

Security Updates – Klingt einfach, aber ist es das auch?

Die verborgene Komplexität der CRA-
Umsetzung

Dr. Nils O. Abeling

Technologieforum „Industrial Security – CRA“

Nürnberg 29.09.2026



Wer bin ich?



**Dr. Nils O.
Abeling**

- Senior Consultant im Bereich „Critical Infrastructures“
- Schwerpunkte: PKI, PQC und regulatorische Compliance in IT und OT
- Neue Themen

Mail: nils.abeling@secunet.com

secunet auf einen Blick

Daten & Fakten

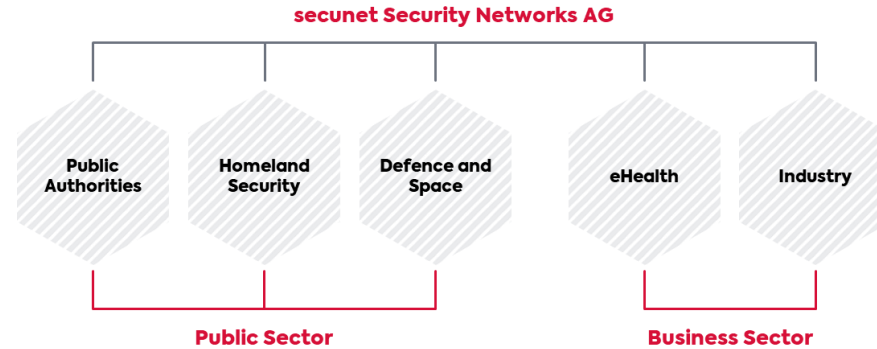
-  Gegründet 1997
-  458m Euro Umsatz (25)
-  51m Euro EBIT (25)
-  13 Standorte in Deutschland
-  ~1.200 Mitarbeiter
-  Hauptanteilseigner: 
-  IT Sicherheitspartner 

Kunden



... und viele mehr

Firmenstruktur



Tochtergesellschaften



Beispiele aus dem Kerngeschäft

- > 250.000 Installationen Hochsichere IT-Infrastruktur 
- 25 Jahre PKI Erfahrung
- > 480 installierte easygates in ganz Europa
- > 84.000 Telematikinfrastruktur-Konnektoren installiert
- secunet edge: IIoT-Gateway zur Anbindung von Maschinen an Cloud-Plattformen für Industrie 4.0
- > 1,3 Millionen aktive Stashcat-Benutzer (Business-Messenger)
- Cybersicherheitsberatung für DAX-Konzerne & Behörden
- Entwicklung eines hochsicheren Cloud-Ökosystems

Unsere Produkte



... und viele mehr

Portfolio und Märkte

Produkte

**BSI-zugelassene
Verschlüsselungslösungen**
**Biometrie-, ID- und
Grenzkontroll-Systeme**
PKI-Lösungen
Sichere IoT-Plattformen

Beratung

Sicherheitskonzepte
IT-Grundschutz / ISMS
**Sicherheitsdesign und
-architekturen**
Penetrationstests

Service

Managed Security Services
Netzwerk-Überwachung
**Implementierungs-
dienstleistungen**
**Support, Wartung und
Betrieb**

Industrie

Sicherheitsarchitekturen für
kritische Netzwerke
IIoT- und Edge-Computing-
Plattformen
Sicherer Fernzugriff mit SINA
und secunet edge
ISMS, Penetrationstests und
Sensibilisierungsschulungen
Cyber-Sicherheit für
Automotive

Gesundheits- markt

Sichere Anbindung von
Arztpraxen und
Krankenhäusern an die
Telematik-Infrastruktur
Entwicklung einer sicheren
Plattform für das deutsche
Gesundheitssystem

Sicherheits- Behörden

Mobile, stationäre und
automatisierte
Grenzkontrollsysteme
Sicherheitslösungen für die
Erfassung und Verarbeitung
biometrischer Daten
Lösungen für die elektronische
Verarbeitung von Verschlusssachen

Verwaltungen

Sicherung von Regierungsnetzwerken
Sichere mobile Endgeräte
Sichere Authentifizierung für
Webanwendungen und Portale
Schutz von eGovernment-
Anwendungen

