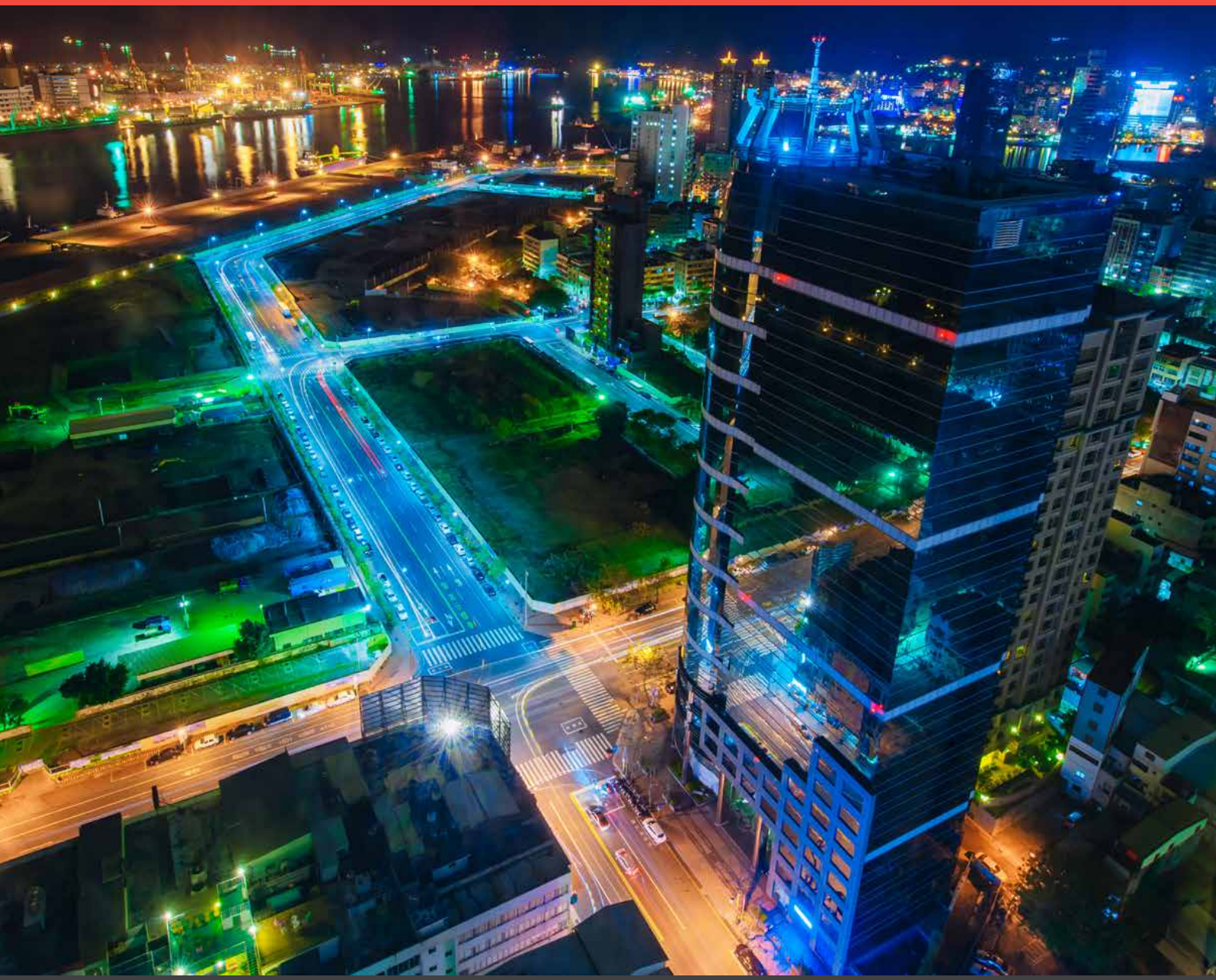
www.pwc.de/cybersecurity

Cybersicherheit: Eine neue Säule in der Energiewirtschaft.

7 Fragen, 7 Antworten zur Stärkung der Cyberresilienz.



pwc

Sieben Fragen an Moritz Anders und Dr. Oliver Hanka,

Experten für Cybersicherheit in der Energiebranche bei PwC Deutschland.

Moritz Anders ist Partner bei PwC Deutschland im Bereich Cyber Security & Privacy. Zu seinen Schwerpunkten zählen Identity & Access Management sowie die Implementierung von technischen Cybersecurity-Lösungen – insbesondere in der Energiewirtschaft.

