Cybersecurity Act, IT-Sicherheitsgesetz 2.0 und die aktuellen Cybergefahren in der Energiewirtschaft

Stefan Loubichi

Abstract

Kurzfassung Überschrift

Terrorists and criminals have discovered cyber security as an interesting target. Most of the big companies have already become victims of cybercrime. According to the latest information from the National Cyber Defense Center, we must except a nearby attack on the energy supply systems in Europe. And we must not forget that Europe was on January 10, 2019 9:00 p.m. shortly before a blackout and we should remind that there are more and more such scenarios every week. For these reasons, it is clear that the Cyber Security Act of the European Union came just in time.

This essay shows by means of facts that cyber security is urgently needed in Europe in the energy sector. It is shown in the current ITU reports that Germany is anything but the leader in digitization or cyber security. Also, we show how cyber security is legally implemented in Russia or China, the two leading cyber crime countries.

Afterwards the essay deals extensively with the European Cyber Security Act. The structure and tasks of the ENISA are presented as well as the certification scheme in the field of cyber security and the requirements of a corresponding certification authority. The current scheme of cyber attacks by APT Berserk Bear on the German energy sector is presented, as well as the helpful ENISA IoT Security Standards Gap Analysis.

Finally, the corresponding IT security law 2.0, which is expected to come into effect in autumn, will be discussed in its most important aspects for the energy industry.

Of course, a conclusion is drawn, what the German energy industry -from the perspective of the author of this essay- has to do to be well prepared for the new challenge. If you want to mention three points in this context, then these are the following:

- *product certification*
- *system certification and*
- *holistic training in the field IT-/OT-security*

Of course, this costs money, but a blackout is more expensive for everyone.

Autor

Prof. h.c. PhDr. Dipl.-Kfm./ Dipl.-Vw. Stefan Loubichi,
International experienced lead auditor for management systems (ISO 27001, ISO 14001, ISO 9001, ISO 45001, ISO 26000), auditor according to § 8 BSI-Law and IT-security catalogue, more than ten years of international experience in implementing IT- and cyber security
Essen, Deutschland

Ist Cybersecurity wirklich erforderlich

Laut einer aktuellen Veröffentlichung des VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. (https://www.vde.com/topics-de/cyber-security) haben VDE Mitgliedsunternehmen angegeben, dass 71 % der Unternehmen mit mehr als 5.000 Mitarbeitenden bereits Opfer von Cyber-Angriffen geworden seien. Dies sind mehr als erschreckende Zahlen. Gemäß des am 15. Juli 2019 von der European Agency for Cybersecurity (ENISA) veröffentlichten 2019er Jahresbericht „Trust Services Security Incidents 2018“ gab es 2018 18 Vorfälle, wohingegen die Anzahl der Vorfälle für das Jahr 2017 noch bei 14 lag und für das Jahr 2016 lediglich ein Vorfall zu verzeichnen war. Dies sind per se erst einmal mehr als alarmierende aktuelle Zahlen.

Womit in Zukunft zu rechnen ist, offenbaren Verlautbarungen des nationalen Cyber-Abwehrzentrums vom August 2018 mit dem Titel „Gefährdungslage der Stromversorgung in Deutschland durch Cyberangriffe“, aus denen wie folgt zitiert wird:

„Sabotageaktionen gegen kritische Energieinfrastrukturen in Deutschland sind bis dato nicht bekannt geworden. Bei den Angriffen auf die Stromversorgung konnte kein unmittelbarer Bezug nach Deutschland festgestellt werden. Anders verhält es sich bei Ausspähungsaktivitäten, bei denen eine Betroffenheit deutscher Unternehmen durchaus festzustellen ist: In der Gesamtheit verdichten sich Hinweise, dass eine oder mehrere Tätergruppen langfristige Anstrengungen unternehmen, um Energie-Infrastrukturen in den USA und Europa aufzuklären. Dafür sprechen die Angriffskampagne Berserk Bear, die sich gegen deutsche und internationale Unternehmen, insbesondere aus dem Energiesektor richtet, Meldungen über Spear-Phishing-Angriffe aus Energieunternehmen von Mitte 2017 sowie eine Reihe anderer Sachverhalte in den letzten Jahren. Die geschilderten Kampagnen belegen, dass Akteure langfristig und mit großem Aufwand Kompetenzen aufbauen und spezifische Angriffsmethoden und -werkzeuge entwickeln, um wirksam Angriffe gegen Prozesssteuerungsanlagen durchführen zu können, vor allem im Energiesektor. Als besonders kritisch ist zu bewerten, dass die beobachteten Aktivitäten nicht nur auf reine Informationsbeschaffung abzielen, sondern auch Sabotagefähigkeiten und -absichten zeigen. Bei diesen Aufklärungsaktivitäten stehen auch deutsche Unternehmen im Fokus der Angreifer. ...

Auch Experten aus der Energiewirtschaft, die im Rahmen des UP KRITIS befragt wurden, schätzen Risiken durch Monokulturen (Smart Meter, IDS High-Leitprodukte, die aufgrund passenden Zuschnitts auf die spezifischen Anforderungen der Branche in vielen Anlagen eingesetzt werden) als wahrscheinlicher ein, als einen Angriff wie 2015 in der Ukraine. ...

Grundlegende Veränderungen durch gravierende (außen-)politische Entwicklungen oder wirtschaftliche Veränderungen und eine tatsächliche oder unterstellte Verwicklung Deutschlands in internationale Konflikte mit ernst zu nehmenden staatlichen Cyberakteuren bergen allerdings das Risiko, dass vor diesem Hintergrund Cybersabotageaktionen gegen IT-Systeme in Deutschland oder deutscher Unternehmen im Ausland durchgeführt werden könnten. KRITIS-Bereiche und hier insbesondere die Energie bzw. Stromversorgung stellen hierbei dann ein bevorzugtes Angriffsziel für Cyberangriffe dar.“

Vergegenwärtigt man sich diese Aussagen aus unterschiedlichen Quellen so wird deutlich, dass Cybersabotage in der Energie bzw. Stromversorgung auch in Deutschland als Gefahr sehr ernst genommen werden sollte.

