Aller Anfang ist schwer: Erfolgreiche erste Schritte in der Welt der Cybersecurity



24.09.2025, Mobile Experience Days 2025 by ifm

© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Agenda

1. Was ist Cybersecurity
2. Secure Development Lifecycle
3. TARA Threat and Risk Analyses / Bedrohungs- und Risikoanalyse
4. TARA - Beispiel
5. Referenzen / Informationen / Quellen

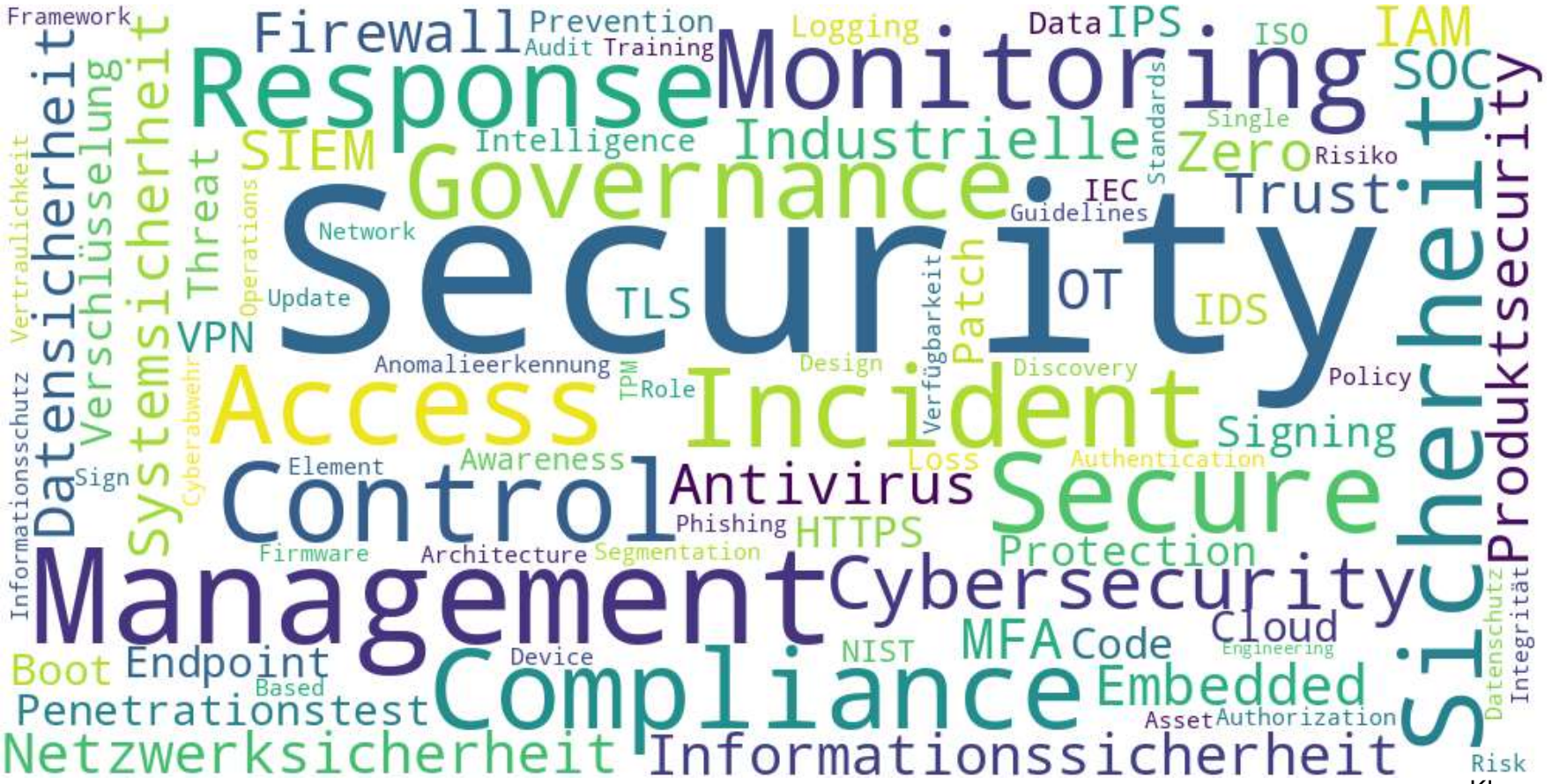
Was ist Cybersecurity?



© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Was ist Cybersecurity?



