CONNECTCOM

Kritische Infrastrukturen in der Energieversorgung

Aktueller Stand und Anforderungen an die Cyber Security

Datum: 17. Oktober 2023

Inhaltsverzeichnis

1. Die Welt im Wandel

Kritische Infrastrukturen wie Stromnetze, Wasserversorgungssysteme, Verkehrsleitsysteme und industrielle Steuerungssysteme sind zunehmend mit dem Internet verbunden. Dadurch erhöht sich das Risiko von Cyberangriffen durch böswillige Akteure, einschliesslich staatlich unterstützter Gruppen, Hackerkollektiven oder Cyberkriminellen. Um diese Angriffe abzuwehren und Schäden zu minimieren, ist eine robuste Cyber Security unerlässlich.

1.1. Gesellschaft

Für das tägliche Funktionieren der Gesellschaft ist das tadellose Funktionieren der kritischen Infrastruktur von entscheidender Bedeutung. So besteht beispielsweise eine grosse Abhängigkeit von einer kontinuierlichen Energieversorgung. Die letzten Jahre haben eindrücklich aufgezeigt, dass wir uns mit uns bisher kaum bekannten Themen wie einer drohenden Strommangellage oder einer Verknappung der Gasreserven konfrontiert sahen. Neben den Auswirkungen von geopolitischen Einflüssen haben Veränderungen durch die Industrie 4.0, mit Aspekten wie der besseren Vernetzung und Digitalisierung der Produktionsumgebungen. Auch die Automatisierung wird in Zukunft noch viel mehr an Bedeutung gewinnen. Durch all diese Veränderungen sehen wir uns auch vermehrt mit neuen Bedrohungen konfrontiert.

1.2. Wirtschaft

Auch aus wirtschaftlicher Sicht können kritische Infrastrukturen einen vulnerablen Bereich darstellen. Ein Angriff auf diese Systeme kann zu erheblichen finanziellen Verlusten führen, die sich auf Unternehmen, Branchen und sogar ganze Volkswirtschaften auswirken können. Der Schutz vor Cyberangriffen ist daher für die Aufrechterhaltung der wirtschaftlichen Stabilität und des Wohlstands von grosser Bedeutung. Kritische Infrastrukturen müssen rund um die Uhr betriebsbereit sein. Ein erfolgreicher Cyberangriff kann zu Ausfällen führen, die zu Unterbrechungen von Dienstleistungen, Produktionsverzögerungen oder anderen schwerwiegenden Konsequenzen führen. Durch die Implementierung einer starken Cyber Security können solche Ausfälle vermieden oder zumindest minimiert werden, um die Betriebskontinuität sicherzustellen.

1.3. Politik

In vielen Ländern gibt es Vorschriften und Standards, die die Cyber Security in kritischen Infrastrukturen regeln, um die Resilienz der kritischen Infrastrukturen gegenüber Cyberangriffen zu erhöhen. Die Einhaltung dieser Vorgaben ist notwendig, um einen einheitlichen Grundschutz über alle kritischen Sektoren einhalten zu können. Ausserdem gilt es den rechtlichen Anforderungen zu genügen, mögliche Strafen zu vermeiden und das Vertrauen der Öffentlichkeit aufrechtzuerhalten.

2. Cyber Security in der Energieversorgung

Cyberbedrohungen sind ein neues Kapitel welche als Energieversorger aktiv gemanagt werden müssen, um eine sichere und unterbrechungsfreie Energieversorgung in der Schweiz gewährleisten zu können. Dies bedingt aber das Umdenken einer gesamten Branche hin zu einem aktiven Riskmanagement im Bereich der Informationssicherheit. Dazu gehören insbesondere auch die kritischen OT-Infrastrukturen, bei welchen heute oftmals noch das Thema stiefmütterlich behandelt wird. Dafür gibt es mehrere Gründe. Einer davon ist das fehlende Bewusstsein oder Wissen über die Gefahren in Bezug auf die Informationssicherheit und OT-Sicherheit. Weitere Gründe sind fehlende Zuständigkeiten und fehlende Vorgaben, auf welche sich gerade auch kleinere Energieunternehmen abstützen können. Hier zeigt sich jedoch eine klare Tendenz der Unterstützung durch Verbände und Behörden. Insbesondere durch das BWL, welches zusammen mit den kritischen Teilsektoren IKT-Minimalstandards erarbeitet und den Unternehmen damit eine Wegleitung bietet, das eigene Unternehmen gegenüber Cyberbedrohungen resilienter zu machen. Link zum IKT Minimalstandard. Des Weiteren gibt es einen politischen Willen, verbindliche Vorgaben für kritische Infrastrukturen im Bereich Informationssicherheit zu definieren. Das BFE ist da ein Vorreiter im Stromsektor. Auf Basis des IKT-Minimalstandards definiert das BFE-Maturitätswerte welche Energieunternehmen anhand ihrer Kritikalität in Bezug des IKT-Minimalstandards zu erfüllen haben. Diese Werte sollen mit der Revision des Strom VG Mitte 2024 verpflichtend werden. Die Unternehmen müssen dann in einem Self-Assessment ihre erreichte Maturität zu den eingeforderten Subkategorien des IKT-Minimalstandards ausweisen und der ELCOM als überprüfende Instanz melden. Der VSE arbeitet eng mit dem BFE zusammen, um einen Leitfaden für die Energiebranche zu erstellen, welcher beschreibt, was die zu erfüllenden Anforderungen sind, und wie diese effizient angegangen werden und mit zielführenden Massnahmen umgesetzt werden können. Einige der wichtigen Domänen, welche durch die Unternehmen hierbei adressiert werden müssen, sind:

- Die Sicherheitsorganisation
- Das Assetmanagement
- Das Risikomanagement
- Eine Sichere Netzwerk- und Systemarchitektur
- Die Befähigung und Schulung der Mitarbeiter
- Die Erkennung und Behandlung von Sicherheitsvorfällen

3. Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen

Quelle: Marcel Suter, Leiter Geschäftsstelle Nationales Zentrum für Cybersicherheit (NCSC), 28.08.23

Das Informationssicherheitsgesetz (ISG) tritt per 01.01.2024 in Kraft. Die Einführung der Meldepflicht wird nun als Revision des ISG umgesetzt. Das ISG wird so erweitert zu einem Informationssicherheitsgesetz mit Auswirkungen auf kritische Infrastrukturen. Es ist geplant, die Meldepflicht im Rahmen einer Verordnung in Kraft treten zu lassen.

3.1. Ziele der Meldepflicht

Frühwarnung und Übersicht zur Bedrohungslage: Mehr Informationen über Cyberangriffe ermöglichen es dem NCSC andere Organisationen schneller und präziser zu warnen und eine gute Übersicht zur Bedrohungslage zu erhalten.
Rechtssicherheit und Rechtsgleichheit: Der freiwillige Informationsaustausch war lange sehr effizient. Er führt allerdings zum Problem des «Freeriding». Alle profitieren von den geteilten Informationen aber nicht alle sind bereit, Informationen über Cyberangriffe zu teilen.
Internationaler Kontext: Mit der NIS-Direktive hat die EU 2018 eine Meldepflicht für Cyberangriffe für alle Mitgliedsstaaten eingeführt.

3.2. Nächste Schritte und Zeitplan der Einführung

Nach Beschluss durch Parlament: Ausarbeitung einer Verordnung mit konkreten Vorgaben zur Meldepflicht.

- Q1 2024: Vernehmlassung der Verordnung
- Q3 2024: Beschluss der Verordnung
- Geplant ist, die Meldepflicht ab 1. Januar 2025 in Kraft treten zu lassen. Der Bundesrat wird das Datum beim Beschluss der Ver ordnung festlegen

3.3. Welche Angriffe müssen gemeldet werden

Ein Cyberangriff muss gemeldet werden, wenn er:

- die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet
- zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat
- über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde
- mit Erpressung, Drohung oder Nötigung verbunden ist.

3.4. Sanktionen Mehrstufiges Verfahren:

- Das NCSC muss die kritische Infrastruktur auf die Unterlassung aufmerksam machen.
- Kommt die Betreiberin trotz dieser Information ihrer Pflicht nicht nach, so erlässt das NCSC eine Verfügung über die umzu setzenden Pflichten.
- Wird die Verfügung ignoriert, erstattet das NCSC Strafanzeige. Möglich sind Bussen bis CHF 100’000.

Weiterführende Informationen zum Thema Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen finden Sie im gleichnamigen Blog-Artikel unter alsec.ch.

Sie wünschen:

- Eine Beratung bezüglich unseren Aktiven OT-Systemen
- Ein kommerzielles Angebot
- Ein “Proof of Concept”
- Unterstützung bei der Konfiguration oder Inbetriebnahme
- Hilfe bei der Fehlersuche/-behebung
- Ein Supportvertrag

Wir von der **Connect Com** stehen Ihnen gerne zur Verfügung!

Connect Com AG
Wahligenstrasse 4a
6023 Rothenburg

www.ccm.ch
info@ccm.ch
+41 41 854 00 00

Sie wünschen:

- Eine Beratung durch einen Experten, spezialisiert auf den Schutz von kritischen Infrastrukturen und Systemen
- Ein Netzwerk Audit, zur Prüfung ihrer IT/OT Sicherheit
- Ihre Cyber Strategie zu verbessern und die Folgen durch System störungen zu minimieren
- Die Widerstandsfähigkeit ihrer Infrastruktur vor Cyberangriffen zu stärken
- aufkommende Bedrohungen frühzeitig zu erkennen und darauf angemessen zu reagieren

Die Firma **ALSEC** steht Ihnen gerne zur Verfügung!

ALSEC Cyber Security Consulting AG
Werkstrasse 12
5080 Laufenburg

www.alsec.ch
info@alsec.ch
+41 62 874 3000

ALSEC Cyber Security Consulting AG
Autor: Reto Amsler / Peter Müller, Alsec