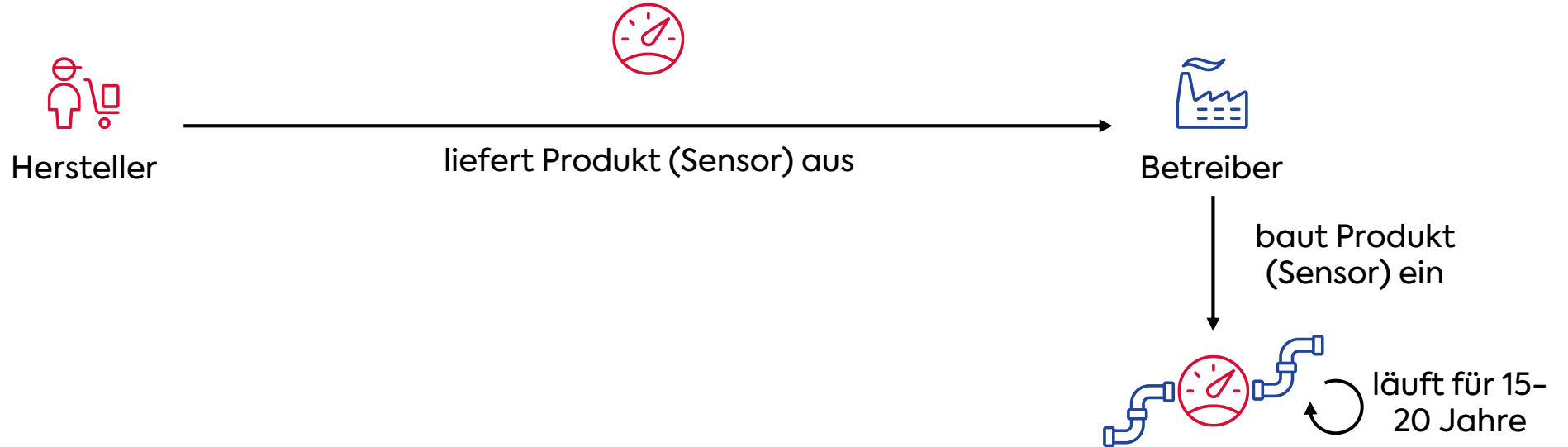
Verteidigung und Raumfahrt

Sichere Netzwerk-
architekturen für
Bundeswehr- und
Missionsnetze
Verschlüsselungslösungen
für eingestufte Daten bis
GEHEIM/NATO SECRET
Sichere Clients und Gateways
Robuste Sicherheitslösungen
für herausfordernde Einsatz-
umgebungen