KI-generated

Mobile Experience Days 2025 by ifm

Was ist Cybersecurity?

Beschreibung

Aus Sicht eines Komponentenherstellers in der Automatisierungsbranche ist Cybersecurity ein strategisch und operativ entscheidender Bestandteil der Produktentwicklung, Systemintegration und Kundenbetreuung.

Cybersecurity ist nicht nur ein technisches Feature, sondern ein kontinuierlicher Prozess, der sich über den gesamten Produktlebenszyklus erstreckt.

Der Prozess umfasst zum einen organisatorische Anforderungen aber auch Projekt-spezifische Aktivitäten

Was ist Cybersecurity?

1 Designphase

Bedrohungs- und Risikoanalyse

2 Entwicklung

Sichere Implementierung

Einbinden von Cybersecurityfunktionen



3 Test & Validierung

Test

Überprüfung und Validieren

4 Inbetriebnahme

Dokumentation

Anleitung

5 Betrieb & Wartung

Überwachung

Schwachstellen- und Vorfallsmanagement

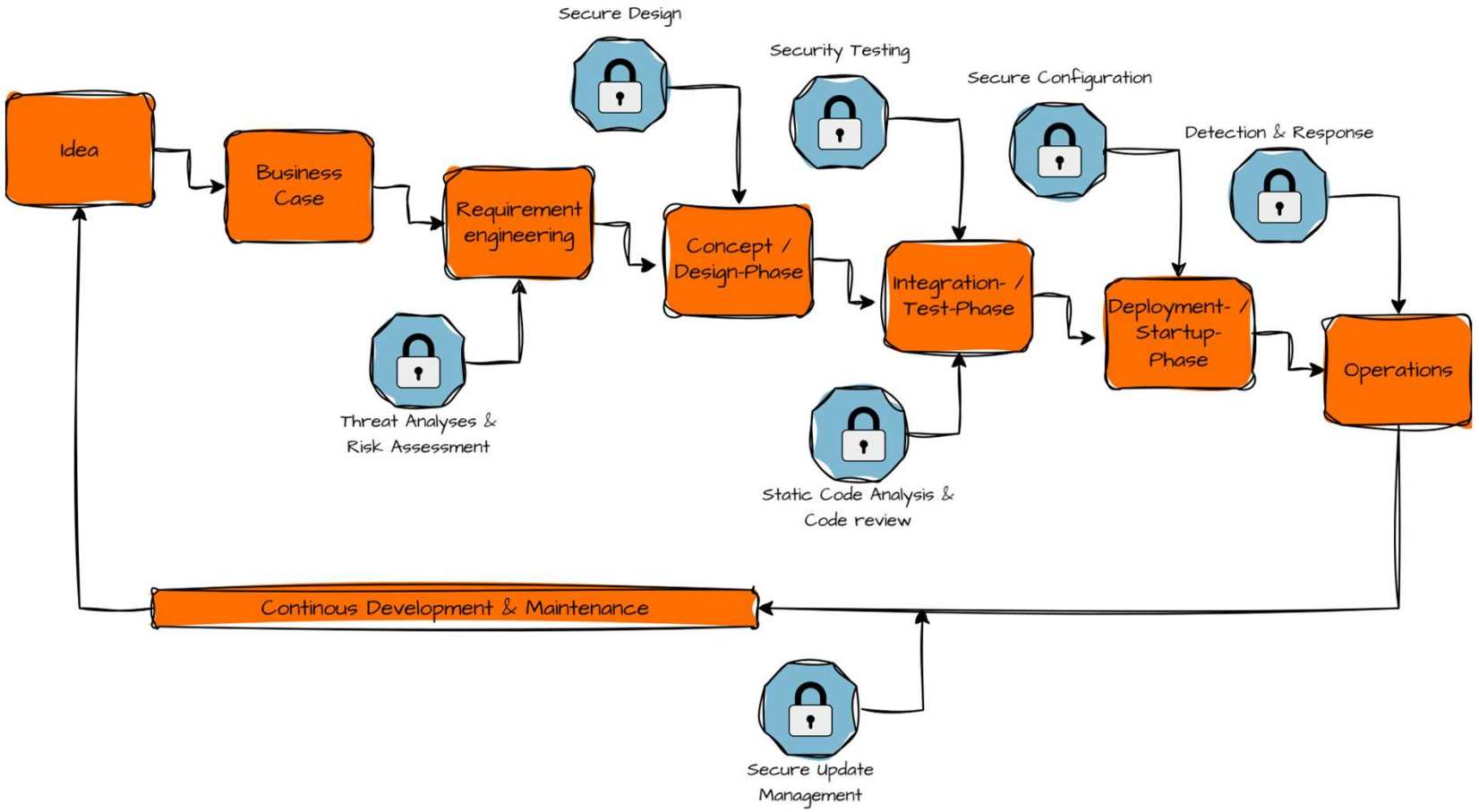
Secure Development Lifecycle



© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Übersicht „Secure Development Lifecycle“



