Cybersecurity

Von größter Bedeutung für die deutsche Wirtschaft

Von Prof. Dr. Stefan Goertz, Lübeck[1]

1 Einleitung

Deutsche Wirtschaftskonzerne wurden im zweiten Halbjahr 2019 mutmaßlich von chinesischen Hackern ausgespäht. Dabei wurden mindestens acht deutsche Unternehmen angegriffen, darunter sechs Dax-Konzerne. Unter den genannten Firmen sind unter anderen BASF, Siemens und Henkel. Anfang April 2019 hatte der Chemie-Riese Bayer bestätigt, Opfer einer Cyber-Attacke gewesen zu sein.[2] Mehrere Dax-Konzerne, darunter auch BASF und Bayer, gründeten im Oktober 2016 die Deutsche Cybersicherheitsorganisation (DCSO), um sich im Kampf gegen Cyberkriminelle auszutauschen.
Trotz zahlreicher öffentlich gewordener Fälle von Cyber-Attacken gegen deutschen Firmen scheint in Deutschland nach wie vor eine gewisse Sorglosigkeit beim Thema Cybercrime und Cyber-Attacken zu herrschen. In einer Anfang Juli 2019 veröffentlichten Erhebung der Wirtschaftsprüfungsgesellschaft KPMG unter rund 1000 Unternehmen gaben 39% an, in den vergangenen zwei Jahren von Computerkriminalität betroffen gewesen zu sein. 85% der betroffenen Unternehmen wüssten nicht, wer hinter den Angriffen stecke. Sie seien damit nicht in der Lage, Angriffe effektiv zu verfolgen und aufzuklären. Damit gehe auch die Gefahr einher, dass Delikte unentdeckt blieben.[3]Durch das Eindringen in Informations- und Kommunikationssysteme durch Cyber-Attacken kann die deutsche Wirtschaft stark geschädigt werden, sowohl finanziell als auch im Sinne eines Vertrauensverlustes.
Dieser Beitrag untersucht einführend die Definition von und den Phänomenbereich Cybersecurity. Dann folgt eine aktuelle Lageanalyse von *„Cybersecurity und deutsche Unternehmen“*. Das Kapitel vier geht auf aktuelle Bedrohungen für die Cybersecurity nach Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein. Abschließend wird im Kapitel fünf ausführlich die *„aktuelle Gefährdungslage Wirtschaft und Kritische Infrastrukturen“* untersucht.

2 Definition und Phänomenbereich

Das Bundesamt für Sicherheit in der Informationstechnik definiert Cybersecurity wie folgt: *Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.*[4]

Wegen der Omnipräsenz von W-LAN und von intelligenten Geräten wie Smartphones, Lautsprechersäulen und Wearables, der Vernetzung von Geräten und Systemen, im Zusammenhang des Internets der Dinge und von Cloud Computing, sowie der Verbreitung von Robotern und KI-Systemen, die mit Menschen und Maschinen interagieren und kommunizieren, ist Cybersecurity aktuell und zukünftig eines der wichtigsten technologischen Themen, bei dem in der Konsequenz durch Cyberkriminalität viele Milliarden Euro verloren werden können.[5] IT-Konzepte, IT-Richtlinien und IT-Maßnahmen sowie spezielle Soft- und Hardware sind Mittel von Cybersecurity und helfen dabei, Systeme und Daten zu schützen. Der Schwerpunkt von

Cybersecurity ist hierbei der unerwünschte bzw. unerlaubte physische Zugriff auf die Hardware sowie der Zugriff auf Hard- und Software über Netzwerke und Schadsoftware durch Hacker bzw. Unbefugte.[6]

