Lebenswichtige Infrastrukturen in Cyber-Gefahr

Autor(en): **Mühlheim, Andy**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **179 (2013)**

Heft 5

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-327674

Lebenswichtige Infrastrukturen in Cyber-Gefahr

2012 legte der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken fest. Sind wir auf dem richtigen Weg und reichen die vorgesehenen Massnahmen? Der Autor, seit Jahren verantwortlich für den Schutz einer kritischen Infrastruktur, antwortet aus praktischer Sicht. *ET*

Andy Mühlheim

Kritische Infrastrukturen leisten Dienste, die für das Funktionieren des Staates und der Wirtschaft unabdingbar sind, wie Wasserversorgung, Elektrizitäts- und Gasversorgung, Strassenverkehr, Eisenbahn, Luftverkehr, Abwasser- und Abfallentsorgung.

Einige Infrastrukturen sind wegen der Abhängigkeiten untereinander kritischer als andere. Deshalb gelten Energieversorgung und Kommunikation als «höchst kritische» Infrastrukturen. Ihr Ausfall löst einen Dominoeffekt aus, zieht andere kritische Infrastrukturen in Mitleidenschaft und richtet immensen Schaden an.

Konsumhaltung und ihre Folgen

Vor allem fehlt es am Verständnis. Strom kommt jederzeit aus der Steckdose, Wasser aus dem Hahn, der Abfall wird pünktlich abgeholt und entsorgt. Daran haben wir uns gewöhnt, speziell in der Schweiz, wo angesichts der hervorragenden Verfügbarkeit von kritischen Infrastrukturen Diskussionen nur noch über Kosten stattfinden.

Lieferketten ohne Lager und «Just-in-time-Produktionen» wurden Standard. Einen Ausfall kann man sich nicht einmal mehr vorstellen. An «Business-Continuity»-Lösungen wird bestenfalls kurz gedacht.

Cyber War

«Der Krieg ist eine blosse Fortsetzung der Politik mit anderen Mitteln.» Das Zitat des Militärtheoretikers Carl von Clausewitz bekommt im Cyberraum eine spezielle Bedeutung.

Ohne Labor, ohne Hightech, ohne Kontakt zu gefährlichen Substanzen und mit wenig Geld kann jeder Cyber War führen. Man braucht dazu weder einen Staat, noch eigenes Territorium, noch Waffen. Ein PC, ein Internetanschluss, und man ist dabei. Gewiss, wenn man «richtig» mitmachen will, ist einiges, nur bei einem kleinen Teil der Erdbevölkerung vorhandenes Wissen nötig. Dieser kleine Teil entspricht einigen Millionen Menschen. Die Fähigkeit «Krieg» zu führen, ist somit nicht mehr Staaten vorbehalten.

Übertrieben? Ja, was sollen die hunderttausende IT-Spezialisten, welche verschiedene Länder offen für Cyber War suchen und ausbilden, den ganzen Tag treiben? Eigene Infrastrukturen schützen und sich die Angriffsfähigkeit aneignen! Erstens haben diese Länder die Möglichkeiten von Cyber War entdeckt und teilweise schon erfolgreich eingesetzt. Zweitens wurde ihnen bewusst, wie abhängig sie selber von kritischen Infrastrukturen sind. Und zum Dritten haben sie erkannt, dass kritische Infrastrukturen fast nicht zu schützen sind. Sie setzen deshalb auf verbale Abschreckung: Die USA beispielsweise vor zwei Jahren mit der Ankündigung, 40 000 Cyber Warriors anzustellen, oder Indien vor ein paar Monaten mit der Erklärung, hunderttausende von «Cyber-Kriegern» auszubilden.

Dies gipfelte in der Aussage eines vormaligen amerikanischen Verteidigungsministers, dass die USA für einen Cyber-Erstschlag bereit wären, sollte dies notwendig werden. Nun weiss man im virtuellen Raum nie so genau, woher Angriffe kommen und was für eine Absicht dahinter steckt. Reaktionen oder Präventivschläge treffen womöglich den Falschen und lösen eine Kettenreaktion aus, die uns in das Zeitalter der offenen Feuerstelle zurück katapultieren kann.

