Cybersecurity ›

Vortrag anlässlich der Spreewindtage 2019
Dipl.-Ing. Florian Lütticken
Prozess- & Informationstechnologie Erneuerbare
Betrieb Erneuerbare Energien
6. November 2019

EnBW

IT Sicherheit – Eine Einführung

Es gibt genügend Gründe für IT-Sicherheit

SICHERHEIT DER STROMVERSORGUNG

27.10.2018

Experte: Windparks nicht sicher genug gegen Cyber-Angriffe

Farbenprächtig leuchten Wolken am Morgenhimmel kurz vor Sonnenaufgang über

Angriffs-Kampagne gegen Energie-Firmen und andere KRITIS-Sektoren

CSW-Nr. 2018-200628-10k3, Version 1.0, 13.06.2018

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner frei weitergegeben werden. Die Information dürfen jedoch nicht veröffentlicht werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum finden Sie am Ende dieses Dokumentes.

erheitswarnung

Sachverhalt

Im Sommer 2017 warnte das BSI seine Partner im Sektor Energie darüber, dass sich Hinweise verdichtet wonach eine oder mehrere Tätergruppen langfristige Anstrengungen unternehmen, um Energie-Infrastrukturen auszuspionieren. Dafür sprachen sowohl aktuelle Meldungen über Spearphishing-Angr auf amerikanische und europäische Energie-Unternehmen und Kernkraftwerks-Betreiber, als auch eine Reihe von Kampagnen der letzten Jahre. Zu diesem Zeitpunkt lagen nur Einzelbeobachtungen von nicht-erfolgreichen Angriffsversuchen in Deutschland vor. Dennoch sah das BSI dies als Anlass genug, um deutsche Energie-Unternehmen mit Indikatoren zur Detektion von Angriffen und mit Präventions-Empfehlungen zu versorgen.

Auch internationale Partner haben in der letzten Zeit vor Angriffen auf den Energie-Sektor und andere Kritische Infrastrukturen gewarnt (z.B. [14]).

Das IT-Sicherheitsgesetz

Kritische Infrastrukturen schützen

Cyber-Sicherheitslage 2019

Top 10 Bedrohungen für Industrial Control Systems - Prozess-IT (OT)

Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	↗
Infektion mit Schadsoftware über Internet und Intranet	↗
Menschliches Fehlverhalten und Sabotage	↑
Kompromittierung von Extranet und Cloud-Komponenten	↑
Social Engineering und Phishing	↘
(D)DoS Angriffe	↑
Internet-verbundene Steuerungskomponenten	→
Einbruch über Fernwartungszugänge	→
Technisches Fehlverhalten und höhere Gewalt	↘
Kompromittierung von Smartphones im Produktionsumfeld	→

Quelle: BSI-CS 005 „Industrial Control System Security -Top 10 Bedrohungen und Gegenmaßnahmen 2019“

Informationssicherheits-Gesetz
Sachstand

§

- Am 12.06.2015 wurde im Bundestag das IT-Sicherheitsgesetz verabschiedet.
  Es wirkt auf folgende EU-Wirtschaftssektoren: **Energie**, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasserversorgung, Ernährung sowie Finanz- und Versicherungswesen
- Es hat das Ziel, die **IT-Sicherheit** von Einrichtungen und Dienstleistungen zu erhöhen, die von **hoher Bedeutung** für das Funktionieren des **Gemeinwesens** sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.
- Aufteilung in **kritische** und unkritische Infrastruktur

Schwellwerte für kritische Infrastrukturen

Energieanlagen	420 MW
Dezentrale Energieerzeugungsanlagen	420 MW
Speicheranlagen	420 MW
Anlagen von Poolanbietern	420 MW

