Cyberangriffe auf Energieversorger

Der Zwischenfall in der Ukraine und die Schweizer Situation

Das Horrorszenario eines Cyberangriffs auf die Energieinfrastruktur eines Landes wurde zwar schon länger diskutiert, aber der Thematik schien bisher etwas Hypothetisches anzuhaften. Bis zum 23. Dezember 2015. In der Ukraine wurde aus dem unwahrscheinlichen Szenario plötzlich Realität: Rund eine Viertelmillion Ukrainer sassen einige Stunden im Dunkeln, weil eine raffinierte Attacke mehrere Stromversorger lahmlegte. Obwohl es weniger offensichtlich ist, sind Betreiber kritischer Infrastrukturen aber auch in der Schweiz Cyberangriffen ausgesetzt.

Radomír Novotný

Am 23. Dezember 2015, kurz vor Schichtende, geschah in der Zentrale des Energieversorgers Prykarpattyaoblenergo etwas Seltsames: Auf einem Monitor fing der Cursor plötzlich an, sich selbst zu bewegen. Ein EW-Mitarbeiter, der gerade seinen Schreibtisch aufräumte, konnte erstaunt mitverfolgen, wie der Cursor auf Schaltflächen zusteuerte, mit denen die Leistungstrennschalter eines Unterwerkes in der Region gesteuert werden konnten – und sie anklickte, um das Unterwerk abzukoppeln. Als dann ein Fenster erschien, um die Aktion zu bestätigen, tat der Cursor auch dies. Der EW-Mitarbeiter versuchte nun, mit der Maus diesem Geschehen ein Ende zu bereiten, aber der Rechner ignorierte die manuellen Eingaben. Der Mitarbeiter wurde plötzlich ausgeloggt. Jegliche Versuche, sich wieder einzuloggen, scheiterten, da die Angreifer auch die Passwörter verändert hatten. Sie fuhren mit dem Ausschalten der Unterwerke fort; insgesamt waren rund 30 dieses EWs betroffen.

Auf die gleiche Weise wurden auch Unterwerke bei zwei weiteren Energieversorgern ausgeschaltet. Zudem wurden die USV-Anlagen zweier Zentralen ferngesteuert deaktiviert und auch die EVU-Betreiber sassen im Dunkeln. Es dauerte mehrere Stunden, bis das Netz grösstenteils wieder in Betrieb war – u.a. dank manuell einschaltbaren Leistungstrennschaltern.

Ein komplexer Angriff

Nach dem Angriff besuchte ein US-Team die Ukraine, um sich vor Ort ein Bild der Ereignisse zu machen. Das Team bestand aus Experten des National Cybersecurity and Communications Integration Centers, des ICS-Cert, das auf industrielle Attacken spezialisiert ist, dem Department of Energy, dem FBI und weiteren Organisationen. Die betroffenen EVU-Mitarbeiter wurden befragt, um Material zur Verhinderung künftiger Attacken zu sammeln.

Bei den Untersuchungen wurde klar, dass die Angriffe koordiniert und zeitgleich durchgeführt wurden – es war keine spontane Sache. Vor dem Angriff wurden während Monaten die Netzwerke der EVUs ausspioniert, um an Passwörter zu gelangen und um den Aufbau der Systeme kennenzulernen. Die Leistungstrennschalter wurden durch mehrere Personen gleichzeitig angesteuert, entweder durch Fernwartungswerkzeuge auf Betriebssystemebene oder durch Software, die via VPN-Verbindungen und Scada auf industrielle Fernsteuersysteme zugriff.

Nach dem Angriff wurden bei allen drei betroffenen EVUs gewisse Systeme mit einem Killdisk-Schadprogramm gelöscht, wobei auch die Master-Boot-Einträge beschädigt wurden. Die Systeme konnten also nicht wieder gestartet wer-

Keystone, Walter Bieri

In der Schweiz ist noch kein Stromausfall bekannt,der durch Cyberattacken verursacht wurde. Am 4. und 5. September 2016 fiel der Strom in Zürich wegen einem defekten Hochspannungsisolator aus.

den, was die Störungsbehebung deutlich erschwerte. Zudem wurde die Firmware in einigen Schnittstellen überschrieben, die serielle Signale zu Ethernet umwandeln. Dadurch war ein Ansteuern – konkret: ein Wiedereinschalten – gewisser Leistungstrennschalter nicht mehr möglich. Schliesslich wurden USV-Systeme in den EVUs aus der Ferne so rekonfiguriert, dass sie beim Angriff, wie erwähnt, deaktiviert werden konnten. Die Angreifer beschränkten sich offensichtlich nicht nur darauf, einen Stromausfall zu verursachen, sondern wollten auch die Ausfallzeit verlängern, indem Wiedereinschaltungsanstrengungen sabotiert wurden.

