Cyber Resilience

Etwa ein Drittel der Menschheit nutzt das Internet – mit steigender Tendenz. In der Schweiz sind es bereits über 80 Prozent. Angetrieben vom «Internet der Dinge», in dem Objekte des Alltags miteinander und mit uns kommunizieren, wird sich die Vernetzung weiter ausdehnen – nicht nur mit positiven Folgen.

→ **VON CATHRIN SENN**

Die globale Vernetzung, in ihrer Extremform «Hyperconnectivity» genannt, zwingt zum radikalen Umdenken – nicht nur angesichts der enormen Möglichkeiten, die sich damit auftun, sondern auch in Bezug auf die Risiken, die damit einhergehen. Dies spiegelt sich einerseits in den Hackern wider, die schon lange nicht mehr nur blosse Einzeltäter sind, sondern sich in mehr oder weniger losen Gruppierungen organisieren; andererseits aber auch in den Cyberattacken selbst, die keinen Halt vor territorialen Grenzen machen. Die vernetzte Welt und die damit einhergehende Komplexität erfordern deshalb neue übergreifende Lösungsansätze.

GLOBALE ATTACKEN

Dass die Verfügbarkeit des Internets keine Selbstverständlichkeit ist, hat sich am Internetblackout in Syrien gezeigt – ob technisches Problem oder absichtliche Störung durch die Regierung sei dahingestellt. Auch gab es schon Aufrufe, das Internet ganz lahmzulegen. Im Februar 2012 kündigte zum Beispiel das Hackerkollektiv Anonymous an, einen globalen Angriff auf das Domain-Name-System (DNS) durchzuführen, das Domänennamen in IP-Adressen umwandelt. Mit einer Distributed-Denial-of-Service-Attacke (DDoS) sollte das Internet dadurch für Stunden oder gar Tage indisponibel gemacht werden.

Das World Economic Forum (WEF) teilt globale Bedrohungen in fünf Gruppen ein: Hacktivism, Corporate Espionage, Government-driven, Terrorism und Criminal. Die Kategorien fokussieren nicht – wie oft üblich – auf die Art der Attacke, beispielsweise DDoS, sondern zeigen auf, welche Motive oder welcher Ursprung bei einem Cyberangriff im Vordergrund stehen können: politischer Aktivismus (wie bei Anonymous), Wirtschaftsspionage, regierungsgetriebene Angriffe, Terrorismus und Cyber Crime; wobei sich die Themengebiete auch teilweise überschneiden können.

Generell stellen Cyberrisiken eine immer wichtiger werdende Bedrohung für Unternehmen dar, insbesondere für Technologie-, IT- und Telekommunikationsunternehmen, aber auch für Firmen, die besonders schützenswerte Daten und Informationen verwalten, zum Beispiel Finanzdienstleister oder auch Organisationen, die SCADA-Systeme (Supervisory Control and Data Acquisition) für kritische Infrastrukturen betreiben, etwa im Energiesektor. Letztlich ist aber jede Organisation ein potenzielles Opfer.

Einen hundertprozentigen Schutz vor Angriffen von aussen gibt es nicht – oder eben nur dann, wenn Organisationen und Systeme komplett von der Welt abgeschottet werden, was weder sinnvoll noch in den meisten Fällen machbar ist. Spezialisten gehen davon aus, dass jedes Unternehmen einmal Opfer einer Cyberattacke werden wird. Die Frage ist also nicht ob, sondern wann und wie der Angriff stattfindet.

«Die Frage ist nicht ob, sondern wann und wie der Angriff stattfindet»
Dr. Cathrin Senn

GLOBALE ANTWORTEN

Vorbeugende Massnahmen können jedoch nicht nur innerhalb von Unternehmen und Organisationen getroffen werden, sondern müssen letztendlich länderübergreifend wirken und setzen einen kontrollierten Informationsaustausch zwischen Parteien des privaten und öffentlichen Sektors voraus. Auch muss eine klare Gesetzgebung und konsequente Rechtsprechung vorhanden sein, mit der auf Cyberangriffe grenzüberschreitend reagiert werden kann. Noch immer sind kriminelle Handlungen in der physischen Welt einfacher zu melden, zu verfolgen und vor Gericht zu bringen als im Cyberraum.

