Security by Design

Best Practice Beispiel der Maschinenfabrik Reinhausen

01.10.2024 Dr. Hubert Feyrer

Dr. Hubert Feyrer

+ Cyber Security-Experte bei der Maschinenfabrik Reinhausen
+ 10 Jahre CISO bei Volkswagen (VW Group Services, VW Sachsen)
+ Studium in technischer Informatik der FH Regensburg
+ Promotion in Informationswissenschaften der Uni Regenburg
+ Dozent Open Source & Systemadministration in USA & Deutschland
+ Systembetreuer, Hard- und Softwareentwickler, IT-Leiter
+ Erster Vortrag beim Chaos Communications Congress vor 20 Jahren
+ Entwickler NetBSD & Mitgründer pkgsrc
+ IPv6 Pionier

Agenda

1. Unternehmensvorstellung MR
2. Best Practice: Governance
3. Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design
4. Best Practice: Cybersecurity Risk Assessment (CS-RISK)
5. Zusammenfassung & Ausblick

Agenda

1. **Unternehmensvorstellung MR**
2. Best Practice: Governance
3. Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design
4. Best Practice: Cybersecurity Risk Assessment (CS-RISK)
5. Zusammenfassung & Ausblick

Maschinenfabrik Reinhausen GmbH

Familienunternehmen seit

1868

in der sechsten Generation
in Familieneigentum

Wirtschaftlich gesund

1 Mrd.

Euro Umsatz in 2023
Höchstes Rating (AAA)

Mitarbeiter

4.000

61 Nationalitäten
an 60 Standorten

Weltmarktführer

50%

des weltweiten Stroms
fließt durch unsere Produkte

Zuverlässigkeit

50+ Jahre

OLTC-Lebensdauer beweisen die
unübertroffene MR-Produktqualität

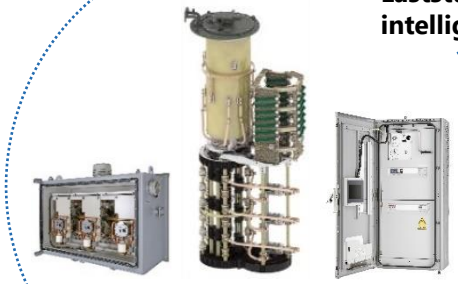
Präsent in aller Welt

8.000

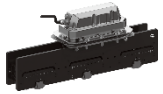
Kunden
in 185 Ländern

Maschinenfabrik Reinhausen GmbH
The Power behind Power

Transformatoren-Zubehör

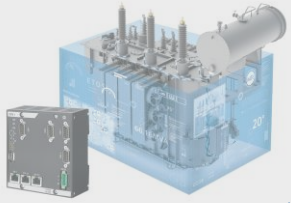


Laststufenschalter & intelligente Antriebe



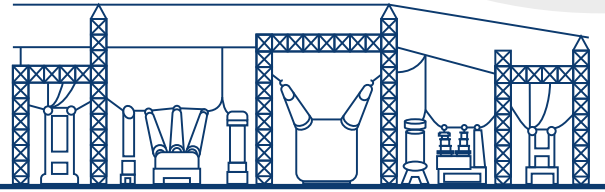
Regeltechnik für Verteiltransformatoren

Dienstleistungen im Umspannwerk



Sensorik, Automatisierung, Digitalisierung

OEM & Systemintegratoren



Netzbetreiber

Lasten & Einspeiser

Hochspannungs-Isolatoren

Hochspannungs-prüftechnik

Power Quality Lösungen

Leistungselektronische Systeme & Komponenten

Drosseln
Mittel- & Niederspannung

Agenda

1. Unternehmensvorstellung MR
2. **Best Practice: Governance**
3. Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design
4. Best Practice: Cybersecurity Risk Assessment (CS-RISK)
5. Zusammenfassung & Ausblick