3 Cybersecurity und deutsche Unternehmen – Eine aktuelle Lageanalyse

Für deutsche Unternehmen summiert sich der durch Cyberkrimininalität entstandene Schaden inzwischen auf über 100 Milliarden Euro jährlich, eine Verdoppelung gegenüber 2017.[7] Die Zahl der Angriffe auf die Produktionsanlagen deutscher Maschinen- und Anlagenbauer nahm im Jahr 2019 besonders stark zu. Der Leiter *Competence Center Industrial Security* des Branchenverbandes Verband deutscher Maschinen- und Anlagenbau (VDMA) erklärt dazu: *„Unsere Umfragen zeigen, dass bereits mehr als ein Drittel der vom VDMA befragten Mitglieder von Produktionsausfällen betroffen waren. Kapitalschäden verzeichnen bereits die Hälfte der befragten Unternehmen“*[8].
Im April und Juli 2019 gab es beispielsweise Cyber-Attacken auf Bayer, BASF, Covestro und Henkel, allesamt Dax-Konzerne mit mehreren Zehntausend Mitarbeitern. Besonders von Cyber-Attacken betroffen ist allerdings der deutsche Mittelstand. Laut einer aktuellen Studie des Digitalverbands Bitkom meldeten drei von vier deutschen Unternehmen in der Größe von 100 bis unter 500 Mitarbeitern, bereits einmal Opfer von Datendiebstahl und Cyberspionage gewesen zu sein. Bei den Unternehmen mit mehr als 500 Mitarbeitern waren immerhin noch 60% der Befragten betroffen.
Allerdings liegt die Dunkelziffer sehr wahrscheinlich noch deutlich höher, denn viele deutsche Unternehmen melden, allen gesetzlichen Verpflichtungen zum Trotz, bis heute nicht jeden Cyberangriff. So ist in vielen Fällen die Sorge vor Imageschäden immer noch groß. Dass die Zahl der Angriffe auf den Mittelstand so hoch ist, ist nicht überraschend, gilt doch der deutsche Mittelstand als innovativ und eng eingebunden in die Lieferketten der großen Konzerne. Der deutsche Mittelstand ist so interessant für die Urheber von Cyber-Attacken, weil sich kleine Unternehmen in der Regel technisch weniger schützen als große Unternehmen.[9]
Das für deutsche Unternehmen seit Monaten und Jahren gestiegene Sicherheitsrisiko hat viele technische Gründe, aber auch neue EU-Regulierungen, die den Handlungsbedarf für deutsche Unternehmen noch konkreter machen. Folgenden aktuellen Entwicklungen schreibt Deloitte großen Einfluss auf die Cybersecurity und damit eine sehr hohe Relevanz für die deutsche Wirtschaft zu:

Big Data: Das Datenaufkommen in deutschen Unternehmen steigt seit Jahren rapide und betrifft betriebliche Prozesse, die immer umfassender digital erfasst, verarbeitet und archiviert werden. Durch den digitalen Footprint in internen und externen Datenbanken wächst auch die Angriffsfläche für Cyberkriminelle.

Industrie 4.0: Die digitale Revolution hat auch die Produktion in Unternehmen deutschlandweit und weltweit längst erfasst, die verarbeitende Industrie ist heute sehr komplex vernetzt. Dadurch steigt aber problematischer Weise auch die Anzahl potenzieller Einfallstore für Hacker, die signifikante Folgen haben können. Weil der Angriff von überall auf der Welt aus erfolgen kann, werden Gegenmaßnahmen und Strafverfolgung erheblich erschwert.

Internet of Things: Das Internet wird sich in der nahen Zukunft von der unmittelbaren Computernutzung lösen und an Alltagsprodukte der Nutzer andocken, vom Wearable bis zum Fahrzeug. Für Cyberkriminelle verspricht ein Eindringen in die Infrastruktur über das Internet der Dinge großes Schadenspotenzial.[10]

4 Aktuelle Bedrohungen für die Cybersecurity – Die Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Nach Angaben des BSI verschiebt sich die Cyber-Kriminalität aktuell in den Bereich der gezielten Cyber-Angriffe. Ein typisches Beispiel dafür war eine wiederholte intensive Ransomware-Kampagne Ende 2018 und Anfang 2019. Als besonders schwerwiegender Cyber-Angriff ist der Vorfall bei einem norwegischen Aluminiumlieferanten zu verzeichnen. So wurde der Konzern im März 2019 Opfer einer massiven Cyber-Attacke mit der Ransomware LockerGoga. Betroffen waren die meisten Geschäftsfelder, die Produktion musste weitgehend auf manuellen Betrieb umgestellt werden.[11]


IT-Labor einer Cybercrime-Dienststelle.

