Digitale Rettungskette des BSI

Hausarbeit

vorgelegt von

Stavros Giannis
aus Düsseldorf

Geboren am: 16. März 1996
Matrikel-Nr.: 1303980

Hochschule Niederrhein
Fachbereich Wirtschaftswissenschaften
Studiengang B.Sc. Cyber Security Management

Sommersemester 2021

1. Prüfer: Prof. Dr. Mehrtens, Matthias
2. Prüfer: Prof. Dr. René Treibert

Inhaltsverzeichnis

Abkürzungsverzeichnis

IT	Informationstechnik
IoT	Internet of Things
BSI	Bundesamt für Sicherheit in der Informationstechnik
BDN	Bundesnachrichtendienst
EU	Europäischen Union
ISMS	Informationssicherheit Management System
ISO	Internationale Organisation für Normung
IEC	Internationale Elektrotechnische Kommission
WWW	World Wide Web
DDoS	Destributed Denial of Service
DoS	Denial of Service
CNS	Cyber-Sicherheitsnetzwerk
KMU	kleine und mittlere Unternehmen

Abbildungsverzeichnis

1 Einleitung

"To alter someone's way of thinking you must understand the way people think and in what modes they think."

Kevin Mitnick in seinem Buch

Social Engineering: The Art of Human Hacking[1]

Durch die rasante Aufwärtsentwicklung der Technologien, insbesondere dessen vielfältiger Einsatz und dauerhafte Bereitstellung, ist seit einigen Jahren die Cybersicherheit eines der am meist diskutierten zentralen Themengebiete in der Informationstechnik (IT) [2] . Durch die kontinuierlichen Innovationen der Informationstechnologie wurden für Unternehmen völlig neue Möglichkeiten eröffnet im Bereich der Vernetzung und IoT. Nichtsdestotrotz existieren sehr viele Gefahren. Ohne die notwendige Sicherheit und Zuverlässigkeit der IT-Infrastruktur wären bestimmte Geschäftsprozesse nicht mehr funktionstüchtig. Doch in unserer Netzwerkwelt, im Zeitalter des Internets, reduzieren sich selbst die größten Distanzen auf die Distanz eines Mausklicks. Kein Unternehmen und auch keine Behörde kann es sich mehr leisten Daten ungeschützt zu lassen.

1.1 Zielsetzung und Aufbau der Arbeit

Ziel dieser Arbeit ist es zu informieren, welche Maßnahmen nötig sind, um die Informationssicherheit eines Unternehmens zu gewährleisten und kontinuierlich zu verbessern. Aufgrund des wachsenden Ausmaßes der IT für Unternehmen nimmt die Bedeutung des Sicherheitsaspektes immer mehr zu. Unternehmen haben neben gesetzlichen Rahmenbedingungen Vorteile für eine ISO/IEC 27001 Ausrichtung. Wie einzelne Geräte, aber auch komplexe vernetzte Systeme wie die eines Unternehmens oder kritischer Infrastrukturen, digital vor Gefahren zu schützen sind, hat sich das Bundesamt für Sicherheit in der Informationstechnik zur Aufgabe gemacht. Diese wissenschaftliche Arbeit wird sich daher mit dem Cyber-Sicherheitsnetzwerk beim BSI auseinandersetzen. Des Weiteren wird signifikant auf der vom BSI methodischen Gefährdungsgrundlage bei Schadprogrammen [3] ausgewertet, auf die die Aufgaben der Digitalen Ersthelfer bei IT-

[1] Mitnick N., 2010, S. 410.
[2] Vgl. BSI (Hrsg.) 2020, S. 8.
[3] Vgl. BSI Lagebericht (2020), S. 9.

Sicherheitsvorfällen sowie deren ersten Handlungsempfehlungen bei IT-Vorfällen im Cyber-Sicherheitsnetzwerk.

2 Das Bundesamt für Sicherheit in der Informationstechnik

2.1 Was ist das BSI?

Das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, befasst sich mit der IT-Sicherheit und der Informationsgesellschaft.[4] Das BSI erweitert den konformen Einsatz von sicheren Informations- und Kommunikationstechniken. Diese Behörde partizipiert mit dem Bundesministerium des Innern. Unter den Adressatenkreis fallen z. B. die öffentlichen Verwaltungen, Wirtschaftsunternehmen, Wissenschafts- und Forschungseinrichtungen und Privatanwender[5]. Unter der Zusammenarbeit mit anderen deutschen Behörden, bietet das BSI technische Expertise und Beratungen an, ob es um Unterstützungen geht oder um bestimmte Maßnahmen bezüglich der Erforschung oder Verhinderung[6]. Darunter fällt auch der Bundesnachrichtendienst (BND).

