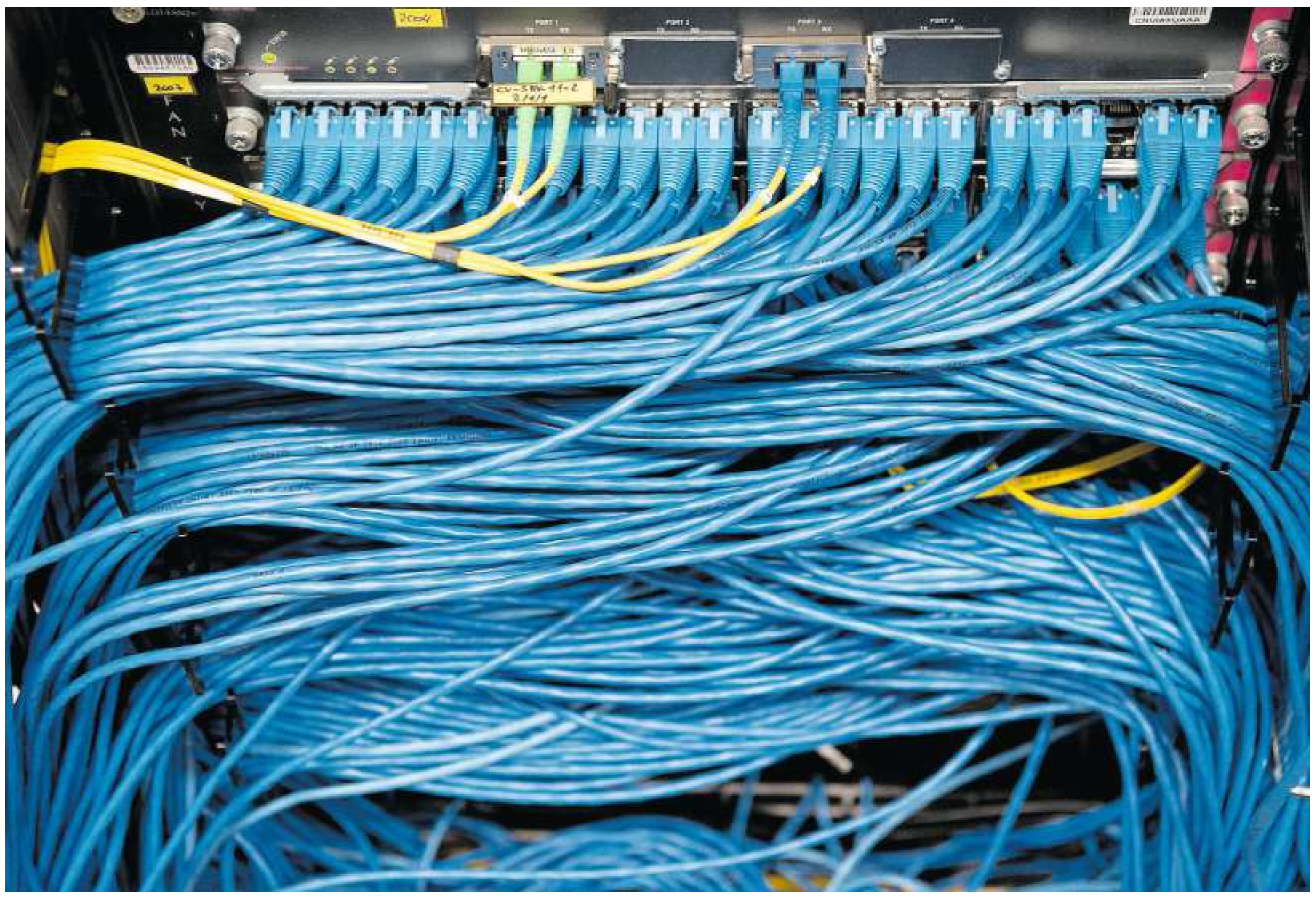
24-Stunden-Monitoring gegen Cyberrisiken

Wie sich Unternehmen und der Staat besser vor digitalen Attacken schützen können. **Von Marc Furrer und Matthias Amgwerd**

Mit der Einführung der neuen Mobilfunktechnologie 5G wird das Internet der Dinge, also die allumfassende Vernetzung, eine Tatsache. Das birgt Gefahren, deren sich Wirtschaft und Gesellschaft schnell bewusst werden müssen.