Pflichten für die Betreiber kritischer Infrastrukturen

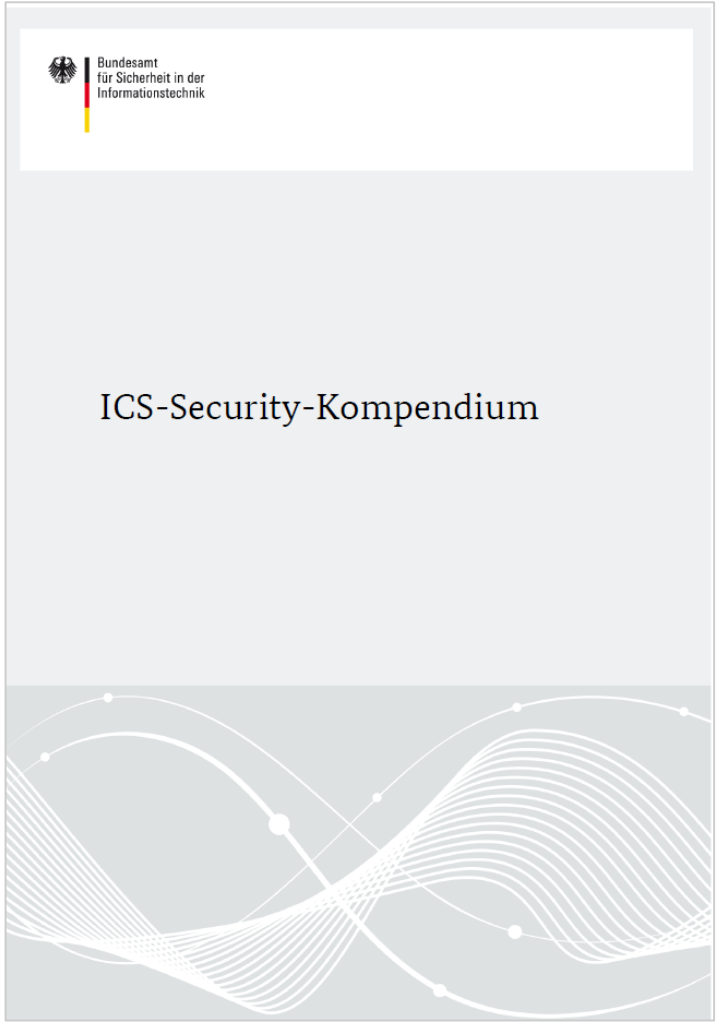
- Einrichten eines Meldeweges und einer Kontaktstelle für Sicherheitsvorfälle
- Informationssicherheitsmanagementsystem (ISMS)
- Umsetzung von IT-Sicherheitsmaßnahmen (IT-Sicherheitskatalog)

Maßnahmenkataloge zur Absicherung von IT- und OT-Komponenten

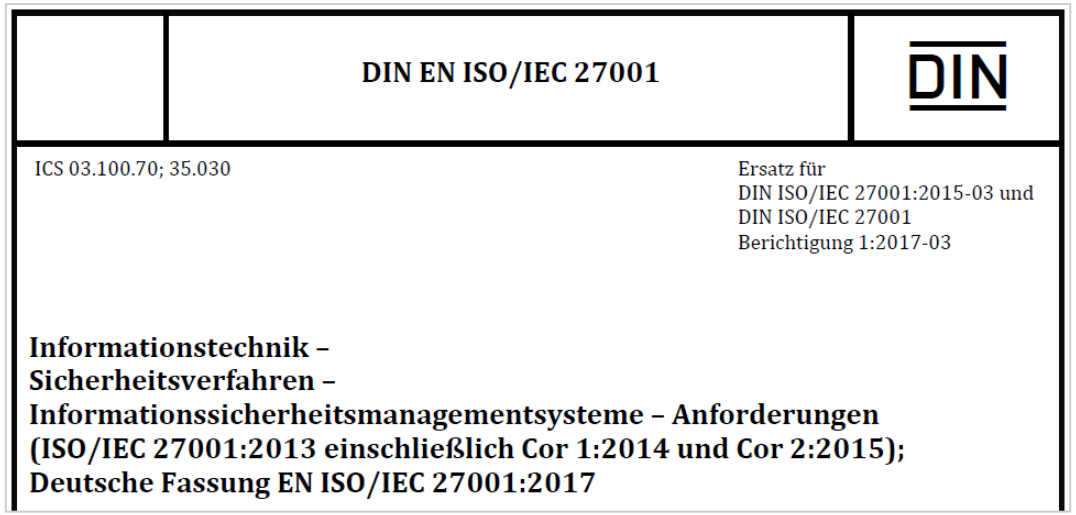
Überblick

- Anerkannte Anforderungs-bzw. Maßnahmenkataloge liefern die typischerweise **umzusetzenden Anforderungen bzw. Maßnahmen** „auf dem Silbertablett“
- Ermöglicht einen **schnellen Einstieg in die Absicherung** konkreter IT-Landschaften oder einzelner IT-Komponenten
- **Keine explizite Risikoanalyse erforderlich**

- **Handlungsempfehlungen** aus BSI CS 005 „Industrial Control System Security Top 10 Bedrohungen und Gegenmaßnahmen 2019“
- **ICS Security Kompendium des BSI** (Kap. 5 Practice Guide für Betreiber)
- **VGB S 175** „IT Sicherheit für Erzeugungsanlagen“
- **BDEW Whitepaper** „Anforderungen an sichere Steuerungs und Telekommunikationssysteme”
- **“Recommended Practices”** für ICS des US Department of Homeland Security
- **Bausteine des BSI Kompendiums**



Informationssicherheitsmanagementsystem (ISMS) nach DIN/ISO 27001



DIN EN ISO/IEC 27001

DIN

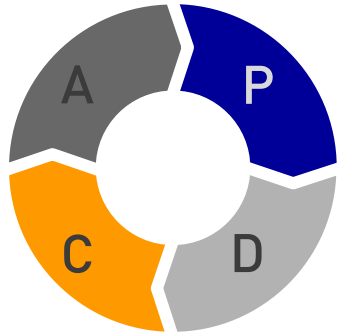
ICS 03.100.70; 35.030

Ersatz für
DIN ISO/IEC 27001:2015-03 und
DIN ISO/IEC 27001
Berichtigung 1:2017-03