Die europäische Dimension der Versorgungssicherheit

Wir dürfen hier im Übrigen auch nicht die europäische Dimension vergessen, denn „Fehler/Probleme“ in Ländern der EU verursachen in der gesamten EU entsprechende Herausforderungen, was das Beispiel 10. Januar 2019 21:00 Uhr zeigte:

In weniger als zwei Minuten sackte die Netzfrequenz europaweit auf den kritischen Wert von 49,8 Hertz ab und drohte weiter zu fallen. Primäre Regelleistung

hätte nicht gereicht, Reservekraftwerke hätten nicht schnell genug angefahren werden können, so dass nur durch das beherzte Eingreifen des französischen Übertragungsnetzbetreibers RTE durch Notlastabwurf aller 22 abschaltbaren Stromgroßverbraucher in Frankreich der Blackout verhindert werden konnte. Hierdurch wurden auf einen Schlag 1.500 MW vom Netz genommen, so dass um 21:25 Uhr die 50,0 Hertz erreicht wurden.

Erst einmal stellt sich die Frage, wie häufig etwas Derartiges überhaupt geschieht. Laut Auskunft der Europäischen Kommission an das Europäische Parlament vom 21. März 2019 (Bezugsdokument E-000428/2019) handelte es sich nach Angaben von ENTSO-E bei diesem Ereignis um einen Störfall der Stufe 1 (auf einer Stufe von 0 bis 3), wobei es laut jüngstem Bericht des ENTSI-E alleine im Jahr 2016 327 derartiger Vorfälle gab.

Laut https://www.netzfrequenzmessung.de/ aktuelles.htm#2019_01 geschah am 10. Januar 2019 folgendes:

„Die Analysen der ÜNBs und von ENTSO-E zeigten, dass der Frequenzabfall durch das Zusammenspiel mehrerer Faktoren zustande kam. Zu der durch den Stundenhandel verursachten deterministischen Frequenzabweichung kam eine fehlerhafte („eingefrorene") Messung auf vier Leitungen zwischen Deutschland und Österreich, wodurch anstelle des aktuellen Leistungsdefizits ein veralteter Wert für die Regelleistungserbringung verwendet wurde.

Um 19:55 Uhr UTC beginnt der durch den Stromhandel bedingte Frequenzabfall zum Stundenwechsel. Um 20:01 Uhr stellt sich eine Stagnation für ca. eine Minute ein. Danach fällt die Frequenz mit ca. 2,5 mHz/Sekunde bis auf 49,800 Hz.

Beim Erreichen der 49,8 Hz wurden erste Maßnahmen zur Frequenzhaltung getriggert, wodurch vorher festgelegte Lasten abgeworfen wurden. Dies können z.B. Pumpspeicher im Ladebetrieb oder Industriebetriebe mit abschaltbaren Lasten sein. So berichtet z.B. der französische Netzbetreiber RTE, dass mehr als 1,5 GW industrielle Lasten automatisch für 20 bis 45 Minuten abgeworfen wurden, was das erste Mal seit Aufbau dieses Instruments gewesen sei.

Die Suche nach dem Grund für diesen Vorfall läuft noch. Es gab ein Kraftwerk in Spanien. dass in dem Zeitraum einen Ausfall hatte (558 MW). Ausfälle in dieser Größenordnung werden normalerweise von der Primärregelleistung (3.000 MW) problemlos abgefangen. Nach aktuellem Stand (siehe Pressemeldung ENTSO-E vom 16.01.2019) gab es bei TenneT Deutschland an der Grenze zu Österreich Fehlmessungen. ...“

Auch wenn der automatische Lastabwurf funktionierte, so stellt sich natürlich die Frage, warum die Primärreglung den langsamen Frequenzabfall nicht aufhalten konnte. Hierzu sieht ENTSO-E die beiden folgenden potenziellen Möglichkeiten:

– Der Fehler in der Leistungsbilanz des Netzes war größer als die zu dem Zeitpunkt aktivierte Primärregelleistung (über 2.600 MW).
– Die Dienstleistung zur Erbringung von Primärregelleistung wurde in diesem Zeitraum von vielen Kraftwerken nicht eingehalten.“

Dieses Beispiel des 10. Januar 2019 mag verdeutlichen, dass Energieerzeugung nur noch in europäischen Dimensionen zu beherrschen ist und folglich der (erfolgreiche) Cyberangriff auf das Stromnetz eines EU-Landes unweigerlich umgehende Auswirkungen auf die gesamte EU hätte. Somit bedarf es einer europäischen Sichtweise auf das Thema Cybersecurity im Strommarkt.

Unkommentiert in diesem Zusammenhang die Antwort unserer Bundesregierung auf eine „Anfrage zur Versorgungssicherheit in Deutschland in Zeiten der Energiewende“ vom 7. März 2018:

„... Die Bundesregierung ist der Überzeugung, dass der 2016 mit der Novelle des EnWG reformierte Strommarkt („Strommarkt 2.0“) jederzeit für einen Ausgleich von Angebot und Nachfrage sorgt. Auch bei zunehmenden Anteilen fluktuierender erneuerbarer Energie stellt er eine zuverlässige Versorgung mit Strom sicher. ...

Vorfestlegungen, welcher Stromverbraucher im Bedarfsfall am Netz bleibt und wer stromlos sein wird, gibt es im Allgemeinen nicht und diese sind auch zumeist nicht möglich. Derartige Entscheidungen fällen die Netzbetreiber im Einzelfall unter Berücksichtigung aller maßgeblichen Umstände. ...“

Quelle: Deutscher Bundestag, Drucksache 19/1104, Antwort der Bundesregierung

Auch wenn nicht mehr ganz aktuell so sollten nach diesseitiger Auffassung die Ausführungen des Büros für Technologiefolgen-Abschätzung beim Deutschen Bundestag mit dem Titel „Was bei einem Blackout geschieht“ zur Kenntnis genommen werden. Die Folgen eines Blackouts in Deutschlands wären letztlich so gravierend wie ein konventioneller Terrorakt.

Quelle: https://www.tab-beim-bundestag.de /de/ pdf/publikationen/buecher/petermann-etal-2011-141.pdf

Wie sieht es eigentlich mit den anderen Cyber-Playern aus?

Betrachten wir an dieser Stelle erst einmal den Global CyberSecurity Index (GCI) 2018 der ITU. Da es sich bei der ITU um eine Sonderorganisation der Vereinten Nationen handelt und die ITU für ihre Fachlichkeit und Unabhängigkeit bekannt ist, werden hier sicherlich viele Personen ob der Rückständigkeit Deutschlands im globalen Ranking erschrecken.

