Cybercrime und die Bedrohungen für die Wirtschaft (Teil 2)

Von ORR Ass. jur. Frank Grantz, Altenholz

3.4 Botnetze

Auch Angriffe über sog. Botnetze, sind ein gängiges Mittel für Cyberattacken. Diese sind oftmals mit anderen Angriffsmethoden verbunden. Unter einem Botnet versteht man einen Zusammenschluss vernetzter Computer, die über ein verstecktes Schadprogramm, dem sog.en Bot, miteinander verbunden sind und die Rechenleistung, Netzwerkanbindung und Daten ihrer Wirte für die Hintermänner nutzbar machen.[1] Der eigentliche Besitzer des Computers bekommt davon in der Regel nichts mit und weiß somit auch nicht, dass sein Rechner Teil eines Botnetzes ist. Überwacht und gesteuert werden die Bots über Command-and-Control-Server, über welche die Hintermänner Befehle in das Netzwerk einspielen oder Daten einsammeln können. Die Attraktivität von Botnetzen liegt in den vielfältigen Einsatzmöglichkeiten. Die meisten Bots sind multifunktional konzipiert, können je nach Einsatzbefehl Daten ausspähen, DDoS Attacken durchführen oder als Erpressungstrojaner fungieren. Zeitweise schlummern sie auch einfach über eine bestimmte Zeit ohne speziell aktiv zu werden. Bots werden gerne zum massenhaften Versand von Spam oder Phishing Mails aber auch zum Verbreiten anderer Viren verwendet. Durch Methoden des Social Engineering werden die Empfänger dazu gebracht, einen Anhang zu öffnen oder auf einen eingefügten Link zu klicken und schon ist das System infiziert. In einer eher passiven Rolle befindet sich der Bot, wenn er schlicht als Speichermedium für illegale Filesharing-Angebote genutzt wird oder wenn er Rechenleistung abzweigt, um beispielsweise Cryptowährung-Mining[2] zu betreiben. Auch das kann für eine Firma u.U. einen Reputationsverlust bedeuten.

3.5 Schadsoftware (Malware)[3]

Eine weitere und im Bereich der Cyberangriffe auf Unternehmen besonders häufig zu findende Angriffsmöglichkeit[4] stellen die sog. Schadprogramme oder die *„Malware“* dar, die oftmals mit anderen Angriffsmethoden kombiniert werden. Dabei werden je nach Bedarf verschiedene Typen von Schadprogrammen programmiert. Bei sog. Rootkits handelt es sich um quasi *„Tarnkappen“* für Schadsoftware. Die eigentliche Gefahr geht dabei nicht von dem Rootkit selbst aus, sondern von den Schadcodes, deren Spuren es verwischt. Seine besondere Fähigkeit liegt darin, Schadprogramme vor Virenscannern und Sicherheitslösungen zu verstecken. Über einen Rootkit können sich entsprechende Angreifer unbemerkt auf dem Computer anmelden oder mit Administrationsrechten Programme ausführen. Beim klassischen Trojaner handelt es sich um eine Software, die heimlich auf Rechnern installiert wird, ohne dass der Nutzer das merkt. Das Programm schleicht sich ins System ein und erfüllt speziell vorprogrammierte Aufgaben. Trojaner spähen beispielsweise Worte oder Zugangsdaten für Online Banking aus, sie können aber auch einfach nur protokollieren was der Angreifer der Anwender auf der Tastatur eingibt. Bei Ransomware-Trojanern handelt es sich um eine Art von Malware, die Geld von Opfern erpressen soll. Oftmals fordert Ransomware eine Zahlung vom Benutzer, damit die Änderungen rückgängig gemacht werden, die der Trojaner auf dem Computer des Opfers vorgenommen hat. Diese Änderungen können Verschlüsselungen der auf der Festplatte befindlichen Daten darstellen – die dann nicht mehr verfügbar sind – oder aber die Blockierung des normalen Zugriffs auf das System bewirken.[5]