Zudem wurden Systeme in jedem der betroffenen EVUs mit BlackEnergy-Schadsoftware infiziert. Welche Rolle diese Software im Cyberangriff aber gespielt hat, ist nicht klar. Klar ist lediglich, dass die Schadsoftware via Spear-Phishing-E-Mails mit angehängten Word-Dokumenten verbreitet wurde.

Gründe für den Angriff

Es gibt diverse Thesen bezüglich der Urheber des ukrainischen Cyberangriffs. Ukrainische Sicherheitsdienste machen Russland verantwortlich, obwohl konkrete Beweise noch ausstehen. Es gibt Stimmen, die die Blackouts in der Ukraine als russische Vergeltung für die Angriffe auf das Elektrizitätsnetz auf der Krim halten. Dies ist kaum wahrscheinlich, denn die Planung der Angriffe auf die ukrainischen EVUs musste Monate vor dem Stromausfall auf der Krim begonnen worden sein.

Gemäss Robert Lee, einem ehemaligen Cyberangriff-Spezialisten der US Air Force, der auch an den Untersuchungen in der Ukraine beteiligt war, könnte der Angriff ein Zeichen an die ukrainische Regierung sein, um Bestrebungen zur Verstaatlichung privater EVUs zu stoppen. Einige der ukrainischen EVUs sollen nämlich im Besitz eines russischen Oligarchen sein, der an einer Verstaatlichung nicht interessiert ist. Robert Lee ist überzeugt, dass der ukrainische Cyberangriff eine Botschaft war. Aber bis heute ist unklar, was diese Machtdemonstration eigentlich erreichen wollte.

Reduktion des Risikos

Das in diese Analyse involvierte amerikanische Industrial Control Systems Cyber Emergency Response Team (ICS-Cert) schlägt diverse Massnahmen vor, die das Risiko solcher Angriffe minimieren sollen.

Der wichtigste Schritt zur Erhöhung der Internetsicherheit bei industriellen Anlagen ist die Implementierung von Best Practices im Management der IT. Dies umfasst die Beschaffung von vertrauenswürdigen Hard- und Softwaresystemen. Zudem soll man einen kontinuierlichen Überblick über die Hardware-Komponenten und die eingesetzte Software in einem Netzwerk behalten. Auch das Aktualisieren der Software und Installieren neuer Patches sind wichtig.

Unternehmen sollten zudem Notfallpläne entwickeln, die beschreiben, wie man sich verhalten muss, wenn Attacken die Sicherheitsmechanismen umgehen.

Die Sicherheit wird zusätzlich durch den Einsatz von Whitelists auf Servern und Eingabe-Rechnern erhöht. Solche Listen spezifizieren, welche Applikationen auf den Rechnern laufen dürfen und erschweren das Ausführen von Schadsoftware.

Eine weitere Methode zur Erhöhung der Sicherheit in Netzwerken ist das Trennen von sicherheitsrelevanten Netzwerken von nicht vertrauenswürdigen Netzwerken wie dem Internet, kombiniert mit dem Abschliessen nicht verwendeter Ports und dem Deaktivieren nicht benötigter Dienste. Dies ist u.a. bei Schweizer AKWs so implementiert, dass das Kontrollzentrum isoliert und nicht am Internet angeschlossen ist. Im Kontrollzentrum läuft ausschliesslich die ICS-Software und es ist beispielsweise nicht einmal möglich, auf einem dieser Geräte ein Word-Dokument zu erstellen.

ICS-Cert empfiehlt Unternehmen, zuerst eine gründliche Risikoanalyse durchzuführen, bevor Abwehrmassnahmen ergriffen werden. In der **Tabelle** ist die prozentuale Wirksamkeit der durch ICS-Cert empfohlenen Massnahmen aufgeführt. Detailliertere Erläuterungen mit guten Beispielen zu den sieben Massnahmen findet man in [1].