– 1. Großbritannien
– 2. USA
– 3. Frankreich
– 4. Litauen
– 5. Estland
– 6. Singapur
– 7. Spanien
– 8. Malaysia
– 9. Kanada und Norwegen
– 10. Australien
– 11. Luxemburg
– 12. Niederlande
– 13. Saudi-Arabien
– 14. Japan und Mauritius
– 15. Südkorea
– 16. Oman
– 17. Katar
– 18. Georgien
– 19. Finnland
– 20. Türkei
– 21. Dänemark
– 22. Deutschland
– 23. Ägypten
– 24. Kroatien
– 25. Italien

Quelle: https://www.itu.int/en/ITU-D/Cybersecurity /Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

Nun mag man vielleicht aus verletztem Nationalstolz argumentieren, dass in Deutschland die Digitalisierung viel weiter fortgeschritten ist, als in Malaysia und dass diese aufgrund geringerer Digitalisierung vor uns im Ranking stehen.

Vergegenwärtigen wir uns hierzu das weltweite Digitalisierungsranking, um den Sachverhalt zu korrelieren:

– 1. Island
– 2. Südkorea
– 3. Schweiz
– 4. Dänemark
– 5. Großbritannien
– 6. Hongkong
– 7. Niederlande
– 8. Norwegen
– 9. Luxemburg
– 10. Japan
– 11. Schweden
– 12. Deutschland
– 13. Neuseeland
– 14. Australien
– 15. Frankreich
– 16. USA
– 17. Estland
– 18. Singapur
– 19. Monaco
– 20. Irland
– 21. Österreich
– 22. Finnland
– 23. Israel
– 24. Malta
– 25. Belgien

Quelle: https://www.itu.int/net4/ITU-D/idi/2017/ index.html

Letztlich gibt es wichtige Staaten mit einer höheren Digitalisierung als Deutschland wie Großbritannien, Südkorea, Niederlande, Norwegen oder Japan, die auch im Bereich der Cybersecurity vor uns liegen.

Interessant ist in diesem Zusammenhang natürlich, wie China und Russland als große Nationen mit staatlichen Cybersecurity-Angriffsmöglichkeiten ihre Cybersecurity legislativ absichern.

Russland:

Zum 1.1.2018 ist in der Russischen Föderation das Cyber-Sicherheitsgesetz (No. 187 FZ) in Kraft getreten. Es ist klar strukturiert, besteht aus nur 14 Artikeln und beschäftigt sich mit der Schaffung eines gesamtstaatlichen Systems zur Informationssicherheit, d.h. das Gesetz geht weit über die Absicherung kritischer Infrastrukturen hinaus. Die Unternehmen werden zu technisch-organisatorischen Cybersicherheitsmaßnahmen verpflichtet und sind zur Teilnahme an einem gesetzlich geregelten Informationsaustausch mit der russischen Bundesbehörde für Informationssicherheit verpflichtet. Kritis-Betreiber (zu denen im Gegensatz zu Deutschland auch Chemie und Bergbau gehören) müssen auch mit unangemeldeten Kontrollen der zuständigen Bundesbehörde rechnen.

Für das Programm „Digitale Wirtschaft“ werden für den Aufbau föderaler und regionaler Cyberabwehrzentren sowie das Ersetzen ausländischer durch russische Software 500 Millionen Euro zur Verfügung gestellt.

Man ist sich somit in Russland dieser Gefahren bewusst und kennt die Schwachstellen. Gemäß einer am 21.07.2019 bekannt gewordenen Datenpanne beim IT-Dienstleister SyTech ist es der bekannten Hackergruppe 0v1ru$ gelungen, beim russischen Inlandsgeheimdienst FSB 7,5 Terrybyte an Daten zu laufenden Projekten und Operationen des russischen Inlandsgeheimdienstes FSB zu entwenden. Informationen wurden dabei zu den Projekten Mentor, Arion, Relation, Hrywnia, Nautilius, Nautilius-S, Hope und Tax-3 erbeutet, wobei Hope und Tax-3 im Falle einer feindlichen Cyberattacke helfen sollen, das russische Netz vom Rest des Internets abzutrennen.

Quelle: https://www.heise.de/newsticker/meldung/Russischer-Geheimdienst-Massiver-Datenver lust-beim-KGB-Nachfolger-FSB-4476027. html

Für alle IoT-Geräte soll es bis September 2019 ein Gesetz geben, dass eine verbindliche Registrierung aller IoT-Gesetze verlangen wird und ein eigenes russisches Betriebssystem für IoT-Geräte findet sich vor der Fertigstellung. Dass Russland selbst oftmals Opfern von Hackerangriffen ist, kann daran ersehen werden, dass 2017 der Verlust bei russischen Unternehmen durch Cyberattacken circa 1,7 Milliarden Euro betrug und circa 20 % der russischen Unternehmen Opfer einer Cyberattacke wurden.

China:

Im Gegensatz zu Europa fasst die Volksrepublik China Datenschutz sowie IT-Sicherheit und Cybersecurity grundsätzlich in einem Gesetz zusammen.

Das zum 1. Juni 2017 in Kraft getretene Cybersecurity-Gesetz (CSG) ist die Basis von circa 300 nationalen Standards. Zielgruppen des CSG sind:

- Nutzer (natürliche und juristische Personen, die das chinesische Internet nutzen)
- Netzwerkbetreiber
- Kritische Infrastruktur (Qualifizierte Netzwerkbetreiber aus bestimmten Branchen mit hohem Schutzbedarf)

Schwellenwerte wie zum Beispiel bei der deutschen KRITIS-VO (Verordnung) gibt es beim Chinesischen Cybersecurity-Gesetz nicht. Wie streng das CSG umgesetzt wird kann daran ersehen werden, dass chinesische Behörden alle Webseiten und Social-Media-Kanäle auf die Einhaltung sozialistischer Werte und der politischen Korrektheit prüfen.

Von besonderer Relevanz sind folgende Aspekte:

- Daten, die beim Betrieb von Kritischen Infrastrukturen anfallen, sind grundsätzlich in China zu speichern.
- Nutzung von staatlich-lizenzierten VPNs ist vorgeschrieben
- Zwingende Anforderungen relevanter nationaler Standards sind einzuhalten, d.h. die Betreiber kritischer Infrastrukturen sind gezwungen nur Netzwerkprodukte und -services einzukaufen, für die die Einhaltung relevanter Standards in Sicherheitsüberprüfungen nachgewiesen ist
- Netzwerkprodukte aus dem Bereich Industrie 4.0 sind mit deren Daten zu erfassen

Berichte, dass chinesische Top-Firmen gehackt wurden, finden sich gut wie kaum. 2016 wurde alibaba gehackt, 2010 baidu. Aktuelle Fälle sind nicht bekannt. Viel mehr ist derzeit nicht bekannt.