3.6 Crime-as-a-service

Das Phänomen crime-as-a-service hat sich insbesondere in Zusammenhang mit der Nutzung des DarkWeb und der Underground Economy (digitale Schwarzmärkte) entwickelt.[6] Aufgrund der hohen Technologie und der breiten Kenntnisse, die für einen entsprechenden Cyberangriff benötigt werden, kann man sich heute über das Darknet quasi *„moderne Verbrecher“*

kaufen. Das Zukunftsmodell Crime-as-a-service der organisierten Kriminalität ermöglicht, dass sich Klient und Auftraggeber nur virtuell treffen und auch gleich wieder trennen können. Das Vorgehen ist damit dezentral und ortsungebunden. Man telefoniert nicht miteinander, sondern kommuniziert ausschließlich über das Internet. Auch die Entlohnungen werden über virtuelle Währungen wie zum Beispiel Bitcoins nicht nachvollziehbar abgewickelt. In diesen Fällen wird häufig auch organisiert und arbeitsteilig vorgegangen: so suchen und verkaufen Hacker Schwachstellen von Software, Entwickler programmieren hierzu passende Schadsoftware, Angreifer nutzen diese, um Informationen auszuspähen und andere kaufen letztlich gestohlene Informationen, nutzen Sie aus und machen sie zu Geld. Die dabei genutzte digitale Währung im wesentlichen Bitcoin sorgt dafür, dass hierbei anonyme, nur schwer nachzuvollziehende Zahlungsvorgänge ermöglicht werden.[7]

3.7 Social Engineering

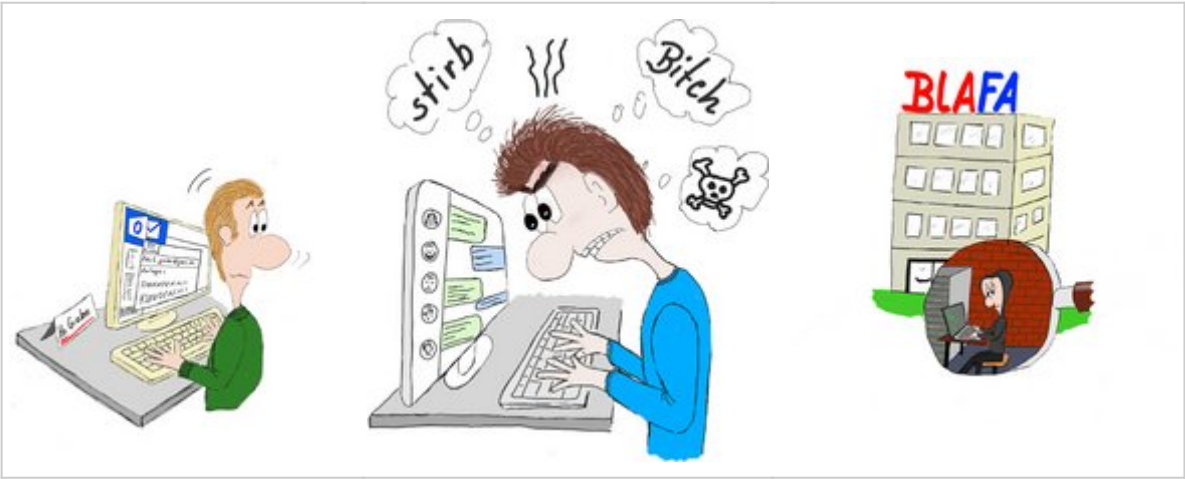
Ein wesentliches Einfallstor für Cyberangriffe bleibt aber stets der Mensch. Ausweislich des Bundesverbandes BITKOM war bei 61% der Befragten ein aktueller oder ehemaliger Mitarbeiter das Einfallstor von Wirtschaftsspionage Sabotage und Datendiebstahl der betroffenen Unternehmen.[8] Auch viele Fälle von Naivität gelten als Ursache und damit ist das Social Engineering mit 19% nicht nur eines der häufigsten Angriffsmittel sondern dient in vielen Fällen auch der Vorbereitung eines erfolgreichen Cyberangriffs. Unter dem Stichwort *„Social Engineering“* werden dabei verschiedene Modalitäten erfasst. Im Wesentlichen versuchen Kriminelle durch Lockmittel ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadsoftware auf ihren Systemen zu installieren. Sie gehen dabei regelmäßig sehr geschickt vor, indem gezielt menschliche Schwächen wie z.B. Neugier, Hilfsbereitschaft usw. ausgenutzt werden. Durch den Trend, persönliche Daten und Informationen mittels eines sozialen Netzwerks oder einer privaten Website verstärkt zugänglich zu machen (Facebook, Instagramm etc.) wird es potentiellen Angreifern sogar möglich gemacht, sich gezielt vorzubereiten, da durch diese Exposition entsprechende Informationen zu Schlüsselpersonen in einem Unternehmen, welches angegriffen werden soll, leicht zu verschaffen sind. So wird mittels gezielter E-Mails das Interesse des Mitarbeiters der Firma, die als Angriffsobjekt dienen soll, dahingehend manipuliert, dass dieser sein Passwort herausgibt bzw. über das Verfolgen von Links und Besuchen von präparierten Websites den Einfall von Schadsoftware im Firmensystem ermöglicht.