**Informationstechnik –
Sicherheitsverfahren –
Informationssicherheitsmanagementsysteme – Anforderungen
(ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015);
Deutsche Fassung EN ISO/IEC 27001:2017**

Ein Information Security Management System (**ISMS**) ist die Aufstellung von **Verfahren und Regeln** innerhalb einer Organisation, die dazu dienen, die **Informationssicherheit** dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

DIN/ISO 27001



- Beschreibt im ersten Teil primär den Aufbau eines Managementsystemes für Informationssicherheit
- Analogien zur DIN/ISO 9000

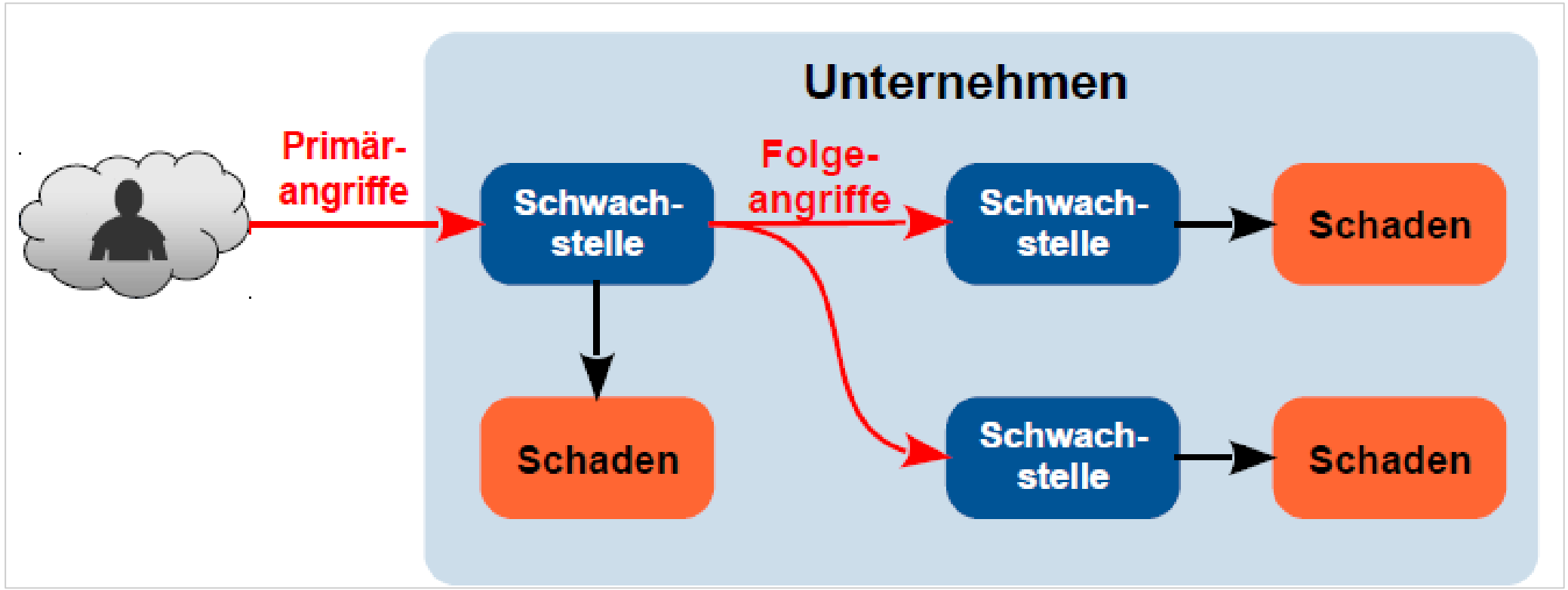
Anhang A

Aufzählung von definerten Maßnahmen zur Erhöhung der IT-Sicherheit

- Personalsicherheit
- Assetmanagement
- Zutrittskontrolle, Physische und Umgebungsbezogene Sicherheit
- Verschlüsselung & Kommunikationssicherheit
- Betriebssicherheit
- Beschaffung, Entwicklung und Wartung von Informationssystemen
- Lieferantenbeziehungen

Maßnahmen – Was sollte ich tun?

Fokus der Bedrohungsliste liegt auf Primärangriffen, mit denen Angreifer in industrielle Anlagen und Unternehmen initial eindringen



Quelle: BSI-CS 005 „Industrial Control System Security -Top 10 Bedrohungen und Gegenmaßnahmen 2019“

! Schutzmaßnahmen vor Primärangriffen sollten vorrangig umgesetzt werden

Zugriffe auf Windkraftanlagen

Angriffsvektoren für Primärangriffe

Verschiedene Parteien haben unterschiedlichen Zugriff auf eine Erzeugungsanlage.