Aufgrund des ungenügenden Verständnisses für den Schutz von kritischen Infrastrukturen fehlen in der Schweiz Sensoren ausserhalb der Unternehmensperimeter, welche Angriffe erkennen. Das Fehlen gesetzlicher Grundlagen, Vorgaben und Verantwortlichkeiten verhindert eine dringend notwendige Zusammenarbeit zwischen Betreibern von kritischen Infrastrukturen, dem Bund und den Kantonen. Die Angst, dass eine zentral geführte Cyber Defense-Organisation in den eigenen Garten schauen könnte, scheint grösser als die Angst vor einem Cyber-Angriff.

Allgemeine Gleichgültigkeit

Bisher ging alles gut. «Stuxnet» ist vergessen und der Überfall auf Postfinance dem Gedächtnis längst entschwunden. Aber: Cyber-Angriffe finden gezielt und unsichtbar statt. Der Angreifer will verhindern, dass heimlich geschaffene Zugänge entdeckt und geschlossen werden. Wenn ein Angriff bekannt wird, ist zu vermuten, dass die dafür geschaffene Sicherheitslücke kurz vor der Enttarnung stand und der Angreifer den Zugriff noch einmal genutzt hat. Oder aber der Angreifer nahm die Entdeckung in Kauf, weil sich das Risiko lohnte und sein Ziel mit dem Angriff erreicht ist, wie mit «Stuxnet». Zudem haben weder Angreifer noch Angegriffene ein Interesse daran, einen Angriff publik zu machen.

Wo stehen wir? Aufgrund der fehlenden Bereitschaft der Nutzer, für die hohe Verfügbarkeit von Basisinfrastrukturen einen entsprechenden Preis zu bezahlen, werden selbst kritische Dienstleistungen und Daten in Billiglohnländer ausgelagert oder in Public Clouds, die aus solchen Ländern betrieben werden. Auch der Bau und Betrieb von kritischen Infrastrukturen werden dorthin vergeben. Selbstverständlich werden hierzu Verträge abgeschlossen, welche die höchstmögliche Sicherheit «garantieren». Oft zu einem Preis, der objektiv betrachtet nicht ein-

Schon drohender Ausfall kritischer Infrastruktur bedeutet leere Einkaufsregale wie in New York vor dem Wirbelsturm «Sandy». Bild: Financial Times Deutschland

mal zum Beschreiben der Sicherheit reicht. Dabei wird davon ausgegangen, dass in allen Ländern die gleichen Sicherheits- und Datenschutzstandards gelten wie bei uns üblich. Aufgrund des Kostendruckes möchte man gar nicht mehr wissen.

Rolle des Staates

Bei den kritischen Infrastrukturen gibt es neben den Unternehmensrisiken noch Risiken, die nicht der Betreiber trägt. Ausfälle von kritischen Infrastrukturen treffen die Gesellschaft und die Wirtschaft als Ganzes. Damit kommt unweigerlich der Staat ins Spiel.

Zum Schutz der Schweiz vor Cyber-Risiken verabschiedete der Bund deshalb eine Strategie, welche Massnahmen aufzeigt, die bis Ende 2017 umgesetzt werden sollen. Ihr Kern liegt darin, dass jeder Akteur für den eigenen Schutz verantwortlich ist.

Um die Situation zu verbessern, setzt der Bund auf bestehende Strukturen, die bisher nicht in der Lage waren, Angriffe zu erkennen, abzuwehren oder deren Folgen zu beheben. Der Staat will nur subsidiär Leistungen erbringen, etwa durch Informationsaustausch und nachrichtendienstliche Erkenntnisse. Gerade die sind der Schlüssel schlechthin. Inwieweit politisch und wirtschaftlich heikle Informationen bei der grossen Anzahl von Akteuren verteilt werden können, werden wir sehen. Und wie die im Vertrauen informierten Sicherheitsexperten den Geschäftsleitungen und Verwaltungsräten erklären sollen, dass sie grössere Investitionen für zusätzliche Sicherheit tätigen müssen, ohne den genauen Grund nennen zu dürfen, wird eine Herausforderung.

