**Cyber-Sicherheit als Gemeinschaftsaufgabe – wo stehen wir heute und welche Herausforderungen gilt es zu bewältigen?**

**Arne Schönbohm**

Wenn wir heute von Digitalisierung sprechen, müssen wir uns eines sehr klar machen. Wir befinden uns erst am Anfang einer Ära der Digitalisierung, die unseren Alltag und unsere Gesellschaft umfassend beeinflussen wird. Leistungsfähige, zuverlässige und sichere Kommunikationssysteme entwickeln sich immer mehr zum zentralen Nervensystem der Gesellschaft im 21. Jahrhundert. Kaum ein Bereich kommt ohne sie aus. Sie sind essenziell für einen modernen und transparent agierenden Staat, eine funktionierende Wirtschaft und für viele weitere Bereiche unserer eng vernetzten Gesellschaft. Aber sie machen den Menschen auch immer abhängiger davon, dass diese Systeme einwandfrei funktionieren.

Ihr Potenzial ist nahezu unbegrenzt: In diesem Jahr werden weltweit rund 1,3 Millionen Industrieroboter miteinander kommunizieren und kooperieren. Im Internet der Dinge werden bis 2020 schätzungsweise 50 Milliarden Endgeräte interagieren. Diese rasante technologische Entwicklung der letzten Jahre und das ebenso dynamische Fortschreiten der Digitalisierung aller Lebensbereiche von Smart Home bis zu Industrie 4.0 eröffnen Staat, Wirtschaft und Gesellschaft enorme Chancen. Damit einher gehen aber auch neue und immer komplexere Herausforderungen in Sachen Informationssicherheit, denen einzelne Unternehmen oder Organisationen letztlich nicht mehr allein wirksam entgegentreten können.

Wie der aktuelle Bericht des BSI zur Lage der IT-Sicherheit in Deutschland[1] zeigt, stellt sich die allgemeine Gefährdungslage hierzulande vielschichtig dar und bleibt weiterhin auf hohem Niveau angespannt. Nicht nur bleiben die bekannten Einfallstore für Cyber-Angriffe wie Sicherheitslücken in Softwareprodukten, Malware oder Phishing unverändert kritisch bestehen. Bedingt durch das rasante Fortschreiten der Digitalisierung und die damit einhergehende zunehmende Vernetzung entsteht zudem eine ganz neue Qualität der Gefährdung. Mit WannaCry und NotPetya hat es im vergangenen Jahr Angriffe mit enormen wirtschaftlichen Schadensausmaß gesehen. Hardware-Schwachstellen, etwa in Computer-Chips, betreffen praktisch jeden einzelnen Computer, sind nicht hundertprozentig patchbar und werden daher einen Austausch der Geräte über einen langen Zeitraum nötig machen. Angriffe auf Kritische Infrastrukturen wie Energieversorger oder Bundeseinrichtungen wie das Auswärtige Amt sind hochspezialisiert und schüren Angst vor Worst-Case-Szenarien. Diese Kombination der neuen Angriffsqualität und der zunehmenden Digitalisierung hebt die Gefährdungslage auf ein neues Niveau und erschüttert die Grundfesten der IT-Sicherheitsarchitektur.

IT-Sicherheit ist damit eines der zentralen Themen der Informations- und Kommunikationstechnologie geworden – gerade in einem Hochtechnologieland wie Deutschland. Es ist höchste Zeit umzudenken. Wenn es auch in Zukunft einen starken und sicheren Standort Deutschland geben soll, sollte mehr in Informations- und Cyber-Sicherheit investiert werden. Die IT-Sicherheit von Produkten und Dienstleistungen darf keine nachlässig ausgeführte Pflichtübung, sondern muss durch „Security by design“ und „Security by default“ von vornherein gewährleistet

1 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

sein. Wir brauchen eine mit der Wirtschaft abgestimmte Entwicklung von Sicherheitsstandards für die IT-Strukturen und den Schutz der Kritischen Infrastrukturen. Deutschland muss in dieser Frage eine Vorreiterrolle einnehmen. So wird Digitalisierung made in Germany ein Erfolgsmodell mit Vorbildcharakter für die internationale Gemeinschaft.