Infektionen durch Schadprogramme sind seit Jahren eine der größten Bedrohungen für die Cyber-Sicherheit, sowohl für Unternehmen als auch für Privatanwender und Behörden. Eine aktuell sehr gefährliche Malware ist Emotet. Das schon seit 2010 bekannte Schadprogramm ist seit Ende 2018 wieder vermehrt mithilfe von schädlichen Office-Dokumenten verteilt worden, aber mit immer ausgefeilteren Mechanismen, beispielsweise dem *„Outlook-Harvesting“,* sprich: der Analyse des Mailverlaufs infizierter Computer, dem Nachladen von beliebigen anderen Schadprogrammen im Kontext kooperierender und arbeitsteiliger Computerkriminalität sowie der Verwendung von Techniken, die bisher nur bei *Advanced Persistens Threats* (APTs) eingesetzt wurden.[12] Auch die Bedrohungslage durch Botnetze – Verbünde von Rechnern oder Systemen, die von einem fernsteuerbaren Schadprogramm [Bot] befallen sind – ist nach Angaben des BSI wie in den Vorjahren anhaltend hoch.
Folgende Angriffsmethoden und -mittel analysiert das BSI aktuell:

Identitätsdiebstahl: Eine häufige Form des Identitätsdiebstahls ist das sog. Phishing, zum einen durch Techniken des Social Engineerings, um das Opfer zur Herausgabe sensibler Informationen zu bewegen. Zum anderen können Identitätsdaten durch den Einsatz spezieller Schadsoftware entwendet werden. Phishing, ein englisches Kunstwort, setzt sich aus einem *„P“* für Passwort und dem Wort *„fishing“* zusammen.[13] Betroffene von wichtigen Datenabflüssen von Kundeninformationen sind aktuell einige namhafte Unternehmen, zum Beispiel die Hotelkette Marriott oder die Social-Media-Plattform Facebook.[14] Als *„Pharming“* wird die Manipulation einer Hostdatei von Webbrowsern beschrieben, um Anfragen auf gefälschte Websites umzuleiten, es handelt sich hierbei um eine Weiterentwicklung des klassischen Phishings.[15]

Schadprogramme (Malware): Schadprogramme umfassen alle Arten von Computerprogrammen, die unerwünschte oder schädliche Funktionen auf einem Computersystem ausführen können. Die Begriffe Trojaner, Viren, Würmer etc. werden in der Presse und den Medien oft synonym für alle Arten von Schadprogrammen genutzt. Schadprogramme sind fester Bestandteil der meisten Angriffsszenarien, z.B. bei der Infektion eines Clients durch Ransomware, bei der Kommunikation von Botnetzen aber auch bei APT-Angriffen. Allein im Jahr 2019 wurden von dem IT-Sicherheits-Unternehmen AV-Test insgesamt rund 114 Mio. neue Schadprogramm-Varianten registriert. Davon entfallen ca. 65 Mio. auf das Betriebssystem Windows, ca. 3,4 Mio. auf Android, ca. 0,09 Mio. auf MacOS und mehr als 39 Mio. in die Kategorie Sonstiges. Dies bedeutet im Durchschnitt ca. 320.000 neue Schadprogramme pro Tag.[16]

Ransomware: Ransomware wurde spätestens mit dem Angriff von WannaCry im Jahr 2017 der breiten Öffentlichkeit bekannt und bezeichnet Schadsoftware, die den Zugriff auf den eigenen Rechner oder die eigenen Dateien verwehrt oder einschränkt. Dies erfolgt meistens durch eine am Bildschirm eingeblendete Nachricht, manchmal ist die Mitteilung nur vorgetäuscht oder sind Einschränkungen leicht zu umgehen. Das Ziel von Ransomware ist die Zahlung eines Lösegelds (Ransom) u fordern, bevor

die Ressourcen wieder freigegeben werden. In den meisten Fällen wird die Zahlung mit einer Krypto-Währung wie Bitcoin oder Ethereum gefordert, um die Anonymität der Täter zu wahren.[17] Digitale Erpressungen können sowohl Wirtschaftsunternehmen als auch Privatpersonen betreffen und gehen meistens mit der Verwirklichung klassischer Cybercrimedelikte, wie beispielsweise Computersabotage einher.[18] Ransomware verbreitet sich durch:

- Spam-E-Mails mit Schadsoftware in Anhängen oder über URLs
- Drive-By-Exploits, Schwachstellen in Browsern, Browser-Plug-Ins oder Betriebssystemen
- Exploit-Kits

Unternehmen mit komplexerer IT-Infrastruktur können von folgenden Cyber-Attacken betroffen sein:

- Schadsoftware für das Ausspähen von Passwörtern
- Zugriff auf Systeme durch Schwachstellen in Fernwartungs-Werkzeugen (Remote Administration Tools)
- Schadsoftware tarnt sich nach der Infektion des Systems als legitimer Prozess

Im Jahr 2019 wurden verschiedene Ransom-Attacken auf Häfen, Flughäfen, Unternehmen im Logistikbereich (Container), Zeitungen und Restaurantketten gemeldet. Unter anderem gab es auch Ransom-Attacken auf deutsche Krankenhäuser.[19]

Distributed Denial of Service (DDoS): DDoS-Angriffe haben häufig zur Folge, dass Websites nicht mehr erreichbar sind, Netzwerkdienste ausfallen oder kritische Geschäftsprozesse wegen Überlastung blockiert werden. Solche DDoS-Angriffe werden von Cyberkriminellen oft genutzt, um gezielt Schaden anzurichten, ihre Opfer zu erpressen, oder Aufmerksamkeit für eine eigene Sache zu erregen, aber auch, um andere Attacken zu verschleiern oder erst zu ermöglichen. Dabei werden die Angriffe häufig mittels einer großen Anzahl von Computern, ggf. Servern, parallel durchgeführt. Die Auswirkungen von DDoS-Angriffen können erheblich sein. So können sie für die betroffenen Institutionen einen großen wirtschaftlichen Schaden verursachen und auch einen Reputationsverlust nach sich ziehen. Deutsche Unternehmen mussten laut einer Studie des Unternehmens Netscout im Jahr 2018 einen DDoS-Gesamtschaden von rund vier Milliarden Euro verzeichnen.[20]

Botnetze: Unter einem Bot versteht man Computersoftware, die weitgehend selbstständig sich wiederholende Aufgaben abarbeitet, ohne dabei mit dem menschlichen Nutzer interagieren zu müssen. Kommunizieren Bots untereinander, spricht man von einem Botnetz, die eine Gruppe von Software-Bots sind, die nach Infektion mit einer Schadsoftware von einer zentralen Einheit ferngesteuert werden. Ein sog. Botmaster kann dabei das Botnetz überwachen und Befehle ausgeben, während die eigentlichen Nutzer des infizierten Computers diese Manipulation nicht bemerken.[21] Durch die Nutzung von Botsoftware haben Cyber-Kriminelle Zugriff auf eine große Zahl von fremden Systemen (Computer, Smartphones, Router, IoT-Geräte etc.) und können diese für kriminelle Zwecke missbrauchen. Neben dem Abgreifen persönlicher Daten des Anwenders und Betrug beim Onlinebanking können auch die Ressourcen des gekaperten Systems von einem Angreifer missbraucht werden, um beispielsweise Kryptowährungen zu berechnen oder DDoS-Angriffe durchzuführen. Aufgrund eines modularen Aufbaus ist aktuelle Schadsoftware in der Lage, ihre Funktionalitäten durch das Nachladen von Erweiterungen dynamisch anzupassen oder zu erweitern. Damit können die Betreiber eines Botnetzes flexibel dessen Einsatzzweck verändern und an aktuelle Gegebenheiten individuell anpassen.[22] In den letzten Monaten wurden Botnetze hauptsächlich zum Informationsdiebstahl, zum Betrug beim Onlinebanking sowie zur Verteilung von Schadprogrammen genutzt. Dazu wurden verstärkt mit Botsoftware infizierte Android-Systeme beobachtet, hier mit einer vergleichsweise hohen Infektionsrate in Deutschland. Allein im Jahr 2019 wurden täglich bis zu 110.000 Botinfektionen deutscher Systeme registriert und über das BSI an die deutschen Internet-Provider gemeldet.[23]

