# Bedrohungsanalyse für die Entwicklung

Karlsruher Entwicklertag 2016

Karlsruhe, 15.06.2016

Dr. Yun Ding

secorvo
security consulting

# Agenda

- Was ist eine Bedrohungsanalyse?
- Varianten der Bedrohungsanalyse
- Bedrohungsanalyse & Risikobewertung strukturiert durchführen: Best Practices
- Rollen und Aufgaben der Stakeholder bei der Bedrohungsanalyse

# Was ist eine Bedrohungsanalyse

# Bedrohungen und Schwachstellen

- Bedrohung ist der Feind!
  - *Diebe könnten ins Rechenzentrum einbrechen und Rechner und Daten klauen.*
  - *Der Kunde kann Opfer eines Phishing-Angriffs werden.*

- Schwachstelle ist man selbst!
- Schwachstelle durch Fehlen an (*effektiven*) Sicherheits-maßnahmen
  - *Das Türschloss ist leicht aufzubrechen.*
  - *Die Transportschicht kann durch fehlerhafte Konfiguration unzureichend abgesichert sein.*
  - *Implementierungsfehler, z.B. Buffer Overflow*

Bedrohung + Schwachstelle = Gefährdung

Bedrohung + Gegenmaßnahme ≠ Gefährdung

# Security Risk Management

- Analyse Schutzbedarf
- Bedrohungs-analyse
- Schwachstellen-analyse

# Was ist eine Bedrohungsanalyse?

- Ein *strukturierter* und *methodischer* Ansatz, um potentielle Bedrohungen …
  - zu identifizieren
  - nach Risiken zu bewerten: Eintrittswahrscheinlichkeit, Schadenspotential
  - Maßnahmen zur Vermeidung/Verminderung der Risiken zu priorisieren

# Zielsetzungen der Bedrohungsanalyse

- *Vollständigkeit*: möglichst „alle“ Bedrohungen finden
- *Nachvollziehbarkeit & Wiederholbarkeit*: vergleichbare Bedrohungen bei gleichen Typen von Systemen
- *Wirtschaftlichkeit*: mit begrenzten Ressourcen Bedrohungsanalyse effizient durchführen

# Was ist wichtig bei Bedrohungsanalyse?

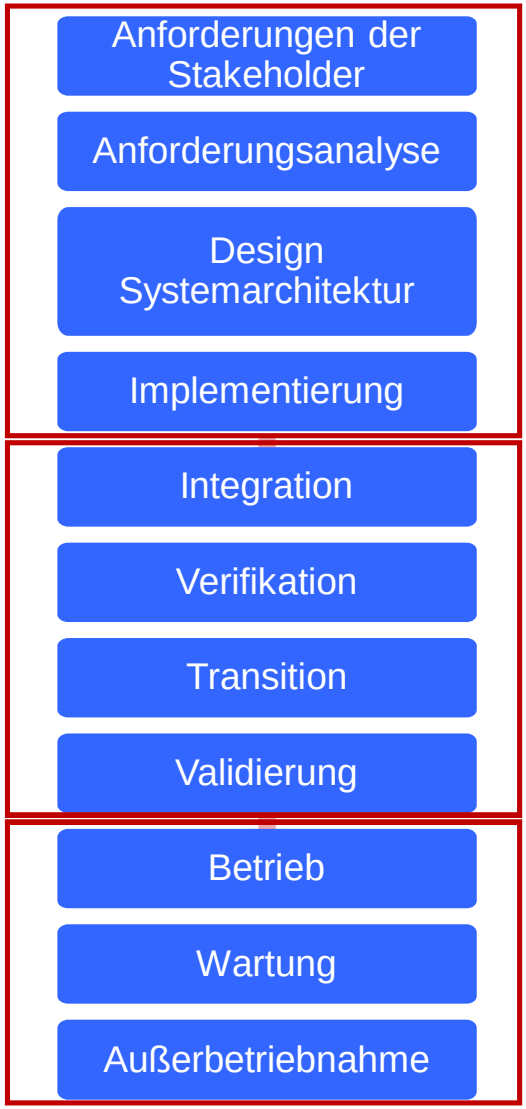
- **Erfahrungen**: Wissen, wonach ich suche
  - Man findet oft nur die Probleme, nach denen man auch genau sucht.

- **Kreativität**: Angreifer sind kreativ!
  - Ein Angreifer muss **eine Schwachstelle** finden – ein Verteidiger muss auf **alle Bedrohungen** vorbereitet sein.

- **Ausdauer**
  - Komplexe Systeme haben große Angriffsfläche.
  - Bei wiederholenden Aufgaben sucht man nach Abkürzungen und lässt (unbewusst, intuitiv) Schritte aus.

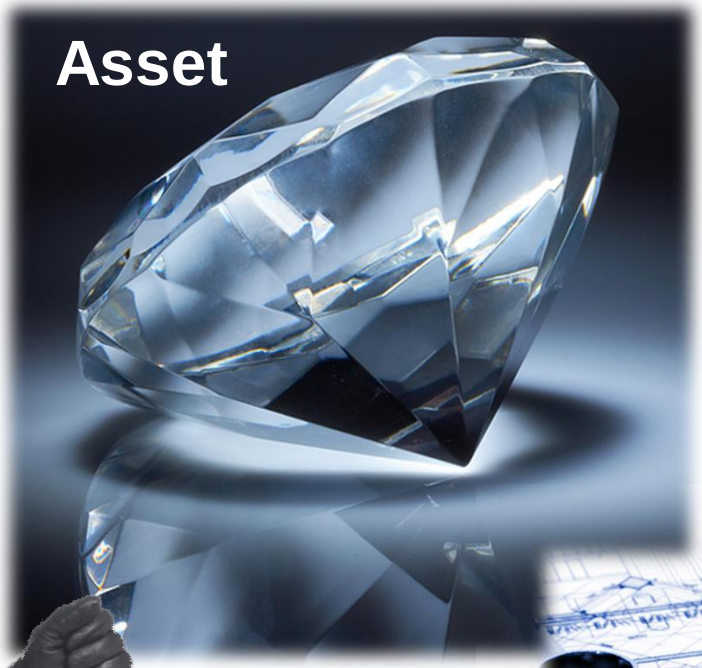
# Wann wird die Analyse durchgeführt?