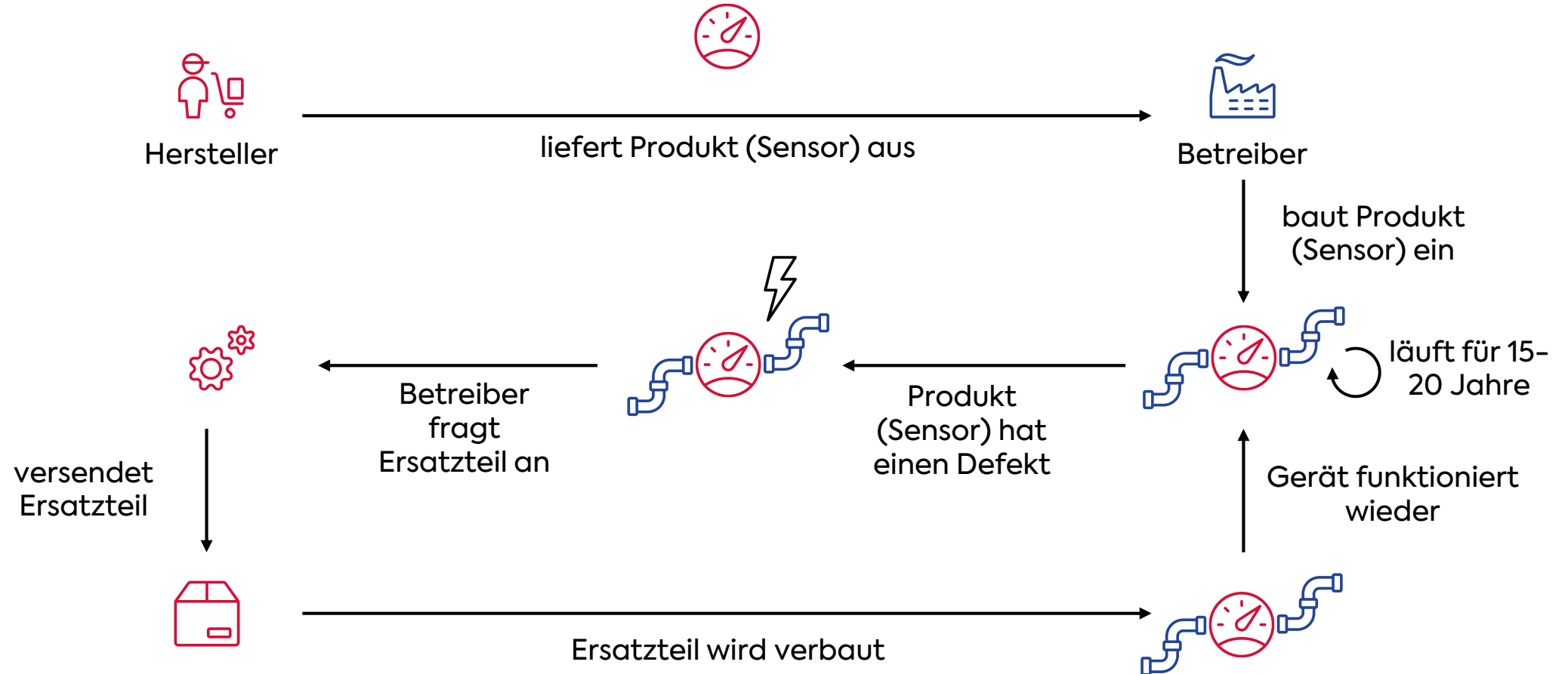
Anforderungen an den Hersteller Früher



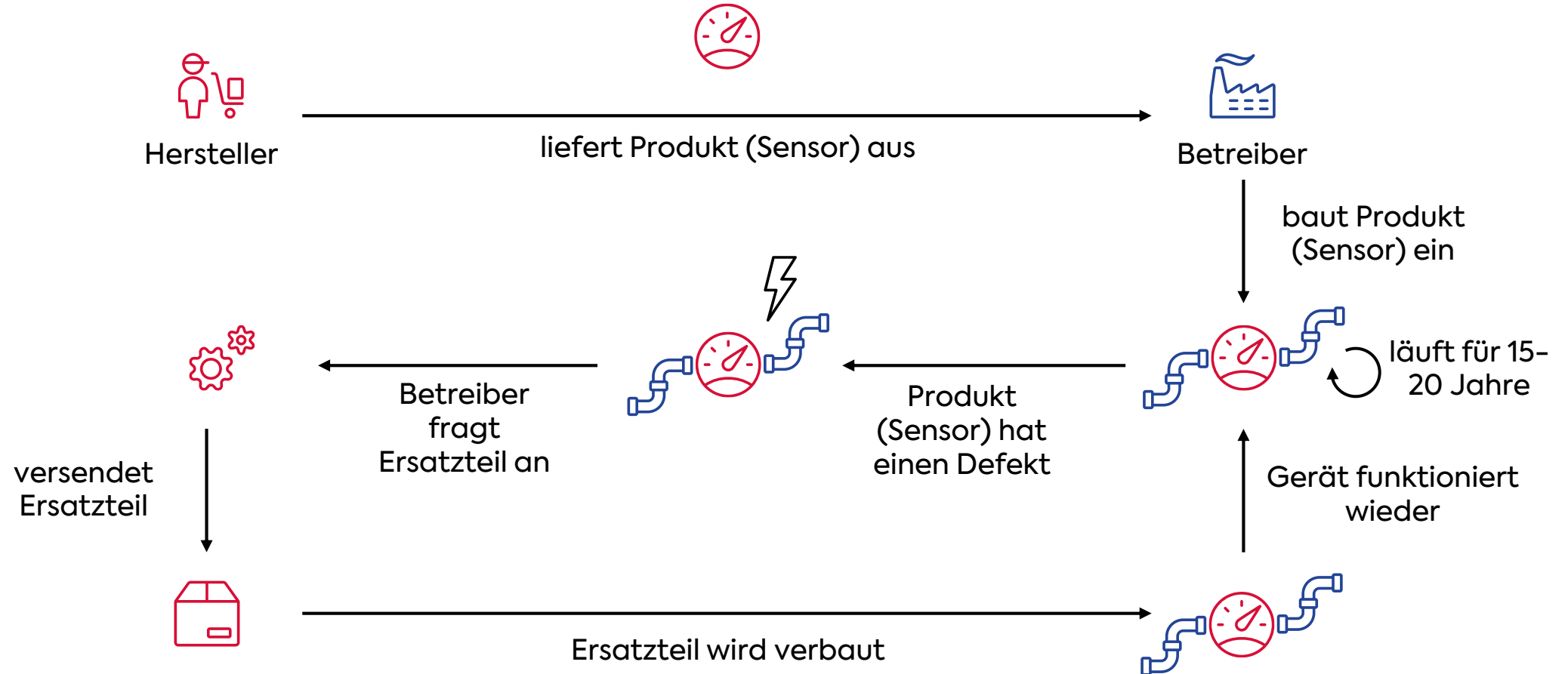
Anforderungen an den Hersteller Früher



Anforderungen an den Hersteller Früher



Anforderungen an den Hersteller Früher



- Keine Security-Updates
- Kaum strukturierte Kommunikation zwischen Hersteller und Betreiber

Anforderungen an den Hersteller: CRA Heute



CRA:

-  Secure-by-Design, Secure-by-Default, Updatefähigkeit
-  Dokumentation (Technische Dokumentation (z. B. Produktinformationen, Produktkontext, SBOM, Nachweise,...), Nutzerinformationen für Betreiber)
-  Eindeutige Versionsstände und klare Supportzeiträume
-  Sichere Entwicklung, Schwachstellenmanagement, Security-Updates
-  Meldewesen

Anforderungen an den Betreiber: NIS2 Heute



Hersteller



liefert Produkt (Sensor) aus



Betreiber

CRA:



Secure-by-Design, Secure-by-Default, Updatefähigkeit



Dokumentation (Technische Dokumentation (z. B. Produktinformationen, Produktkontext, SBOM, Nachweise,...), Nutzerinformationen für Betreiber)



Eindeutige Versionsstände und klare Supportzeiträume



Sichere Entwicklung, Schwachstellenmanagement, Security-Updates



Meldewesen

NIS2:



Systematische Risikoanalysen



Lieferkettenrisiken



Organisatorische wie technische Maßnahmen



Asset-Management



Incident-Response und Meldepflichten (NIS2)



Patch- und Schwachstellenmanagement

Mehrarbeit für Betreiber = Mehrarbeit für Hersteller



Betreiber brauchen künftig Antworten auf Fragen wie:



Ist das Produkt über die **Nutzungsdauer** **updatefähig**?



Wie werden **Schwachstellen** gemeldet, bewertet und behoben?



Welche **Nachweise** bekomme ich für Audit, Risikoanalyse und Lieferantenbewertung?



Wie kann ich **Updates testen** und kontrolliert **ausrollen**?

