Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 114 (2023)
Heft: 5

Artikel: Cyber-Resilienz stärken = Renforcer la cyber-résilience
Autor: Röcher, Dror-John
DOI: https://doi.org/10.5169/seals-1053164

dossier.

Cyber-Resilienz stärken

Geopolitische Konflikte | Cyberangriffe auf kritische Infrastrukturen sind heute de facto ein Werkzeug der Geopolitik. Energieversorger müssen dies in ihren Bedrohungsanalysen berücksichtigen – und Lösungen im Verbund finden.

Renforcer la cyber-résilience

Conflits géopolitiques | Les cyberattaques contre les infrastructures critiques sont aujourd'hui de facto un outil de la géopolitique. Les fournisseurs d'énergie doivent en tenir compte dans leurs analyses des menaces – et trouver ensemble des solutions.

Bild / Figure: Evgeniy Maloletka

DROR-JOHN RÖCHER

Der vermutlich bekannteste Cyberangriff auf einen Energieversorger führte zu einer Unterbrechung der Stromversorgung in Teilen der Ukraine im Dezember 2015. Verantwortlich war mutmasslich die Sandworm-Gruppe, die mit dem russischen Militärnachrichtendienst GRU in Verbindung gebracht wird [1]. Darüber hinaus gibt es zahlreiche weitere Beispiele für Angriffe auf kritische Infrastrukturen: Der Beginn des russischen Überfalls auf die Ukraine im Februar 2022 wurde durch Cyberangriffe gegen Terminals des Satellitenkommunikationsbetreibers Viasat begleitet, die zu Kollateralstörungen bei einem deutschen Windparkbetreiber führten. Im Mai 2021 wurde das Abrechnungssystem des U.S.-amerikanischen Pipelinebetreibers Colonial Pipelines Opfer eines Ransomware-Angriffs. In der Folge unterbrach Colonial Pipelines den Betrieb wichtiger Öl- und Gas-Pipelines. Der regionale Energieversorger Enercity aus Hannover wurde im Herbst 2022 zum Ziel eines Angriffs, der zu Beeinträchtigungen des Kundenservice und der Zahlungsabwicklung sowie zum Abfluss personenbezogener Kundendaten führte [2].

Schon vor Jahren haben Militärs und Nachrichtendienste weltweit die Bedeutung des Cyberraums für ihre Aufgaben erfasst. Die Snowden-Leaks 2013 haben das Ausmass staatlich gelenkter offensiver Cyberaktivitäten zum ersten Mal ins Bewusstsein einer breiteren Öffentlichkeit gerückt. Seitdem hat sich die Cyberdomäne als Bestandteil der Geopolitik etabliert, und viele Staaten haben in ihren Armeen eigene offensive Cybereinheiten aufgebaut. So hat die Nato in Tallinn das Cooperative Cyber Defence Centre of Excellence (CCDCOE) aufgebaut, und aus China heraus betreiben sowohl die Armee als auch das Ministerium für Staatssicherheit weltweit Cyberspionage, die sich auch gegen Betreiber kritischer Infrastrukturen richtet [3].

Vielschichtige Bedrohungslage

Der Krieg Russlands gegen die Ukraine hat Europa vor Augen geführt, wie abhängig Europas Wohlstand vom Zugang zu günstiger Energie ist. Der Umbau der Energiewirtschaft ist eine strategische Entscheidung, die auch auf die zunehmenden Unsicherheiten der geopolitischen Situation zurückzuführen ist.