2.2 Die Aufgabenbereiche des BSI

Der Aufgabenbereich des BSI wird durch das BSI-Gesetz bestimmt. Dieser ist für die folgenden Aufgaben repräsentativ[7]:

- „Schutz der Netze des Bundes, Erkennung und Abwehr von Angriffen auf die Regierungsnetze“
- „Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen“
- „Warnung vor Schadprogrammen oder Sicherheitslücken in IT-Produkten und -Dienstleistungen“
- „IT-Sicherheitsberatung für die Bundesverwaltung und andere Zielgruppen“
- „Information und Sensibilisierung der Bürger für das Thema IT- und Internet-Sicherheit“

[4] Vgl. BSI (2021).
[5] Vgl. ebd.
[6] Vgl. ebd.
[7] Vgl. ebd.

- „Entwicklung einheitlicher und verbindlicher IT-Sicherheitsstandards“
- „Entwicklung von Kryptosystemen für die IT des Bundes.“

Die Handlungsfähigkeit und Souveränität Deutschlands müssen auch im Zeitalter der Digitalisierung gewährleistet sein. Durch die zukunftsgerichtete Cyber-Sicherheitsstrategie[8] wird der EU, ebenso aber in Deutschland, eine Möglichkeit gegeben, internationale Normen und Standards im Cyberraum festzulegen und gleichzeitig die Zusammenarbeit mit Partnern auf der ganzen Welt zu stärken.

2.2 Definition von Informationssicherheit

Das wichtigste Anliegen der Informationssicherheit wird in der Gewissheit von gespeicherten Daten, also Informationen, registriert. Die Charakterisierung der Informationssicherheit wird wie folgt aufgebaut[9]:

- Durch die Vertraulichkeit soll sichergestellt werden, dass auf die Informationen nur von zulässigen Prozessen sowie anderen IT-Systemen kriegen kann
- Die Integrität stellt sicher, dass die Informationen absolut nicht manipuliert werden können. Insbesondere bedeutet dies, dass die gespeicherten Daten in keinen Fällen durch unbefugte und unbeabsichtigte Manipulationen verändert wurden
- Unter der Verfügbarkeit wird festgelegt, dass die Informationen gemäß den Compliance-Vorgaben des Unternehmens zur Verfügung stehen.

Zusammenschließend bewähren sie eine sichere Einstufung des Unternehmens, wenn ihre Vertraulichkeit, Integrität und Verfügbarkeit in der geforderten Menge gewährleistet werden kann.

3 Das Cyber-Sicherheitsnetzwerk des BSI

Das Cyber-Sicherheitsnetzwerk ist ein freiwilliger Zusammenschluss von qualifizierten Troubleshooting-Profis, die sich verpflichtet haben, ihr Fachwissen und persönliches Know-how zur Behebung von Sicherheit, IT-Vorfällen und zur Verbesserung der IT-Sicherheitslage in Deutschland einzubringen [10] . IT-

[8] Vgl. BSI (2021).
[9] Vgl. BSI Lagebericht (2020), S. 23.
[10] Vgl. BSI (2021), Cyber-Sicherheitsnetzwerk.

Sicherheitsvorfälle sollten erfasst und durch Reaktionsmaßnahmen analysiert werden, um das Schadensausmaß zu begrenzen und weiteren Schaden zu verhindern. Als Cybersicherheitsbehörde für Staat, Wirtschaft und Gesellschaft will das BSI sein reaktionsschnelles Angebot insbesondere für kleine und mittlere Unternehmen und Bürger stärken. Als Anlaufstelle im Falle von Cyber-Angriffen wurde das Konzept eines dezentralen Support-Netzwerks konzipiert – das Cyber-Sicherheitsnetzwerk (CSN). Das Ziel des Cyber-Sicherheitsnetzwerkes ist der Aufbau einer dezentralen Struktur [11], die KMU und Bürger bei einem IT-Sicherheitsvorfall effizient und wirtschaftlich unterstützt und zusätzlich zu bestehenden präventiven Beratungsangeboten. Das Cyber-Sicherheitsnetzwerk ist die erste Anlaufstelle sowohl für Betroffene als auch für Experten.

