# Kritische Infrastrukturen

Cybersicherheit ist Voraussetzung für den Erfolg der Digitalisierung

**ARNE SCHÖNBOHM**
Geboren 1969 in Hamburg, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Die Digitalisierung hat mittlerweile fast alle Bereiche unseres Lebens erreicht. In der Verwaltung und in den Dienstleistungsbranchen arbeiten wir bereits heute IT-gestützt und hochgradig vernetzt. Industrie 4.0 umschreibt die grundlegenden Veränderungen im Produktionsbereich. Smart Home, Mobile Work, E-Health und Entwicklungen wie selbstfahrende Autos sind weitere Beispiele für die fortschreitende Digitalisierung, die Chancen eröffnet, aber auch Risiken beinhaltet. Cybersicherheit wird dabei zum wesentlichen Erfolgsfaktor.

Die Digitalisierung ist zu einer wichtigen Grundlage für technologischen Fortschritt sowie wirtschaftlichen und gesellschaftlichen Wohlstand geworden. Die Digitalisierung erschließt erhebliche gesellschaftliche und volkswirtschaftliche Vorteile, beinhaltet aber auch, dass wir immer mehr sensible Prozesse vernetzten IT-Systemen überantworten, bis hin zu autonomen Fahrzeugen und lebenswichtigen Einrichtungen der Daseinsvorsorge.

Besondere Herausforderungen entstehen im Bereich der Prävention, Detektion und Abwehr digitaler Angriffe, die zunehmend professionalisiert durchgeführt

werden. Digitalisierung, Vernetzung und zunehmende Komplexität der IT bieten Cyberangreifern weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Im Fokus der Cyberangriffe stehen dabei Unternehmen und Kritische Infrastrukturen ebenso wie Verwaltung, Forschungseinrichtungen und Bürger.

## ANGRIFFE DURCH RANSOMWARE

Im Jahr 2016 wurden die IT-Systeme von Unternehmen, Kommunen und Kritischen Infrastrukturen wie Krankenhäusern verstärkt und erfolgreich mit Ransomware angegriffen. Ransomware ist eine Malware, die Computer infiziert, sperrt und Geld dafür verlangt, diese wieder zu entsperren. Die Täter waren in der Lage, Dateien zu verschlüsseln, und versuchten, die Betroffenen zu erpressen. Einer Umfrage des BSI zur Betroffenheit der deutschen Wirtschaft von Ransomware zufolge war jedes dritte befragte Unternehmen (32 Prozent) von Ransomware betroffen. Die Auswirkungen waren zum Teil erheblich: Während siebzig Prozent der Unternehmen angaben, dass einzelne Arbeitsplatzrechner befallen waren, kam es in jedem fünften Unternehmen (22 Prozent) zu einem erheblichen Ausfall von Teilen der IT-Infrastruktur, elf Prozent der Betroffenen erlitten einen Verlust wichtiger Daten.

Die Vorfälle mit Ransomware sind nach wie vor hochaktuell und haben deutlich gemacht, wie verwundbar unsere digitalisierte Gesellschaft ist. Dabei sind Angreifer den Verteidigern von IT-Systemen häufig einen Schritt voraus. Sie können ihre Ziele über das Internet einfach erreichen und nutzen viele Methoden, die Angriffswege zu verschleiern. Zudem bietet die heutige Informationstechnik aufgrund ihrer Komplexität zahlreiche potenzielle Angriffspunkte. Die Täter nutzen nicht nur neue und bislang unbekannte Schwachstellen aus, sondern schlagen auch Kapital daraus, dass Updates und Patches von den Anwendern in der Praxis häufig verspätet eingespielt werden.