Intervention des britischen Geheimdienstes

Eine weitere Massnahme, die man eigentlich als selbstverständlich betrachten würde, ist die Verwendung individueller Schlüssel für die Verschlüsselung von übertragenen Daten beispielsweise bei Smart Meters. Kryptografische Verfahren sollten nicht nur aus Datenschutzgründen eingesetzt werden, sondern auch, um das Risiko zu reduzieren, dass Hacker die in manchen elektronischen Zählern vorhandenen Breaker ansteuern. In manchen Ländern werden solche Unterbrecher u.a. eingesetzt, um säumige Zahler vom Stromnetz zu trennen.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI hat nun den Wireless M-Bus Standard (EN) überarbeitet. Bislang hat der Standard nur Verschlüsselung umgesetzt, was aus Sicherheitsgründen nicht ausreicht. D.h. ein Wireless-M-Bus-Zähler mit Breaker, der die BSI-Vorgaben nicht erfüllt, bietet keine ausreichende Sicherheit gegen unerwünschte Beeinflussung.

In England hat sich gemäss der Technologie-Zeitung The Inquirer der britische Nachrichtendienst GCHQ beim landesweiten Smart-Meter-Rollout eingeschaltet. GCHQ, für Kryptografie und Datenübertragung zuständig, hat festgestellt, dass für alle zu installierenden 53 Millionen Smart Meter der gleiche Kodierschlüssel vorgesehen war. Hacker hätten so ein leichtes Spiel, sich Zugriff zu den (teilweise mit Breakern ausgestatteten) Zählern im ganzen Land zu verschaffen und einen massiven Stromausfall zu verursachen. [2]

Schweizer Situation

Die Wahrscheinlichkeit für einen ähnlichen Cyberangriff in der Schweiz scheint u.a. aus politischen Gründen geringer zu sein als in der Ukraine. Aber der Zwischenfall mit der Ruag-Spionage, die dank Informationen aus dem Ausland entdeckt werden konnte, schreckt auf. Dass vertrauliche Daten über die Schweizer Sondereinheit AAD 10 der Armee entwendet werden konnten, und dies von Rechnern eines Unternehmens, das selbst spezielle Software und Trainings gegen Cyberangriffe verkauft, hätte wohl niemand gedacht.

Strategie	Anteil abgewehrter Angriffe
Whitelists implementieren	38 %
Korrekte Konfiguration und Patches sicherstellen	29 %
Angriffsoberfläche reduzieren	17 %
Umgebung schaffen, die sich verteidigen lässt	9 %
Autentifizierung verwalten	4 %
Monitoring und Reaktion	2 %
Sicheren Fernzugriff implementieren	1 %

Strategien zum Schutz industrieller Steuersysteme und ihre Wirksamkeit gemäss ICS-Cert.[1]

Gemäss Experten sieht die Situation bei Schweizer Energieversorgern ziemlich gut aus. Max Klaus, der stellvertretende Leiter der Melde- und Analysestelle Informationssicherung des Bundes (Melani), präzisiert: «Wie in jeder Branche gibt es Unterschiede, die zum Teil auch unternehmensabhängig sind. Tendenziell dürfte das Thema bei grossen Energieversorgern präsenter sein als bei kleineren Unternehmen.» Bei Swissgrid, dem Betreiber des Schweizer Übertragungsnetzes, nimmt man die Bedrohung durch Cyberangriffe sehr ernst und handhabt entsprechende Risiken aktiv, um den Forderungen der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken zu entsprechen. Nebst der Implementierung von technischen Schutzmassnahmen steht vor allem auch die intensive Zusammenarbeit mit der nationalen und internationalen Energiebranche sowie mit den entsprechenden Bundesstellen im Fokus.

Nationale Schutzstrategie

Die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» [3] wurde am 27. Juni 2012 vom Bundesrat verabschiedet. Ein NCS-Teilprojekt, das sich mit der Verbesserung der Resilienz der kritischen Teilsektoren befasst, schlägt unter anderem organisatorische und technische Massnahmen vor. Zu ersteren gehört das sogenannte «Vier-Augen-Prinzip», implementiert durch die Trennung von Administratoren- und Schaltrechten; zu letzteren redundante Rechnerinfrastrukturen.

