Cyberrisiken

in Gegenwart und Zukunft. Steigende Digitalisierung rückt Cybersecurity immer stärker in den Fokus

Mag. Monika Schuh
Industriellenvereinigung Österreich
DI Dr. Michael Fuchs, MBA
Wiener Landesfeuerwehrverband, Feuerwehr Katastrophenhilfsdienst Wien

Information und Informationstechnologie ist seit jeher zentraler Bestandteil unseres wirtschaftlichen und gesellschaftlichen Lebens. Breitband, Industrie 4.0, ACTA, Cybercrime und Social Networks sind Begriffe, die kaum zwanzig Jahre alt sind, für unsere volkswirtschaftliche Entwicklung und den Standort Österreich aber eine zentrale Bedeutung erlangt haben.

Die Grundlagen unseres heutigen Wohlstandes wären ohne tragfähige und ökonomisch leistbare Informationstechnologie nicht denkbar. „Information Technology" hat die Verbreitung und Verarbeitung von Innovation, Wissenschaft und Know-How erst ermöglicht und somit das Fundament geschaffen, auf dem die Industrie bzw. unser Wirtschaftssystem aufgebaut werden konnte. Jedes Industrieprodukt, das heute produziert wird, ist Ausdruck einer Idee, die lange vor der tatsächlichen Fertigung des Gegenstandes als CAD (Computer Animated Design) Zeichnung in einem Computer, als digitales Gebilde aus Nullen und Einsen entstanden ist. Eine Idee, die per E-Mail oder auf USB-Datenträgern hunderte oder tausende Male verschickt, weiterentwickelt und virtuell getestet wurde und dabei eine Spur quer durch die globalisierte, digitale Welt gezogen hat. Die Datenmenge, die bei Planung, Produktion, Betrieb und Überwachung von Maschinen entsteht, ist gigantisch und stellt alles bisher Dagewesene in den Schatten. Ein moderner Computertomograph zeichnet in einem Betriebsjahr mehr Daten auf, als in allen produzierten Büchern des Jahres 1800 niedergeschrieben waren. Im Laufe einer Stunde werden weltweit mehr Informationen generiert, als in allen jemals gedruckten Büchern enthalten waren. In den nächsten sechs Jahren soll sich die weltweit gespeicherte Menge digitaler Daten nochmals um das Vierzig- bis Fünfzigfache erhöhen (Quelle: Siemens, 2014). In dieser Menge von Einsen und Nullen steckt ein unglaubliches Wissen, das insbesondere für die europäische Industrie große Perspektiven eröffnet: eine digitale Revolution, die alle Wirtschaftsbereiche umfassend verändern wird. Die „Informatisierung" der Wirtschaft wird weiter voranschreiten und zu einem möglichen Paradigmenwechsel der Wertschöpfung führen, vor allem im Zusammenhang mit den Entwicklungen zu Industrie 4.0. Die Wettbewerbsfähigkeit der Industrie wird dabei maßgeblich von einer leistungsfähigen und zukunftsfähigen Informations- und Kommunikationstechnologie bestimmt.

Neben dem Aufbau weitreichenderer Strukturen und einer grundsätzlichen Erhöhung der Komplexität ist aber auch das gänzliche Ineinanderfließen oder jedenfalls teilweise Verschränken von aus technischen Gründen oder auch aus solchen der Risikominimierung historisch getrennten Netzstrukturen bzw. -ebenen ein Zug der Zeit. So ist die zwar weiterhin anzustrebende, möglichst strikte Trennung der für die Elektrizitätsversorgung notwendigen Stromnetz-IT von der Business-IT immer schwerer aufrechtzuerhalten. So benötigen etwa Abrechnungssysteme Verbrauchsdaten von der operationalen IT der Energieversorger.

Auch eine Digitale Evolution ist nicht nur einseitig

Parallel zur wachsenden technischen Komplexität, die mit diesen grundsätzlich positiven Visionen einhergeht, verändert sich auch das Umfeld jener, die die allgegenwärtige Konnektivität nutzen, um damit Schaden anzurichten. Bereits jetzt zeichnet sich ab, dass Täter im Cyberspace mehr Zeit und Sorgfalt darauf verwenden, die anzugreifenden Ziele umfassend aufzuklären und gezielt nach technischen und menschlichen Schwachstellen zu suchen. Dabei können Cybertäter auf professionelle „Dienstleister" zurückgreifen und es stehen diesem Kreis auch immer anspruchsvollere und leistungsfähigere technische Infrastrukturen zur Verfügung.

