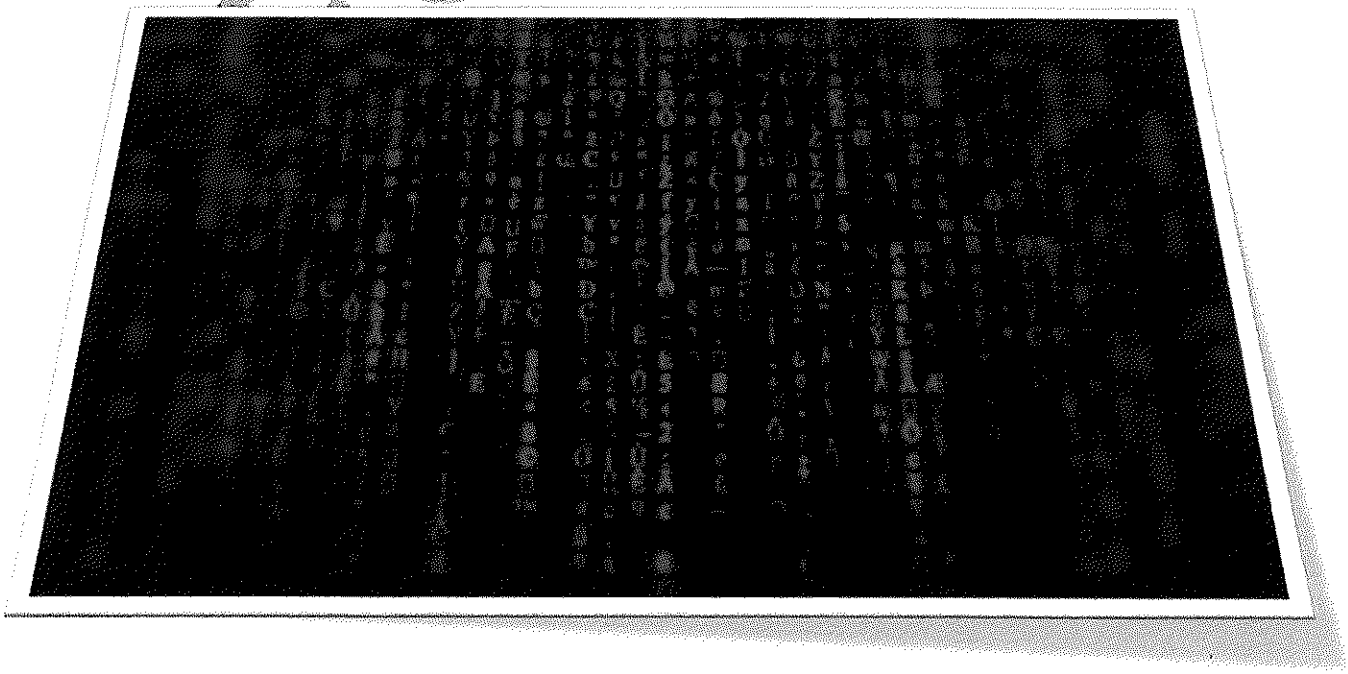
Nationales
Cyber-Abwehrzentrum

Informationen des Nationalen Cyber-Abwehrzentrums

08/2018

Gefährdungslage der Stromversorgung in Deutschland durch Cyberangriffe



Inhaltsverzeichnis

[redacted]

Nationales Cyber-Abwehrzentrum

Beteiligte Behörden:

BBK, BfV, BKA, BND, BSI

Herausgabedatum:

22. August 2018

Herausgeber:

Nationales Cyber-Abwehrzentrum
c/o Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

E-Mail: cyber-az@bsi.bund.de
Tel.: 0228 99 9582 6000

Einleitung

Kritische Infrastrukturen (KRITIS) sind Organisationen und 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[1]. Dies gilt insbesondere für die Branche Elektrizität, die unter den Kritischen Infrastrukturen eine Schlüsselrolle einnimmt – schließlich hängen alle anderen Sektoren von der Stromversorgung ab. Ein Blackout kann somit über Kaskadeneffekte zu weitreichenden KRITIS-Ausfällen führen. Bereits 2010 stellte das Büro für Technikfolgenabschätzung beim Deutschen Bundestag fest, dass ein großflächiger, langanhaltender Stromausfall in Deutschland einer nationalen Katastrophe gleichkäme[2].

Störungen im deutschen Stromnetz könnten auch durch Cyberangriffe hervorgerufen werden. Dabei unterscheidet sich das mögliche Ausmaß je nach Art und Qualität des Angriffs erheblich. Einfache, im elektrotechnischen Umfang begrenzte Störungen lassen sich aufgrund der hohen physischen Redundanz im Netz durch Schaltmaßnahmen relativ schnell wieder beheben. Bei größerem Störungsumfang könnte die Stabilität des deutschen Stromnetzes oder sogar des europäischen Verbundnetzes gefährdet werden und ein großflächigerer Stromausfall eintreten. Die Behebung eines solchen Schwarzfalls nimmt bereits deutlich längere Zeit in Anspruch. Gelingt durch einen Cyberangriff sogar die physische Zerstörung von Komponenten wie Transformatoren oder Hochspannungsschaltanlagen, so können diese unter Umständen erst mittel- oder langfristig ersetzt werden, so dass bei einem solchen Cybersabotageangriff ein langanhaltender Stromausfall mit entsprechenden Konsequenzen herbeigeführt werden könnte.

In den letzten Jahren wurden immer wieder Berichte über Cyberangriffe auf die Stromversorgung westlicher Staaten zur möglichen Sabotagevorbereitung veröffentlicht[3]. Zuletzt beschuldigten die USA russische staatliche Akteure solcher gezielter Angriffe[4] und auch das Vereinigte Königreich hat dies bereits öffentlich als deutliche Gefährdung eingeschätzt[5]. In der Ukraine kam es sogar 2015 und 2016 zu den weltweit ersten bekannten Stromausfällen, die auf Cyberangriffe zurückzuführen waren. Vor diesem Hintergrund stellt sich die grundsätzliche Frage, wie stark die Stromversorgung in Deutschland tatsächlich durch Cyberangriffe gefährdet ist.

Im Folgenden werden daher zunächst die bereits erfolgten Cyberangriffe auf Stromnetzbe-

[1] Bundesministerium des Innern: *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*, 17.06.2009

[2] Petermann et al.: *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung*, Arbeitsbericht Nr. 141, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (2010)

[3] Bspw. Symantec Corporation: *Dragonfly: Western energy sector targeted by sophisticated attack group*, 20.10.2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks (letzter Zugriff: 21.08.2018); CrowdStrike: *2018 Global Threat Report*, 26.02.2018, Cyber-AZ: Cyber-Lage vom 01.08.2017 (VS-NfD); Süddeutsche Zeitung Magazin: *Gegen den Strom.*, 04.05.2018

[4] US-CERT: *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, Alert TA18-074A, 15.03.2018, https://www.us-cert.gov/ncas/alerts/TA18-074A (letzter Zugriff: 20.08.2018)

[5] UK NCSC: *Cyber security: fixing the present so we can worry about the future*, 15.11.2017, https://www.ncsc.gov.uk/news/cyber-security-fixing-present-so-we-can-worry-about-future (letzter Zugriff: 20.08.2018)

[redacted]

treiber sowie Erkenntnisse über bekannte Gruppierungen, die als Angriffsziel die Stromversorgung wählen, dargelegt. Im Anschluss erfolgt eine Bewertung der technischen Angriffsmöglichkeiten auf die Stromversorgung, der relevanten Angreifergruppierungen, ihrer Ziele und Fähigkeiten, sowie des Schutzniveaus deutscher Stromnetzbetreiber, bevor Schlussfolgerungen für die Gefährdung der Stromversorgung in Deutschland durch Cyberangriffe gezogen und Handlungsempfehlungen zur Verbesserung von Schutzmaßnahmen gegeben werden.