Der CyberSecurity-Act

Prinzipiell geht es beim Cybersecurity Act der Europäischen Union um zwei Dinge:

- ein dauerhaftes Mandat für die EU-Cybersicherheitsagentur (ENISA) anstelle ihres bislang befristeten Mandats, welches 2020 ausgelaufen wäre, sowie eine deutliche (letztlich aber immer noch zu geringe) Aufstockung der Mittel der Agentur, damit sie ihre Aufgaben erfüllen kann, sowie
- eine Stärkung der ENISA im neuen Rahmen für die Zertifizierung der Cybersicherheit, damit sie die Mitgliedstaaten dabei unterstützen kann, wirksam auf Cyberangriffe zu reagieren, und damit sie eine größere Rolle bei der Zusammenarbeit und Koordinierung auf Unionsebene übernehmen kann.

Darüber hinaus wird die ENISA dazu beitragen, die Cybersicherheitskapazitäten innerhalb der EU zu erhöhen als auch den Kapazitätsaufbau und die Abwehrbereitschaft zu fördern. Des Weiteren wird die ENISA als unabhängiges Kompetenzzentrum dienen, das einerseits dazu beiträgt, ein hohes Problembewusstsein der Bürger*innen und Unternehmen zu fördern, und andererseits die EU-Organe und die Mitgliedstaaten bei der Politikentwicklung und -umsetzung unterstützt.

Durch diesen Rechtsakt zur Cybersicherheit wird zudem ein EU-weit geltender europäischer Zertifizierungsrahmen für die Cybersicherheit von Produkten, Verfahren und Diensten geschaffen. Dies ist bahnbrechend, denn es handelt sich um die erste Binnenmarktvorschrift zur Bewältigung der Herausforderung, die Sicherheit von vernetzten Produkten, von Geräten des Internets der Dinge und von kritischen Infrastrukturen mithilfe solcher Zertifikate zu erhöhen. Aufgrund eines solchen Rahmens für die Cybersicherheitszertifizierung werden Sicherheitsmerkmale bereits in der Frühphase der technischen Konzeption und Entwicklung berücksichtigt („eingebaute Sicherheit“). Darüber hinaus gibt der Rahmen den Nutzern die Möglichkeit, sich über das Sicherheitsniveau zu vergewissern, und gewährleistet, dass diese Sicherheitsmerkmale von unabhängiger Seite überprüft werden.

In der Ausbaustufe sollen die Strukturdaten der ENISA wie folgt aussehen:

- Anzahl der Mitarbeitenden: 125
- Jahresbudget: 23 Millionen EURO

Geschäftsführender Direktor der ENISA ist derzeit Prof. Dr. Udo Helmbrecht. Sitz der ENISA ist Iraklio auf der griechischen Insel Kreta.

Vergegenwärtigen wir uns an dieser Stelle die normativen Eckpunkte:

- Bei der Entwicklung der Zertifizierungsschemata soll ENISA die europäischen Normungsorganisationen konsultieren (Erwägungsgrund 53).
- Es geht (zumindest zum Beginn) um die Schaffung eines Rahmens für die freiwillige Zertifizierung von Cybersicherheit auf der Basis verschiedener Schemata, welche sich auf die Vertrauenswürdigkeitsstufen
  - niedrig
  - mittel
  - hoch

  beziehen.
- Vergleichbar mit der Kontext-Philosophie des Normkapitels 4 der ISO/IEC 27001 soll eine Stakeholder Cybersecuri-

ty Certification Group und eine Advisory Group zur Unterstützung und Beratung gebildet werden, in denen Repräsentanten der europäischen, aber auch der internationalen Normungsorganisation eingebunden sein sollen. Es bleibt somit zu hoffen, dass sich die Entitäten der Energiewirtschaft nicht auf das „Meckern" beschränken, sondern aktiv mitarbeiten, um die entsprechenden Einflussmöglichkeiten wahrzunehmen.
- Sowohl auf europäische als auch auf internationale Normen sollten sich die Zertifizierungsschemata stützen (Erwägungsgrund 69)
- Sind geeignete Normen nicht vorhanden, so sollen technische Spezifikationen herangezogen werden (Erwägungsgrund 75). Gerade in Hinblick auf die stets diskutierbare Thematik des Standes der Technik ist dies für Branchenorganisation die Möglichkeit, technische Spezifikationen zu entwickeln und einzubringen.
- Das Arbeitsprogramm für Cybersicherheitszertifizierungssysteme soll im Rahmen der Normungsaufträge der Europäischen Kommission hinreichend berücksichtigt werden (Erwägungsgrund 84)
- Wenn gemäß Artikel 2 Absatz 19 von einer Norm gesprochen wird, so sind darunter Dokumente zu verstehen, welche von den Normungsorganisationen angenommen worden sind. Die Betonung liegt hier eindeutig auf dem Wort angenommen.
- Nur wenn es im Rahmen der Zertifizierungssysteme an internationalen, europäischen oder nationalen Normen fehlt, sind technische Spezifikationen referenzierbar.

Gerade in Hinblick auf den Normencharakter des Cybersecurity Acts sind aber bereits heute einige Fragen evident:
- Wer entscheidet darüber, welche Norm zur Anwendung kommt?

  Gerade in Hinblick auf die Mächtigkeit und Komplexität der ISO/IEC 62443 – Familie ist dieser Sachverhalt von Relevanz.
- Wie wir mit widersprüchlichen Normen umgegangen?

  Vergegenwärtigt man sich zum Beispiel das erstklassige BDEW Whitepaper, welches gerne als Best Practice im Rahmen der Adaption des IT-Sicherheitskataloges nach § 11 Abs. 1b EnWG angesehen wird, so muss gleichwohl bei der Erwähnung verschiedener Normen die Frage erlaubt sein, ob es überhaupt stets möglich ist, die „einzig wahre" Norm zu finden.
- Mit welchen Standardisierungsgremien erfolgt eine Zusammenarbeit, wenn es konkurrierende Gremien geben sollte?