Best Practice: Governance

Betroffenheit: Gesetze, Kunden

- Gesetzliche Auflagen: CRA, NIS-2, ...
- Kundenanforderungen
- Projekte: Anforderungen & Risiken, Umsetzung
- Resultierende Anforderungen an Lieferanten

Entwicklungsmodell:

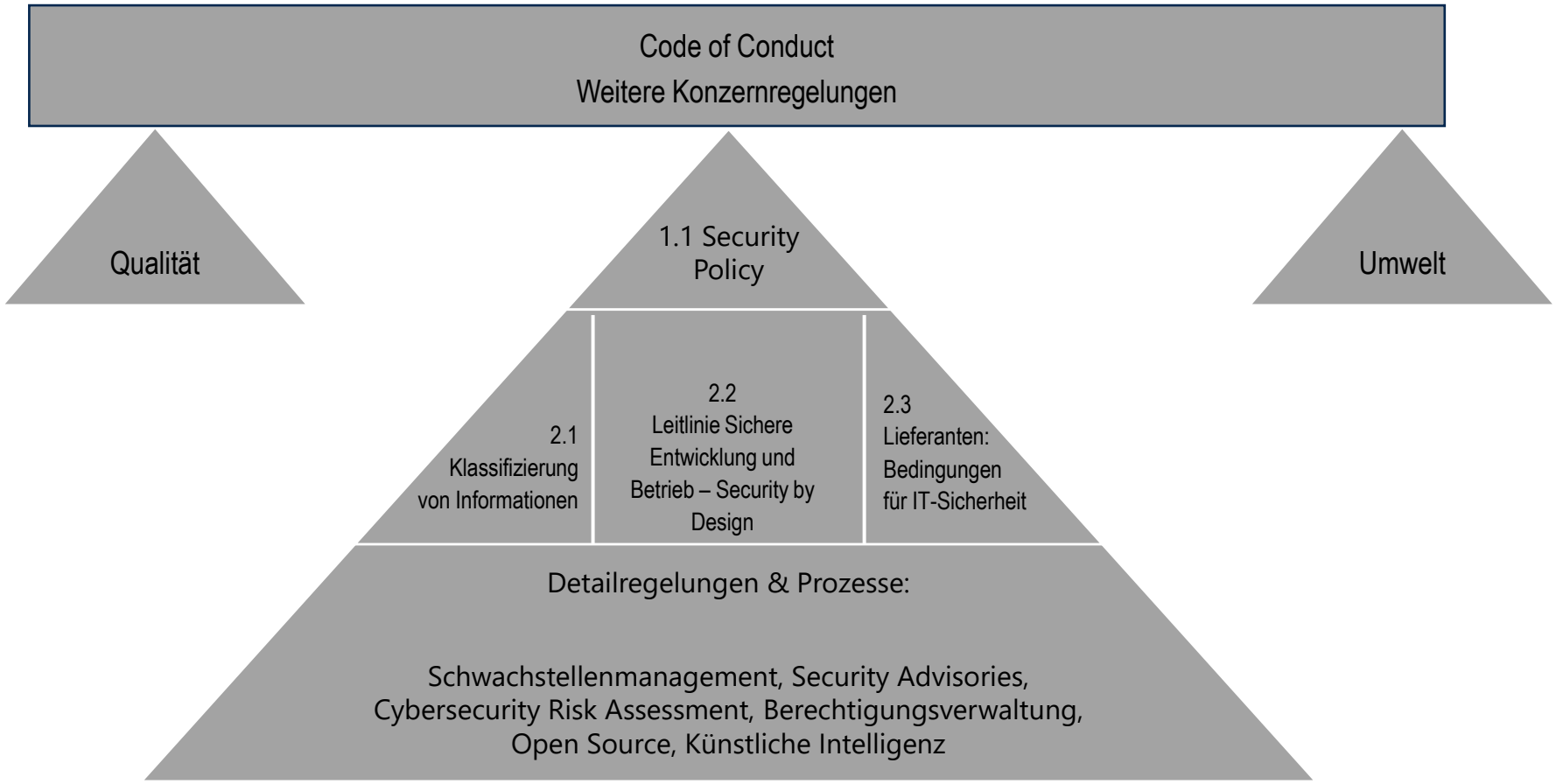
Vorgaben: von Embedded bis Web

Dokumentationspflicht

Agenda

1. Unternehmensvorstellung MR
2. Best Practice: Governance
3. **Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design**
4. Best Practice: Cybersecurity Risk Assessment (CS-RISK)
5. Zusammenfassung & Ausblick