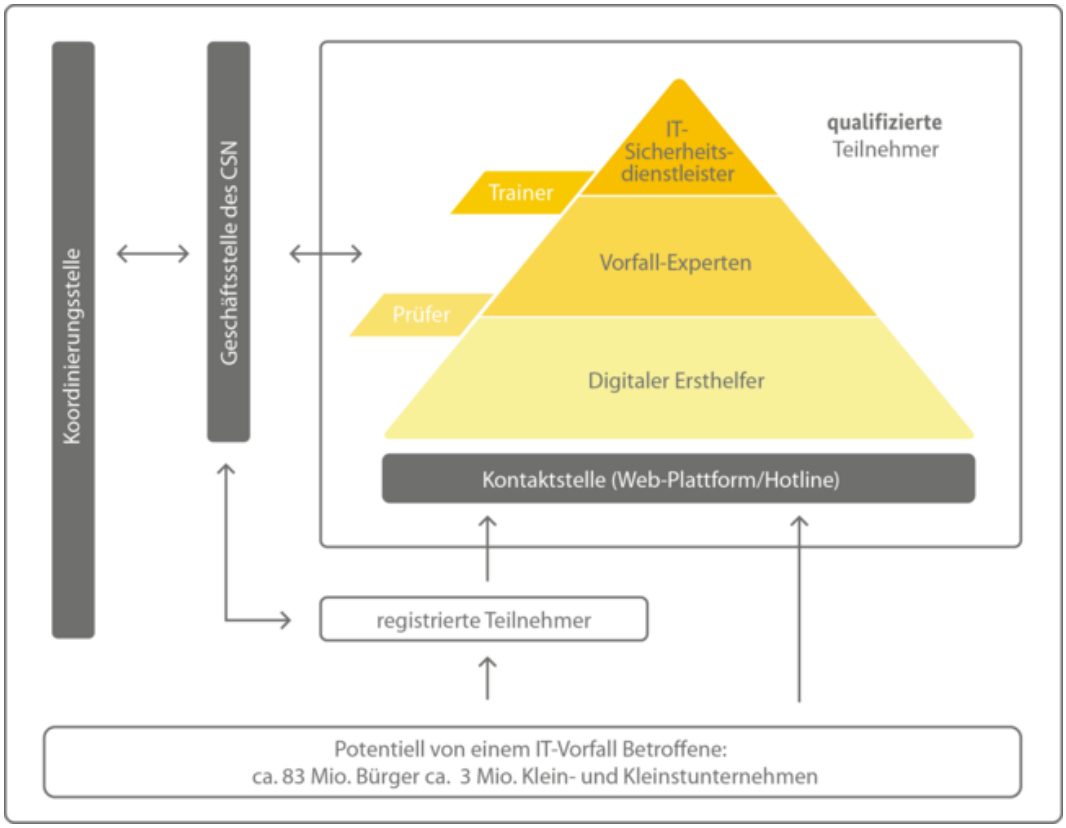

Abbildung 1: Rollenverständnis im Cyber-Sicherheitsnetzwerk; Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html)

Ausbilder und Prüfer unterstützen den Qualifizierungsgedanken und sichern die Qualität des unterstützenden Leistungsangebots durch Schulungen und

[11] Vgl. BSI (2021), Cyber-Sicherheitsnetzwerk.

Prüfungen [12] . Das Cybersicherheitsnetzwerk ist eng mit der Allianz für Cybersicherheit verbunden und ergänzt sein Angebot mit reaktiven Diensten.

3.1 Definition eines IT-Sicherheitsvorfalls

Ein IT-Sicherheitsvorfall ist ein Ereignis, das die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, IT-Services, IT-Systemen oder IT-Anwendungen gefährdet und zu schweren Schäden führen kann. Integrität bedeutet, die Richtigkeit der Informationen und das ordnungsgemäße Funktionieren von Systemen sicherzustellen. Die Verfügbarkeit von IT-Systemen, IT-Anwendungen oder IT-Netzen und -Informationen sind gewährleistet, wenn sie von einem berechtigten Nutzer jederzeit bestimmungsgemäß genutzt werden können. Diese Störungen können durch verschiedene Arten digitaler Bedrohungen verursacht werden. Bei einem IT-Sicherheitsvorfall stehen oft die Informationen zum System im Fokus, nicht das System selbst. Dabei ist es unerheblich, ob der Sicherheitsvorfall ein unerwünschtes oder beeinträchtigtes Ergebnis verursacht hat oder nur latent schädlich ist.[13]

3.2 Definition einer IT-Störung

Eine IT-Störung ist ein Ereignis, das unerwartet eintritt. Bei einem IT-Ausfall kann der Nutzer sein IT-System kontrollieren bzw. bei einem IT-Ausfall ist die Einflussnahme Dritter mit krimineller Absicht ausgeschlossen. Vielmehr wird davon ausgegangen, dass im Falle eines IT-Ausfalls ein technischer Ausfall oder ein versehentlicher Missbrauch des IT-Systems durch den Nutzer vorliegt.

3.3 Digitale Gefahren

3.3.1 Schadprogramme

Nach den Jahrzehnten, seitdem der PC in den 80er Jahren in immer mehr Büros und private Haushalte einzog, entwickelte sich die Form der Schadprogrammen in vielerlei Hinsicht. Das World Wide Web (WWW), wie wir es heute kennen, gab es in der damaligen Zeit nicht. Schadprogramme konnten daher nur über

[12] Vgl. BSI (2021), Die Aufbaustruktur des Cyber-Sicherheitsnetzwerks
[13] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.8.

