Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall-Experten

Version 2.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: info@cyber-sicherheitsnetzwerk.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Inhaltsverzeichnis 3

Abbildungsverzeichnis 10

Tabellenverzeichnis 11

1 Einführung in das Cyber-Sicherheitsnetzwerk (VP&VE) 12

1.1 Einführung 12

1.2 Intention und Lernziele 12

1.3 Überblick über relevante Gesetze 13

1.3.1 BSI Gesetz 13

1.3.2 EU-Datenschutz-Grundverordnung (EU-DSGVO) 13

1.3.3 Bundesdatenschutzgesetz (BDSG) 13

1.3.4 Telemediengesetz (TMG) 14

1.3.5 Telekommunikationsgesetz (TKG) 14

1.3.6 Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) 14

1.3.7 Urheberrechtsgesetz (UrhG) 14

1.3.8 IT-Strafrecht im Strafgesetzbuch (StGB) 14

1.3.9 Gesetz gegen den unlauteren Wettbewerb (UWG) 14

1.4 Meldepflichten 15

1.4.1 Meldepflichten und -prozesse eines Betroffenen 15

1.4.2 Meldepflichten kritischer Infrastrukturen 15

1.4.3 Meldepflichten und -prozesse 15

1.5 Kurzüberblick über das Cyber-Sicherheitsnetzwerk (CSN) 16

1.5.1 Aufbau und Struktur 16

1.5.1.1 Organisatorische Anlaufstelle 16

1.5.1.2 Strategische Unterstützung 17

1.5.1.3 Von einem Vorfall betroffene Personen und Institutionen 17

1.5.1.4 Registrierte Teilnehmer 17

1.5.1.5 Aktive Helferinnen und Helfer sowie Expertinnen und Experten des CSN 17

1.5.2 Die Digitale Rettungskette 17

1.5.2.1 Schnittstellen zu anderen Hotlines und Anlaufstellen 18

1.5.3 Qualifizierung und Erfahrungsaustausch 18

1.5.3.1 Selbststudium 18

1.5.3.2 Schulungen durch Trainerinnen und Trainer sowie Schulungsanbieter 19

1.5.3.3 Austausch in Regionale Foren sowie Forenleiterinnen und Forenleiter 19

1.5.3.4 Erfahrungsaustausch 19

1.5.4 Helferinnen und Helfer des Cyber-Sicherheitsnetzwerks 19

1.5.4.1 Der kompetente „Digitale Ersthelfer“ 19

1.5.4.2 Der geschulte Vorfall-Praktiker 20

1.5.4.3 Der zertifizierte Vorfall-Experte 20
1.5.4.4 Der zertifizierte IT-Sicherheitsdienstleiter: Vorfallbearbeitung 21
1.5.4.5 Einbindung von Fachpersonal 21
1.5.4.6 Zielsetzung einer betroffenen Person oder Institution 21
2 Verhalten am Telefon und nichttechnische Maßnahmen (VP) 23
2.1 Intention und Lernziele 23
2.2 Serviceorientiertes Telefongespräch 23
2.2.1 Professionelles Verhalten am Telefon 23
2.2.2 Verhaltensregeln IT-Sicherheitsvorfall 24
2.3 Nicht technische Maßnahmen 25
3 Gefährdungen und Angriffsformen (VP) 27
3.1 Einführung 27
3.2 Intention und Lernziele 27
3.3 Begriffserklärungen 27
3.3.1 Angriff 27
3.3.2 Angriffsvektor 27
3.3.3 Bedrohung (englisch "threat") 27
3.3.4 Gefährdung (englisch "applied threat") 28
3.3.5 Schwachstelle (englisch "vulnerability") 28
3.3.6 Wert (englisch "asset") 28
3.4 Zusammenhang 28
3.5 Arten von Angriffen bzw. Angriffsformen 29
3.6 Ursachen von Angriffen 30
3.7 Angriffsmethoden 31
3.8 Phasen eines Cyber-Angriffs 32
3.8.1 Angreifertypen 32
3.8.2 Angriffsabsichten und Angriffsziele 34
3.8.3 Angriffsvorbereitung 34
3.8.4 Angriffswerkzeug 35
3.8.5 Angriffstarnung 37
3.8.6 Angriffspunkte und Spurenbeseitigung 37
4 Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen (VE) 39
4.1 Einführung 39
4.2 Intention und Lernziele 39
4.3 Notwendige Basiskenntnisse 39
4.3.1 Betriebssysteme 40
4.3.2 Netzwerk 40
4.3.3 Schadprogramm 41

4.4 Angriffsformen 41
4.4.1 Identitätsdiebstahl (Phishing) 41
4.4.2 Ransomware 42
4.4.3 Distributed Denial-of-Service (DDoS) 42
4.4.4 Botnetz 43
4.4.5 Advanced Persistent Threat 43
4.5 Darstellung forensischen Vorgehens 43
4.5.1 Methode Live-Forensik 44
4.5.2 Methode Dead-Forensik 45
4.5.3 Gegenüberstellung der IT-Forensik-Methoden 45
4.6 Datensammlung/-erhebung 45
4.6.1 Full-Image 46
4.6.2 Memory-Image 46
4.6.3 Triage-Forensik 46
4.7 Datenanalyse 46
4.8 Toolhandling 47
4.9 Grenzen der Analyse 47
4.9.1 Beweissicherung fehlerhaft oder unzureichend 48
4.9.2 Beauftragung wird überstiegen 48
4.9.3 Analyse führt zu keinen Ergebnissen 48
4.9.4 Betroffener verzichtet auf eine detaillierte Analyse 48
5 Ablauf des Standardvorgehens (VP&VE) 49
5.1 Einführung 49
5.2 Intention und Lernziele 49
5.3 Identifikation des IT-Sicherheitsvorfalls 49
5.3.1 Kontaktaufnahme über den Digitalen Ersthelfer 50
5.3.2 Direkte Kontaktaufnahme 50
5.4 Eindämmung des Schadensausmaßes 50
5.4.1 Isolierung des infizierten Systems 51
5.4.2 Sperrung und Änderung von Zugangsdaten 51
5.4.3 Arbeiten am betroffenen System einstellen 51
5.4.4 Gerät nicht herunterfahren 52
5.4.5 Keine weiteren Maßnahmen eigenständig umsetzen 52
5.5 Ermittlung der Ursache 52
5.5.1 Beweissicherung 53
5.5.2 Analyse 54
5.5.3 Gesamtbewertung 54
5.6 Wiederherstellung der Systeme 55

6 Behandlung von speziellen IT-Sicherheitsvorfällen (VP&VE) 56
6.1 Phishing 56
6.1.1 Einführung 56
6.1.2 Intention und Lernziele 56
6.1.3 Arten von Phishing 56
6.1.3.1 Spear-Phishing 56
6.1.3.2 Whaling 57
6.1.3.3 Emotet / Dynamite Phishing 57
6.1.4 Abgrenzung / Einordnung zu verwandten Themen 57
6.1.4.1 Social Engineering 57
6.1.4.2 Gefälschte Online-Shops 57
6.1.5 Phishing-Kanäle 57
6.1.5.1 E-Mail 58
6.1.5.2 Anrufe 58
6.1.5.3 SMS und Messenger-Anwendung 58
6.1.5.4 Social-Media-Kanäle 58
6.1.5.5 Typosquatting 58
6.1.6 Erkennung von Phishing-Angriffen 58
6.1.6.1 Gefälschte Absenderin oder Absender 59
6.1.6.2 Persönliche Anrede 59
6.1.6.3 Verunsicherung des Opfers 59
6.1.6.4 Aufruf zu ungewöhnlichen Aktionen 60
6.1.6.5 Sprachliche Ungenauigkeiten 60
6.1.6.6 Analyse von E-Mail-Headern 60
6.1.7 Reaktion auf erfolgreiche Phishing-Attacken 61
6.1.7.1 Sperren von Benutzerkonten 61
6.1.7.2 Kontaktaufnahme zum Plattform-Betreibenden 61
6.1.7.3 Ändern der betroffenen Zugangsdaten auf allen Webseiten 62
6.1.7.4 Achten auf ungewöhnliche Aktivitäten bei den betroffenen Benutzerkonten 62
6.1.7.5 Datenschutzbeauftragten alarmieren 62
6.1.7.6 Anzeige bei der Strafverfolgungsbehörde erstatten 62
6.1.8 Schutz gegen Phishing 62
6.1.8.1 E-Mail-Signaturen 62
6.1.8.2 Webseiten selbstständig aufrufen, anstatt auf Links zu klicken 63
6.1.8.3 Nachfragen bei vermeintlicher Absenderin oder beim vermeintlichen Absender über zweiten (sicheren) Kanal 63
6.1.8.4 Grundsätzliches Misstrauen bei Nachrichten mit Anhängen oder Links 63
6.1.8.5 2-Faktor-Authentifizierung 63
6.2 Ransomware 64

6.2.1 Einführung 64
6.2.2 Intention und Lernziele 64
6.2.3 Einfallstor 65
6.2.4 Bewältigung des Vorfalls 65
6.2.4.1 Isolierung betroffener Systeme 65
6.2.4.2 Bereinigung der Systeme 65
6.2.4.3 Einspielung von Backups 66
6.2.4.4 Selbstständige Entschlüsselung der Daten 66
6.2.4.5 Analyse von Log-Dateien 66
6.2.4.6 Bezahlung des Lösegelds 66
6.2.5 Kommunikation 67
6.2.5.1 Interne Mitarbeitende 67
6.2.5.2 Strafverfolgungsbehörden 67
6.2.5.3 Versicherungen 67
6.2.5.4 Geschäftspartnerinnen und Geschäftspartner 68
6.2.5.5 Angreifende 68
6.2.5.6 Datenschutzbeauftragte und Datenschutzbeauftragter 68
6.2.5.7 Juristinnen und Juristen 69
6.2.6 Ransomware verhindern 69
7 Remote-Unterstützung (VP) 70
7.1 Einführung 70
7.2 Intention und Lernziele 70
7.3 Begriffsbestimmung der Fern- oder Remote-Unterstützung 70
7.4 Voraussetzungen und Rahmenbedingungen 71
7.4.1 Technische Voraussetzungen 71
7.4.2 Rahmenbedingungen 72
7.5 Verbindungs- und Zugriffsmöglichkeiten 72
7.5.1 Konferenztools 73
7.5.2 Fernwartungstools 73
7.5.3 Virtual Private Network (VPN) 74
7.6 Datensammlungs- und Analysemöglichkeiten 74
8 Vorfallsbearbeitung bei IT-Systemen „abseits der üblichen Büroanwendung“ (VP&VE) 75
8.1. Einführung 75
8.2 Intention und Lernziele 75
8.3. Notwendige Basiskenntnisse 75
8.4 Unterschiede von OT zu Standard-IT 76
8.5 Weiteres relevantes Fachpersonal 77
8.6 Ablauf des Standardvorgehens bei OT 78

8.6.1 Identifikation des Sicherheitsvorfalles 78
8.6.2 Eindämmung des Schadensausmaßes 78
8.6.3 Beweissicherung & Analyse 78
8.6.4 Wiederherstellung 78
9 Vor-Ort-Unterstützung: Überblick verschaffen (VE) 79
9.1 Einführung 79
9.2 Intention und Lernziele 79
9.3 Vorfall-Experte als Krisenmanager etablieren 79
9.3.1 Erscheinungsbild 80
9.3.2 Körpersprache 80
9.3.3 Ausdrucksweise 80
9.4 Analysefähigkeit des Unternehmens einschätzen 80
9.4.1 Personalressourcen und Kompetenzen identifizieren 81
9.4.1.1 Identifikation der Ansprechpartnerinnen und Ansprechpartner 81
9.4.1.2 Kompetenzen der Ansprechpartnerinnen und Ansprechpartner 81
9.4.1.3 Einbindung von externen Dienstleistern 82
9.4.2 Analysieren der IT-Infrastruktur des betroffenen Unternehmens 82
9.4.2.1 Netzwerkdokumentation 82
9.4.2.2 Systemdokumentation 82
9.4.2.3 Analyse- und Auswertungseinrichtungen 83
9.5 Organisatorische Voraussetzungen ermitteln 83
9.5.1 Beschreibung des IT-Sicherheitsvorfalls 83
9.5.2 Ermittlung von Notfallplänen 83
9.5.3 Einbindung von Dienstleistern 84
9.6 Festlegung von Rahmenbedingungen der Zusammenarbeit 84
9.6.1 Geheimhaltungsvertrag 84
9.6.2 Auftragsverarbeitungsvertrag 84
9.6.3 Kommunikationswege 85
9.6.4 Dokumentation 85
9.6.5 Was kann nicht geleistet werden? 85
10 Vor-Ort-Unterstützung: Vorfallbearbeitung (VE) 86
10.1 Einführung 86
10.2 Intention und Lernziele 86
10.3 Analyse des IT-Sicherheitsvorfalls 86
10.3.1 Tiefgründige Analyse 87
10.3.2 Identifikation betroffener Systeme 87
10.3.3 Analyse des Auslösers 87
10.3.4 Schadensfeststellung 88

10.4 Planung der Vorgehensweise 88
10.5 Notbetrieb 89
10.5.1 Prüfung 90
10.5.2 Herstellung des Notbetriebes 90
10.5.2.1 Isolierung 90
10.5.2.2 Verlagerung 90
10.6 Bereinigung der Systeme 91
10.6.1 Beseitigung des Schadprogramms 91
10.6.2 Neuinstallation des Betriebssystems 92
10.7 Wiederherstellung der Systeme 92
10.8 Nachbereitung 92
11 Nach einem Vorfall ist vor einem Vorfall (VP&VE) 94
11.1 Einführung 94
11.2 Intention und Lernziele 94
11.3 Sensibilisierung für Prävention 94
11.3.1 IT-Systemlandschaft 95
11.3.2 Systemhärtung 95
11.3.3 Schwachstellenmanagement 95
11.3.4 Mitarbeitende 96
11.4 Aufbau eines Sicherheitsbewusstseins 96
11.5 Analyse von Geschäftsprozessen 97
11.6 Aufbau eines Sicherheits- und Notfallkonzepts 98
11.6.1 Sicherheitskonzept 98
11.6.2 Notfallkonzept 98
11.7 Konzeption von Übungen 99
12 Anhang 100
12.1 Übersicht über den Vorfall-Bearbeitungsprozess 100
12.2 Checkliste zur IT-Infrastruktur-Analyse 101

Abbildungsverzeichnis

Abbildung 1: Begriff Gefährdung 29
Abbildung 2: Phasen eines Cyber-Angriffs 32
Abbildung 3: Zeitliche Einordnung der IT-Forensik 44
Abbildung 4: Auszug aus einem E-Mail-Header 60
Abbildung 5: Automatisierungspyramiede 76
Abbildung 6: Übersicht über den Vorfall-Bearbeitungsprozess 100

Tabellenverzeichnis

Tabelle 1: Gegenüberstellung der IT-Forensik-Methoden 45
Tabelle 2: Hinweise zum Erscheinungsbild 80
Tabelle 3: Hinweise zur Körpersprache 80
Tabelle 4: Hinweise zur Ausdrucksweise 80
Tabelle 5: Kompetenz-Checkliste für Ansprechpartnerinnen und Ansprechpartner 81
Tabelle 6: Fragestellungen zur Planung der Vorgehensweise 89
Tabelle 7: Checkliste zur Dokumentation 101
Tabelle 8: Checkliste zur Analyse- und Auswertungseinrichtungen 101

1 Einführung in das Cyber-Sicherheitsnetzwerk (VP&VE)

Der vorliegende Leitfaden ersetzt den Leitfaden „Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Experten“. Mit der Einführung der neuen Rolle des Vorfall-Praktikers wurden die Inhalte erweitert.

Dieser Leitfaden ist Grundlage für die Schulung zum Vorfall-Praktiker, bzw. die Schulung zum Vorfall-Experten. Die jeweilige Relevanz der Kapitel für die Prüfung ist durch die farblichen Abkürzungen VP (= Vorfall-Praktiker) und VE (=Vorfall-Experte) in der jeweiligen Kapitelüberschrift gekennzeichnet.

1.1 Einführung

Cyberkriminalität ist in den heutigen Zeiten der Digitalisierung allgegenwärtig und nimmt außerdem stetig zu. Die steigende Zahl digitaler Geräte bietet Cyberkriminellen immer neue potenzielle Ziele. Allein in Deutschland bewegt sich der jährlich summierte Schaden durch Cyberkriminalität in großer Höhe und kann existenzbedrohend sein. Sowohl Institutionen jeder Größe als auch Privatpersonen können dabei Opfer werden.

Aufgrund der starken Abhängigkeit von einer funktionierenden Informationstechnik, ist es essentiell angemessen auf IT-Sicherheitsvorfälle zu reagieren und somit das Schadensausmaß möglichst auf ein Minimum zu reduzieren. Nicht jede Institution besitzt hierbei die Kompetenzen, um eine ordnungsgemäße Reaktion gewährleisten zu können. In diesem Fall gilt es, sich über geeignete Kanäle Hilfe zu suchen. Bei der Behandlung von IT-Sicherheitsvorfällen kann dabei ein ausgebildeter Vorfall-Praktiker oder Vorfall-Experte[1] konsultiert werden.

1.2 Intention und Lernziele

Dieses Kapitel stellt das Einstiegsmodul Qualifizierung zum Vorfall-Praktiker und Vorfall-Experte dar und beschäftigt sich mit den grundlegenden Rahmenbedingungen im Zuge der Leistungserbringung. Dabei wird ein grober Überblick über relevante Gesetze vermittelt, Meldepflichten aufgezeigt sowie die Rolle des Vorfall-Praktikers und Vorfall-Experten in der Digitalen Rettungskette definiert. Neben den Verantwortlichkeitsgrenzen wird die Zielvorstellung einer betroffenen Person oder Institution präzisiert.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

 Rechtliche Vorgaben zur Informationssicherheit und IT-Compliance wiederzugeben.

 Meldeprozesse hinsichtlich möglicher Meldepflichten zu reflektieren.

 Die Rolle des Vorfall-Praktiker und Vorfall-Experte in die Digitale Rettungskette einzuordnen.

 Die Grenzen der Leistungserbringung sowie die Zielvorstellung eines Betroffenen nachzuvollziehen.

[1] auch bekannt als Incident Handler oder First Responder.

1.3 Überblick über relevante Gesetze

Um den Gefahren, die die hohe Abhängigkeit von IT-Systemen mit sich bringen, entgegenzuwirken, hat der Gesetzgeber in verschiedenen Gesetzen Anforderungen definiert. Die Anforderungen richten sich hauptsächlich an die Bereiche Informationssicherheit, Informationsverfügbarkeit, Datenaufbewahrung und Datenschutz.

Die diversen Gesetzesabschnitte verfolgen das Ziel, den bestmöglichen Schutz von Informationen und Informationssysteme zur Wahrung der drei Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität) zu erreichen" - Es sollen nicht nur die Informationen geschützt werden, sondern auch die Systeme, die diese verarbeiten.

Die nachfolgend aufgelisteten Gesetze haben eine besondere Bedeutung hinsichtlich der Informationssicherheit und enthalten konkrete Vorgaben oder Regelungen zum Umgang mit Informationen, Daten und Informationstechnik.

Die verschiedenen Gesetzestexte können auf der Webseite Gesetze im Internet abgerufen werden. Es ist zu beachten, dass für die folgenden Gesetze ein Abgleich zur Aktualität erfolgen sollte.

Die nachfolgenden Gesetze und Vorgaben nicht abschließend, sondern nur beispielhaft. Jeder Vorfall-Praktiker und Vorfall-Experte sollte sich über die für ihn relevante aktuelle Gesetzeslage auf dem Laufenden halten.

1.3.1 BSI Gesetz

Heutige Grundlage der Arbeit des BSI ist das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ (BSI-Gesetz/BSIG), welche zunächst als „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ am 20. August 2009, nach einer grundlegenden Überarbeitung, in Kraft trat und seither mehrere Male novelliert wurde. Darüber hinaus gibt es eine Reihe von spezialgesetzlichen Regelungen, in denen Aufgaben des BSI im Zusammenhang mit bestimmten Themen definiert sind, etwa im Rahmen der Energiewende oder im Bereich der Telekommunikation. Entscheidend erweitert wurden die Aufgaben und Befugnisse des BSI durch das im Juli 2015 in Kraft getretene „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz).). Mit verbindlichen Mindestanforderungen an die IT-Sicherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen (KRITIS) und erhöht die Netzsicherheit in den Bereichen, deren Ausfall oder Beeinträchtigung dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätte. Außerdem besteht eine Verpflichtung von KRITIS-Betreibern zur Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI.

Mit dem Entwurf des IT-Sicherheitsgesetzes 2.0 wird der Auftrag des BSI 2021 erneut erweitert, um den Herausforderungen der fortschreitenden Digitalisierung zu begegnen. Mit dem IT-SiG 2.0 wird der digitale Verbraucherschutz im BSI verankert. Als Gestalter einer sicheren Digitalisierung in Deutschland unterstützt das BSI Verbraucherinnen und Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten, etwa durch die Einführung eines IT-Sicherheitskennzeichens.

Das SiG 2.0 sieht zudem weitere Befugnisse des BSI gegenüber der Bundesverwaltung vor. Hier werden die Kontroll- und Prüfbefugnisse zum Schutz der Regierungsnetze ausgebaut. Bei wesentlichen Digitalisierungsvorhaben des Bundes soll das BSI frühzeitig beteiligt werden.

1.3.2 EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die europäische Datenschutzgrundverordnung (EU-DSGVO) ist eine Verordnung der Europäischen Union. Sie zielt darauf ab, den Datenschutz in Europa zu vereinheitlichen und somit gleiche Datenschutzstandards für alle Mitgliedsstaaten zu schaffen. Die Datenschutz-Grundverordnung gilt seit dem 25. Mai 2018.

