efzn

Energie-Forschungszentrum
Niedersachsen

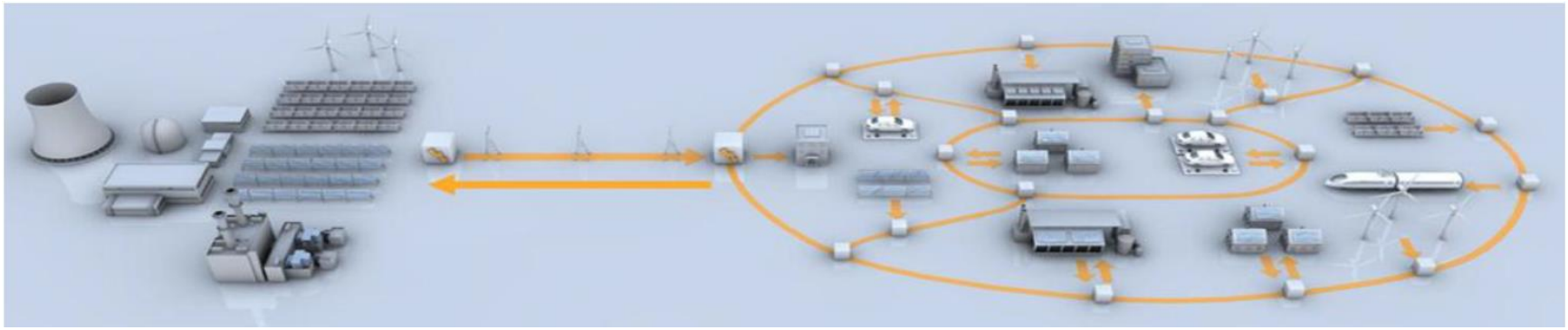
9. Göttinger Tagung

Digitalisierung der Energiewirtschaft-
Welche Substanz hat eine Wolke?

Prof. Dr.-Ing. Hans-Peter Beck
Vorstandssprecher EFZN

Göttingen, 9. Mai 2017

IT-Sicherheitsstandards für Digitalisierung der Energiewende



- Der Erfolg der Energiewende steht in Abhängigkeit einer intelligenten Vernetzung von Systemen und Akteuren im Smart Grid der Zukunft
- Das Gesetz zur Digitalisierung der Energiewende (GDEW) regelt die technischen und rechtlichen Grundlagen für die Etablierung eines Smart Grids in Deutschland
- Festlegung von Standards des BSI zur technischen und organisatorischen Durchsetzung von Datenschutz, Datensicherheit und Interoperabilität

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Aktueller Zeitungsartikel zum Thema Cyberattacken

Der Feind in meinem Computer

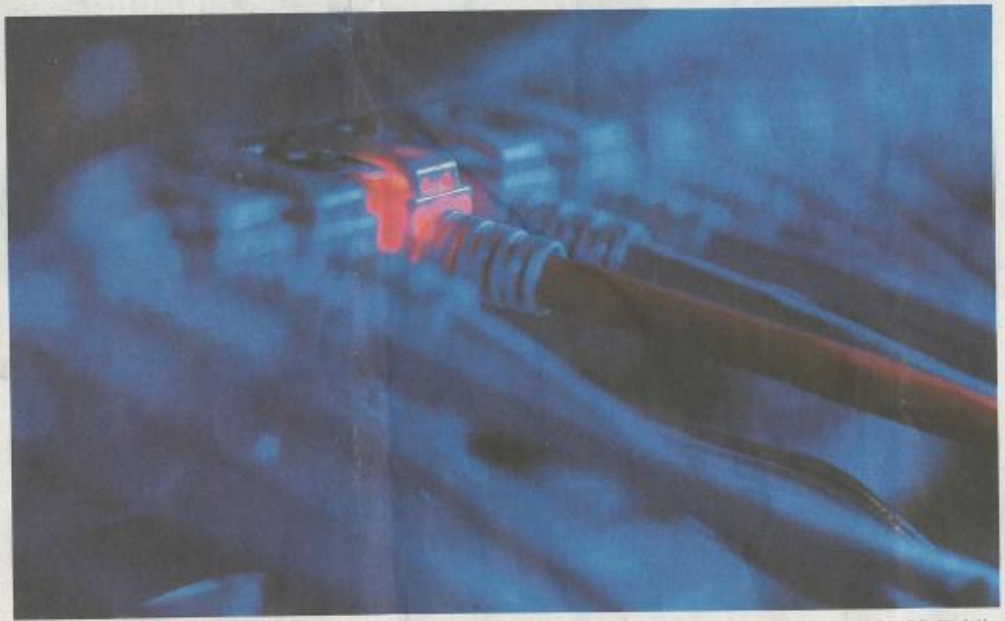
Cyberattacken kosten die deutsche Wirtschaft 50 Milliarden Euro im Jahr, schätzt der Verfassungsschutz. Anzeigen gibt es aber kaum