Das Bundesamt für Sicherheit in der Informationstechnik muss zudem feststellen, dass die Bedrohung für Staat und Wirtschaft durch professionelle und vermutlich staatlich gelenkte Angreifergruppen weiterhin hoch ist. Die einschlägigen Beispiele illustrieren die politische Dimension und Wirkrichtung der Cyberangriffe. Neben dem Angriff auf die IT-Systeme des Deutschen Bundestages 2015 hat das BSI auch Cyberangriffe auf Parteien, Medien und staatliche Einrichtungen beobachtet, die die Sorge vor einer gezielten Manipulation der öffentlichen Meinung durch Dritte begründen.

Das BSI beobachtet die Lage diesbezüglich intensiv und wird sich für den Zeitraum der Bundestagswahl 2017 in besonderer Weise aufstellen, um möglichen Cyberangriffen begegnen zu können. So optimieren wir ständig die Verteidigungsfähigkeit des Bundesnetzes und tauschen uns auch mit anderen europäischen Ländern aus, in denen demnächst Wahlen sind. Darüber hinaus unterstützt das BSI den Bundeswahlleiter, den Deutschen Bundestag und die politischen Parteien. Auf Wunsch stellen wir Informationen über Risiken, Angriffsformen und Schutzmaßnahmen zur Verfügung und beraten

bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen, insbesondere zur Härtung von IT-Systemen und IT-Netzen.

## NATIONALES CYBER-ABWEHRZENTRUM

Das BSI hat über Jahre hinweg, unter anderem durch die Verantwortung für den Schutz der Netze der Bundesverwaltung, Kompetenzen bei der Prävention, Detektion und Reaktion auf komplexe Cyberangriffe und IT-Sicherheitsvorfälle aufgebaut und unter Beweis gestellt. Diesen Wissensvorsprung stellen wir anderen staatlichen Stellen zur Verfügung, auch in den Ländern.

Wichtiger Baustein der behördenübergreifenden Zusammenarbeit bei der Analyse von IT-Sicherheitsvorfällen und der Abwehr von Cyberangriffen ist das Nationale Cyber-Abwehrzentrum (Cyber-AZ). Es wurde im Jahr 2011 eingerichtet, um den Informationsaustausch zwischen den relevanten Behörden zu verbessern. Das Cyber-AZ ist beim Bundesamt für Sicherheit in der Informationstechnik angesiedelt, also bei der für Cybersicherheit zuständigen nationalen Sicherheitsbehörde, der durch das Bundesinnenministerium die Federführung übertragen wurde.

In den vergangenen Jahren hat sich das Cyber-AZ von einer reinen Informationsdrehscheibe zu einer Kooperationsplattform weiterentwickelt, in der die operativen Tätigkeiten der einzelnen Behörden koordiniert werden. Bundesinnenminister Thomas de Maizière hat vorgeschlagen, das Cyber-AZ so weiterzuentwickeln, dass es bei komplexen Schadenslagen die Einsatzführung an sich ziehen kann, um etwa die schnellen Eingreiftruppen anderer Sicherheitsbehörden, gegebenenfalls auch der Bundeswehr, zu koordinieren. Das BSI unterstützt diesen Vorschlag und wird sein Lagezentrum personell noch einmal deutlich verstärken, um rund um die Uhr die Bewältigung dieser neuen Aufgabe sicherstellen zu können.

Durch das IT-Sicherheitsgesetz von 2015 wird die Rolle des BSI als zentrale Stelle für die Belange der Cybersicherheit vor allem gegenüber der Wirtschaft gestärkt. Mit der Übertragung von mehr Verantwortung und Kompetenzen durch die Erweiterung der bisherigen operativen Aufgaben wächst aber auch die Verpflichtung des BSI, dieser Verantwortung gerecht zu werden. Als die nationale Cyber-Sicherheitsbehörde gestalten wir deshalb die Digitalisierung in Staat, Wirtschaft und Gesellschaft mit einem ausgeprägten kooperativen Ansatz. Den strategischen Rahmen für mehr Sicherheit im Cyberraum setzt dabei die neue Cyber-Sicherheitsstrategie der Bundesregierung. Wir wollen ein sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt ermöglichen. Dafür müssen Staat und Wirtschaft zusammenarbeiten und muss Deutschland auch weiterhin eine aktive Rolle in der europäischen und internationalen Cyber-Sicherheitspolitik einnehmen.