Laut Cyber-Strategie des Bundes handeln alle Akteure selber. Die Massnahmen reichen von Risikoanalysen bis zur internationalen Zusammenarbeit. Die Koordination liegt bei den «zuständigen und verantwortlichen Stellen und Strukturen über alle Ebenen». Was bedeutet dies für die Betreiber? Sollen sie auch Analysen fertigen und eine internationale Koordination anstreben? Und wie sollen die diversen «zuständigen und verantwortlichen Stellen und Strukturen über alle Ebenen» Cyber Defense koordinieren, wenn Zuständigkeiten und Verantwortlichkeiten nicht definiert sind und keine gemeinsam getragenen Schutzziele bestehen? Ein solcher dezentraler Ansatz greift viel zu kurz und wird der Gefährdung nicht gerecht. So stehen die Betreiber vor der Herausforderung, ihrerseits die staatlichen Stellen für Cyber Defense zu sensibilisieren und zu koordinieren. Sobald es konkret wird, verweisen diese rasch auf fehlende gesetzliche Grundlagen und Zuständigkeit

Zusammenarbeit im Bereich Cyber Defense

Gegen «normale» Angriffe aus dem Internet sind kritische Infrastrukturen gut geschützt. Sorgen bereitet Cyber War, also organisierte Kriminalität oder staatlich unterstützte komplexe, mehrschichtige Angriffe. Laut Aussagen von Sicherheitsexperten des Bundes finden sie jedoch nicht statt, da wir uns ja nicht im Krieg befinden. Deshalb dürfen die Wörter Cyber War und Cyber Defense beim Bund nicht verwendet werden. Man spricht weltweit wohl einzigartig vom «Schutz vor Cyber-Risiken».

Ich rede hier von Cyber War. Kritische Infrastrukturen sind strategische Ziele und sie werden angegriffen, jeden Tag. Ein Ausfall bedeutet rasch unvorstellbare Schäden.

Optimierungen nötig

Wie wäre Cyber Defense anzugehen? Ein erster Schritt ist das Überdenken der Zusammenarbeit zwischen Staat und Betreibern. Dazu braucht es gesetzliche Grundlagen. Pro Infrastruktur muss ein Sicherheitsziel festgelegt werden. Was soll erreicht werden, welches Restrisiko ist das Unternehmen, welches der Staat zu tragen bereit? Daraus folgen Massnahmen, abgestimmt auf die Möglichkeiten der Betreiber und des Staates und aufeinander. Der Stand der Umsetzung ist regelmässig zu prüfen und es ist nachzuweisen, dass die Sicherheitsziele erreicht werden.

Cyber Defense braucht nachrichtendienstliche Aufklärung und internationale Zusammenarbeit weit im Vorfeld. Man muss übergehen zu einem Best-Practice-Austausch unter Betreibern. Nötig sind moderierte Kommunikationsplattformen für die verschiedenen Akteure, Schulung der Mitarbeitenden, Überprüfungen und Sanktionen. Und die Möglichkeit, bei Bedarf rasch mit Massnahmen zu reagieren. Also Aufgaben, welche zentral orchestriert werden müssen und dem Staat vorbehalten sind. Ein rein dezentraler Ansatz wie ihn die nationale Strategie für den Schutz vor Cyber-Risiken vorgibt, greift viel zu kurz. Ein solcher ist weder effizient noch nachhaltig und wird den Risiken, der eine kritische Infrastruktur als strategisches Ziel ausgesetzt ist, auf keinen Fall gerecht.

Wir gehen davon aus, wir hätten ein verbrieftes Recht auf die stetige Verfügbarkeit der Dienste von kritischen Infrastrukturen, und vergessen, dass diese Infrastrukturen speziellen Schutz benötigen. Ein Schutz, der nicht gratis zu haben ist und ganz sicher nicht von den Betreibern alleine sichergestellt werden kann. ■

Major
Andy Mühlheim
El. Ing. HTL, MBA
Leiter Informatik und Security, Swissgrid AG
5235 Rüfenach