Sachverhalt

Stromausfall in der Ukraine am 23.12.2015

Der hier dargestellte Sachverhalt ist die erste, den beteiligten Behörden bekannte, erfolgreiche Cybersabotage eines Stromnetzes.

Der Stromausfall

Am 23. Dezember 2015 nachmittags begannen Störungen im Stromverteilnetz in der Ukraine, die bei mehreren Hunderttausend Einwohnern des westukrainischen Verwaltungsbezirkes Iwano-Frankiwsk zu einer Unterbrechung der Stromversorgung geführt haben. Der Stromausfall dauerte bis zu sechs Stunden.

Ursächlich für die Störungen waren koordinierte Cybersabotageangriffe auf die Steuersysteme von lokalen Verteilnetzbetreibern, die mittlerweile der Angreifergruppe Sandworm (s.u.) zugeschrieben werden. Nach unterschiedlichen Angaben waren bis zu drei Verteilnetzbetreibern [redacted] betroffen, bei denen der Angriff tatsächlich zu einem Ausfall der Stromversorgung geführt hat [redacted] und bis zu sechs weitere angegriffen worden.

Ursache: Der Cyberangriff

Der Angriff auf einen ortsansässigen ukrainischen Energieversorger begann dabei mit einer *Phishing-Mail*, die eine mit Schadcode versehene Exceltabelle enthielt. Mit dem Öffnen der Exceltabelle soll die Schadsoftware auf dem Opfersystem installiert worden sein. Der genaue Zeitpunkt dieser Erstinfektion ist hierbei nicht bestimmt worden, es wird jedoch von sehr ähnlichen Angriffen im Frühjahr 2015 auf andere Betreiber im Energie-Sektor der Ukraine berichtet, so dass sie vermutlich in Teilen bereits im März 2015 erfolgte.

Dann erlangte der Angreifer schrittweise Zugriff auf weitere Systeme im Netz des Energieversorgers, darunter auch Anlagensteuerungssysteme (sog. SCADA-Systeme). Der Angreifer konnte sich über lange Zeit zielgerichtet im Netz bewegen und setzte unterschiedliche Techniken ein, um den Angriff zu verschleiern, dessen Wirkung zu erhöhen und die Beseitigung der Infektion zu erschweren.

Der eigentliche Sabotageangriff erfolgte dann in mehreren Schritten.

Im ersten Schritt wurden die eigentlichen Hochspannungsleistungsschalter einer größeren Anzahl von Umspannwerken bzw. Schaltanlagen geöffnet (Quellen sprechen von 30 bis 50 Anlagen), was unmittelbar zum Ausfall der Stromversorgung bei den Betroffenen geführt hat. Gleichzeitig wurden die Überwachungssysteme der Netzleitstellen "eingefroren" bzw. abgeschaltet, so dass die Störung hier nicht feststellbar war. Die Quellen sind auch hierzu nicht eindeutig.

Im zweiten Schritt wurden koordinierte TDoS-Angriffe (*Telephone Denial of Service*) auf die Callcenter der Verteilnetzbetreiber gestartet. Diese führten zu einer Überlastung der Telefonleitungen, wodurch telefonische Störungs-

meldungen durch Betroffene verhindert wurden.

Im dritten Schritt erfolgte die Erschwerung der Störungsbeseitigung. Hierfür wurde zunächst eine KillDisk-Komponente eingesetzt. Dieses Modul löscht Daten auf Windows-Systemen und macht damit das Betriebssystem unbrauchbar. Eine vollständige Neuinstallation wird erforderlich, um das System wieder in Betrieb zu nehmen. Neben der zwischenzeitlich weit bekannten Sabotage der Steuerungsrechner mittels KillDisk wurde die Störungsbeseitigung zusätzlich noch durch weitere Eingriffe erschwert. Laut US DHS änderten die Angreifer in mehreren Fällen Passwörter für zentrale Systeme und sperrten so legitime Nutzer während der Störungsbeseitigung aus[6]. Auch die Firmware auf Seriell-Ethernet-Konvertern, die die Schnittstelle zwischen Anlagensteuerung und Steuerungssoftware bilden, wurde überschrieben, wodurch diese effektiv zerstört wurden. Zudem wurden die unterbrechungsfreien Stromversorgungen (USV) der Server in den Zentralen der Energieversorger von den Angreifern über die Management-Schnittstellen abgeschaltet. Der Stromausfall betraf dadurch unter anderem auch einen internen Telefonserver sowie das Datencenter und somit die Arbeitsfähigkeit der mit der Störungsbeseitigung beschäftigten Mitarbeiter des betroffenen Energieversorgers[7].

[6] US DHS: IR-ALERT-H-16-043-01AP *Cyber-Attack Against Ukrainian Critical Infrastructure*, Update A, 07.03.2016, https://www.eenews.net/assets/2016/07/19/document_ew_02.pdf (letzter Zugriff: 20.08.2018)

[7] SANS ICS & E-ISAC: *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Defense Use Case, 18.03.2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (letzter Zugriff: 20.08.2018)

Aufgrund der Sabotage der im Regelbetrieb für die Fernsteuerung der Umspannwerke genutzten Leittechnik mussten die Schaltvorgänge in den Umspannwerken lokal manuell ausgelöst werden. Dadurch wurde die Wiederherstellung der Stromversorgung deutlich verzögert.

Bewertung

Anders als in vielen Presseberichten behauptet, kann kein direkter Zusammenhang zwischen der eingesetzten Schadsoftware und der Unterbrechung der Stromversorgung abgeleitet werden. Die Schadsoftware hat also nicht autark und automatisiert die Stromversorgung unterbrochen, sondern erlaubte lediglich manuellen Zugriff auf die Steuerungssysteme durch die Angreifer. Ob alle Systemausfälle am 23.12.2015 tatsächlich allein auf Cyberangriffe zurückzuführen sind, ist nicht belegbar, Cyberangriffe als Hauptangriffsvektor erscheinen aber sehr wahrscheinlich. Die Beteiligung eines Innentäters ist hiesiger Einschätzung nach allerdings nicht auszuschließen.

