Sustainable Cyber Resilience im Energiesektor:

Energieerzeuger, Übertragungs- und Verteilnetze

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Energieversorger zählen zu den kritischen Infrastrukturen und sind ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Energiesektor so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyber-Angriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetz (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist Energie mit den Sparten Elektrizität, Gas und Mineralöl. Angriffe auf den Energiesektor könnten besonders gravierende Folgen haben und ein ganzes Land destabilisieren. Denn fällt die Stromversorgung über längere Zeit aus, kommt es zu einem Kaskadeneffekt, der auch andere kritische Infrastrukturen mitreißt. Die Kühlkette in der Nahrungsmittelversorgung funktioniert dann nicht mehr, die Elektronik in Krankenhäusern fällt aus, die Telekommunikation ist gestört und die Wasserversorgung wird beeinträchtigt. So kommt nach und nach das gesamte gesellschaftliche Leben zum Erliegen. Der Autor Marc Elsberg hat ein solches Szenario in seinem Bestseller „Blackout" anschaulich geschildert.

Der Weltenergierat warnte in einer Studie bereits 2016 vor den zunehmenden Cyber-Attacken auf die Infrastruktur im Energiesektor. Er verzeichnete eine deutliche Zunahme von Angriffen auf Strom-, Öl, und Atomkonzerne. Die Attacken dienen häufig nicht nur dazu, Industriespionage zu betreiben oder sensible Daten abzugreifen, sondern sollen Sabotage betreiben. Unternehmen der Energiewirtschaft sind sich dieser Bedrohung bewusst. Laut einer Umfrage des Risikoberaters Marsh zu Cyber-Angriffen, gaben mehr als drei Viertel der befragten Manager an, dass sie sich am meisten vor Betriebsunterbrechungen fürchten. 26 Prozent bestätigten, dass ihr Unternehmen in den vergangenen zwölf Monaten Opfer einer erfolgreichen Cyber-Attacke war.

Beispiele für Cyber-Attacken auf Energie-Infrastrukturen

In den vergangenen Jahren gab es weltweit bereits zahlreiche Angriffe auf kritische Infrastrukturen im Energiesektor. Ein prominentes Beispiel ist der Blackout in der Ukraine im Dezember 2015. Hacker attackierten drei Stromversorger in der westukrainischen Region Ivano-Frankiwsk und infizierten deren Netzwerke mit der speziell dafür entwickelten Schadsoftware BlackEnergy. 225.000 Kunden waren für drei Stunden lang ohne Strom. 2016 wurde die Ukraine erneut Opfer eines ähnlichen Vorfalls, diesmal in der Hauptstadt Kiew, wo für rund eine Stunde die Lichter ausgingen. Auch hier kam eine ausgefeilte Malware zum Einsatz. In beiden Fällen stand die russische Regierung wegen des schwelenden politischen Konflikts mit der Ukraine im Verdacht, hinter den Hacker-Angriffen zu stehen. Bewiesen wurde dies jedoch nicht. Sicherheitsexperten vermuten, dass die Attacke von 2016 nur ein Testlauf war, um eine verbesserte, deutlich weiterentwickelte Malware auszuprobieren. Sie agiert vollautomatisiert und ist in der Lage, sehr schnell einen Blackout herbeizuführen.

Das Sicherheitsunternehmen Symantec berichtete im Oktober 2017 von einer neuen Welle von Cyber-Angriffen auf Energieversorger in Nordamerika und Europa. Betroffen waren unter anderem der irische Übertragungsnetzbetreiber EirGrid und das Kernkraftwerk Wolf Creek im US-Staat Kansas. In beiden Fällen wurde der Betrieb glücklicherweise nicht beeinträchtigt. Vermutlich dienten die Attacken dazu, Systeme auszuspionieren, um künftige Angriffe vorzubereiten. Die Handschrift der Angreifer lässt auf die Hackergruppe Dragonfly schließen, die bereits seit 2011 aktiv ist, so Symantec, und jetzt wohl versucht, Kontrolle über Energieversorgungssysteme zu erlangen.

