Die vernachlässigte Bedrohung

Cyberangriffe gefährden das souveräne Handeln von Staaten wie auch von Unternehmen. Essentielle Infrastrukturen wie die Energieversorgung oder der Verkehr sind in der Schweiz ungenügend gegen Risiken geschützt.

von René Droz

In den vergangenen Jahren ist der Bund vermehrt Opfer von Cyberangriffen geworden. Als der bundeseigene Rüstungskonzern Ruag im Jahr 2014 angegriffen wurde, flog die Tarnung von Schweizer Elitesoldaten[1] auf, und unbekannte Mengen an geheimen Daten wurden gestohlen. Alle IT-Komponenten der gängigen Technologien haben und generieren stetig neue Schwachstellen. Angreifer nutzen diese aus. Einige der Schwachstellen sind bekannt[2] oder werden es in kurzer Zeit sein. Es gibt aber auch solche, die nie bekannt werden. Ganz ausschliessen könnte man Cyberangriffe nur in einem vollständig unter eigener Kontrolle stehenden IT-Netzwerk inklusive aller notwendigen IT-Dienste, Applikationen, Zugriffe und Zutritte zu sämtlichen Systemkomponenten. Aus Kosten- und Effizienzgründen wird jedoch im allgemeinen auf solche Systeme verzichtet.

Identifizieren kann man Urheber von Cyberangriffen nur im Ausnahmefall, nämlich dann, wenn sie Amateure sind und grobe Fehler machen. Andernfalls ist eine Zuordnung nur möglich, wenn sie mehrmals die gleichen Methoden anwenden. Profis sind beinahe unmöglich zu identifizieren oder nur schon zu lokalisieren. Sie können ungehindert und unerkannt weltweit operieren. Auf internationale Abkommen zur Bekämpfung der Cyberkriminalität ist kein Verlass. Deren Instrumente funktionieren nicht oder sind langwierig und kompliziert. Ausserdem liegen sie oft nicht im Interesse der beteiligten Staaten.

Cyberangriffe werden von unterschiedlichsten Akteuren ausgeführt. Das Verteidigungsdepartement (VBS) unterscheidet zwischen Hobbyhackern, wohlorganisierten und professionellen Cyberkriminellen sowie Geheimdiensten und Staaten. Cybergrossmächte wissen alles über Hintertüren und Schwachstellen von IT-Systemen.

Einsparungen auf Kosten der Sicherheit?

Vital für die Schweiz sind ihre kritischen Infrastrukturen. Auf diese müssen wir uns täglich verlassen können. Dazu gehören beispielsweise die Energieversorgung, Wasserversorgung, Verkehrswege und Kommunikationsmittel. Viele Kraftwerke, Staudämme und auch Verkehrsbetriebe weisen keine adäquate IT-Sicherungen auf. Immerhin könnten Schäden durch Cyberangriffe auf Energie- und Wasserversorgung innerhalb einer unkritischen Zeitspanne[3] behoben werden, aber nur dann, wenn die Verkehrswege und Kommunikationsmittel intakt bleiben.

Die Kommunikationsmittel, insbesondere die der kritischen Infrastrukturen, sind sehr komplex. Bis vor kurzer Zeit waren diese für eine fast 100prozentige Verfügbarkeit in sich genügend redundant, oder sie konnten sich mindestens gegenseitig im Notfall aushelfen. Man denke da zum Beispiel ans Mobilfunknetz, auf das selbst die Armee ergänzend abstellt. Als Anfang Jahr das Swisscom-Netz mehrmals überlastet war, waren die Notfallnummern über längere Zeit nicht erreichbar. Das gibt zur Sorge Anlass. Diese Vorfälle nähren die Vermutung, dass die Sicherheit bei den Telekom-Anbietern je länger, je mehr in den Hintergrund rückt und nur noch die Kosten respektive das Preisgefüge im Markt für Endnutzer zählen. Wir müssen für die Sicherheit eine angemessene Redundanz aufrechterhalten. Der Trend in Industrie und Verwaltung zielt jedoch auf Vereinheitlichungen und Zentralisierungen zugunsten eines öffentlichkeitswirksam vorgegaukelten, aber kaum nachweisbaren Spareffektes. Das Ausfallrisiko bedingt aber Notfallvorkehrungen, die äusserst komplex sein können und nicht einfach auszutesten sind. Wir laufen zunehmend Gefahr, dass notwendige adäquate Anpassungen der Notfallpläne zu kompliziert sind und ausbleiben, zu spät kommen oder gar nicht mehr umzusetzen sind. Die Folge wären längere Ausfallzeiten und Folgeschäden. Generell wird es durch die zunehmende Komplexität immer schwieriger, Risiken realistisch einzuschätzen. Die Statistik hilft da nicht, denn jeder Vorfall ist anders und findet meist unter neuen Prämissen statt. Nur das lückenlose Durchdenken aller realistischen Eventualitäten und präventive oder reaktive Vorkehrungen gegen jeden einzelnen möglichen Vorfall bereiten uns angemessen auf einen Ernstfall vor.