1.3.3 Bundesdatenschutzgesetz (BDSG)

Das neu konzipierte Bundesdatenschutzgesetz (BDSG) ergänzt ab dem 25. Mai 2018 die unmittelbar geltende Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) um die Bereiche, in denen die EU-Verordnung

den Mitgliedstaaten Gestaltungsspielräume belässt. Daneben werden mit dem BDSG wesentliche Teile der Richtlinie (EU) 2016/680 (Datenschutz-Richtlinie Polizei und Justiz) umgesetzt.

1.3.4 Telemediengesetz (TMG)

Das Telemediengesetz (TMG) regelt die rechtlichen Rahmenbedingungen für alle Telemedien in Deutschland. Unter Telemedien versteht man nahezu alle Angebote, die im Internet zu finden sind, wie zum Beispiel Webshops, Informationsdienste, Webportale, private Websites und viele weitere.

1.3.5 Telekommunikationsgesetz (TKG)

Der Zweck des Telekommunikationsgesetzes (TKG) ist, durch technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten. Während das TMG Ausgestaltungen von Angeboten im Internet regelt, gibt das TKG Regelungen vor unter welchen Voraussetzungen das Internet und andere Telekommunikationsleistungen wie die Telefonie, bereitgestellt werden dürfen.

1.3.6 Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)

Seit dem 1. Dezember 2021 gilt das neue Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG), das die bislang bestehenden Datenschutzregelungen aus dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) in einem neuen Gesetz bündelt. Ziel des TTDSG ist es einerseits, die das TKG und TMG betreffenden datenschutzrechtlichen Bestimmungen an die EU Datenschutz-Grundverordnung (DSGVO) anzupassen und andererseits, Teile der ePrivacy-Richtlinie (RL 2002/58/EG in der durch die RL 2009/136/EG geänderten Fassung) in nationales Recht umzusetzen.

1.3.7 Urheberrechtsgesetz (UrhG)

Die Urheberinnen und Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe des Urheberrechtsgesetzes (UrhG). Vorgaben, die die Urheber- aber auch die Verwertungsrechte regeln, ergeben sich zum einen aus den allgemeinen Regelungen für urheberrechtliche Werke und speziell für Software aus den §§ 69a-69g UrhG.

1.3.8 IT-Strafrecht im Strafgesetzbuch (StGB)

Das Strafgesetzbuch (StGB) regelt in Deutschland die Kernmaterie des materiellen Strafrechts. In diversen Paragrafen des StGB wird versucht den vermehrt auftretenden Straftaten im Internet entgegenzuwirken (beispielsweise Computerbetrug § 263a StGB, Ausspähen von Daten u.a. §§ 202 a-c StGB, Datenveränderung § 303a StGB, Computersabotage § 303b StGB). Im Rahmen der Bearbeitung eines Vorfalls ist es möglich, dass der Vorfalls-Experte Einsicht in nicht für ihn bestimmte Daten einnehmen kann. Daher sei an dieser Stelle im Besonderen die Datenhehlerei gem. § 202d StGB erwähnt, mit dem Hinweis, dass nichtöffentliche Daten nicht durch den Vorfall-Praktiker und Vorfall-Experten unbefugten Stellen zur Verfügung gestellt werden dürfen.

1.3.9 Gesetz gegen den unlauteren Wettbewerb (UWG)

Das Gesetz gegen den unlauteren Wettbewerb (UWG) dient dem Schutz der Mitbewerberinnen und Mitbewerber, der Verbraucherinnen und Verbraucher sowie der sonstigen Marktteilnehmerinnen und Marktteilnehmer vor unlauteren geschäftlichen Handlungen. Es schützt zugleich das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb.

1.4 Meldepflichten

Die richtige Reaktion auf IT-Sicherheitsvorfälle schließt oftmals eine Meldung des Sachverhalts an verschiedene Stellen mit ein. Die Meldung kann dabei gesetzlich oder vertraglich verpflichtend sein oder auch auf freiwilliger Basis erfolgen. Die vorgeschriebenen Meldungen sind von den Unternehmen, bspw. den KRITIS-Betreibern, selbstständig durchzuführen. Im Rahmen der Vorfallbearbeitung sollte durch den Helfenden sollten kein Rechtsrat erfolgen.

1.4.1 Meldepflichten und -prozesse eines Betroffenen

Liegt aufgrund eines IT-Sicherheitsvorfalls eine Datenschutzverletzung bzw. ein Vorstoß gegen die Regelungen der DSGVO vor, haben die Verantwortlichen gemäß Art. 33 DSGVO unverzüglich, möglichst aber innerhalb von 72 Stunden nach Kenntnisnahme die zuständige Aufsichtsbehörde zu informieren. Geht von dem Verstoß ein hohes Risiko aus, so sind gem. Art. 34 DSGVO zudem die betroffenen Personen zu benachrichtigen. Ein IT-Sicherheitsvorfall, der gleichzeitig eine Datenschutzverletzung darstellt, liegt vor, wenn es sich bei dem Angriffsziel um personenbezogene Daten handelt oder handeln könnte. Dies ist beispielsweise der Fall, wenn sich eine Angreiferin oder ein Angreifer Zugriff auf personenbezogene Daten verschaffen konnte oder personenbezogene Daten von einer Angreiferin oder einem Angreifer veröffentlicht werden.

Auch aus abgeschlossenen Verträgen mit Kunden und Dienstleistern können Meldepflichten beim Auftreten eines IT-Sicherheitsvorfalls verankert sein. In diesem Fall hat die Meldung an diese zu erfolgen.

Neben den gesetzlichen und vertraglichen Meldepflichten hat eine betroffene Person zudem die Möglichkeit einen IT-Sicherheitsvorfall bei zentralen Stellen[2] zu melden, die sich mit der Behandlung von Sicherheitsvorfällen beschäftigen. Eine solche Meldung erfolgt i. d. R. auf einer freiwilligen Basis und ist nicht verpflichtend, ist jedoch zu empfehlen. Auf diese Weise kann eine breite Masse auf aktuelle Bedrohungen hingewiesen werden und Maßnahmen zum Schutz empfohlen werden.

1.4.2 Meldepflichten kritischer Infrastrukturen

Die Meldepflicht gem. § 8b Absatz 4 BSI-Gesetz betrifft Betreiber Kritischer Infrastrukturen, die anhand der in der BSI-Kritisverordnung (BSI-KritisV) festgesetzten Schwellenwerte als Kritische Infrastrukturen im Sinne des BSI-Gesetzes identifiziert wurden.

„Betreiber Kritischer Infrastrukturen haben folgende Störungen unverzüglich über die Kontaktstelle an das BSI zu melden:

- Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,
- erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können. [...]"

Die Meldung muss unverzüglich nach Erkennung der IT-Störung erfolgen, d. h. ohne schuldhaftes Zögern. Alle Erkenntnisse, die zum Zeitpunkt der Meldung vorliegen, müssen an das BSI gemeldet werden. Dabei gilt für die Erstmeldung grundsätzlich Schnelligkeit vor Vollständigkeit.

1.4.3 Meldepflichten und -prozesse

Für den Vorfall-Praktiker und Vorfall-Experten existieren in erste Linie keine vergleichbaren Meldepflichten im Hinblick auf den Betroffenen, die durch gesetzliche oder vertragliche Anforderungen entstehen könnten.

[2] z. B. bei der ACS - Allianz für Cyber-Sicherheit

Der Vorfall-Praktiker und Vorfall-Experte sollten dennoch über die entsprechenden Meldepflichten einer betroffenen Person informiert sein und diese dabei unterstützen können.

Ähnlich verhält sich diese Thematik bezüglich der freiwilligen Meldung. In diesem Fall kann der Meldeprozess durch den Vorfall-Praktiker und Vorfall-Experten angestoßen und auch letztlich durchgeführt werden. Dabei ist jedoch die Zustimmung der betroffenen Person erforderlich. Ohne diese ist eine Meldung durch den Vorfall-Experten ggf. nicht erlaubt, auch wenn es sich möglicherweise um eine neue oder weiterentwickelte Angriffsform handelt und infolgedessen die Meldung wichtig wäre, um andere Personen und Unternehmen darauf aufmerksam zu machen.

1.5 Kurzüberblick über das Cyber-Sicherheitsnetzwerk (CSN)

Die Digitalisierung schreitet immer weiter und schneller voran. Heutzutage werden in fast allen Unternehmen wichtige und sensible Geschäftsprozesse mit Hilfe von moderner Informationstechnik (IT) durchgeführt.

Aber was passiert, wenn sich „unberechtigte“ Dritte Zugang zu unseren digitalen Systemen verschaffen? Wenn Daten abfließen, Schadprogramme eingespielt wird oder erpresserische Forderungen gestellt werden, so dass dadurch die Nutzung der IT langfristig nicht möglich ist?

Ein solcher Vorfall kann eine existenzbedrohende Situation für ein Unternehmen bedeuten!

Das Risiko, dass Ihr Unternehmen von einem Cyber-Angriff bedroht sein könnte, ist nicht gering und wird sehr oft unterschätzt. Doch was ist zu tun, wenn dieser Fall eintritt?

Das Cyber-Sicherheitsnetzwerk steht als erste Anlaufstelle bei IT-Sicherheitsvorfällen zur Verfügung und bietet eine effiziente Unterstützung bei der Vorfallbehandlung von IT-Sicherheitsvorfällen. Die Helferinnen und Helfer der „Digitalen Rettungskette“ unterstützen dabei mit ihrer fachlichen Expertise. Die Art und Weise der Unterstützung unterscheidet sich dabei je nach Vorfall- und Zielgruppe.
Ziel des CSN ist es, den betroffenen Personen und Institutionen entsprechend der gemeldeten IT-Sicherheitsvorfälle angemessene Unterstützungsangebote und Hilfsangebote zur Verfügung zu stellen. Zielgruppe dabei sind vor allem kleinere und mittlere Unternehmen (KMU), sowie Verbraucherinnen und Verbraucher.

Das Cyber-Sicherheitsnetzwerk ist ein immer größer werdender Zusammenschluss qualifizierter und regierter Helferinnen und Helfern. Sie alle stellen ihre vielfältigen Expertisen und ihr individuelles Know-how bei Behebung von IT-Sicherheitsvorfällen zur Verfügung, um IT-Sicherheitsvorfälle zu bearbeiten.

Die Digitale Rettungskette ist eine Kernkomponente des CSN. Sie legt ein abgestimmtes Arbeiten der Helferinnen und Helfer im CSN fest und gibt so das strukturiertes und nachvollziehbares Vorgehen vor. Mit diesem wird eine Kette unterschiedlicher reaktiver Hilfsangebote, beginnend bei Identifizierung der geeigneten Helferinnen und Helfer, über Hilfestellungen, bis hin zur umfassenden Lösungsbetreuung und Vorfallklärung ermöglicht.

Eine qualitativ hochwertige Vorfallbearbeitung der qualifizierten Helferinnen und Helfer wird durch ein einheitliches und qualitätsgesichertes Qualifizierungsprogramm sichergestellt.

Das Angebot eines Erfahrungsaustauschs in regionalen Foren oder das jährlich stattfindende Forum des Cyber-Sicherheitsnetzwerks runden die Angebotspalette ab.

1.5.1 Aufbau und Struktur

Das CSN[3] ist als eine flächendeckende dezentrale Struktur aufgebaut, die effizient KMU, aber auch Verbraucherinnen und Verbraucher bei IT-Sicherheitsvorfällen Unterstützung anbietet.

1.5.1.1 Organisatorische Anlaufstelle

Die Geschäftsstelle des CSN ist über die E-Mail-Adresse info@cyber-sicherheitsnetzwerk.de erreichbar, welche ebenfalls zur Registrierung der Teilnehmerinnen und Teilnehmer des Cyber-Sicherheitsnetzwerks dient.

[3] Detaillierte Informationen zum Cyber-Sicherheitsnetzwerk erhalten Sie auf den Webseiten unter: https://www.bsi.bund.de/Cyber-Sicherheitsnetzwerk

Dabei agiert das BSI nicht als Auftraggeber. Die Geschäftsstelle des CSN unterstützt zu allgemeinen Fragen zum Cyber-Sicherheitsnetzwerk und bei der Registrierung der Teilnehmenden.

1.5.1.2 Strategische Unterstützung

Die strategische Ausrichtung sowie die Koordinierung für das CSN übernimmt die Koordinierungsstelle des BSI. Diese wird von einem „Round-Table", bestehend aus Vorfall-Experten sowie Vertretern von Behörden, Bildungsinstitutionen und unterschiedlichen Interessengruppen, unterstützt.

1.5.1.3 Von einem Vorfall betroffene Personen und Institutionen

Die Zielgruppe des CSN ist in erster Linie, die von einem IT-Sicherheitsvorfall betroffenen Verbraucherinnen und Verbraucher, Kleinstunternehmen (KKU) sowie kleinere und mittlere Unternehmen (KMU). Gerade die genannten Zielgruppen haben oft Schwierigkeiten bei einem IT-Sicherheitsvorfall. Denn oft sind diese Zielgruppen bei einem IT-Sicherheitsvorfall technisch und ressourcenbedingt überfordert, können keine realistische Einschätzung über das Angriffsszenario sowie über das Ausmaß der Auswirkungen treffen. Auf Grundlage dieser Prämissen benötigen die Zielgruppen eine besondere Unterstützung sowie eine notwendige Soforthilfe beim Eintritt eines IT-Sicherheitsvorfalls durch eine vertrauensvolle Stelle, die sich als zuverlässige Anlaufstelle für IT-Sicherheitsvorfälle bewährt.

Das CSN möchten für diese betroffenen Personen und Institutionen deutschlandweit eine zentrale Anlaufstelle nach einem IT-Sicherheitsvorfall sein und sich zukünftig auch als solche positionieren.

Kritische Infrastrukturen und größere Unternehmen liegen nicht im Fokus des CSN, da diese über individuelle Prozesse und eigenes Know-how für die Vorfallbehandlung verfügen.

1.5.1.4 Registrierte Teilnehmer

Für jedes Unternehmen (nicht für Privatpersonen) besteht zusätzlich die Möglichkeit, sich als registrierter Teilnehmer (durch ein Antragsverfahren) in das CSN aufnehmen zu lassen. Registrierte Teilnehmer erwerben zusätzliche Möglichkeiten, beispielsweise erhalten registrierte Institutionen vom CSN ein „Welcome-Paket" und regelmäßige Lageinformationen. Darüber hinaus erhalten registrierte Institutionen Zugang zu regionalen Foren und werden zu Veranstaltungen des CSN eingeladen. Weiterhin besteht die Möglichkeit aktiv den Prozess mitzugestalten und im direkten Austausch mit Expertinnen und Experten sowie dem BSI in Kontakt zu treten.

1.5.1.5 Aktive Helferinnen und Helfer sowie Expertinnen und Experten des CSN

Die erste persönliche Anlaufstelle des CSN in der Digitalen Rettungskette ist die Kontaktstelle. Diese besteht aus einem Web-Angebot „Hilfe zur Selbsthilfe" und einer zentralen Hotline, die den betroffenen Personen und Institutionen bei Kontaktaufnahme auf die Kontaktlisten der Helferinnen und Helfer verweist.

Mithilfe der auf den Webseiten des BSI bereitgestellten Listen mit qualifizierten Helferinnen und Helfern ist es für betroffene Personen und Institutionen schnell möglich, einen geeigneten regionalen Ansprechpartner herauszufinden, der bei der Vorfallbearbeitung effektiv und gezielt unterstützt.

Ebenfalls werden entsprechende Listen mit qualifizierten Helferinnen und Helfern in den Regionen den Zielgruppen auf der Webseite des CSN zur Verfügung gestellt.

1.5.2 Die Digitale Rettungskette

Um allen betroffenen Personen und Institutionen angemessene Unterstützungsleistungen anbieten zu können, sieht das CSN die sogenannte „Digitale Rettungskette" vor. Die Digitale Rettungskette besteht aus mehreren Eskalationsstufen und verfolgt das Ziel, nach einem IT-Sicherheitsvorfall den betroffenen Personen und Institutionen eine schnelle qualifizierte Erstversorgung und Hilfsangebote anzubieten.

An erster Stelle der Digitalen Rettungskette steht die „Hilfe zur Selbsthilfe“. Wichtige „**Erste-Hilfe-Maßnahmen**[4] zur Selbsthilfe“ finden die betroffenen Personen und Institutionen auf der Webseite des CSN. Diese enthalten in folgende Maßnahmenpakete die wichtigsten Erste-Hilfe-Maßnahmen:

- TOP 12 Maßnahmen bei Cyber-Angriffen
- Maßnahmenkatalog zum Notfallmanagement - Fokus IT-Notfälle –
- Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1

Die Checklisten Checkliste Organisatorisches bzw. Checkliste Technik führen nach dem Prinzip Hilfe zur Selbsthilfe online kurz und knapp durch die ersten Schritte zur Bewältigung eines IT-Sicherheitsvorfalles. Die Service Center-Hotline) ist die erste persönliche Anlaufstelle der Digitalen Rettungskette des CSN. Unter der kostenfreien Telefonnummer 0800-274 1000 ist das Service Center zwischen 8:00 Uhr und 18:00 Uhr erreichbar. Mitarbeiterinnen und Mitarbeiter der Kontaktstelle unterstützen betroffene Personen und Institutionen bei der richtigen Einschätzung eines IT-Sicherheitsvorfalls und helfen Ihnen bei der Auswahl des richtigen Glieds der Digitalen Rettungskette (Eskalationsstufe).

In den ersten Eskalationsstufen unterstützen die „Digitalen Ersthelfer“ betroffene Personen und Institutionen, vor allem Verbraucherinnen und Verbraucher und Kleinst-Unternehmen (KKU) bei der Behebung von kleineren IT-Störungen und IT-Sicherheitsvorfällen mit einer ersten Hilfe.

Auf der Webseite finden betroffene Personen und Institutionen eine Übersicht über die **Liste registrierter „Digitalen-Ersthelfer“**[5]. Über die Suchfunktion der Liste lässt sich schnell eine Auswahl regionaler „Digitaler Ersthelfer“ finden. Die erste Unterstützung von kleinen und mittleren Unternehmen (KMU) übernehmen die **„Vorfall-Praktiker”.**

Handelt es sich um eine komplexeren IT-Sicherheitsvorfall, so kann auf die nächste Eskalationsstufe verwiesen werden. Hierfür stehen **zertifizierte Vorfall-Experten** oder IT- Sicherheitsdienstleister zur Verfügung, die auch auf einer **Liste**[6] **auf der Webseite zu finden sind.** Diese sind in der Lage, den jeweiligen Vorfall tiefer zu analysieren und entsprechende Hilfestellung zu geben – ggf. auch vor Ort bereitstellen.

1.5.2.1 Schnittstellen zu anderen Hotlines und Anlaufstellen

Das Cyber-Sicherheitsnetzwerk bietet bestehenden kostenfreien IT-Sicherheits-Hotlines die Möglichkeit sich an das CSN anzuschließen. So haben Betroffene eine zentrale Anlaufstelle, aber auch die Möglichkeit sich aus einem regionalen Angebot eine entsprechende Unterstützungsleistung einzuholen.

1.5.3 Qualifizierung und Erfahrungsaustausch

Das CSN sieht drei Qualifizierungsstufen der Helferinnen und Helfer vor:

1. Den Basiskurs als kostenlose Online-Schulung im Selbststudium für den „Digitalen-Ersthelfer“.
2. Die Zusatzschulung als zweitägige Schulung mit abschließender Prüfung bei einem registrierten Schulungsanbieter zum „Vorfall-Praktiker“.
3. Die Aufbauschulung als dreitägige Schulung bei registrierten Schulungsanbieter zum „Vorfall-Experten“ mit der Möglichkeit einer anschließenden Personenzertifizierung beim BSI.

1.5.3.1 Selbststudium

Digitale Ersthelfer qualifizieren sich durch das Selbststudium des „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“. Zur Unterstützung bietet das CSN einen kostenfreien Basiskurs als Online

[4] Erste-Hilfe-Maßnahmen: https://www.bsi.bund.de/DE/IT-Iicherheitsvorfall/Unternehmen/unternehmen.html

[5] Liste der Digitalen Ersthelfer: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Digitaler_Ersthelfer/Digitaler_Ersthelfer_node.html

[6] Liste der Vorfall-Experten: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Personen/Vorfall-Experte/Liste-Vorfall-Experte/liste-Vorfall-Experte_node.html

Schulung an. Dieser gliedert sich in drei Module. Diese Module basieren auf dem „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“. Am Ende jedes Moduls steht ein Kompetenztest zur Verfügung. Nach der Teilnahme und dem erfolgreichen Abschluss aller drei Module des Basiskurses ist eine Registrierung als „Digitaler Ersthelfer“ und eine Aufnahme auf die Liste der Digitalen Ersthelfer möglich.

1.5.3.2 Schulungen durch Trainerinnen und Trainer sowie Schulungsanbieter

Die Qualifikation der Vorfall-Praktiker und Vorfall-Experten erfolgt durch Schulungsanbieter. Diese Schulungsanbieter können IT/Informationssicherheits-Schulungsanbieter, Verbände oder Universitäten sein, die die Digitalen Ersthelfer, Vorfall-Praktiker, Mitglieder, Studierenden aber auch Mitarbeitende von Unternehmen qualifizieren.
Aufgabe des Schulungsanbieters ist es, auf der Grundlage eines Curriculums[7] , eigenständig Schulungen beziehungsweise Prüfungen zu konzipieren und anzubieten. Die Organisation, die Abwicklung und die Durchführung der Schulungen obliegt ausschließlich den Schulungsanbietern.

1.5.3.3 Austausch in Regionale Foren sowie Forenleiterinnen und Forenleiter

Mit den regionalen Foren bieten Forenleiter des CSN sowohl Unternehmen als auch Helferinnen und Helfern die Möglichkeit, in einer gesicherten Umgebung die Bewältigung eines Vorfalls zu trainieren.

Mit dem Trainingskoffer stellt das CSN eine kostenfreie Übungs- bzw. Spielesammlung zur Verfügung.