Auch deutsche Energieversorger sind laut Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) Ziel einer großangelegten weltweiten

Cyber-Angriffskampagne geworden. Das BSI ermittelt 2018 in einer Vielzahl von Verdachtsfällen und analysiert diese gemeinsam mit den betroffenen Unternehmen. In mehreren Fällen konnten Spuren der Angreifer nachgewiesen werden, die auf Angriffsvorbereitungen zur späteren Ausnutzung hindeuten. Erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke gab es nach aktuellem Wissensstand jedoch nicht.

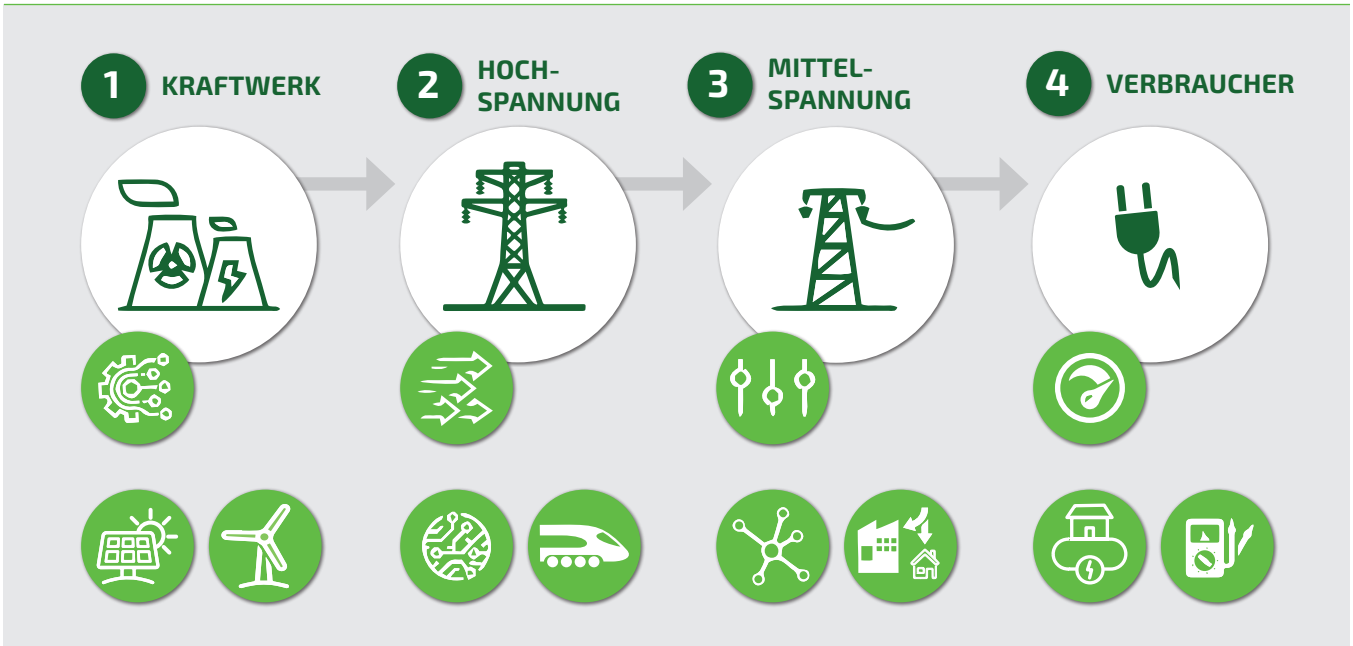
IT-Systeme und Prozesse im Energiesektor

Einige Beispiele für IT-gestützte Abläufe in der Energieversorgung sind in der Grafik unten abgebildet. Kraftwerke (1) nutzen digitale Mess- und Steuerungssysteme für das Management, zum Beispiel des Energiemixes (Wind, Solar, Brennstoff), den ein Erzeuger nutzen kann. Bei der Übergabe in die Hochspannungsnetze (2) kommt es auf die bedarfsgerechte, teils internationale Verteilung an, sowohl an Großverbraucher wie etwa den Schienenverkehr als auch an Mittelspannungsnetze (3). Diese übernehmen die weitere Verteilung, sind aber noch stärker der Varianz des eigentlichen Verbrauchs ausgesetzt – je nach Anteil von privaten Haushalten und Industrie. Beim Verbraucher (4), gerade in privaten Haushalten, sind SmartHome, SmartFactory und insbesondere Smartmeter ein Angriffspunkt. Hier spielen Attacken auf IoT-Devices auch für Energieversorger eine Rolle – wenn etwa 10.000 Elektroherde gleichzeitig auf volle Leistung gestellt werden.