Ein Blick auf die politische Grosswetterlage zeigt, wie sehr sich die Welt im Umbruch befindet. China agiert konsequent entlang der strategischen Fünfjahrespläne und hat das Potenzial, ein neuer globaler Hegemon zu werden. Dazu projiziert es seine Machtansprüche nach innen und aussen, baut mit der Belt-and-Road-Initiative globale Infrastrukturen auf und weitet seine militärische Präsenz in Afrika aus. Russland versucht mit allen Mitteln, ein panslawisches Grossreich aufzubauen und sieht sich an der Seite Chinas als Gegenspieler des Westens. Die USA sind im Inneren durch die Spaltung der Gesellschaft stark mit sich selbst beschäftigt. Gleichzeitig müssen sie die Nato im Osten stärken und im Pazifik China Paroli bieten. Indien und Pakistan treten auf der weltpolitischen Bühne immer

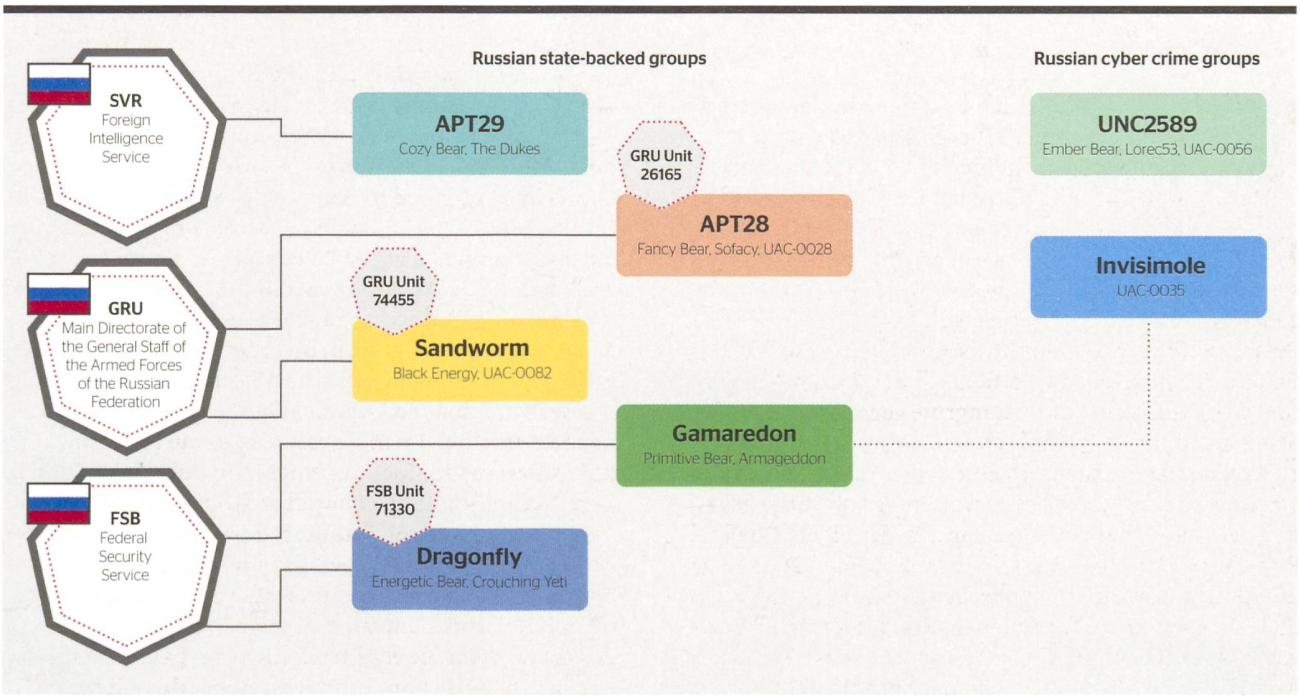
La cyberattaque probablement la plus connue contre un fournisseur d'énergie a entraîné une interruption de l'approvisionnement en électricité dans certaines parties de l'Ukraine en décembre 2015. Le responsable présumé: le groupe Sandworm, attribué au service de renseignement militaire russe GRU [1]. Mais il existe encore de nombreux autres exemples d'attaques contre des infrastructures critiques: le début de l'invasion russe de l'Ukraine en février 2022 a été accompagné de cyberattaques contre des terminaux de l'entreprise spécialisée dans les télécommunications par satellite Viasat, qui ont entraîné des perturbations collatérales chez un exploitant de parc éolien allemand. En mai 2021, le système de facturation de l'exploitant de pipelines américain Colonial Pipelines a été victime d'une attaque par ransomware qui l'a mené à interrompre l'exploitation d'importants oléoducs et gazoducs. Quant au fournisseur régional d'énergie Enercity de Hanovre, il a été la cible d'une attaque à l'automne 2022 qui a entraîné des perturbations au niveau du service clientèle et du traitement des paiements, ainsi que des fuites de données personnelles des clients [2].