Dr. Oliver Hanka ist Director bei PwC und verantwortlich für das Thema Industrial & IoT Security. Er hat über 14 Jahre Erfahrung im Bereich der Härtung von eingebetteten Systemen, IoT, OT (Operational Technology), Enterprise IT sowie Entwicklung von Safety-kritischen Systemen.

1. Welches sind aktuell die größten Herausforderungen für Energieversorger im Bereich Cybersicherheit?

„Smart Grid trifft auf veraltete OT-Infrastruktur. Das öffnet den Cyberkriminellen Tür und Tor.“

Oliver Hanka: Der Schwenk in Richtung Smart Grid beschäftigt derzeit alle in der Branche. Die besondere Herausforderung besteht darin, die alten Legacy-Systeme mit modernen Smart-Grid-Komponenten in Einklang zu bringen. Klassische Operational-Technology(OT)-Systeme, die bis jetzt als Insellösungen funktionierten, müssen nun mit den neuen Smart-Grid-Systemen zusammenspielen.

Moritz Anders: Auf der einen Seite steht also der hohe Drang zur Digitalisierung durch Smart Grid, also das digitale intelligente Stromnetz, und Smart-Meter-Gateways, die digitalen Stromzähler. Auf der anderen Seite sehen wir in der Branche eine sehr veraltete OT-Infrastruktur in Kraftwerken und Umspannwerken. Dort sind teilweise 30 oder 40 Jahre alte Softwaremodule im Einsatz, die eine unsichere Sicherheitslage darstellen.

Oliver Hanka: Dadurch öffnet man Cyberkriminellen Tür und Tor, die Systeme zu kompromittieren. Denn diese müssen jetzt nicht mehr physisch in das hoch gesicherte Kraftwerk einsteigen, um es zu stören. Sie haben jetzt viel mehr Möglichkeiten, über das intelligente Zusammenspiel der einzelnen Smart-Grid-Komponenten eine Netzüberlastung herzustellen, sodass das System aus Sicherheitsgründen runterfahren muss. Wenn Hacker:innen also wissen, an welche neuralgischen Punkte sie müssen, können sie das ganze Netz damit lahmlegen.

Smart Grid

Als „Smart Grid“ werden intelligente Stromnetze bezeichnet, die Erzeugung, Speicherung und Verbrauch kombinieren. Die Netze werden zentral gesteuert und aufeinander abgestimmt, um Leistungsschwankungen, etwa durch erneuerbare Energien, auszugleichen. In einem Smart Grid werden nicht nur Energie, sondern auch Daten ausgetauscht. So haben Netzbetreiber jederzeit aktuelle Informationen zu Energieproduktion und -verbrauch – und wissen, wann und wo durch dezentrale Erzeugungsanlagen Strom ins Netz eingespeist wird. Durch die intelligente Vernetzung über Smart Grids können erneuerbare Energien integriert und effizient genutzt sowie die Netzauslastung optimiert werden. In puncto Sicherheit entstehen durch Smart Grids aber neue Angriffspunkte, die Unternehmen gezielt absichern müssen.

Quelle: www.umweltbundesamt.de

2. Wo sehen Sie aktuell die größten Risiken, auf die sich Unternehmen vorbereiten müssen?

„Die aktuelle Bedrohungslage: Ransomware- und Nation-State-Angriffe nehmen zu.“

Moritz Anders: Stark zugenommen haben in den vergangenen Jahren Ransomware-Attacken, also Angriffe mit dem Ziel der Erpressung. Die Angreifer verschlüsseln dabei wichtige Unternehmensdaten und geben diese erst wieder frei, wenn das Opfer Lösegeld bezahlt. Den Cyberkriminellen geht es also in erster Linie darum, Geld zu erpressen. Ein Ransomware-Angriff kann im Prinzip Unternehmen jeder Größe und Branche treffen.

Großer Reputationsschaden kann dabei durch Daten-Leaks entstehen, die häufig Teil des Ransomware-Angriffs sind. Im Zuge der Digitalisierung sammeln die Energieunternehmen immer mehr Informationen über ihre Kund:innen. Wenn diese Daten nach außen dringen oder von den Angreifer:innen im Zuge der Erpressung bewusst „geleakt“ werden, entsteht ein Vertrauensverlust, der nur schwer wiedergutzumachen ist.

Oliver Hanka: Neben den Ransomware-Angriffen beobachten wir einen zweiten Trend: Immer häufiger werden Nation-State-Angriffe bekannt, wo Staaten eine Art Cyber-Krieg führen. Hier besteht das Ziel darin, die kritische Infrastruktur eines Landes – etwa Krankenhäuser, Finanzsysteme oder eben die Stromversorgung – lahmzulegen oder komplett auszuschalten. Wenn der Cyber-Kriminelle einem Land massiv schaden möchte, ist die Energiebranche das perfekte Einfallstor.