Unternehmen müssen sich vor Cyberangriffen schützen, weil unsere Netze immer unsicherer werden. LAURENT GILLIERON / KEYSTONE

Autonomes Fahren oder gänzlich neue logistische Abläufe, die den Transport, aber auch die Bewirtschaftung von Gütern erleichtern – all dies könnte mit dem Internet der Dinge schon bald Wirklichkeit sein. Doch birgt diese allumfassende Vernetzung nicht nur Chancen, sondern auch neue Angriffspunkte für Cyberkriminelle. Unsere Netze und Infrastrukturen werden zunehmend unsicherer und verwundbarer. Es ist also höchste Zeit, dass sich Unternehmen angemessen vor Cyberangriffen schützen.

Zwar sind gerade grössere Unternehmen auf dieses Thema sensibilisiert, man schützt sich aber noch nicht konsequent genug. Dies betrifft gerade auch kritische Infrastrukturen und industrielle Anlagen, wo bereits vorhandene Technologien den nötigen umfassenden Schutz verbessern könnten, es aber oft noch nicht tun. Umfassender Schutz bedeutet, in einer Organisation systematisch festzulegen, was wie genau zu schützen ist (identify/protect), rechtzeitig zu erkennen, ob und wo man angegriffen wird (monitor/detect), und zu wissen, wie im Angriffsfall zu reagieren ist (respond/recover). In der Schweiz werden Datenlecks nur in 13 Prozent der Fälle effektiv und zeitnah entdeckt. Ein solches Monitoring, also eine 24-stündige Überwachung der Datenbanken und Systeme, ist gerade für exponierte Unternehmen unerlässlich – etwa mittels eines Security Operations Center, das auch als Service bei Dritten bezogen werden kann.

Cybersicherheit ist also nicht einfach ein «Hype», sondern ein Gebot der Stunde. Gefordert sind Unternehmen, Organisationen und der Staat. Bei Unternehmen ist sie Teil der Selbstverantwortung sowie des strategischen Risikomanagements und damit Aufgabe des Verwaltungsrates. Dabei geht es nicht nur um Selbstschutz, sondern auch um Rücksicht und Verantwortung anderen gegenüber. Denn wer sich nicht genügend schützt, kann auch Dritte schädigen und von diesen zur Verantwortung gezogen werden. 60 Prozent der Hackerangriffe werden über Dritte ausgeübt. Viren etwa werden oft durch Geschäftspartner, zum Beispiel Lieferanten, ins Netz geschleust. Auch der neue europäische Datenschutzrahmen (DSGVO) verlangt eine umfassende Datensicherheit. Werden Daten gestohlen oder verfälscht, kann ein Unternehmen zur Rechenschaft gezogen werden, was neben Schadenersatzforderungen auch eine Busse zur Folge haben kann. Nicht zu unterschätzen sind zudem etwaige Reputationsschäden. Cybersicherheit sollte somit ein zentrales Thema von Geschäftsleitungen und Verwaltungsräten sein. Jede Organisation tut gut daran, einen Sicherheitsverantwortlichen (CISO) zu bestellen. Dieser sollte direkt der Geschäftsleitung oder sogar dem Verwaltungsrat rapportieren, denn er muss unabhängig auf etwaige Schwachstellen im Unternehmen hinweisen können.

Staat soll koordinieren

Da es um die Sicherheit von Wirtschaft und Gesellschaft geht, ist aber auch der Staat herausgefordert. Doch welche Rolle kommt ihm zu? Militärische Cyberdefence und die Cyberstrafverfolgung sind unbestrittenermassen Teil des Gewaltmonopols und damit staatliche Aufgaben. Es stellt sich aber die Frage, ob und wie der Staat die Cybersicherheit in der Wirtschaft vorschreiben beziehungsweise steuern soll.