4 Angriffsziele und Möglichkeiten

Als Angriffsziele für solche Hacking bzw. Cybercrime Angriffe gelten die Behörden auf Verwaltungsebene, die Wirtschaft aber auch der Privatanwender. Gemäß des BSI[9] werden durchschnittlich einmal pro Monat mittels DDoS-Angriffen Websites der Bundesbehörden attackiert. Behörden verfügen über viele personenbezogene und andere sensible Daten und Informationen und stellen damit ein lukratives Ziel dar. Privatanwender sind häufig vom Datendiebstahl oder beim Onlinebanking Geschädigte.

Als Beispiel können dafür die zuerst in 2014 genutzten Angriffsmodalitäten via Emotet[10] genommen werden.
Angriffe auf Wirtschaftsunternehmen werden in verschiedenen Studien genauer betrachtet. So wurden bspw. durch den Bundesverband Bitkom im Jahre 2015[11] sowie 2018[12] verschiedene Unternehmen in Deutschland befragt und die erhobenen

Daten ausgewertet. Auch das BSI hat entsprechende Berichte zur Lage der IT-Sicherheit herausgegeben.[13] Ausweislich dieser Studien handelt es sich bei den häufigsten Delikten der Cybercrime um die digitale Wirtschaftsspionage, die Sabotage und den Datendiebstahl[14]. Hierzu werden vielfach direkt oder indirekt Cyberangriffe durchgeführt, teilweise wird aber auch konkret die Hardware angegriffen, beispielsweise durch Diebstahl von Computern, Smartphones, Tabletts oder Daten von Unternehmen. Aus diesen Geräten werden dann die sensiblen ausgelesen.
Mehr als 68% aller deutschen Unternehmen sind von Cyberangriffen betroffen, 73% davon sind mittelständische Unternehmen mit 100-500 Mitarbeitern.[15] Als Grund für diese hohe Zahl wird angeführt, dass gerade mittelständische Unternehmen über innovative Techniken verfügen, die dann im Speziellen größeren Unternehmen zugeliefert werden, diese Unternehmen aber regelmäßig über wenig Mittel und Möglichkeiten zur Einrichtung von Abwehrmechanismen gegen Cybercrime verfügen. So werden diese mittelständischen Unternehmen ein Einfallstor, um an die Daten der oftmals besser geschützten Großkonzerne zu kommen. Betrachtet man die Betroffenheit nach Unternehmensbereichen zeigt sich, dass mit 74% die Chemie- und Pharmabranche im Beurteilungszeitraum 2018 am stärksten betroffen war, die Automobilindustrie mit 68% am zweit häufigsten Objekt von Cyberangriffen wurde.[16] Dieses wird u.a. damit begründet, dass gerade im Bereich der Automobiltechnik Deutschland sich auf einem hohen Innovationsniveau befindet.[17] Hieran schließen sich der Maschinen- und Anlagenbau, sowie die Herstellung von Kommunikations- und Elektrotechnik als Ziel von Cyberangriffen an.[18] Mit wenigen Ausnahmen richten sich nahezu alle Angriffe auf digitale Daten oder an die Informations- und Kommunikationsinfrastruktur.[19] Von 550 der befragten Unternehmen gaben 34% an, das konkret ihr IT-System Gegenstand eines Angriffs gewesen sei.[20] 45% gaben an, dass sie regelmäßig Gegenstand eines Cyberangriffs werden, 9% davon registrieren einen täglichen Angriff, 30% gaben an, mindestens einmal im Monat Gegenstand eines solchen Angriffs geworden zu sein.[21] In 19% aller Fälle soll ein Angriff durch Social Engineering vorbereitet worden sein.[22]