Von Frank Jansen und Heike Jahberg

Berlin - Die deutsche Wirtschaft wird offenbar massiv durch Cyberattacken und andere Formen von Spionage und Sabotage getroffen. Jährlich entstehe ein Schaden von schätzungsweise 50 Milliarden Euro, sagte der Präsident des Bundesamtes für Verfassungsschutz (BfV), Hans-Georg Maaßen, am Donnerstag in Berlin. Eine genaue Zahl lasse sich nicht nennen, da viele Angriffe erst spät entdeckt würden. Maaßen äußerte sich auf der Sicherheitstagung des BfV und des Bundesverbandes der „Allianz für Sicherheit in der Wirtschaft" (ASW).

Auch der Vorstandsvorsitzende des ASW-Bundesverbandes, Volker Wagner, sieht enorme Risiken. Die „Bedrohungslage" habe sich verschärft. Aus Wagners Sicht ist die deutsche Wirtschaft nicht hinreichend gegen die Attacken gewappnet. Die Gefahren für IT-System und -Prozesse seien zumindest in Teilen „ein Stück weit unterschätzt" worden, sagte der ASW-Chef. Maaßen ergänzte, viele Unternehmen sähen bei der Entwicklung neuer Produkte „Sicherheit als eine Bremse". Mitverantwortlich seien Kunden, „die lieber ein komfortables Produkt haben wollen als ein sicheres". Auch die Mentalität der Kunden müsse sich ändern, forderte der BfV-Präsident. „Nicht das günstigste Produkt, sondern Sicherheit muss ein Faktor sein."

Viele Unternehmen registrierten erst spät, dass sie angegriffen wurden, sagte Maaßen. Das dauere teilweise ein halbes oder dreiviertel Jahr. Oft bemerkten die Firmen sogar überhaupt nicht, dass eine Attacke stattfand, weil ein ausländischer Nachrichtendienst den von ihm gesteuerten Angriffstrojaner vernichte. Der Schaden für das Unternehmen sei erst sichtbar, wenn eine ausländische Firma „baugleiche Produkte auf den Markt bringt".



Attacke aus dem Netz: *Viele Angriffe bleiben unbemerkt.* Foto: Felix Kästle/dpa

Die umfassende Digitalisierung der Wirtschaft eröffne neue Chancen, rufe aber auch „bislang unbekannte oder unvorstellbare Risiken und Verwundbarkeiten hervor", warnte Maaßen. Deutschland als Hochtechnologie- und Wirtschaftsstandort gerate „immer stärker in den Fokus von Spionageaktivitäten staatlicher und nichtstaatlicher Akteure". Der BfV-Präsident nannte Cyber-Attacken aus Russland, China, Indien und Iran.

Ein Beispiel: Das Bundesamt für Verfassungsschutz hatte vor einem Jahr gewarnt, die mutmaßlich vom russischen Militärgeheimdienst GRU gesteuerte Hackergruppe „Sofacy" bereite Angriffe auf deutsche Unternehmen der Energiebranche vor. Wie der Tagesspiegel erfuhr, haben die Attacken auch tatsächlich stattgefunden. Die Namen betroffener Firmen nennt das BfV aber nicht. Eine Veröffentlichung könnte Kunden eines Unternehmens abschrecken und wäre geschäftsschädigend.

Die Behörde nennt die „Sofacy"-Aktivitäten „APT 28". Die Abkürzung steht für „Advanced Persistant Threat" (fortgeschrittene, andauernde Bedrohung). Mit der Zahl 28 wird die Hackerkampagne gelistet. Maaßen sagte, „APT 28" versuche flächendeckend, Server zu infizieren. Betroffen war auch der Bundestag, bei dem im Frühjahr 2015 insgesamt 14 Server attackiert und Daten im Volumen von 16 Gigabyte abgesaugt wurden.