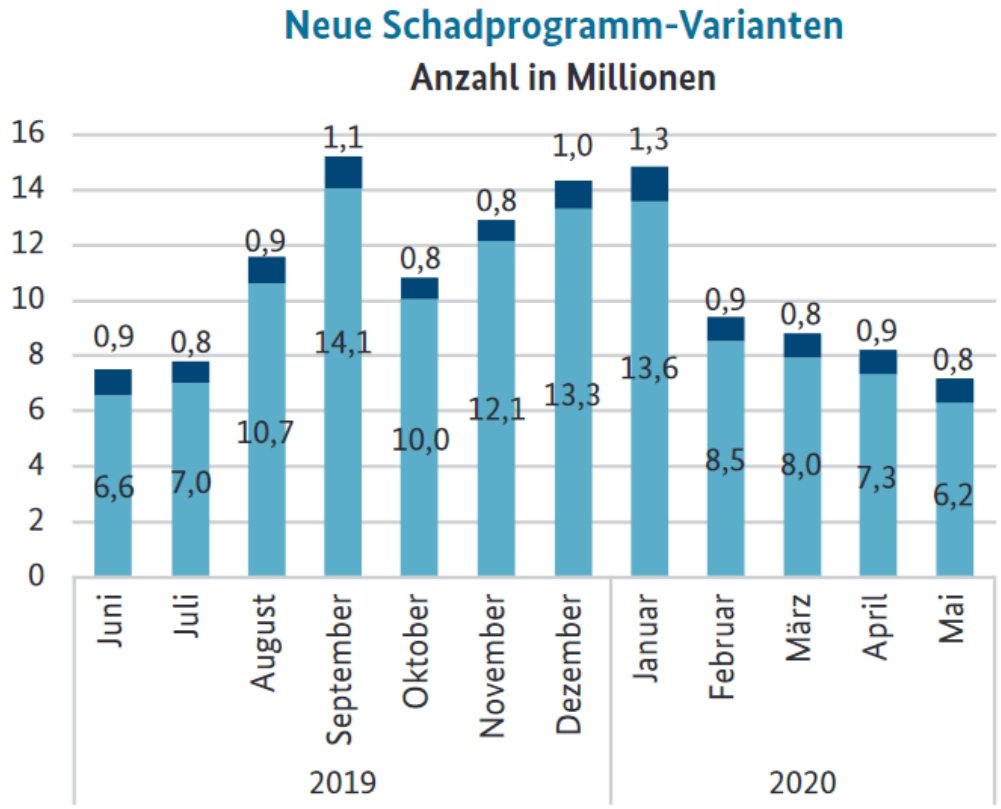

Abbildung 2: Neue Schadprogramm-Varianten; Quelle: BSI Lagebericht (2020), S. 9.

austauschbare Datenträger wie Disketten oder später CD-ROMs von einem System zum nächsten übertragen werden. Auch heute spielen externe Datenträger wie zum Beispiel USB-Sticks oder USB-Festplatten eine Rolle bei der Verbreitung der Schadsoftware [14]. Doch im heutigen Zeitalter ist das Internet eindeutig zum wichtigsten Infektionsweg geworden. [15] Schadprogramme sind lediglich multifunktionale Programme, die meist schädlich für das System sind. Im Zeitraum Juni 2019 bis Mai 2020, gab es rund 117,4 Millionen neue Schadprogramm-Varianten. In Abbildung 1 erkennt man deutlich starke Schwankungen in den Monaten zwischen Juli 2019 und August 2019, ebenso zwischen Januar 2020 und Februar 2020 (siehe Abbildung 1). Im Vergleich zu früheren Zeiträumen fiel der Verlauf im aktuellen Zeitraum gedämpfter, jedoch nicht weniger bedrohlich aus[16]. Der Grund hierfür lag insbesondere an der neuen Schadsoftware Emotet, welche

[14] Vgl. BSI Lagebericht (2020), S. 9.
[15] Vgl. BSI (2021), Schadprogramme – Fragen & Antworten.
[16] Vgl. BSI Lagebericht (2020), S. 10.

viele Schadprogramm-Varianten gebührt [17]. Durch gezielte Schadprogramm-Angriffe wird der Einsatz immer innovativer und intelligenter[18].

3.3.1.1 Phishing

Die Ausspionierung von Daten nennt sich Phishing und wird meist über täuschend echten E-Mails oder Malware-Spam [19] versendet. Die Ausspionierung bzw. Abgreifen personenbezogener Informationen oder Zugangsdaten [20] wird bei dieser Methode ausgenutzt. Durch eine Nachahmung von professionellen Websites, auf die das Opfer im Text verweist, werden als Köder überzeugend vorgetäuscht. Dieses Problem haben riesige Unternehmen mit einer umfangreichen Kundenreichweite wie zum Beispiel die deutsche Sparkasse[21] (siehe Abbildung 2).