Angesichts der zunehmenden Komplexität von Angriffsmethoden und der Professionalisierung der Angreifer wird es für einzelne Akteure immer schwieriger, wirksame Sicherheitskonzepte zu entwickeln und umzusetzen. Damit die Erhöhung der Cyber-Sicherheit am Standort Deutschland gelingen kann, ist ein kooperativer Ansatz gefordert, der Anwender in der Wirtschaft, IT-Hersteller und Cyber-Sicherheitsexperten aus IT-Branche und Forschung an einen Tisch bringt. Das BSI als nationale Cyber-Sicherheitsbehörde nimmt diesen Auftrag gerne an und lebt ihn intensiv. Das BSI verfügt schon heute auf Basis seiner technisch tiefgehenden Expertise über eine integrierte Wertschöpfungskette von der Cyber-Abwehr über die Beratung und Entwicklung sicherheitstechnischer Lösungen bis hin zur Standardisierung und Zertifizierung. Mit der Allianz für Cyber-Sicherheit oder dem UP-KRITIS hat das BSI zudem äußerst erfolgreiche Kooperationsplattformen geschaffen, über die sich kleine und große Unternehmen, Kommunen, Institutionen und Organisationen genauso wie Betreiber Kritischer Infrastrukturen zur IT-Sicherheit austauschen und von der Expertise des BSI und der zahlreichen weiteren Teilnehmern profitieren. Auch zu den prägenden Themen der digitalisierten Zukunft bringt das BSI die handelnden Akteure an einen Tisch und gestaltet dabei die Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung. Themen wie 5G, das maschinelle Lernen, die smarte Energiewende, Quantencomputing und vieles mehr werden beim BSI von Anfang an und in enger Zusammenarbeit mit Partnern aus Staat, Wirtschaft und Gesellschaft sicher entwickelt. Auch das IT-Sicherheitsgesetz, das 2015 beschlossen wurde, führte in einer gemeinsamen Anstrengung mit den Betreibern Kritischer Infrastrukturen zu einer Erhöhung des IT-Sicherheitsniveaus am Standort Deutschland. Das intakte Vertrauensverhältnis zwischen dem BSI und den KRITIS-Betreibern sorgt für einen engen und intensiven Austausch, der zu einem aktuellen Lagebild und einer schnellen Umsetzung von Hilfestellungen und Empfehlungen. Auch aus diesem Grund wird das Erfolgsmodell IT-Sicherheitsgesetz derzeit fortgeschrieben und künftig voraussichtlich auf weitere Unternehmen und Branchen ausgeweitet. Für Bürger und Verbraucher setzt sich das BSI ebenfalls ein. Sie profitieren nicht nur vom hohen Sicherheitsniveau der Kritischen Infrastrukturen und der damit gewonnenen Versorgungssicherheit. Über www.bsi-für-bürger.de und über die Service-Hotline unter 0800 2741000 stehen den Anwenderinnen und Anwendern auch zahlreiche Hilfestellungen und leicht verständliche Empfehlungen zur Verfügung, die eigene Cyber-Sicherheit nochmals deutlich zu erhöhen. Künftig wird auch ein IT-Sicherheitskennzeichen die IT-Sicherheitseigenschaften von Endgeräten transparent machen, so dass die Sicherheitsaspekte schon bei der Kaufentscheidung berücksichtigt werden können. So stärkt das BSI auch den digitalen Verbraucherschutz.

Der Dreiklang der Digitalisierung, der zunehmenden Vernetzung und der extrem hohen Innovationsgeschwindigkeit macht es dabei umso wichtiger, dass es auch in Zukunft für das Thema Informationssicherheit einen zentralen Ansprechpartner gibt. Behörden, Unternehmen und Organisationen müssen wissen, wer die zentrale Stelle für Cyber-Sicherheit in Deutschland ist: die nationale Cyber-Sicherheitsbehörde, das BSI. Aus diesem Selbstverständnis heraus gestalten wir auch in Zukunft die Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft.

**Zum Autor:** Dipl.-Betriebswirt Arne Schönbohm ist Präsident des Bundesamtes für die Sicherheit in der Informationstechnik