Industrieanlagen selbst dagegen werden oft durch APT-Angriffe attackiert und bei Banken geht es im Wesentlichen um das Abschöpfen der verschlüsselten Kontodaten wie beispielsweise im Angriffsszenario *„Heartland“*.[23] Angriffe auf Produktionsnetze sind speziell mit dem Namen *„Dragon Fly“*[24] verbunden. Die Hacker griffen hierbei gezielt drei europäische Hersteller von Steuerungssoftware an, und tauschten auf deren Servern Updates dieser Software gegen infizierte Versionen aus. Durch die Installation dieser ausgetauschten Software hat sich dann das programmierte Virus in den firmeneigenen Produktionsnetzen verbreitet. Auch Betriebssysteme auf den Unternehmensrechnern werden Gegenstand von Angriffen. Dabei werden nicht nur Windows-Systeme sondern auch Linuxdistributionen angegangen, wie beispielsweise 2014 durch Shellshock.[25] Schließlich wurde in den Studien von BITKOM auch betrachtet, inwieweit besondere, spezielle Unternehmenseinrichtungen, die unter dem Schlagwort KRITIS[26] zusammengefasst werden, von Cyberangriffen betroffen sind. Allerdings war in diesem Bereich keine besondere Angriffshäufigkeit zu verzeichnen, Angriffe korrelieren mit denen auf sonstige Unternehmens- und Wirtschaftseinrichtungen. Bisher sind 45% solcher KRITIS Einrichtungen von Cyberangriffen betroffen gewesen.



5 Reaktionsmöglichkeiten

Ausweislich der oben dargestellten Szenarien und Studien werden die Cyberangriffe auf Wirtschaftsunternehmen unstreitig zunehmen. Es stehen jedoch diverse Mittel und Wege zur Verfügung, die nur noch durch die Unternehmen umgesetzt werden müssten.

5.1 Anzeigeverhalten verbessern

Laut BITKOM sei das Anzeigeverhalten grundsätzlich gut. Lediglich 2% der angegriffenen Unternehmen hätten darauf verzichtet, ihre Sicherheitsvorfälle an staatliche Stellen zu melden.[27] Ein Großteil der befragten Unternehmen ([78]%) habe zudem zwar Strafanzeige gestellt[28], jedoch erfolgten viele der Anzeigen und Meldungen nur im Rahmen oder aufgrund von gesetzlich verpflichteten Meldungen ([20]%).[29] Als Begründung für eine Nichtanzeige wurden von den befragten Unternehmen mehrere Argumente angeführt. So befürchten die Unternehmen zum einen, dass mit einer Anzeige (Reputations-)Schäden verbunden sein könnten ([38]%) und zum anderen, dass es sich dabei um einen *„sich nicht rechnenden“* Aufwand handeln würde ([37]%). 35% der befragten Unternehmen befürchteten, dass mit der Anzeige negative Konsequenzen für sie verbunden seien, wie beispielsweise im Rahmen Ermittlungen beschlagnahmte oder sichergestellte Hardware ([36]%). 38% der Befragten schließlich führten an, dass sie glauben, dass die Täter ohnehin nicht gefasst werden würden.[30] Gerade für die Ermittlungsbehörden ist jedoch ein gutes Anzeigeverhalten erforderlich, um durch die immer stärker aufgestellten Spezialdienststellen die Aufklärung dieser Fälle und damit auch die Prävention sicherzustellen.[31] Ein etwaiges *„Risiko“* für die Unternehmen könnte bspw. durch eine inzwischen von sämtlichen Versicherungen angebotene Cyberversicherung ausgeglichen werden.[32]