Il y a des années déjà que les militaires et les services de renseignement du monde entier ont saisi l'importance du cyberespace pour leurs missions. En 2013, avec les « Snowden Leaks », le grand public a pour la première fois pris conscience de l'ampleur des cyberactivités offensives dirigées par les États. Depuis, le cyberdomaine s'est imposé en tant qu'élément de la géopolitique, et de nombreux États ont créé leurs propres cyberunités offensives au sein de leurs armées. Ainsi, l'OTAN a créé à Tallinn le Cooperative Cyber Defence Centre of Excellence (CCDCOE), et du côté de la Chine, tant l'armée que le ministère de la Sécurité de l'État ont recours au cyberespionnage à l'échelle mondiale, visant également les exploitants d'infrastructures critiques [3].

Une menace aux multiples facettes

La guerre menée par la Russie contre l'Ukraine a montré à l'Europe à quel point sa prospérité dépend de l'accès à une énergie bon marché. La transformation du secteur énergétique est un choix stratégique qui s'explique également par les incertitudes croissantes liées à la situation géopolitique.

Un coup d'œil sur la situation politique générale montre à quel point le monde est en pleine mutation. La Chine agit de manière conséquente selon ses plans stratégiques quinquennaux et a le potentiel de devenir une nouvelle nation dominante à l'échelle mondiale. Pour ce faire, elle projette ses ambitions de puissance à l'intérieur et à l'extérieur de ses frontières, développe des infrastructures mondiales avec la « Belt and Road Initiative » et étend sa présence militaire en Afrique. La Russie tente par tous les moyens de construire un grand empire panslave et se considère comme un adversaire de l'Occident aux côtés de la Chine. Les États-Unis sont bien occupés sur le plan intérieur par la division de la société et doivent, en même



Verbindungen zwischen Bedrohungsakteuren und russischen Nachrichtendiensten gemäss Trustwave.
Liens entre les cyberacteurs malveillants et les services de renseignement russes, selon Trustwave.

selbstbewusster auf und vertreten ihre eigenen wirtschaftlichen Interessen. Die Annäherung zwischen dem Iran und Saudi-Arabien deutet auf eine fundamentale Neuordnung im Mittleren und Nahen Osten hin. Wie Israel, einer der erfahrensten Cyber-Akteure, darauf reagieren wird, ist noch unklar. All diese Umbrüche und Verschiebungen führen zwangsläufig zu Konflikten und Kriegen, in denen der Cyberraum in allen Phasen Schauplatz von staatlich gelenkten Angriffen und Aktionen ist.

Staatliche Angreifer kooperieren mit Kriminellen

Die etablierte Unterscheidung von Angreifergruppen in staatlich gelenkte Spionagegruppen, politisch motivierte Hacktivisten und Cyberkriminelle verschwimmt zunehmend. Einerseits übernehmen Kriminelle vermehrt die fortgeschrittenen Methoden und Werkzeuge staatlicher Akteure. Andererseits setzen Nachrichtendienste manchmal auch Cyberkriminelle ein.