- In der **Design**-Phase
  - Bedrohungen helfen, **Anforderungen** zu identifizieren
  - **Sicherheitsmaßnahmen** frühzeitig in das Design integrieren
  - Sicherheitsprobleme **proaktiv** vorbeugen
- In der **Test**-Phase
  - Bestehende Sicherheitsmaßnahmen validieren
- Kontinuierliches **Update**
  - Änderungen in Design und Betrieb
  - Ständige Entwicklung der Bedrohungs-Landschaft

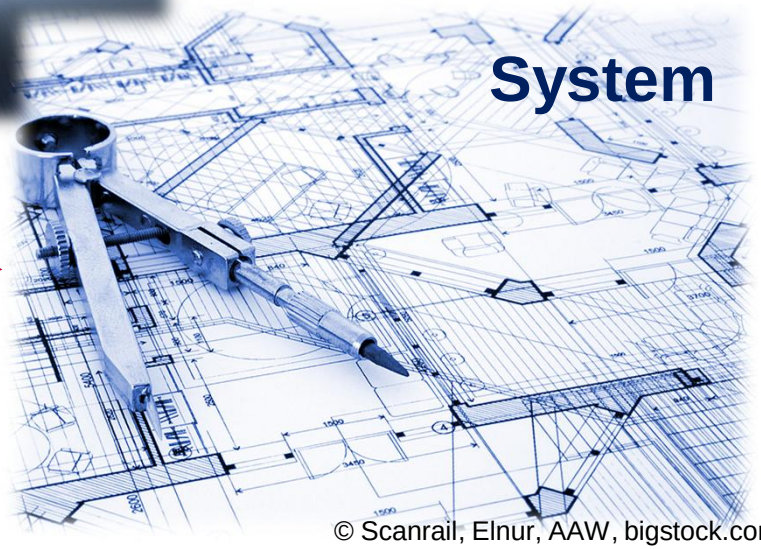


# Varianten der Bedrohungsanalyse

# Varianten der Bedrohungsanalyse

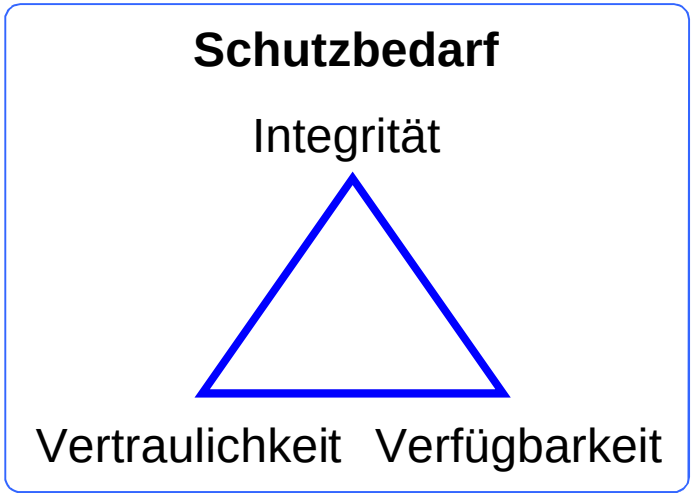



Angreifer



# Asset-zentriert

- Identifizierung von Assets: Kronjuwelen des Unternehmens
- Klassifizierung & Priorisierung von Assets – nach *Schutzbedarf*