Risiken

- Hardware vor Ort kann nur bedingt gegen unbefugte Zugriffe (physisch) geschützt werden.
- Die Lieferanten haben während der Vollwartungsverträge meist direkten Zugriff auf die Anlage
- Das Parknetzwerk und alle darin befindlichen Komponenten sind für den Betreiber meist eine BlackBox, da die Verantwortung während der Vollwartungsverträge beim Hersteller liegt
- Bei älteren Anlagen teils veraltete Hard- und Software

Das Parknetzwerk muss als nicht sicheres Netz betrachtet werden.

Maßnahmen

- Hersteller sollen bei Neuprojekten vertraglich zu einem Mindeststandart an IT-Securitymaßnahmen und einer Mitwirkungspflicht verpflichten
- Mehr Transparenz und tiefere IT-Dokumentation zur Erkennung der IT-Risiken beim Hersteller einfordern
- Kontrolle des Internetzugangs = Kontrolle des Datenflusses

Mindestmaßnahmen zur Härtung der IT-Sicherheit
Best-Practise

- **Deaktivierung nicht benötigter Services und Dienste**
- Sichere Installation und Konfiguration von Software
- Absicherung der Zugänge und Zugriffe
- **Unterbinden des Zugriffs ins Internet**
- Deaktivierung nicht benötigter Schnittstellen
- Firewalling- und Netzwerksegmentierung

- **Benutzerverwaltungs- und Berechtigungsmanagement**
- **Patch- und Changemanagement**
- Assetmanagement
- Incidentmanagement
- Klare Verantwortlichkeiten

IT Sicherheit bei EnBW

Informationssicherheit
Roadmap der Erneuerbaren

Prävention → **Detektion & Reaktion**

Technisch
- Netzsegmentierung
- Sichere Anbindung
- EPIT Domäne
- Policies
- Firewalling
- Virenscanner
- Remotewartung
- Site-2-Site
- Konzernservices

Organisatorisch
- ISMS (inkl. Zertifizierung)

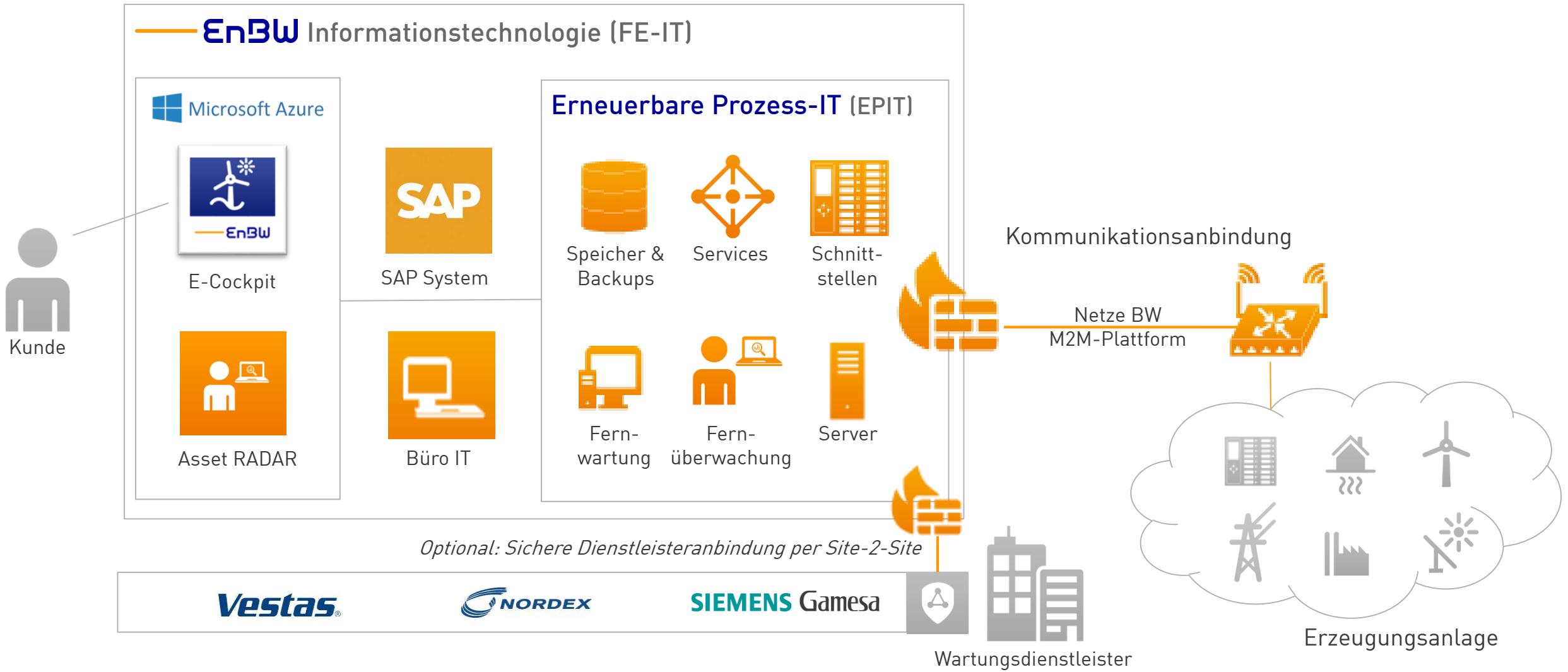
  - Risikomanagement
  - Prozesse
  - Verantwortlichkeiten
  - (Nachweis-) dokumentation
- „Ausprägung eines Sicherheitsbewusstseins“