3. Wie gut sind die Energieunternehmen gegen Cyberangriffe gewappnet?

„Die Schwachpunkte: die OT und die fehlende Automatisierung bei der Cyberabwehr“

Moritz Anders: Aus meiner Sicht verfügt die Branche über eine solide Cyberabwehr, denn jedes Energieunternehmen ist regulatorisch dazu verpflichtet, entsprechende Vorkehrungen zu treffen und tut das längst auch. Das schreibt das IT-Sicherheitsgesetz Netzbetreibern sowie Energieunternehmen bei Überschreitung der Schwellenwerte vor. Was den Unternehmen bei der Umsetzung der Sicherheitsmaßnahmen dennoch fehlt, ist die Automation. Gerade die großen Energieversorger haben Cybersicherheit mittlerweile weit oben aufgehängt. Was aber vielfach fehlt, ist eine automatische Erkennung von Angriffen – und zwar für alle Teile: von der Cloud bis zu den OT-Komponenten.

Oliver Hanka: Die OT ist sicher die Achillesferse. Hier setzte man in der Vergangenheit auf einen physikalischen Schutz, in Form von hohen Mauern oder Zäunen. Jetzt gehen diese Komponenten durch den Smart-Grid-Trend aber auch ans Netz und werden somit leichter angreifbar. Denn die Geräte sind wie gesagt oft alt und wurden nie mit dem Sicherheitsgedanken im Hinterkopf entwickelt. Vieles wird in der OT noch händisch gemacht und es gibt keine Automatismen, um Unwägbarkeiten oder Anomalien zu erkennen.

4. Was müssen Energieversorger jetzt tun, um sich hier besser aufzustellen?

„Expertise aufbauen – und auf Security by Design setzen“

Oliver Hanka: Wichtig ist es zum einen, personell aufzurüsten. Gerade kleinere, lokale Unternehmen wie Stadtwerkbetriebe haben jedoch Mühe, hoch qualifizierte Cyberexpert:innen zu rekrutieren. Selbst wenn sie Stellen für Cybersicherheit schaffen, bekommen sie diese nicht so einfach besetzt, weil momentan alle Firmen in Deutschland händeringend nach IT-Sicherheitsexpert:innen suchen.

Moritz Anders: Eine Alternative, um sich hoch spezialisierte Expertise einzukaufen, sind Managed Services. Aber auch da stellen sich viele Fragen: Wie steuere ich diese Dienste? Wie verlagere ich das Risiko? Inwiefern nimmt der Serviceprovider mir die Risiken ab und haftet? Hat der Anbieter seinen Sitz in Deutschland oder im Ausland? Umso wichtiger ist es deshalb, auf Security by Design zu setzen, Sicherheit also von Anfang an mitzudenken, wenn ein neues System eingeführt wird.

Security by Design

„Security by Design“ beschreibt den Ansatz, die Sicherheit beim Design einer neuen Lösung direkt mitzudenken. Während ein Unternehmen ein neues System plant, führt es also parallel dazu Risk-Analysen durch, um unter anderem folgende Fragen zu adressieren:

- Welche Assets gilt es in unserem Unternehmen zu schützen?
- Was sind die Auswirkungen, wenn bestimmte Elemente ausfallen?
- Wie ist der typische Angriffspfad?
- Wie schwer ist es für den Angreifer, dorthin zu gelangen?

Aus den Ergebnissen dieser Analyse lassen sich die Risiken ablesen und in eine Risikomatrix übertragen. Unternehmen können dann abwägen, welche Risiken ihnen zu hoch sind – und für diese gezielte Abwehrmaßnahmen aufbauen. Die Analyse muss sich regelmäßig wiederholen, weil permanent neue Angriffsmethoden oder -vektoren dazukommen.

5. Mit welchen Investitionen für Cybersicherheit müssen Unternehmen rechnen?

„Bei OT gilt: 10 bis 15 Prozent des Budgets für Security einplanen“

Oliver Hanka: Im OT-Bereich gilt: Wer ein neues System plant, sollte zwischen 10 und 15 Prozent des Budgets für Sicherheit einkalkulieren. Das ist natürlich eine ganze Menge und mehr als bei Digitalisierungsprojekten. Diese hohen Kosten machen dann schnell die Marge, die man sich erhofft hat, kaputt. Aber leider ist Cybersicherheit alternativlos.