Ein nicht zu unterschätzender Nebenkriegsschauplatz besteht darin, dass ENISA mit 125 Mitarbeitenden letztlich personell unterbesetzt ist und es viele konkurrierende Organisationen auf EU Ebene gibt, wie zum Beispiel:
- CERT-EU (Computer Emergency Response Team): zuständig für Angriffe auf die IT in den EU-Einrichtungen
- EC3 (European Cybercrime Centre): zuständig, wenn entsprechende Anfragen aus dem Europol-Cyber-Intelligenzteam kommen, welches sich wiederum aus dem CSIRT (National Network of Computer Security Incident Response Teams) zusammensetzt, den nationalen Pendants zum CERT-EU
- EDA (European Defence Agency): zuständig für die Cybersecurity im Rahmen der gemeinsamen Sicherheits- und Verteidigungspolitik der EU.
- EU-LISA (European Agency for the operational Management of large-scale IT-Systems): zuständig für den Schutz großer Informationssysteme wie Visa (VIS) und Fingerabdrücke (EURODAC).
- EASA (European Aviation Safety Agency): zuständig für die Cybersecurity in der Luftfahrt [wobei es ähnliche Einrichtungen noch für den Schienen- und Schiffsverkehr gibt]

Es ist eindeutig verbesserungsfähig, wenn wir so viele unterschiedliche Cybersecurity-Instanzen in der Europäischen Union haben, denn es wird keine Linearität bei Cyber-Angriffen geben. Die NATO hatte im Cyber-security Bereich die gleichen Probleme, bis Koen Gijsbers GM der NATO Communication and Information Agency wurde und eine schlagkräftige Vereinheitlichung realisiert wurde. Wären seine Ideen früher realisiert worden, hätten die Chinesen große Teile der Baupläne des NATO Kampfjets F 35 nicht kopiert und diese dann zur Entwicklung des eigenen Kampfjets Shenjang J 31 genutzt.

Wirklich hilfreich sein werden die im Rahmen des Cyber Security Act durch die ENISA durchzuführenden Cybersicherheitsübungen, die man gerade im Falle des KRITIS-Sektors Energie benötigt. Der vorstehend beschriebene Fall des 10. Januar 2019 mag verdeutlicht haben, warum man Ausfälle im Energiebereich EU-weit behandeln muss. In diesem Zusammenhang sei auch auf die nachstehend aufgeführte aktuelle Forschungsarbeit der TU Dresden verwiesen.

Kommen wir nun nochmals abschließend zur Thematik der Zertifizierungen. Diese sind derzeit grundsätzlich freiwillig, sofern dazu nichts anderes im Unionsrecht oder im Recht der Mitgliedsstaaten festgelegt ist. Gleichwohl wird die EU-Kommission in bestimmten Zeitintervallen prüfen, ob Cybersicherheitsverifizierungen als verbindlich festgeschrieben werden sollten.

Vergegenwärtigt man sich zum Beispiel die vorstehend beschriebene russische und chinesische Cybergesetzgebung und vergegenwärtigt man sich den Fall Huawei in den USA, so wird deutlich, dass Produktzertifizierungen mit einer nicht geringen Wahrscheinlichkeit zur Pflicht werden könnten. Nun kann man dies natürlich auch als Verdrängungswettbewerb im Produktbereich der industriellen Automatisierung sehen oder als Industriepolitik für einen bestimmten Konzern, der seit Jahren hier exzellente Arbeit betreibt bzw. oftmals Vorreiter in der Produkt- und Systemzertifizierung von SCADA-Systemen ist. In meiner Eigenschaft als Lead-Auditor im Bereich des IT-Sicherheitskataloges nach § 11 Abs. 1a EnWG erlaube ich mir an dieser Stelle jedoch auf nachfolgende Erfahrungswerte im SCADA-Umfeld bei entsprechenden Audits verwiesen:
- Es wurden Systeme gefunden, zu denen es keine hinreichende Bedienerdokumentation gab, da die alten Hersteller von Dritten aufgekauft wurden und die Dokumentation bzw. die Funktionalität des Systems nicht weiter gepflegt wurde.
- Es wurden Systeme gefunden, bei denen es nicht die Möglichkeit gab, Passwörter zu ändern.
- Es wurden Systeme gefunden, bei denen es nur vorgesehen war, dass Updates ein Mal im Jahr durchgeführt werden können.

Diese Liste könnte man beliebig fortsetzen und sie dürfte aufzeigen, warum eine Produktzertifizierung in Sachen Cybersecurity großen Sinn machen würde.

Nachstehend zur Kenntnis, welche Anforderungen die Konformitätsbewertungsstellen im Bereich der Cybersecurity zukünftig erfüllen müssen:

Anforderungen an Konformitätsbewertungsstellen

Gemäß des Anhangs zur Verordnung (EU) 2019/881 müssen Konformitätsbewertungsstellen (nachfolgend nur noch KBS genannt) unter anderem die nachfolgenden Kriterien erfüllen:
- eigene (nationale) Rechtspersönlichkeit
- unabhängiger Dritter, der mit ITK-Produkten, -Dienstleistungen oder- Prozessen (, die er bewertet) keine Verbindung hat
- Unabhängigkeit bzw. Interessenskonfliktfreiheit zu nationalen Behörde für Cybersicherheitszertifizierung (für den Fall dass die KBS Eigentum einer öffentlichen Stelle ist)
- Gewährleistung von Vertraulichkeit, Objektivität und Unparteilichkeit
- finanzielle Unabhängigkeit
- Unterauftragsvergabe nur an zuverlässige, fachkundige Dritte sowie vollumfängliche Dokumentation
- Mitarbeitende der KBS müssen erforderliche fachliche Kompetenz und einschlägige Erfahrung haben
- Es müsse angemessene Verfahren und Regelungen zur Durchführung der Kon-

formitätsbewertungen vorhanden sein
- Es müssen hinreichend finanzielle Mittel vorhanden sein
- Prüfende müssen solide Fach- und Berufsausbildung für alle KBS-Tätigkeiten haben, angemessene Kenntnis und Verständnis der Anforderungen/Prüfnormen haben und des Reportings haben
- Die Vergütung der KBS Mitarbeitenden muss unabhängig von der Zahl oder dem Ergebnis der Konformitätsbewertungen sein
- Hinreichende Haftpflichtversicherung
- Realisierung des Schutzes des geistigen Eigentums und der Verschwiegenheit
- KMU-Relevanz muss gegeben sein
- Anforderungen der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, welche die Zertifizierung von IKT-Produkten, -Diensten oder Prozesse vornehmen muss gegeben sein. Dies gilt auch für entsprechende Prüflabore.