Wagner appellierte an die Wirtschaft, „wir müssen uns darauf konzentrieren, Anomalien rechtzeitig zu entdecken". Nach dem Grundsatz „detect and response" müssten dann auch Maßnahmen ergriffen werden, den Schaden zu reduzieren. Wagner mahnte zudem, Unternehmen und Sicherheitsbehörden bräuchten „Wirtschaftsschutzbeauftragte". Maaßen ging noch einen Schritt weiter. Er hält es für nötig, dass ein Angreifer „gestohlene Daten verliert". Es müsse möglich sein, diese zu vernichten.

Nicht nur der Bundesverfassungsschutz, auch das Bundeskriminalamt warnt schon seit Langem vor Cyberangriffen. „Dieses Phänomen wird uns mit der fortschreitenden Technisierung und Digitalisierung unseres Alltags sicherlich noch stärker fordern", glaubt der Präsident des Bundeskriminalamts, Holger Münch. Nach einer Studie des Deutschen Instituts für Wirtschaftsforschung (DIW) aus dem Jahr 2015 gibt es pro Jahr rund 14.7 Millionen Fälle von Cyberkriminalität, das Bundeskriminalamt meldete 2015 aber nur 40 Millionen Euro an Schäden durch Cyberattacken. „Die Dunkelziffer ist hoch", räumt Münch ein. Wie Maaßen weist auch Münch darauf hin, dass viele Angriffe von den Firmen nicht bemerkt werden würden. Und selbst wenn die Unternehmen aufmerksam werden, sehen viele Firmenchefs von Anzeigen ab. Sie haben Angst vor dem Reputationsverlust, weiß der BKA-Präsident.

Gefährdet sind nicht nur die Großen, sondern zunehmend auch mittelständische Unternehmen. Nach einer repräsentativen Forsa-Erhebung im Auftrag des Versicherungsverbands GDV hat mehr als jeder vierte Mittelständler bereits finanzielle und materielle Schäden durch Attacken aus dem Netz erlitten. Die Versicherungsbranche sieht hier ein wachsendes Aufgaben- und Umsatzfeld. Sie hat daher Musterbedingungen für eine Cyberversicherung entwickelt, die sich speziell an Unternehmen mit einem Umsatz bis 50 Millionen Euro und einer Größe bis 250 Mitarbeiter richtet.

Quelle: Tagesspiegel 28.04.2017

Aktueller Zeitungsbericht zum Thema Digitalisierung der Energiewende (Ausschnitt)

Offene Scheunentore für Hacker

Die Stadtwerke in Ettlingen ließen ihre Verwundbarkeit für Cyberangriffe testen – und staunten. Binnen kurzer Zeit könnten die Bürger ohne Wasser und Strom sein.

Von Rüdiger Soldt

ETTLINGEN, 20. April

Eberhard Oehler hat die Kamera seines Smartphones mit schwarzer Folie abgeklebt. Oehler, studierter Elektroingenieur, ist eigentlich ein technikaffiner Mensch. Doch seit der Geschäftsführer der Ettlinger Stadtwerke 2013 erfahren hat, wie stark das kleine Versorgungsunternehmen im Süden Karlsruhes Hackerangriffen ausgesetzt sein kann, ist er vorsichtig geworden mit Smartphones und Computern. Dave Eggers „The Circle" und das Buch „Blackout" von Marc Elsberg stehen bei ihm Seite für Seite durchgearbeitet im Regal. Eigentlich war es ein Zufall, dass er sich mit dem Thema Hackerangriffe auf Energieversorgungsunternehmen beschäftigt hat, der Fernsehsender Arte wollte vor vier Jahren für eine Dokumentation die Datensicherheit der deutschen Stromversorger testen. Bei den großen Konzernen kamen die Journalisten nur bis zum Pförtner. Einem derart heiklen Versuch wollte sich niemand aussetzen. Durch einen privaten Kontakt kam dann ein Gespräch mit Oehler zustande, die Ettlinger Stadtwerke waren einverstanden, stimmten dem fiktiven, von einer privaten Computerfirmen inszenierten „Penetrationstest" zu.