Der Trainingskoffer ist ein einfaches spielerisches Training für die Vorfallbearbeitung „out of the box“. Dieser ist so gestaltet, dass die Trainingseinheiten leicht selbst erstellt und schnell eingesetzt werden können.

Regionale Foren sind ca. zweistündige Erfahrungsaustauschformate, welche als Frühstücksrunde, Business-Lunch oder als Stammtisch am Abend stattfinden können und werden in der Regel von erfahrenen Vorfall-Praktiker oder Vorfall-Experten organisiert und geleitet. Die regionalen Foren können regelmäßig sowohl physisch als auch virtuell an einem bestimmten Ort stattfinden. Mit diesem Format können sich insbesondere teilnehmende Unternehmen sowie “Digitale Ersthelfer” ihre Kompetenz bei der Vorfallbearbeitung im CSN ausbauen und so ihre Kompetenz erweitern.

1.5.3.4 Erfahrungsaustausch

Das CSN bietet neben einer Austauschplattform, auch regelmäßige Formate für einen Erfahrungsaustausch für die einzelnen Zielgruppen.

1.5.4 Helferinnen und Helfer des Cyber-Sicherheitsnetzwerks

Aufgabe der Helferinnen und Helfer des Cyber-Sicherheitsnetzwerkes ist es betroffene Personen oder Institutionen nach einem IT-Sicherheitsvorfall im Rahmen der Digitalen Rettungskette Unterstützung bei der Vorfallbearbeitung anzubieten. Das BSI stellt für die Vorfall-Behandlung keine Expertise zur Verfügung.

1.5.4.1 Der kompetente „Digitale Ersthelfer“

“Digitale Ersthelfer” können alle interessierten und IT-affinen Personen werden.

Die Grundvoraussetzung ist die Absolvierung eines **Basiskurses**[8] , basierend auf dem **„Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer“**[9] , welcher direkt durch das Cyber-Sicherheitsnetzwerk angeboten wird.

---

7 Curriculum für die Qualifikation zum Vorfall-Bearbeiter: tbd
und Curriculum für die Qualifikation zum Vorfall-Experten: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210122_Curriculum_Qualifikation_Vorfall_Experten.pdf

8 Basiskurs für Digitale Ersthelfer:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html

9 Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale-Ersthelfer: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210712_Leitfaden_Digitaler_Ersthelfer.pdf

Nach der Teilnahme und dem erfolgreichen Abschluss aller Module des Basiskurses können sich die Absolventinnen und Absolventen beim Cyber-Sicherheitsnetzwerk als „Digitale Ersthelfer“ registrieren. Nach erfolgter Registrierung werden die “Digitalen Ersthelfer” auf den Webseiten und in der Liste der Digitalen Ersthelfer des Cyber-Sicherheitsnetzwerkes veröffentlicht.

Für die **First-Level-Unterstützung** in der Digitalen Rettungskette sind im CSN die Digitalen Ersthelfer registriert. Diese unterstützen vorwiegend Verbraucherinnen und Verbrauchern sowie Kleinstunternehmen mit schneller, telefonischer Ersthilfe. Betroffene Personen und Institutionen können die Ersthilfe, zu den angegebenen Servicezeiten der Anlaufstelle, per Telefon oder E-Mail anfragen. Die Aufgabe des Digitalen-Ersthelfers ist es, eine qualifizierte Einschätzung des IT-Sicherheitsvorfalls zu geben. Die betroffene Person oder Institution soll dadurch eine erste Hilfe bei kleineren IT-Störungen und IT-Vorfällen sowie erste Handlungsempfehlungen erhalten. Den Rahmen für die Mitarbeit als “Digitalen Ersthelfers (DEH)” gibt der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale-Ersthelfer“ vor. Dieser Leitfaden unterstützt die Digitalen Ersthelfer auch bei der Analyse von IT-Sicherheitsvorfällen und gibt ihnen dafür Handlungsempfehlungen.

1.5.4.2 Der geschulte Vorfall-Praktiker

Vorfall-Praktiker sind z.B. Unternehmen wie IT-Sicherheitsdienstleister, Computerfirmen oder auch IT-System-Administratoren von Unternehmen.

Für die Qualifikation zum Vorfall-Praktiker wird eine zweitägige **Zusatzschulung** angeboten**,** die mit einem halbtägigen Prüfungsworkshop abschließt.

Der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Praktiker und Vorfall Experten“ gibt den Rahmen für die Qualifikation. Für die Mitarbeit als Vorfall-Praktiker im CSN ist eine Registrierung erforderlich. Für die Registrierung beim CSN ist neben der

- Vorlage der erfolgreichen Prüfung zum “Vorfall-Praktiker”,
- eine einjährige Tätigkeit als DEH (oder einer vergleichbaren Tätigkeit) sowie
- ein Nachweis einer IT-Sicherheitstechnischen Qualifikation z.B. als System-Administratorin, -Administrator oder gleichwertiger Kompetenz

vorzulegen.

Die Vorfall-Praktiker sind die **First-Level-Unterstützung** von den KMU hinsichtlich der Digitalen Rettungskette. Diese bieten KMU schnelle telefonische Ersthilfe an und stehen ihnen innerhalb ihrer beim CSN angegebenen Servicezeiten telefonisch oder per E-Mail zur Verfügung. Sie geben diesen eine qualifizierte Einschätzung, führen eine Analyse durch und geben Handlungsempfehlungen.

Ist der Vorfall weder mit angemessenem Aufwand noch in einem ersten Gespräch zu beheben, empfiehlt der Vorfall-Praktiker den Vorfall durch einen Vorfall-Experten analysieren zu lassen.

Die gewonnenen Erkenntnisse und empfohlenen Maßnahmen, die zur Behebung des IT-Sicherheitsvorfalls durchgeführt wurden, werden fortlaufend in einem Vorfallbericht dokumentiert. Dieser Vorfallbericht kann der betroffenen Person oder Institution nach Beendigung der Vorfallbehandlung und des Unterstützungsangebotes zugesandt.

1.5.4.3 Der zertifizierte Vorfall-Experte

Vorfall-Experten sind in der Regel IT-Fachleute, die sich zusätzlich im Rahmen einer Aufbauschulung für das CSN als Vorfall-Experten qualifizieren. Dazu müssen sie eine dreitägige, kostenpflichtige Aufbauschulung bei einem beim CSN registrierten IT- Schulungsanbieter[10] absolvieren.

Diese Aufbauschulung basiert auf dem „Leitfaden zur Reaktion auf IT- Sicherheitsvorfälle für Vorfall-Experten“ [11]. Nach der Schulung schließt sich eine Personenzertifizierung durch die Zertifizierungsstelle des BSI an, die neben der Prüfung der Nachweise auch eine Kompetenzprüfung in Form eines Tests umfasst.

[10] Seminarangebote der Schulungsanbieter: https://www.bsi.bund.de/CSN_Schulungsanbieter

[11] Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Vorfall-Experten: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CSN/210712_Leitfaden_Vorfall_Experte.pdf

Erst nach der erfolgreichen Zertifizierung ist es möglich, sich als Vorfall-Experte im Cyber-Sicherheitsnetzwerk registrieren zu lassen.

Zu den Aufgaben eines Vorfall-Experten gehört es, nach der bereits durch den Digitalen Ersthelfer oder Vorfall-Praktiker erstellten ersten Analyse, eine tiefergehende Analyse oder eine Vor-Ort-Unterstützung anzubieten. Grundlage für die Tätigkeit ist, wie auch in den anderen Stufen, ein individueller Dienstleistungsvertrag, der zwischen der betroffenen Person oder Institution und dem Vorfall-Experten zu Beginn der Vorfallbehandlung geschlossen wird.

Der IT-Sicherheitsvorfall kann an einen IT-Sicherheitsdienstleister abgegeben werden, wenn zur Analyse und Behebung oder, zusätzlich zu einer forensischen Untersuchung, ein Team unterschiedlicher Spezialistinnen und Spezialisten erforderlich ist, dass über einen gewissen Zeitraum vor Ort den betroffenen Personen und Institutionen Unterstützungsleistungen anbietet.

1.5.4.4 Der zertifizierte IT-Sicherheitsdienstleiter: Vorfallbearbeitung

Beschäftigt ein IT-Sicherheitsdienstleister mindesten drei beim BSI registrierte Vorfall-Experten, so kann er sich als IT-Sicherheitsdienstleiter für den Bereich Vorfallbearbeitung beim BSI zertifizieren lassen. Für diese Zertifizierung muss der Dienstleister neben den Kompetenznachweisen seines Personals durch die Personenzertifizierungen, auch noch weitere Nachweise über die Berufs- und Projekterfahrung erbringen.

Die Verfahrensbeschreibung „IT-Sicherheitsdienstleister-Zertifizierung: Programm Vorfallbearbeitung durch Vorfall-Experten“ stellt unter anderem die Anforderungen an IT-Sicherheitsdienstleister als Vorfall-Experten bereit.[12]

1.5.4.5 Einbindung von Fachpersonal

Um eine angemessene Reaktion auf einen IT-Sicherheitsvorfall zu gewährleisten, ist es unter Betrachtung der Art und der Schwere der Problematik möglicherweise erforderlich sowie auch empfehlenswert weiteres Fachpersonal in die Behandlung zu integrieren.

Hinter dem Begriff Fachpersonal verstecken sich hierbei insbesondere die nachfolgenden Stellen:

- **Juristin und Jurist (IT-Anwälte)**
  Klärung von sämtlichen Fragen hinsichtlich einer möglichen Strafanzeige, der Haftung sowie sonstiger rechtlicher Aspekte sowie bei der Beweissicherung (IT-Forensik), wenn eine zivil- oder strafrechtliche Verwertbarkeit sichergestellt sein muss.
- **Kommunikationsspezialistin und -spezialist**
  Verantwortung sowohl für die interne (gegenüber Mitarbeiterinnen und Mitarbeitern) als auch die externe (Öffentlichkeit/Presse und Stakeholder) Kommunikation bei einem IT-Sicherheitsvorfall.
- Datenschutzbeauftragte und **Datenschutzbeauftragter**
  Klarstellung von datenschutzrechtlichen Fragestellungen insbesondere in Bezug auf die Beweissicherung.
- **Betriebsrat/Personalrat**
  Abstimmung bezüglich möglicher personalrelevanter Daten und den Zugriff auf verschiedenen Informationen.

Die Einbindung der aufgelisteten Stellen ist abhängig von der jeweiligen Unternehmensgröße. Dabei ist es denkbar, dass vereinzelte Stellen nicht existieren oder auch an externe Personen vergeben sind.

1.5.4.6 Zielsetzung einer betroffenen Person oder Institution

Wendet sich eine betroffene Person oder Institution, aufgrund eines IT-Sicherheitsvorfalls durch einen Cyber-Angriff, an einen Helfer, so ist bei der Beauftragung ein besonderes Augenmerk auf die Zielvorstellung zu

[12] Verfahrensbeschreibung für IT-Sicherheitsdienstleister für den Bereich Vorfallbehandlung: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Vorfall-Experte-Sicherheitsdienstleister.pdf

legen. Diese kann je nach Situation unterschiedlich ausfallen. Grundsätzlich wird jedoch eine betroffene Person oder Institution in jedem Fall dazu bestrebt sein, dass der Vorfall möglichst schnell und kostengünstig behoben wird. Hinter dieser Idealvorstellung bei der Zielsetzung kann sich jedoch situationsabhängig ein Widerspruch verbergen. Infolgedessen werden hierbei die beiden Perspektiven in Form der „Schnellen Behebung“ sowie der „Vollständigen Aufklärung“ unterschieden und entsprechend dargestellt, um mögliche Konflikte bei den Zielvorstellungen eines Betroffenen aufzuzeigen.

Schnelle Behebung

Im Kontext einer schnellen Behebung eines IT-Sicherheitsvorfalls steht die Herstellung der Arbeitsfähigkeit der betroffenen Systeme im Vordergrund. Die Ursache bzw. der Grund wie es zu dem Vorfall kommen konnte ist hierbei weitestgehend unerheblich. Ebenso wird die Sicherung von Beweisen nicht gefordert. Demzufolge soll die Problemstellung schnellstmöglich beseitigt werden, um die Arbeitsfähigkeit im Wesentlichen wiederherzustellen und das mit vertretbarem Aufwand sowie geringen Kosten für die betroffenen Personen und Institutionen.

Die Gefahr bei dieser Vorgehensweise besteht darin, dass aufgrund einer fehlenden bzw. einer stark beschränkten Schadensanalyse die Infektionskette nicht genau genug untersucht wird und somit nicht in jedem Fall eine vollständige Bereinigung erzielt werden kann. Es ist denkbar, dass Hintertüren nicht entdeckt werden, wodurch das erneute Auftreten eines Vorfalls der gleichen Art nicht auszuschließen ist. Außerdem kann den verschiedenen Stakeholdern keine Antwort geliefert werden, was mit ihren Daten passiert ist, bzw. sein könnte oder ob die Angreifer Zugriff auf Kunden oder Lieferantensysteme hatten.

Vollständige Aufklärung

Der Rahmen einer vollständigen Aufklärung bezieht sich auf den ganzheitlichen Ansatz der gefahrlosen Wiederverwendung der entsprechenden Systeme, sobald der IT-Sicherheitsvorfall vollumfänglich aufgearbeitet und beseitigt wurde. Allerdings bei "größeren" Cyber-Angriffen (z.B. Ransomware) haben die Angreifer oftmals Administrationsrechte der gesamten IT-Infrastruktur. Außerdem lassen sich nicht alle Systeme vollständig analysieren (Ressourcengründe) und somit bleibt ein Restrisiko, dass doch irgendwo eine Backdoor ist.

Diesbezüglich ist eine möglichst genaue Analyse durchzuführen, um zum einen das Schadensausmaß bzw. die Dimension des Angriffs, und zum anderen die Ursache einschließlich des Angriffswegs zu ermitteln. Dahingehend ist es notwendig beispielsweise eine Beweissicherung durch die Erstellung eines System-Abbildes durchzuführen sowie Protokolldateien, bspw. den Netzwerkverkehr zu erfassen. Anhand der gesammelten Daten kann eine detaillierte Analyse durchgeführt werden. Infolgedessen kommt dem Gebiet der IT-Forensik eine besondere Bedeutung zu. Als Teilgebiet der Forensik beschäftigt sich die IT-Forensik mit verschiedenen Analyse-, Ermittlungs- und Beweissicherungstechniken, um Vorfälle auf IT-Systemen beleuchten und aufklären zu können. In Anbetracht der jeweiligen Anforderungen an die methodische Vorgehensweise sollte eine Gerichtsverwertbarkeit gewährleistet werden.

Der Umfang der notwendigen Analyse hängt dabei stark von der Systemlandschaft sowie dem vorliegenden IT-Sicherheitsvorfall ab. Eine gründliche Untersuchung kann dabei fallbezogen einige Zeit und Kosten in Anspruch nehmen.

Erst nachdem die Problemstellung komplett erfasst und verstanden wurde, kann der IT-Sicherheitsvorfall behandelt werden. Dies bedarf einiges an Erfahrung und Ressourcen, die häufig nur bei IT-Sicherheitsdienstleistern mit einem Team von Vorfall-Experten vorliegt.

Konnte der IT-Sicherheitsvorfall schließlich erfolgreich bereinigt werden, gilt es diesen im Nachgang aufzubereiten, indem eine entsprechende Auswertung durchgeführt wird. Dadurch können oftmals Verbesserungspotentiale ermittelt werden, um die Sicherheit zu optimieren.

2 Verhalten am Telefon und nichttechnische Maßnahmen (VP)

2.1 Intention und Lernziele

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

Professionalität gegenüber den betroffenen Personen und Institutionen auszustrahlen.

Sicher und kompetent am Telefon aufzutreten.

2.2 Serviceorientiertes Telefongespräch

Neben dem entsprechenden Fachwissen in der Informationstechnik ist es von essenzieller Bedeutung ein angemessenes Auftreten am Telefon zu wahren.

In den nachfolgenden Abschnitten wird dargelegt, wie ein formelles Telefonat geführt wird und welche Punkte bei einem serviceorientierten Telefongespräch zu berücksichtigen sind. Ausschlaggebend für eine akkurate Verhaltensweise am Telefon ist die gezielte und richtige Aufnahme der Problemstellung. Diesbezüglich wird dargestellt, wie Anrufer entsprechend in Empfang zu nehmen sind und welche grundlegenden Fragen im Zuge der Aufnahme zu klären sind.

2.2.1 Professionelles Verhalten am Telefon

Mit einem professionellen Verhalten am Telefon erhöhen Sie die Chancen das Gespräch erfolgreich zu gestalten. Zudem hinterlassen Sie beim Anrufer einen guten Eindruck. Die folgenden Tipps helfen Ihnen sowohl professionell als auch freundlich am Telefon aufzutreten:

- **Freundliche und positive Begrüßung!**
  - Melden Sie sich stets mit Ihrem Vor- und Nachnamen, damit der Anrufer sofort weiß, wer seine Ansprechperson ist. Stellen Sie sich nicht mit möglichen Titeln wie Prof. oder Dr. vor. Um den Anrufenden freundlich zu animieren die Problematik darzustellen, können Floskeln wie „Was kann ich für Sie tun?“ verwendet werden.

- **Haben Sie Geduld!**
  - Einige Kunden bestehen auf eine sofortige Lösung des Problems, die aber nicht möglich ist. Dann heißt es Geduld zu beweisen und dem Anrufer gegenüber freundlich zu bleiben.

- **Passen Sie sich an!**
  - Nicht jeder Kunde ist gleich. Während einer hauptsächlich einen Ansprechpartner benötigt, wünschen andere Kunden sachliche Lösungsvorschläge. Für jeden Anrufer-Typ sollte mit Fingerspitzengefühl die Gesprächsführung angepasst werden.

- **Stimme macht Stimmung!**
  - Sprechen Sie in Ihrer natürlichen Stimmlage. Alles andere wirkt gekünstelt. Hitzige Situationen am Telefon kann man entschärfen, indem man ruhig und entspannt spricht. Setzt man zudem ein Lächeln auf, klingt die Stimme gleich viel freundlicher.

- **Anrufer beim Namen nennen!**

  - Notieren Sie sich den Namen des Anrufers. Sprechen Sie die Person im Laufe des Gesprächs ein bis, zweimal mit Namen an. So zeigen Sie Interesse. Wiederholen Sie den Namen nicht zu oft – das wiederum wirkt aufgesetzt.

- **Notizen machen!**
  - Machen Sie sich möglichst viele Notizen. Hierzu kann man eine einfache Textdatei, eine Word Datei oder einen Notizblock benutzen.

- **Lassen Sie den Anrufer stets ausreden!**
  - Lassen Sie den Anrufer stets ausreden und unterbrechen Sie ihn nicht, das ist unhöflich. Vermitteln Sie mit Zwischenkommentaren wie „aha okay“, oder „verstehe“, dass Sie den Ausführungen des Anrufers folgen.

- **Vermeiden Sie Umgebungsgeräusche!**
  - Stellen Sie Nebentätigkeiten für die Dauer des Telefonats ein. Sollten Sie Informationen aus Ihren Unterlagen oder dem Internet benötigen, weisen Sie den Anrufer darauf hin. „Einen Moment bitte, ich schaue kurz in meine Unterlagen“. Vollkommen unangebracht sind Tätigkeiten wie Essen, Trinken, Rauchen, Papierrascheln oder lautes Brüllen in den Hörer.

2.2.2 Verhaltensregeln IT-Sicherheitsvorfall

Auf Basis der vorgenommenen Eingrenzung der Problematik können nun Handlungsempfehlungen ausgesprochen werden.

Die Voraussetzung für die gezielte Aussprache von Handlungsempfehlungen ist eine klare Identifikation des Problems. Ein Digitaler Ersthelfer muss also eindeutig wissen, um welche IT-Störung oder welchen IT-Sicherheitsvorfall es sich tatsächlich handelt. Demzufolge ist eine sorgfältige Aufnahme und Eingrenzung die wesentliche Grundlage bei der konkreten Auswahl von Handlungsempfehlungen.

Erlaubt die Eingrenzung der Problematik dem Digitalen Ersthelfer den Sachverhalt eindeutig zu identifizieren, können zielgerichtete Handlungsempfehlungen ausgesprochen werden, die im Idealfall das Problem beheben.

Es besteht aber auch die Möglichkeit, dass der Anrufende den vermeintlichen IT-Sicherheitsvorfall mit den ausgesprochenen Handlungsempfehlungen nicht abschließend beheben kann. In diesem Falle verweist der Digitaler Ersthelfer den Anrufenden an einen Vorfall-Praktiker und spricht daher lediglich generelle Verhaltensregeln aus, z.B.:

- Ruhe bewahren und nicht in Panik geraten.
- Arbeiten mit bzw. an dem IT-System sofort einstellen.
- Betroffenes IT-System vom Netzwerk isolieren.
- Bisher durchgeführte Schritte und Unregelmäßigkeiten dokumentieren, sowie Beobachtungen ggf. in Form von Screenshots festhalten.
- Keine weiteren Maßnahmen zur Problemlösung eigenständig umsetzen.
- Bei einer nicht behebbaren IT-Störung sofort den entsprechenden IT-Support kontaktieren.
- Bei einem nicht behebbaren IT-Sicherheitsvorfall, sofort einen Vorfall-Praktiker kontaktieren.
- Weitere Maßnahmen erst nach Rücksprache mit dem entsprechenden IT-Support oder einem Vorfall-Praktiker einleiten bzw. umsetzen.

2.3 Nicht technische Maßnahmen

Digitale Ersthelfer sind technisch versierte Fachleute, aber didaktisch/sozial nicht für den Kontakt mit Verbraucherinnen und Verbrauchern geschult. Verbraucherinnen und Verbraucher, die sich an Digitale Ersthelfer wenden, sind in einer Notlage und müssen das Gefühl haben ernst genommen und nicht verurteilt zu werden. Auch muss es ihnen im Sinne von Usable Security[13] leicht gemacht werden, ihre Probleme mit Hilfe des digitalen Ersthelfers zu verstehen, zu lösen und für die Zukunft eine Lösungskompetenz zu entwickeln.

