert.

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

**Beispiele:**

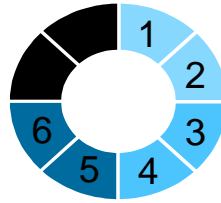
- Admin mit  $x$  und  $y$
- Vertrieb mit  $x$  und  $y$

# Risiken bewerten



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

# Risiken bewerten



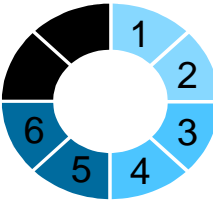
potenzielle Auswirkung

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

Komplexität des Angriffs



# Risiken bewerten

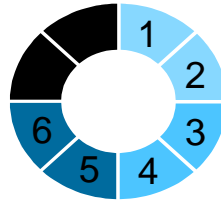


## Gefahrenpunkt „Zugriff“:



- 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

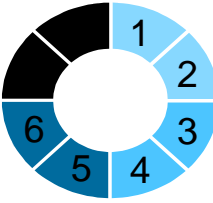


potentielle Auswirkung

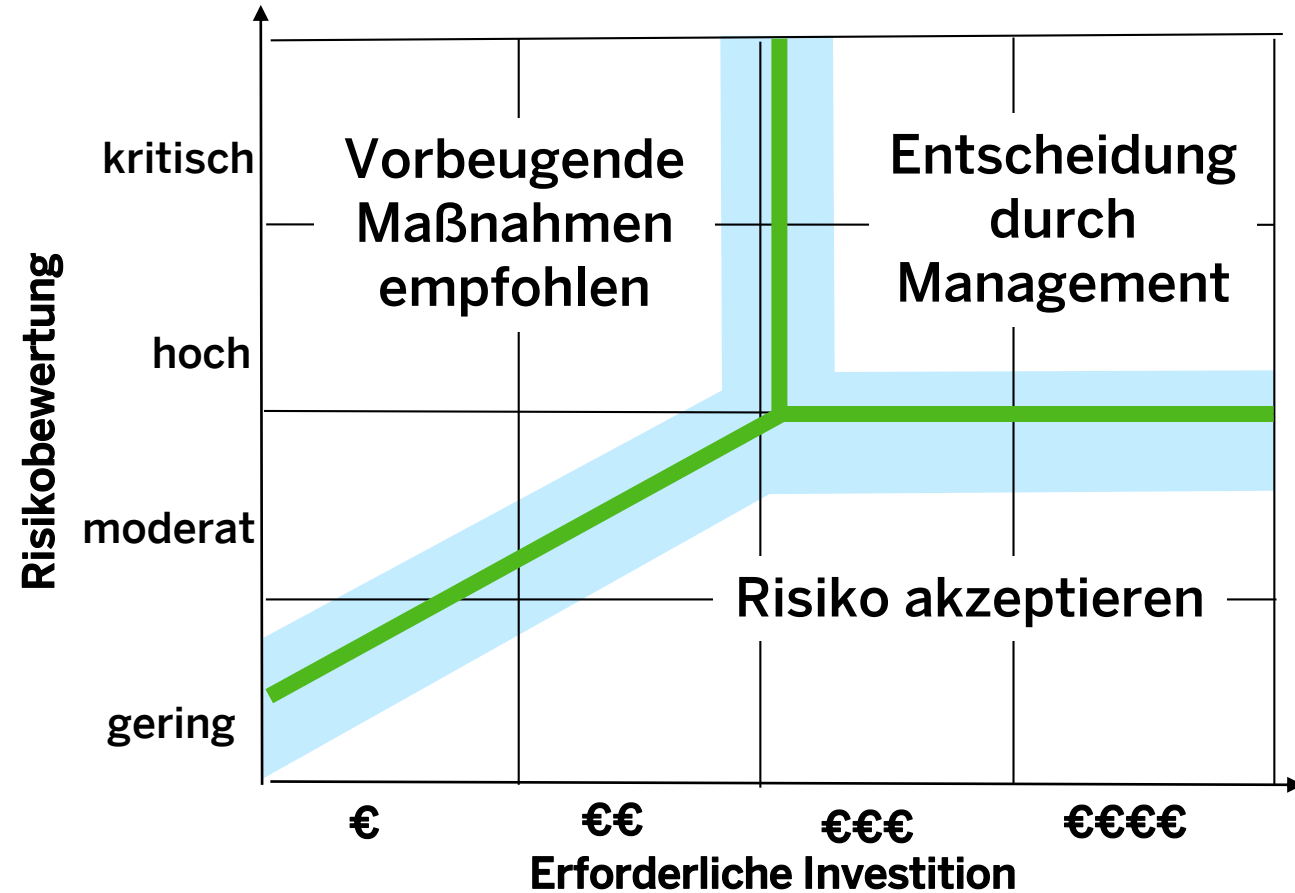
|          |              |         |           |          |
|----------|--------------|---------|-----------|----------|
| kritisch | hoch         | hoch    | kritisch  | kritisch |
| hoch     | mittel       | hoch    | kritisch  |          |
| moderat  | niedrig      | mittel  | mittel    | hoch     |
| gering   | niedrig      | niedrig | mittel    | mittel   |
|          | Sehr komplex | komplex | aufwendig | einfach  |