5.2 BSI und Zusammenschlüsse nutzen; Austausch, gemeinsame Konzepte

Sowohl von Seiten staatlicher Organisationen als auch von privaten Einrichtungen werden umfassende Schutzmöglichkeiten angeboten. So stellt das BSI bspw. Anleitungen und Hilfen für Unternehmen her und bietet diese zum Abruf. Hier sind z.B. das IT-Grundschutzkompendium[33] sowie entsprechende Sicherheitszertifikate des BSI ISO 27001 [34] zu nennen, die entsprechende IT-Grundschutzbausteine gezielt für verschiedene Unternehmensbereiche bereithalten. Darüber hinaus gibt es auch gezielt Zusammenschlüsse und Vereinigungen, die gemeinsam Initiativen gegen Cyberangriffe ergreifen. So bietet bspw. die Allianz für Cybersicherheit in ihrem Downloadbereich Videos und Materialen für den Unternehmensschutz an. Aktuell gehören dieser Initiative 3608 Unternehmen und Institutionen an.[35] Auch Zusammenschlüsse wie die Charter of Trust [36] bieten eine gute Strategie gegen Cyberangriffe. Aber auch für einzelne Unternehmenskategorien werden umfangreiche Hilfen bereit gestellt, so z.B. durch die BaFin für Finanzinstitute.[37] oder die Möglichkeit des Erwerbs von Sicherheitszertifikaten für Unternehmen, z.B. in Form eines Audit.[38]

5.3 IT-Sicherheitsmanagement/ Complience[39]

Wichtig erscheint aber auch ein geschlossenes Konzept für das Management des jeweiligen IT-Systems im Unternehmen zu gestalten. Je nach Größe und Umfang des Unternehmens müssen Konzepte für das Funktionieren des IT- und Kommunikationssytems als auch für das Mitarbeitermanagement zur IT-Sensibilisierung erstellt, kontrolliert und überwacht werden. Dieses könnte z.B. im Wege eines umfassenden IT-Complience[40] sichergestellt werden. Dieses sollte zunächst die technische Ebene berücksichtigen. Ein aktuell gepatchtes Betriebssystem mit darauf ausgerichteter Virenschutzsoftware bzw. Firewall stellt schon die erste große Hürde für einen potentiellen Angreifer dar. Leider nutzen nur 71% der befragten Unternehmen ein solches System, kleine und mittelständische Unternehmen gar nur zu 65%.[41] Auch regelmäßige Kontrollen der IT-Systeme mit besonderer Detektionssoftware wie z.B. Rootkitrevealern etc. sollten durchgeführt werden.[42] Der Datenverkehr muss bei Verdacht eines Angriffs immer überwacht werden. Hierzu gibt es verschiede Programme, z.B. Wireshark, die u.U. sogar ein Übertrag von gestohlenen Passworten ermöglichen. Anhand dieser Informationen können die Ermittlungsbehörden dann gezielt eingeschaltet werden.[43] Für den Fall, dass Auffälligkeiten festgestellt werden, sollte auch ein unternehmensbezogener Notfallplan erstellt werden, in welchem die Möglichkeiten beschrieben werden, einen Datenabfluss zu stoppen oder wie ggf. systemsichernde Elemente eingesetzt werden müssen. Auch erste Ansprechpersonen sollten aufgeführt werden. Ein solches Notfallmanagement wird aktuell allerdings nur bei 43% der befragten Unternehmen vorgehalten.[44] Ein wichtiges und besonders erforderliches Element des Complience wird aber immer ein überzeugendes Mitarbeitermanagement bezogen auf die IT-Systeme darstellen. Dieses wird bisher nur von 59% der befragten Unternehmen überhaupt durchgeführt bzw. berücksichtigt.[45] Sicherheitsüberprüfungen von Personal bzw. auch von entsprechenden Ex-Mitarbeitern sind erforderlich, zudem sind gegebenenfalls entsprechende vertragliche und haftungsrechtliche Regelungen in den Arbeitsvertrag oder in Betriebsvereinbarungen aufzunehmen. Schließlich sollte regelmäßig auch eine finanzielle Absicherung insbesondere kleinerer und mittlerer Unternehmen erfolgen. Dieses kann bspw. durch eine Cyberversicherung geschehen. Diese Leistungen werden inzwischen von diversen Versicherungsanbietern individuell angeboten.[46]

