Cyber Security in der Energiewirtschaft

14.05.2025; Berlin

TÜVRheinland®
Precisely Right.

Digitale Innovationen im Energiesystem - Betrieb & Netz

Digitaler Zwilling (Windkraft, Wasserkraft)

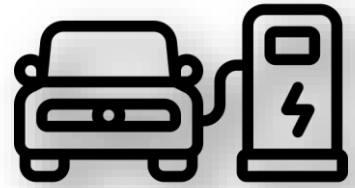
- Digitale Echtzeitmodelle von Energieanlagen bilden Betriebs- undZustandsdaten kontinuierlich ab
- Simulationen unterstützen die Planung, Wartung und Optimierung der Anlagenleistung
- Führt zu weniger Ausfällen, geringeren Wartungskosten und höherer Effizienz im Betrieb

KI-Drohnen für Anlageninspektion

- Autonome Drohnen erfassen per Kamera den Zustand von Rotorblättern, Masten und Infrastruktur
- Eine KI analysiert die Bilddaten automatisch und erkennt Schäden oder Verschleiß frühzeitig
- Spart Zeit, reduziert Risiken für Personal und senkt langfristig die Inspektionskosten

Smart Charging (z. B. Intelligent Octopus Go)

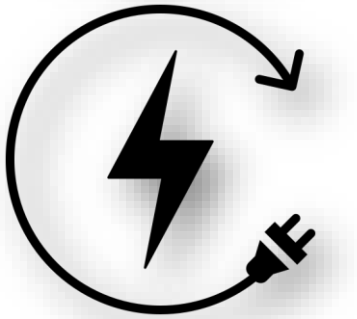
- Intelligente Ladesysteme steuern das Laden von E-Autos nach Strompreis und Netzbelastung
- Die Verbindung zu Strombörsen und dynamischen Tarifen ermöglicht kosteneffizientes Laden
- Senkt Energiekosten für Nutzer und entlastet gleichzeitig das Stromnetz bei Lastspitzen



Digitale Innovationen im Energiesystem - Verbraucher & neue Geschäftsmodelle

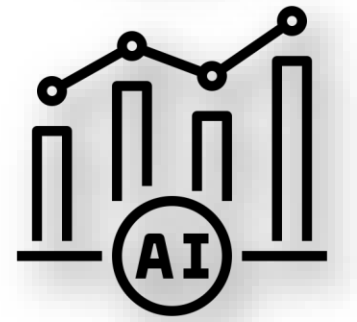
Zero-Bills-Häuser (energieautark & digital gesteuert)

- Gebäude mit PV, Batterie und Wärmepumpe erzeugen und verwalten ihren Strom vollständig selbst
- Eine digitale Plattform steuert Verbrauch und Einspeisung automatisch nach Bedarf und Wetter
- Bewohner zahlen dauerhaft keine Stromkosten und leben komplett energieautark



Bidirektionales Laden (Vehicle-to-Grid)

- Elektroautos dienen als Stromspeicher und geben Energie bei Netzbedarf wieder ab
- Die Steuerung erfolgt automatisiert über bidirektionale Wallboxen und intelligente Plattformen
- Unterstützt die Netzstabilität und ermöglicht zusätzliche Einnahmen für Fahrzeughalter



KI-Energieberatung & dynamische Tarife

- Künstliche Intelligenz analysiert Verbrauchsdaten und schlägt automatisch Optimierungen vor
- Strompreise und Gerätesteuerung werden in Echtzeit angepasst, je nach Bedarf und Markt
- Spart Energie, senkt Kosten und fördert ein bewussteres Verbrauchsverhalten im Alltag

Warum Cyber Security?

Cyberkriminalität

Wie sicher sind erneuerbare Energien vor Hackern?

[Cyberangriffe auf den Energie- und Versorgungssektor haben sich innerhalb von zwei Jahren mehr als verdoppelt]

Zusätzlich zur Verlagerung hin zu erneuerbaren Energien durchläuft die Branche auch eine digitale Transformation. Hinzu treten Bedrohungen durch...

Cyberattacke auf Stadtwerke Schwerte

Die Stadtwerke Schwerte wurden Ziel eines Cyberangriffs. Das Versorgungsnetz ist jedoch nicht betroffen.

Sie laufen noch auf Windows XP

Hacker haben bei Windparks leichtes Spiel

PSI Software

Hacker legen wichtigen Dienstleister für Energieunternehmen lahm

Cyberangriffe bedrohen die Zukunft der Solarenergie

IT-Sicherheit als Schlüssel zur Energiesicherheit

TÜVRheinland®
Precisely Right.