Die einzelnen Angriffsbausteine besitzen in sich jeweils keine besondere technische Komplexität. Sie nutzen bereits bekannte Schwachstellen und die – immer noch erfolgreiche – Methode des *Social Engineering*, um eine Infektion zu bewirken. Höher qualifizierte und technisch anspruchsvollere Methoden und Techniken (z.B. *Zero-Day-Exploits*) waren für diesen Angriff nicht erforderlich, die für den Angriff eingesetzten Mittel waren bereits ausreichend. Die Angreifer verfügten allerdings über ausreichende Kenntnisse über die Systeme und Prozesse der Betreiber, um über den geschaffenen Fernzugriff durch gezielte Schalthandlungen großflächige Stromausfälle zu bewirken.

Der tatsächlich angerichtete Schaden an Komponenten beschränkte sich lediglich auf IT-gestützte Kommunikationssysteme im Bereich

der Stations- und Netzleittechnik und nicht auf die eigentlichen stromführenden Anlagen. Reparaturen bzw. Austausch solcher elektrotechnischer Anlagen hätten wohl eher Wochen oder gar Monate benötigt. Aber selbst ohne das Herbeiführen physischer Zerstörungen wären durch systematischere Schalthandlungen wohl großflächigere, länger anhaltende Stromausfälle erreichbar gewesen. Dies legt die mehrfach geäußerte Einschätzung nahe, dass die Angreifer deutlich mehr Schaden hätten anrichten können, als sie verursacht haben[8].

Stromausfall in der Ukraine am 17.12.2016

Der Stromausfall

Am 17.12.2016 gegen Mitternacht Ortszeit kam es in der Ukraine wieder zu einem Stromausfall, der laut Medienberichten einige hunderttausend Einwohner betraf, aber lediglich etwa eine Stunde andauerte. Bei diesem erneuten Cybersabotageangriff wurde die Station Kiew des ukrainischen Übertragungsnetzbetreibers [redacted] angegriffen. Erneut erfolgte die Wiederherstellung manuell[9].

Ursache: Der Cyberangriff

Es wird vermutet, dass die Angreifer wiederum bereits Monate zuvor die Netze des ukrainischen Energieversorgers [redacted] kompromittiert hatten.

Bei dem eigentlichen Cybersabotageangriff am 17.12.2016 soll eine hochentwickelte Schadsoftware namens CrashOverride bzw. Win32/Industroyer[10] eingesetzt worden sein, die gezielt auf die weltweit in der Energieinfrastruktur eingesetzten ICS/SCADA-Komponenten optimiert wurde. Es handelt sich um ein modular aufgebautes Framework, das industrielle Steuerungsprotokolle nutzt und laut dem Virenschutzhersteller ESET in der Lage ist, Leistungsschalter und Schaltanlagen in Umspannwerken direkt zu kontrollieren. Bei der Schadsoftware handelt es sich um einen Windows-Trojaner, so dass die Angreifer das Netzwerk in einem ersten Schritt erkunden, um dann die passenden Module zur Kompromittierung nachzuladen.

Ein hervorzuhebendes Merkmal der Schadsoftware ist ihre Art der Kommunikation: Sie verfügt über spezielle Module, die die Kommunikation zu den gängigsten Protokollen ermöglichen. Das bedeutet, dass Industroyer keine Lücken ausnutzen muss, sondern direkt mit den jeweiligen Industriekomponenten kommunizieren kann. Zudem ist keine direkte Kommunikationsverbindung zu C&C-Servern notwendig. Über im Vorfeld terminierte Aktionen kann die Schadsoftware auch hinter einem sogenannten *Air Gap* agieren, wenn sie erst einmal eingeschleust werden konnte[11].

Ein weiteres Kennzeichen ist die modulare Aufbauweise, die es den Angreifern ermög-

[8] New York Times: *Utilities Cautioned About Potential for a Cyberattack after Ukraine's*, 29.02.2016, http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html (letzter Zugriff: 20.08.2018); Wired: *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, 03.03.2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (letzter Zugriff: 20.08.2018)

[9] Wired: *How an Entire Nation Became a Test Lab for Cyberwar*, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ (letzter Zugriff: 20.08.2018)

[10] Die Firma Dragos Inc. bezeichnet die Schadsoftware als CrashOverride, die Firma ESET hingegen hat den Namen Win32/Industroyer vergeben.

[11] North American Electric Reliability Corporation (NERC): *Modular Malware Targeting Electric Industry Assets in Ukraine*, Industry Advisory, 13.06.2017, https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERCAlert_A-2017-06-13-01_Modular-Electric-Industry-Malware.pdf (letzter Zugriff: 20.08.2018)

licht, die Schadsoftware den jeweiligen Umgebungen und Zielen individuell anzupassen. Dies setzt voraus, dass die Angreifer zuvor detaillierte Erkenntnisse zu den jeweiligen Opfernetzwerken erlangt haben müssen.

Die Schadsoftware verfügt darüber hinaus über ein Modul mit Löschfunktion, das sämtliche Spuren verwischen, Konfigurationsdateien löschen und das Betriebssystem zerstören kann. So ist die destruktive Komponente von Industroyer beispielsweise in der Lage, gezielt nach ABB-Dateien[12] zu suchen und diese zu löschen.

Weiterhin besitzt die Schadsoftware eine Komponente, die DoS-Angriffe gegen SIEMENS SIPROTEC-Geräte ermöglicht. Dabei handelt es sich um Schutzgeräte, die Schäden durch Spannungsspitzen in Stromleitungen und Transformatoren verhindern sollen. Nach einem solchen DoS-Angriff kann das Schutzgerät seine Funktion erst nach einem manuellen Neustart wieder ausüben. In der Zwischenzeit ließen sich durch einen weiteren Angriff potentiell Zustände herbeiführen, die schwerwiegende Schäden an Geräten wie Transformatoren und damit physische Zerstörungen an Komponenten zur Folge hätten, wenn kein Schutzrelais mehr greift[13]. Zur erfolgreichen Durchführung eines solchen Angriffs wären nach Einschätzung des Virenschutzherstellers Dragos Inc. allerdings noch signifikant mehr Ressourcen und Vorbereitung von Seiten Angreifer erforderlich gewesen als in diesem Fall gezeigt, da verschiedene Arten von Schutzrelais im Einsatz sind[14].

Bewertung

Mit dem modularen *Framework* steht erstmals ein Tool zur Verfügung, mit dem Schadsoftware speziell für ICS/SCADA-Umgebungen erstellt werden kann. In Industroyer steckt laut ESET viel Entwicklungsaufwand: Im ICS-Bereich benötigt der Angreifer Kenntnisse über die verwendeten Steuerungsprotokolle, um die Schadsoftware entsprechend zu programmieren.

Die modulare, erweiterbare Architektur, sowie die detaillierten Implementationen von ICS-Protokollen legen den Schluss nah, dass der Angreifer über aufwändige Test-Umgebungen verfügt und das langfristige Ziel verfolgt, in ICS-Netzwerke einzudringen.

Die von den Sicherheitsexperten veröffentlichten Analysen basieren auf *Samples* vom Dezember 2016. Es kann erwartet werden, dass das *Framework* seitdem weiter überarbeitet und verbessert wurde.