Die SBB haben ihren Betrieb stark automatisiert. Aber auch sie sind auf IT-Ausfälle vorbereitet und kennen jeweils Notfallpläne zur Wiederherstellung des Verkehrs. Ob diese ausreichen, wird sich weisen. Beim Strassenverkehr denken heute viele über automatische Verkehrsführung mit selbstfahrenden Fahrzeugen nach. Doch bis jetzt denkt niemand an Notfallplanungen, die entscheidend wären, sollten dafür notwendige IT-Strassen-Führungszentren der-

«Nicht oder schwer bemerkbare Schäden sind schwierig zu behandeln und werden darum flächendeckend unterschätzt. Ohne öffentliche Aufmerksamkeit gibt es in der Verwaltung keinen Handlungsdruck.»

René Droz

einst ausfallen. Heute reicht es, wenn die ausgefallene Ampelsteuerung einfach automatisch auf Gelb umschaltet. Der Autofahrer übernimmt dann selbst die Verantwortung für den unfallfreien Betrieb. Bei einer künftig möglichen zentralen Verkehrsführung mit selbstfahrenden Fahrzeugen wird das deutlich komplizierter. Fahrzeuge, die zum Beispiel stehen bleiben, weil sie die korrekte Steuerung durch das Verkehrsleitsystem verloren haben, das vielleicht sogar dafür gezielt sabotiert wurde, sind nicht nur ärgerlich für die einzelnen Autofahrer, sondern verstopfen in kurzer Frist den gesamten Verkehr und beeinträchtigen somit eine kritische Infrastruktur. Wie bringt man in dieser Situation zum Beispiel lebensrettende Einsatzfahrzeuge an ihren Bestimmungsort? Sie hätten nicht Stunden Zeit für eine allfällige Wiederherstellung eines IT-Strassen-Führungszentrums, das danach die stehen gebliebenen Fahrzeuge wieder aufräumt. Für die Bewältigung solcher Fälle in der Zukunft gibt es darum noch viele strategische, konzeptionelle und auch juristische Hausaufgaben zu machen. Es ist zu befürchten, dass nach dem Hochjubeln der Innovation zuerst etwas Katastrophales passieren muss, bis Handlungsbedarf erkannt wird.

Viele Schäden bleiben unbemerkt

Meist redet man nur von bemerkbaren Schäden. Dagegen helfen Notfallplanungen. Auffangbar sind diese Risiken mit materieller Reservebildung, Redundanz von Systemen und der Abwälzung eines Teils des Risikos auf Vertragspartner beziehungsweise auf kritische Infrastrukturen des Bundes oder der Armee.

Nicht oder schwer bemerkbare Schäden sind schwierig zu behandeln und werden darum flächendeckend unterschätzt. Ohne öffentliche Aufmerksamkeit gibt es in der Verwaltung keinen Handlungsdruck. Irreguläre Datenabflüsse aus den internen Netzen können kaum bemerkt werden, wie etwa ein Fall von 2012 zeigt, als interne Dokumente des Aussendepartements an eine unbekannte Täterschaft abgeflossen sind. Dieser Fall wurde erst 2014 publik. Im Datenstrom der IT-Netzwerke gibt es heute unzählige verschlüsselte Datenabflüsse. In der Regel handelt es sich dabei um Serviceleistungen von Herstellern und Anbietern. Unter den abfliessenden Daten können aber auch solche von Benutzern und Organisationen versteckt sein, die durch Schadcodes von Cyberangriffen generiert wurden. So gelangen kritische Daten leicht an unbeabsichtigte Adressaten.