Mehrarbeit für Betreiber = Mehrarbeit für Hersteller



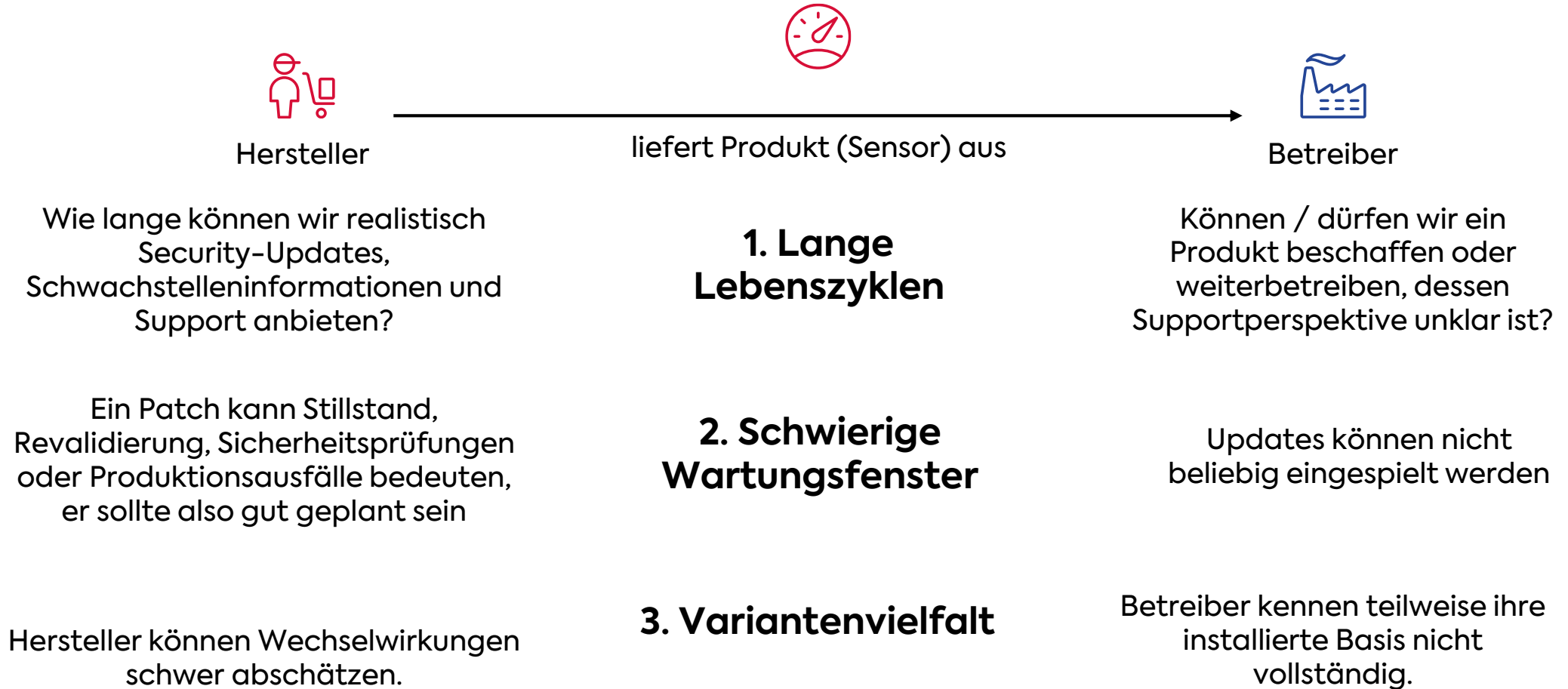
Hersteller brauchen künftig folgende Antworten / Lösungen:

-  **Supportzeitraum festlegen und Sicherheitsupdates bereitstellen**
-  **Vulnerability-Handling-Prozess inkl. Meldeweg**
-  technische Dokumentation und Nachweise vorbereiten
-  Test-, Rollout- und Fallback-Konzepte

Betreiber brauchen künftig Antworten auf Fragen wie:

-  ← Ist das Produkt über die **Nutzungsdauer** **updatefähig**?
-  ← Wie werden **Schwachstellen** gemeldet, bewertet und behoben?
-  ← Welche **Nachweise** bekomme ich für Audit, Risikoanalyse und Lieferantenbewertung?
-  ← Wie kann ich **Updates testen** und kontrolliert **ausrollen**?

Warum ist das in der OT ein Problem?