Bei diesen Massnahmen stehen aber nicht nur Cyberattacken im Fokus, sondern auch physische Gefährdungen wie Natur- und Elementarereignisse, beispielsweise überschwemmte Rechenzentren, die Störungen verursachen können. Kriminelle Aktionen wie die Manipulation vom Strommarkt bzw. Handelsdaten oder Erpressung werden auch analysiert.

Gewisse kriminelle Aktionen, wie die von Hackern, die sich mit ihrem «Erfolg» öffentlich brüsten möchten oder von Hacktivists wie Anonymous, die die Aufmerksamkeit auf ihre Anliegen lenken wollen, sind sichtbarer als andere, höher motivierte. Die höchste Stufe stellen Angriffe mit Malware wie Stuxnet im Iran dar, bei denen Scada-Systeme manipuliert wurden.

Scada-Systeme sind auch für EVUs wichtig, da sie zentrale Funktionen erfüllen, beispielsweise für den Abruf von Regelenergie durch Swissgrid. Dies geschieht über einen Verbund über verschiedene Netzebenen hinweg, wobei diverse Unternehmen involviert sind. Diese Vernetzung ist natürlich mit Sicherheitsmechanismen ausgestattet. Zudem vertrauen die Netzverantwortlichen den Scada-Anweisungen und Statusanzeigen nicht blind, sondern kontrollieren die Plausibilität.

Der Bund und der VSE erarbeiten auch Massnahmen im Bereich Smart Metering und Smart Grids, denn je mehr smarte Elemente in einem Netz miteinander kommunizieren, desto verwundbarer wird das Netz. Eine mögliche Massnahme zur Erhöhung der Versorgungssicherheit ist der Schutz vor korrupten Smart-Meter-Werten, die u.U. falsche Steuerbefehle auslösen können. Dabei stellt Hacking zwar den Worst Case dar, aber fehlerhafte Upgrades können genauso zu Ausfällen führen. Das BFE baut zurzeit eine Kontrollstelle auf, die deshalb Sicherheitsstandards definiert, um Geräte künftig entsprechend zertifizieren zu können.

Eine Zukunftsvision ist die Entwicklung eines eidgenössischen Fachausweises für Weiterbildungen im Kontext der Scada-Informatik. Heute kann man sich zwar im IT-Bereich in zahlreichen Bereichen weiterbilden, wie z.B. IT für Mobile-Anwendungen, aber bezüglich dem Betrieb von komplexen Scada-Systemen, die eine Lebensdauer von bis zu 20 Jahren aufweisen, besteht eine Lücke. Da ist man auf das Know-how der Hersteller angewiesen. Ob die Rechtsgrundlagen einmal diesbezüglich angepasst werden, ist aber noch offen.

Dass die Cyberangriff-Problematik für Schweizer Energieversorger nicht neu ist, sieht man u.a. daran, dass bereits 2011 vom VSE ein Dokument veröffentlicht wurde, das für kritische ICT-Infrastruktu-

Electrosuisse / ITG-Kommentar

Neue Herausforderungen für Energieversorger

«Die aktuellen Trends in der Energieversorgung führen zu einer zunehmenden Dezentralisierung der Energieerzeugung, zur Digitalisierung der Netze (z.B. Smart Meters, Smart Grids) und zu zahlreichen neuen Anwendungsfällen, die durch die enge Verknüpfung industrieller und kommerzieller Systeme ermöglicht werden. All diese Trends erhöhen die Anzahl der zu schützenden Objekte massiv – gleichzeitig versagen jedoch bisher bewährte Schutzkonzepte, welche auf einer Abschottung der Systeme basieren. Einfache Lösungen gibt es nicht. Eine systematische, kontinuierliche Risikoanalyse und ein umfassendes IT-Sicherheitsdispositiv mit regelmässigen Wirksamkeitsüberprüfungen wird somit Pflicht für alle Versorger.
Dafür benötigen wir kompetente Fachkräfte – in den Anwenderunternehmen selbst oder bei spezialisierten Beratungsunternehmen –, welche die Versorger mit ihrer Erfahrung in IT-Sicherheit und den jeweils spezifischen Anwendungen umfassend beraten können. Und wir benötigen Aufsichtsorgane und leitende Angestellte in den Versorgungsunternehmen, welche sich kritisch mit der Thematik auseinandersetzen und die richtigen Fragen stellen, bevor man durch ein Schadenereignis zum Handeln gezwungen wird.»
Dr. **Thomas Wettstein,** ITG-Präsident und CEO der Avectris.