Prinzipien eines guten Beratungsgesprächs
Ein erfolgreiches Beratungsgespräch am Telefon benötigt sowohl fachliche als auch soziale Kompetenzen. Folgende Prinzipien der Gesprächsführung sollen dabei helfen, eine gute Gesprächsatmosphäre für die Anrufenden und Helfenden zu schaffen. Gleichzeitig kann der Informationsfluss, um effektiver zu helfen, erleichtert werden:

Verständliche Sprache
"Beratung ohne Termin" versteht man besser als "die Möglichkeit zur unterminierten Konsultation"
Vor allem in der Kommunikation mit Verbraucherinnen und Verbrauchern ist es wichtig eine Sprache zu verwenden, die dem Wissensstand des Gegenübers entspricht. Hören Sie aktiv zu, um ein Gefühl dafür zu bekommen, wie der Wissensstand Ihres Gegenübers ist und gehen Sie auf die Person ein. Nutzen Sie nach Möglichkeit wenige Fachbegriffe und fragen Sie im Zweifelsfall nach, ob Ihre Ausführungen für das Gegenüber verständlich sind.

Erklären
"Ich habe das Problem behoben." gibt dem Anrufer weniger Informationen als *"Das System verhält sich so, weil ... und die Lösung xyz wähle ich weil..."*
Verbraucherinnen und Verbraucher, die verstehen warum ein gewisses Problem entstanden ist, können die zum Problem führende Handlung in Zukunft vermeiden. Neben der Ursachenforschung ist die Aufklärungsarbeit zur Prävention möglicher Vorfall-Ereignisse entscheidend, um zukünftig den betroffenen Personen und Institutionen mögliche Ansätze für Lösungsstrategien und Maßnahmenentwicklung anzueignen. Die Übermittlung eines allgemeinen Verständnisses für IT-Sicherheit und IT-Risiken führt dazu, mögliche Berührungsängste mit Problemen und Fehlern zu beseitigen. Eine Black Box macht Angst. Präventionsunterlagen, beispielsweise Informationen und Erklärungen, sollten so formuliert sein, dass sie einfach nachvollziehbar sind ohne dass man sich mit der Technik in der Tiefe beschäftigen muss. Einfache Erklärungen wie z.B. beim Arztgespräch "Wenn Hormon A sinkt, entsteht ein Überschuss von Hormon B" sind hilfreich.

Nachfragen
"Wie war die Situation beim Auftreten des Problems?" - solche Fragen helfen dabei, um den Kontext des Problems besser zu verstehen.
Nachfragen können sehr hilfreich sein, weil die Verbraucherinnen und Verbraucher sich damit ernst genommen fühlen und auf die persönliche Situation Rücksicht genommen wird. Nachfragen sollten aber vorsichtig formuliert werden. Fast jede Verbraucherin und jeder Verbraucher reagiert empfindlich auf die Nachfrage, ob der Stecker gesteckt ist, auch wenn dies ein häufig auftauchender Fehler ist. Wenn die Verbraucherin und der Verbraucher eine Situation schildern, kann man die Schilderung mit eigenen Worten zusammenfassen und nachfragen, ob man die Schilderung so richtig verstanden hat.

Fragetechniken
"Wie was sehen Sie auf dem Bildschirm?" erleichtert technisch unbeholfenen Personen eher die Zusammenarbeit mit dem Ersthelfer als "Sehen sie Ihren Login-Screen?"

[13] Usable Security bezeichnet inter- und transdisziplinäre Methoden, um sicherheitsfördernde Maßnahmen so auszugestalten, dass deren Benutzende bei ihren sicherheits- bzw. datenschutzrelevanten Zielen und Vorhaben bestmöglich unterstützt werden.

Es gibt verschiedene Arten Fragen zu stellen, unter anderem öffnende und schließende Fragen. Durch den Gebrauch offener W-Fragen (Was? Wann? Wer? Wie? etc.) kann die Suche nach Lösungen gefördert werden, weil die gefragte Person ins Erzählen kommt und man sich einen Überblick über die Gesamtsituation verschaffen kann. Geschlossene Fragen wirken hingegen eingrenzend und ermöglichen durch einfache und kurze Antworten, wie Bestätigungen oder Verneinungen, schneller auf ein konkretes Problem zu sprechen zu können. Geschlossene Fragen sollten jedoch gezielt eingesetzt werden, da eine Häufung solcher bei den befragten Personen schnell ein bedrängendes Gefühl auslösen kann.

Fehler

"Jeder macht Fehler und Fehler helfen uns weiter, die Gebrauchstauglichkeit des Systems/Gerätes zu verbessern."

Fehler werden fast immer unabsichtlich gemacht und jeder macht Fehler. Dies kann man Nutzerinnen und Nutzern vermitteln, indem man sich selbst nicht über sie stellt, sondern darstellt, dass man aus Fehlern lernen kann, z.B. durch "ich habe auch schon mal mein Passwort vergessen und zurücksetzen lassen müssen, seitdem...". Wenn viele Nutzerinnen und Nutzer ähnliche Fehler machen, kann dies einen guten Aufschluss über Schwachstellen des Gerätes im Bereich der Gebrauchstauglichkeit (Usability) oder der Transparenz geben. Werden Fehler als Feedback zur Nutzung aufgenommen und weitergegeben, können sie die Fehlertoleranz des Digitalen Systems (wie eine automatische Rechtschreibkontrolle) und die Usability des Systems (z.B. einen Button an eine bestimmte Stelle zu platzieren, da er dort nicht unabsichtlich gedrückt werden kann) erhöhen. Fehler der Nutzerinnen und Nutzern sind also hilfreich und ihre Beachtung erhöht die Robustheit von Systemen.

Empathie

"Wir schauen uns das mal an." drängt den Anrufenden weniger in die Position des Verursachers als "Wo liegt das Problem?".

Ein IT-Sicherheitsvorfall oder eine Störung können dafür sorgen, dass betroffene Personen emotional reagieren zum Beispiel angespannt, frustriert oder aufgeregt sind. Eine empathische Gesprächsatmosphäre kann dazu beitragen, dass die Anspannung etwas nachlässt und man sich dem Problem auf einer sachlichen Ebene besser nähern kann. Neben den bereits erwähnten Fragetechniken kann es helfen eigene Ich- und Wir-Botschaften zu vermitteln, um der betroffenen Person ein gutes Gefühl zu vermitteln, zum Beispiel "Wir schauen uns das Problem an" oder "Ich möchte mit Ihnen überprüfen, ob es sich um eine Störung Ihres Internetanschlusses handelt".

3 Gefährdungen und Angriffsformen (VP)

3.1 Einführung

Die Komplexität zum Schutz der eigenen Ressourcen ist enorm gewachsen. Was heute noch als sicher eingestuft wird, kann durch unterschiedliche Wirkungen schon morgen eine Sicherheitsschwachstelle darstellen und Angriffspunkt eines Cyber-Angriffs sein. Bei einem Cyber-Angriff ist die Angriffsmethode davon abhängig, welches Ziel der Angreifende verfolgt und ob er die Organisation infiltrieren oder schädigen möchte.

Weiter gehen von den Angriffen auch Gefährdungen aus, welche sich kritisch auf die Überlebensfähigkeit der Organisation auswirken. Dabei können die Gefährdungen Einfluss auf die Infrastruktur, Finanzlage und/oder betriebsnotwendige Daten nehmen, wodurch der Angreifende einen wesentlichen Träger einer Organisation schädigt.

3.2 Intention und Lernziele

Dieses Kapitel stellt Begriffserklärungen, Angriffsarten, Angriffsursachen, Angriffsmethoden sowie Phasen eines Cyber-Angriffs dar.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

- Verschiedene Arten sowie Ursachen von Angriffen zu erkennen und zu unterscheiden.
- Verschiedene Angriffsmethoden zu unterscheiden.
- Die verschiedenen Phasen eines Cyber-Angriffs zu erkennen.

3.3 Begriffserklärungen

3.3.1 Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifende können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

3.3.2 Angriffsvektor

Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifender Zugang zu IT- Systemen verschafft.

3.3.3 Bedrohung (englisch "threat")

Eine Bedrohung ist allgemein ein Umstand oder Ereignis, durch den oder durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzenden bzw. Benutzenden der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche

Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

3.3.4 Gefährdung (englisch "applied threat")

Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. Sind beispielsweise Schadprogramme eine Bedrohung oder eine Gefährdung für Anwenderinnen und Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwenderinnen und Anwender prinzipiell durch Schadprogramme im Internet bedroht sind. Der Anwendende, der eine virenverseuchte Datei herunterlädt, wird von dem Schadprogramm gefährdet, wenn sein IT-System anfällig für diesen Typ des Schadprogramms ist. Für Anwenderinnen und Anwender mit einem wirksamen Virenschutz, einer Konfiguration, die das Funktionieren des Schadprogramms verhindert oder einem Betriebssystem, das den Code des Schadprogramms nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

3.3.5 Schwachstelle (englisch "vulnerability")

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Gefährdungen.

3.3.6 Wert (englisch "asset")

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

3.4 Zusammenhang

Für einen Angriff nutzt ein Angreifender in der Regel Schwachstellen in den IT-Systemen, Social Engineering bei den Nutzerinnen und Nutzern, Hacking-Technologien für die Installation von Malware und weitere Angriffstechniken (wie Exploits, JavaScript-Code, Programme zum automatischen Auffinden von Schwachstellen oder Brute-Force-Angriffe), sowie im Weiteren die Schadfunktion in der Malware (Keylogger, Ransomware, Trojanisches Pferd, Spyware, DDoS-Malware ...), um den speziellen Angriff auf dem identifizierten unsicheren IT-System ausführen zu können.

Je mehr potenzielle Schwachstellen vorhanden sind, desto höher ist die Wahrscheinlichkeit eines erfolgreichen Angriffs auf ein IT-System oder eine IT-Infrastruktur. Szenarien, welche durch die folgende Veranschaulichung dargestellt werden:

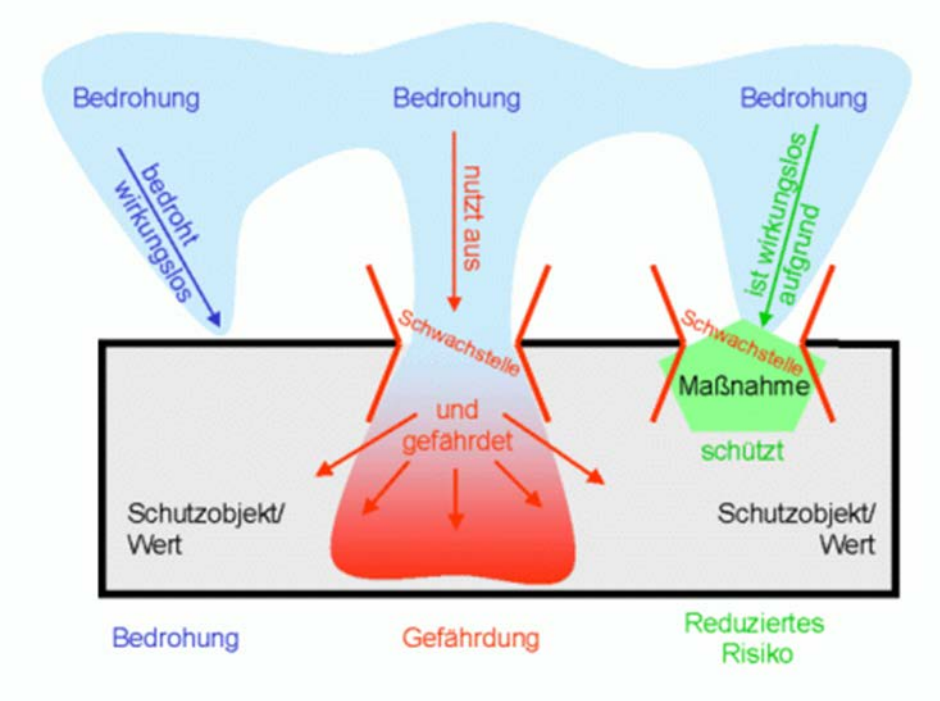


Abbildung 1: Begriff Gefährdung

Quelle: https://www.bsi.bund.de/SharedDocs/Bilder/DE/BSI/Themen/Internet_Sicherheit/Begriff-Gefaehrdung_gif.htmlSchwachstelle.

3.5 Arten von Angriffen bzw. Angriffsformen

Cyber-Angriffe werden häufig anhand des Angriffszwecks kategorisiert, also entsprechend der Wirkung, welche die Angreiferinnen und Angreifer auf den Angriffszielen herbeiführen wollen:

- Angriffe auf die **Vertraulichkeit**: Die Täterinnen und Täter können versuchen, vertrauliche Informationen auszuspionieren, z.B. in dem sie unberechtigte Einsicht in Unternehmensinformationen erhalten.
- Angriffe auf die **Integrität**: Manipulationen, zum Beispiel Manipulation von Informationen und Informationssystemen, Software oder Schnittstellen, spielen bei vielen Cyber-Angriffen eine wichtige Rolle.
- Angriffe auf die **Verfügbarkeit**: Störung des Betriebes von Informationssystemen führt dazu, dass die darauf enthaltenen Informationen nicht mehr verfügbar sind. Die Täterinnen und Täter können versuchen, Informationen oder IT-Dienste zu sabotieren, beispielsweise durch verteilte Denial-of-Service-Angriffe (DDoS-Angriffe).

Hierbei ist zu beachten, dass Cyber-Angriffe häufig mehrere Angriffsschritte umfassen, wobei die einzelnen Schritte unterschiedliche Zwecke haben können. Ein Cyber-Angriff mittels eines Spionage-Schadprogramms umfasst beispielsweise zumindest die Installation des Schadprogramms (Angriff auf die Integrität) und den eigentlichen Abfluss von Informationen (Angriff auf die Vertraulichkeit).

Neben dem Angriffszweck können Cyber-Angriffe auch dahingehend unterschieden werden, ob es sich um gezielte Angriffe (ein Ziel oder wenige ausgesuchte Ziele) oder um großflächige Angriffe (möglichst viele beliebige Ziele gleichzeitig) handelt. Diese beiden Angriffsarten sind mit bestimmten Vor- und Nachteilen für Täterinnen und Täter verbunden: Ein breit gestreuter Angriff verspricht z. B. eine höhere Wahrscheinlichkeit, dass der Angriff zum Erfolg führt. Allerdings fallen derart großflächige Angriffe meist eher auf und provozieren so zeitnahe Gegenmaßnahmen.

Eine umfassende Übersicht der gegenwärtig bekannten Cyber-Angriffsmethoden hat das BSI in der Cyber-Sicherheits-Analyse "Register aktueller Cyber-Gefährdungen und -Angriffsformen" zusammengestellt[14].

3.6 Ursachen von Angriffen

Die Ursache vieler Angriffe ist meist auf eine oder mehrere Schwachstellen zurückzuführen. Um erfolgreiche Cyber-Angriffe durchzuführen, machen sich Täterinnen und Täter vor allem die folgenden Arten von Schwächen zunutze: Software-Schwachstellen, Design-Schwachstellen, Konfigurationsschwachstellen und menschliche Fehlhandlungen. Alle diese Arten von Schwächen lassen sich bei der heutigen Komplexität der Informationsverarbeitung prinzipiell nicht vollständig vermeiden. Folgende Schwachstellen lassen sich unterscheiden:

- **Organisatorische Mängel**
  Eine erhöhte Eintrittswahrscheinlichkeit für einen Cyberangriff geht aus möglichen organisatorischen Mängeln hervor. Diese sind mitunter:
  - Fehlende oder unzureichende Prozesse oder Regelungen zur IT-Sicherheit usw.
  - Ressourcenmangel oder Personalausfall z.B. fehlende Zuständigkeiten oder Vertretungsregelungen
  - Unvollständiges Patch- und Änderungsmanagement
  - Mangelnde Sensibilisierung und Schulung personeller Ressourcen
  - Unzureichender Umgang bei Sicherheitsvorfällen bzw. fehlendes Notfallmanagement
  - Unzureichende Dokumentation, Protokollierung und Nachweisführung,
  - Unzureichendes Privacy Management z. B. in Sozialen Netzwerken
  - Unzureichende Zugriffskontrollen

- **Software-Schwachstellen** (Implementierungs-Schwachstellen): Oft können Schwachstellen auf Programmierfehler zurückgeführt werden. Da der Quellcode größerer Software-Produkte mehrere Millionen Programmierzeilen lang sein kann, sind solche Software-Schwachstellen nicht selten. Auch veraltete Software, die nicht mehr dem Stand der Technik entspricht, ist eine Schwachstelle. Ebenso können Hardware-Schwachstellen für einen Angriff genutzt werden.
- **Design-Schwachstellen**: Anders als Software-Schwachstellen sind Design-Schwachstellen nicht in der konkreten Programmierung einer Software begründet, sondern in der Spezifikation von Funktionsweisen, Schnittstellen, Datenformaten, Übertragungsprotokollen o.ä.
  Auch Fehler bei der Implementierung stellen Schwachstellen dar, die von Angreifenden ausgenutzt werden können.
- **Konfigurationsschwachstellen**: Software-Produkte lassen sich in der Regel mittels Konfigurationseinstellungen an die jeweilige konkrete Einsatzumgebung anpassen. Solche Einstellungen haben häufig auch Einfluss auf die Sicherheit, sodass durch ungeeignete Konfiguration von Software ebenfalls Schwachstellen entstehen können, z. B. wenn Sicherheitsfunktionen deaktiviert oder Zugriffsrechte nicht restriktiv genug konfiguriert werden.
- **Menschliche Fehlhandlungen**: Täterinnen und Täter verwenden vielfältige Angriffsmethoden, um Mitarbeiterinnen und Mitarbeiter zur Mithilfe bei Cyber-Angriffen zu bewegen („Social Engineering") und einen Zugang zu den Ressourcen der Organisation zu erhalten. Zum Beispiel werden bei der

[14] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.html

Phishing-Mail-Methode E-Mails, die mit einem Schadprogramm infiziert sind, an viele unternehmensinterne Mailaccounts gesendet. Die E-Mails sind so konzeptioniert, dass eine möglichst hohe Eintrittswahrscheinlichkeit besteht eine Empfängerin oder einen Empfänger zum Aktivieren des Schadprogramms durch Öffnen eines Links oder einer Datei herzuleiten. Erfolgt die Versendung der Mails nicht massenhaft, sondern gezielt an einzelne mit individualisierten, auf den Empfangenden angepasste Inhalte, spricht man von Spear-Phishing (siehe auch 6.1.3 Arten von Phishing). Eine weitere Methode ist die telefonische Kontaktaufnahme, indem sich der Anrufende z.B. als IT-Service Mitarbeitender ausgibt, um sich so Zugang zu Informationen zu verschaffen. In all diesen Situationen ist den Mitarbeiterinnen und Mitarbeitern gar nicht bewusst, dass sie zu einem Cyber-Sicherheitsvorfall beitragen.

Weitere Schwachstellen, die auf menschliche Fehlhandlungen zurückzuführen sind, sind beispielsweise Anwendungsfehler bei Nutzung der eingesetzten technischen Ressourcen (Endgeräte) oder durch die nicht Einhaltung der Wartungsintervalle sowie regelmäßige Durchführung von Software-Updates.

Hersteller veröffentlichen oft Aktualisierungen (Patches/Updates) für ihre Produkte, wenn technische Schwachstellen darin bekannt werden. Dies ist bei Design-Schwachstellen in der Regel schwieriger als bei Software-Schwachstellen. Meist ist es Aufgabe der Benutzerinnen und Benutzer, die Aktualisierungen auf ihren Systemen einzuspielen, um die jeweiligen Schwachstellen zu beseitigen. Verfahren, bei denen Software-Produkte selbsttätig im Internet nach Aktualisierungen suchen und diese gegebenenfalls einspielen, gewinnen zunehmend an Bedeutung.

Um den Zeitraum bis zur Veröffentlichung eines Patches zu überbrücken, werden häufig auch sogenannte Workarounds veröffentlicht. Hierbei handelt es sich um Hinweise, wie durch Änderungen der Konfiguration, der Anwendungsumgebung, der Nutzungsart o. ä. vermieden werden kann, dass die Schwachstelle ausgenutzt wird. Workarounds können auch darin bestehen, bestimmte Funktionen der Software nicht zu nutzen, bis ein entsprechender Patch zur Verfügung steht.

Insgesamt wird der Erfolg von Cyber-Angriffen vor allem durch folgende Faktoren begünstigt:

- In vielen Fällen nutzen Täterinnen und Täter technische Schwachstellen aus, bevor sie öffentlich bekannt werden („Zero Day"). Programme, die solche neuen Schwachstellen ausnutzen („Exploits"), werden auf Untergrundmarktplätzen gehandelt.
- In dem Zeitraum zwischen dem Bekanntwerden einer Schwachstelle und dem Erscheinen eines entsprechenden Patches sind viele betroffene Systeme ungeschützt. Workarounds sind oft unbequem oder können aus organisatorischen Gründen nur schwer umgesetzt werden.
- Neu veröffentlichte Updates und Patches werden bei vielen Institutionen erst nach Tagen, Wochen oder überhaupt nicht eingespielt. Dies kann zum Beispiel an mangelnden Ressourcen, organisatorischen Problemen oder an Inkompatibilitäten zwischen verschiedenen Komponenten liegen.
- Informationstechnik und die damit verbundenen Sicherheitsaspekte sind heute so komplex, dass viele Benutzerinnen und Benutzern trotz Sensibilisierung und Schulung mit der Einhaltung der Sicherheitsrichtlinien überfordert sind.

3.7 Angriffsmethoden

Täterinnen und Täter wenden bei Cyber-Angriffen eine Vielzahl unterschiedlicher Methoden an. Häufig werden diese nicht einzeln, sondern in Kombination eingesetzt, um das Angriffsziel zu erreichen.