5 Die aktuelle Gefährdungslage Wirtschaft und Kritische Infrastrukturen (KRITIS)

KRITIS sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen. Ihre Systeme und Dienstleistungen, wie beispielsweise die Versorgung mit Wasser oder Wärme, ihre Infrastruktur und Logistik sind seit Jahren immer stärker von einer reibungslos funktionierenden Informationstechnik abhängig. Eine Störung, Beeinträchtigung oder gar ein Ausfall durch einen Cyber-Angriff oder IT-Sicherheitsvorfall kann zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen.[24]

Auch andere Wirtschaftsunternehmen sind aufgrund ihres technologischen Know-hows, durch ihre Auslandsaktivität und im Rahmen von breit gestreuten Angriffen Ziele für Cyber-Attacken. Hierbei sind es vor allem die finanziellen Folgen durch Produktionsausfälle, Beschädigungen des Maschinenparks, Patentdiebstahl oder Cyber-Erpressung, die erhöhte IT-Sicherheitsvorkehrungen notwendig machen.

Die Gefährdungslage im Bereich Kritischer Infrastrukturen liegt weiterhin auf hohem Niveau. Die Cyber-Sicherheit von KRITIS stellt sich asymmetrisch dar: Um eine Kritische Infrastruktur erheblich beeinträchtigen zu können, muss ein Angreifer nur eine einzige Schwachstelle erfolgreich ausnutzen. Betreiber Kritischer Infrastrukturen müssen allerdings einen ganzheitlichen, aufwändigen Schutz gewährleisten, um sich umfassend abzusichern. Im Bereich der Technik verdeutlichten Meldungen zahlreicher KRITIS-Betreiber, dass Ausfälle im Bereich der Hard- und Software, insbesondere nach Updates und Patches von relevanter IT-Infrastruktur, Beeinträchtigungen und Ausfälle der kritischen Dienstleistungen verursachten. Dabei waren die am intensivsten betroffenen Branchen diejenigen, deren Kritische Infrastrukturen eher im Bereich der IT zu finden sind als im Bereich der Operational Technology. Beispielhaft sind hier das Gesundheits-, Finanz- und Versicherungswesen zu nennen.

Bei den Meldungen über Cyber-Attacken gegen die deutsche Wirtschaft ist das Thema Ransomware weiterhin zentral. Schwachstellen, Fehler und Versäumnisse des IT-Betriebs und auch der Nutzer haben durch die ausgefeilten Methoden der Angreifer massive Konsequenzen für die Unternehmen. Sogar wenn Backups erstellt wurden, entstehen den Unternehmen Schäden durch den Ausfall der verschiedenen Netze und Systeme, durch die Zeit der Wiederherstellung aus den Backups sowie durch die Datenverluste aufgrund der Zeit zwischen der letzten Sicherung und dem Schadenseintritt. Wenn trotz der regelmäßigen Berichterstattung und Sensibilisierung zum Thema keine Backups verfügbar sind, oder diese nicht adäquat geschützt sind, sodass sie ebenfalls verschlüsselt werden, entstehen hohe bis sehr hohe Schäden.[25]

Allein durch die Zeit, die eine (Teil-)Wiederherstellung benötigt, entstehen der Wirtschaft in Verbindung mit Produktionsausfällen große Verluste. Diese können für kleinere Unternehmen gar existenzbedrohend sein.

Das BSI warnte in den vergangenen Monaten davor, dass durch das gezielte Sammeln von Adress- und E-Mail-Informationen – das sog. *„Outlook-Harvesting“* – authentisch aussehende Angriffs-(Spam-)Mails erstellt werden können. Dazu liest die Schadsoftware Kontaktbeziehungen und seit Ende des Jahres 2018 auch E-Mail-Inhalte aus den Postfächern bereits infizierter Systeme aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms in nachfolgenden Spam-Kampagnen, sodass die Empfänger fingierte E-Mails von Absendern erhalten, mit denen sie erst kürzlich in Kontakt standen. Jeder Infizierte wird so zu einer Gefahr für seine Kontakte. Hier sind zukünftig technische Maßnahmen gefragt, um so weit und so aktuell wie möglich Infektionen zu verhindern und, falls diese doch im Einzelfall erfolgreich sind, sicherzustellen, dass die Kompromittierung eines einzelnen Systems nicht zur Gefährdung des gesamten Netzes führt.[26]