Eine Antwort auf diese neue Art der Bedrohung will die «Cyber Resilience» geben (übersetzbar etwa mit «Cyberwiderstandskraft», vgl. Textbox rechts). Bei diesem Ansatz geht es nicht nur darum, sich vor Angriffen zu schützen (etwa mittels Security-Software und dem Patchen von Systemen), sondern um eine holistischere Herangehensweise, die zwar Ausfälle nicht verhindern kann, aber den völligen Zusammenbruch von Netzwerken und Computersystemen abwenden soll. Ein Vorstoss in Richtung globaler Bekämpfung von Cyberrisiken ist die vom World Economic Forum 2012 in Davos lancierte Initiative «Partnering for Cyber Resilience». In deren Rahmen werden zahlreiche Unternehmen, Organisationen und Regierungen an einen Tisch gebracht, um Informationen zur Security im Netz global auszutauschen und gemeinsam nach Lösungen zu suchen. Unternehmen und Regierungen unterschreiben dabei ein «Commitment to Cyber Resilience», welches das eigene Engagement bekräftigt, entsprechende Schritte umzusetzen. Die WEF-Initiative stellt dabei Themen wie Corporate Governance in den Vordergrund, möchte auf Ebene Geschäftsführung mehr Awareness schaffen und den Informationsaustausch zwischen Organisationen verbessern.

Die WEF-Initiative ist dabei eines der neueren Projekte rund um das Thema Internet Security und Cyber Resilience. Daneben existieren auch einige Gruppierungen, die sich dem Thema als Ganzem schon seit mehreren Jahren widmen, einerseits aus der Perspektive der Privatwirtschaft, andererseits aus Sicht des öffentlichen Sektors.

Hinter der Vereinigung ICASI (Industry Consortium for Advancement of Security on the Internet), die 2008 gegründet wurde, stehen namhafte Unternehmen wie Cisco, Intel, IBM und Microsoft. Bei den Regierungsorganisationen sind zum Beispiel IMPACT (International Multilateral Partnership Against Cyber Threats) der Vereinten Nationen oder die 2004 gegründete ENISA (European Network and Information Security Agency) zu erwähnen, Letztere die zentrale Anlaufstelle für Information Security in der Europäischen Union.

GLOBALE ZUSAMMENARBEIT

Initiativen und Organisationen, die sich der Themen Cyber Resilience und Internet Security annehmen, sind wichtig. In einer globalen, vernetzten Welt ist eine Zusammenarbeit von relevanten Organisationen im öffentlichen und privaten Sektor zentral, um ein so wichtiges Medium wie das Internet und andere kritische Netze vor Angreifern zu schützen. Jedoch ist es nicht immer einfach, solche Initiativen am Leben zu halten und ein ernstgemeintes Commitment von allen Parteien zu erreichen. Bei manchen Gruppierungen besteht auch der Verdacht, dass das Thema Internetsicherheit nicht nur aus purem Altruismus aufgegriffen wird, sondern, dass dahinter auch wirtschaftliche Interessen und PR-Aktivitäten stehen.

Wenn Menschen und Objekte in Zukunft noch stärker miteinander vernetzt sind, wird eine ungestörte Kommunikation in der Cyberwelt jedoch immer elementarer werden. ←

Dr. Cathrin Senn ist CFO, Senior Consultant & Teilhaberin des Beratungsunternehmens OneConsult GmbH → **www.oneconsult.com**

Begriffsklärung

- **Cyber Resilience:** Die Widerstandskraft von Systemen oder Organisationen gegenüber einem Cyberevent, gemessen durch eine Kombination aus der mittleren Zeitspanne bis zum Ausfall und der mittleren Zeitspanne bis zur Wiederherstellung (nach WEF: «Partnering for Cyber Resilience»).
- **Cyberrisiko:** Ein Ereignis, welches das Internet oder eine andere Netzwerkinfrastruktur wie beispielsweise Telekommunikationsnetze, betrifft und das mit einer Eintrittswahrscheinlichkeit und einem erwarteten Schaden assoziiert ist.
- **Distributed Denial of Service (DDoS):** Verteilter Angriff, dessen Anfragen die Überlastung eines Systems bezwecken, um so das betroffene System nicht mehr verfügbar zu machen.
- **Hyperconnectivity:** Der Zustand, überall und immer verbunden zu sein durch den Gebrauch von mehreren Kommunikationsgeräten; oft aber auch benutzt zur Beschreibung einer allgemeinen starken Vernetzung.
- **Internet der Dinge:** Die Vernetzung von digital «intelligent» gemachten Objekten, etwa wenn der Kühlschrank weiss, dass keine Milch mehr da ist, und neue bestellt. In diesem Zusammenhang werden oft auch die Schlagworte «Pervasive Computing», «Ubiquitous Computing» oder «Everyware» verwendet.

Weiterführende Links zum Thema:
→ **www.enisa.europa.eu**
→ **www.icasi.org**
→ **www.impact-alliance.org**
→ **www.weforum.org/cyber**