Auswirkungen der Cybersicherheit auf die Energieinfrastruktur

- Energie- und Versorgungsnetze sind das Rückgrat der modernen Gesellschaft, da sie wichtige Dienstleistungen wie Strom, Wasser und Gas bereitstellen.
- Eine Unterbrechung dieser Dienste kann zu erheblichen wirtschaftlichen und sozialen Auswirkungen führen: Beispiel Spanien/Portugal
- Cyberangriffe können auf diese Systeme abzielen und Stromausfälle, Probleme bei der Wasserversorgung und Gasmangel verursachen, die ganze Regionen lahmlegen können.
- Die Gewährleistung einer robusten Cybersicherheit ist für die Aufrechterhaltung der Stabilität und Zuverlässigkeit dieser kritischen Dienste unerlässlich.

Durch die Kontrolle der Stromeinspeisung in das Netz könnte ein Angreifer diese Kaskadeneffekte ausnutzen, um einen systemweiten Stromausfall mit Auswirkungen auf die Verteilung und Übertragung zu verursachen.

TÜVRheinland®
Precisely Right.

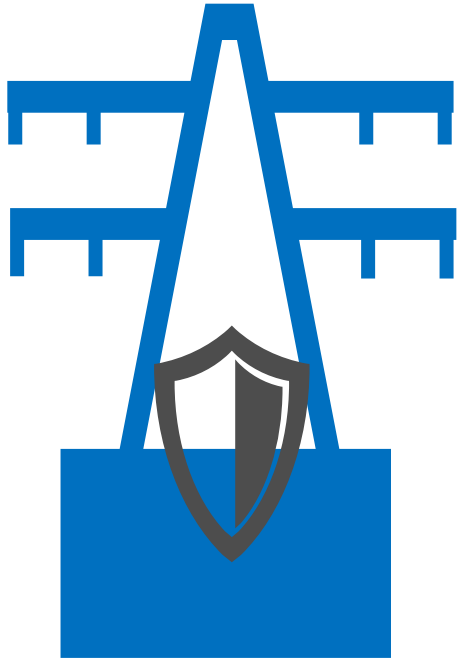
Ein paar Statistiken …

Cybersicherheit – Allgemeine Trends

- Im Jahr 2024 verursachten Cyberangriffe weltweit Schäden in Höhe von **9,5 Billionen US-Dollar**
- Die Zahl der gemeldeten Sicherheitslücken (CVEs) stieg bis Mitte 2024 um **30 % im Vergleich** zu 2023