Moritz Anders: Wir Berater:innen werden gern dafür kritisiert, schwarzzumalen und Untergangsszenarien aufzuzeigen. Aber viele Beispiele aus der jüngsten Vergangenheit geben uns leider recht: etwa der Cyberangriff auf Colonial Pipeline, einen der wichtigsten Betreiber von Öl-Pipelines in den USA. Der Angriff hatte verheerende Folgen für die Benzin- und Kerosinversorgung an der kompletten Ostküste der USA. Aber auch die Hackerangriffe auf deutsche Firmen, etwa den Lebensmitteleinzelhändler tegut oder die Funke-Mediengruppe, zeigen: Es kann jeden treffen – Konzerne ebenso wie deutschlandweit tätige Mittelständler. Und wenn es passiert, ist ein Unternehmen unter Umständen Monate lang damit beschäftigt, den Scherbenhaufen zu beseitigen. Das ist im Zweifelsfall teurer, als präventiv in Cybersicherheit zu investieren.

6. An welchen Elementen eines Cybersicherheitsansatzes kommen Energieunternehmen nicht vorbei?

„Am Anfang steht eine Bestandsaufnahme. Das langfristige Ziel sind automatische Kontrollen.“

Oliver Hanka: Der erste Schritt ist eine klassische Bestandsaufnahme, also ein Maturity-Assessment. So können sich Energieversorger einen Überblick verschaffen, wo sie in puncto Cybersecurity stehen. Solche Analysen, etwa in Form von Assessments, lassen sich relativ schnell umsetzen und liefern innerhalb von drei Monaten brauchbare Ergebnisse, die sich mittelfristig umsetzen lassen. Wenn die Schwachstellen dann bekannt sind, können Unternehmen zunächst die am höchsten priorisierten Risiken angehen.

Was wirklich Zeit braucht und sich deshalb nur mittelfristig umsetzen lässt, ist das Monitoring und die permanente Evaluation. Bis ein Unternehmen in diesem Bereich komplette Sichtbarkeit erreicht hat, braucht es Zeit. Das lässt sich nicht innerhalb weniger Monate realisieren.

Moritz Anders: Ich würde hier auch zwischen Pflicht und Kür unterscheiden. Jedes Energieunternehmen ist verpflichtet, ein Information Security Management System (ISMS) einzuführen. Zum Standard gehört auch ein vernünftiges Risikomanagement, um die Gefahren einschätzen zu können.

In Zeiten der Digitalisierung braucht es aber mehr – und zwar möglichst automatische Kontrollen: Aufgrund der ansteigenden Bedrohungslage und immer ausgefeilterer Techniken, gepaart mit Personalknappheit, müssen Energieunternehmen ihre Systeme so aufstellen, dass sie hochgradig automatisieren. Wenn ich alles mit der Hand am Arm mache, wie es mit einem ISMS theoretisch möglich ist, dann brauche ich viel Personal, aber das fehlt ja gerade.

7. Inwiefern trägt eine solide Cybersecurity-Strategie dazu bei, die Energieunternehmen zukunftsfähig zu machen und ihnen einen Wettbewerbsvorteil zu verschaffen?

„Deutschland darf den Smart-Grid-Zug nicht verpassen.“

Oliver Hanka: Die Energiebranche ist in Deutschland vergleichsweise gut aufgestellt. Das zeigt auch ein Vergleich mit den USA, wo die Kabel häufig über die Dächer laufen und es bei kräftigen Windstößen oder Schneestürmen zu Stromausfällen kommen kann. Deutschland gilt international als zuverlässiger Partner in der Branche und hat immer auch Strom ins Ausland exportiert.

Moritz Anders: Wenn wir jetzt aber wegen Sicherheitsbedenken den Zug bei Smart Grid verpassen und langsamer digitalisieren als die Nachbarländer, könnten wir diesen Vorteil verspielen und unseren Ruf als vertrauenswürdiger Partner aufs Spiel setzen. Smart Grid ist eine große Chance für die Branche. Um diese zu nutzen, müssen Unternehmen die damit verbundenen Risiken früh adressieren – und dazu gehört unbedingt das Thema Cyberabwehr.

Ihre Ansprechpartner

Moritz Anders
Partner, PwC Deutschland
Tel.: +49 151 5545-5621
moritz.anders@pwc.com

Oliver Hanka
Director, PwC Deutschland
Tel.: +49 160 510-5836
oliver.hanka@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 155 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Rund 12.000 engagierte Menschen an 21 Standorten. 2,3 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

www.pwc.de