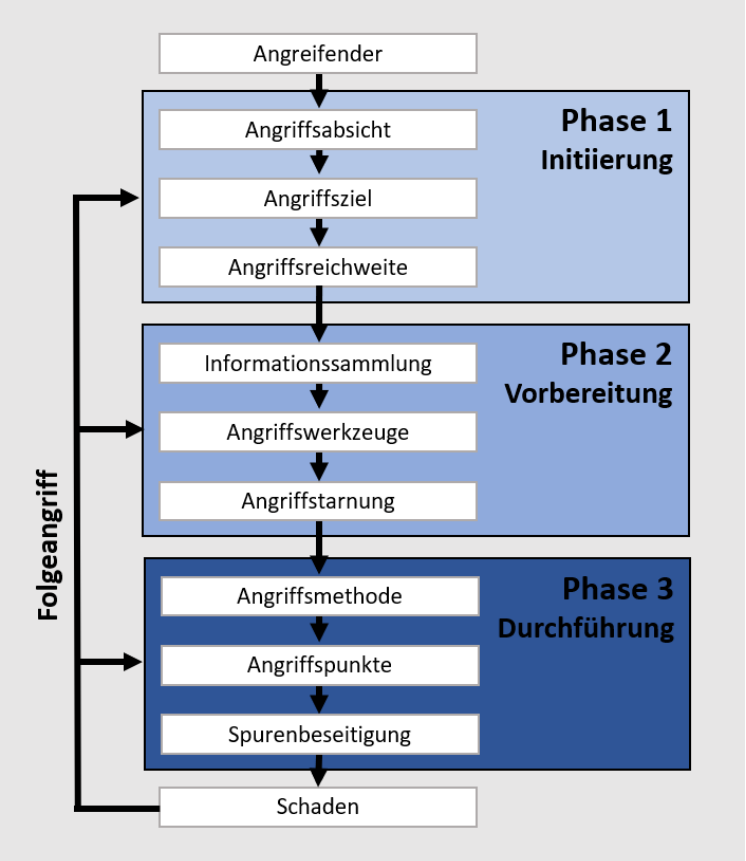
Folgende Bedrohungskategorien (Angriffsvektoren) werden unterschieden:

- Schadprogramme (Malware)
- Hacking und Manipulation
- Missbrauch (z. B. missbräuchliche Nutzung von Berechtigungen bzw. Fernzugriffen)
- Physische Angriffe (z. B. Diebstahl, Verlust oder Zerstörung)
- Technisches Versagen
- Höhere Gewalt (z. B. Ausfall von Infrastrukturen oder von Cloud-Diensten)

- Verhinderung von Diensten (z. B. DDoS durch Botnetze, gezielter Systemabsturz durch Ausnutzung von Schwachstellen)
- Identitätsmissbrauch (z. B. Diebstahl von Zugangsdaten oder Zertifikaten, Verschleierung von Identitäten)

3.8 Phasen eines Cyber-Angriffs

Ein Cyber-Angriff setzt das vorsätzliche, unerlaubte Handeln eines Angreifenden mit bestimmter Absicht voraus. Der Angreifende entscheidet in der Phase 1 zunächst über die Angriffsziele und wählt in diesem Zusammenhang auch die Angriffsreichweite: Ein gezielter Angriff richtet sich gegen wenige Ziele oder sogar nur gegen ein einzelnes System, ein Flächenangriff richtet sich gegen möglichst viele Ziele gleichzeitig.



In der Phase der Angriffsvorbereitung (Phase 2) werden Informationen über das anzugreifende Ziel erhoben. Hier werden auch die Angriffswerkzeuge konstruiert bzw. vorbereitet sowie Maßnahmen zur Angriffstarnung ergriffen.

Es folgt ein Primärangriff in Phase 3, der mithilfe bestimmter Angriffsmethoden an einem oder mehreren Angriffspunkten durchgeführt wird. Anschließend werden Täterinnen oder Täter gegebenenfalls versuchen, die von ihnen erzeugten Spuren zu beseitigen.

Falls das Angriffsziel mit einem Primärangriff nicht erreicht wurde oder dieser nur einen Zwischenschritt zum Erreichen des eigentlichen Angriffsziels darstellt, wird nach dem Primärangriff eventuell ein Folgeangriff durchgeführt.

Abbildung 2: Phasen eines Cyber-Angriffs

Quelle: BSI-CS 026 / Version 2.0 vom 11.07.2028, BSI- Veröffentlichung zur Cyber-Sicherheit / Register aktueller Cyber-Gefährdungen und –Angriffsformen.

3.8.1 Angreifertypen

Trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden kann die Motivation hinter einem Cyber-Angriff häufig auf finanzielle Interessen, Informationsbeschaffung, Sabotage, Einflussnahme oder Durchsetzung politischer Interessen zurückgeführt werden. Die im Cyber-Raum vorsätzlich handelnden Angreiferinnen und Angreifer lassen sich in folgende Gruppen einteilen:

- **Cyber-Aktivistinnen und Cyber-Aktivisten**

  Angreifende, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen, zählen zur Gruppe des sogenannten Hacktivismus. Die Motivation hinter dem

Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte „ethische Hacker“ begründen ihr Handeln mit gesellschaftlichen oder sozialen Themen.

- **Cyber-Kriminelle**

  Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.

  - Organisierte Cyberkriminalität reicht vom Identitätsdiebstahl mit Warenbetrug über den Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Organisierte Cyber-Kriminelle nutzen die genannten Vorteile von Cyber-Angriffen bei ihren Aktivitäten mit hoher Professionalität aus.
  - Im Gegensatz zur organisierten Kriminalität sind einfache Cyber-Kriminelle meist Einzelpersonen oder kleine Gruppen, die sich durch geringere Professionalität in ihrem Handeln auszeichnen. Dementsprechend ist auch die Auswahl der Angriffsziele eingeschränkt und der verursachte Schaden typischerweise geringer.

- **Konkurrenzausspähung/Industriespionage im Cyber-Raum**

  Durch die Vorteile des Internets ergeben sich für die Ausforschung eines Unternehmens durch Wettbewerberinnen und Wettbewerber oder private Akteure neue Möglichkeiten. Konkurrenzausspähung dient finanziellen Interessen. Interne Informationen über Mitbewerberinnen und Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.

- **Staatliche Nachrichtendienste im Cyber-Raum**

  Cyber-Angriffe durch staatliche Nachrichtendienste sowie staatlich gelenkte Wirtschaftsspionage dienen – im Gegensatz zur Konkurrenzausspähung – primär der Informationsbeschaffung und der Einflussnahme, auch um den eigenen nationalen Wirtschaftsunternehmen Vorteile auf den internationalen Märkten zu verschaffen.

- **Staatliche Akteure im Cyber-War**

  Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.

- **Cyber-Terroristinnen und Cyber-Terroristen**

  Terroristinnen und Terroristen können Cyber-Angriffe, wie staatliche Akteure und Kriminelle, nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.

- **Hobbyisten/Skript-Kiddies**

  Die Gruppe der Hobbyisten und Skript-Kiddies führt Cyber-Angriffe aus Neugier durch, um ihre Fähigkeiten und ihr Wissen in der Praxis zu testen. Diese Gruppe verfolgt keine finanziellen Interessen. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.

- **Innentäterinnen und Innentäter**

  Cyber-Angriffe durch Innentäterinnen und Innentäter haben größere Aussicht auf Erfolg als Angriffe von außen, da der Angreifende bereits Zugang zu internen Ressourcen einer Organisation hat und so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren kann. Zusätzliche Vorteile genießen Innentäterinnen und Innentäter durch das ihnen entgegengebrachte Vertrauen einer Organisation. Externe Dienstleister, die durch ihre Tätigkeit Einfluss oder direkten Zugang zur Organisation haben, werden hier ebenfalls zu den Innentäterinnen und Innentäter gezählt.

- **IT-Sicherheitsforscherinnen und IT-Sicherheitsforscher**

  IT-Sicherheitsforscherinnen und IT-Sicherheitsforscher haben ein primär akademisches Interesse an der Aufdeckung von Risiken und der Durchführung von Cyber-Angriffen. Die unkoordinierte Veröffentlichung ihrer Ergebnisse („Full Disclosure”) kann reale Attacken anderer Angreiferinnen und Angreifer zur Folge haben.

3.8.2 Angriffsabsichten und Angriffsziele

Cyber-Angriffe stehen den klassischen Grundwerten der Informationssicherheit entgegen. Typisch sind somit folgende Absichten hinter einem Angriff:

- Angriffe auf die Vertraulichkeit, z. B. das Ausspionieren vertraulicher Informationen. Solche Angriffe werden beispielsweise ermöglicht durch: direktes Abhören (z. B. Kabel, Funk, Netze), einen Direktzugriff, Diebstahl, das Abfangen kompromittierender Abstrahlung, Ausspähen oder Passive Reconnaissance, die Wiederherstellung gelöschter Informationen oder mittels Profiling und Überwachung.
- Angriffe auf die Integrität, z. B. durch die Manipulation von: Informationen, Speichermedien, IT-Diensten, Software, Kommunikationskanälen, Schnittstellen oder Zugängen, zentralen dezentralen und externen Komponenten, Internet-Strukturen, Spezial-IT oder von Sicherheitskomponenten.
- Angriffe auf die Verfügbarkeit, z. B. das Sabotieren von Informationen oder IT-Diensten durch: Denial of Service-Angriffe, physikalische Zerstörung oder Diebstahl.
- Schädigung des Ansehens von Personen oder Institutionen infolge oben genannter Angriffe
- Angriffe auf die Integrität umfassen als Spezialfall auch Angriffe auf die Authentizität, beispielsweise das Vortäuschen einer falschen Absenderin oder eines falschen Absenders.
- Angriffe auf Branchen spezifische Schutzziele wie beispielsweise im Gesundheitswesen die Patientensicherheit.

Durch Cyber-Angriffe sind vorrangig folgende Arten von Objekten innerhalb und außerhalb einer Institution bedroht:

- **Informationen** (z. B. Forschungs- und Entwicklungsdaten, Kunden- und Rechnungsdaten Kryptodaten, Schlüssel, Zertifikate)
- **Speichermedien** (z. B. Datenbanken)
- **IT-Dienste** (z. B. Telekommunikationsdienste, Netzwerkdienste
- **Software und Anwendungen** (z.B. Benutzerschnittstellen, Browser, Plug-ins. Client-Server-Anwendungen, Internet-Anwendungen, mobile Anwendungen, Apps, Quellcode)
- **Kommunikationskanäle** (z. B. E-Mails, Soziale Netze und Foren)
- **Schnittstellen und Zugänge** (z. B. Fernzugänge, Drahtlose Zugänge, Übertragungsprotokolle)
- **Zentrale interne Komponenten** (z. B. Private Cloud-Komponenten, Netzwerkkomponenten)
- **Dezentrale Komponenten** (z. B. Mobile Clients, Endgeräte, Drucker)
- **Externe Komponenten** (z. B. IT von Partnern, Kunden, Dienstleistern, Cloud-Computing)
- **Internet-Strukturen** (z. B. Internet-Dienstleister, Hosting-Provider TLS, SSL-Zertifizierungsstellen)
- **Spezial-IT (z.B.** Zutrittskontrollsysteme, Videoüberwachungssysteme, Prozesssteuerung, -automatisierung, -leittechnik, Digitale Mess-, Steuerungs-, Regelsysteme, Smart Grid, Smart Metering)

3.8.3 Angriffsvorbereitung

Um die Erfolgsaussichten für Cyber-Angriffe zu verbessern, sind Angreiferinnen und Angreifer bemüht, im Vorfeld nützliche Informationen über die Angriffsziele zu beschaffen. Mittels dieser Informationen können Angriffe auf das Ziel zugeschnitten und besser getarnt werden.

Typische Informationen zur Angriffsvorbereitung sind:

- Identifikation möglicher Angriffspunkte
- Informationen über das Angriffsziel

- Abschätzung der Risiken eines Angriffs und Strategien zur Tarnung
- Abschätzung der Folgen eines Angriffs

Diese Informationen werden über verschiedene Wege eruiert, zum Beispiel:

- Social Engineering
- Sammlung und Auswertung frei verfügbarer Informationen über das Ziel
- Sammlung und Auswertung von Informationen über Systeme und Zugänge des Angriffsziels

Einen besonders hohen Stellenwert hat die Informationssammlung, wenn ein gezielter Angriff vorbereitet wird. Bei großflächigen Angriffen stehen hingegen eher statistische Informationen im Vordergrund, beispielsweise über den Verbreitungsgrad einer bestimmten Software.

3.8.4 Angriffswerkzeug

Täterinnen und Täter bedienen sich bei Cyber-Angriffen vielfältigen Hilfsmitteln und Werkzeugen. Häufig werden unterschiedliche Typen von Schadprogrammen oder Exploits zur Ausnutzung von Software-Schwachstellen genutzt, um Zugriff auf ein System zu erlangen. Hacking-Tools können beispielsweise dazu dienen, schwache Passwörter zu ermitteln oder verwundbare Systeme zu identifizieren. Datenträger werden manipuliert, Kommunikationskanäle und Software werden missbraucht. Je nach Art des Angriffs kann auch spezielle Hardware zum Einsatz kommen.

Schadsoftware

Schadsoftware (auch Malware, Schadcode oder Schadprogramm) ist Software, die bei Ausführung auf dem Zielrechner schädliche Operationen ausführt. Dabei werden allgemein die nachfolgenden Klassen unterschieden. Allerdings besteht moderne Schadsoftware vielfach aus einer Kombination verschiedener Funktionalitäten, ist modular aufgebaut und durch Nachladen weiterer Schadcodes dynamisch veränderbar. Entwicklung und Vertrieb von Schadsoftware werden zunehmend professionalisiert, wobei die Angreiferinnen und Angreifer mit Webseiten, Support oder Hosting Verfahren der normalen Software-Entwicklung adaptieren. In diesem Zusammenhang spricht man von „Malware-as-a-Service".

Datenträger und Kanäle

Vermeintlich unbedenkliche Datenträger und ungeschützte Kommunikationskanäle können zu einem Angriffswerkzeug werden, wenn ein Angreifender diese unter seine Kontrolle bringt, sie manipuliert oder Angriffstools darin versteckt (z.B. Mobile Endgeräte, Webseiten (infiziert oder manipuliert bzw. gefälscht), E-Mails (infiziert oder manipuliert bzw. gefälscht), unverschlüsselte Netzwerkverbindungen.

Software

Es existieren viele unterschiedliche Arten von Software, die Angreiferinnen und Angreifer bei der Durchführung von Cyber-Angriffen unterstützen.

- **Aktive Inhalte**: Die Manipulation gegebener aktiver Inhalte, wie beispielsweise JavaScript-Code, sind häufig Ausgangsbasis für Cross-Site-Scripting oder SQL-Injection-Angriffe.
- **Administrationswerkzeuge**: Schlecht abgesicherte Administrationswerkzeuge, z. B. zur Fernwartung, erlauben Angreiferinnen und Angreifern u. U. einen einfachen Zugriff auf Systeme.
- **Sicherheits-/Hacking-Tools**: Darunter fallen beispielsweise Programme zum automatischen Auffinden von Schwachstellen in einem Netzwerk, Tools zum Anpassen von Exploits oder Schadsoftware sowie Programme zur Durchführung von Brute-Force-Angriffen.
- **Internet-Client-Software**: Browser oder andere Internet-Clients sind nicht nur Ziel von Cyber-Angriffen, sondern werden auch bei der Durchführung von Angriffen benutzt.

- **Exploit**: Als Exploit bezeichnet man eine Methode oder einen Schadcode, mit dem über eine Schwachstelle in Hardware- oder Softwarekomponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Schadcode ausgeführt werden.

Internet-Strukturen

Nützliche Internet-Strukturen können als Angriffswerkzeuge missbraucht werden. Andere Internet-Dienste sind speziell für die Durchführung von Cyber-Angriffen entwickelt worden.

- **Cloud-Dienstleistungen**: Flexible Cloud-Dienstleistungen können als Angriffswerkzeug missbraucht werden, wenn über sie z. B. Phishing-Seiten gehostet, DDoS-Angriffe durchgeführt oder Rechenkapazitäten für Brute-Force-Angriffe bereitgestellt werden. Abgesehen davon ist ein Missbrauch als unauffällige Steuerungsinfrastruktur möglich.
- **Bulletproof-Hoster**: Bulletproof-Hoster sind Dienstleister, die Webspace, IP-Adressen oder andere Ressourcen im Internet bereitstellen und dabei den Missbrauch ihrer Dienstleistungen, z. B. auch für Cyber-Angriffe, bewusst in Kauf nehmen. Bulletproof-Hoster arbeiten nicht mit Strafverfolgungsbehörden oder anderen Autoritäten im Internet zusammen.
- **Botnetze**: Große Botnetze stellen durch ihre potenziellen Ressourcen an Rechenkapazität und Bandbreite eine vielfältige Bedrohung dar. Sie werden als Angriffswerkzeug häufig für DDoS-Angriffe oder den Versand von Spam-Nachrichten verwendet. Bots werden weiterhin für Click-Betrug, für das Hosting von Phishing-Seiten oder als Dropzone missbraucht.
- **Command & Control-Server**: Command & Control-Server sind zentrale Elemente eines Botnetzes und verteilen die Kommandos an die einzelnen Bots. Es existieren jedoch auch Botnetze, die Kommandos mittels Peer-to-Peer-Kommunikation weitergeben und somit auf einen zentralen Server verzichten können.
- **Dropzones**: Dropzones sind Speicher im Internet, an die von Schadprogrammen aufgezeichnete Daten automatisch übermittelt werden. Der Angreifende holt die Daten dann von der Dropzone ab. Ein direkter Zugriff des Angreifenden auf das System des Opfers wird somit unnötig.
- **Internet-Basisdienste (DNS, Routing)**: Zugriff auf und Manipulationen an Internet-Basisdiensten, wie z. B. DNS oder Routing, können für Angriffe durch Umleitung, Man-in-the-Middle oder Phishing missbraucht werden.

Geräte

Je nach Methode und Ziel eines Cyber-Angriffs kommen spezielle Geräte zum Einsatz oder vorhandene Geräte werden so manipuliert, dass sie zu einem Angriffswerkzeug werden. So werden z. B. Störgeräte für Angriffe auf drahtlose Netze genutzt. Von einer Organisation ausgesonderte Komponenten (z. B. Router) können ebenfalls, wenn sie nicht korrekt gelöscht und entsorgt wurden, für Angriffe auf die Organisation genutzt werden.

Angriffsunterstützende Informationen

Informationen sind wichtige Hilfsmittel für Cyber-Angriffe. Gestohlene Identifikationsmerkmale erlauben Zugriff auf Dienste und Dateien, Insider-Wissen erleichtert das Auffinden lohnender Ziele und die Durchführung von Angriffen. Dazu gehören:

- gefälschte Identitätsmerkmale
- gestohlene Identitätsmerkmale
- gefälschte Kryptodaten
- gestohlene Kryptodaten
- Schwachstellendatenbanken
- Insider-Wissen
- Öffentlich zugängliche Informationen

3.8.5 Angriffstarnung

Um die Aufdeckung eines Cyber-Angriffs oder die Rückverfolgbarkeit des Angreifenden zu erschweren, werden verschiedene Methoden zur Tarnung eingesetzt.

Beispiele hierfür sind:

- **Anonymisierungsdienste**: Anonymisierungsdienste versuchen, bestimmte Informationen, die auf die Identität eines Internet-Nutzenden hindeuten könnten, zu verschleiern.
- **Fälschung von IP-Adressen, Absendern, etc.**: Einige Protokolle im Internet lassen es zu, Daten einer Absenderin oder des Absenders zu manipulieren, ohne dass der Empfänger oder die Empfängerin diese Manipulation erkennen kann. Ein Beispiel sind gefälschte Absenderin oder Absender bei Spam- oder Phishing-Mails.
- **Nutzung mehrerer Zwischenstationen**: Um die Rückverfolgbarkeit eines Angriffs zu erschweren, nutzen Angreiferinnen und Angreifer mitunter mehrere Zwischenstationen, bevor sie ein Ziel angreifen. Diese Zwischenstationen können Anonymisierungsdienste, VPN-Dienste mit Endpunkten im Ausland oder andere Systeme sein, die unter der Kontrolle des Angreifenden stehen, z. B. Bots.
- **Tarnung auf dem Angriffsziel**: Um ein Ziel über einen möglichst langen Zeitraum kontrollieren oder ausspionieren zu können, muss ein Angreifender auch seine Aktivitäten auf dem Angriffsziel tarnen. Dazu werden oft Rootkit-Techniken angewendet, um eine Erkennung durch Virenschutzprogramme zu erschweren. Die Kommunikation mit dem Angreifenden kann über getarnte Kommunikationskanäle laufen, die auf den ersten Blick unbedenklich erscheinen.
- **Abschalten vorhandener Sicherheitsmaßnahmen**: Angreiferinnen und Angreifer versuchen häufig, Sicherheitsmaßnahmen zu deaktivieren oder so zu manipulieren, dass der Angriff nicht erkannt wird, aber die Sicherheitsmaßnahme dem Anschein nach weiter ordnungsgemäß funktioniert.
- **Protokollierung**: Viele IT-Systeme protokollieren die Nutzung oder die Kommunikation mit Dritten genau. Um einen Cyber-Angriff zu tarnen, muss diese Protokollierung gegebenenfalls deaktiviert, umgangen oder so manipuliert werden, dass daraus keine Rückschlüsse auf den Angriff gezogen werden können.
- **Missbrauch fremder Identitäten**: Angreiferinnen und Angreifer nutzen oft fremde Identitäten, wie z. B. Zugangsdaten von Dritten, damit ihre Aktivitäten nicht als Angriff, sondern als scheinbar legitimes Verhalten interpretiert werden.