Die meisten Cyberangriffe werden aus kommerziellen Motiven ausgeführt und treffen ungezielt einzelne, die sich nicht mit ausreichenden Abwehrmassnahmen ausgerüstet haben. Weitaus gefährlicher sind jedoch gezielte Cyberangriffe. Der verletzte Datenschutz des einzelnen ist dabei noch das kleinste Risiko. Es drohen nachhaltige Schäden: Gefährdung der kritischen Infrastruktur, Unfälle und Katastrophen, Verlust von Geschäfts- und Staatsgeheimnissen, Manipulationen von Wahlergebnissen via E-Voting oder die Schädigung der Reputation der Schweiz (wenn beispielsweise Cyberangriffe unter falscher Schweizer Flagge getätigt werden), im Extremfall – bei Datenverfälschungen – der Verlust der Führungsfähigkeit von Bund und Armee. Gefälschte, falsch adressierte oder gelöschte Dokumente oder Anweisungen können zu heilloser Verwirrung und Fehlentscheiden in jeder Organisation führen. Insbesondere bei professionellen Gegnern wie Geheimdiensten sind politische Verwicklungen programmiert. Man denke an das abgehörte Handy von Angela Merkel oder an den Fall des Computerwurms «Stuxnet». Beim elektronischen Abstimmen droht zudem der Verlust des Vertrauens in die Demokratie, weil aufgrund des Abstimmungsgeheimnisses die elektronischen Auswertungen nie wirklich kontrolliert werden können.

Unternehmen müssen investieren

Für Wirtschaft und Industrie gilt grundsätzlich das Prinzip der Eigenverantwortlichkeit: Die Unternehmen müssen die notwendigen Investitionen für die Cybersicherheit tätigen; diese sollten

natürlich geringer sein als die damit mutmasslich verhinderten Cyberschäden. Das funktioniert bei Banken und Versicherungen zurzeit recht gut, weil sie für die Berechnung solcher Schäden brauchbare Statistiken verwenden.

Bei KMU hingegen stellt man immer wieder fest, dass diese kaum oder überhaupt nicht gegen Cyberangriffe gewappnet sind. Schadenfälle sind bei ihnen relativ selten, das zu erwartende Ausmass wird daher oft unterschätzt und die nötigen Investitionen werden als zu teuer angesehen. Die in der jüngeren Vergangenheit öfters vorgekommenen Ransomware-Angriffe[4] gehören zu mittleren Bedrohungen, gegen die auch KMU sich schützen könnten und müssten. Nötig sind dazu eine erhöhte Aufmerksamkeit der Nutzer und der IT-Betreiber sowie mehrere Back-ups jeglicher Dateien und eine Wiederherstellungskonzeption. Dies bedingt eine minimale interne IT-Sicherheits-Infrastruktur und entsprechende Investitionen in Personal und Ausrüstung. Es ist fahrlässig und unverantwortlich, wenn Unternehmungen heute IT einsetzen und auf diese Vorkehrungen verzichten.

Beim Bund wurde in den Jahren 2012 bis 2017 eine Cyberstrategie entwickelt.[5] Dort werden die Risiken beschrieben und Handlungsfelder, Zuständigkeitsbereiche und Massnahmen definiert, mit denen diese Risiken minimiert werden sollen. Für die kritischen Infrastrukturen des Bundes werden die in der Strategie definierten Massnahmen angewendet, soweit die nötigen Ressourcen vorhanden sind. Fragt man Spezialisten, reichen die entsprechenden Budgets allerdings nirgendwo hin. Jede Innovation bringt neue Herausforderungen für die Sicherheitseinrichtungen. Das Restrisiko soll subsidiär durch die Armee getragen werden. Restrisiken sind solche, die man aufgrund des seltenen Auftretens nicht bestimmen kann, die aber ein hohes Schadenspotenzial haben. Mit solchen unberechenbaren Risiken kann die Verwaltung schlecht umgehen. Im Ernstfall steht die Armee rund um die Uhr zur Verfügung, Schadenfälle im Bereich der kritischen Infrastrukturen zu lindern und zu beheben.