Best Practice: Security by Design
Vorgaben zur Cybersecurity in der Produktentwicklung



Agenda

1. Unternehmensvorstellung MR
2. Best Practice: Governance
3. Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design
4. **Best Practice: Cybersecurity Risk Assessment (CS-RISK)**
5. Zusammenfassung & Ausblick

Best Practice:
Cybersecurity Risk Assessment (CS-RISK) - Überblick

Anforderungen:

+ Gesetzlich
+ Vertraglich
+ Regulatorisch
+ DSGVO / BDSG
+ ISO 27001
+ IEC 62443
+ OWASP Top 10
+ MITRE EMB3D
+ NIST
+ NERC CIP
+ CRA (Entwurf)
+ ...

Cybersecurity Risk Assessment

Datenklassifikation: Schutzbedarf

+ Verfügbarkeit
+ Vertraulichkeit
+ Integrität
+ Hosting

Sicherheitsmaßnahmen:

+ ...
+ ...
+ ...

Projekt:

+ Prämissen
+ Maßnahmen
+ Umsetzung

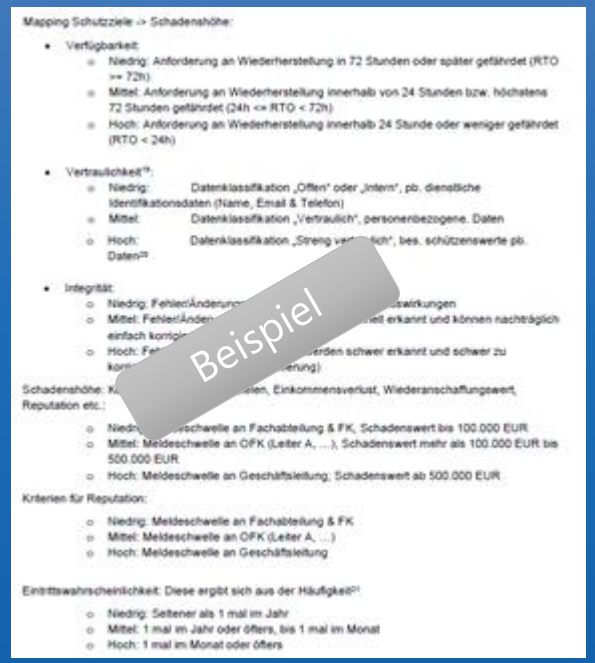
=> Dokumentation

Best Practice:
Cybersecurity Risk Assessment (CS-RISK) - Beratungsprozess

				Im Lead
1. Grundlage: Leitlinie für sichere IT/OT Entwicklung und Betrieb - Security by Design				
2. Cybersecurity Risk Assessment:				
	Teil 1: Basisinformation & **Datenklassifikation**			
		1.	**Überblick** über Projekt an IT-Security: 1) Fachkonzept 2) IT-Konzept 3) IT-Security-Konzept (wenn Vorhanden)	Projekt
		2.	**Allgemeine Daten** zum Datenstand, Projekt, wer die Bewertung von Seiten IT-Security und Fachbereich durchgeführt hat	IT-Security
		3.	**Datenklassifikation**: Hilfe siehe ISMS-Risikomanagement, v.a. für Wertebereiche Verfügbarkeit, Vertraulichkeit, Integrität	IT-Security
		4.	**Weitere Angaben**: Je nach Projekt	IT-Security
	Teil 2: **Maßnahmen** & Umsetzung			
		1.	Nach Befüllen von Teil 1 werden die bekannten Maßnahmen anhand der Datenklassifikation bewertet und als **relevant / nicht relevant** markiert	IT-Security
		2.	Im Rahmen der IT-Security Bewertung werden Maßnahmen bzgl. Relevant **geprüft, besprochen**	IT-Security
		3.	Anschließend erfolgt **Übergabe** an das Entwicklungsprojekt	IT-Security
		4.	**Umsetzung** der relevanten Anforderungen / Maßnahmen im Projekt, Doku wie umgesetzt in Spalten "Umgesetzt" und "Wie umgesetzt?"	Projekt
		5.	**Abweichungen**: Punkte, die nicht umgesetzt werden, sind im Projekt bzgl. der resultierenden Risiken zu bewerten, ggf. inkl. IT-Security	Projekt