Auch bei diesem Stromausfall wurde die Vermutung geäußert, dass es sich um eine Machtdemonstration[15] oder um einen Test der Reaktionen bzw. Training[16] gehandelt habe: Die Angreifer hätten mit der hier gefundenen Schadsoftware wohl zumindest längere Strom-

[12] Dateien, die in diesem Fall dem Hersteller *ABB* zugeordnet werden; *ABB* ist neben *Siemens* ein weiterer Hersteller von ICS-Komponenten.

[13] ESET: Industroyer: *Biggest threat to industrial control systems since Stuxnet*, 12.06.2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (letzter Zugriff: 20.08.2018)

[14] Dragos Inc: *Crashoverride. Analysis of the Threat to Electric Grid Operations*, 12.06.2017, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf (letzter Zugriff: 20.08.2018)

[15] Dragos Inc: *Crashoverride. Analysis of the Threat to Electric Grid Operations*, 12.06.2017, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf (letzter Zugriff: 20.08.2018)

[16] Wired: *How An Entire Nation Became Russia's Test Lab for Cyberwar*, 20.06.2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ (letzter Zugriff: 20.08.2018)

[redacted]

ausfälle provozieren oder über die DoS-Angriffskomponente gegen Schutzgeräte sogar physische Zerstörungen hervorrufen können.[17]

Ein Zusammenhang zu Angriffen der Gruppierung Sandworm (s.u.) konnte in diesem Fall zwar nicht nachgewiesen werden. Dennoch weisen die Vorfälle hinsichtlich Fähigkeiten, Komplexität und Ziel deutliche Parallelen auf. Der zweite Vorfall stellt allerdings eine stark automatisierte Version des ersten Angriffs dar, so dass augenscheinlich eine stetige Weiterentwicklung der Angriffsfähigkeiten zu beobachten ist[18].

Erkenntnisse zu mutmaßlich verantwortlichen Gruppierungen

[redacted]

Cyberangriffskampagne Sandworm

Die seit mindestens 2014 aktive Angriffskampagne Sandworm verfolgt erkennbar auch das Ziel der Cybersabotage. Zu den Zielen der auch u.a. unter den Namen VoodooBear, Electrum, Quedagh und SCADA-Connection bekannten Gruppierung zählen Regierungsstellen, Bildungseinrichtungen, Energieversorger, Telekommunikationsunternehmen sowie die NATO. Auch Angriffe auf den Flughafen Kiew und ukrainische Medienunternehmen werden dieser Angreifergruppe zugeschrieben[19]. [redacted]

Sandworm nutzt die Schadsoftware BlackEnergy. Diese Software liefert ein modulares System, das sich auf die Bedürfnisse des Nutzers anpassen lässt und durch ein sehr einfaches Interface zu bedienen ist. Sie wurde zeitgleich mit dem Angriff auf die Stromversorgung Ende 2015 auch auf den IT-Systemen des ukrainischen Energieversorgers [redacted] entdeckt.

Kurzer Exkurs zu BlackEnergy:

BlackEnergy wird in verschiedenen Entwicklungs- und Ausbaustufen seit Jahren durch unterschiedliche Gruppen verwendet, die hiermit Angriffe auf verschiedene Ziele in West- und Osteuropa, aber auch in der NATO und den USA durchführen.

In früheren Versionen – die Softwarefamilie gibt es bereits seit über zehn Jahren – handelte es sich laut iSIGHTPartners bei BlackEnergy primär um einen kriminell genutzten DDoS-Trojaner, zu dem später noch Finanzdatendiebstahl als Zielsetzung hinzukam[20]. Erst 2014 wurde BlackEnergy dann im Rahmen von

[17] Dragos Inc: *Crashoverride. Analysis of the Threat to Electric Grid Operations*, 12.06.2017, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf (letzter Zugriff: 20.08.2018)

[18] North American Electric Reliability Corporation (NERC): *Modular Malware Targeting Electric Industry Assets in Ukraine*, Industry Advisory, 13.06.2017, https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERCAlert_A-2017-06-13-01_Modular-Electric-Industry-Malware.pdf (letzter Zugriff: 20.08.2018)

[19] Cys-Centrum: *Киберугроза BlackEnergy2/3. История атак на критическую ИТ инфраструктуру Украины* (BlackEnergy2 / 3 cyber threats. History of attacks on critical IT infrastructure of Ukraine), 06.01.2016, https://cys-centrum.com/ru/news/black_energy_2_3 (letzter Zugriff: 20.08.2018)

[20] iSIGHTPartners: *SandWorm. Russian Cyber Espionage Operators Sandworm Team Leverage Zero-Day Vulnerability (CVE-2014-4114)*, 2014

[redacted]

APT-Angriffen verwendet[21] *und eine Gruppe begann, SCADA-bezogene Plugins zu BlackEnergy zu nutzen*[22].

Cyberangriffskampagne Berserk Bear
Die Angriffskampagne Berserk Bear (auch Energetic Bear, Dragonfly, Crouching Yeti, Koala Team, Dymalloy) ist seit mindestens 2011 aktiv. Sie konzentrierte sich in der Anfangsphase auf Verteidigungs- und Luftfahrtunternehmen in den USA und Kanada. 2013 wechselte der Fokus jedoch auf den Energiesektor und davon abhängige Branchen.

Aktuell liegen Erkenntnisse vor, die sich auch gegen deutsche Unternehmen aus dem Energiesektor richten. Im aktuellen Zielspektrum der Angreifer liegen vorwiegend KRITIS-Unternehmen (z.B. Energieversorgung, aber auch Wasserver- und -entsorgung sowie IKT). Dabei richteten sich die Angriffe der letzten Monate insbesondere gegen Infrastrukturkomponenten (z.B. Router).

Die Angreifer verwenden vielfach öffentlich zugängliche Angriffswerkzeuge und versuchen unzureichend gesicherte Systeme unter ihre Kontrolle zu bringen.[23]

Berserk Bear operiert auch mit *Spear-Phishing Mails* und *Watering-Hole*-Angriffen. Die Kampagne kompromittierte dabei laut dem IT-Sicherheitsunternehmen Symantec z.B. Webseiten mit Bezug zum Energiesektor. Ruft ein Opfer eine dieser präparierten Seiten auf, wird das Opfersystem auf Schwachstellen geprüft und anschließend mit Schadcode infiziert.[24]

Bewertung

[redacted]

[21] F-Secure: *Blackenergy & Quedagh. The convergence of crimeware and APT attacks*, 2014
[22] Kaspersky Lab: *BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents*, 28.01.2016, https://securelist.com/ blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/ (letzter Zugriff: 20.08.2018)
[23] Am 16. April 2018 haben das Department of Homeland Security (DHS), das Federal Bureau of Investigation (FBI) und das National Cyber Security Centre (NCSC) gemeinsam eine Erklärung (US-CERT-Alert TA18-106A) veröffentlicht, die dieselbe APT betrifft.
[24] Für weitere Details s. BfV Cyber-Brief, Nr. 01/2018, *Hinweis auf aktuelle Angriffskampagne*, 13.06.2018, https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2018-06-bfv-cyber-brief-2018-01 (letzter Zugriff: 20.08.2018)