Graphiken: Andreas Dondera, LKA Hamburg.

Anmerkungen

1. www.pcwelt.de/ratgeber/Botnetze-Definition-Gefahren-Schutzmassnahmen-10097077.html.
2. Bitcoin-Mining z.B. ist ein Prozess, bei dem Rechenleistung zur Transaktionsverarbeitung, Absicherung und Synchronisierung aller Nutzer im Netzwerk zur Verfügung gestellt wird. Das Mining ist eine Art dezentrales Bitcoin-Rechenzentrum mit Minern aus der ganzen Welt. Dieser Prozess wird analog zum Goldschürfen Mining genannt. Anders als beim Goldschürfen gibt es beim Bitcoin-Mining eine Belohnung für nützliche Dienste. Die Auszahlung der jeweiligen Bitcoin-Anteile richtet sich nach der zur Verfügung gestellten Rechenkapazität.
3. Darunter werden alle Arten von Computerprogrammen zusammengefasst, die unerwünschte und schädliche Funktionen auf einem Computersystem ausführen.
4. www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html, Bericht zur Lage der IT-Sicherheit in Deutschland 2018, S. 19.
5. Aktuell ist z.B. der Verschlüsselungstrojaner GrandCrab im Einsatz, der getarnt als *„Bewerbungsemail“* gezielt an Personalabteilungen von Firmen versendet wird. Die durch die Infektion verschlüsselten Daten sind dann nicht mehr durch die Firma nutzbar.
6. Vgl. BKA Lagebild 2017, S. 25 www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html.
7. Kriminelle Hacker nutzen teilweise auch eigene Finanzinstitute im Netz. Von diesen Untergrund Banken weiß man recht wenig, allerdings ist in Amerika die Website Liberty Reserve im Jahr 2013 erkannt und geschlossen worden. Sie stellte nach Angaben der US-Behörden damals das Finanzzentrum der Cybercrime-Welt dar. Von 2006 bis zur Schließung 2013 sollen über Liberty Reserve Transaktionen im Gesamtwert von 6 Milliarden Dollar getätigt worden sein, vgl.: www.heise.de/newsticker/meldung/Illegaler-Bezahldienst-Liberty-Reserve-Gruender-bekennt-sich-der-Geldwaesche-schuldig-3088621.html.
8. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 28.
9. www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html, Bericht zur Lage der IT-Sicherheit in Deutschland 2018, S. 7.
10. Emotet ist ein Banking-Trojaner, der erstmals im Jahr 2014 von Sicherheitsexperten entdeckt wurde. Emotet war ursprünglich als Banking-Schadsoftware entwickelt worden, deren Ziel es war, in fremde Computer einzudringen und dort vertrauliche private Daten auszuspähen. In späteren Programmversionen wurde weitere Schadsoftware hinzugefügt, zum Beispiel Spamming-Funktionen und andere Banking-Trojaner. Emotet ist in der Lage, herkömmliche Antivirenprodukte zu täuschen und die Erkennung durch gängige Virenschutzprogramme zu umgehen.
11. www.bitkom.de/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html.
12. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html.
13. www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html, Bericht zur Lage der IT-Sicherheit in Deutschland 2018, S. 23 ff.
14. www.bitkom.de/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html S. 8; siehe hierzu auch im Überblick: breachlevelindex.com.
15. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 14.
16. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 17.
17. www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-im-digitalen-Zeitalter.html, S. 9.
18. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 17.
19. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 19.
20. www.bitkom.de/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html S. 13.
21. www.bitkom.de/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html S. 12.
22. www.bitkom.de/Presse/Presseinformation/Studie-zu-Wirtschaftsschutz-und-Cybercrime.html S. 20; www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 28.
23. Noch heute gilt der 2008 erfolgte Cyberangriff auf das US-Unternehmen Heartland Payment Systems als einer der größten Hacks aller Zeiten, soweit es um Kreditkartenbetrug geht. Heartland ist einer der weltweit größten Anbieter für