Das Ergebnis war aufschlussreich und besorgniserregend: Der mit dem Hackerangriff beauftragte Computerfachmann Felix Lindner habe nur wenige Minuten gebraucht, bis er das Passwort der Software entschlüsselt hatte, sagt Oehler. Es wäre ein Leichtes gewesen, 40 000 Stromkunden und einen Großteil der 200 000 Wasserkunden in Ettlingen und der Region von der Versorgung abzuschneiden. Der versierte Hacker hätte 18 Stunden gebraucht, dann wären die Bürger in Ettlingen ohne Strom und ein paar Tage später, wenn die Trinkwasserhochbehälter nicht mehr per Pumpen hätten befüllt werden können, auch ohne Wasser gewesen. Alle Organisationen und Unternehmen, die Wasser, Strom und Gas liefern oder für die Gesundheitsversorgung oder den Transport verantwortlich sind, haben in den Zeiten von Cyberkriminalität eine angreifbare, kritische Infrastruktur. Im Februar 2016 brach bei einem Cyberangriff auf das Lukaskrankenhaus in Neuss das zentrale Managementsystem zusammen.

Oehler hat seit dem fingierten Hackerangriff 50 Vorträge gehalten, in denen er vor den Gefahren der Cyberkriminalität warnt. Softwarefirmen beschreiben die Schutzschirme zur Abschirmung von IT-Netzen mit Metaphern aus der Süßwarenwerbung: „Außen knusprig, innen cremig." Mit der Realität hat das wenig zu tun. Denn um in ein IT-Netz einzudringen, muss der Hacker nur eine Schwachstelle finden. So gab es in Ettlingen in den Tagungsräumen der Stadtwerke gut zugängliche Netzwerksteckdosen. Der Zutritt zu solchen Räumen ist schwer zu kontrollieren, es hätte ausgereicht, wenn ein Krimineller im Auftrag eines Hackers ein W-Lan- oder 3-G-Funkmodul in einer dieser Netzwerkdosen installiert hätte. Mit einem solchen Modul hätte ein Hacker binnen kurzer Zeit einen perfekten Zugang in das Computernetz der Stadtwerke gehabt. Zur Not hätte der Angreifer einen Pizzaboten mit 3-G-Modulen im Tornister in den Schulungsraum geschickt. Gefährliche Schnittstellen sind Notstromaggregate oder Multifunktionsdrucker, die heute in der Regel zur Wartung über einen eigenen Internetanschluss verfügen. Die Zentrale der Ettlinger Stadtwerke ist zu Beginn der neunziger Jahre gebaut worden, damals war „Cyberkriminalität" kein Thema.

Die deutsche Energiewirtschaft war seit 2007 mindestens fünf größeren Attacken mit Schadsoftware ausgesetzt. „Bis wir den Test gemacht haben", erzählt Oehler, „konnte ich zum Beispiel von meinem Rechner aus in die Systeme unserer Leitstelle hineinschauen, das war gar nicht nötig, man hat das damals wohl aus Unachtsamkeit eingerichtet." Nach dem Test war