Authentizität, Aktualität, Non-Repudiation, …

# Angreifer-zentriert

**Freizeitforscher** → **Neue Industrie**

Neugierige

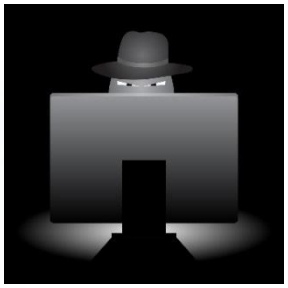
Ruhm-
süchtige

Script-
Kiddies

**Geld**

Gerechtig-
keitskämpfer

**Macht**

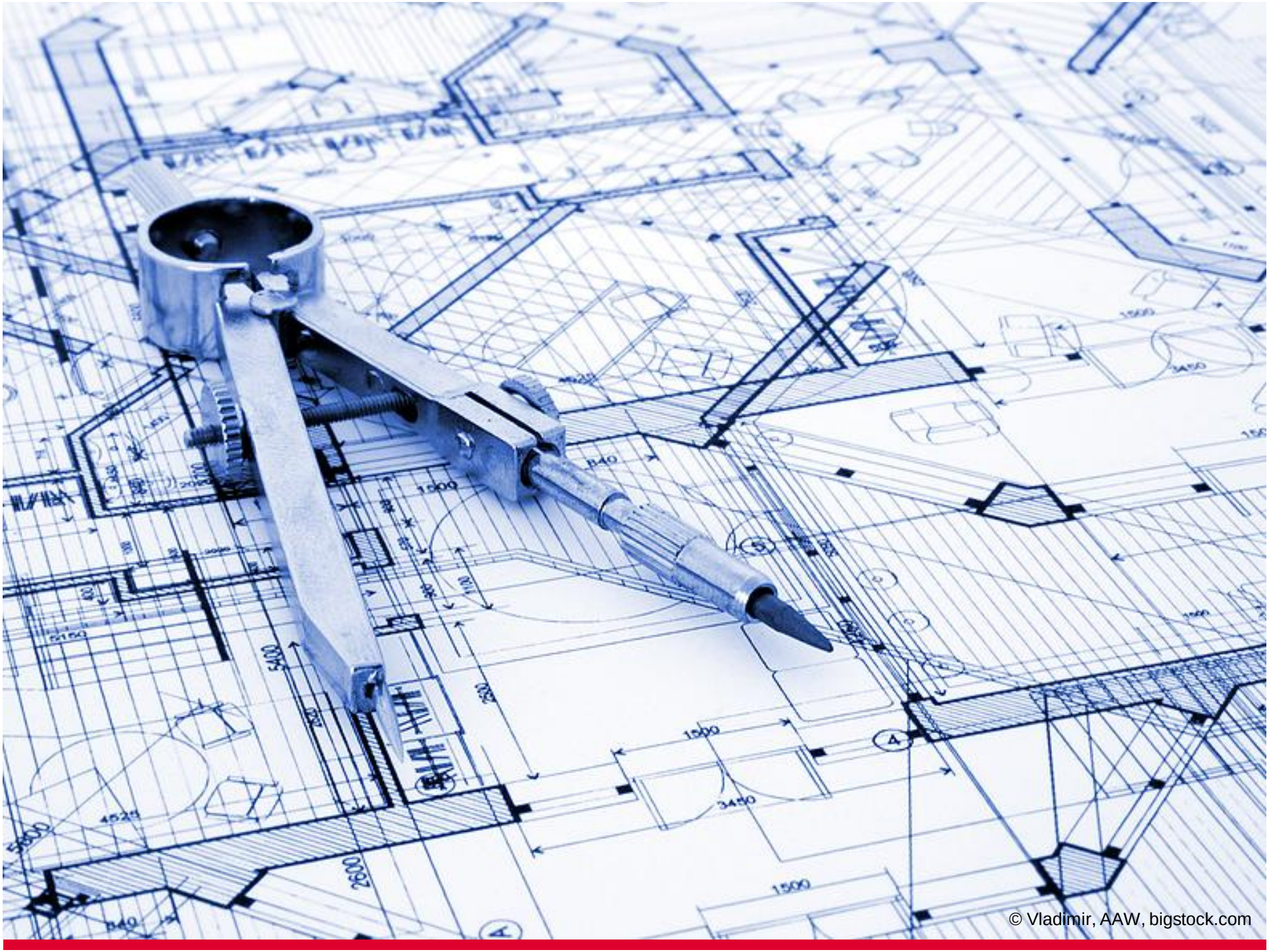


organisierte
Kriminalität

**Macht**
**Geld**

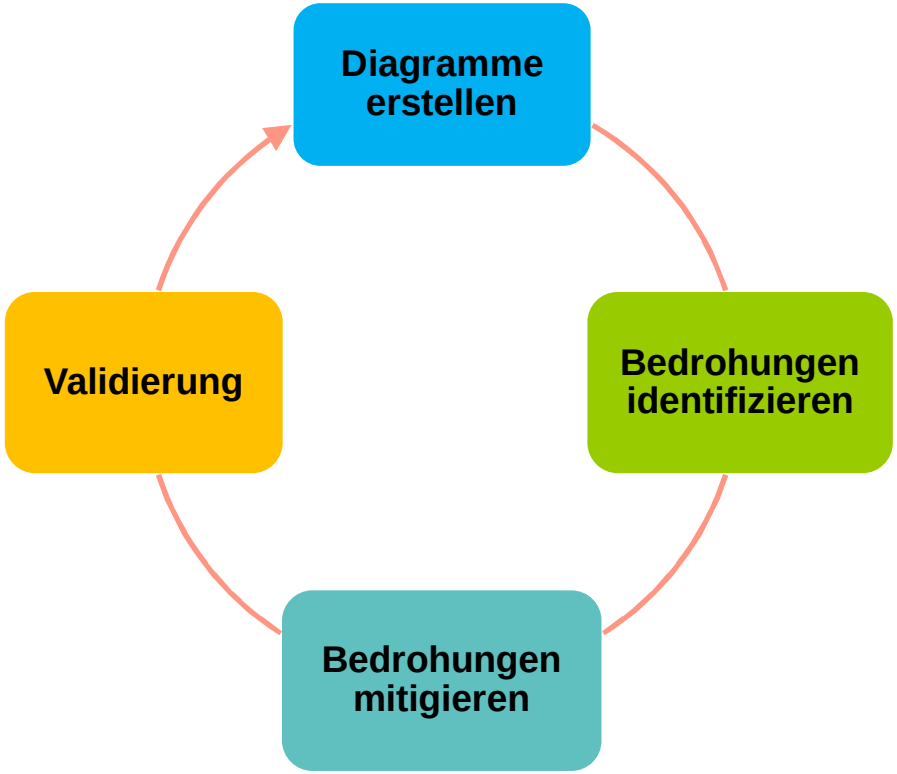
staatliche
Hacker

**Macht**


© Vladimir, AAW, bigstock.com

# System-zentriert

- Generiere Datenflussdiagramme (DFD) für das System
- Generiere Bedrohungen für Elemente und Datenflüsse
- Mitigiere Bedrohungen mit Sicherheitsmaßnahmen
- Validierung der Maßnahmen, Risikobewertung