Umstritten seit langem war bei der Armee selbst der Grad der Abschottung vom Internet. Daraus ergab sich die Frage, ob es zwei IT-Architekturen geben soll oder nur eine. Ist die Flexibilität von Datenanwendungen das relevante Kriterium, so entscheidet man sich für eine, ist es die Sicherheit, so für zwei. Wiederholt geriet in der Vergangenheit im Streben nach Kosteneffizienz die Sicherheit aus dem Blick. So gab der Bund im Jahr 2003 das Armeenetz TRANET zugunsten eines «kostengünstigeren» gemeinsamen Verwaltungsnetzes auf. Etliche Male fanden diesbezügliche Paradigmenwechsel statt, lange ohne dass nachhaltige und gleichzeitig realisierbare Konzeptionen erkennbar waren. Zurzeit tendiert das VBS wieder zu zwei Architekturen, wobei jetzt aber die Telefonie im Datennetz integriert ist.

Vertrauen kann man nur sich selber

Die Schweiz steht im internationalen Vergleich – wenn man die Grossmächte ausklammert – gut da. Der Bund hat präventive und reaktive Massnahmen gegen Cyberangriffe auf die kritischen Infrastrukturen festgelegt. Die Sensibilisierung der KMU für die eigene Informationssicherheit findet zwar statt, müsste aber wirksamer sein. Kaum geschützt sind wir aber gegen Wirtschaftsspionage und Reputationsverluste durch gezielte, ungewollte Datenabflüsse der höheren Bedrohungsstufen.

Das Risiko der Lahmlegung von lebenswichtigen, kritischen Infrastrukturen in der Schweiz ist wohl – mindestens zurzeit noch – in jeweils genügend kurzer Zeit in den Griff zu bekommen. Doch eine nicht nachlassende Aufmerksamkeit und entsprechende Ressourcen bleiben zwingend. Die gröbsten Risiken, wie jenes von E-Voting, sollten wir souverän eliminieren durch Verzicht, schon deshalb, weil ein allfälliger Nutzen in keinem Verhältnis zum Risiko steht. Von der Armee darf erwartet werden, dass sie ihre Führungsfähigkeit auch im Cyberkrieg behält. Weitergehende Ansprüche in bezug auf IT-Unterstützung sind aber mit Vorsicht zu formulieren. Wirtschaft und Industrie sind gezwungen, ihre Aufwendungen für die IT den Sicherheitsbedürfnissen anzupassen, um nachhaltig bestehen zu können.

Die Schweiz kann aber weder Grossmacht spielen noch eine eigene IT-Technologie im grossen Stil aufbauen und vermarkten. Wirklich sichere Infrastrukturen sind preislich wohl nie konkurrenzfähig und könnten nur in Nischenmärkten existieren. Die Frage stellt sich deshalb, welchem Technologieriesen man sich anschliessen will: China oder den USA? Chinesische Produkte beinhalten nachweislich geheime Chips, bei welchen unklar ist, wozu sie dienen. Bei amerikanischen Produkten ist die Transparenz höher, schon nur dank der tieferen Sprachbarriere. Jedoch ist bekannt, dass auch die US-amerikanischen Geheimdienste IT-Sicherheitslücken ausnutzen. Eine schwierige Wahl. Vertrauen kann man letztlich nur seinen eigenen Sicherheitskonzeptionen, wenn sie die qualitativen Anforderungen erfüllen und Risiken durch vertrauensunwürdige Komponenten ausschliessen können. ‹

[1] www.nzz.ch/nzzas/cyber-attacke-gegen-ruestungskonzern-ruag-russische-hacker-enttarnen-geheime-schweizer-elitetruppe-ld.18562
[2] Liste des National Institute of Standards and Technology (N.I.S.T.).
[3] Energieversorgung und Wasserversorgung werden nicht vor 1 bis 3 Tagen kritisch. So lange können Notstromgruppen und Wassertanks die wichtigsten Funktionen bei relevanten Infrastrukturen überbrücken.
[4] Angriffe durch Verschlüsselung der Daten mit anschliessender Erpressung für die Wiederherstellung.
[5] www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

René Droz

ist ehemaliger Ressortleiter für Überwachung und Sicherheit des einstigen militärischen Netzes TRANET. Zudem war er als operativer Chef und Gesamtprojektleiter für den Aufbau des militärischen Emergency Response Teams (milCERT) in der Führungsunterstützungsbasis verantwortlich.