Operativ
- EnBW Cyber Defence Model
- Betrieb intelligenter IT-Security Systeme
  - Cyber Detection
  - Cyber Abwehr
- Kennzahlen & Reporting

Stand der Technik | In Umsetzung | In Planung

IT Infrastruktur zur Betriebsführung

Überblick



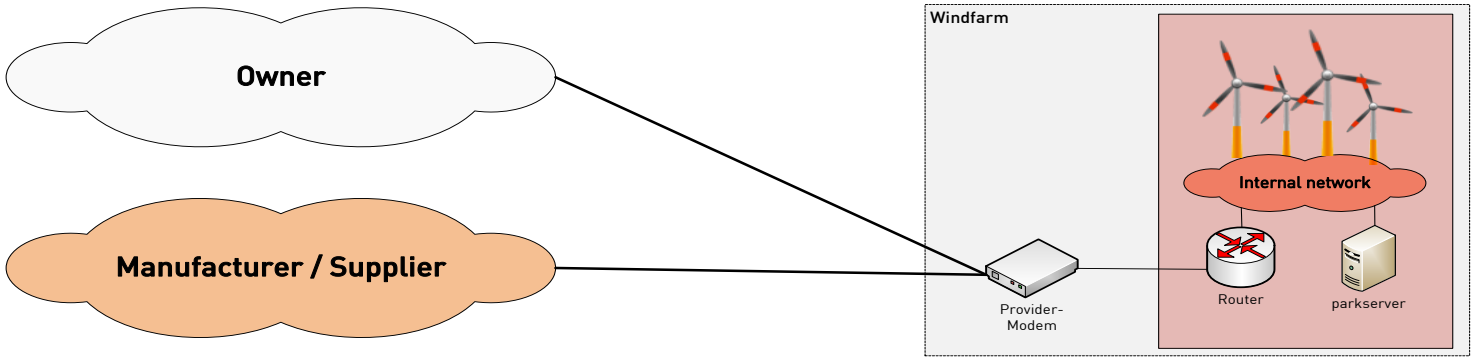
Raus aus dem Internet
Datenfluss kontrollieren

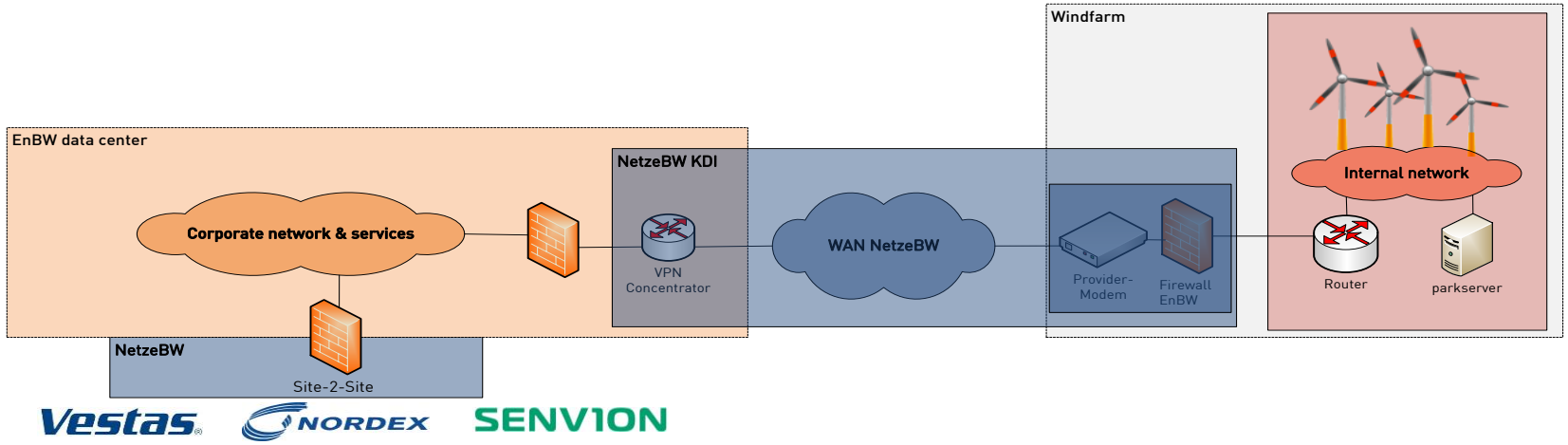
Branchenstandard

- Parallele VPN-Verbindungen für den Betreiber und Servicedienstleister
- Der Windpark ist über das Internet grundsätzlich erreichbar
- Datenfluss und Verbindungen können nicht kontrolliert werden.