Aktuelles Schema der Cyberangriffe der APT Berserk Bear auf den deutschen Energiesektor

Vergegenwärtigen wir uns nachfolgend das Angriffs- und Aufklärungsschema der APT Berserk Bear (auch unter den Namen Energetic Bear, Crouching Yeti oder Dragonfly bekannt):

Die Angreifer verwenden in der Regel öffentlich zugängliche Angriffswerkzeuge und versuchen unzureichend gesicherte Systeme unter ihre Kontrolle zu bringen. In einem ersten Schritt scannen die Angreifer einen Netzbereich mit potenziellen Opfern mit einem Portscanner, um einen Überblick über die Ports und Dienste zu erhalten, die offen vom Internet aus zu erreichen sind. Im Fokus stehen hierbei vor allem:
- Secure Shell (SSH, Port 22 TCP)
- Telnet (Telnet, Port 23 TCP)
- Hypertext Transport Protocol (HTTP, Port 80 TCP)
- Simple Network Management Protocol (SNMP, Port 161/162 UDP)
- Cisco Smart Install (SMI, Port 4786 TCP)

Neben möglichen Brute-Force-Angriffen auf die Fernwartungsprotokolle Telnet und SSH zwecks Erraten von Zugangsdaten senden die Angreifer SNMP- und SMI-Pakete mit entsprechenden Parametern an aktive Netzwerkkomponenten (z.B. Router) der Opfer. Falls Schutzmaßnahmen vor unbefugtem Zugriff wie Access Control Lists (ACL) auf den Komponenten konfiguriert wurden, werden die entsprechenden SNMP-Pakete mit gefälschten Absender-IP-Adressen versehen (IP-Spoofing, UDP Port 161), um die Schutzmaßnahmen zu umgehen. Die an die Komponenten per SNMP oder SMI übermittelten Steuerbefehle veranlassen die Netzwerkkomponente, die aktuellen Konfigurationseinstellungen (u.a. die sog. running-config) an einen vom Angreifer kontrollierten Server via Trivial File Transfer Protokoll (TFTP) zu senden.

Die vom Opfer übermittelten Daten enthalten sensible Informationen u.a. zu der aktuellen Konfiguration, Modell, Hardware und Firmware des Routers, zur Infrastruktur des Netzwerkes und der Routingtabelle, zu freigegebenen Ports, Usernames und Passwörtern bzw. Hashwerten von Passwörtern.

In manchen Fällen wurden zudem unbefugte Änderungen an der Konfiguration der Netzwerkkomponenten vorgenommen, die zu einer Umlenkung von Datenverkehr über Angreifer kontrollierte Systeme führten (GRE-Tunnel, Re-Routing). Dies ermöglicht den Angreifern das Auslesen und Manipulieren des umgeleiteten Netzwerkverkehrs (sog. Man-in-the-Middle-Angriff, kurz: MITM) sowie das Abschöpfen weiterer Zugangsdaten. Als weiteren Angriffsvektor verwendet der Angreifer Spear Phishing Mails mit Anhängen oder vom Angreifer veränderte Webseiten, die einen sogenannten UNC-Verweis auf eine vom Angreifer kontrollierte, scheinbare Windows-Dateifreigabe enthalten (SMB3-Capture bzw. SMBTrap). Dies kann Windows-basierte Opfersysteme dazu veranlassen, den Benutzernamen und zugehörige Authentifizierungsdaten (NTLM-Hash) an das Angreifersystem zu übermitteln. Die erbeuteten Login-Daten erleichtern es dem Angreifer, gegebenenfalls weitere Zugriffe auf das Opfernetzwerk über Remote-Services durchzuführen. Durch Verwendung legitimer Login-Daten fallen diese Zugriffe unter Umständen nicht sofort auf.

Auch wenn es wenig spektakulär ist, so ist der wirksamste Weg, um zu erkennen, ob man von einem Angriff betroffen ist, die Durchsicht der Netzwerklogs auf:
- ungewöhnliche Zugriffsversuche auf ggf. von außen erreichbare Telnet- und SSH-Dienste
- unerwartete SNMP- bzw. SMI-Pakete
- ungewöhnliche TFTP-Verbindungen mit Zielen außerhalb der eigenen Netzgrenzen

Die nachfolgenden Punkte sollten dabei ebenfalls zum Standardprogramm gehören, zumal wir aufgrund der OT-Thematik logischer Weise nicht immer die neuesten Komponenten haben:
- Deaktivieren Sie bei Netzwerkkomponenten (z.B. Router, Switches) nicht verschlüsselte LegacyProtokolle wie z.B. Telnet, SNMPv1 oder SNMPv2c. Verwenden Sie nach Möglichkeit moderne verschlüs-selte Protokolle wie SSH oder SNMPv3.
- Durchsuchen Sie die Logdateien nach Datenverkehr, der an die Ports 23 TCP (Telnet), 161/162 UDP (SNMP) oder 4786 TCP (Cisco SMI) gerichtet ist. Prüfen Sie, ob die unten aufgelisteten netzwerkbasierten IOC in den Logdateien vorkommen.
- Durchsuchen Sie die Logdateien nach ausgehendem TFTP-Datenverkehr, der an das Internet gerichtet ist. Sollten Sie einen Zusammenhang zwischen eingehendem SNMP-Verkehr und kurz darauffolgendem ausgehenden TFTP-Verkehr finden, ist eine gründliche Analyse dieses Verkehrs empfehlenswert.
- Konfigurieren Sie Ihre Firewall entsprechend, sodass in das Internet ausgehender TFTP-Verkehr blockiert wird.
- Überprüfen Sie regelmäßig die Gerätekonfigurationen der Netzwerkkomponenten. Insbesondere sollte geprüft werden, ob es unbefugte Änderungen an Routingtabellen und Access Control Lists (ACL) gibt und ob ungewöhnliche GRE5-Tunnel eingerichtet wurden.
- Sperren Sie unerwünschten eingehenden Datenverkehr (aus dem Internet) und ausgehenden Datenverkehr (in Richtung Internet) auf den folgenden von SMB verwendeten Ports: 137-139, 445. Weitere Informationen zur sicheren Konfiguration von SMB finden Sie in den Richtlinien von Microsoft für die Sperrung bestimmter Firewall-Ports, um zu verhindern, dass SMB-Datenverkehr die Unternehmensumgebung verlässt.
  Und sollten Sie nicht wissen wie es funktioniert, so finden Sie hier die entsprechende Richtlinie:
  https://support.microsoft.com/de-de/help/ 3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic

In diesem Zusammenhang wird empfohlen, sich zumindest die nachfolgenden Warnmeldungen der Cybersecurity and Infrastructure Agency (CISA) der US-Regierung zu vergegenwärtigen:
- **Alert TA18-071A**
  Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors
  Quelle: https://www.us-cert.gov/ncas/alerts/TA18-074A
- **Alert AA19-122A**
  New Exploits for Unsecure SAP Systems
  Quelle: https://www.us-cert.gov/ncas/alerts/AA19-122A
- **Alert AA19-168A**
  Microsoft Operating Systems BlueKeep Vulnerability
  Quelle: https://www.us-cert.gov/ncas/alerts/AA19-168A

In Hinblick auf die Vorgehensweise von Berserk Bear sei darauf verwiesen, dass man sich dort mittlerweile einer sehr wichtigen Thematik bewusst zu sein scheint, welche für das zuverlässige Funktionieren technischer Infrastrukturnetzwerke von großer Relevanz ist, der Auswirkung von kaskadierenden Ausfällen.