Innovation und Qualifikation als Teil der Lösung
Verändert sich das Bild der Risiken und Gefahren im Cy-

berspace der Zukunft, so wirkt sich das auf die Anforderungen an die Sicherheitslösungen aus. Diese müssen immer stärker die organisations- und prozessübergreifende Zusammenarbeit berücksichtigen. Adäquate Sicherheitslösungen für die Cybersicherheit von morgen entstehen daher nur in einem neuen Ökosystem, in dem Nutzer, Entwickler, Anbieter und der Staat eng und vertrauensvoll zusammenarbeiten. Risikofreude, eine ausgeprägte Bereitschaft zu Experimenten und hohe Leistungsfähigkeit sind einige der Eigenschaften der Akteure dieses neuen Ökosystems. Diese Eigenschaften müssen gefördert werden, damit aus Ideen marktfähige Produkte entstehen, die sich im internationalen Wettbewerb behaupten können.

Cyberattacken, die den Kern unserer innovativen Industrie treffen, verursachen finanzielle und qualitative Schäden und können die Existenzen von Betrieben bedrohen. 31 % aller österreichischen Unternehmen waren schon einmal Opfer von Wirtschafts- und Industriespionage, wobei ein geschätzter Schaden von hochgerechnet 880 Mio. Euro entstand. Besonders betroffen sind die Sparten Gewerbe und Handwerk, sowie die Industrie – hier ereigneten sich mehr als 50 % der verzeichneten Vorfälle. Aber auch Cyberangriffe auf fundamentale Infrastrukturen unserer Gesellschaft, wie Stromversorgung, Wassernetz oder Luftraumkontrolle, stellen eine reale Bedrohung dar. Ein einziger 48-stündiger Stromausfall verursacht Schäden in Höhe von 1,7 Mrd. Euro, aber auch kurzfristige Ausfälle sind für Betriebe und die Industrie ein Problem. Mit zunehmend intelligenteren Netzen, bei denen nicht nur Umweltinformationen mittels Sensoren gesammelt werden, sondern auch aktiv eingegriffen wird (Kraftwerkssteuerung, Verkehrssteuerung, etc.), verstärken sich die potenziellen Folgen von Cyberattacken erheblich. Vor dieser Gefahr erheben auch immer mehr internationale Experten mahnend ihre Stimme. Exemplarisch sei hier nur der mehrfach ausgezeichnete IT-Sicherheitsexperte Eugene Kaspersky genannt, auf dessen Aussagen im Zuge eines Executive-Briefing zum Thema Cybersecurity der Industriellenvereinigung im Haus der Industrie 2014 einige der hier dargestellten Überlegungen fußen.

Zukünftiger ordnungspolitischer Rahmen

Die heute bestehenden regulatorischen Rahmenbedingungen in Österreich sind grundsätzlich bereits gut ausgebildet und angemessen. Es gilt, aus regulatorischer Sicht primär Anreize zu setzen, denn nur so kann die essentielle Innovationskraft der Unternehmen aktiviert werden. Technologievorsprung durch eben diese Innovationskraft erscheint auch als einzig wirksame, aber neu auszubauende Abwehrmaßnahme. Eine gerade aus ordnungspolitischer Sicht zu beantwortende Frage ist jene der Angemessenheit des notwendigen Regulativs. Im Rahmen der festzulegenden Niveaus der Cybersicherheit muss man sich darüber verständigen, welche Schutzziele angestrebt werden:

- Was muss gewährleistet sein?
- Wie lange wird – gesellschaftlich und wirtschaftlich – ein Ausfall welcher Leistungen verkraftet?
- Was wird heute schon getan, und was muss man in Zukunft tun, um erkannte Lücken bei der Sicherheitsvorsorge im Cyberspace zu schließen?

Das sind einige der Fragen, die es durch Staat und Unternehmen gemeinsam zu beantworten gilt.

Gegenwärtig wird vor diesem Hintergrund eine Zielsetzung diskutiert, noch in der laufenden Legislaturperiode einen Vorschlag für ein modernes Cybersicherheitsgesetz auszuarbeiten. Eine österreichische Insellösung ist nicht zielführend, eine Kohärenz mit international bereits existierenden Standards ist jedenfalls sicherzustellen, um Doppelgleisigkeiten und Wettbewerbsnachteile zu vermeiden.

Cybersicherheit kann nur in einem umfassenden Ansatz verfolgt werden. Die Erarbeitung eines künftigen Cybersicherheitsgesetzes kann daher nur unter intensiver Einbindung aller relevanten Stakeholder, insbesondere der Industrie, erfolgreich sein. Österreichs Industrie ist bereit und willens, Verantwortung zu tragen und die notwendigen Schritte für mehr Cybersecurity aktiv und in enger Abstimmung mit den Behörden voranzutreiben.

Factbox:

- Institutionalisierte und professionelle Cyberkriminalität
- 31 % aller österreichischen Unternehmen waren schon einmal Opfer von Wirtschafts- und Industriespionage
- geschätzter Schaden hochgerechnet 880 Mio. Euro