Ein eindrückliches Beispiel für diese Art der Kooperation ist im März 2023 [4] durch die Publikation vertraulicher Analysen bekannt geworden. Die Veröffentlichung umfasst Hunderte Dokumente, die U.S.-amerikanische Nachrichtendienste erstellt haben sollen. Die teilweise Echtheit der Dokumente wurde bestätigt; zugleich wurde durch eine unabhängige Recherchegruppe nachgewiesen, dass ein Teil der Dokumente manipuliert wurde [5]. Laut den veröffentlichen Dokumenten hatte die russische Hacktivistengruppe Zarya im Februar 2023 Zugriff auf die Steuerungstechnik einer Verteilstation eines unbenannten

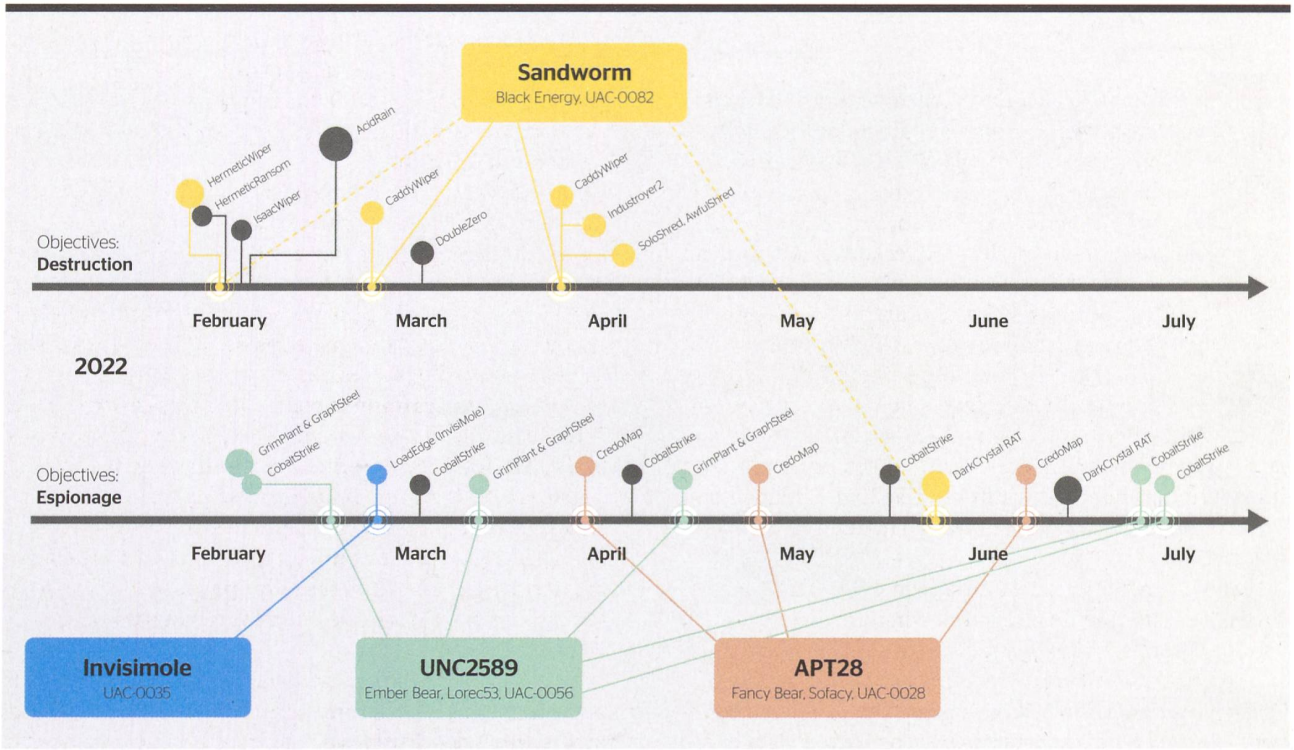
temps, renforcer l'OTAN à l'Est et résister à la Chine dans le Pacifique. L'Inde et le Pakistan apparaissent de plus en plus sûrs d'eux sur la scène politique mondiale et défendent leurs propres intérêts économiques. Enfin, le rapprochement entre l'Iran et l'Arabie saoudite laisse présager une réorganisation fondamentale au Moyen-Orient et au Proche-Orient. On ne sait pas encore comment Israël, l'un des cyberacteurs les plus expérimentés, va réagir. Tous ces bouleversements et décalages conduisent par la force des choses à des conflits et des guerres dans lesquels le cyberespace est, à toutes les étapes, le théâtre d'attaques et d'actions dirigées par des États.