3.8.6 Angriffspunkte und Spurenbeseitigung

Primäre Angriffspunkte für Cyber-Angreiferinnen und Cyber-Angreifer sind die über Netze, insbesondere das Internet, erreichbaren IT-Komponenten der angegriffenen Ziele. Je größer diese exponierte Angriffsfläche ist, umso einfacher ist es für den Angreifenden, einen Angriffspunkt zu identifizieren und die ersten Schritte eines Cyber-Angriffs erfolgreich durchzuführen. Viele der Ziele sind in gleicher Weise auch Angriffspunkte und somit das Objekt, das angegriffen wird, um das Angriffsziel zu erreichen.

Beispiele hierfür sind:

- **Anwendungen mit Internetzugang**: Browser, E-Mail-Programme, mobile Endgeräte, usw. sind Angriffspunkte für die über sie verarbeiteten Informationen.
- **Server**: Webserver, Kommunikationsserver, Firewalls, Remote-Wartungszugänge, usw. sind Angriffspunkte für Daten, die durch sie verarbeitet, übertragen oder geschützt werden.
- **Schnittstellen und Zugänge**: ...sind Angriffspunkte, um Zugriff auf dahinterliegende Systeme und Netze zu erhalten oder diese zu stören.
- **Dienste**: ...sind Angriffspunkte, um die durch sie bereitgestellte Funktion zu stören, zu manipulieren oder um Identitäten innerhalb des Dienstes zu missbrauchen.

Um die Entdeckung eines Cyber-Angriffs und die Ermittlung des Täters oder Täterin zu erschweren, versuchen Angreiferinnen und Angreifer meist, von vornherein keine Spuren zu hinterlassen oder die Spuren des Angriffs im Nachhinein zu beseitigen.

Dazu bedienen sie sich unter anderem folgender Techniken:

- Löschen oder Verbergen der auf dem Angriffspunkt genutzten Software, wie Hacking-Tools oder Schadprogramme.
- Löschen oder Verbergen der Spuren in Protokolldateien, mittels derer ein Cyber-Angriff im Nachhinein entdeckt werden könnte.
- Löschen oder Verbergen von Dropzones, Command & Control-Servern und ähnlicher Infrastruktur, die den Angreiferinnen und Angreifern während des Angriffs als Hilfsmittel dienten.

4 Angriffsszenarien und Sofort- bzw. Gegenmaßnahmen (VE)

4.1 Einführung

Das Abwehren von Cyber-Angriffen ist ein wesentlicher Aspekt, um Cybersicherheit erfolgreich zu gewährleisten. Um sich effektiv und erfolgreich vor Cyber-Angriffen zu schützen, wäre es essentiell, alle möglichen Angriffsszenarien zu kennen. Da im Durchschnitt täglich hunderttausende neue Schadprogramme entwickelt werden, ist dies leider unmöglich. Neue Erkenntnisse über Schwachstellen bei Hard- und Software werden immer schneller für Cyber-Angriffe genutzt. Umso wichtiger ist es, neu entdeckte Angriffstypen oder Schwachstellen zu identifizieren und den entsprechenden Stellen, zum Beispiel dem CERT-Bund des BSI, zu melden. Werden entdeckte Angriffsarten nicht veröffentlicht, können diese in letzter Konsequenz auch weltweit zu massiven wirtschaftlichen Schäden oder sogar – z. B. im Zusammenhang mit autonomem Fahren oder Medizinsystemen – zu gesundheitlichen Schäden bei Menschen führen.

4.2 Intention und Lernziele

Dieses Kapitel des Experten-Leitfadens zeigt notwendige Basis-Kenntnisse in Bezug auf Betriebssysteme und Netzwerkinfrastrukturen auf, die ein Vorfall-Experte besitzen sollte. Weiterhin werden relevante Angriffswege von Cyber-Kriminellen beschrieben, die in der Vergangenheit maßgeblich waren. Zudem bietet das Kapitel einen Einstieg in die IT-Forensik im Hinblick auf verschiedene Methoden sowie insbesondere die Datensammlung und -analyse. Der Bereich der IT-Forensik ist ein großes Feld mit diversen Spezialgebieten, das nur am Rande als Zusatzthema behandelt wird. Zuletzt werden mögliche Grenzen bei einer Datenanalyse aufgezeigt.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:


Relevante Angriffswege und -formen zu erkennen und zu verstehen.


Forensische Maßnahmen zu kennen und widerzuspiegeln.


Grenzen der Analyse zu erkennen.

4.3 Notwendige Basiskenntnisse

Es gibt einige notwendige Basiskenntnisse, die jeder Vorfall-Experte mitbringen muss, um einem Betroffenen bei der Reaktion auf IT-Sicherheitsvorfälle unterstützen zu können. Wird ein Vorfall-Experte im Rahmen des BSI Cyber-Sicherheitsnetzwerks konsultiert, ist davon auszugehen, dass es sich um einen Cyber-Angriff handelt. Durch eine fehlerhafte Behandlung eines IT-Sicherheitsvorfalls kann anstelle einer Lösung die Folgen eines Angriffs maßgeblich verschlimmert werden. Um eine unsachgemäße Behandlung zu vermeiden, ist es unabdingbar, dass jeder Vorfall-Experte mindestens die nachfolgend aufgeführten Basis-Kenntnisse mit sich bringen.

4.3.1 Betriebssysteme

Die DIN 44300 definiert ein Betriebssystem folgendermaßen:

> *Die Programme eines digitalen Rechensystems, die zusammen mit den Eigenschaften dieser Rechenanlage die Basis der möglichen Betriebsarten des Rechensystems bilden und die insbesondere die Abwicklung von Programmen steuern und überwachen.*

Letztendlich ist ein Betriebssystem eine Software, die den Funktionsablauf eines Computers steuert. Das Betriebssystem enthält die Benutzeroberfläche des Computers. Es gibt verschiedene Betriebssysteme, sowohl für Desktop-PCs als auch für mobile Geräte. Die gängigsten Betriebssysteme für den Desktop-Betrieb sind Windows, Linux und Mac OS X. Die meist verwendeten mobilen Varianten sind Android und iOS.

Vorfall-Experten sollten mindestens im Bereich der wichtigen Betriebssysteme über nachweisliche (z.B. durch Schulungen, Zertifizierungen) Administrationskenntnisse verfügen. Alternativ sind langjährige Erfahrungswerte denkbar. Hier wird auf einschlägige Schulungs- und Zertifizierungsmöglichkeiten im Bereich Windows, Linux und MacOS verwiesen.

Um mögliche Sicherheitslücken zu schließen, ist es wichtig für die IT-Sicherheit, die Betriebssysteme jeweils auf dem aktuellsten Stand zu halten und Updates schnellstmöglich zu installieren. Nicht selten kommt es in Unternehmen weltweit vor, dass IT-Systeme im Einsatz sind, auf denen ein Betriebssystem läuft, für das der Support eingestellt wurde (z. B. Windows 7). Ohne Patches und Bugfixes wächst das Risiko, Opfer einer Cyber-Attacke zu werden. Dies erlebten laut Europol zahlreiche Unternehmen im Mai 2017, als weltweit mehr als 230.000 Computer in 150 Länder mit dem Schadprogramm „WannaCry“ befallen wurden. Hintergrund war veraltete Software, welche nicht mehr vom Hersteller unterstützt wurde. Der Schaden habe sich schätzungsweise auf mehrere Milliarden US-Dollar summiert.

4.3.2 Netzwerk

Im Wesentlichen verbindet ein Netzwerk diverse Systeme miteinander, um eine Kommunikation und einen Austausch von Daten zu ermöglichen. Genaugenommen kann auch eine Verbindung zwischen zwei Computern, die miteinander kommunizieren und Datenpakete austauschen können, als Netzwerk bezeichnet werden. Ein IT-Netzwerk ist also die Verbindung verschiedener Knotenpunkte, die insgesamt gesehen ein intaktes Netz bilden.

Üblicherweise besteht ein Netzwerk aus mehreren verschiedenen Netzwerkkomponenten. Man unterscheidet zwischen aktiven und passiven Netzwerkkomponenten. Passive Netzwerkkomponenten kommen ohne eigene Stromversorgung aus. Das sind zum Beispiel Netzwerkkabel, Netzwerkdosen aber auch Netzwerk- und Verkabelungs- oder Patch-Schränke. Aktive Netzwerkkomponenten haben eine eigene Logik und benötigen eine eigene Stromversorgung. Zu den aktiven Netzwerkkomponenten zählen Geräte wie Server, Hubs, Firewalls, Router und Switches. Einzelne Bestandteile eines Computers, wie zum Beispiel eine Netzwerkkarte, können ebenso eine aktive Netzwerkkomponente darstellen.

Damit in einem Netzwerk Datenpakete ausgetauscht und die verschiedenen Netzwerkkomponenten miteinander kommunizieren können, sind sogenannte Netzwerkprotokolle notwendig. Diese Protokolle enthalten Vorgaben für den Datenaustausch und regeln so die Voraussetzungen für den anschließenden Transport, die Adressierung, das Routing (Weg des Pakets) und die Fehlerüberprüfung. Je nach Art des Netzwerkes, der daran angeschlossenen Komponenten sowie der Anzahl der Kommunikationsteilnehmerinnen und -teilnehmer gibt es eine Vielzahl unterschiedlicher Netzwerkprotokolle. Klassische Protokolle zur Datenübertragung sind TCP/IP und UDP oder HTTP und IMAP als Anwendungsprotokolle.

Jedes Unternehmen muss sich für eine Netzwerkstruktur entscheiden und diese sinnvoll umsetzen. Diese Struktur wird sich im Laufe der Zeit verändern und weiterentwickeln. Kommt es zu einem IT-Sicherheitsvorfall, ist es wichtig, mit einer Ansprechpartnerin oder einem Ansprechpartner zu kommunizieren, die sich in der Struktur und den Komponenten des Netzwerks bestmöglich auskennen und zurechtfinden. Dies kann die

Administratorin oder der Administrator des Unternehmens, gerade bei KMU aber auch ein externer IT-Dienstleister sein.

Letztendlich sollte sich in der heutigen Zeit jedes Unternehmen, aber auch jede Privatperson, das Ziel setzen, ein möglichst sicheres Netzwerk aufzubauen und zu betreiben. Unter Netzwerksicherheit versteht man alle technischen und organisatorischen Maßnahmen, mit denen die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen innerhalb eines Netzwerkes gewährleistet werden sollen. Zur Netzwerksicherheit gehört aber auch die Erkennung und Abwehr bzw. Eindämmung von Risiken. Dies ist beispielsweise mit verschiedenen Lösungen aus dem Bereich Intrusion Detection (IDS) möglich. Die Intrusion Prevention (IPS) erkennt Angriffsversuche nicht nur, sondern wehrt diese auch ab. Es gibt viele Möglichkeiten, ein Netzwerk sicher zu betreiben. Vorfall-Experten sollten ihr Wissen steht auf dem neuesten Stand halten, um sich gegen die unzähligen möglichen Cyber-Angriffe wehren zu können.

4.3.3 Schadprogramm

Der Begriff Schadprogramm (engl. Malware) umfasst alle Arten von Computerprogrammen, die unerwünschte oder schädliche Funktionen auf einem Computersystem ausführen können. Malware wird überwiegend eingesetzt, um geheime und sensible Informationen zu erlangen und diese Informationen illegal weiterzuverkaufen. Außerdem wird Malware für Cyberspionage, Cybervandalismus und sogar für Cyber-Kriege genutzt. Infizierungsmöglichkeiten bestehen unter anderem durch unseriöse Dateidownloads, den Besuch einer infizierten Webseite oder in einer E-Mail mit einem scheinbar harmlosen Link oder Anhang.

Typische Beispiele für Schadprogramme sind Viren, Ransomware, Trojaner, Spyware oder Würmer. Laut des Lageberichts zur IT-Sicherheit in Deutschland 2020, wurden insgesamt rund 117,4 Millionen neue Schadprogramm-Varianten registriert. Dies bedeutet im Durchschnitt fast 322.000 neue Schadprogramme pro Tag. Man muss davon ausgehen, dass auch in Zukunft jeden Tag zahlreiche neue Schadprogramme entwickelt werden.

Weitere Details zur aktuellen Lage und zur Entwicklung von Schadprogrammen können dem Bericht zur Lage der IT-Sicherheit in Deutschland des Bundesamts für Sicherheit in der Informationstechnik entnommen werden.

4.4 Angriffsformen

In der heutigen Zeit sorgen die vielfältigen technologischen Entwicklungen für eine starke Dynamik im Bereich der Cyberkriminalität, die sowohl Organisationen als auch Privatpersonen gleichermaßen betreffen. Auf der einen Seite werden Systeme durch diese Entwicklungen sicherer, auf der anderen Seite nimmt jedoch auch die Qualität und Vielfältigkeit von Cyber-Angriffen stetig zu. Insbesondere aufgrund der steigenden Vernetzung durch das Internet of Things (IoT) im Bereich Industrie 4.0 wächst zunehmend die Angriffsfläche für Cyber-Kriminelle.

Betrachtet man nun die verschiedenen Angriffsformen, sind hierbei keine wesentlichen Neuheiten zu erkennen. Vielmehr ist eine Weiterentwicklung von Schadprogrammen und Angriffswegen zu registrieren. Grundlage für die verschiedenen Angriffsszenarien ist dabei in den meisten Fällen ein Schadprogramm.

In den nachfolgenden Abschnitten werden die in der Vergangenheit relevantesten Angriffsformen aufgeführt und kurz beschrieben.

4.4.1 Identitätsdiebstahl (Phishing)

Im Hinblick auf die Informationssicherheit versteckt sich hinter dem Begriff der Identität eine Anzahl von Merkmalen, welche die Echtheit einer Person sicherstellt. In Verbindung mit dem Einsatz von Informationstechnik bzw. im Internet erfolgt die Verifikation einer Identität i. d. R. durch die Abfrage von Identifikations- und Authentisierungsdaten (z. B. Benutzername und Passwort).

Demzufolge wird unter einem Identitätsdiebstahl im Sinne von Cyberangriffen die unrechtmäßige Aneignung solcher Informationen verstanden.

Einer der am weitesten verbreiteten Formen ist das Phishing. Dabei wird das Opfer mittels Social-Engineering-Techniken per E-Mail zur Herausgabe sensibler Daten bewegt. Durch die große Menge an öffentlichen Identitätsdaten (Social Media) erlaubt dies dem Angreifenden personalisierte, Angriffe zu fahren. Die E-Mails scheinen auf den ersten Blick vom Originalabsender zu sein und enthalten oftmals einen Link. Die Internetseiten, welche sich hinter den Links verstecken, sind ebenso vom Original kaum zu unterscheiden. Im Fokus stehen insbesondere Online-Banking-Portale, Online-Händler und sonstige Zahlungsplattformen.

Neben Phishing können Identitätsdaten aber auch unter dem Einsatz von Schadprogrammen oder durch das Ausnutzen von Schwachstellen entwendet werden.

4.4.2 Ransomware

Ransomeware-Angriffe spielen bereits seit geraumer Zeit eine Rolle. In letzter Zeit konnte zudem ein Anstieg solche Angriffsformen verzeichnet werden. Durch den „Wanna-Cry-Angriff“ 2017 hat der Begriff Ransomware schließlich die mediale Aufmerksamkeit der Öffentlichkeit erlangt.

Hinter dem Begriff Ransomware versteckt sich ein besonderes Schadprogramm, das darauf abzielt, den Zugriff auf Dateien oder den Rechner einzuschränken oder gar komplett zu verwehren. Dies erfolgt dabei i. d. R. durch entsprechende Verschlüsselung des Zugriffs. Bemerkbar machen sich Ransomware-Angriffe durch eine auf dem Bildschirm erscheinende Mitteilung, welche die Aufforderung zur Zahlung eines Lösegelds enthält oder zu anderen Handlungen auffordern, um eine Entschlüsselung der IT-Systeme zu erwirken.

Doch auch die Zahlung eines Lösegelds oder die Durchführung sonstiger Handlungen hat in der Vergangenheit nicht immer eine Freigabe der betroffenen Systeme bewirkt.

. Aus diesem Grund ist von einer Lösegeldzahlung immer abzuraten. Zusätzlich droht der Angreifende damit die erbeuteten Daten zu veröffentlichen, wenn die oder der Betroffene nicht zahlt.

Nachfolgend werden mögliche Einfallswege für Ransomware aufgeführt. Dabei handelt es sich um die gängigsten Angriffsvektoren:

- Spam-E-Mails mit schadhaftem Anhang
- Drive-By-Downloads
- Ausnutzung von Schwachstellen

Auf der Webseite der Allianz für Cyber-Sicherheit werden weitere Informationen zum Thema Ransomware: Bedrohung, Prävention, Reaktion behandelt.

4.4.3 Distributed Denial-of-Service (DDoS)

Unter einem DDoS-Angriff ist ein Netzwerkangriff zu verstehen, bei dem Kapazitätsgrenzen von Netzwerkressourcen ausgenutzt werden und auf diese Weise Online-Dienste in ihrer Verfügbarkeit gestört werden. Um die Verfügbarkeit entsprechend zu stören, werden solange Anfragen an einen Webserver gesendet, bis die Kapazitätsgrenzen erreicht werden. Der verfolgte Zweck ist es, die angegriffene Webressource durch die wiederholten Anfragen zu überlasten, um auf diese Weise die Servicequalität zu reduzieren oder gar einer vollständigen Störung des Dienstes zu erwirken.

Zu den klassischen Zielen von DDoS-Angriffen zählen sämtliche Unternehmen, die Online-Services anbieten, insbesondere diejenigen, bei denen eine Störung oder Ausfall kundenseitig wahrgenommen werden können.

Die Auswirkungen von DDoS-Attacken erstrecken sich von erheblichen finanziellen Schäden bis hin zu einem Reputationsverlust und sind demzufolge nicht zu vernachlässigen.

4.4.4 Botnetz

Der Begriff Botnetz wird charakterisiert durch eine Gruppe von gekaperten Rechnern, die zu kriminellen Zwecken missbraucht bzw. von dem Angreifenden aus der Ferne gesteuert werden können. Die Betroffenen wissen dabei i. d. R. nichts davon, Teil eines Botnetzes zu sein.

Die Übernahme des Rechners erfolgt dabei durch eine Infizierung mit einem entsprechenden Schadprogramm. Diese ermöglicht einem Angreifenden die Übernahme der Kontrolle des Systems. Dabei können zum einen Daten eingesehen, manipuliert oder missbraucht werden, der Rechner aber auch für sonstige kriminellen Zwecke entfremdet werden. Dabei wird die Rechenleistung, die Internetverbindung oder auch der Speicherplatz missbraucht.

Im Nachfolgenden werden typische kriminelle Aktivitäten aufgelistet, die hinsichtlich der Nutzung eines Botnetzes denkbar sind:

- Datendiebstahl/-manipulation
- Durchführung von DDoS-Angriffen
- Verteilung von Spam/Schadprogramm
- Illegale Datenspeicherung

Betroffen von der Bedrohung eines Botnetzes sind grundsätzlich alle vernetzten Geräte mit einer aktiven Verbindung zum Internet. Eine besondere Bedeutung kommt demnach dem Internet of Things zu, da hier der Sicherheitsstatus in viele Bereichen bisweilen unzureichend ist.

4.4.5 Advanced Persistent Threat

Ein Advanced Persistent Threat (APT) liegt dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter, Angreifender zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.

Diese ermöglicht einem Angreifenden die Übernahme der Kontrolle des Systems. APT-Angriffe sind technisch aufwendige und zielgerichtete Attacken auf einzelne IT-Infrastrukturen und Netzwerke, die oft lange unentdeckt bleiben und zudem sehr schwierig zu entdecken sind.

Grundgedanke eines APT-Angriffs ist das Erlangen einer dauerhaften Zugriffsmöglichkeit, oftmals mit dem Hintergrund des Datendiebstahls. Nachdem ein Angreifender Zugriff erlangt hat, gestaltet sich der nächste Schritt im Etablieren von Hintertüren, um weitere Schadprogramme unbemerkt in dem Netzwerk zu platzieren und sich weiter auszubreiten.

Die Ziele von APT-Angriffen sind oftmals Unternehmen in Bereichen, bei denen sehr wertvolle Informationen zu erlangen sind.

Auf der Webseite des BSI werden weitere Informationen zum Thema Advanced Persistent Threat behandelt, sowie eine Liste mit qualifizierten APT-Dienstleistern zur Verfügung gestellt.

4.5 Darstellung forensischen Vorgehens

Es ist nicht möglich, mit einem IT-System zu interagieren, ohne darauf digitale Spuren zu hinterlassen. Deshalb fallen bei der Datenverarbeitung in IT-Systeme überall digitalen Spuren an. Beispielsweise werden schon beim Einschalten des Geräts digitale Spuren hinterlassen, wie etwa Zeitstempel im Dateisystem, Log-Dateien des Betriebssystems oder durch Laden von Daten in den Arbeitsspeicher.

Die digitale Forensik (auch IT-Forensik) ist die streng methodisch vorgenommene Datenanalyse von Datenträgern und in Computernetzen zur Aufklärung von IT-Sicherheitsvorfällen unter Einbeziehung der Möglichkeiten des Betreibers eines IT-Systems und zudem ein Weg, eine gerichtsverwertbare Beweisdokumentation zu erstellen.

In Abgrenzung zur IT-Sicherheit geht es bei der IT-Forensik zentral um die Fragen „Was ist passiert?“ sowie „Wer ist dafür verantwortlich?“ und nicht um die Frage „Was könnte passieren?“.

Das zentrale Ziel ist daher die Sicherung, Aufbereitung und Analyse von digitalen Spuren in einer Weise, die in einer möglichen späteren Gerichtsverhandlung akzeptiert wird.