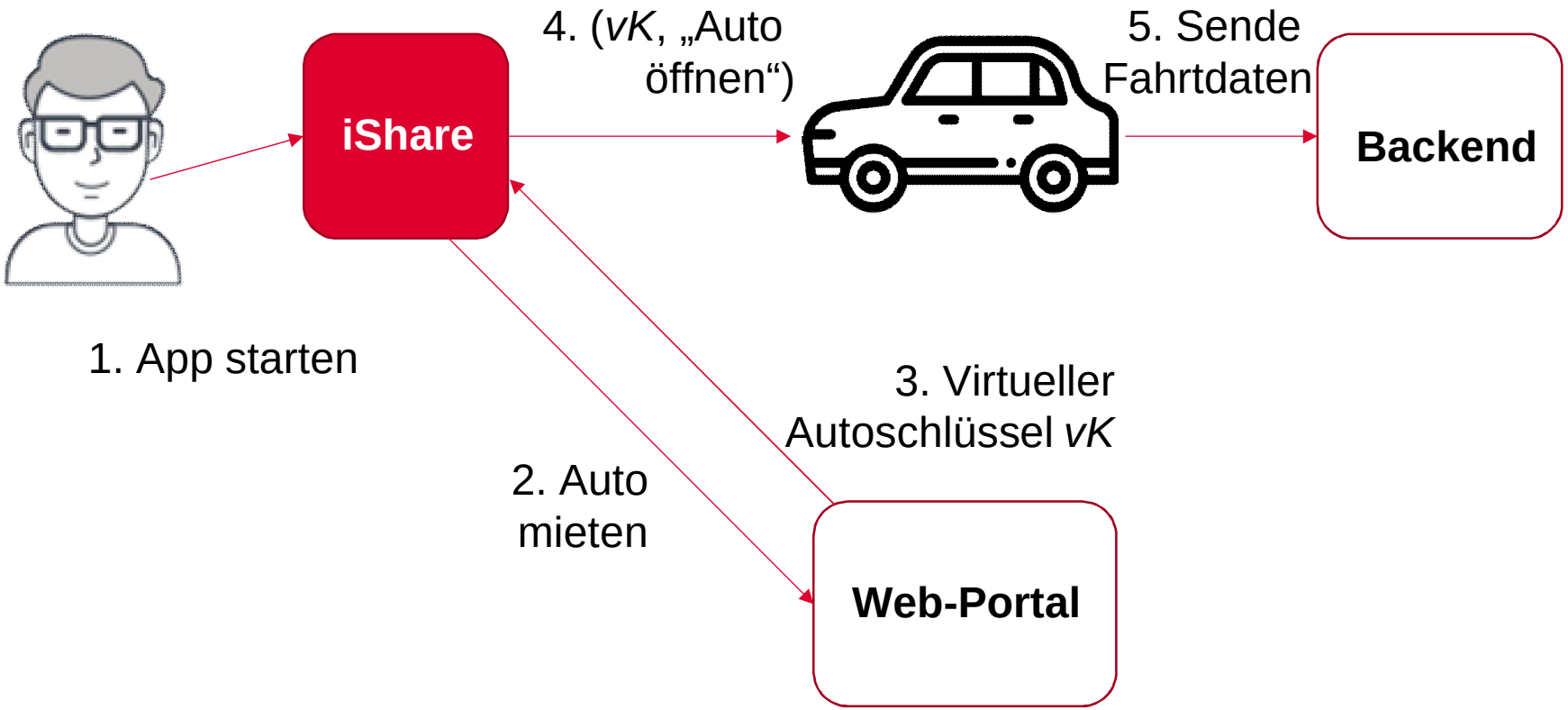


# Bedrohungsanalyse & Risikobewertung strukturiert durchführen

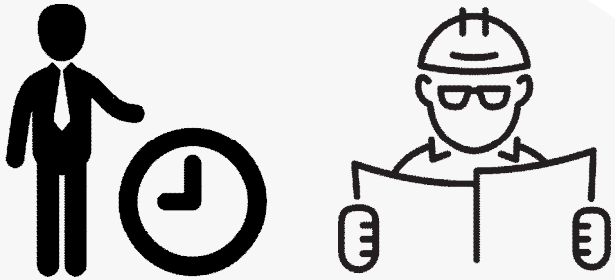
- Architekturdiagramme erstellen
- Bedrohungen & Schwachstellen erfassen
- Schutzmaßnahmen entwickeln
- Risiko bewerten