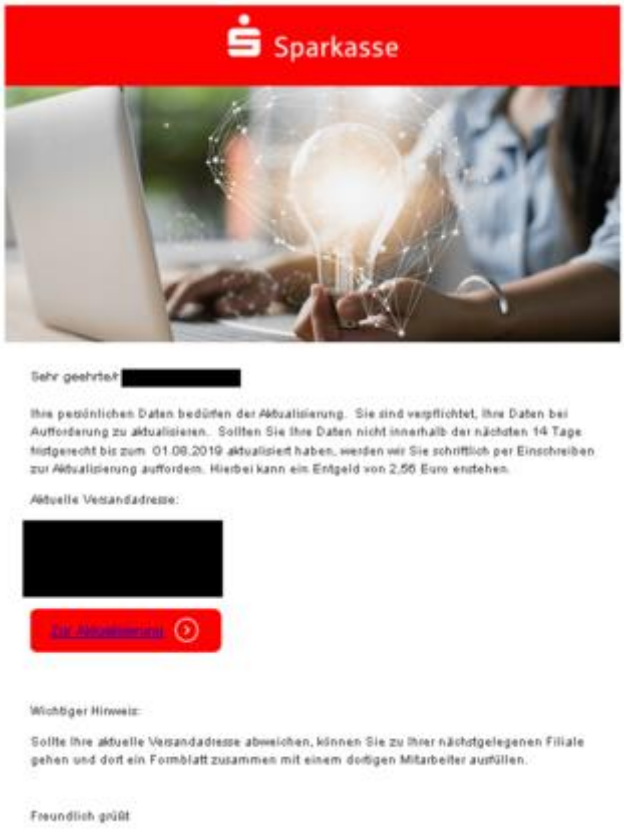

Abbildung 3: Beispiele für Phishing-Angriffe; Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html, 2021.

3.3.1.2 Ransomware

Die Ransomware bezeichnet Arten von Schadprogrammen, die den Zugriff auf die Daten einschränken beziehungsweise unterbinden wie zum Beispiel durch die Verschlüsselung bestimmter Daten. Für die Entschlüsselung der verschlüsselten Daten wird dann meist ein Lösegeld (engl. ransom) verlangt. Ein prominentes Beispiel über einen Ransomware Angriff der verhindert hätte werden können, ist der Wurm

[17] Vgl. BSI Lagebericht (2020), S. 10.
[18] Vgl. BSI Lagebericht (2020), S. 10.
[19] Vgl. BSI Lagebericht (2020), S. 15.
[20] Vgl. BSI Lagebericht (2020), S. 15.
[21] Vgl. BSI (2021), Beispiele für Phishing-Angriffe.

„WannaCry“ aus dem Jahr 2017[22]. In nur drei tagen verschlüsselte WannaCry in über 150 Ländern Daten auf mehr als 200.000 Windows Rechnern und Weltweit vermutlich über Millionen von Rechnern[23].

3.3.2 Distributed Denial of Service

Ein Distributed Denial of Service (DDoS) Angriff ist eine Form des Denial of Service (DoS), welche sich unter den Eigenschaften der Anfragen sich unterscheidet. Bei einem DDoS Angriff werden sehr viele Anfragen versendet aus unterschiedlichen Quellen[24]. Diese Quellen sind meist Rechner oder ganze Botnetze aus aller Welt. Ziel des Angriffs ist die Nicht-Erreichbarkeit einer Webseite, Produktionsstillstand oder Zusammenbruch der elektronischen Kommunikation[25]. Durch angepasste Maßnahmen wie zum Beispiel eine Firewall, ist es möglich solche Angriffe zu prävenieren. Der gezielte DDoS Angriff auf die Amazon Cloud-Sparte war vermutlich der größte DDoS Angriff aller Zeiten[26] mit 2,3 Terabit pro Sekunde.

3.4 Die Digitale Rettungskette

Die digitale Rettungskette ist eine Methodik, die kleine und mittlere Unternehmen sowie Einzelpersonen bei der Reaktion auf IT-Sicherheitsvorfälle durch Cyberangriffe unterstützen soll[27]. Die folgende Abbildung zeigt den Aufbau der digitalen Rettungskette:

[22] Vgl. BSI (2021), WannaCry: Weltweit mehrere hunderttausend Windows-Systeme betroffen.
[23] Vgl. BSI (2021), WannaCry: Weltweit mehrere hunderttausend Windows-Systeme betroffen.
[24] Vgl. BSI Lagebericht (2020), S. 29.
[25] Vgl. BSI Lagebericht (2020), S. 29.
[26] Vgl. AWS Shield (2020), S. 2.
[27] Vgl. Mehrtens, M. (2021): Digitale Rettungskette

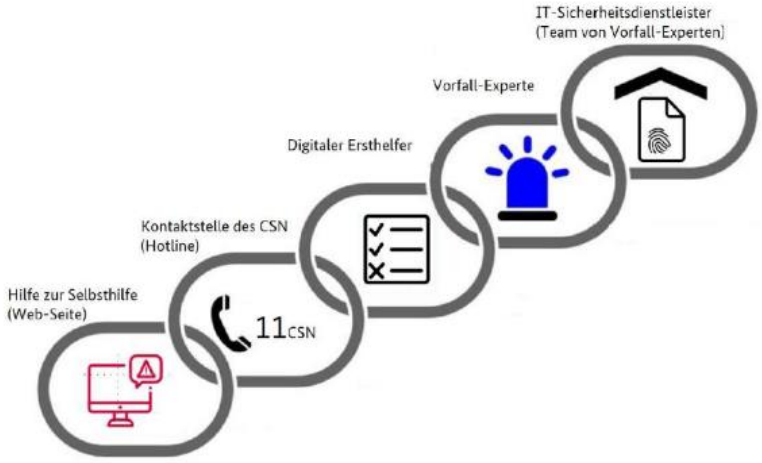

Abbildung 4: Ablauf der Digitalen Rettungskette; Quelle: Mehrtens, M. (2021).