Konkretes Beispiel für Komplexität: Updates



Hersteller brauchen künftig folgende Antworten / Lösungen:

-  **Supportzeitraum festlegen und Sicherheitsupdates bereitstellen**
-  **Vulnerability-Handling-Prozess inkl. Meldeweg**
-  technische Dokumentation und Nachweise vorbereiten
-  Test-, Rollout- und Fallback-Konzepte

Betreiber brauchen künftig Antworten auf Fragen wie:

-  Ist das Produkt über die **Nutzungsdauer** **updatefähig?**
-  Wie werden **Schwachstellen** gemeldet, bewertet und behoben?
-  Welche **Nachweise** bekomme ich für Audit, Risikoanalyse und Lieferantenbewertung?
-  Wie kann ich **Updates testen** und kontrolliert **ausrollen**?

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 1: Technische Produktfähigkeit

Das Produkt muss Updates überhaupt sicher annehmen können. Dafür braucht es die richtige Architektur.

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 1: Technische Produktfähigkeit

Das Produkt muss Updates überhaupt sicher annehmen können. Dafür braucht es die richtige Architektur.

Dazu gehören:

-  eindeutige Produkt- und Versionsidentität
-  signierte Updatepakete
-  Prüfung von Authentizität & Integrität
-  Secure Boot oder vergleichbare Integritätsmechanismen
-  Rollback- und Recovery-Fähigkeit
-  Schutz gegen Downgrade-Angriffe
-  Trennung von Firmware, Konfiguration und Prozessdaten
-  Kompatibilität mit verschiedenen Hardware-Revisionen

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 1: Technische Produktfähigkeit

Das Produkt muss Updates überhaupt sicher annehmen können. Dafür braucht es die richtige Architektur.

Dazu gehören:

-  eindeutige Produkt- und Versionsidentität
-  signierte Updatepakete
-  Prüfung von Authentizität & Integrität
-  Secure Boot oder vergleichbare Integritätsmechanismen
-  Rollback- und Recovery-Fähigkeit
-  Schutz gegen Downgrade-Angriffe
-  Trennung von Firmware, Konfiguration und Prozessdaten
-  Kompatibilität mit verschiedenen Hardware-Revisionen

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 2: Schlüssel- und Identitätsmanagement

Sobald Updates signiert werden, braucht der Hersteller ein Schlüsselmanagement. Der eigentliche Aufwand liegt oft in der Vertrauensinfrastruktur dahinter.

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 2: Schlüssel- und Identitätsmanagement

Sobald Updates signiert werden, braucht der Hersteller ein Schlüsselmanagement. Der eigentliche Aufwand liegt oft in der Vertrauensinfrastruktur dahinter.

Dazu gehören:



Wer darf Releases signieren?



Wo liegen private Schlüssel?



Wie werden Schlüssel rotiert?



Was passiert bei Schlüssel-Kompromittierung?



Wie werden alte Geräte im Feld mit neuen Vertrauensankern versorgt?



Gibt es eine PKI oder ein alternatives Vertrauensmodell?



Wie werden Produktions-, Test- und Kundenumgebungen getrennt?

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 3: Release- und Freigabeprozess

Ein Security-Fix muss entwickelt, getestet, freigegeben und kommuniziert werden. Sie sind ein organisationsweiter Prozess.

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

Herausforderung 3: Release- und Freigabeprozess

Ein Security-Fix muss entwickelt, getestet, freigegeben und kommuniziert werden. Sie sind ein organisationsweiter Prozess.

Dazu gehören:

- | | | | |
|---|--|---|--|
|  | Security-Triage |  | Dokumentation der behobenen Schwachstelle |
|  | Regressionstests |  | Risikobewertung für nicht patchbare Versionen |
|  | Kompatibilitätsmatrix |  | Abstimmung mit Service und Kundenkommunikation |
|  | Freigabe durch Produktmanagement, Engineering und Security | | |

Die Anforderungen gehen nicht nur in die Breite, sondern auch in die Tiefe

Auf dem Papier klingt „**Security-Updates bereitstellen**“ einfach.
Im OT-Bereich bedeutet das aber:

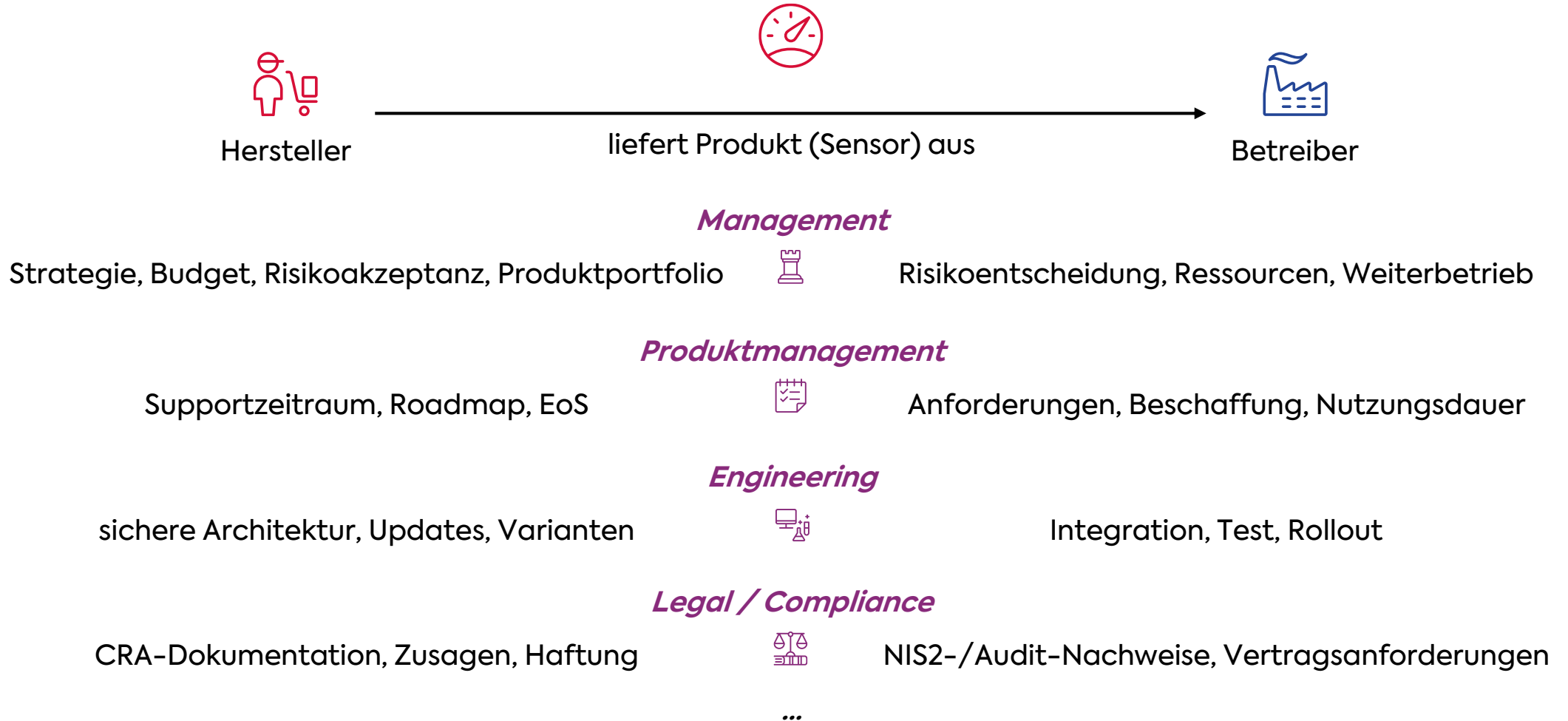
Herausforderung 4: Betriebsrealität beim Betreiber

Der Betreiber muss entscheiden, wann und wie er das Update einspielt. Ob daraus Risikoreduktion wird, entscheidet sich im Betrieb.

Dazu gehören:

-  Wartungsfenster
-  Testumgebung
-  Validierung
-  Backup und Wiederanlauf
-  Fallback-Plan
-  Dokumentation für Audit und Risikomanagement
-  temporäre Kompensationsmaßnahmen, wenn ein Patch nicht sofort möglich ist

Fazit: Für die CRA-Erfüllung werden viele benötigt



secunet