# BMW CONNECTED DRIVE SERVICES & APPS.

# Beispiel: App-basierte Autovermietung



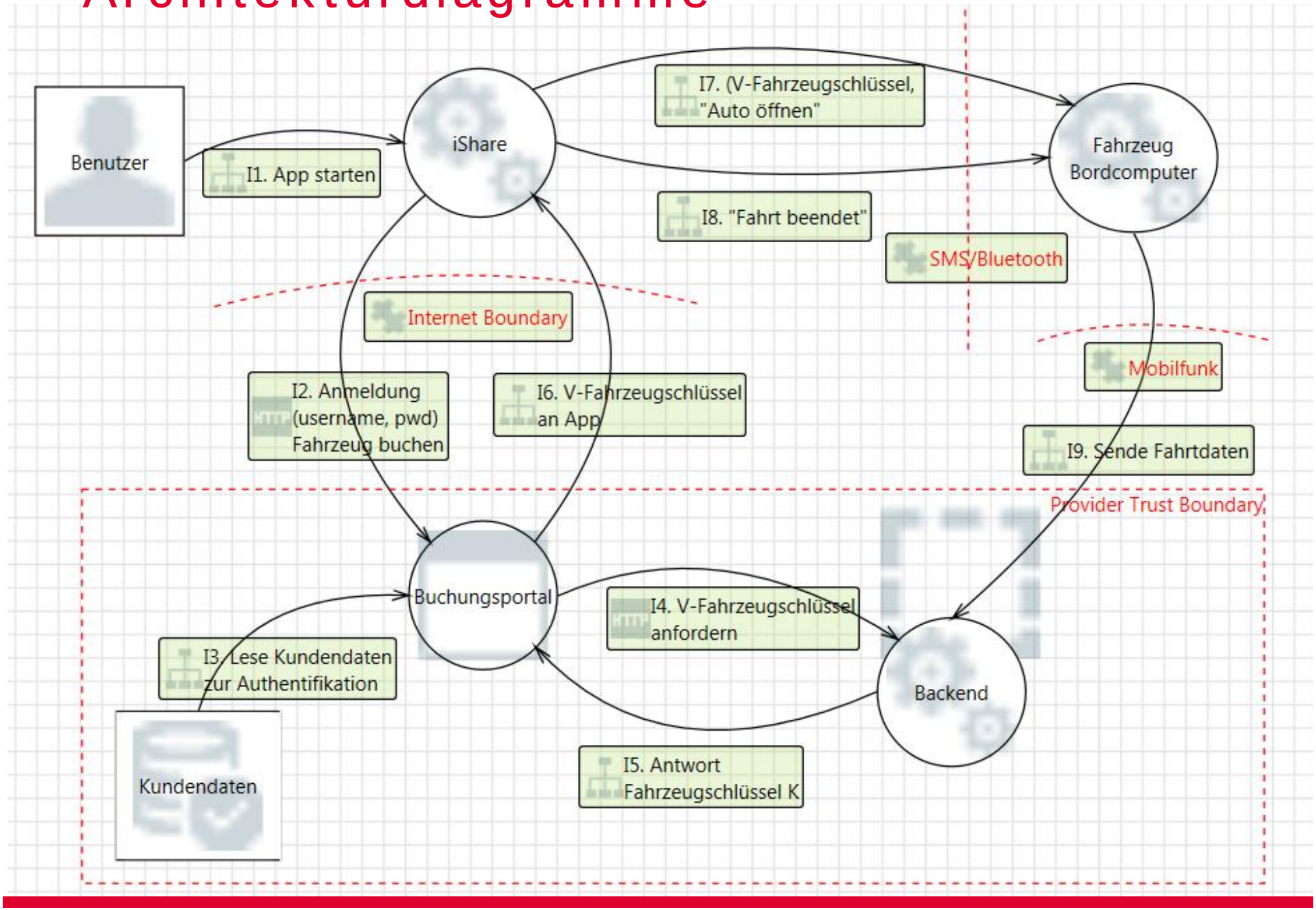
- **Architekturdiagramme erstellen**
- Bedrohungen & Schwachstellen erfassen
- Schutzmaßnahmen entwickeln
- Risiko bewerten



Produkt-
manager

System-
Architekt

# Architekturdiagramme



# Best Practices - Architekturdiagramme

- **Iterative Vorgehensweise**: kein vollständiges, perfektes Diagramm von Anfang an erforderlich
  - Diagramme iterativ verfeinern: z.B. neue Interaktionen durch Einführung von Sicherheitsmechanismen möglich
  - Neue, detaillierte Diagramme hinzufügen, falls notwendig
- **Hierarchische Diagramme** mit unterschiedlichen *Granularität*
  - Kontext-Diagramm: erklärt (den Kunden) das gesamte System
  - Level 1 Diagramm: fokussiert auf ein Szenario oder eine Funktionalität
  - Level 2 Diagramm: eine Funktionalität in Sub-Komponenten zerlegt

- Architekturdiagramme sind wertvoll
  - Gemeinsames Verständnis über die Anwendung
  - Interdisziplinäre Kommunikation zwischen den Stakeholders

# Annahmen

- Annahmen grenzen den Untersuchungsbereich der Bedrohungs- und Risikoanalyse ab.
- Beispiele
  - ***AN 1**: Die technische Umgebung der Kunden (z. B. Browser und Smartphone) werden als nicht vertrauenswürdig eingestuft.*
  - ***AN 2**: Die Backend-Anwendungen werden als vertrauenswürdig angenommen.*
  - ***AN 3**: Der externe Dienstleister ist nach dem Standard xxx zertifiziert. Die Prozesse, die von diesem Dienstleister durchgeführt werden, sind nicht Gegenstand der Analyse.*
- Annahmen sind zu dokumentieren.
- Gültigkeit der Annahmen ist zu prüfen und kann sich ändern.

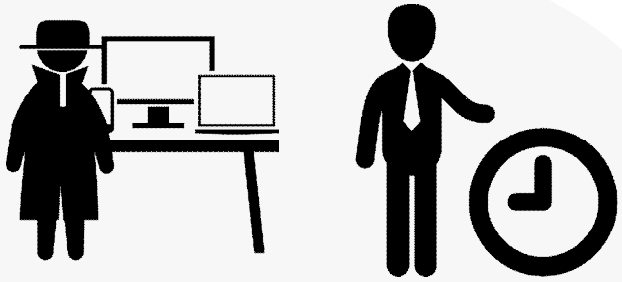
# Externe Abhängigkeiten

- Wie wird die Anwendung in der Produktion eingesetzt?
  - Die Backend-Anwendung läuft auf einem Apache-Server
  - Die Client-Anwendung speichert sensitive Information im iOS Keychain
  - Die Client-Anwendung kommuniziert über SSL mit dem Backend

- Was sind die Anforderungen für die externen Komponenten?
  - Der Apache-Server muss nach dem Stand der Technik gehärtet werden
  - iOS Keychain muss sichere Speicherung zur Verfügung stellen
  - iOS muss Transportsicherheit anbieten

- Externe Abhängigkeiten sind zu dokumentieren.