Les attaquants étatiques coopèrent avec les criminels

La distinction établie entre les groupes d'attaquants actifs dans des groupes d'espionnage dirigés par des États, les « hacktivistes » à motivation politique et les cybercriminels, s'estompe de plus en plus. D'une part, les criminels adoptent de plus en plus les méthodes et outils avancés des acteurs étatiques. D'autre part, les services de renseignement font parfois appel à des cybercriminels.

Un exemple frappant de ce type de coopération a été révélé en mars 2023 [4] par la publication d'analyses confidentielles. Celle-ci comprend des centaines de documents qui auraient été produits par les services de renseignement américains. L'authenticité partielle des documents a été confirmée ; en même temps, un groupe

Bilder | Figures: Trustwave



Detektierte Cyber-Angriffe auf die ukrainische Infrastruktur.
Cyberattaques détectées contre l'infrastructure ukrainienne.

kanadischen Gas-Pipeline-Betreibers. Zarya bat laut der Veröffentlichung einen Offizier des russischen Inlandsnachrichtendienstes FSB um weitere Instruktionen [6]. Staatliche Angreifer kooperieren aber auch mit regulären IT-Dienstleistern, wie eine andere Veröffentlichung vertraulicher Informationen durch einen russischen Whistleblower zeigt [7]. Der russische IT-Dienstleister Vulkan-NTC hat im Auftrag mehrerer russischer Nachrichtendienste Angriffswerkzeuge entwickelt, die laut veröffentlichten Schulungsdokumenten auch gegen kritische Infrastrukturen eingesetzt werden können. So wird in einem Schaubild der Schulungsdokumente das stillgelegte Kernkraftwerk Mühleberg gezeigt [8].

Diese Gemengelage aus Unsicherheiten der geopolitischen Situation sowie Vermengung staatlicher und krimineller Cyberakteure, die in ihren Aktionen an keine Landesgrenzen oder Regionen gebunden sind, trifft auf der Gegenseite auf Infrastrukturen, die ihrerseits zunehmend komplexer und immer umfassender vernetzt sind. Die lang praktizierte Trennung von IT (Information Technology) und OT (Operational Technology) wird zunehmend durchbrochen. Geografisch abgelegene Infrastrukturen werden mittels Mobilfunk- und Satellitenanbindungen direkt mit dem Internet bzw. Cloud-Diensten verbunden, unter anderem, um übliche Software-Aktualisierungen durchführen zu können. Dadurch ergeben sich Infrastrukturen mit deutlich erweiterter Angriffsfläche und gestiegener Verwundbarkeit.

de recherche indépendant a démontré qu'une partie des documents avait été manipulée [5]. Selon les documents publiés, le groupe de hacktivistes russes Zarya a eu accès en février 2023 à la technique de commande d'une station de distribution appartenant à un exploitant de gazoduc canadien dont le nom n'a pas été mentionné. Selon la publication, Zarya a demandé des instructions supplémentaires à un officier du FSB, le service de renseignement russe chargé des affaires de sécurité intérieure [6]. Mais les attaquants étatiques coopèrent également avec des fournisseurs de services informatiques réguliers, comme le montre une autre publication d'informations confidentielles par un lanceur d'alerte russe [7]. Le prestataire de services informatiques russe Vulkan-NTC a développé pour le compte de plusieurs services de renseignement russes des outils d'attaque qui, selon les documents de formation publiés, peuvent également être utilisés contre des infrastructures critiques. L'un des schémas des documents de formation montre ainsi la centrale nucléaire désaffectée de Mühleberg [8].