[redacted]

Beobachtete Angreiferfähigkeiten

Spätestens mit Bekanntwerden des Stuxnet-Virus im Jahr 2010 wurde der breiten Öffentlichkeit die Gefährdung sicherheitskritischer IT-Systeme durch Cybersabotageangriffe eindringlich vor Augen geführt. Bei Stuxnet hatte

es sich um einen sehr hochwertigen erfolgreichen Cybersabotageangriff auf das iranische Atomprogramm gehandelt. Eine direkte deutsche Betroffenheit durch schädliche Auswirkungen von Stuxnet war zwar nicht zu erkennen, der Vorfall hatte aber deutlich gemacht, dass auch die deutschen (Kritischen) Infrastrukturen durch solche oder artgleiche Cybersabotageangriffe potentiell als gefährdet anzusehen sind. Das ist einerseits damit zu begründen, dass die bei Cyberangriffen verwendeten, insbesondere zur Informationsabschöpfung / Spionage dienenden Schadprogramme – je nach Platzierung / Nähe zu den für die betrieblichen Prozesse der Stromversorgung relevanten IKT-Systemen (Netzleittechnik, OT, ...) – durch Programmänderungen auch für Sabotagezwecke eingesetzt werden können. Hat ein Angreifer zudem erst einmal vollen Zugriff auf ein IT-System erlangt, kann er dort ungehindert weitere Aktionen durchführen, darunter auch solche gegen dessen Integrität und Verfügbarkeit.

Andererseits können selbst solche zur Informationsabschöpfung/ Spionage dienenden Schadprogramme ausgenutzt werden, die sich mangels Nähe zu den eigentlichen, für die betrieblichen Prozesse der Stromversorgung relevanten IKT-Systemen nicht direkt in wirkungsvolle Sabotagewerkzeuge umwandeln lassen: Sie können dennoch eine komfortable Ausgangsbasis für die Kompromittierung relevanter IKT-Systeme bieten, wobei die zuvor über sie gewonnenen Informationen dem Angreifer ggf. weiter den Weg ebnen.

Für die Energieversorgung allgemein und insbesondere die Stromversorgung von besonderer Bedeutung ist die nach dem Angriff auf die Stromversorgung in der Ukraine vom Dezember 2016 im betroffenen Umspannwerk gefundene Schadsoftware CrashOverride. Diese ist strukturiert, modular erweiterbar aufgebaut und greift unmittelbar in die Kommunikationsprotokolle IEC 60870-5-101 und -104 sowie IEC 61850 ein, die ganz spezifisch in der Netz- und Stationsleittechnik eingesetzt werden, und kann über diese Protokolle technische Komponenten insbesondere in Umspannwerken und Schaltanlagen selbst und unmittelbar steuern bzw. schalten. CrashOverride eignet sich in der gefundenen Form ausschließlich für Angriffe auf IKT-gestützte Systeme, die spezielle Kommunikationsprotokolle nutzen, wie sie insbesondere in der Energieversorgung verwendet werden – kurz, für Angriffe auf sogenannte OT in der Energieversorgung.

Damit ist hier nachgewiesenermaßen eine Stufe der Expertise und des Ressourceneinsatzes von Angreifern und eine Qualität ihrer Angriffswerkzeuge speziell für spezifische IKT-gestützte Technologien der Stromversorgung erreicht, die analog zur Schadsoftware Stuxnet für SCADA-/ICS- und Prozesssteuerungstechnologien allgemein ist. Der Einsatz von hochmodularer Schadsoftware mit erweiterbarer Architektur sowie die detaillierten Implementationen von ICS-Protokollen legen zudem den Schluss nahe, dass die Urheber über aufwändige Test-Umgebungen verfügen und das langfristige Ziel verfolgen, in ICS-Netzwerke einzudringen. Die Komplexität der Angriffe und der hierzu erforderliche Ressourceneinsatz sprechen dafür, dass hinter den Angriffen staatlich gesteuerte Akteure gestanden haben.

Festzuhalten ist zudem, dass die Angreifer bei dem Stromausfall in der Ukraine am 17.12.2016 mittels der festgestellten Software wohl auch längere Stromausfälle hätten provozieren – oder sogar über die DoS-Angriffskomponente gegen Schutzgeräte physische Zerstörungen hervorrufen können. Es kann nur spekuliert werden, ob hierin eine Machtdemonstration zu sehen und/oder ob bei ggf. zukünftigen Angriffen mit einer Weiterentwicklung des

[redacted]

Angriffsmodus und einem noch umfangreicheren Schadensausmaß zu rechnen ist.

Beobachtete Zielsetzung

Unmittelbare Deutschlandbezüge ergaben sich bei dem ersten ukrainischen Stromausfall durch einen Cyberangriff im Dezember 2015 nicht. [redacted] Dennoch zeigen diese Fälle, dass es dem Angreifer mit seinem Eindringen in das Netz des Energieversorgers vordergründig nicht um das Abgreifen von Informationen (also Spionage) ging, sondern vielmehr um das gezielte Ausschalten von Versorgungsinfrastruktur. Damit hat sich bereits mit dem ersten Angriff auf die ukrainische Stromversorgung ein Fall von schwerwiegender Cybersabotage auf einen Betreiber Kritischer Infrastrukturen - von dem grundsätzlich auch vergleichbare Einrichtungen in Deutschland betroffen werden könnten - verwirklicht.

Die im zweiten Cybersabotageangriff auf die ukrainische Stromversorgung eingesetzte Schadsoftware CrashOverride zielt technisch insbesondere auch auf diejenigen Kommunikationsprotokolle ab, die auch von Energieunternehmen in Europa insbesondere im Bereich der Strom- und Gasversorgung eingesetzt werden. [redacted]

Umgesetzte bzw. geplante Schutzkonzepte/ -maßnahmen der Stromnetzbetreiber

Betreiber von Strom- und Gasversorgungsnetzen müssen zur Absicherung der IKT-Systeme, die für den sicheren Netzbetrieb notwendig sind, den Sicherheitskatalog der BNetzA dauerhaft umsetzen[25] und dies der BNetzA durch ein spezifisches Zertifikat nachweisen – erstmalig zum 31.01.2018. Die auf dieser Grundlage von Betreibern ggf. zusätzlich getroffenen Maßnahmen wirken auch den hier geschilderten Bedrohungen entgegen.

Betreiber von Energieanlagen (Strom/Gas), die unter die BSI-KritisV fallen, werden künftig ebenfalls einen Sicherheitskatalog der BNetzA umsetzen müssen[26], den die BNetzA derzeit im Benehmen mit dem BSI erstellt. Betreiber von Anlagen oder Systemen zur Bündelung/ Steuerung elektrischer Leistung (insb. Direktvermarkter, virtuelle Kraftwerke), die unter die BSI-KritisV fallen, müssen angemessene Maßnahmen zum Schutz ihrer IKT-Systeme treffen, die für die Funktionsfähigkeit ihrer Anlagen maßgeblich sind[27], und dies gegenüber dem BSI geeignet nachweisen[28], erstmalig spätestens zum 03.05.2018.