- Architekturdiagramme erstellen
- **Bedrohungen & Schwachstellen erfassen**
- Schutzmaßnahmen entwickeln
- Risiko bewerten



Security-Experte

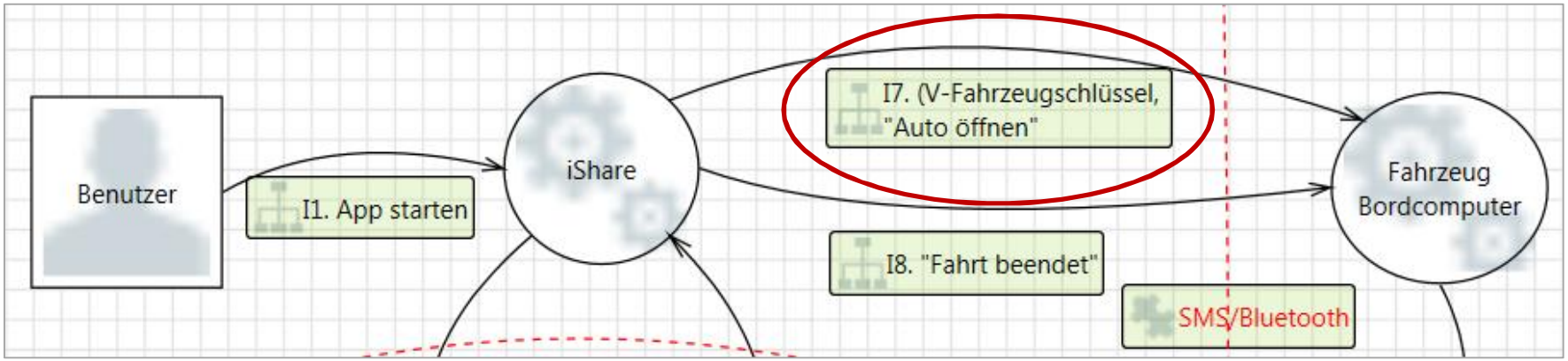
Produkt-manager

# Microsoft Threat Modeling Tool 2016

- Freies Werkzeug für die Windows-Umgebung
- Generiert generische **STRIDE**-Bedrohungen automatisch

| Bedrohung | Sicherheitseigenschaft |
|---|---|
| **S**poofing | Authentifizierung |
| **T**ampering | Integrität |
| **R**epudiation | Nichtabstreitbarkeit |
| **I**nformation disclosure | Vertraulichkeit |
| **D**enial of service | Verfügbarkeit |
| **E**levation of privilege | Autorisierung |

- Keine strikte Unterscheidung zwischen Bedrohungen & Schwachstellen




- *“iShare may be spoofed by an attacker and this may lead to unauthorized access to Fahrzeug Bordcomputer. Consider using a standard authentication mechanism to identify the source process.”*

Þ **BE 1**: Ein Angreifer kann sich gegenüber dem Bordcomputer als der legitime Benutzer ausgeben.

- *“Fahrzeug Bordcomputer may be spoofed by an attacker and this may lead to information disclosure by iShare. Consider using a standard authentication mechanism to identify the destination process.”*

Þ **BE 2**: Ein Angreifer kann abgefangene Nachrichten wiedereinspielen (Replay-Angriffe)

**BE 3**: Ein Angreifer kann unautorisiert auf vertrauliche Informationen im Datenpaket des virtuellen Fahrzeugschlüssels zugreifen.

# Weitere Bedrohungen

- **BE 4**: Ein Angreifer kann selbst einen virtuellen Fahrzeugschlüssel fälschen.
- **BE 5**: Ein Angreifer kann den abgefangenen virtuellen Fahrzeugschlüssel unautorisiert modifizieren.
- **BE 6**: Ein Angreifer kann abgefangenen Befehle des Benutzers an den Bordcomputer unautorisiert modifizieren.
- …

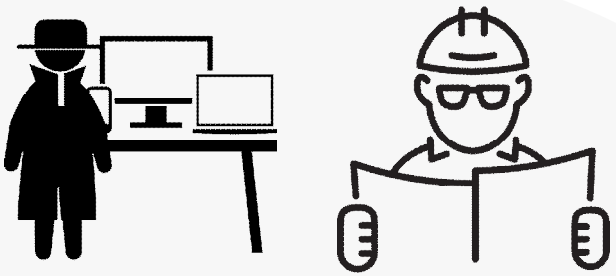
# Automatisch generierte Bedrohungen

- STRIDE sagt nicht aus, **wie** eine Bedrohung **ausgeführt** werden kann.
  - Spoofing-Bedrohung: Anmeldedaten können erraten bzw. abgefangen werden
- STRIDE gibt auch konkrete Information an, **welche Schwachstellen** eine Bedrohung ausnutzen kann.
  - Eine Spoofing-Bedrohung kann folgende Schwachstellen ausnutzen
    - Unsicheres Passwort
    - Unsicheres Session-Management
    - Unsichere Speicherung von Anmeldedaten

# Best Practices – Bedrohungen & Schwachstellen

- Kein automatisches Werkzeug kann das Wissen erfahrener Security-Experten ersetzen
  - Automatisch generierte Bedrohungen dienen als *Anhaltspunkte*
  - Werkzeuge sind wertvoll gegen das *Übersehen* und unterstützt die *Ausdauer*
- Bedrohungen und Schwachstellen zentral sammeln
  - Angriffsbibliotheken: OWASP Top Ten, CWE (Common Weakness Enumeration), CAPEC (Common Attack Pattern Enumeration and Classification) …
  - Aktuelle Pressemeldungen: heise Security, Secorvo Security News
  - Angriffsbibliotheken fokussieren auf bekannten Angriffen in der Vergangenheit: keine vollständige Liste der Bedrohungen!