EnBW Lösung

- Der Dienstleister wird an das EnBW-Netzwerk angeschlossen und nutzt die EnBW-Infrastruktur, um Zugang zum Windpark zu erhalten.
- Der Windpark ist nicht über das Internet erreichbar.
- Datenfluss und Verbindungen können gesteuert werden





Zugriffsmöglichkeiten einschränken

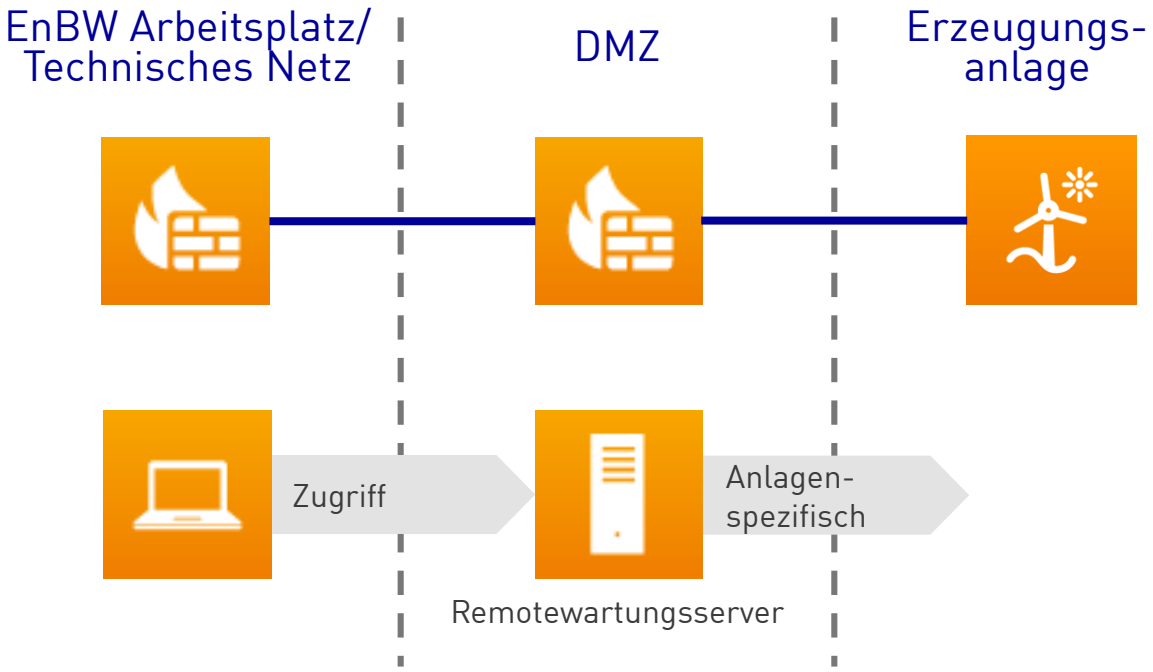
Fernzugriffe kanalisieren

Grundlagen

- Ein direkter Zugriff von Rechnern im Netzwerk auf ein System oder eine Anlage ist nicht möglich.
- Der Zugriff auf die Anlage erfolgt über zentrale Terminalserver.
- Jeder Terminalserver kann nur auf explizit freigegebene Anlagen oder Systeme zugreifen.

Zugriff

- Die Einwahl erfolgt im ersten Schritt auf einen dedizierten Terminalserver.
- Im zweiten Schritt kann vom Terminalserver eine Verbindung zur Anlage mit definierten Diensten und auf den Servern installierten Programmen aufgebaut werden.