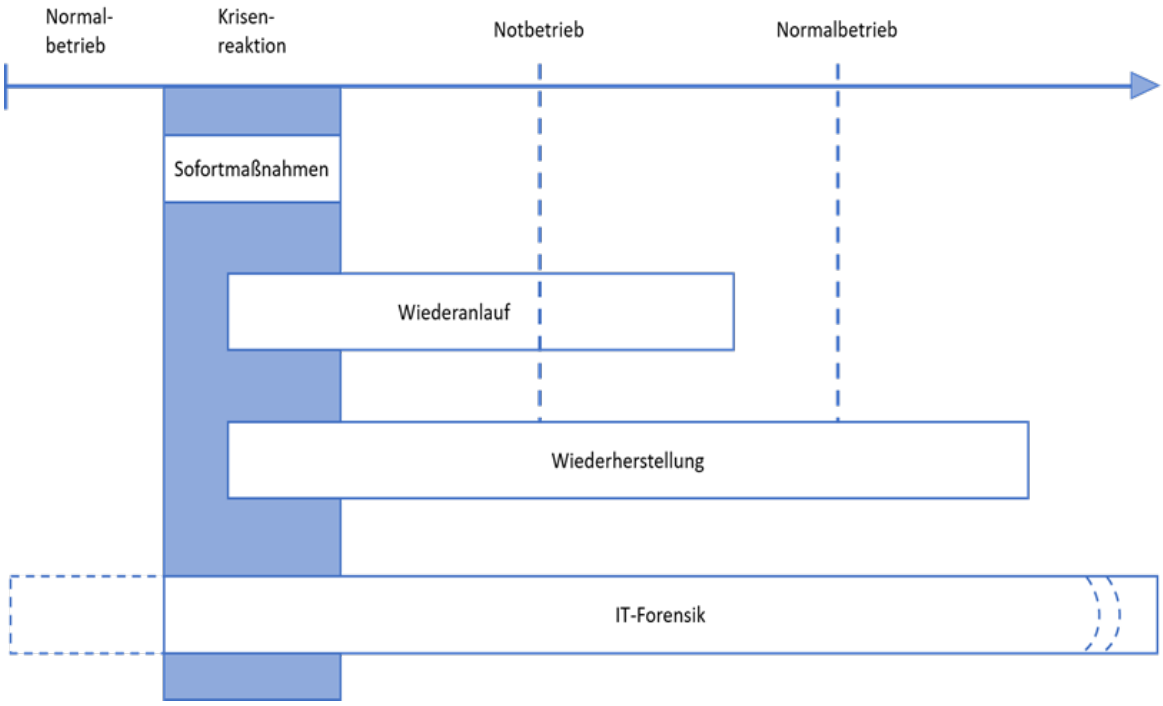


Abbildung 3: Zeitliche Einordnung der IT-Forensik

Das Bundesamt für Sicherheit in der Informationstechnik liefert mit dem BSI Leitfaden IT-Forensik ein umfangreiches Nachschlagewerk für praxisbezogene Problemstellungen und stellt darin detaillierte Informationen zur Vorgehensweise dar.

In der IT-Forensik kann man grob 2 Untersuchungsverfahrensweisen unterscheiden.

4.5.1 Methode Live-Forensik

Bei der Live-Forensik (auch bekannt als Online-Forensik) beginnt die Untersuchung bereits während der Laufzeit des IT-Sicherheitsvorfalls. Hier wird vordringlich versucht, so genannte flüchtige Daten zu gewinnen und zu untersuchen. Diese beinhalten unter anderem den Hauptspeicherinhalt, Informationen über bestehende Netzwerkverbindungen und gestartete Prozesse.

Diese Vorgehensweise ist nützlich, wenn beispielsweise Dateisysteme verschlüsselt werden, bei denen dadurch die Verschlüsselungsverfahren gesichert werden können und in einigen Fällen das logische Festplattenvolumen abgebildet werden kann, bevor der Computer heruntergefahren wird.

Es gibt eine Vielzahl von verwertbaren Informationen, die in einem Live-System gefunden werden könnten. Das Ausschalten kann zum Verlust von flüchtigen Daten wie laufenden Prozessen, Netzwerkverbindungen und gemounteten Dateisystemen führen.

Hinweis: Bestimmte Handlungen in der Live-Forensik können Angreifende auch alarmieren und u. U. destruktive Handlungen auslösen.

4.5.2 Methode Dead-Forensik

Bei der Dead-Forensik (Post-Mortem Analyse/ Offline-Forensik) findet die Untersuchung nach einem IT-Sicherheitsvorfall statt. Dies geschieht im Wesentlichen durch die Untersuchung von Datenträgern der betroffenen-Rechnersysteme. Die Post-Mortem-Forensik hat als Untersuchungsgegenstand die Analyse nicht flüchtiger Spuren auf betroffener Systeme bzw. Datenträger. Die Post-Mortem-Forensik erlaubt einen Blick in die Vergangenheit des Vorfalls (Der Sicherheitsvorfall liegt schon sehr lange zurück). Flüchtige Spuren sind hierbei weniger relevant. Die Vorteile der Dead-Forensik-Analyse an einer forensischen Datenträgerkopie sind darin zu sehen, dass flüchtige Daten nicht aus Versehen zerstört werden können und der gesamte Analyseprozess bzw. der Tooleinsatz planbar ist, da die Informationen nicht verloren gehen können.

Bei der Dead-Forensik Analyse spielt die Untersuchung der Zeiten in den Metadaten eine wichtige Rolle. Da diese vom System beeinflusst werden, muss festgehalten werden, wie das System konfiguriert war. Dazu gehört z.B. welche Zeitzone eingestellt war und ob eine Synchronisation mit einem Zeitserver aktiviert war oder ob es eine lokale Besonderheit gab. Gleichzeitig gilt es zu beachten, dass sich die Betriebssysteme beim Setzen eines Zeitstempels unterschiedlich verhalten bzw. konfiguriert sein können. Zudem können die Zeitinformationen einer Datei leicht manipuliert werden.

4.5.3 Gegenüberstellung der IT-Forensik-Methoden

Die nachfolgende Tabelle 1 zeigt die grundlegenden Unterschiede der beiden Methoden.

Live-Forensik	Dead-Forensik
Live-Forensik wird auf einem laufenden System durchgeführt	Dead Forensik wird an ausgeschalteten Systemen durchgeführt
Live-Forensik ist ein proaktiver Ansatz	Dead Forensik ist ein reaktiver Ansatz
Beweissicherung von flüchtigen Daten möglich	Vergängliche Daten sind verloren
Live Forensik übernimmt proaktiv den Prozess der Automatisierung zur forensischen Beweiserhebung, so dass die digitalen Geräte (Computer etc.) mögliche Beweise sammeln können. Bei der Live-Forensik wird die Beweiserhebung nicht automatisiert durchgeführt. Es geht hierbei darum die flüchtigen Daten (wie schon beschrieben) zu sichern.	Die Dead Forensik arbeitet nach dem Prinzip: „Warte bis etwas ausfällt und unternehme dann nötige Schritte, um das Problem zu beheben“, dies führt oft zu Stunden oder sogar Tagen verlorener Produktivität. Diese erlaubt einen Blick in die Vergangenheit des Vorfalls.

Tabelle 1: Gegenüberstellung der IT-Forensik-Methoden

4.6 Datensammlung/-erhebung

Die forensische Datensammlung beginnt mit der Erhebung einfacher Informationen. Dies kann die Systemzeit sein, aber auch andere Informationen beinhalten. Die dafür verwendeten Programme sollten keinerlei Systemdateien überschreiben oder ändern und in der Lage sein, notwendige Hardwaredaten zu berücksichtigen. Die nächsten Schritte sind nur möglich wenn das System noch eingeschaltet ist. Zuerst können die im System laufenden Prozesse aufgenommen werden. Dabei gilt es vor allem, die Informationen der „Prozessdaten“ zu betrachten.

Im Anschluss an die vollständige Erhebung der Systemprozesse werden schließlich die offenen bzw. geöffneten Netzwerkverbindungen untersucht und betrachtet. Diesbezüglich sind ebenso Programme zu berücksichtigen, die eigenständig Netzwerkverbindungen aufbauen oder Ports öffnen oder diesen zugeordnet sind. Eine besondere Bedeutung kommt hierbei den Kommunikationsprotokollen zu. Aus diesem Grund ist die Erfassung daran auszurichten. Neben den bereits aufgeführten Daten ist es weiter bedeutsam die angemeldeten Benutzerinnen und Benutzer festzuhalten sowie generelle Ereignislogs und Sitzungsdaten der Benutzerinnen und Benutzer zu sichern.

Alle zur Datenerfassung verwendeten forensischen Tools sollten Veränderungen am System vermeiden. Sollte dies nicht möglich sein, so sind die Änderungen zu dokumentieren.

Alle verwendeten Tools sollten aus sicheren Quellen stammen. Es sollten keine Tools verwendet werden, die auf dem System bereits vorhanden sind.

Anschließend kann mit der forensischen Duplikation der Festplatten, Laufwerke oder Wechseldatenträgern, wie USB oder mobilen Datenträgern, begonnen werden. Da in diesem Schritt unter Umständen sensible Informationen gesammelt werden, ist zu prüfen, inwiefern es notwendig ist, die gesammelten Informationen zu verschlüsseln. Zusätzlich sollten Write-Blocker[15] eingesetzt werden, um das Überschreiben von Informationen zu verhindern.

Ein Datenträger wie eine Festplatte sollte immer als „Full-Image“ forensisch gesichert werden.

4.6.1 Full-Image

Ein Full-Image (Forensisches-Image) definiert sich durch eine vollumfängliche Kopie einer Festplatte oder von Datenträgern. Bei diesem Verfahren wird von dem Datenträger eine bitweise (Sektorweise) Kopie erzeugt. Diese Kopie umfasst Dateien vom System oder verfügbaren Speicherbereich auf dem Datenträger, sowie möglicherweise auch gelöschte Daten. Durch das Erstellen eines Full-Images wird verhindert, dass Daten auf dem ursprünglichen Laufwerk verloren gehen. Es gilt zu beachten, dass die Systemwerkzeuge gängiger Betriebssysteme (Windows, MacOS oder Linux) nicht den Anforderungen an das Erstellen forensischer Abbilder genügen.

4.6.2 Memory-Image

Die temporären Speicherbereiche eines Systems enthalten oft wichtige Informationen wie Netzwerkverbindungen, Zugangsdaten, Internetverläufe, kryptografische Schlüssel, laufende Prozesse oder eingeschleuste Code-Fragmente. Diese Informationen sind für forensische Analysen von hohem Wert. Es sollten daher geeignete Tools verwendet werden, die in der Lage sind, den flüchtigen Speicher ohne Datenverlust zu sichern.

4.6.3 Triage-Forensik

Triage-Forensik ist ein "hybrides Vorgehen". Hierbei werden bzw. können die Systeme zielgerichtet nach Angriffsspuren untersucht und gleichzeitig Daten für die Analyse gesammelt.

Ein Triage Image ist ein kleiner Teil eines Full-Disk Images. Im Triage Image sind die "wichtigsten" forensischen Artefakte (AmCache, Windows EventLogs, Windows Registrierungsdatenbank, etc, - bsp. hier WIndows Betriebssystem)) eines Systemes enthalten. Sollte sich nach der Analyse des Triage Image der "Verdacht" ergeben, dass noch mehr auf dem System passiert sein könnte, wird das Full Disk Image analysiert. Beim Triage Image geht es demnach also erstmal darum einen ersten Eindruck vom System zu bekommen und Zeit zu sparen.

Falls die Tools mit ausreichend guten und validen Daten vorbereitet worden sind, d. h. IoC (Indicator of Compromise) wurden bei der Einsatzvorbereitung auf Tools eingespielt, ist der Einsatz einfach. Der Vorteil solcher Tools besteht darin, dass diese auch von Nutzerinnen und Nutzern ohne besondere Expertise ausgeführt werden können. Anders als bei den im Folgenden vorgestellten Methoden wird beim Triage-Prozess die Menge der erhobenen Daten geringgehalten, da dieses Verfahren keine vollumfängliche Kopie des Systems erzeugt.

4.7 Datenanalyse

Im weiteren Verlauf dieses Kapitels werden unterschiedliche, mögliche Quellen für Spuren kurz beschrieben. Die genannten Quellen erheben keinen Anspruch auf Vollständigkeit. Hier wird auf spezifische Einträge und Kommandozeilenbefehle eingegangen und welche Ergebnisse diese liefern. Dabei sei darauf hingewiesen,

[15] Write Blocker (Schreibblocker) werden im Rahmen der Forensik dazu verwendet, Änderungen während einer Auswertung zu verhindern, um eine Gerichtsverwertbarkeit herzustellen.

dass nicht die auf den Systemen vorhandenen Kommandozeilenbefehle genutzt werden. Zusätzlich müssen die eingesetzten Tools von einer gesicherten Quelle stammen.

Die Datenanalyse stellt einen wichtigen Bestandteil der Forensik dar. In dieser Phase können gesammelte Daten korreliert werden, um anschließend einen gemeinsamen Zeitstrahl zu ermitteln. Zusätzlich können in dieser Phase der Forensik mehrere Datenquellen in ein Verhältnis gesetzt werden. Oft ist es nicht nur notwendig, lokale Daten zu analysieren, sondern auch aus anderen Datenquellen, die Aufschluss über den IT-Sicherheitsvorfall geben können. Im Folgenden werden die drei am häufigsten verwendeten Systeme behandelt.

4.8 Toolhandling

Es gibt viele Hersteller, die forensischen Tools- und Toolkits auf dem Markt vertreiben. Die bekannten Tools sind zuverlässig einsetzbar und halten in der Regel das, was sie versprechen. Die Funktionen von professionellen forensischen Tools variieren recht stark, je nachdem, welchen Aspekt der forensischen Analyse sie behandeln und für welchen Markt sie gedacht sind. Jede Benutzerin und jeder Benutzer sollte sich also im Vorfeld überlegen, für welche Software bzw. welches Toolkit man sich entscheidet. Es gibt auch kostenfreie Tools auf dem Markt, für die es aber häufig nur mangelhaften oder gar keinen Support gibt. Es kann auch Sinn machen, bei der Analyse verschiedene forensische Tools parallel zu verwenden. Da kein Tool die vollständige Bandbreite der Vorräte IT-Forensik abdeckt, können sich verschiedene Tools häufig gut ergänzen und so eine größere Bandbreite abgedeckt werden.

Wichtig zu beachten ist, dass eine Einarbeitung in die Handhabung und Bedienungsweise der Tools erforderlich ist. Zu erwarten, eine Software zu erwerben und diese sofort professionell nutzen zu können, ist ein naives Wunschdenken. Eine Einarbeitung, am besten in Form einer Schulung oder eines Trainings im Vorfeld, ist immer erforderlich.

Nichtsdestotrotz sind viele der Tools nach kurzer Eingewöhnungszeit einfacher zu bedienen, als oft zunächst befürchtet. Die großen Hersteller von Softwarelösungen und Tools schließen einen weiten Bereich von forensischen Datenservices in einem einzigen Paket ein. Viele forensische Spezialistinnen und Spezialisten ziehen es dennoch vor, ihre eigenen individualisierten Werkzeugkisten aus einzelnen Tools zusammenzustellen, die exakt auf ihre Bedürfnisse ausgerichtet sind.

4.9 Grenzen der Analyse

Um die Auswirkungen eines IT-Sicherheitsvorfalls detailliert zu ermitteln, ist es im Zuge der Forensik erforderlich, eine detaillierte Analyse von Beweisen durchzuführen. Auf diese Weise können oftmals offene Fragen hinsichtlich des zugrundeliegenden IT-Sicherheitsvorfalls geklärt werden und dieser wirksam und vollständig behoben werden, im Idealfall sogar ein erneutes Auftreten ausgeschlossen werden.

Im Verlauf der Analyse kann die Komplexität des IT-Sicherheitsvorfalls stark zunehmen. In diesem Fall sollte der Vorgang an spezialisierte, externe IT-Sicherheitsdienstleister mit Forensik-Expertinnen und Forensik-Experten bzw. möglicherweise an die entsprechenden Strafverfolgungsbehörden abgegeben werden.

Doch auch die Möglichkeiten der Analyse sind nicht unendlich. Diese können an Grenzen stoßen, an denen eine Fortsetzung nicht mehr sinnvoll oder auch unerwünscht ist bzw. gesetzliche Vorgaben überschreiten würde.

Die folgenden Abschnitte führen Grenzen der Analyse auf, an die Vorfall-Experten bei ihren Tätigkeiten stoßen kann.

4.9.1 Beweissicherung fehlerhaft oder unzureichend

Grundlage für die Analyse ist eine ordnungsgemäße und möglichst detaillierte Beweissicherung. Kommt es im Zuge der Sicherung von potenziellen Beweisen zu Fehlern, die eine Manipulation der entsprechenden Daten zufolge hat, so würden jegliche Analysetätigkeiten die Sinnhaftigkeit verlieren. Gleiches gilt, wenn Beweise vollständig vernichtet werden.

4.9.2 Beauftragung wird überstiegen

Die Tätigkeiten eines Vorfall-Experten sind durch den Betroffenen zu beauftragen. Diesbezüglich ist es aus Sicht des Betroffenen womöglich wünschenswert, einen gewissen Aufwand bezüglich der Kosten zu definieren, der nicht überschritten werden soll. Nichtsdestotrotz ist es bei den meisten IT-Sicherheitsvorfällen erforderlich, Analysen von ermittelten Beweisen durchzuführen, um die Ursache entsprechend aufklären zu können. Es ist jedoch notwendig, die Analysetätigkeiten an dem beauftragten Aufwand zu orientieren, um keine zusätzlichen Kosten zu verursachen. Hierbei besteht die Gefahr, dass die Analyse zu kurz kommt und nicht in der nötigen Tiefe durchgeführt werden kann.

4.9.3 Analyse führt zu keinen Ergebnissen

Im Kontext der Analyse von gesicherten Beweisen kann der Vorfalls-Experte an einen Punkt geraten, an der die Analysetätigkeiten keine Anhaltspunkte und keine Ergebnisse bezüglich der Ursachen bzw. des Ausmaßes liefern. Ein Grund dafür ist beispielsweise eine verspätete oder mangelhafte Beweissicherung. Gelangt ein Vorfall-Experte an einen solchen Punkt, ist es nicht zielführend, die Analysetätigkeiten weiterzuführen.

4.9.4 Betroffener verzichtet auf eine detaillierte Analyse

Je nach Zielsetzung eines Betroffenen kann dieser möglicherweise im Hinblick auf eine schnelle Wiederherstellung der betroffenen Systeme auf eine detaillierte Analyse verzichten. In diesem Fall sind Analysetätigkeiten lediglich in einer stark eingeschränkten Form notwendig. Die Gefahr besteht, dass hierbei die Ursache nicht vollständig behoben werden kann und ein erneutes Auftreten wahrscheinlicher wird.

5 Ablauf des Standardvorgehens (VP&VE)

5.1 Einführung

Unternehmen sowie auch Privatpersonen haben heutzutage immer mehr mit Bedrohungen durch IT-Sicherheitsvorfälle zu kämpfen. Als Opfer eines Cyber-Angriffs ist es wichtig angemessen zu reagieren, um das Schadensausmaß möglichst gering zu halten. Vor allem bei kleineren Unternehmen und Privatpersonen können hierbei jedoch nicht die erforderlichen Kompetenzen vorgehalten werden. Die angemessene Reaktion auf bzw. Behandlung von IT-Vorfällen erfordert somit die Unterstützung von externen Expertinnen und Experten.

Um bestmögliche Ergebnisse zu erreichen, ist es erforderlich ein einheitliches Vorgehen hinsichtlich der Reaktion auf IT-Sicherheitsvorfälle im Vorhinein zu bestimmen. Dabei sind die verschiedenen Schritte entsprechend darzustellen und zu beschreiben. Als Vorfall-Praktiker oder Vorfall-Experte gilt es nach dieser zielgerichteten und geordneten Verfahrensweise zu agieren. Die hier dargestellte Standardvorgehensweise bietet dabei die Möglichkeit weitere Vorfall-Praktiker oder Vorfall-Experten bei der Behandlung problemlos hinzuzuziehen und führt i. d. R. zu vergleichbaren Ergebnissen.

5.2 Intention und Lernziele

Dieses Kapitel des Experten-Leitfadens behandelt die Ausführung der unterschiedlichen Schritte des Standardvorgehens. Diese gehen von der Vorbereitung über die Identifikation bis hin zu einer Wiederherstellung der betroffenen Systeme. Weiterhin wird die ordnungsgemäße Dokumentation des IT-Sicherheitsvorfalls und Aufarbeitung für weiterführende Stellen thematisiert.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:


Die Standardvorgehensweise bei der Behandlung von IT-Vorfällen anzuwenden.


Einen IT-Sicherheitsvorfall angemessen zu erfassen und die erforderlichen Schritte einzuleiten.

5.3 Identifikation des IT-Sicherheitsvorfalls

Die Grundlage für eine ordnungsgemäße Reaktion auf IT-Sicherheitsvorfälle stellt die Identifikation der Problematik dar. Um eine Reaktion auf IT-Sicherheitsvorfälle durchführen zu können, ist neben Fachwissen entsprechende Erfahrung und Routine notwendig.

Somit kommt der korrekten Identifikation eine essenzielle Rolle im Hinblick auf eine erfolgreiche Behebung zu. In diesem Zusammenhang ist es erforderlich, den Sachverhalt entsprechend nachvollziehen und verstehen zu können. Lediglich bei dieser Vorgehensweise ist es möglich, zielgerichtete Schritte einzuleiten, um den zugrundeliegenden IT-Sicherheitsvorfall vollständig zu beseitigen.

Ausgangspunkt für eine korrekte Identifikation ist eine detaillierte Erfassung der Problemstellung. Dabei gilt es, durch gezielte Fragen den Sachverhalt möglichst genau aufzunehmen. Um die Erfassung übersichtlich zu gestalten, ist es empfehlenswert, die Ergebnisse angemessen zu dokumentieren. Dafür steht ein entsprechendes Formular bereit, welches diesbezüglich herangezogen werden kann.