Darüber hinaus wurden durch das IT-SiG Meldepflichten für alle Betreiber von Strom- und Gasversorgungsnetzen sowie Betreiber von solchen Energieanlagen, die unter die BSI-KrititsV fallen, sowie für Betreiber von Anlagen oder Systemen zur Bündelung/Steuerung elektrischer Leistung (insb. Direktvermarkter und virtuelle Kraftwerke) eingeführt.[29] Das BSI informiert alle o.g. Betreiber Kritischer

[25] § 11 Abs. 1a EnWG
[26] § 11 Abs. 1b EnWG
[27] § 8a Abs. 1 BSIG
[28] § 8a Abs. 3 BSIG
[29] § 11 Abs. 1c EnWG und § 8b Abs. 4 BSIG

[redacted]

Infrastrukturen über für sie relevante Informationen zur allgemeinen IT-Sicherheitslage, zu konkreten informationstechnischen Schwachstellen und über IKT-gestützte Angriffe[30], so dass sie anlassbezogen weitere Anpassungen ihrer Schutzkonzepte oder konkreten Abwehrmaßnahmen vornehmen können.

Für Betreiber von Energieanlagen oder Anlagen oder Systemen zur Bündelung/Steuerung elektrischer Leistung, die aufgrund der Unterschreitung von Schwellenwerten nicht unter die BSI-KritisV fallen, gelten diese gesetzlichen Regelungen so jedoch nicht. Diese Betreiber können durch Beitritt zum UP KRITIS ebenfalls an das Melde- und Informationswesen des BSI angeschlossen werden und erhalten dann ebenfalls aktuelle Informationen zur IT-Sicherheitslage, aktuelle Schwachstellen sowie aktuelle Cyber-Angriffe. Sie werden zudem vom BSI auf Anfrage bzgl. der Absicherung ihrer IT beraten. Sie sind allerdings – außer im Rahmen der allgemeinen Sorgfaltspflicht und daraus bei Vorfällen unter Umständen resultierender Haftungsfragen sowie gegebenenfalls vertraglich aufgrund gängiger Industrienormen – nicht im Voraus zur Umsetzung von angemessenen Maßnahmen nach dem Stand der Technik verpflichtet.

Nach einer Abfrage im Rahmen des UP KRITIS halten die Experten die bestehenden Maßnahmen, wie beispielsweise die Trennung von Leitsystem und Bürokommunikation durch ein Zonenmodell, für ausreichend. Trotz der hohen flächendeckend eingeführten Basisschutzmaßnahmen, der sensibilisierten Mitarbeiter und der Segmentierung halten sie ein Szenario wie in der Ukraine im Dezember 2015 in Deutschland nicht für völlig ausgeschlossen. Allerdings sehen sie den nötigen Aufwand und das benötigte Insiderwissen, um solch ein Szenario zu erreichen, als deutlich höher an.

[redacted]

Schlussfolgerungen für die Bedrohungslage der Energieversorgung in Deutschland

Sabotageaktionen gegen kritische Energieinfrastrukturen in Deutschland sind bislang nicht bekannt geworden. Bei den Angriffen auf die Stromversorgung in der Ukraine 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 Gesamtschau verdichten sich Hinweise, dass eine oder mehrere Tätergruppen langfristige Anstrengungen unternehmen, um Energie-Infrastrukturen in den USA und Europa aufzuklären. Dafür sprechen die aktuel-

[30] § 8a Abs. 2 BSIG

[redacted]

le Angriffskampagne „Berserk Bear", die sich gegen deutsche und internationale Unternehmen, insbesondere aus dem Energiesektor richtet, Meldungen über *Spear-Phishing*-Angriffe auf Energie-Unternehmen von Mitte Juli 2017 sowie eine Reihe anderer Sachverhalten 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 Sabotage-Fähigkeiten und -Absichten zeigen.

Bei diesen Aufklärungsaktivitäten stehen auch deutsche Unternehmen im Fokus der Angreifer.

[redacted]

Kritische Infrastrukturen in Deutschland sind Gegenstand umfangreicher Schutzmaßnahmen (siehe Unterkapitel „Umgesetzte Schutzkonzepte /-maßnahmen der Stromnetzbetreiber). Auch Experten aus der Energiewirtschaft, die im Rahmen des UP KRITIS befragt wurden, schätzen Risiken durch Monokulturen (z.B. 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.

[redacted]

Grundlegende Veränderungen durch gravierende (außen-)politische Entwicklungen oder wirtschaftliche Veränderungen und eine tatsächliche oder unterstellte mögliche Verwicklung Deutschlands in internationale Konflikte mit ernstzunehmenden 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.

Zusammenfassend liegen aktuell keine Erkenntnisse vor, die für eine konkrete/ unmittelbare Gefährdung deutscher Unternehmen aus dem Energiesektor durch Cybersabotageangriffe mit dem Ziel der Herbeiführung eines Stromausfalls sprechen.

Ausblick: Konsequenzen/Schlussfolgerungen für andere KRITIS-Sektoren

Die Angreifergruppierung Sandworm zielt neben Energieunternehmen auch auf andere Sektoren Kritischer Infrastrukturen ab, z.B. Transport- oder Telekommunikationsunternehmen. Die Cybersabotage-Beispiele aus der

Ukraine zeigen, dass auch hier Angriffe auf andere Sektoren erfolgten.

Aufgrund des modularen Aufbaus der Schadsoftware CrashOverride ist prinzipiell eine Erweiterung des *Frameworks* um andere Protokolle möglich, sodass sowohl *Payloads* für weitere Industrieprotokolle als auch weitere Schadfunktionen implementiert werden können. Dadurch ist der Einsatz der Schadsoftware auch in anderen Sektoren denkbar. Analysen der IT-Sicherheitsexperten deuten zudem an, dass die hinter der Entwicklung von CrashOverride steckenden Hacker tatsächlich auch Module für weitere Steuerungsanlagen entwickelt haben dürften. Es muss folglich davon ausgegangen werden, dass zukünftig nicht nur der Energiesektor von Angriffen dieser Art bedroht ist.

Im aktuell beobachteten Aufklärungsinteresse stehen zudem auch andere Sektoren, z.B. Wasserver- und -entsorgung sowie Informationstechnik und Telekommunikation. Gerade erstere verwendet in Teilen die gleiche bzw. ähnliche Technik wie die Stromversorgung, so dass hier eine Anpassung von Angriffswerkzeugen ggf. leichter möglich ist.

Andere Vorfälle zeigen, dass Angriffe, die möglicherweise physische Zerstörungen mit sich bringen könnten, auch in anderen Branchen bereits durchgeführt werden. Im Fall von TRITON/TRISIS sollen Angreifer versucht haben, ein Sicherheitssystem (*Safety Instrumented System)* einer Industriesteueranlage im Nahen Osten so zu manipulieren, dass es im Fall einer technischen Störung eine Beschädigung der Anlage nicht mehr hätte verhindern können[31].