Résumé

Des cyberattaques contre les fournisseurs d'énergie

L'incident en Ukraine et la situation suisse

Le scénario catastrophe d'une cyberattaque sur l'infrastructure énergétique d'un pays fait l'objet de discussions depuis longtemps déjà mais jusqu'à présent, le sujet semblait rester hypothétique. Jusqu'au 23 décembre 2015, quand ce scénario est devenu réalité en Ukraine : environ 250 000 ukrainiens se sont retrouvés dans l'obscurité pendant quelques heures lorsqu'une attaque raffinée a paralysé simultanément plusieurs fournisseurs d'électricité. Même si cela semble moins évident, les fournisseurs sont des infrastructures critiques et la Suisse est également exposée aux cyberattaques. La « Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) », entre autres, se penche sur cet état de fait. La stratégie adoptée par le Conseil fédéral le 27 juin 2012 comprend, entre autres, des mesures organisationnelles et techniques, comme des infrastructures informatiques redondantes. Toutefois, ces mesures ne se concentrent pas uniquement sur les cyberattaques mais également sur les risques physiques comme les évènements naturels et élémentaires, par exemple l'inondation d'un centre informatique, susceptibles de provoquer des défaillances. Les actes criminels tels que la manipulation du marché de l'électricité ou des données commerciales, de même que l'extorsion sont également analysés. No

ren von EVUs konkrete Handlungsempfehlungen formuliert. [4] Dieser Minimalstandard beinhaltet Analysen, Vorgaben und Anweisungen, die von jedem Elektrizitätsunternehmen schriftlich festgehalten werden sollen. Zurzeit wird an einer aus technischer Sicht ausführlicheren Version gearbeitet. Gemäss Daniel Caduff, stellvertretendem Geschäftsstellenleiter des Bereichs IKT im Bundesamt für Wirtschaftliche Landesversorgung, werden bei dieser Version verschiedene internationale Standards berücksichtigt, unter anderem auch der weltweit bekannteste Standard zur ICT-Security für die Strombranche aus den USA, der als NERC-CIP-Standard bezeichnet wird. [5] Er wurde durch die North American Electric Reliability Corporation (NERC) unter dem Begriff «Critical Infrastructure Protection» (CIP) veröffentlicht und behandelt den physischen Schutz, Cyber-Risiken sowie Business-Continuity-Prozesse und die Ausbildung von Mitarbeitenden. Durch die Berücksichtigung dieses strengen Standards erhält man einen Schweizer Standard, der einerseits dem aktuellen Stand der Technik entspricht und andererseits optimal auf die lokalen Anforderungen der Schweizer Situation zugeschnitten ist.

Literatur

- Kim Zetter, «Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid», Wired, 3.3.2016.
- ISC-CERT, «Cyber-Attack Against Ukrainian Critical Infrastructure», 25. Februar 2016, ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Referenzen

[1] ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf
[2] Graeme Burton, «GCHQ intervenes to prevent catastrophically insecure UK smart meter plan», The Inquirer, 21. März 2016.
[3] www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/roadmap.html
[4] ICT Continuity, Umsetzungsempfehlungen zur Gewährleistung der ständigen Disponibilität der Informatik- und der Kommunikationstechnologie zwecks Sicherstellung der Versorgung, VSE, 2011. www.strom.ch/fileadmin/user_upload/Dokumente_Bilder_neu/010_Downloads/Branchenempfehlung/VSE_ICT-Continuity_12-2011_D_01.pdf
[5] www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Autor

Radomír Novotný ist Chefredaktor Electrosuisse beim Bulletin SEV/VSE.

Electrosuisse, 8320 Fehraltorf
radomir.novotny@electrosuisse.ch

Daniel Caduff, stellvertretender Geschäftsstellenleiter des Bereichs IKT im BWL, beantwortet gerne Fragen im Zusammenhang mit dem Schutz der Schweiz vor Cyber-Risiken: daniel.caduff@bwl.admin.ch