## „MOBILE INCIDENT RESPONSE TEAMS“

Im Bereich der Kritischen Infrastrukturen (KRITIS) kooperiert das BSI im Rahmen einer Öffentlich-Privaten-Partnerschaft unter dem Titel UP KRITIS mit den Betreibern in gefährdeten Sektoren, wie zum

Beispiel Energie, Gesundheit, Ernährung und Wasser. Zentrales Ziel des UP KRITIS mit seinen rund 400 Mitgliedern ist es, die Versorgung mit lebensnotwendigen Dienstleistungen auch im Zeitalter der Digitalisierung möglichst uneingeschränkt aufrechtzuerhalten. Um Bundesbehörden und Kritische Infrastrukturen vor Ort bei der Bewältigung und Analyse von IT-Sicherheitsvorfällen unterstützen zu können, baut das BSI derzeit „Mobile Incident Response Teams" (MIRT) auf.

Im Rahmen der Allianz für Cybersicherheit (www.allianz-fuer-cybersicherheit.de), der mehr als 2.000 Institutionen angehören, aber auch bilateral, treibt das BSI die Zusammenarbeit mit der Wirtschaft voran. Dazu gehört ein intensiver Austausch über Bedrohungen und Schutzmaßnahmen, dazu gehört die Meldung von IT-Sicherheitsvorfällen an das BSI, dazu gehört aber auch die Warnung vor Angriffen und die Erarbeitung praxisorientierter Handlungsempfehlungen, die das BSI der Wirtschaft zur Verfügung stellt. Vor dem Hintergrund der Ransomware-Vorfälle hat das BSI entsprechende Hinweise und Empfehlungen einer Vielzahl von Krankenhäusern zur Verfügung gestellt. Ziel dieser Maßnahmen ist es, die Widerstandsfähigkeit des Standortes Deutschland, insbesondere die der kleinen und mittelständischen Unternehmen, gegenüber Cyberangriffen zu stärken.

In den großen Digitalisierungsprojekten in Deutschland bringt sich das BSI verstärkt ein und wird übergreifend für staatliche und private Akteure im Sinne der Gewährleistung der Sicherheit tätig. So leisten wir unseren Beitrag zum Gelingen der Energiewende durch die Erarbeitung von Sicherheitskriterien für die Infrastruktur der intelligenten Stromzähler und unterstützen bei der Erarbeitung der Sicherheitsaspekte einer Verkehrsinfrastruktur, in der autonome oder hochautomatisierte Fahrzeuge Realität werden. Darüber hinaus hat das BSI die wesentlichen Sicherheitsanker der elektronischen Gesundheitskarte und der dazu notwendigen Systeme mitgestaltet und zertifiziert.

Die Angebote und Maßnahmen des BSI entlassen jedoch die Wirtschaft nicht aus ihrer Verantwortung, die Cybersicherheit für Unternehmen und deren Kunden zu verbessern und die eigenen Maßnahmen zur Prävention und Sensibilisierung auszubauen. Das BSI steht bereit, um bei der Gestaltung der einzelnen Maßnahmen zu unterstützen.

Die durch die Digitalisierung angestoßenen Entwicklungen sind durchgreifend und werden Deutschland verändern. Die Frage der Sicherheit der eingesetzten Informationstechnik stellt sich damit nicht mehr nur nebenbei. Sie stellt sich auch nicht länger nur einem eingeweihten Kreis der IT-Spezialisten. Vielmehr ist die Informationssicherheit eine wesentliche Vorbedingung für das Gelingen der Digitalisierung in Deutschland geworden. Das BSI stellt sich weiterhin der Aufgabe, die Informationssicherheit zu gestalten und so zum Erfolg der Digitalisierung in Staat, Wirtschaft und Gesellschaft beizutragen.