		6.	**Review**: Am Ende des Projektes erfolgt Durchsprache der Umsetzung und verbleibenden Risiken mit IT-Security	Projekt
		7.	**Ablage** der Projekt-Risikoliste	IT-Security
		8.	Bewertung der Restrisiken und ggf. Aufnahme der verbleibenden Risiken in bestehendes **Risikomanagement** (ISMS / Turtle)	IT-Security

Best Practice:
Cybersecurity Risk Assessment (CS-RISK) - Schutzbedarf

Risikomanagement: Wertgrenzen



Mapping Schutzziele -> Schadenshöhe:

- Verfügbarkeit:
  - Niedrig: Anforderung an Wiederherstellung in 72 Stunden oder später gefährdet (RTO >= 72h)
  - Mittel: Anforderung an Wiederherstellung innerhalb von 24 Stunden bzw. höchstens 72 Stunden gefährdet (24h <= RTO < 72h)
  - Hoch: Anforderung an Wiederherstellung innerhalb 24 Stunde oder weniger gefährdet (RTO < 24h)
- Vertraulichkeit[3]:
  - Niedrig: Datenklassifikation „Offen" oder „Intern", pb. dienstliche Identifikationsdaten (Name, Email & Telefon)
  - Mittel: Datenklassifikation „Vertraulich", personenbezogene. Daten
  - Hoch: Datenklassifikation „Streng ver… lich", bes. schützenswerte pb. Daten[4]
- Integrität:
  - Niedrig: Fehler/Änderung… …swirkungen
  - Mittel: Fehler/Änden… …eit erkannt und können nachträglich einfach korrigi…
  - Hoch: Fe… …erden schwer erkannt und schwer zu ko… …erung)

Beispiel

Schadenshöhe: K… …ien, Einkommensverlust, Wiederanschaffungswert, Reputation etc.:

- Niedr… …schwelle an Fachabteilung & FK, Schadenswert bis 100.000 EUR
- Mittel: Meldeschwelle an OFK (Leiter A, …), Schadenswert mehr als 100.000 EUR bis 500.000 EUR
- Hoch: Meldeschwelle an Geschäftsleitung, Schadenswert ab 500.000 EUR

Kriterien für Reputation:

- Niedrig: Meldeschwelle an Fachabteilung & FK
- Mittel: Meldeschwelle an OFK (Leiter A, …)
- Hoch: Meldeschwelle an Geschäftsleitung

Eintrittswahrscheinlichkeit: Diese ergibt sich aus der Häufigkeit[5]:

- Niedrig: Seltener als 1 mal im Jahr
- Mittel: 1 mal im Jahr oder öfters, bis 1 mal im Monat
- Hoch: 1 mal im Monat oder öfters

Datenklassifikation

Datenklassifizierung:	(Hilfe)	
Verfügbarkeit:		TODO
Vertraulichkeit:		TODO / hoch / mittel / niedrig
Integrität:		TODO
Weitere:		
Erreichbarkeit via Internet:		TODO
Hosting Extern / Cloud:		TODO

Schutzbedarf:

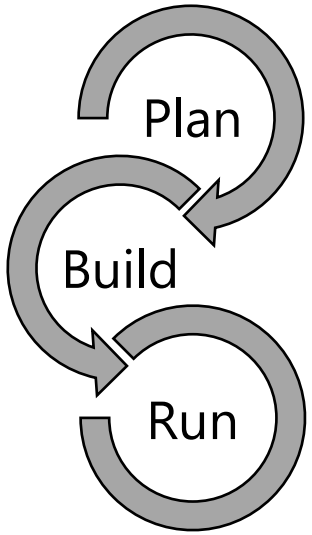
Relevanz von Maßnahmen:

Relevant	Maßnahme
	Plan: Datenklassifikation
ja	Datenklassifikation durchgeführt, siehe ISMS-Handbuch, Kapitel „7.1.2 Bewertungskriterien & Quantifizierung:"

Festlegung jeweils basierend auf Datenklassifikation
=> Regelsatz

Best Practice:
Cybersecurity Risk Assessment (CS-RISK) - Maßnahmen

+ Stark abhängig von Maßnahmen, Anforderungen, Risikogrenzen
+ Beispiel MR Kategorien:



MR: ca. 60 Maßnahmen

Sicherheitsmaßnahmen (Kategorien):

+ Plan: Datenklassifikation
+ Plan: Anmeldung – Authentifizierung
+ Plan: Berechtigungen - Authorisierung
+ Plan: Verschlüsselung - Kryptographie
+ Plan: Protokollierung
+ Build: Sichere Codierung
+ Plan: Sicherer Betrieb
+ Plan: Notfallmanagement
+ Plan: Datenschutz (Privacy by Design)
+ Weitere
+ Regelmäßige Neubewertung

Best Practice:
Cybersecurity Risk Assessment (CS-RISK) – Beispiel: CRA

- EU Cyber Resilience Act, Arbeitsstand Anfang 2024
- Beispiel: Ableitung von Maßnahmen (Auszug)

Sicherheitsmaßnahmen (Kategorien):

Maßnahme
Eingabe-Validierung: Testen von Mindest- und Höchstlängen (z.B. Buffer Overflows), Umlaute, Einfügen von Steuerbefehlen (z.B. SQL Injection, XSS) (EU Cyber Resilience Act, Annex I 1.(3)(i))
Produkte sind gehärtet und in einer sicheren Default Konfiguration und mit minimaler Angriffsoberfläche auszuliefern. Die Möglichkeit zum Factory-Reset muss bestehen. (EU Cyber Resilience Act, Annex I 1.(3)(a) und (h))
Eine vollständige Liste aller Software Componenten (Software Bill of Materials, SBOM) inkl. aller Abhängigkeiten ist zu erstellen, aktuell zu halten bei Änderungen / Updates und auch in der Benutzer- und Betriebsanleitung abzudrucken. (EU Cyber Resilience Act, Annex I 2.(1), Annex II und V)
Bei Schwachstellen in Produkten sind Sicherheits-Updates für Kunden bereitzustellen (z.B. über das MR myReinhausen Kundenportal) und Kunden / Benutzer bei schweren Schwachstellen in Form von Security Advisories zu informieren. Kontakt zur Erstellung von Security Advisories: MR-CERT (EU Cyber Resilience Act, Annex I 1.(3)(k) und 2.(4))

Agenda

1. Unternehmensvorstellung MR
2. Best Practice: Governance
3. Best Practice: Vorgaben zur Cybersecurity in der Produktentwicklung – Security by Design
4. Best Practice: Cybersecurity Risk Assessment (CS-RISK)
5. **Zusammenfassung & Ausblick**

Zusammenfassung

+ Governance
+ Vorgaben zur Cybersecurity in der Produktentwicklung
+ Cybersecurity Risk Assessment (CS-RISK)

Anforderungen

CS Risk Assessment

Datenklassifikation: Schutzbedarf

Sicherheits-maßnahmen

Projekt:

+ Prämissen
+ Maßnahmen
+ Umsetzung

=> Dokumentation

Software Development Life Cycle Management (SDLC/SSDLC)

Ausblick

+ Big Picture: (Security) Software Development Life Cycle – hier nur Fokus auf Design

+ Für Produktpflege: Schwachstellenmanagement -> u.a. Heise devSec() 2023

+ Bedrohungslage im Auge behalten – Gesetzlich, Kundenumfeld, Technisch, Organisatorisch

+ Dranbleiben – kontinuierliche Verbesserung, Managementsystem (ISMS)

+ Anfangen!