Kaskadierende Ausfälle, d.h. Kettenreaktionen von Ausfällen verschiedener Infrastrukturen, sind Ursache vieler Ausfälle ganzer Netzwerke wie z.B. großen Teilen der europäischen Stromverbundnetze. Obwohl kaskadierende Ausfälle meist durch netzwerkweite nichtlineare Dynamik zwischen den einzelnen Ausfällen beeinflusst werden, konzentrierte sich deren Modellierung bisher vor allem auf die Analyse von Sequenzen von Ausfallereignissen einzelner Infrastrukturen – die Dynamik zwischen diesen Ereignissen blieb bis zu der im Mai 2018 veröffentlichten Forschungsarbeit der TU Dresden aber weitestgehend unberücksichtigt.

Die an der Grundlagenforschung beteiligten Wissenschaftler untersuchten die Fehlerkaskaden mittels einer Kombination aus Computer-Simulationen und mathematischen Analysen einfacher Netzmodelle. Im Rahmen eines simulierten Netzes, bei dem gezielt Verbindungen unterbrochen werden, wurde der statische Ansatz mit dem neuen dynamischen Ansatz verglichen. Oft zeigt die umfassendere dynamische Sichtweise, dass das Netz komplett instabil werden kann, auch wenn der statische Ansatz noch Stabilität vorhersagt.

Im Rahmen des dynamischen Ansatzes wurde dabei auch untersucht, welches die kritischen Leitungen sind, deren Ausfall im Rahmen einer Kaskadierung zu einem europaweiten Blackout führen kann.

Quelle: https://tu-dresden.de/tu-dresden/newsportal/news/ausfaelle-in-stromnetzen-dyna- misch-induzierte-kaskaden?set_language =de

IoT Security Standards Gap Analysis der ENISA

Als besonders hilfreich zur entsprechenden Cybersecurity Analyse, hat sich auch das vorstehend benannte Dokument der Version 1.0 (ausgegeben: Dezember 2018) der ENISA herausgestellt.

Quelle: https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

Hiernach sollten auch die nachstehenden Normierungen für die Cybersecurity berücksichtigt werden:

- ITU Y 4806
- ISO/IEC 15408-1, -2 und -3
- ISO 29550
- ISO/IEC 27005
- ISO/IEC 27002
- ISO/IEC 29134
- ETSI TS 103 305
- ISO 55000
- ETSI TS 103 645
- ETSI TS 103 533
- ISO 11770
- ISO 29147
- ISO/EC 11889
- ISO/IEC 29192-5
- ITU X.1362
- ISO 29100
- ISO/IEC 19790
- ITU-T Y.4415
- ISO 27034
- ISO 27033
- ISO 27040
- ISO 27017

Es stellt sich in diesem Zusammenhang aber auch die Frage, welche Unternehmen/Organisation sich überhaupt derart große Teams an Cybersecurity- und IT-Security-Experten leisten können, welche überhaupt einen hinreichenden Überblick über die Thematik haben können.

Arbeitet man hier mit der Systematik der Schwellenwerte, unterhalb derer sich nicht mit dieser Thematik zu beschäftigen ist, so wird schnell ersichtlich, dass sich Unternehmen unterhalb dieser Schwellenwerte aus organisatorischen Gründen überhaupt nicht mit diesen Herausforderungen beschäftigen können und somit schnell Opfer von Cyberattacken werden können.

Somit muss an dieser Stelle natürlich auch die Frage erlaubt sein, ob die Implementierung der Cybersecurity Standards somit nicht zwangsläufig zu einer Marktkonzentration im Bereich der Kritischen Infrastrukturen führen wird.

Und was kommt jetzt auch noch durch das IT-Sicherheitsgesetz 2.0?

Im Rahmen des IT-Sicherheitsgesetzes 2.0 wird es zu Erweiterungen der Kategorisierung der kritischen Infrastrukturen kommen. Zum einen erfolgt die Schaffung eines Sektors „Entsorgung“, zum anderen die Schaffung eines Sektors „Infrastruktur von besonderem öffentlichen Interesse“, wobei dieser unbestimmte Begriff zumindest auf die Bereiche Rüstung und Infrastrukturen mit kritischer Bedeutung für die Geschäftstätigkeit von Unternehmen des Prime Standard an der Frankfurter Wertpapierbörse anzuwenden sein wird.

Der Einsatz von Systemen der Angriffserkennung wird Pflicht. Die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung legt das BSI in einer Technischen Richtlinie zeitnah fest.

KRITIS-Kernkomponenten dürfen nur von solchen Herstellern bezogen werden, die vor dem erstmaligen Einsatz der Komponenten eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben haben (Vertrauenswürdigkeitserklärung). Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers. Das Bundesministerium des Innern, für Bau und Heimat erlässt die Mindestanforderungen für die Vertrauenswürdigkeitserklärung durch Allgemeinverfügung, die im Bundesanzeiger bekannt zu machen, sein wird.

Im Bereich der Kritis-Sektors Energie fallen hierunter:

IT-Produkte für die Kraftwerksleittechnik, für die Netzleittechnik oder für die Steuerungstechnik zum Betrieb von Anlagen oder Systemen zur Stromversorgung, Gasversorgung, Kraftstoff- oder Heizölversorgung oder Fernwärmeversorgung.

Darüber hinaus müssen Hersteller von KRITIS-Kernkomponenten alle Störungen bzgl. Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Software unverzüglich dem Bundesamt melden, wenn die Anwendung dieser Software zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit von Kritischen Infrastrukturen führen kann.

Umstritten sind die nachfolgenden Punkte:

- Zukünftig wird das BSI im Internet nach unsicheren Geräten suchen, z.B. mit Portscans. Das betrifft nicht nur die klassische IT, sondern auch schlecht abgesicherte Geräte im „Internet der Dinge“ wie Überwachungskameras.