IT bildet heute also die Grundlage für nahezu alle Geschäftsprozesse und alle Kundenprodukte der Energiewirtschaft. Um einen Zustand der Sustainable Cyber Resilience zu erreichen, müssen Energieversorger das gesamte Spektrum der vernetzten Systeme, Geräte und Applikationen berücksichtigen. Dazu zählt sowohl Unternehmens-IT als auch Operational Technology (OT). IT-Systeme zur Unternehmensadministration und zur Kundendatenverwaltung enthalten sensible Geschäftsgeheimnisse oder personenbezogene Daten, die unter die EU-Datenschutz-Grundverordnung (DSGVO) fallen. In Kraftwerken und bei der Verteilung kommen Systeme zur Steuerung und zum Monitoring zum Einsatz. Dazu gehören zum Beispiel zentrale Netzleit- und Netzführungssysteme, Kraftwerks-Leitsysteme, zentrale Systeme zur Überwachung und Steuerung von verteilten Erzeugern und Lasten, Systeme zur Störungsannahme und zur Einsatzplanung sowie zur Datenarchivierung.

Auch die Technologie auf Kundenseite muss berücksichtigt werden. Zunehmend kommen hier Smart Meters zum Einsatz, intelligente Stromzähler, die an das Internet angeschlossen sind. Sie senden Verbrauchsdaten digital an den Energieversorger und ermöglichen es dem Konsumenten, seinen Energieverbrauch jederzeit in einer App einzusehen. Dadurch soll es einfacher

Beispiele für IT-gestützte Abläufe in Stromnetzen



werden, Energie zu sparen. Gleichzeitig können die Smart Meter auch Daten zu den verfügbaren Energiekapazitäten empfangen. So wird es künftig zum Beispiel möglich, Engpässe zu vermeiden und elektrische Geräte nur dann zu betreiben, wenn der Strom gerade günstig ist. Smart Meter stehen jedoch auch in der Kritik, denn sie sind ein zusätzliches Einfallstor für Hacker.

Besondere Herausforderungen für Resilience im Energiesektor

Die Digitalisierung verändert die IT-Landschaft im Energiesektor erheblich. Mit der zunehmenden Verbreitung von dem Internet der Dinge (IoT) und Industrie 4.0 wächst der Anteil an Embedded-IT. Immer mehr Geräte verfügen über integrierte Betriebssysteme und die Möglichkeiten der Datenkommunikation. Mit jedem vernetzten Gerät vergrößert sich auch die Angriffsfläche. Zudem nutzen Mitarbeiter verstärkt mobile Endgeräte in ihrem Arbeitsalltag. Cloud Computing und Big-Data-Anwendungen setzen sich zunehmend durch. Das bedeutet für Unternehmen der Energiewirtschaft, dass sie ein komplexes, heterogenes Spektrum an Systemen, Geräten und Applikationen aus verschiedenen Generationen berücksichtigen müssen, um Resilience herzustellen. Die Kombination aus Legacy Systemen und brandneuen Geräten sorgt oft für Sicherheitslücken und Unzulänglichkeiten. Verbunden mit Governance- und Regulierungsrichtlinien, die zu widersprüchlichen Handlungen auffordern, entsteht ein wahres Chaos. Wenn die IT-Verantwortlichen diese Sachlage ignorieren, wird unweigerlich jede IT-Sicherheitsarchitektur ineffizient und angreifbar und damit zu einem Bremsfaktor für die gesamte Organisation. Gleichzeitig macht der zunehmende Grad an Automatisierung durch Smart Grids und Smart Meter mögliche Angriffe noch gefährlicher.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeiten eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffes zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

Greenbones Schwachstellenmanagement funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden. Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hackerangriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**