Unternehmensreaktionen

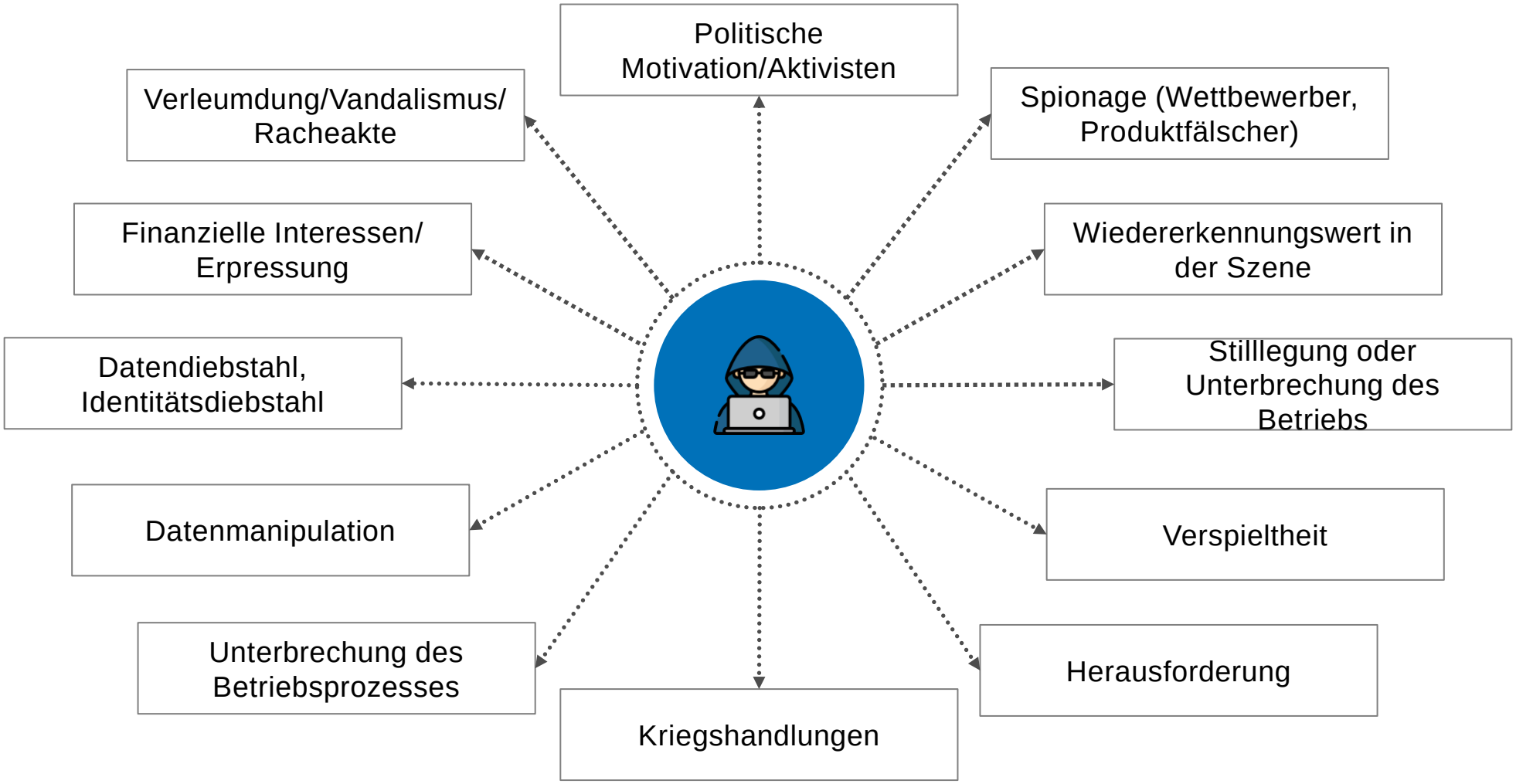
- 65 % der Energieexperten betrachten Cybersicherheit als das **größte aktuelle Risiko** für ihr Unternehmen
- 71 % erwarten 2025 erhöhte Investitionen in Cybersicherheit, insbesondere in **Betriebstechnologie (OT)**
- 84 % der Mitarbeiter wissen, wie sie auf potenzielle Cyberbedrohungen reagieren sollen



Cybersicherheit in der Energiewirtschaft

- Im Jahr 2023 erlitten **90 %** der weltweit größten Energieunternehmen Sicherheitsverletzungen
- Im Jahr 2024 berichteten 67 % der befragten Energieunternehmen von Ransomware-Angriffen
- Ransomware-Angriffe auf Energie- und Versorgungsunternehmen stiegen 2024 im Vergleich **zum Vorjahr um 80 %**
- Cyberangriffe auf US-Versorgungsunternehmen nahmen 2024 um 70 % gegenüber 2023 zu
- Der Markt für Cybersicherheit in der Energiebranche wurde 2023 auf etwa 9,5 Milliarden US-Dollar geschätzt und soll bis 2032 jährlich um etwa 10,5 % wachsen

Motivation der Angreifer



TÜVRheinland®
Precisely Right.

Arten von Cyber-Bedrohungen, die auf den Energiesektor abzielen

Ransomware:
Verschlüsselung kritischer Systeme oder Daten, unterbrechen den Betrieb und Erpressung von Zahlungen, um den Zugang wiederherzustellen

Phishing:
Täuschungstechniken, um sensible Informationen wie Passwörter und andere Kronjuwelen zu stehlen

DoS/DDoS-Attacken:
Überlastung von Systemen oder Netzen des Energiesektors, was zu Betriebsausfällen oder Störungen führt

Angriffe auf die Lieferkette:
Ausnutzung von Schwachstellen von Software von Drittanbietern oder eigener Software, um in Energienetze einzudringen

Datenschutzverletzungen:
Unbefugter Zugriff, der die Vertraulichkeit von Daten gefährdet

Unterbrechung der intelligenten Netze:
Ausnutzung von IoT- und Smart-Grid-Schwachstellen, um den Energiefluss zu manipulieren oder Stromausfälle zu verursachen

TÜVRheinland®
Precisely Right.