- Architekturdiagramme erstellen
- Bedrohungen & Schwachstellen erfassen
- **Schutzmaßnahmen entwickeln**
- Risiko bewerten



Security-Experte

System-Architekt

# Schutzmaßnahmen ableiten

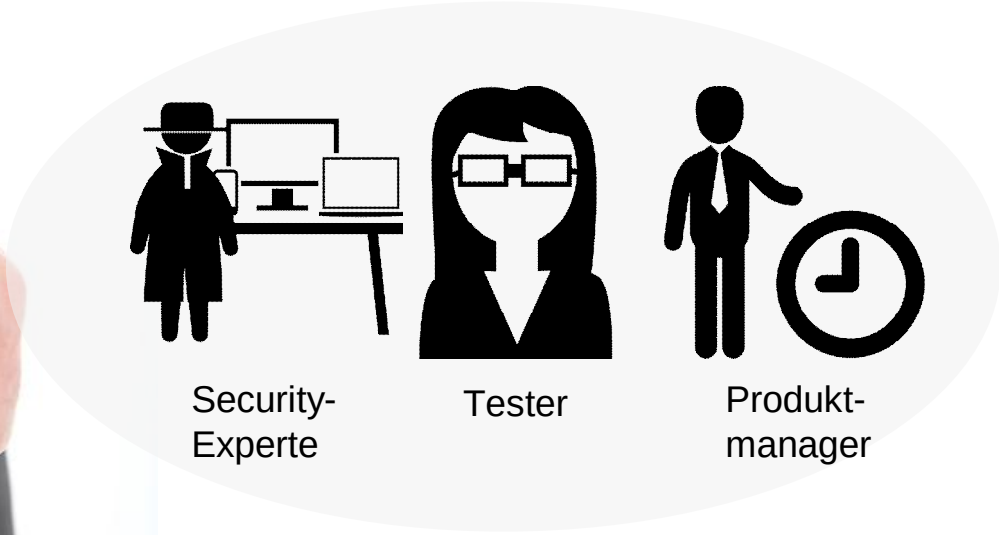
- Bedrohungen Þ Sicherheitsanforderung Þ Gegenmaßnahmen

| Bedrohungen | Anforderungen | Maßnahmen |
|---|---|---|
| **BE 1**: „Spoofing“ des Benutzers | **RE 1**: Authentifikation des Benutzers | **MA 1**: Sitzungsschlüssel |
| **BE 2**: Replay-Angriffe | **RE 2**: Aktualität der Nachrichten | **MA 2**: Zeitstempel |
| **BE 3**: Unautorisierte Zugriffe auf virtuellen Fahrzeugschlüssel | **RE 2**: Vertraulichkeit des Sitzungsschlüssels | **MA 3**: Datenpaket des virtuellen Schlüssels verschlüsseln |
| | | **MA 4**: HTTPS-Verbindung zum Buchungsportal |
| **BE 4**: Fälschen des virtuellen Schlüssels | **RE 3**: Authentizität des virtuellen Schlüssels | **MA 5**: HMAC-SHA1 auf den virtuellen Schlüssel |
| **BE 5**: Modifizierung des virtuellen Schlüssels modifizieren | **RE 5**: Integrität des virtuellen Schlüssels | Siehe **MA 5** |

# Best Practices: Schutzmaßnahmen

- Schutzmaßnahmen **nachvollziehbar** ableiten
- Architekturdiagramme um Schutzmaßnahmen anpassen bzw. ergänzen: iterative Vorgehensweise
- Schutzmaßnahmen zentral sammeln

- Architekturdiagramme erstellen
- Bedrohungen & Schwachstellen erfassen
- Schutzmaßnahmen entwickeln
- **Risiko bewerten**



# Risiko analysieren

- **Angriffsziele** konstruieren
  - Welche **Bedrohungen** und **Schwachstellen** sind dabei involviert?
  - Welche **Sicherheitsmaßnahmen** sind geplant bzw. vorhanden, die den Angriff erschweren?
  - Welche *Restrisiken* verbleiben?

| Angriffsziel | Bedrohungen | Maßnahmen | DREAD+ | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | D | R | E | A | D | R |
| „Spoofing“ des Benutzers – Sitzungsschlüssel aus dem Speicher auslesen | **BE 1** „Spoofing“ des Benutzers<br>**WE 1** Mobiles Gerät kompromittiert | **MA 1** Sitzungsschlüssel | | | | | | |
| „Spoofing“ des Benutzers – Sitzungsschlüssel bei der Übertragung abfangen | **BE 1** „Spoofing“ des Benutzers<br>**WE 2** Fehler in der TLS/SSL Konfiguration<br>**WE 3**: Unsichere TLS/SSL Middleware | **MA 1** Sitzungsschlüssel<br>**MA 4**: HTTPS-Verbindung zum Buchungsportal | | | | | | |
| Virtuelle Schlüssel fälschen | **BE 4**: Fälschen des virtuellen Schlüssels<br>**WE 4**: Unsichere Kryptographie | **MA 5**: HMAC-SHA1 auf den virtuellen Schlüssel | | | | | | |

# Risiko bewerten

- Das Risiko setzt sich aus *Eintrittswahrscheinlichkeit* und *Schadensausmaß* zusammen
- „Traditionell“
  - Risiko **=** Eintrittswahrscheinlichkeit **x** Schadensausmaß
  - (sehr hohes Schadenspotential, sehr geringe Eintrittswahrscheinlichkeit)
    Þ Einstufung: geringes Risiko