[31] Dragos Inc.: *TRISIS Malware. Analysis of Safety System Targeted Malware,* 13.12.2017, https://dragos.com/blog/trisis/TRISIS-01.pdf (letzter Zugriff: 20.08.2018); Fireeye: *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure,* 14.12.2017, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (letzter Zugriff: 20.08.2018)

Handlungsempfehlungen

Angesichts der zunehmend professionell durchgeführten Cyberangriffe in der Ukraine und der feststellbaren Ausspähungsaktivitäten auch gegen deutsche Unternehmen erscheint eine stetige Analyse der Angreiferfähigkeiten und Verbesserung der Schutzmaßnahmen angebracht.

Die betroffenen Infrastrukturen liegen zumeist in privatwirtschaftlicher Hand, so dass eine Umsetzung entsprechender Schutzmaßnahmen durch die Wirtschaft erfolgen muss. Dem Staat obliegt lediglich die Möglichkeit – insbesondere vor dem Hintergrund der Daseinsvorsorge – regulatorisch nachzusteuern, wenn der allgemeine Stand umgesetzter Schutzmaßnahmen unzulänglich erscheinen sollte.

Die zuständigen staatlichen Stellen sollten dabei zunächst einen ständigen, zeitnahen Informationsaustausch über neue Erkenntnisse mit den Betreibern aufrecht erhalten sowie konsequent vertrauensbildende Maßnahmen verfolgen, um gerade bei Vorfällen bei Betreibern, die hierzu nicht verpflichtet sind, eine höhere Quote freiwilliger Meldungen zu erreichen.

Eine konsequente Sensibilisierung der Betreiber, die nicht unter gesetzliche Verpflichtungen wie § 11 Abs. 1b EnWG oder § 8a Abs. 1 BSIG fallen, einschließlich der Werbung für die Umsetzung bestehender Maßnahmenkataloge wie bspw. branchenspezifischer Sicherheitsstandards nach §8a Abs. 2 BSIG oder des

IT-Grundschutz-Kompendiums des BSI, bietet sich ebenfalls weiter an.

Vielfach sind die Betreiber der Infrastrukturen allerdings auf die Sicherheit und Qualität des Designs der von Dritten gekauften ICS/ SCADA-Komponenten sowie ein adäquates Schwachstellen- und Patch-Management durch Lieferanten, Hersteller und Dienstleister angewiesen. Der UP KRITIS hat Best-Practice-Empfehlungen für entsprechende Anforderungen an Dritte veröffentlicht[32], die in den relevanten Verträgen der Betreiber verankert werden sollten. Beim Kauf von sogenannten *Off-the-shelf*-Produkten können diese allerdings kaum zur Anwendung kommen. Auch in der relevanten, bestehenden Gesetzgebung wie dem IT-SiG, beziehungsweise dem EnWG, sind derzeit keine Anforderungen an Lieferanten für KRITIS-Betreiber festgeschrieben. Hier bietet sich eine Überprüfung der Standards der Hersteller und gegebenenfalls eine legislative Anpassung an[33].

Neben der betreiberseitigen Verbesserung von Schutzmaßnahmen zur Reduzierung der Vulnerabilität besteht insbesondere bezüglich der Veröffentlichung von Infrastrukturdaten allerdings auch staatlicher Regelungsbedarf: Um Angriffsziele zu identifizieren, über die ein größeres Schadensausmaß erreicht werden könnte, werden grundlegende Daten zu den relevanten Infrastrukturen benötigt. Dem stehen teilweise Transparenzpflichten wie die INSPIRE-Richtlinie der Europäischen Union, gesetzlich geregelte Auskunftsersuchen wie Anfragen nach dem DigiNetzG oder dem IFG oder andere öffentliche Datensammlungen (z.B. OpenStreetMap) gegenüber. Eine Prüfung von Ausnahmeregelungen oder speziellen Sicherheitsanforderungen für besonders sensible Daten von KRITIS-Betreibern erscheint angebracht.

Selbst bei optimal umgesetzten Schutzmaßnahmen bleibt ein Restrisiko, dass ein Cybersabotageangriff auf die Stromversorgung doch seine Wirkung entfalten könnte. Für diesen Fall sollte der Dialog mit den Betreibern gesucht werden, um auf im Vorfeld ausführlich ausgearbeitete Pläne zum Wiederanfahren der Stromversorgung auch nach Kompromittierung der IT-Systeme hinzuwirken. Das Vorhalten solcher Pläne ist momentan keine Anforderung an die Betreiber nach EnWG oder IT-SiG. Auch gemeinsamen Krisenübungen von Staat und Betreibern kommt in diesem Kontext eine hohe Bedeutung zu, um das gegenseitige Verständnis für die jeweiligen Strukturen und Vorgehensweisen zu erhöhen und die Abläufe einer Krisenbewältigung einschließlich der gegenseitigen Information zu optimieren.

Die Möglichkeit, dass ein Stromausfall auch durch einen Cybersabotageangriff herbeigeführt werden könnte, verdeutlicht schließlich einmal mehr den hohen Stellenwert, der den Maßnahmen zur Abmilderung der Konsequenzen eines solchen Ereignisses beigemessen werden sollte. Dies betrifft einerseits die Vorbereitung von geeigneten Strukturen, um eine

[32] UP KRITIS: *Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen*, Juni 2017, https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Anforderungen_an_Lieferanten.pdf?__blob=publicationFile (letzter Zugriff: 20.08.2018)

[33] Im aktuellen Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode ist bereits die Absicht hinterlegt, die Verbreitung sicherer Produkte unter anderem über Einführung eines Gütesiegels für IT-Sicherheit sowie über klare Regelungen zur Produkthaftung zu fördern (Zeilen 1986ff.).

solche Krise abzuarbeiten[34], aber andererseits auch die Umsetzung geeigneter vorbereitender Maßnahmen, bspw. zur Notstromversorgung kritischer Bereiche[35] oder zur Sicherstellung einer ausreichenden Treibstoffversorgung für die Krisenbewältigung[36].