Herausforderungen für die Cybersicherheit bei zunehmender Digitalisierung der Energienetze

Erweiterte Angriffsfläche

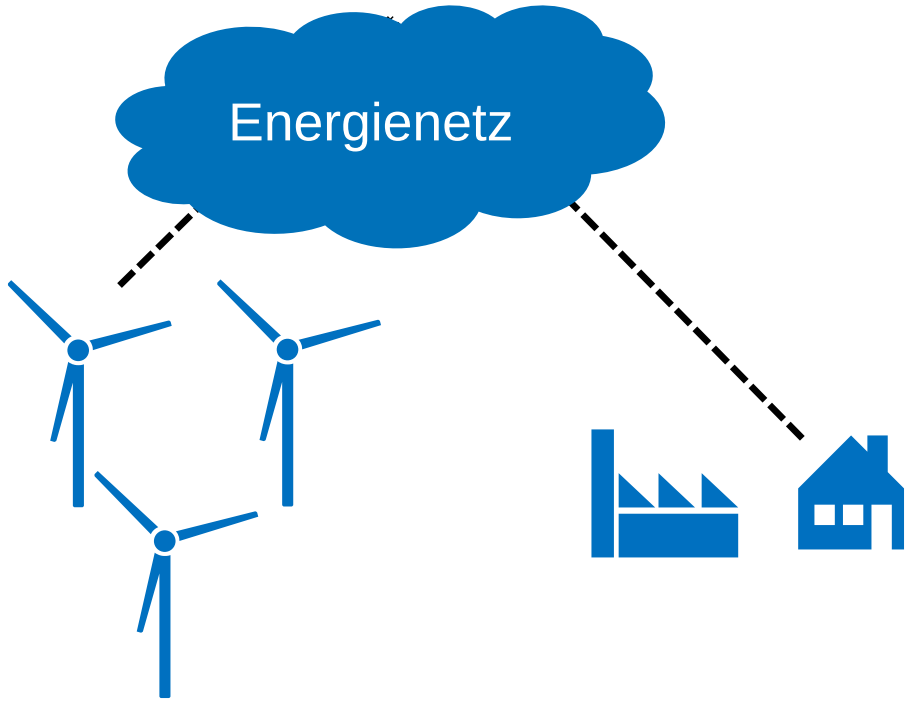
- Mit der zunehmenden Vernetzung des Energienetzes und der Kontrollsysteme steigt die Zahl der potenziellen Angriffspunkte für Cyber-Angreifer.
- Dazu gehören auch Drittanbieter und IoT-Geräte, was die Netzwerksicherheit erschwert.

Grenzüberschreitende Komplexität

- Energienetze erstrecken sich oft über mehrere Gerichtsbarkeiten, die jeweils eigene Cybersicherheitsvorschriften haben. Diese Vielfalt an Vorschriften erschwert die Einhaltung und Koordinierung der Cybersicherheit.
- Cyber-Bedrohungen kennen keine Grenzen, und ein Angriff in einer Region kann sich weltweit ausbreiten.

Betriebliche Unterbrechungen

- Cyber-Vorfälle können erhebliche Geschäftsunterbrechungen verursachen, die zu Umsatzeinbußen, Sanktionen und Rufschädigung führen.
- Kritische Infrastrukturen und die öffentliche Sicherheit sind durch diese Unterbrechungen gefährdet



TÜVRheinland®
Precisely Right.

Herausforderungen und Entwicklungen

Handlungsbedarf wird aufgrund zahlreicher Faktoren hervorgerufen. Mangel an Fachkräften, unausgereifte Technik, fortschrittliche Sicherheitsanalysen und neue/wachsende Regulierung sind Herausforderungen

DIGITALISIERUNG DER INDUSTRIE

	**Vernetzung**	Vernetzte Systeme steigern die Effizienz, die Daten-einsicht und das Kundenerlebnis. Die Unternehmen bauen ihre Vernetzung weiter aus (z.B. Remote-Zugänge, Notfallschalter, Big Data, Analytics)		**Safety & Reliability Risiken**	Systemausfälle, Fehlkonfigurationen und Cyberbedrohungen können sich auf die Sicherheit der Mitarbeiter und die Prozessstabilität auswirken und zu Geldstrafen und Reputationsschäden führen
	**Zunehmende anspruchsvollere Cyber-Angriffe**	Anzahl der Cybersicherheitsangriffe wird weiter zunehmen, ausgereifter sein und auf größere Auswirkungen ausgerichtet sein. Mit Bedrohungen und Angriffen Schritt zu halten, wird ohne professionelle Hilfe unmöglich sein.		**Kritische und industrielle Infrastrukturen sind gefährdete Ziele**	Die Bedrohungen zielen auf Schäden an kritischen Infrastrukturen und die Exfiltration sensibler Daten ab. Besonders kritisch sind hierbei Safety-Aspekte, die Schäden an der Umwelt und dem Leib und Leben von Menschen verursachen können.
	**Weltweiter Mangel an (industriellen-) Cybersicherheits-fachkräften**	Die Nachfrage nach Cybersicherheit insbesondere Industrial Security wird weiter ansteigen. Die Suche nach qualifizierten Ressourcen für die Bewältigung von Cyber-Angriffen wird ohne die Hilfe von außen unmöglich sein.		**Regulatorik und Gesetzgebung als Treiber**	Die Einhaltung von NIS2, CRA und IEC 62443 oder ISO 27001 ist heute für viele Branchen obligatorisch und erfordert bessere Sicherheitskontrollen und ein besseres Risikomanagement.