Cette combinaison d'incertitudes liées à la situation géopolitique et de cyberacteurs étatiques et criminels, dont les actions ne sont liées à aucune frontière nationale ou régionale, est confrontée à des infrastructures de plus en plus complexes et interconnectées. La séparation longtemps pratiquée entre l'IT (Information Technology) et l'OT (Operational Technology) est de moins en moins effective. Des infrastructures géographiquement isolées

Auf diese Infrastrukturen wirken unterschiedlichste Angriffe ein: von Überlastangriffen über das direkte Eindringen durch verwundbare Systeme bis hin zu Phishing-Angriffen, die oftmals den Auftakt für Spionage oder Erpressung mit Ransomware bilden, und Angriffen, die Vertrauensstellungen in den Lieferketten ausnutzen. Zusätzlich zu diesen Cyberangriffen auf die Infrastrukturen manipulieren staatliche Akteure mittels Desinformationen die öffentliche Meinung. Die Meinungsmanipulation war schon immer eine Methode, mit der staatliche Akteure ihren Interessen Vorschub geleistet haben. Die Allgegenwärtigkeit der sozialen Netzwerke mit ihren direkten, ungefilterten Verbindungen und Interaktionen haben die Effektivität und Effizienz von Desinformationskampagnen jedoch in neue Höhen katapultiert.

Dass Desinformationskampagnen auch den Energiesektor betreffen, zeigen Beispiele rund um die deutschen Gasvorräte im Winter 2022/2023 und die Ermittlungen zur Explosion der Nord-Stream-Pipeline [9]. Die rasant voranschreitende Entwicklung der künstlichen Intelligenz, sowohl für die Generierung von Text als auch von Bild, Ton und Video, wird zu einer weiteren quantitativen und qualitativen Zunahme von Fake News führen.

Cyber-Resilienz koordiniert stärken

Betreiber kritischer Infrastrukturen stehen den Cyberangriffen jedoch nicht hilflos und auch nicht allein gegenüber. Eine geordnete Herangehensweise, die Technik, Organisation und Strategie vereint, kann die Cyber-Resilienz, d.h. die Kombination aus Widerstandsfähigkeit gegen Cyberangriffe und Wiederherstellungsfähigkeit nach erfolgreichen Angriffen, steigern.

Auf der strategischen Ebene ist zunächst die Erkenntnis bei Vorständen und Verwaltungsräten zu vermitteln, dass geopolitische Ereignisse ihr Echo im Cyberraum haben und die kontinuierliche Bewertung der Lage zu einer besseren Vorbereitung führen kann. Diese Erkenntnis muss dann in der gesamten Führung sowie in den Bereichen, die mit der Cybersicherheit beauftragt sind, verankert werden, damit notwendige Aktivitäten abgeleitet und in der Organisation etabliert werden können.

In der Organisation sind die Prozesse zur Bewältigung von Vorfällen und Krisen regelmässig zu prüfen und anzupassen. Tabletop-Übungen, die bestimmte Vorfalls-Szenarien nachstellen, haben sich als effektive Methode erwiesen, Schwachstellen in den eigenen Prozessen aufzudecken und gleichzeitig bei den Beteiligten Handlungssicherheit herzustellen. In unterschiedlichen Szenarien können Übungsschwerpunkte von der Erkennung eines Vorfalls bis zur Wiederherstellung des Normalbetriebes gesetzt werden.

Diejenigen Abteilungen, die mit der technischen Cybersicherheit betraut sind, müssen personell und finanziell so aufgestellt sein, dass sie über die nötigen Werkzeuge und Informationen verfügen, um effektiv und effizient den Dreiklang aus Prävention, Erkennung und Behandlung von Vorfällen bewältigen zu können.

sont directement reliées à Internet ou à des services en nuage (cloud services) au moyen de connexions mobiles et satellites, notamment pour pouvoir effectuer les mises à jour logicielles usuelles. Il en résulte des infrastructures avec une surface d'attaque nettement plus étendue et une vulnérabilité accrue.