Die strategische Ausrichtung und die Rahmenbedingungen des Cyber-Sicherheitsnetzwerks werden von einer Koordinierungsstelle im BSI gesteuert, die aus Störfallexperten sowie Vertretern von Behörden und Einrichtungen, Bildung und verschiedenen Interessengruppen zurückgreift. Digitale Ersthelfer, Unfallexperten und IT-Sicherheitsdienstleister arbeiten nach dem Konzept der digitalen Rettungskette.

3.4.1 Der Digitale Ersthelfer

Bei IT-Sicherheitsvorfällen hat der Digitaler Ersthelfer die Aufgabe, den Vorfall qualifiziert einzuschätzen und den Betroffenen bei kleineren IT-Ausfällen und IT-Vorfällen Erste Hilfe zu leisten sowie erste Handlungsempfehlungen zu geben[28]. IT-Ausfälle können jederzeit aufgrund technischer Mängel zu ungeplanten und unpassenden Zeiten auftreten. Daher ist es für einen störungsfreien Betrieb unabdingbar, angemessen auf IT-Ausfälle zu reagieren. Die Rolle des digitalen Ersthelfers besteht darin, bei IT-Sicherheitsvorfällen eine qualifizierte Begutachtung des Vorfalls durchzuführen und bei IT-Störungen und kleineren IT-Vorfällen Erste Hilfe für den Betroffenen zu leisten sowie erste Empfehlungen zu geben zum Handeln[29]. Ein digitaler Ersthelfer leistet noch keinen Vor-Ort-Dienst, sondern leistet Erste Hilfe hauptsächlich telefonisch oder im Einzelfall auch per E-Mail oder ähnlichem. Ein Ersthelfer wird mithilfe von 3 Modulen in Form eines

[28] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.14.
[29] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.16.

Online-Kurs in Videoformat ausgebildet. Nach dem Abschluss der Online Module wird nach einem Test das Zertifikat als Ersthelfer ausgestellt.

3.4.1.1 Aufgaben des Digitalen Ersthelfers

Die Bearbeitung eines IT-Sicherheitsvorfalls beginnt in dem Moment der Kontaktaufnahme des Betroffenen mit dem Digitaler-Ersthelfer und dessen Zustimmung zur Bearbeitung des Vorfalls. Innerhalb seiner Service-Zeiten steht der Digitaler-Ersthelfer für die Ersthilfe in der Digitalen Rettungskette des CSN zur Verfügung. Der Digitale Ersthelfer beginnt mit dem Vorfallbericht und generiert eine eindeutige CSN-Vorfall-nummer. Der Digitaler-Ersthelfer holt sich dessen Zustimmung für die nähere Analyse des Vorfalls. Der digitale Ersthelfer analysiert den Vorfall anhand des Handbuchs. Die Incident-Analyse wirkt innerhalb eines begrenzten Zeitrahmens sowie des fachlich-technischen Rahmens: Der digitale Ersthelfer muss zu einem bestimmten Zeitpunkt über das Ende der Level-One-Unterstützung und die weitere Vorgehensweise entscheiden[30]. Am Ende der Erstversorgung schickt der digitale Ersthelfer die Unfallmeldung per E-Mail an die zuständige Person. Wird der Vorfall nicht behoben, wird der betroffenen Person mitgeteilt, dass sie sich an das nächste oder jedes vorgelagerte Glied in der digitalen Wiederherstellungskette innerhalb des CSN wenden kann. IT-Sicherheitsdienstleister sollten mit einem Team von Veranstaltungsexperten durchziehen. Die im Ereignisbericht markierten Felder werden vom digitalen Ersthelfer in einem statistischen Bericht zusammengefasst, unabhängig davon, ob der Fehler korrigiert oder an den CSN gesendet wird[31].

„Der Digitaler-Erst-helfer weist den Betroffenen explizit darauf hin, dass der Sicherheitsvorfall anonymisiert in einer Statistik erfasst wird“[32].

3.4.1.2 Grenzen des Digitalen Ersthelfers

Digitale Ersthelfer sind durch die obige Anleitung eingeschränkt. Als Ersthelfer sind Fähigkeiten und Fachwissen aus relevanten Bereichen verschiedener Veranstaltungen gefragt. Wenn die aktuelle Expertise eines Vorfalls die Kompetenzen übersteigt, sollte der digitale Ersthelfer den Vorfall gemäß den

[30] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.18.
[31] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.22.
[32] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.22.