Organisation- / Projekt-spezifische Anforderungen



- Entwicklungsprozess
- Festlegen der Verantwortlichkeiten
- Feststellen der Anwendbarkeit
- Fachkompetenz
- Prozesseingrenzung
- Integrität von Artefakten
- Sicherheit der Entwicklungsumgebung
- Überwachung von digitalen Schlüsselmaterial
- Anforderungen an Zulieferer (Supply Chain)
- Schwachstellen-Vorfalls-Management

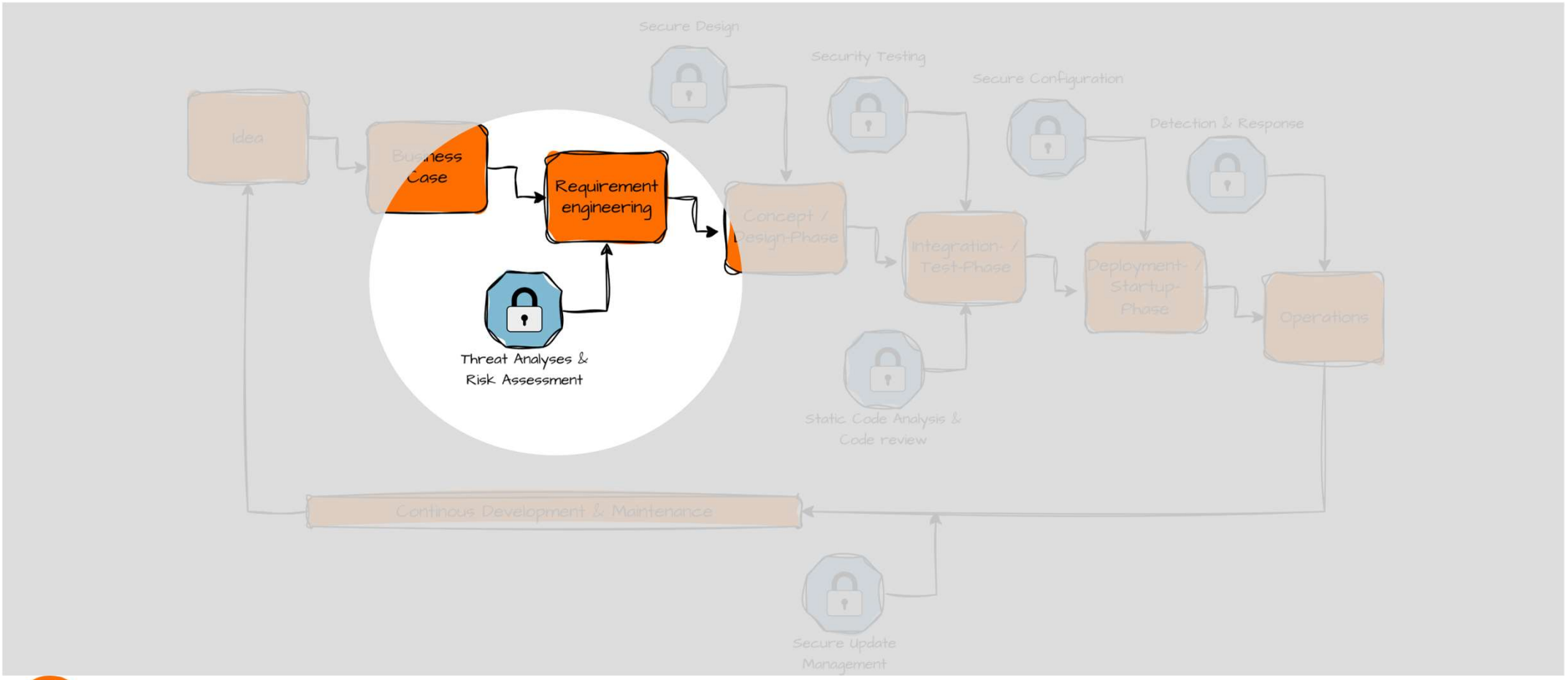
Organisation- / Projekt-spezifische Anforderungen