Durch den Einsatz von neuen Techniken, die bislang nur im Umfeld fortschrittlicher APT-Angriffe festgestellt wurden, gelingt es aktueller Schadsoftware, sich innerhalb von Unternehmensnetzen auszubreiten (*Lateral Movement*) und sie vollständig zu infiltrieren. Diese Schadprogramme ermöglichen den Angreifern dann zum Beispiel über das Auslesen von Zugangsdaten und Schwachstellen in verbreiteten Netzwerkprotokollen, sich selbstständig in einem IT-Netz auszubreiten und Remote-Zugriff auf die Systeme zu erlangen. Bei ungünstiger Netzwerkkonfiguration kam es dabei zu Ausfällen kompletter Unternehmensnetzwerke. Aufgrund aktueller und regelmäßiger Modifikationen werden die Schadprogramme meistens nicht von gängigen Virenschutzprogrammen erkannt und nehmen tiefgreifende Änderungen an den infizierten Systemen vor. Darüber hinaus bleiben Bereinigungsversuche meistens erfolglos und bergen die Gefahr, dass Teile der Schadsoftware auf dem System verbleiben. Daher sind einmal infizierte Systeme grundsätzlich als vollständig kompromittiert zu betrachten und müssen neu aufgesetzt werden. In mehreren dem BSI gemeldeten Fällen hatte dies massive Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke vollständig neu aufgebaut werden mussten.

Hierbei ist folgender Sachverhalt eines bekannten deutschen IT-Dienstleisters zu nennen:

Ein deutscher IT-Dienstleister wurde im zweiten Quartal des Jahres 2019 Opfer einer Cyber-Attacke. Dabei gelang es den Tätern zunächst, Firmeninterna sowie Kundendaten zu exfiltrieren und im Anschluss Daten zentraler IT-Systeme zu verschlüsseln. Der IT-Dienstleister kam der sechsstelligen Lösegeldforderung nicht nach, um die kriminellen Machenschaften nicht zu fördern. Daraufhin machten die Täter die Drohung wahr und veröffentlichten die Daten über einen Webserver.[27] Das von der Cyber-Attacke betroffene IT-Dienstleistungsunternahmen schaltete sofort die Strafverfolgung über das zuständige Landeskriminalamt in diesem schwerwiegenden Fall und aufgrund der Betroffenheit von personenbezogenen Daten wie Namen, Telefonnummern und E-Mail-Adressen erfolgte beim zuständigen Landesdatenschutzbeauftragten eine Vorfallsmeldung gemäß Datenschutzgrundverordnung (DSGVO) sowie eine Information der Kunden. Die Cyber-Attacke wurde im Nationalen Cyber-Abwehrzentrum eingebracht. Daneben wurden die betroffenen Betreiber Kritischer Infrastrukturen über die Information des IT-Dienstleisters hinaus durch das BSI informiert und um Risikobewertung bezüglich der abgeflossenen Daten gebeten. Das BSI erklärt in diesem Zusammenhang, dass IT-Sicherheitsvorfälle einen sehr hohen Reputationsschaden auslösen können, der

schnell, z.B. durch Auftragsrückgänge oder Schadensersatzforderungen von Kunden, zu einem immensen finanziellen Schaden führen kann. Bisher wurden Opfer im Rahmen von Ransomware-Angriffen mit Lösegeldforderungen erpresst, um die Daten wieder entschlüsselt zu bekommen. Falls nicht gezahlt wird, kommt es zu einem Datenverlust, der durch Backups rückgängig gemacht werden kann. Durch die Veröffentlichung von zuvor ausgespähten Daten können die Täter weiteren Druck auf die Opfer ausüben, selbst wenn diese über Backups verfügen.[28]