Richtlinien entweder an einen Vorfallspezialisten oder einen IT-Sicherheitsbeauftragten mit einem Team von Vorfallexperten übergeben. Eine Grenze ist erreicht, wenn der Umfang der Aufgabe über die Bearbeitung des Ereignisses hinausgeht. Um Missverständnisse zu vermeiden, werden die allgemeinen Bedingungen der Versammlung zu Beginn der Versammlung festgelegt.

3.4.2 Aufgaben der Vorfall Experten

Aufgabe der Vorfall Experten ist es, nach der Erstanalyse des digitalen Ersthelfers einen zusätzlichen Support-Service zur Reaktion auf IT-Sicherheitsvorfälle bereitzustellen[33]. Vorfallexperten sind meist unabhängige Sachverständige oder kleinere regionale IT-Sicherheitsdienstleitungen, die bei einem IT-Sicherheitsvorfall die Kontaktaufnahme sowohl telefonisch als auch vor Ort unterstützen. Grundlage der Tätigkeit ist der zu Beginn der Vorfallbearbeitung zwischen der betroffenen Person und dem Vorfallspezialisten abgeschlossene individuelle Dienstleistungsvertrag. Die Grundlage für die richtige Reaktion auf IT-Sicherheitsvorfälle stellt die Identifizierung des Problems dar. Die richtige Identifizierung spielt daher eine wichtige Rolle für eine erfolgreiche Lösung[34]. Um als Vorfall-Experte arbeiten zu können, muss ein Nachweis der Personenzertifizierung beim Bundesamt für Sicherheit in der Informationstechnik eingereicht werden. Auch muss eine Registrierung bei einer Geschäftsstelle vom Cyber-Sicherheitsnetzwerk erfolgen.

3.5 Leitfaden – IT-Sicherheitsvorfälle für Digitale Ersthelfer

3.5.1 Modul 1 – IT-Störungen durch technische Defekte

Der folgende Abschnitt behandelt die Grundsätze, die Ersthelfer beim Umgang mit IT-Sicherheitsvorfällen befolgen müssen[35]. An dieser Stelle sei noch einmal darauf hingewiesen, dass vor einer Handlungsempfehlung das Problem richtig erkannt werden muss. Ebenso kann kein separater oder ähnlicher Lösungsvorschlag verwendet werden. Im Zweifelsfall sollten Ersthelfer sofort auf die Möglichkeit

[33] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.15.
[34] Vgl. Mehrtens, M. (2021): Digitale Ersthelfer, S.16.
[35] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 8.

hinweisen, dass ein Spezialist für den Vorfall hinzugezogen werden kann. Das erste Modul beschreibt außerdem, wie IT-Ausfälle identifiziert und die häufigsten Ausfälle behoben werden können[36]. Es werden umfassende IT-Sicherheitsthemen behandelt. Unbehandelt kann es zu langfristigen Stromausfällen oder Netzwerkverschlechterungen kommen. Kriminelle sind besonders an Daten interessiert, die verarbeitet werden und nicht direkt mit dem Netzwerk. Bei einem IT-Sicherheitsvorfall ist es unerheblich, ob der Schaden eingetreten ist oder noch auftritt, da die meisten Betroffenen nicht erkennen, dass sie von dem IT-Sicherheitsvorfall betroffen sind. In einem solchen Fall ist der angerichtete Schaden nicht mehr vollständig heilbar, sondern nur bis zu einem gewissen Grad einzudämmen. Entsprechend der Definition zwischen IT-Störung und Vorfall werden die angehenden Ersthelfer gebeten, Beispiele für Vorfälle oder Sicherheitsvorfälle zu nennen. Eines der häufigsten Probleme ist beispielsweise, dass das Gerät nicht startet. [37] In Form von Videos werden direkte Handlungsempfehlungen zum Umgang mit individuellen Situationen gegeben.

3.5.2 Modul 2 – IT-Vorfälle durch Cyber-Angriffe

Modul 2 befasst sich mit Computervorfällen, die durch Cyberangriffe verursacht werden. Anschließend werden klassische oder typische IT-Vorfälle, die aus einem Cyber-Angriff resultieren, behandelt[38]. Der Digitale Ersthelfer ist somit in der Lage, vor allem IT-Vorfälle zu erkennen und, wenn möglich, Handlungsempfehlungen auszusprechen. Diese können gezielt eine Lösung für das zugrunde liegende Problem bieten, stellen aber im Wesentlichen Sofortmaßnahmen dar. Dies kann das mögliche Schadensausmaß begrenzen oder eine weitere Ausbreitung verhindern[39]. Dies kann den Computersicherheitsvorfall jedoch nicht abschließend beheben. Wenden Sie sich diesbezüglich an einen Unfallexperten.

3.5.3 Modul 3 – Serviceorientiertes Telefongespräch

Das Modul 3 befasst sich mit den Themen rund um die Führung eines serviceorientierten Telefongesprächs [40] . Kernstück des Moduls ist neben der

[36] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 8.
[37] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 20.
[38] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 21.
[39] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 24.
[40] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 47.