Gegenschläge im Netz werden geprüft

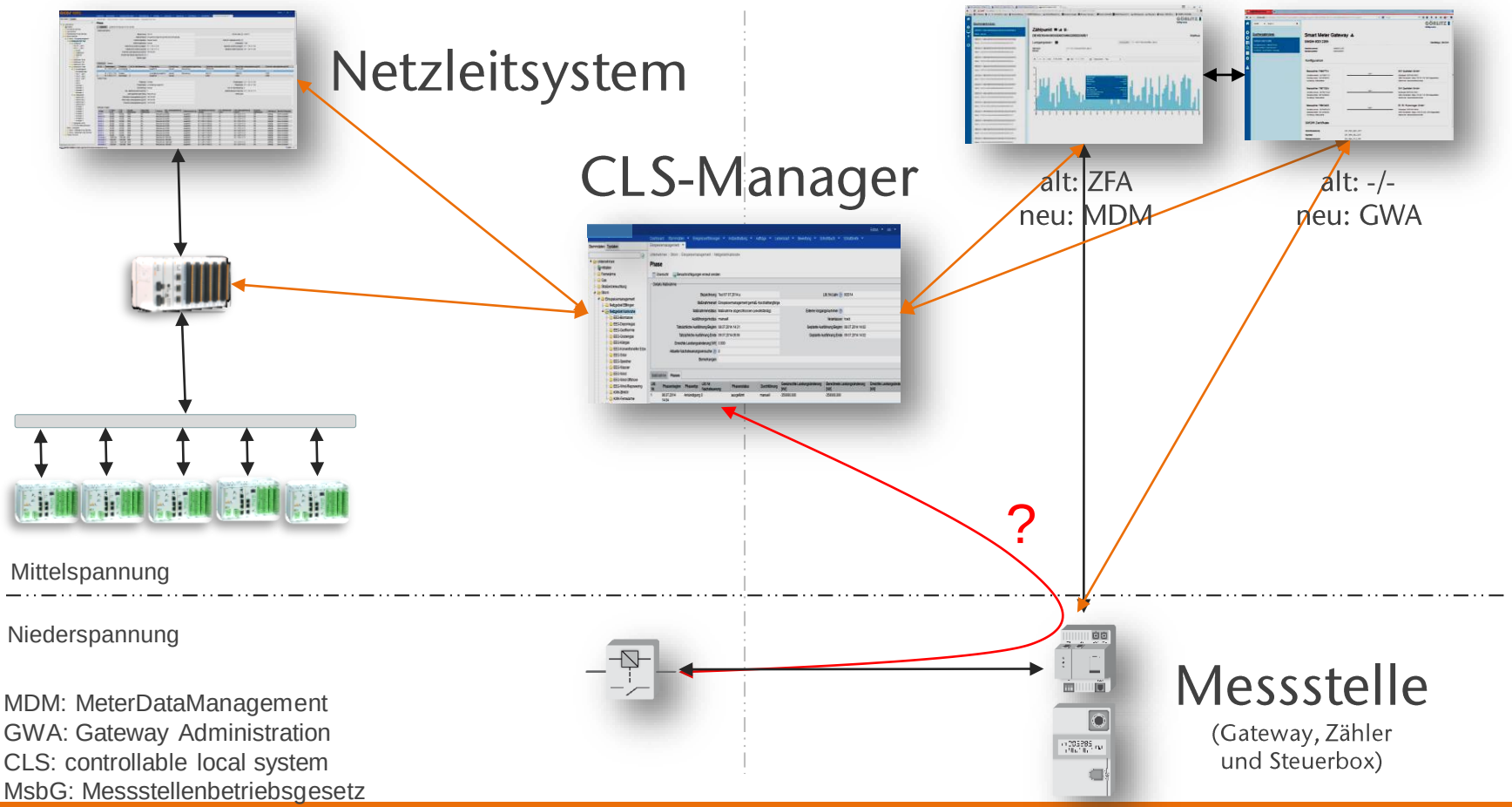
Die Bundesregierung will umfassend prüfen, welche rechtlichen und technischen Möglichkeiten noch zu schaffen sind, um Cyberangriffe, also Attacken auf deutsche Einrichtungen über das Internet, noch besser abwehren zu können und gegebenenfalls mit Gegenangriffen zu reagieren. Das Bundesinnenministerium teilte mit, dass man nationale und internationale Regeln brauche, „die neben Schutz und Abwehr die Rückverfolgung eines Angriffs aus dem Ausland und gegebenenfalls das Unschädlichmachen eines Servers im Ausland ermöglichen". In Sicherheitskreisen wird ein solcher Gegenangriff auf einen Server, von dem eine Attacke ausgeht, als „Hack Back" bezeichnet. Ein solcher ist allerdings nicht nur wegen der noch offenen rechtlichen und technischen Fragen schwer durchzuführen, sondern auch deswegen, weil bei vielen Angriffen kaum oder gar nicht zu klären ist, von welcher Quelle sie ausgingen. Das Innenministerium sagte, es sei wichtig, dass ein Staat sich „als wehrhafte Demokratie" vergewissere, dass Angriffe aus dem Ausland „gegebenenfalls auch mit Wirkung auf Server im Ausland" unterbleiben. Über Rechtsgrundlagen und technische Fähigkeiten seien zu Beginn der kommenden Legislaturperiode „wichtige Entscheidungen" zu treffen. Die „Süddeutsche Zeitung" hatte berichtet, dass der Bundessicherheitsrat beschlossen habe, bis zum Sommer eine Analyse zu dem Thema erstellen zu lassen. (elo.)

Usw.

Quelle: FAZ 21.04.2017

Folgen durch neue gesetzliche Vorgaben des MsbG

- Netzbetrieb
- Messstellenbetrieb



MDM: MeterDataManagement
GWA: Gateway Administration
CLS: controllable local system
MsbG: Messstellenbetriebsgesetz

Inventarisierung der Steuerungs- und Kommunikationstechnik

Erzeugungsanlagen	Übertragungswege	Akteure
Windenergie	Internet	Hersteller
Photovoltaik	Mobilfunk	Betreiber
	Langwellenfunk	Direktvermarkter
	Bluetooth, WLAN	Netzbetreiber*
	Verbindungskabel	
	Datenträger	

* Nicht Gegenstand der Studie

Weitere Wege?