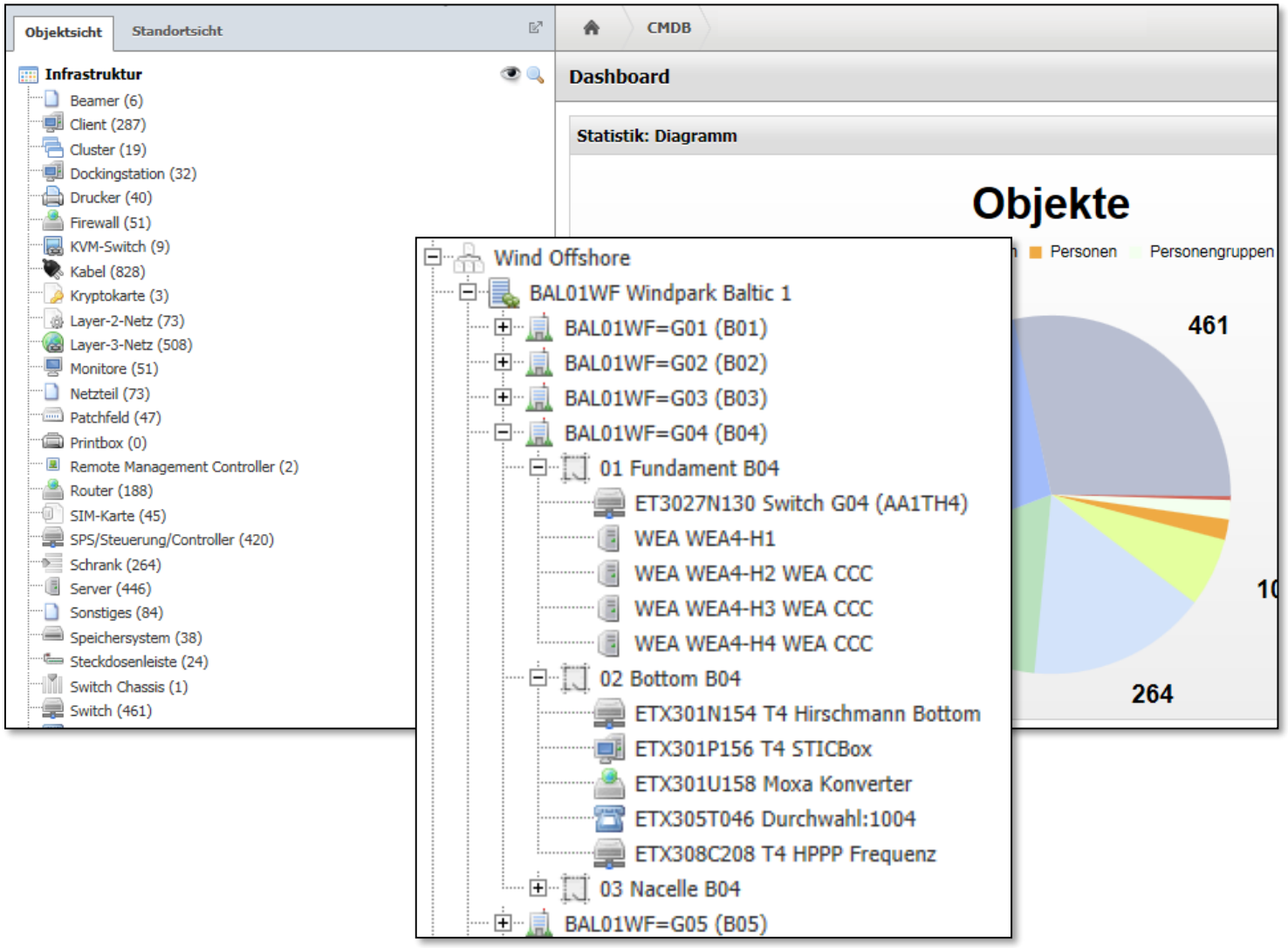


- Integration in AD und Policies
- Überwachung des Datentransfer
- Log der Zugriffe