Auflistung der Rahmenbedingungen und des Verhaltens am Telefon die Erfassung und Eingrenzung des Problems und schließlich die Aussprache von Handlungsempfehlungen. Das Erste-Hilfe-Gespräch dient der Behebung des Problems. Eine endgültige Lösung ist jedoch nicht immer das Ergebnis, da digitale Retter nur im Rahmen ihrer Möglichkeiten agieren können. In diesen Fällen sollte ein Vorfallexperte kontaktiert werden[41]. Trotz alledem ist die Einhaltung der Verhaltensregeln von größter Bedeutung, um dem Anrufer Hilfe leisten und den zu erwartenden Schaden so gering wie möglich halten zu können. Nach Abschluss dieses Moduls kann ein potenzieller digitaler Ersthelfer Telefonanrufe entgegennehmen und das Opfer bei der Lösung des entsprechenden Problems unterstützen[42].

4 Fazit

Das BSI gestaltet die Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das Ziel vom BSI ist der sichere Einsatz von Informationstechniken auf mehreren Ebenen und somit ein Leitfaden für die Umsetzung. Dies bewirkt, dass wichtige Sicherheitsaspekte für die IT-Infrastrukturen und Anwendungen berücksichtigt werden. Durch stätige Verbesserungen von Sicherheitsstandards und Auswertungen von Daten können Schwachstellen und manipulierbare IT-Komponente verhindert werden. Von diesem Einfluss profitieren nicht nur Verbraucher, sondern auch KMUs. Regelmäßige Überprüfung vom Umsetzungsstand, Wirksamkeit, Kennzahlen und Zertifizierung auf Basis von IT-Grundschutz sind die ausschlaggebenden Punkte für eine Zukunftssichere IT. Durch die qualitativ steigenden Schadprogramme wird die Anwesenheit vom BSI und dem CSN eine noch wichtigere Rolle repräsentieren. Der Bedarf nach einer kompetenten Cybersicherheitsbehörde steigt und somit muss das BSI dem nachkommen.

[41] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 50.
[42] Vgl. BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, S. 51.

Quellenverzeichnis

Mitnick, N. (2010): Social Engineering: The Art of Human Hacking, (Hrsg.): John Wiley & Sons.

BSI (2020): Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf;jsessionid=48CDFB1F75A1AA72C07AB7E533C3AB54.1_cid500?__blob=publicationFile&v=2 , Zugriff am 09.07.2021.

BSI (2021): Fragen und Antworten zu Aufgaben und Themen des BSI, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html , Zugriff am 10.07.2021.

BSI (2021): Was sind die Aufgaben des BSI?, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html , Zugriff am 10.07.2021.

BSI (2021): Wen adressiert das BSI mit seinen Angeboten?, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html , Zugriff am 10.07.2021.

BSI (2021): Arbeitet das BSI mit anderen deutschen Behörden, zum Beispiel auch dem BND, zusammen?, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html , Zugriff am 10.07.2021.

BSI (2021): Was ist die Cyber-Sicherheitsstrategie?, https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html , Zugriff am 10.07.2021.

BSI (2020): Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf;jsessionid=48CDFB1F75A1AA72C07AB7E533C3AB54.1_cid500?__blob=publicationFile&v=2 , Zugriff am 10.07.2021.

BSI (2021): Schadprogramme – Fragen & Antworten, https://www.bsi-fuer-

buerger.de/BSIFB/DE/Risiken/Schadprogramme/schadprogramme_node.html , Zugriff am 26.01.2021

BSI (2021): WannaCry: Weltweit mehrere hunderttausend Windows-Systeme betroffen, https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Schadprogramme/Ransomware/ransomware_node.html , Zugriff am 11.07.2021.

BSI (2021): Beispiele für Phishing-Angriffe, https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/BeispielePhishingAngriffe/beispielephishingangriffe_node.html , Zugriff am 11.07.2021.

BSI (2021): Cyber-Sicherheitsnetzwerk, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html, Zugriff am 11.07.2021.

BSI (2021): Cyber-Sicherheitsnetzwerk, Eckpunktepapier Version 3.1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210122_Eckpunktepapier.pdf?__blob=publicationFile&v=8 , Zugriff am 11.07.2021.

Mehrtens, M. (2021): Digitale Ersthelfer. Cyber Sicherheitsnetzwerk des BSI (CSN), 2021.

BSI (2021): Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer, Version 1.0, https://moodle.hsnr.de/pluginfile.php/734500/mod_resource/content/1/Leitfaden_Digitaler-Ersthelfer_1.0.pdf , Zugriff am 12.07.2021.

Eidesstattliche Erklärung

Ich versichere hiermit Eides statt, die von mir vorgelegte Arbeit selbstständig verfasst zu haben. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Arbeiten anderer entnommen sind, habe ich als entnommen kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Düsseldorf, 11 Juli 2021	Stavros Giannis
Ort, Datum	Rechtsverbindliche Unterschrift