Cyber Security wird getrieben von vielfältigen Innovationen gehemmt durch die wachsenden Bedrohungen durch Cyberkriminalität.

TÜVRheinland®
Precisely Right.

Überblick regulatorischer Rahmen für Cybersicherheit im Energiebereich (1/2)

European Commission

Bundesamt für Sicherheit in der Informationstechnik

Gesetz über die Widerstands-fähigkeit im Internet (CRA)	NIS-2-Richtlinie	KRITIS
Ziel ist es, die Cybersicherheit von Produkten zu verbessern und ihre Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen	Ziel ist es, die Widerstandsfähigkeit der Betreiber kritischer Infrastrukturen zu verbessern	Konzentriert sich auf wesentliche Dienstleistungen wie Energie

TRBS	KAS-51	Energiewirtschaftsgesetz (EnWG)
Enthält Leitlinien, die sowohl physische als auch Cyber-Risiken für wesentliche Infrastrukturen abdecken	Bietet Leitlinien für Cybersicherheit und Widerstandsfähigkeit speziell für kritische Infrastrukturen	Sie gewährleistet zuverlässige, sichere und nachhaltige Energieversorgungsnetze.

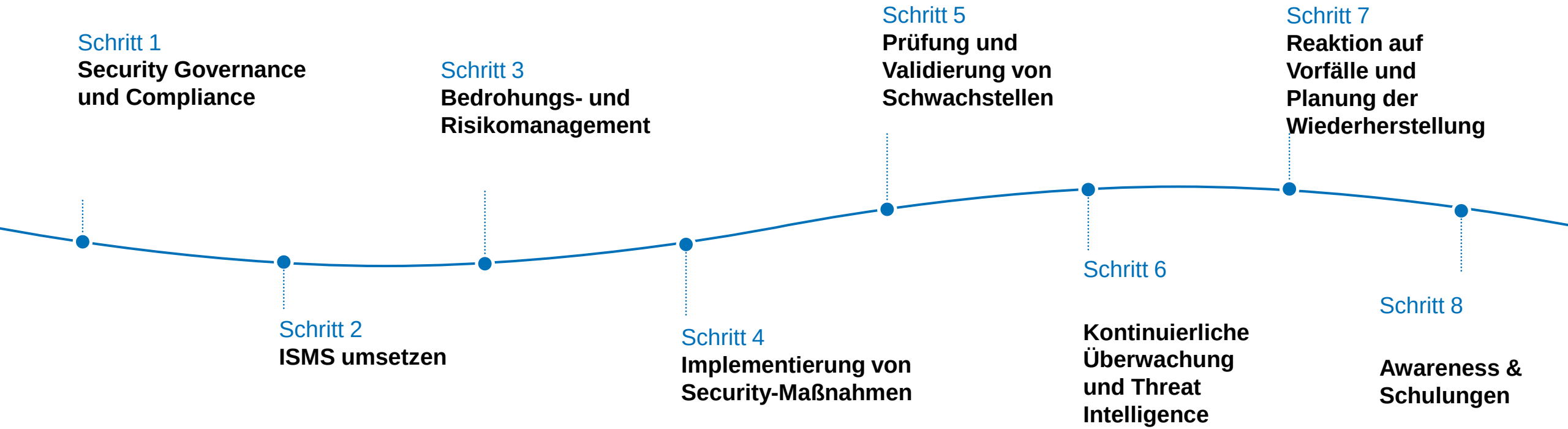
TÜVRheinland®
Precisely Right.

Überblick regulatorischer Rahmen für Cybersicherheit im Energiebereich (2/2)

TÜVRheinland®
Precisely Right.

Cybersicherheit für Energie

Schritte zu einer verbesserten Sicherheit im Energiesektor



TÜVRheinland®
Precisely Right.

Fragen und Antworten.

Vielen Dank für Ihre Aufmerksamkeit!

Andrzej Wozniczka
Head of OT Cyber Security Consulting
Andrzej.Wozniczka@i-sec.tuv.com
T +49 221 56783 295
M +491607840142

TÜVRheinland®
Genau. Richtig.