In der EU trat im August 2016 die Richtlinie über Netz- und Informationssicherheit in Kraft. Sie enthält Sicherheitspflichten für Betreiber kritischer Infrastrukturen und digitaler Dienste, einschliesslich einer Meldepflicht bei sicherheitsrelevanten Ereignissen. Die Mitgliedstaaten sind verpflichtet, solche Unternehmen zu identifizieren und nationale Behörden als Anlaufstelle bereitzustellen. Im Dezember 2018 hat die EU zudem die Cybersecurity Act verabschiedet. Damit soll einerseits die Cybersicherheitsagentur Enisa gestärkt und andererseits ein europäisches Zertifizierungssystem geschaffen werden. Die Schweiz ist in diesem Bereich weit weniger dirigistisch und setzt derweil auf Selbstverantwortung und Kooperation. Am 18. April 2018 hat der Bundesrat die mit der Wirtschaft, den Kantonen und den Hochschulen überarbeitete Nationale Strategie zum Schutz vor Cyberrisiken (NCS) für die Jahre 2018–2022 verabschiedet. Sie ist zwar noch wenig verbindlich, doch werden breit angelegte Handlungsfelder definiert und zahlreiche Massnahmen empfohlen, so auch die Evaluation branchenspezifischer Mindeststandards, die Einführung einer Meldepflicht von Vorfällen und die Sensibilisierung der Öffentlichkeit. Zu begrüssen ist, dass sich die NCS nun verstärkt auch an KMU und die Bevölkerung richtet. In organisatorischer Hinsicht gab der Bundesrat Ende Januar den Startschuss für ein Kompetenzzentrum Cybersicherheit unter strategischer Leitung eines Delegierten für Cyberfragen, der direkt Bundespräsident Ueli Maurer, dem Vorsteher des Eidgenössischen Finanzdepartements, unterstellt ist. Operativ soll das Zentrum auf der etablierten Melde- und Analysestelle Informationssicherheit (Melani) aufbauen.

Unternehmen in der Pflicht

Eine sinnvolle Massnahme wären minimale Sicherheitsstandards, die nach Grösse der Unternehmen beziehungsweise nach Branchenzugehörigkeit variieren können und unter Einbezug der Verbände erarbeitet werden sollten. Das Bundesamt für wirtschaftliche Landesversorgung (BWL) hat Ende 2018 einen nützlichen Minimalstandard zur Verbesserung der IKT-Resilienz herausgegeben, der konkrete Massnahmen zum Schutz vor Cyberattacken empfiehlt. Dieser richtet sich als Empfehlung an die Betreiber von kritischen Infrastrukturen, er kann und sollte aber auch von anderen Marktteilnehmern herangezogen werden. Ein weiterer sinnvoller Schritt wäre eine Zertifizierung für die geleisteten Sicherheitsvorkehrungen. Ein solches «Cyberlabel» würde einerseits Transparenz schaffen, andererseits wäre es auch Motivation, das Nötige zum Schutz der eigenen Organisation zu unternehmen – ganz nach dem Grundsatz: Selbstverantwortung statt staatlicher Interventionismus. Aber auch der Staat steht nun in der Verantwortung und muss seine lenkende und koordinierende Rolle effektiv wahrnehmen. Zum Schutz von Rechtsgütern, Wirtschaft und Gesellschaft.

Marc Furrer ist Partner bei Monti Stampa Furrer & Partner, ehemaliger Direktor des Bakom und ehemaliger Präsident der Comcom. **Matthias Amgwerd** ist Partner bei Burkhalter Rechtsanwälte. Beide beschäftigen sich mit Cybersicherheit und Datenschutz.

Aus der Lehre und aus der Praxis

zz. · An dieser Stelle erhalten Juristen jeweils die Gelegenheit, einen Gastbeitrag zu verfassen. Mit der vor kurzem lancierten Rubrik «Recht und Gesellschaft» will die NZZ Themen des Rechts mehr Raum geben und Juristen aus der Praxis, aber auch aus der Lehre eine Plattform bieten. Beleuchtet werden aktuelle Rechtsfragen, ein juristisches Problem, ein rechtlicher Missstand oder schlicht Themen, die sich an der Schnittstelle zwischen Recht und Gesellschaft bewegen. Auch Nichtjuristen sollen sich von den Beiträgen angesprochen fühlen. Die neue Rubrik erscheint zweimal im Monat. Sie finden die Beiträge auch im Internet.