Ces infrastructures sont la cible d'attaques très diverses : des attaques par saturation aux attaques par hameçonnage, qui sont souvent le prélude à l'espionnage ou au chantage au moyen de ransomwares, en passant par l'intrusion directe à travers des systèmes vulnérables et les attaques qui exploitent les positions de confiance dans les chaînes d'approvisionnement. En plus de ces cyberattaques contre les infrastructures, les acteurs étatiques manipulent l'opinion publique par le biais de la désinformation. La manipulation de l'opinion a toujours été une méthode utilisée par les acteurs étatiques pour servir leurs intérêts. L'omniprésence des réseaux sociaux, avec leurs connexions et interactions directes et non filtrées, a toutefois propulsé l'efficacité et l'efficience des campagnes de désinformation à de nouveaux sommets.

Les campagnes de désinformation touchent aussi le secteur de l'énergie, comme le montrent les exemples liés aux réserves allemandes de gaz pour l'hiver 2022/2023 et les enquêtes sur l'explosion du gazoduc Nord Stream [9]. Le développement fulgurant de l'intelligence artificielle, tant pour la génération de textes que d'images, de sons et de vidéos, mènera à une nouvelle augmentation quantitative et qualitative des fake news.

Renforcer la cyber-résilience de manière coordonnée

Les exploitants d'infrastructures critiques ne sont toutefois pas impuissants face aux cyberattaques, et ils ne sont pas seuls non plus. Une approche ordonnée, alliant technique, organisation et stratégie, peut renforcer la cyber-résilience, c'est-à-dire la combinaison de la résistance aux cyberattaques et de la capacité de récupération après des attaques réussies.

Au niveau stratégique, il convient tout d'abord de faire prendre conscience aux comités directeurs et aux conseils d'administration que les événements géopolitiques ont un écho dans le cyberespace, et que l'évaluation continue de la situation peut conduire à une meilleure préparation. Cette prise de conscience doit ensuite être ancrée dans l'ensemble de la direction ainsi que dans les domaines chargés de la cybersécurité, afin que les activités nécessaires puissent être déduites et établies dans l'organisation.

Au sein de l'organisation, les processus de gestion des incidents et des crises doivent être régulièrement examinés et adaptés. Les exercices de simulation (tabletop exercises), qui reproduisent certains scénarios d'incidents, se sont révélés être une méthode efficace pour mettre en évidence les points faibles des propres processus et, simultanément, pour instaurer une sûreté d'action chez les personnes concernées. Différents scénarios permettent de

Die Kooperation und der regelmässige strukturierte Austausch von Erkenntnissen und Erfahrungen mit anderen Organisationen können im Angriffsfall zu einem entscheidenden Vorteil für alle werden. Dieser Austausch sollte sowohl die strategische als auch die technische Ebene umfassen. Im besten Fall lassen sich Synergien nutzen und Aufwände für jede einzelne Organisation reduzieren und gleichzeitig die Resilienz aller steigern. Dieser Austausch kann im Rahmen staatlicher Initiativen erfolgen [10], durch Brancheninitiativen wie dem EE-ISAC [11] oder auch in branchenübergreifenden globalen Expertenvereinigungen [12].

Beim Blick auf die Bedrohungen darf vor allem der Daseinszweck des Energiesektors nicht in den Hintergrund geraten. Ziel aller Bemühungen muss es sein, die Versorgung der Bevölkerung und Wirtschaft mit Energie aufrechtzuerhalten. Sämtliche defensiven Cyberaktivitäten der Versorger sind auf dieses Ziel hin auszurichten.