# Das DREAD+ Bewertungsmodell

- Risiko **=** Eintrittswahrscheinlichkeit **+** Schadensausmaß
- DREAD+ setzt sich aus folgenden Faktoren zusammen
  - Schadenspotential (**D**amage)
  - Reproduzierbarkeit (**R**eproducibillity)
  - Ausnutzbarbeit (**E**xploitability)
  - Betroffene Benutzer (**A**ffected Users)
  - Anfälligkeit/Entdeckbarkeit (**D**iscoverability)
  - Reaktionsmöglichkeit (**R**eactionability)
- Schadensausmaß: $S = f(D_{amage}, R_{epro}, A, R_{eact})$
- Eintrittswahrscheinlichkeit: $W = g(E, D_{iscover})$

- Die Funktionen *f* und *g* sind anwendungsspezifisch anzupassen!

# Bewertung der DREAD+ Faktoren

| Faktoren | 0 (vernachlässigbar) | 1 (gering) | 2 (mittel) | 3 (hoch) |
|---|---|---|---|---|
| **Damage – Schadenspotential** | Kein Schaden | Löst nicht direkt eine kritische Aktion aus | Einzelne wenige kritische Aktion auslösen, z.B. Fahrtdaten ändern | Beliebige sicherheits-kritische Aktionen auslösen: z.B. Auto öffnen |
| **Reproducibility – Reproduzierbarkeit** | Nicht reproduzierbar | Erfordert sehr spezifische Vorbedingungen | Erfordert wenige Vorbedingungen | Jederzeit zuverlässig reproduzierbar |
| **Exploitability – Ausnutzbarkeit** | Nicht praktisch umsetzbar | Erfordert hohen Aufwand | Erfordert mittleren Aufwand | Erfordert geringen Aufwand |
| **Affected Users – Betroffene Kunden** | Kein Bordcomputer betroffen | Wenige Bordcomputer betroffen | Mehrere Bordcomputer betroffen | Alle Bordcomputer betroffen |
| **Discoverability – Entdeckbarkeit** | Schwachstelle nicht erkennbar | Zur Zeit keine Schwachstelle erkennbar | Prinzipielle Schwach-stelle bekannt | Schwachstelle allgemein bekannt oder offensichtlich |
| **Reaction – Reaktionsmöglichkeit** | Unterbinden weiterer Angriffe | Mit Funktions-einbußen weitere Angriffe unterbindbar | Geringe reaktive Möglichkeit (Verfahrenswechsel) | Keine reaktive Möglichkeit |

# Risikobewertung

| Schadensausmaß \ Eintrittswahrscheinlichkeit | 0 | 1 | 2 | 4 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 4 |
| 1 | 1 | 2 | 3 | 5 |
| 2 | 2 | 3 | 4 | 6 |
| 3 | 3 | 4 | 5 | 7 |
| 4 | 4 | 5 | 6 | 8 |
| 5 | 5 | 6 | 7 | 9 |

- Strategien zur Risikobehandlung
  - Mitigieren: Maßnahmen zur Reduzierung der Risiken ableiten
  - Akzeptieren: geringe Risiken (z.B. „won´t fix“), dauerhafte Überwachung mittlerer Risiken
  - Vermeiden: Verfahren einstellen

# Best Practices: Risiko bewerten

- Risikobewertung dient dem **Vergleich** bzw. der **Priorisierung** zwischen den verschiedenen Risiken: keine absolute Werte
  - Individuelle Anpassung der Gewichtung der DREAD+ Faktoren erforderlich

- Möglichst konkrete Beispiele für die DREAD+ Bewertungsstufen definieren: ermöglicht eine konsistente Bewertung

# Fazit

- Bedrohungsanalyse ist **interdisziplinär**
  - Datenflussdiagramme sind wertvoll für das gemeinsame Verständnis und die Kommunikation zwischen den Stakeholders
- Automatische Werkzeuge
  - unterstützen die **Vollständigkeit** der Bedrohungsanalyse
  - ersetzen nicht das Wissen der Security-Experten: Knowledge-Base für (Bedrohungen, Schwachstellen, Maßnahmen) zentral sammeln
- Bedrohungsanalyse in Entwicklungsprozesse **integrieren**
  - durchführbar in der Design- und Testphase
  - iterative Vorgehensweise mit kontinuierlichem Update
  - Integration der Ergebnisse  in Issue-Tracker-Werkzeuge (z.B. JIRA)


Bedrohungsanalyse
Þ
nachvollziehbare
Sicherheitsziele &
Schutzmaßnahmen
© eelnosiva, bigstock.com


TOP
CONSULTANT
IT-Berater
2015
secorvo
security consulting
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

# Secorvo

- Unabhängiges Beratungsunternehmen für IT-Sicherheit und Datenschutz (seit 1998)
- Über 250 Jahre Berufserfahrung
- Über 850 Projekte
- Kunden: BMW, Daimler, BASF, Heidelberger, Deutsche Bank, EZB, Finanz Informatik, Datev, EnBW, Toll Collect, Krones, KfW, Tchibo, Commerzbank, Bundesbank, BSI, Deutsche Bahn, Benteler, SEW, Linde, Liebherr, Novartis, Deutsche Post, FhG, BNetzA, DZ-Bank, VW, Pfizer, Paul Hartmann, SWR, Bosch, SAP, ZF, ...

TOP CONSULTANT IT-Berater 2015

BEST OF CONSULTING 2010 — 2. PLATZ „IT-STRATEGIE" Wirtschafts Woche

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

L-BANK
Landespreis für junge Unternehmen

INNOVATIONSPREIS 2007
initiative mittelstand
AUSZEICHNUNG IT-Security