[34] Siehe auch BMI: *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement,* Leitfaden für Unternehmen und Behörden (2. Auflage), 2011, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf?__blob=publicationFile (letzter Zugriff: 20.08.2018)

[35] Siehe auch BBK: *Notstromversorgung in Unternehmen und Behörden,* Praxis im Bevölkerungsschutz Band 13, 2015, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_13_Notstromversorgung.pdf?__blob=publicationFile (letzter Zugriff: 20.08.2018)

[36] Siehe auch BBK: *Treibstoffversorgung bei Stromausfall. Empfehlung für Zivil- und Katastrophenschutzbehörden,* Praxis im Bevölkerungsschutz Band 18, 2017, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_18_Praxis_BS_Treibstoffversorgung.pdf?__blob=publicationFile (letzter Zugriff: 20.08.2018)

Anhang

Glossar

Air Gap	Als *Air Gap* wird in der Informatik ein Prozess bezeichnet, der zwei IT-Systeme voneinander physisch und logisch trennt, aber dennoch die Übertragung von Nutzdaten zulässt. Er wird eingesetzt, um zwei oder mehr unterschiedlich vertrauenswürdige Rechner oder Rechnernetze voneinander zu isolieren, die jedoch Daten des jeweils anderen Systems verarbeiten müssen.
APT	Als APT (*Advanced Persistent Threat*) bezeichnet man eine auf Dauer angelegte, systematische Operation die mit höchst entwickelten Methoden und Techniken, meist durch einen staatlichen Akteur gestützt, durchgeführt wird um langfristig Informationen abzuschöpfen. Die deutschen Cyber-Abwehrbehörden benutzen hierfür auch den Begriff des „Fallkomplexes".
BNetzA	Bundesnetzagentur
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG
C&C-Server	Als *Command & Control-Server* (C&C) wird ein Rechnersystem bezeichnet, welches Befehle und weitere Schadsoftware an bereits kompromittierte Opfersysteme verteilt. Die Kommunikation mit den Opfersystemen erfolgt meist in kryptierter oder verschleierter Form. Die Weiterentwicklung von C&C-Servern führt zunehmend zu *Peer-to-Peer*-Topologien, bei denen jedes Opfersystem als C&C-Server fungieren kann.
DigiNetzG	Gesetz zur Erleichterung des Ausbaus digitaler Hochgeschwindigkeitsnetze
DDoS-Angriff	(*Distributed-Denial-of-Service*) Ein DDoS-Angriff ist ein Angriff gegen die Verfügbarkeit von IT-Systemen. Dabei werden aus vielen, dislozierten Systemen Verkehre produziert mit dem Ziel, die Kommunikationsfähigkeit eines Opfersystems zu lähmen (Entzug der nutzbaren Bandbreite).
DoS-Angriff	(*Denial-of-Service)* Dieser Oberbegriff bezeichnet Angriffe, deren Ziel die Verhinderung der vorgesehenen Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte (meist durch gezielte Überlastung) darstellt.
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz)
Framework	Ein *Framework* ist ein Programmiergerüst, das in der Softwaretechnik, insbesondere im Rahmen der objektorientierten Softwareentwicklung sowie bei komponentenbasierten Entwicklungsansätzen, verwendet wird. Es ist selbst noch kein fertiges Programm, sondern stellt den Rahmen zur Verfügung, innerhalb dessen der Programmierer eine Anwendung erstellt.
ICS	(*Industrial Control System*) ICS sind in der Industrie eingesetzte

	Steuersysteme, wie z.B. SCADA (*Supervisory control and data acquisition*), DCS (*Distributed control system*), oder Steuersystemkonfigurationen (z.B. PLC - *programmable logic controllers*). Diese werden u.a. auch bei Kritischen Infrastrukturen (z.B. Kraftwerkssteuerungen) eingesetzt.
IDS *High-Leit*	Software für SCADA-Systeme zur hybriden Verarbeitung von Prozessdaten, die als Netzleitsystem für Anwendungen in der Netzleittechnik der Energie- und Wasserversorgung, im Abwasser- und Umweltbereich sowie für industrielle Aufgabenstellungen konzipiert ist.
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz)
INSPIRE-Richtlinie	Richtlinie 2007/2/EG zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
KRITIS	Kritische Infrastrukturen (KRITIS) sind Organisationen und 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.
Off-the-shelf-Produkt	(auch "*Commercial off the Shelf*"-Produkt), bezeichnet seriengefertigte Produkte aus dem Elektronik- oder Softwaresektor (vgl. Standardsoftware), die in großer Stückzahl völlig gleichartig (ugs. „von der Stange“) aufgebaut und verkauft werden.
OT	(*Operational Technology*) Oberbegriff für Hard- und Software, die zur direkten Überwachung, Steuerung oder Regelung von physischen Geräten und Prozesslösungen eingesetzt wird. Hierzu zählen insbesondere industrielle Steuerungssysteme (ICS), Prozessleittechnik sowie Automationslösungen.
Payload	„Nutzlast“ – unmittelbar schädigend wirkende Funktionen einer Schadsoftware
Plugin	Ein *Plugin* ist eine optionale Software-Komponente, die eine bestehende Software erweitert bzw. verändert. *Plugins* werden meist von der entsprechenden Hauptanwendung während der Laufzeit eingebunden. Sie können nicht ohne die Hauptanwendung ausgeführt werden.
SCADA	(*System Control And Data Acquisition*) Systemüberwachung und Datenübernahme aus den Telemetrie- und Steuereinheiten einer Industrieanlage, bspw. eines Kraftwerks.
Smart Meter	Ein intelligenter Zähler (englisch *smart meter*) ist im engeren Sinne ein Stromzähler, der digital Daten empfängt und sendet und dazu in ein Kommunikationsnetz eingebunden ist. Modellabhängig kann er Daten

	auch im schnellen Rhythmus an das Energieversorgungsunternehmen übertragen – er bildet dann neben dem automatischen Last- und Ressourcenmanagement einen Bestandteil von intelligenten Stromnetzen.
Social Engineering	Ausspionieren über das persönliche Umfeld, durch zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung, meist unter Verschleierung der eigenen Identität (Verwenden einer Legende). *Social Engineering* hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.
Spear-Phishing	Bei *Spear-Phishing* Angriffen werden die Opfer im Vorfeld langfristig aufgeklärt, um dann an selbige eine auf ihre Interessen zugeschnittene E-Mail zu versenden. Dabei wird das Opfer verleitet, einen Link zu einer präparierten Website oder einen infizierten Anhang zu öffnen. Im Unterschied zu herkömmlichen *Spam* sind *Spear-Phishing-Mails* hochgradig an das Opfer angepasst und von regulären Mailverkehr kaum zu unterscheiden. Meist sind auch Absenderadressen adäquat gefälscht.
TDoS	Als TDoS (englisch *Telephone Denial of Service*) werden Vorfälle bezeichnet, bei denen es bei einer sehr hohen Anzahl von Anrufen zur Überlastung von Telefonanschlüssen kommt.
UP KRITIS	Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland
VPN	(*Virtual Private Network*) Ein Netzwerk, welches für die Übertragung von Daten auf vorhandene öffentliche Netzwerke, wie beispielsweise das Internet, zurückgreift. Durch kryptologische Verfahren wie Verschlüsselung und digitale Signaturen wird im öffentlichen Netz ein privates, virtuelles Netz aufgebaut.
Watering Hole-Angriffe	Als *Watering Hole*-Angriff wird eine Methode bezeichnet, bei welcher der Angreifer die Opfergruppe hinsichtlich ihrer Vorlieben für bestimmte Webseiten analysiert und dementsprechende Websites mit Schadcode infiziert.
Zero-Day-Exploit	Ein *Zero-Day(-Exploit)* ist eine Sicherheitslücke in einem Software-System, die noch nicht öffentlich bekannt ist und für die es daher auch noch keinen *Patch* gibt.

[redacted]