Weitere Akteure?

Grafiken: elenia

Quelle: ECOFYS

Identifizierte Störszenarien

Ausfall öffentlicher Kommunikationsnetze (Internet, Mobilfunk, …)

Ausfall/Fehlfunktion Steuerungstechnik

Ausfall öffentlicher Versorgungsnetze (Black-Out)

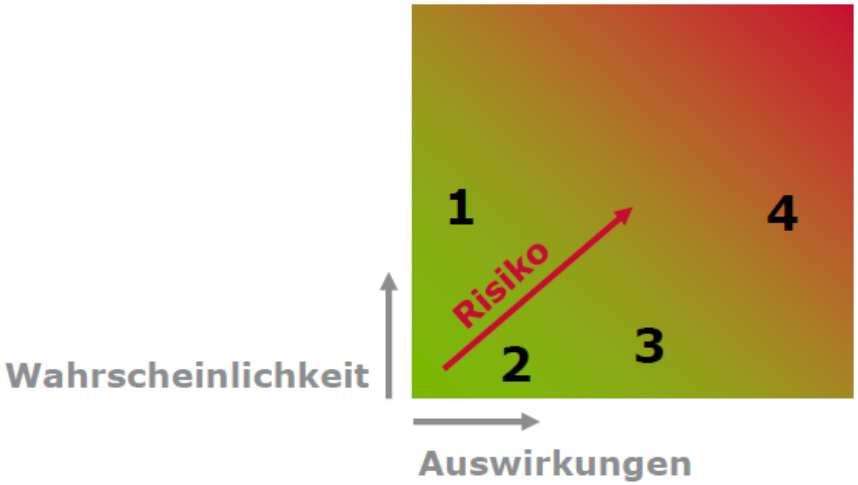
Fremdzugriff/ Cyberangriff

Weitere Szenarien?

Grafiken: elenia

Quelle: ECOFYS

Risikoeinschätzung



1. **Ausfall öffentlicher Kommunikationsnetze (Internet, Mobilfunk)**
   Wahrscheinlichkeit: *mittel* Auswirkungen: *gering*
2. **Ausfall öffentlicher Versorgungsnetze (Black-Out)**
   Wahrscheinlichkeit: *gering* Auswirkungen: *gering bis hoch*
3. **Ausfall/Fehlfunktion Steuerungstechnik**
   Wahrscheinlichkeit: *gering* Auswirkungen: *mittel*
4. **Fremdzugriff/Cyberangriff**
   Wahrscheinlichkeit: *mittel* Auswirkungen: *hoch*

Quelle: eigene Darstellung / ECOFYS

Priorisierung von Diensten und Datenklassen zur Simplifizierung der gefühlten Komplexität der „digitalisierten Energiewende“

Forschungsfrage: Wer hat Vorfahrt?

OT (Blackout relevant) ←

<u>autonom</u>

- Frequenzhaltung
- Spannungshaltung ****
- Blindleistungsbereitstellung
- Kurzschlussleistung
- Momentanreserve
- Schutzfunktion (Netz/Anlage) etc.

→ IT (Systemrelevant)

<u>proprietär</u>

- Firmware Updates *
- Erzeugerprognosen
- Diagnosen / Monitoring
- Smarthome-Anwendungen
- etc.

<u>prioritär</u>

- Powermanagement (Redispatch)
- Regelenergie / SDL
- Eingriffe Netzbetreiber ***
- etc.

<u>Smart-Meter-Gateway</u>

(Gesetz zur Digitalisierung der Energiewende)

- Messstellenbetrieb; Abrechnung
- Preissignale
- Energiehandel **
- etc.

OT: Operation Technology, realtime

*:Priorität?

IT: Information Technology

efzn

Energie-Forschungszentrum
Niedersachsen

Vielen Dank für Ihre Aufmerksamkeit!

Das EFZN ist ein gemeinsames wissenschaftliches Zentrum der Universitäten:

TU Clausthal

Technische Universität Braunschweig

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Leibniz Universität Hannover

CARL VON OSSIETZKY universität OLDENBURG