6 Fazit und Ausblick

Die Zeitschrift WirtschaftsWoche kritisiert, dass Vorstände und Aufsichtsräte der deutschen Wirtschaft häufig erst nach einer schädlichen Cyber-Attacke erkennen, wie dringlich Investitionen in die IT-Sicherheit sind. Vorher stoßen die Warnungen der Cybersecurity-Verantwortlichen oftmals auf taube Ohren.[29] So würden viele ihrer Warnungen nicht ernstgenommen und trotz vieler Aufklärungskampagnen sähen Firmenchefs höhere Investitionen in die Cybersicherheit eher als lästiges Übel und unnötigen Kostenfaktor, der sowieso keine zusätzliche Sicherheit bringt. *„In weiten Teilen des deutschen Mittelstandes regiert das Prinzip Hoffnung“,* erklärt der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) das Ergebnis einer Umfrage des Marktforschungsinstituts Forsa. Zwar schätzen weit über zwei Drittel der deutschen Mittelständler die Risiken durch Cyberangriffe als hoch ein, blenden aber die Gefahr für das eigene Unternehmen aus. Viele reden sich ein, dass ihre Unternehmen zu klein und damit auch ihre Daten zu uninteressant seien.[30]
Das BSI warnt seit Jahren vor einer neuen Qualität an Cyber-Angriffen und vor einer großen Vulnerabilität der deutschen Wirtschaft. Bereits im Jahr 2018 hatte das BSI die Schadsoftware Emotet als eine der größten Cyber-Bedrohungen der Welt bezeichnet und vor einer professionellen Weiterentwicklung gewarnt. Im Jahr 2019 kam es dann zu gezielten Ransomware-Angriffen auf deutsche Unternehmen. Ransomware zählt aktuell und in der Zukunft zu den größten Bedrohungen für Unternehmen, Behörden und andere Institutionen sowie für Privatanwender. Immer wieder kommt es zu Komplettausfällen von Rechnern und Netzwerken, aber auch von Produktionsanlagen der Wirtschaft. Das Schadenspotenzial dabei ist enorm: Die Kosten u.a. für Produktionsausfälle, Datenverlust, Bereinigung und Wiederherstellung der Systeme gehen in die Millionen, Dienstleistungen von Einrichtungen des Gemeinwesens sind nicht oder nur eingeschränkt verfügbar.[31]
Als Ausblick bleibt festzuhalten: In der gesamten deutschen Unternehmenskultur und über alle Abteilungsgrenzen hinweg muss so schnell wie möglich umgedacht werden. Weil Cyber-Attacken praktisch jeden Unternehmensbereich betreffen können, muss Cybersecurity in deutschen Unternehmen unternehmensweit gewährleistet sein.

Anmerkungen

1. Prof. Dr. Stefan Goertz lehrt und forscht im Fachbereich Bundespolizei der Hochschule des Bundes in Lübeck.
2. www.dw.com/de/hacker-greifen-dax-konzerne-an/a-49727717; 26.4.2020.
3. Ebd.
4. www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html; 26.4.2020.
5. wirtschaftslexikon.gabler.de/definition/cybersecurity-99856; 26.4.2020.
6. Ebd.
7. www.dw.com/de/deutsche-wirtschaft-klagt-über-zunehmende-cyber-attacken/a-51142386; 26.4.2020.
8. www.tagesschau.de/wirtschaft/boerse/cybersecurity-101.html; 26.4.2020.
9. Ebd.
10. www2.deloitte.com/de/de/pages/risk/articles/Cyber_Security.html; 26.4.2020.
11. Bundesamt für Sicherheit in der Informationstechnik (2019): Die Lage der IT-Sicherheit in Deutschland. Bonn 2019, S. 7.
12. Ebd.

13. Niehoff, Peter (2019): Cyber-Crime. In: Keller, Christoph (Hrsg.): Basislehrbuch Kriminalistik, S. 719.
14. BSI 2019, S. 8.
15. Niehoff 2019, S. 720.
16. BSI 2019, S. 11.
17. Ebd., S. 15-18.
18. Niehoff 2019, S. 721.
19. Ebd.
20. BSI 2019, S. 18.
21. Niehoff 2019, S. 721-722.
22. BSI 2019, S. 21.
23. Ebd.
24. BSI 2019, S. 46.
25. Ebd., S. 46-47.
26. Ebd., S. 48.
27. Ebd., S. 49.
28. Ebd,
29. www.wiwo.de/technologie/digitale-welt/cybersecurity-das-zeitspiel-der-chefs/25566622.html; 26.4.2020.
30. Ebd.
31. Ebd., S. 75.