elektronische Zahlungsabwicklung. Im Zuge des Hacks wurden rund 130.000.000 Kreditkarten-Informationen gestohlen. Der Schaden für Heartland belief sich auf mehr als 110 Millionen Dollar, die zum größten Teil für außergerichtliche Vergleiche mit Kreditkartenunternehmen aufgewendet werden mussten.

24. www.welt.de/wirtschaft/article129674310/Hacker-infizieren-Schaltzentralen-der-Stromnetze.html.
25. www.security-insider.de/exploit-szenarien-fuer-shellshock-a-460947/.
26. KRITIS = Kritische Infrastrukturen. Es sind damit Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen gemeint, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe erhebliche Störung der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
27. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 34.
28. Was mit der Einrichtung von zentralen Anlaufstellen für Cybercrime in den einzelnen Bundesländern begründet wird, vgl. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 33.
29. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 32.
30. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 34.
31. www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html, S. 28f.
32. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html S. 51.
33. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.html.
34. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI zertifizierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehört eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Auditberichts.
35. Mit der 2012 gegründeten Allianz für Cyber-Sicherheit verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Aktuell gehören der Initiative 3607 Unternehmen und Institutionen an – und jeden Tag kommen weitere Teilnehmer dazu.
36. Größere Firmen schließen sich oftmals zusammen, so wie z.B. im *„Charter of Trust“*. Diesem gehören inzwischen auch andere Mitglieder mit großen Namen an, wie z.B. Airbus, Daimler, Cisko, Allianz, Dell, IBM bis hin zu Ölunternehmen wie Total.
37. BaFin, Mindestanforderungen an das Risikomanagement, www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1709_marisk_ba.html. Bankaufsichtliche Anforderungen an die IT (BAIT), www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html.
38. www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html.
39. www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html.
40. IT-Compliance bedeutet, dass die IT eines Unternehmens nachweislich alle ihr aufgetragenen Regeln und Gesetze sowohl technisch, als auch organisatorisch befolgt. Hierbei ist es unwichtig, ob die IT-Leistungen ausschließlich unternehmensintern oder durch externe Dienstleister erbracht werden (darunter fallen auch Entwicklungs-, Hosting- und Outsourcing-Verträge).
41. www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html.
42. Rootkitrevealer, die versteckte Schadsoftware aufspüren können werden jedoch nur von 23 % der Befragten eingesetzt, siehe: www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html S. 16.
43. www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html, S. 21.
44. www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Cyber-Sicherheits-Umfrage/CyberSicherheitsUmfrage_2018/cs_umfrage_2018_node.html, S. 23.
45. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 43.
46. www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html, S. 51.