Unstrittig unsicher, aber immer noch häufig zu finden sind Systeme mit veralteter Software, ohne Passwort-Schutz oder mit Standard-Passwörtern wie „0000“ und „admin“. Um herauszufinden, ob ein Gerät unsichere Passwörter nutzt, soll das BSI das Recht erhalten, sich darauf einloggen zu dürfen. Inwieweit dies kein Verstoß gegen das informationelle Recht der Selbstbestimmung sein wird, werden sicherlich zeitnah die höchsten Gerichte in Deutschland feststellen dürfen.

Für den Fall, dass das BSI Sicherheitsprobleme oder Angriffe erkennt, soll es Betroffene benachrichtigen dürfen. Um dies zu realisieren, sollen Telekommunikationsanbieter der Bundesbehörde zu einer IP-Adresse eigentlich schützenswürdige Daten übermitteln dürfen, d.h. mitteilen, auf wen ein Internet-Anschluss registriert ist.

- Wenn Kritische Infrastrukturen angegriffen werden, soll das BSI Internet-Anbietern anordnen können, das Gerät, von dem der Angriff ausgeht, dergestalt aus dem Verkehr zu ziehen, dass dessen Datenverkehr blockiert oder umgeleitet wird.

In einem nächsten Schritt sollen potenziell schädliche Geräte auch aktiv verändert werden, um sie zu sichern. Was potenziell schädlich ist, muss aber noch dringend eingehend geklärt werden. Das BSI soll Provider in diesem Falle zu folgendem verpflichten dürfen:

- Bereinigung“ von IT-Geräten
- Installation von lückenschließender Software (Patches)
- Löschung von Schadsoftware

Begründet wird dies mit der real existierenden Gefahr der Botnetze. Diese Bots werden bekanntlicher Weise von zentralen Servern gesteuert. Zur Gefahrenabwehr will das BSI den Internet-Verkehr solcher

Kommando-Server auf eigene Server umleiten lassen, um hierdurch die Kontrolle über das Botnetz zu übernehmen. In einem nächsten Schritt sollte dann „Bereinigungssoftware“ an die Bots ausgeliefert werden, um die Schadsoftware zu entfernen. Und aufgrund der Tatsache, dass User oft nicht wissen, dass ihr Gerät mit Schadsoftware befallen ist, will der Staat diese Geräte selbst säubern dürfen.

Der Bußgeldrahmen für Verstöße von IT-Sicherheitspflichten soll substanziell angehoben werden. Für den Fall, dass Unternehmen vollziehbare Anordnungen des BSI zur IT-Sicherheit nicht nachkommen, sieht der Referentenentwurf einen Bußgeldrahmen von bis zu EUR 20.000.000,00 oder 4 % des jährlichen Unternehmensumsatzes vor. Darüber hinaus können andere Verstöße im Höchstmaß immerhin noch mit EUR 10.000.000,00 bzw. 2 % des Unternehmensumsatzes geahndet werden können.

FAZIT

Die Energiewirtschaft in Europa ist in den Fokus der Cyber-Kriminellen geraten und die (noch nicht einmal durch Cyber-Kriminalität verursachten) Störfälle im europäischen Netz nehmen zu. Wir benötigen somit unbedingt zeitnah einen Rahmen zum Handeln, zumal Deutschland sowohl in Hinblick auf die Digitalisierung noch in Hinblick auf Cybersecurity auf einem der Spitzenplätze liegt. Die NIS-Direktive, das deutsche IT-Sicherheitsgesetz 1.0 sowie die Kritis-VO haben letztlich bei einigen Kritis-Sektoren versagt, da es oftmals günstiger ist, Strafen zu zahlen denn Sicherheit zu implementieren und zu zertifizieren. Dies ändert sich alles mit dem Cybersecurity Act, der trotz aller Verbesserungspotentiale zusammen mit der Normenfamilie IEC 62443 als Schritt in die richtige Richtung anzusehen ist.

Um erfolgreich zu bestehen, muss die Energiewirtschaft jetzt zwei wichtige Schritte umsetzen:

- Einsatz von nach IEC 62443 produktzertifizierten OT-Komponenten und wirksame Systemzertifizierungen.
- Durchführung von Schulungen im Bereich Cybersecurity, wobei diese sich nicht auf effekthaschende Red-Blue-War Games beschränken sollten. Hier sollte ein modularer, ganzheitlicher Ansatz gewählt werden, der aus folgenden Komponenten besteht: Social Competence, IT-OT/-Produktschulungen inkl. Zertifizierung, Training im Simulator.

Nur so werden wir die Gefahren meistern!

Referenzen

https://www.vde.com/topics-de/cyber-security

https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018

Nationales Cyber-Abwehrzentrum 08/2018: Gefährdungslage der Stromversorgung in Deutschland durch Cyberangriffe

http://www.europarl.europa.eu/doceo/document/E-8-2019-000428-ASW_DE.htm

https://docstore.entsoe.eu/Documents/SOC%20documents/Incident_Classification_Scale/180214_2016_ICS_Annual_Report.pdf

https://www.netzfrequenzmessung.de/aktuelles.htm#2019_01

https://www.itu.int/en/ITU-D/Cybersecu-rity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

https://www.heise.de/newsticker/meldung/Russischer-Geheimdienst-Massiver-Datenverlust-beim-KGB-Nachfolger-FSB-4476027.html

https://www.itu.int/net4/ITU-D/idi/2017/ index.html

https://www.asien-pazifik-ausschuss de/downloads/press/CC_11-12-2018_APA.pdf

Nationalen Cyber-Abwehrzentrum: Gefährdungslage der Stromversorgung in Deutschland durch Cyberangriffe, 22.08.2018

https://www.tab-beim-bundestag.de /de/pdf/publikationen/buecher/petermann-etal-2011-141.pdf

Deutscher Bundestag, Drucksache 19/1104, Antwort der Bundesregierung

https://www.verfassungsschutz.de/embed/broschuere-2018-06-bfv-cyber-brief-2018-01-neu.pdf

US-CERT-Alert TA18-106A

https://support.microsoft.com/de-de/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic

https://www.us-cert.gov/ncas/ alerts/TA18-074A

https://www.us-cert.gov/ncas/ alerts/AA19-122A

https://www.us-cert.gov/ncas/ alerts/AA19-168A

https://tu-dresden.de/tu-dresden/news portal/news/ausfaelle-in-stromnetzen-dynamisch-induzierte-kaskaden?set_language=de

https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019R0881