- Bedrohungs- und Risikoanalyse
- Sichere Entwurfsgrundsätze
- Defense in depth design
- Secure design best practices
- Secure coding standards
- Testverfahren für Cybersecurity
- Cybersecurity Dokumentation für Kunden
- Management von sicherheitsbezogenen Problemen
- Cybersecurity Update Management
- Nachvollziehbarkeit und Dokumentation

Mobile Experience Days 2025 by ifm

Übersicht „Secure Development Lifecycle“



TARA
Threat and Risk Analyses / Bedrohungs- und Risikoanalyse



© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Threat and Risk Analyses / Bedrohungs- und Risikoanalyse

Beschreibung

Die Bedrohungs- und Risikoanalyse (Threat- and Risk-Analyses; TARA) dient dazu, über den risikobasierenden Ansatz, die notwendigen Schutzmaßnahmen festzulegen, um die **Auswirkung** und dessen **Risiko** einer möglichen **Bedrohung** auf ein akzeptables Niveau zu reduzieren.

Mobile Experience Days 2025 by ifm

Threat and Risk Analyses / Bedrohungs- und Risikoanalyse

Risiko

$$Risiko = Bedrohung * Schwachstelle * Auswirkung$$

$$Risiko = Wahrscheinlichkeit * Auswirkung$$

*Quantitative Wahrscheinlichkeit, dass eine Handlung, ein Ereignis oder ein Vorfall eintreten kann

Aus Sicht der Cybersecurity bezeichnet Risiko die Kombination aus der Wahrscheinlichkeit, dass eine Bedrohung eine Schwachstelle ausnutzt, und den potenziellen Auswirkungen, die ein solcher Vorfall auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Systemen haben kann.

Mobile Experience Days 2025 by ifm

Threat and Risk Analyses / Bedrohungs- und Risikoanalyse

Risikobewertung / Risikomatrix

			Wahrscheinlichkeit				
Auswirkung			Häufig	Wahrscheinlich	Möglich	Selten	Unwahrscheinlich
			5	4	3	2	1
	Schwer	4	20	16	12	8	4
	Wichtig	3	15	12	9	6	3
	Medium	2	10	8	6	4	2
	Gering	1	5	4	3	2	1

Beispiel, DIN EN 61010-1 August 2023

Mobile Experience Days 2025 by ifm

Threat and Risk Analyses / Bedrohungs- und Risikoanalyse

Risikominimierung

- **Risikovermeidung**

Die Risiken können vermieden werden, indem der Informationsverbund so umstrukturiert wird, dass die Gefährdung nicht mehr wirksam werden kann. Dies bietet sich beispielsweise an, wenn Gegenmaßnahmen zwar möglich sind, aber einen zu hohen Aufwand bedeuten und gleichzeitig das Risiko nicht akzeptiert werden kann.

- **Risikoreduktion** (Risikomodifikation) durch weitere Sicherheitsmaßnahmen

Die Risiken können durch zusätzliche, höherwertige Sicherheitsmaßnahmen verringert werden.

- **Risikotransfer**

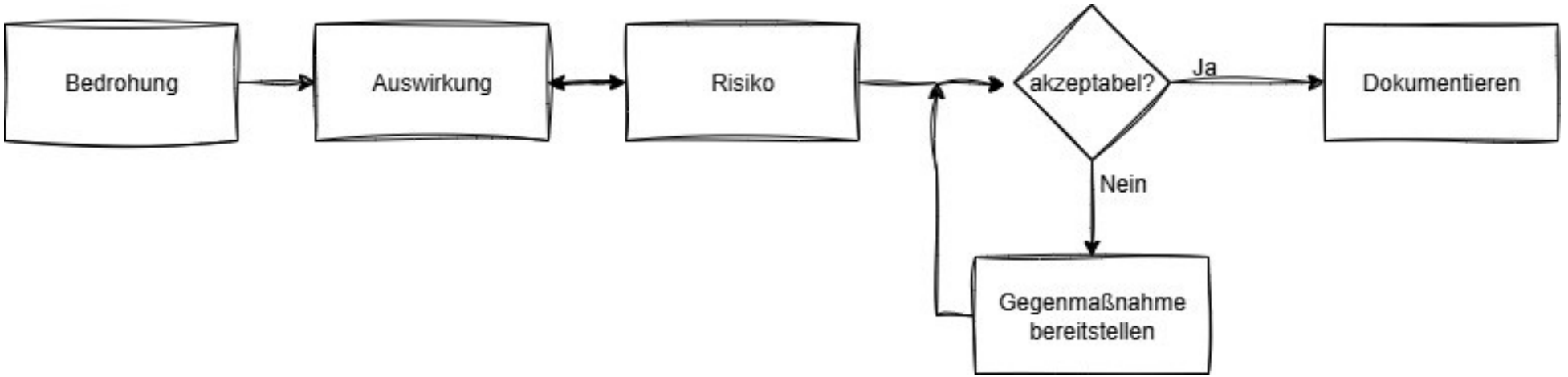
Die Risiken werden verlagert. Durch Abschluss von Versicherungen oder durch Auslagerung der risikobehafteten Aufgabe an einen externen Dienstleister kann zum Beispiel ein möglicher finanzieller Schaden (zumindest teilweise) auf Dritte abgewälzt werden.