Referenzen | Références

[1] Siehe auch: bulletin.ch/de/news-detail/cyberangriffe-auf-energieversorger.html
[2] www.enercity.de/presse/betrieb-und-baustellen/2022/it-stoerung
[3] EU-Warnung vor chinesischer Cyberspionage cert.europa.eu/files/data/TLP-CLEAR-JointPublication-23-01.pdf
[4] www.bloomberg.com/news/articles/2023-04-10/what-to-know-about-alleged-us-classified-documents-leak-from-pentagon-on-ukraine
[5] www.bellingcat.com/news/2023/04/09/from-discord-to-4chan-the-improbable-journey-of-a-us-defence-leak
[6] zetter.substack.com/p/leaked-pentagon-document-claims-russian
[7] www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics
[8] www.watson.ch/digital/schweiz/598263734-geleakte-dokumente-verraten-russische-plaene-fuer-cyberangriffe
[9] correctiv.org/faktencheck/2022/10/13/doch-die-deutschen-gasvorraete-reichen-laenger-als-bis-weihnachten; correctiv.org/faktencheck/2022/11/02/explosionen-an-gaspipelines-leiter-der-nord-stream-ermittlungen-heisst-weder-erik-ollsen-noch-ist-er-tot
[10] Beispielhaft: www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Kooperationen/kooperationen_node.html
[11] Für die europäische Energiebranche zum Beispiel www.ee-isac.eu
[12] www.first.org

Autor | Auteur
Dror-John Röcher ist CEO der Intcube GmbH.
Dror-John Röcher est CEO d'Intcube GmbH.
→ Intcube GmbH, DE-10115 Berlin
→ dror@intcube.io

Ursache für den im Einstiegsbild gezeigten Stromausfall in Kiew, Ukraine, war ein russischer Raketenangriff vom 23. November 2022, und keine Cyber-Attacke. Ein grossflächiger, durch eine Cyber-Attacke verursachter Stromausfall fand in der Ukraine am 23. Dezember 2015 statt.

mettre l'accent des exercices sur les diverses étapes, de la détection d'un incident au rétablissement du fonctionnement normal.

Les services chargés de la cybersécurité technique doivent être dotés des ressources humaines et financières leur permettant de disposer des outils et des informations nécessaires pour gérer de manière efficace et efficiente le triptyque prévention, détection et traitement des incidents.

La coopération et l'échange régulier et structuré de connaissances et d'expériences avec d'autres organisations peuvent devenir un avantage décisif pour tous en cas d'attaque. Ces échanges devraient porter à la fois sur le niveau stratégique et sur le niveau technique. Dans le meilleur des cas, il est possible d'exploiter les synergies et de réduire les efforts de chaque organisation tout en augmentant leur résilience. Ces échanges peuvent avoir lieu dans le cadre d'initiatives gouvernementales [10], d'initiatives sectorielles telles que l'EE-ISAC (European Energy Information Sharing and Analysis Centre) [11] ou d'associations mondiales d'experts intersectorielles [12].

Lors de l'examen des menaces, il ne faut surtout pas perdre de vue la raison d'être du secteur de l'énergie. Le but de tous les efforts doit être de maintenir l'approvisionnement en énergie de la population et de l'économie. Toutes les cyberactivités défensives des fournisseurs doivent être orientées vers cet objectif.

La panne d'électricité à Kiev, en Ukraine, utilisée en tant qu'image de titre, est à imputer à une attaque de missiles russes perpétrée le 23 novembre 2022, et non à une cyberattaque. Une panne d'électricité à grande échelle causée par une cyberattaque a eu lieu en Ukraine le 23 décembre 2015.

Das Leben ist schön, solange nichts passiert.
Die Mitglieder der Sicherheits-Charta bekennen sich mit ihrer Unterschrift kompromisslos zu Sicherheitsmassnahmen und setzen die lebenswichtigen Regeln oder ihre eigenen Sicherheitsregeln aktiv um. Sie sorgen so für mehr Arbeitssicherheit und Wirtschaftlichkeit in ihren Betrieben. Treten auch Sie online bei: www.sicherheits-charta.ch

CHARTA
STOPP BEI GEFAHR / GEFAHR BEHEBEN / WEITERARBEITEN