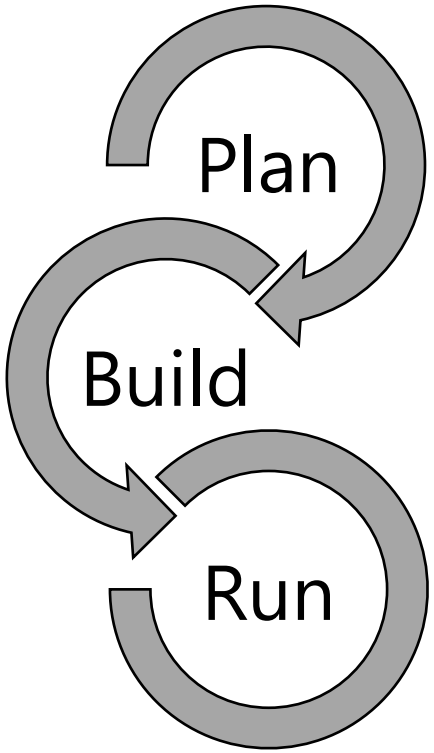
THE POWER BEHIND POWER.

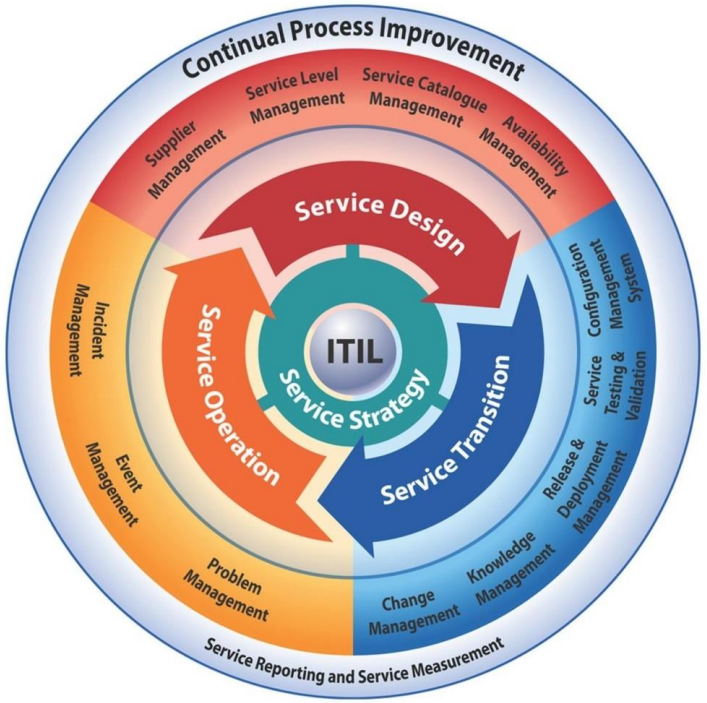
reinhausen.com

Governance: Anforderungen

- Gesetzliche Auflagen: CRA, NIS-2, …
- Kundenanforderungen
- Projekte: Anforderungen & Risiken, Umsetzung
- Resultierende Anforderungen an Lieferanten

Governance: Entwicklungsmodell





Governance: Leitplanken für alle
Von Embedded bis Web Entwicklung

Governance: Dokumentation & Nachweise

Auflagen:

+ Cyber Resilience Act
+ Datenschutz
+ Produkthaftung
+ Etc.