Kenne deine Anlagen

Configuration Management Database

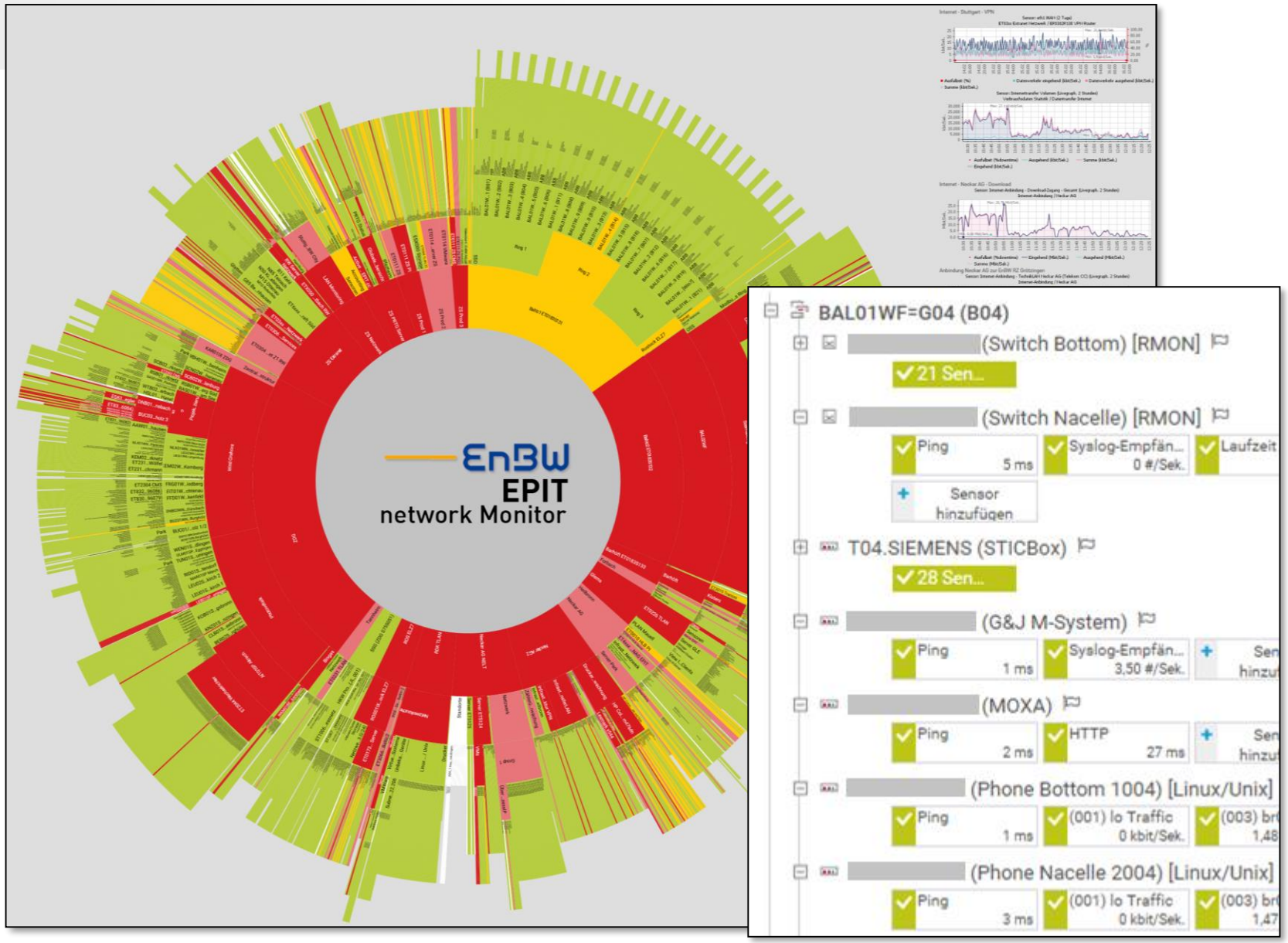
- Die Configuration Management Database (CMDB) ist das zentrale System zur Verwaltung der gesamten EPIT-Infrastruktur
  - Dokumentation
  - Planung / Change Management
  - ISMS und IT-Sicherheit
  - Operative Prozesse
- Zentrale Datenbank für vernetzte Systeme und Dienste
- ISMS: Die CMDB ermöglicht es, die Umsetzung der Maßnahmen und Prozesse (Kontrollen) eines Informationssicherheitsmanagementsystems einfach zu dokumentieren und nachzuweisen.



Überwache deine Anlagen

Netzwerk- und Systemüberwachung

- Alle IP-fähigen Endgeräte und Systeme in den Erzeugungsanlagen und im technischen Netz werden überwacht (Verfügbarkeitsüberwachung)
- Je nach vorhandenen Systemfunktionalitäten werden zusätzliche Systemzustände erfasst (z. Bsp. Festplattenkapazität, Prozessorloast, Netzwerkverkehr)
- Zum Überwachen können unterschiedliche Berichte und Übersichten individuell zusammengestellt werden
- Der Zugriff wird über ein gruppen- und rollenbasiertes Berechtigungs- konzept per AD-Integration geregelt



Betrieb sicher machen

Zertifizierungen im Bereich IT & Informationssicherheit

Teilbereich	Betrieb durch	Leistungsbeschreibung	Zertifizierungen
1 Anlagenanbindung 	Netze BW Ein Unternehmen der EnBW	› Interner TK / IP-Netz Dienstleister › Planung und Betrieb der Kommunikationsanbindungen	› ISO 27001 › ISO/IEC 20000
2 Konzern-IT Infrastruktur (CIT) 	EnBW Informationstechnologie	› Interner IT Dienstleister › Betrieb der Konzern IT-Services inklusive des Core-Netzwerks und der Rechenzentren	› ISO/IEC 27001 › ISO 27001 IT-Grundschutz › ISO/IEC 20000 › DIN EN ISO 9001 › TÜV TSI Level 4
3 Prozess-IT Infrastruktur (PIT) 	EnBW Produktionsservice Erneuerbare EPIT	› Betrieb der Prozess-IT-Infrastruktur zur Fernüberwachung und Betriebsführung	› Zertifizierung ISO 27001 in Q1 2020

Vielen Dank für Ihre Aufmerksamkeit!

Dipl.-Ing. Florian Lütticken

Teamleiter Prozess- & Informationstechnologie
Betrieb Erneuerbare Energien

EnBW AG
Schelmenwasenstraße 15
70567 Stuttgart

f.luetticken@enbw.com