- **Risikoakzeptanz**

Die Risiken können akzeptiert werden, sei es, weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen könnte, sei es, weil keine hinreichend wirksamen Gegenmaßnahmen bekannt sind oder aber weil der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch ist.

Mobile Experience Days 2025 by ifm

Threat and Risk Analyses / Bedrohungs- und Risikoanalyse



TARA - Beispiel



© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Beispiel - Bedrohungs- und Risikoanalyse

Diebstahl von Geräten

Feuer

Ungünstige klimatische Bedingungen

Verlust von Geräten

Wasser

Großereignisse im Umfeld



Verschmutzung, Staub, Korrosion

Sabotage

Ausfall oder Störung von Dienstleistern

Unbefugtes Eindringen in Systeme

Unberechtigte und fehlerhafte Nutzung von Geräten

Mobile Experience Days 2025 by ifm

Evolution – neue Funktion – neue Risiken





Beispiel - Bedrohungs- und Risikoanalyse



Beispiel - Bedrohungs- und Risikoanalyse

Informationen oder Produkte aus unzuverlässiger Quelle

Bedrohung

Ein Angreifer verwendet betrügerische Methoden, um einen Benutzer oder einen automatisierten Prozess dazu zu veranlassen, gefährlichen Code herunterzuladen und zu installieren, von dem angenommen wird, dass es sich um ein gültiges Update handelt, das von einer vom Angreifer kontrollierten Quelle stammt.

Risiko

$$Medium\ (3) * Hoch\ (3) = Medium\ (9)$$

Auswirkung

Das Ausführen von nicht vertrauenswürdigem Code kann die Ablaufsteuerung des Programms beeinträchtigen. Der nicht vertrauenswürdige Code kann von Angreifern gesteuerte Befehle ausführen, vertrauliche Ressourcen lesen oder ändern oder verhindern, dass die Software für legitime Benutzer ordnungsgemäß funktioniert.

Gegenmaßnahme bereitstellen

- Keine aktualisierbare Software Bereitstellen, Funktion nicht vorhanden
- Signierung und/oder Verschlüsselung der Firmware
- Bereitstellen von Hinweisen in der Dokumentation oder Überprüfung von Prüfsummen
- Das ist nicht das Problem des Herstellers oder, wir kümmern uns nicht darum

Quelle: MITRE CAPEC

Mobile Experience Days 2025 by ifm

Zusammenfassung TARA

A Bestimmen

Festlegen des Systems

Bestimmen der Schnittstellen

B Bewerten

Bedrohungs- und Risikoanalyse



C Entgegenwirken

Bereitstellen von Maßnahmen

D Dokumentieren

Erstellen der Dokumentation

Benutzeranleitung

Anleitungen

Vielen Dank

Matthias Schmidt
Director Product Security
ifm group services



© ifm • Author: Matthias Schmidt

Referenzen / Informationen / Quellen



© ifm • Author: Matthias Schmidt

Mobile Experience Days 2025 by ifm

Referenzen / Informationen / Quellen

- KI-generated, Einsatz von Microsoft CoPilot
- IEC EN 62443 Serie in Kombination mit ISO/ SAE 21434
- Threat and Risk Analyses / Bedrohungs- und Risikoanalyse, DIN EN 61010-1 August 2023
- BSI; Elementare Gefährdungen
- BSI; Risiken behandeln
- MITRE CAPEC