Komplexität des Angriffs

# Risiken bewerten

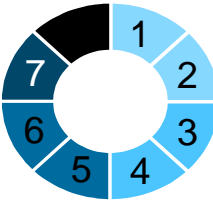


Praxis  
Beispiel  
Einführung



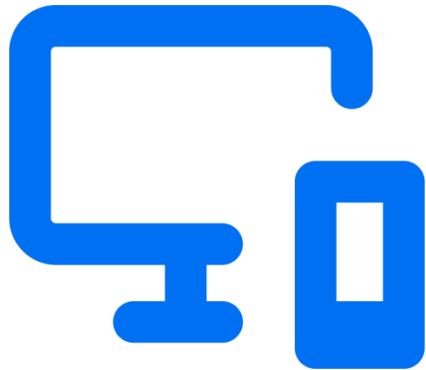
**ACHTUNG:** Zusätzlich dazu sollten rechtliche Anforderungen zum Datenschutz oder sonstige rechtliche Rahmenbedingungen ([HIPAA](#), [NIS-2](#), [GDPR](#), ...) sollten bei der Risikobetrachtung gegebenenfalls gesondert beachtet werden

# Mögliche schützenswerte Güter



## 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)

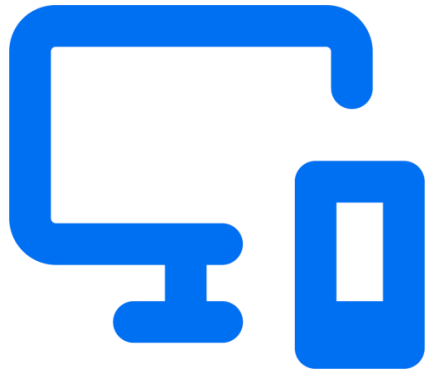


# Mögliche schützenswerte Güter



## 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)



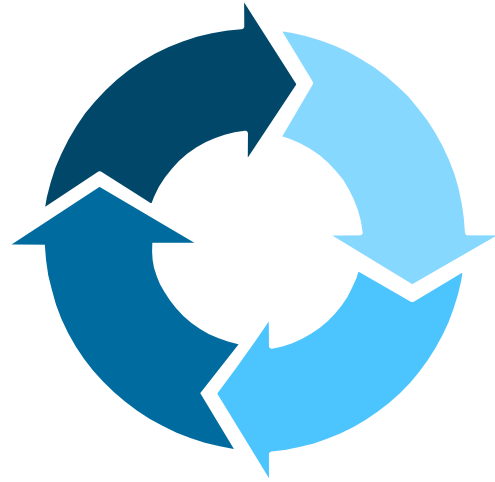
# Ergebnisse eines Threat Modeling



- 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 ...



- 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 ...



## 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

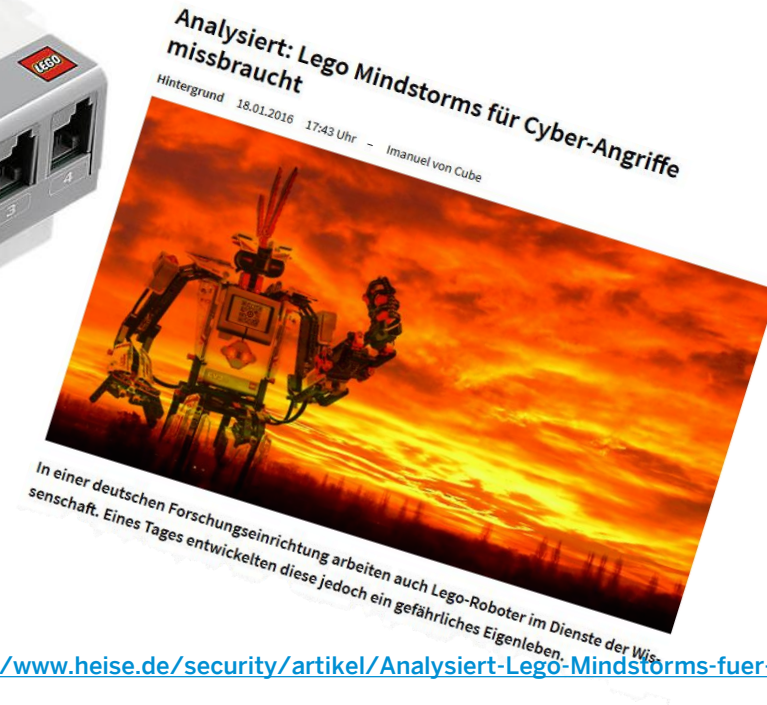
   82



(Bild: Sergey Nivens/Shutterstock.com)

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

# Bedrohungen weit denken ...



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

# Bedrohungen weit denken ...



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

# Akzeptierte Risiken: „assume the breach“ ...



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

# Threat Modeling ...



- 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](http://www.sap.com/germany/contactsap)

© 2021 SAP SE oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP SE oder ein SAP-Konzernunternehmen nicht gestattet.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von SAP SE oder deren Vertriebsfirmen angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der SAP SE oder einem SAP-Konzernunternehmen bereitgestellt und dienen ausschließlich zu Informationszwecken. Die SAP SE oder ihre Konzernunternehmen übernehmen keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die SAP SE oder ein SAP-Konzernunternehmen steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere sind die SAP SE oder ihre Konzernunternehmen in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen. Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen der SAP SE oder ihrer Konzernunternehmen können von der SAP SE oder ihren Konzernunternehmen jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.

SAP und andere in diesem Dokument erwähnte Produkte und Dienstleistungen von SAP sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP SE (oder von einem SAP-Konzernunternehmen) in Deutschland und verschiedenen anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen.

Zusätzliche Informationen zur Marke und Vermerke finden Sie auf der Seite [www.sap.de/trademark](http://www.sap.de/trademark).





Follow us



[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/trademark](http://www.sap.com/trademark) for additional trademark information and notices.