Nach abgeschlossener Erfassung der Problemstellung gilt es, im Kontext der Identifikation eine Entscheidung zu treffen, ob tatsächlich ein IT-Sicherheitsvorfall vorliegt. Diesbezüglich sind die aufgenommenen Informationen auszuwerten. Dabei sind Systemauffälligkeiten entsprechend zu beurteilen und sonstige Unregelmäßigkeiten zu bewerten, um dabei mögliche Zusammenhänge zu erkennen, die Aufschluss über den IT-Sicherheitsvorfall liefern.

Kommt ein Vorfall-Praktiker oder Vorfall-Experte dabei zu dem Entschluss, dass es sich um keinen IT-Sicherheitsvorfall handelt, können die Tätigkeiten an dieser Stelle eingestellt werden. Liegt jedoch ein IT-Sicherheitsvorfall vor, ist der entsprechende Angriffstyp zu bestimmen, um darauf aufbauend die nächsten Schritte gezielt einleiten zu können.

Im Rahmen der Erfassung und Identifikation sind für den Vorfall-Praktiker und Vorfall-Experten zwei wesentliche Szenarien möglich:

1. Kontaktaufnahme über den Digitalen Ersthelfer
2. Direkte Kontaktaufnahme

5.3.1 Kontaktaufnahme über den Digitalen Ersthelfer

Die Kontaktaufnahme zu einem Vorfall-Praktiker oder Vorfall-Experten kann über den Digitalen Ersthelfer erfolgen. In diesem Fall hat sich ein Betroffener über die Hotline des Cyber-Sicherheitsnetzwerks (CSN) an einen Digitalen Ersthelfer gewendet, der die Problematik jedoch nicht lösen konnte. Eine Erfassung der Problematik kann dabei unter Verwendung des Vorfall-Berichts bereits durchgeführt worden sein. Dieses wird der Expertin oder dem Experten entsprechend zur Verfügung gestellt und bildet die Grundlage für den Einstieg in die Thematik. Dennoch sind die festgehaltenen Informationen zu verifizieren und ggf. durch weiterführende Fragestellungen zu ergänzen.

5.3.2 Direkte Kontaktaufnahme

Bei der direkten Kontaktaufnahme zu einem Vorfall-Praktiker oder Vorfall-Experten wird der Digitalen Ersthelfer im Hinblick auf die Digitale Rettungskette übersprungen. Ein Betroffener wendet sich dabei über die Hotline des Cyber-Sicherheitsnetzwerks unmittelbar an einen Vorfall-Praktiker oder Vorfall-Experten. Zu diesem Zeitpunkt ist somit noch keine Aufnahme durch einen Digitalen Ersthelfer erfolgt. Demzufolge gestaltet sich die grundlegende Erfassung als erster Schritt.

5.4 Eindämmung des Schadensausmaßes

Liegt ein IT-Sicherheitsvorfall vor, ist es erforderlich, zügig, aber auch korrekt zu handeln. Die übereilte Umsetzung von Maßnahmen ist an dieser Stelle nicht empfehlenswert, da als Folge gegebenenfalls ein höherer Schaden entstehen kann. Nichtsdestotrotz ist das Schadensausmaß durch die Realisierung von verschiedenen Sofortmaßnahmen einzudämmen und damit eine weitere Ausbreitung zu unterbinden. Die Eindämmung der Auswirkung eines Angriffs ist ein wesentliches Prinzip, um den Schaden möglichst auf ein Minimum zu begrenzen. Die Auswahl von und Entscheidung über Sofortmaßnahmen bedürfen ein ausreichend hohes Maß an Fachwissen und Erfahrung.

Es muss aber darauf hingewiesen werden, dass jede solche Aktion, die durchgeführt wird, eine Beweissicherung erschwert oder unmöglich macht. Infolgedessen wird dann auch die IT-forensische Analyse erschwert. Daher müssen die durchgeführten Sofortmaßnahmen wohl überlegt sein. Bei der Auswahl der Sofortmaßnahmen ist unter Betrachtung des vorliegenden Sachverhalts eine Entscheidung durch den Vorfall-Praktiker oder Vorfall-Experten zu treffen und die Umsetzung einzuleiten oder je nach Möglichkeit selbst durchzuführen. Dabei sind die nachfolgenden Fragestellungen zu berücksichtigen:

- Konnten die betroffenen Systeme zweifelsfrei identifiziert werden?
- Welche Schäden könnten entstehen? Besteht eine Cyber-Versicherung (siehe auch 6. 2.5.3. Versicherungen)?

- Wird eine Strafverfolgung angestrebt?
- Ist die Isolierung der Systeme möglich und erforderlich?

Unter Abwägung der aufgeführten Fragen kann eine mögliche Schadenseindämmung angestoßen werden. Diesbezüglich werden in den folgenden Abschnitten grundlegende Optionen aufgezeigt und beschrieben.

5.4.1 Isolierung des infizierten Systems

Eine in der Praxis meist verwendete Eindämmungsmaßnahme stellt die Isolierung dar. Voraussetzung für eine ordnungsgemäße und wirksame Isolierung des betroffenen Systems ist die möglichst eindeutige und korrekte Identifizierung. Dann ist das betroffene System zum einen vom Produktivnetz zu trennen und zum anderen eine aktive Verbindung zum Internet zu unterbrechen. Dazu ist das Netzwerkkabel zu ziehen und ggf. die WLAN-Verbindung zu deaktivieren. Eine Separierung des infizierten Systems in ein eigenes VLAN-Segment, welches keine Verbindung zum restlichen IT-Umfeld hat, sollte erfolgen.

Neben einzelnen Systemen kann es aber auch erforderlich sein, mehrere Geräte oder Netzsegmente zu isolieren, sofern diese von einer Infizierung bzw. dem Angriff betroffen sein könnten.

Neben der Eindämmung des Schadensausmaßes ist auch ein Ziel, die Kommunikation zum angreifenden wirksam und vollständig zu unterbinden.

Durch diese Isolierung des Systems wird die Kommunikation mit dem Angreifer entsprechend unterbunden. Infolgedessen werden eine weitere Ausbreitung sowie ein unbefugter Datenabfluss verhindert. Wichtig hierbei ist, dass im Zuge der Isolierung alle betroffenen Systeme betrachtet werden, um den möglichen Schaden wirksam einzudämmen. Hierbei ist zu beachten, dass durch solche Maßnahmen, der Angreifer zu destruktiven (Gegen)Maßnahmen greifen kann.

5.4.2 Sperrung und Änderung von Zugangsdaten

Je nach Art des IT-Sicherheitsvorfalls kann es auch notwendig sein, Zugangsdaten entsprechend zu ändern. Wird dies bereits durch den Angreifenden verhindert, so sind die relevanten Benutzerkonten entsprechend zu sperren.

Ziel dieser Maßnahme ist es, den Zugriff des Angreifenden auf die betroffene Umgebung wirksam zu unterbinden. Dabei ist es unter Umständen erforderlich, ebenso die Passwörter von weiteren Diensten zurückzusetzen, insbesondere bei Ähnlichkeiten der Zugangsdaten. Wird dies bereits durch den Angreifenden verhindert, so sind die relevanten Benutzerkonten entsprechend zu sperren. Hier sollte beachtet werden, dass der Angreifende bereits umfangreiche administrative Berechtigungen erlangt haben könnte („Golden-Ticket“).

Systeme (zum Beispiel Domain Controller) sollten auf suspekte Benutzerkonten überprüft werden. Weiterhin sind Benutzerkennungen verdächtig, welche zu ungewöhnlichen Zeiten genutzt worden sind oder Dienste ausgeführt haben. Deshalb sollten nach Möglichkeit alle betroffenen Systeme identifiziert werden. Die geplanten Kontenänderungen und -Sperrungen sollten möglichst zeitgleich durchgeführt werden.

Bei einem größeren Befall müssen gegebenenfalls Systeme wie Domaincontroller außer Betrieb genommen werden. Dies kann u. U. so weit gehen, die ganz gesamte IT-Infrastruktur vom Internet zu trennen. Deshalb sollten die Maßnahmen vorab gut durchdacht werden.

Im Rahmen dieser Änderung kann es auch hilfreich sein, Sicherheitsmechanismen wie beispielsweise eine Mehr-Faktor-Authentifizierung zu aktivieren, sollte die Möglichkeit dazu bestehen.

5.4.3 Arbeiten am betroffenen System einstellen

Bei vielen Systemen werden wiederkehrende Regeln und regelmäßige Tätigkeiten durch die Administratoren durchgeführt. Finden solche Arbeiten plötzlich nicht mehr statt, kann dies einen Angreifenden alarmieren.

In der Folge kann ein Angreifender ggf. destruktive Maßnahmen (z.B. das Löschen von wichtigen und sensiblen Daten) durchführen oder die Spuren verändern. Diese Möglichkeit sollte bei allen durchgeführten Maßnahmen und Aktivitäten in die Entscheidungsfindung einfließen.

Als kompromittiert eingestufte Systeme bzw. Geräte sind mit Vorsicht zu behandeln, insbesondere wenn eine Beweissicherung durchgeführt werden soll oder noch nicht abgeschlossen ist. Handlungen mit dem infizierten System sind, wenn möglich, komplett zu vermeiden. Sollte es unvermeidlich sein, Arbeiten durchzuführen, sind diese angemessen zu dokumentieren und sollten im Idealfall im 4 Augen-Prinzip mit dem Vorfall-Praktiker oder Vorfall-Experten erfolgen. Dennoch sollten die vorgenommenen Aktionen auf ein Minimum beschränkt werden. Jeder Vorgang am kompromittierten System kann im schlimmsten Fall dazu führen, dass ermittlungsrelevante Daten unwiderruflich verändert, zerstört oder gelöscht werden.

Hinsichtlich der angemessenen Dokumentation von Tätigkeiten an einem infizierten System sind die folgenden Informationen festzuhalten:

- Zeitpunkt
- System
- Nutzerkonto
- Art der Aktion

Die geplanten Schritte bedürfen einer guten Abschätzung.

5.4.4 Gerät nicht herunterfahren

Um den IT-Sicherheitsvorfall angemessen untersuchen und analysieren zu können, ist es wichtig, eine Beweissicherung durchzuführen. Gleiches gilt für die Einleitung bzw. Bearbeitung einer Strafanzeige. Aus diesem Grund ist es wichtig, betroffene Geräte nicht auszuschalten oder herunterzufahren, bevor die Erhebung von Beweisen abgeschlossen ist. Das vorschnelle Herunterfahren kann hierbei wichtige Informationen und Beweise, insbesondere von flüchtigen Speichern wie dem Arbeitsspeicher, unwiderruflich löschen. Nach erfolgter Beweissicherung kann das System ausgeschaltet werden. Bei kompromittierten Systemen ist ein hartes Ausschalten wiederum zu empfehlen.

5.4.5 Keine weiteren Maßnahmen eigenständig umsetzen

Führt ein Betroffener Maßnahmen durch, ohne dies vorher mit dem Vorfall-Praktiker oder Vorfall-Experten abzustimmen, kann nicht ausgeschlossen werden, dass sich dadurch das Schadensausmaß erhöht. Vorschnell verwirklichte Handlungen können hierbei beispielsweise eine weitere Ausbreitung der Infizierung nach sich ziehen oder auch wichtige Informationen im Hinblick auf die Beweissicherung verfälschen oder zerstören. Aus diesem Grund ist dem Betroffenen von der eigenständigen Umsetzung von Maßnahmen in jedem Fall abzuraten.

5.5 Ermittlung der Ursache

Nachdem eine Ausbreitung durch die Umsetzung von Sofortmaßnahmen verhindert werden konnte bzw. die Kommunikation zum Angreifenden wirksam unterbrochen wurde, kann der zugrundeliegende Sachverhalt genauer untersucht und analysiert werden. Es ist zu beachten, dass häufig die Ausbreitung zunächst nur gebremst oder verzögert werden kann.

Ziel ist es, die Ursache bzw. den Auslöser des IT-Sicherheitsvorfalls zu ermitteln. Im Zuge dessen ist der Angriffsweg zu bestimmen und das Schadensausmaß der betroffenen Systeme zu beurteilen.

Die Übersicht der betroffenen Systeme sowie die Ergebnisse der Analyse bilden die Basis für die gezielte Bereinigung und Wiederherstellung. Darüber hinaus kann im Rahmen der Ursachenermittlung ein Angreifender möglicherweise erfolgreich identifiziert werden und Beweise für eine strafrechtliche bzw. gerichtliche Verfolgung gesichert werden. Das Verfahren gliedert sich dabei im Wesentlichen in die Identifizierung und

Sicherstellung von Informationen und Daten im Sinn der Beweissicherung, die Analyse der gesammelten Informationen sowie einer kontextuellen Bewertung des Gesamtzusammenhangs.

Das Ziel ist die Beantwortung der folgenden Fragen:

- Was ist geschehen?
- Wo ist es passiert?
- Welche Systeme bzw. Netzsegmente sind betroffen?
- Wann ist es passiert?
- Wie ist es passiert?

Neben den aufgeführten Fragestellungen können zudem die nachfolgenden Fragen relevant werden, insbesondere, wenn eine gerichtsverwertbare Nachverfolgung angestrebt wird.

- Wer hat es getan?
- Was kann gegen eine Wiederholung getan werden?

5.5.1 Beweissicherung

Grundlage für eine strukturierte Ursachenermittlung ist die möglichst ausführliche Sicherung von Beweisen. In der Breite und Tiefe kann die Beweiserhebung allerdings Unterschiede ausweisen, welche sich ebenso im Aufwand der Erhebung widerspiegeln. Ausschlaggebend ist hierbei in erster Linie die zum Einsatz kommende IT-Infrastruktur. Nichtsdestotrotz nehmen hierbei auch die Zielsetzung des Betroffenen sowie der Kostenfaktor eine wichtige Rolle ein.

Angelehnt an den Vorstellungen des Betroffenen ist ein entsprechender Arbeitsauftrag festzulegen, welcher die Ziele der Untersuchung unter Berücksichtigung der zur Verfügung stehenden Ressourcen priorisiert. Infolgedessen kann es erforderlich sein, bei der Beweiserhebung einschränkende Entscheidungen zu treffen. Bei der Auftragserteilung sollte vereinbart werden, ob eine gerichtsverwertbare Sicherung und Dokumentation erfolgen muss, oder ob darauf verzichtet werden kann. Zusätzlich sind mögliche Anforderungen von Versicherungen zu betrachten.

Unter Betrachtung der Größe, der Komplexität, dem Aufbau der Systemlandschaft sowie der Zielsetzung des Betroffenen kann schließlich eine Beweismittelsicherung für eine spätere Analyse angestoßen werden.

Dabei gilt es im ersten Schritt, sämtliche digitalen Spuren zu identifizieren und zu lokalisieren, welche als Beweis im Hinblick auf die Ermittlung des Auslösers dienen können. Bei der Datensammlung sind alle potenziell betroffenen Systeme zu berücksichtigen.

Der zweite Schritt wird durch die Speicherung der identifizierten Daten dargestellt. Im Idealfall erfolgt eine vollständige Erfassung und Sicherung unter der Voraussetzung, dass durch die Sicherungsmaßnahmen keine Daten verfälscht wurden.

Ein wichtiger Punkt bei der Datensammlung im Zuge der Beweissicherung ist die Sicherungsreihenfolge. Die Daten können hierbei in zwei Kategorien eingeteilt werden:

- Flüchtige Daten
- Nichtflüchtige Daten

Der wesentliche Unterschied liegt in der Erhaltbarkeit. Während nichtflüchtige Daten, welche sich auf Massenspeichern wie z. B. der verbauten Festplatte befinden, auch nach dem Herunterfahren bzw. Ausschalten des Gerätes weiterbestehen, gehen flüchtige Daten unwiderruflich verloren. Sie befinden sich überwiegend im Arbeitsspeicher, sind aber auch u. a. in Registern des Prozessors zu finden. Ein besonderes Augenmerk bei der Reihenfolge ist somit auf flüchtige Speicher zu legen, sofern diese Spuren enthalten könnten.

Unter Berücksichtigung der Flüchtigkeit von Daten ergibt sich infolgedessen die folgende Reihenfolge der Vorgehensweise:

1. Prozessor-Register und -Cache
2. Arbeitsspeicherinhalt, Netzstatus, Routingtabellen, Prozessliste und ARP-Cache
3. Temporäre Dateien und SWAP-Bereiche
4. Inhalte von Massenspeichern
5. Protokolldateien (z. B. Logging- und Monitoringdaten)
6. Physische Konfigurationen und Netzwerktopologien
7. Archivierte Medien

5.5.2 Analyse

Nach erfolgter Beweissicherung ist es erforderlich, die gesammelten Daten zu analysieren. Ziel der Analyse ist es, den zugrundeliegenden IT-Sicherheitsvorfall möglichst zu rekonstruieren, um auf diesen Weg den Auslöser zu ermitteln und das Schadensausmaß zu beurteilen.

Diesbezüglich gilt es, die gesammelten Daten bzw. Beweise detailliert zu untersuchen. Im Rahmen der Analyse ist ein besonderer Fokus auf die Identifizierung von Zusammenhängen zwischen den unterschiedlichen Daten zu legen, um auf diese Weise Rückschlüsse zu der Ursache zu erschließen.

Da in der Praxis oftmals mehrere Komponenten einer Systemlandschaft von einem IT-Sicherheitsvorfall betroffen sind, ist eine erfolgreiche Analyse hierbei von der richtigen Interpretation der vorliegenden Daten und der korrekten Identifizierung von Zusammenhängen abhängig. Gleichzeitig hängt der Erfolg der Datenanalyse aber auch von der zur Verfügung stehenden Zeit ab. Wie bei der Beweiserhebung beschrieben, kommt es hierbei auf die Zielvorstellungen des Betroffenen im Hinblick auf den beauftragten Aufwand an.

Sollte der Vorfall-Praktiker oder Vorfall-Experte bei der Analyse an seine Grenzen stoßen, so sollte er die Vorfall-Bearbeitung an einen registrierten IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten abgeben.

5.5.3 Gesamtbewertung

Aufbauend auf der Beweissicherung sowie der nachfolgenden Analyse erfolgt zuletzt eine Bewertung der Situation. Dabei werden die Ergebnisse der Analyse aufbereitet und in den Kontext eingeordnet. Zweck der Gesamtbewertung ist es, einen Betroffenen über die Ursache des IT-Sicherheitsvorfalls sowie das genaue Schadensausmaß in Kenntnis zu setzen und gezielten Sofortmaßnahmen vorzuschlagen, um eine zügige und korrekte Wiederherstellung der Systeme zu ermöglichen.

Der Angriffs- bzw. Einbruchsweg kann hierbei in zwei generelle Kategorien eingeteilt werden:

- **Technische Schwachstellen:**
  Unter einer technischen Schwachstelle wird grundsätzlich eine Sicherheitslücke in den zum Einsatz kommenden Systemen verstanden. Ursache kann hierbei u. a. auch Fehler in der Konfiguration sein. Ein Angreifender nutzt die Lücken aus, um schadhafte Software einzuschleusen.
- **Menschliche Schwachstellen:**
  Unter einer menschlichen Schwachstelle wird im Wesentlichen eine Fehlhandlung des Benutzenden verstanden. Größtenteils geschieht eine menschliche Fehlhandlung unwissentlich oder versehentlich. Ein Angreifender nutzt hierbei die Unwissenheit und Ahnungslosigkeit aus. Jedoch ist an dieser Stelle auch eine vorsätzliche Fehlhandlung nicht auszuschließen.

5.6 Wiederherstellung der Systeme

Cyber-Angriffe können zum Teil weitreichende Auswirkungen mit sich bringen. Die Folgen sind dabei oftmals tiefgreifende Änderungen an den betroffenen Systemen. Durch eine frühzeitige Umsetzung von Sofortmaßnahmen wird eine Ausbreitung bzw. das Schadensausmaß möglichst auf ein Minimum reduziert. Nach durchgeführter Analyse und Untersuchung von digitalen Spuren und Beweisen erfolgt schließlich die Wiederherstellung der Systeme. Bevor die betroffenen Systeme jedoch wieder in die Produktivumgebung eingebunden werden können, ist eine vollständige Bereinigung erforderlich. Im Zuge dessen gilt es den, Angriffsweg bzw. den Infektionsvektor zu schließen. Dabei wird zwischen zwei grundlegenden Methoden unterschieden:

- **Neuaufbau/Neuinstallation der Systeme**
  In diesem Fall wird das IT-System grundlegend neu aufgesetzt, indem alle Daten gelöscht werden und das Betriebssystem erneut installiert wird. Um hierbei einen Datenverlust zu vermeiden, ist vorher zu prüfen, ob „saubere“ Datensicherungen vorliegen (siehe dazu auch 6.2.4.2 Bereinigung der Systeme). Ist das der Fall, können die Daten nach der Einrichtung wiederhergestellt werden. Durch eine vollständige Neuinstallation kann weitestgehend ausgeschlossen werden, dass durch Hintertüren eine erneute Infizierung möglich ist. Darüber hinaus ist es empfehlenswert, die Systeme entsprechend zu härten und verfügbare Patches und Updates von Sicherheitssoftware zu installieren.
- **Bereinigung des Systems durch Löschung des Schadprogramms**
  Um eine Bereinigung anhand einer Entfernung des Schadprogramms durchzuführen, ist es notwendig, während der Ursachenanalyse den genauen Angriffsweg bzw. Einbruchsweg zu kennen. Ausschließlich in diesem Fall ist eine gezielte Bereinigung möglich. Im Zuge dessen werden die schadhaften Dateien eliminiert. Auch bei dieser Methode ist es sinnvoll, die Systeme zu härten und verfügbare Updates und Patches für installierte Software zu installieren.

Nach vorgenommener Bereinigung sind die Systeme wieder nutzbar und können in die Umgebung eingebunden werden. Systeme für kritische Geschäftsprozesse sollten dabei priorisiert werden. Diese sind in Abstimmung mit dem Betroffenen zu ermitteln.

Die bereinigten Systeme sind jedoch vor allem zu Beginn gesondert zu betrachten bzw. zu beobachten. Aufgrund der heutigen Komplexität der Angriffsmethoden, sollte keineswegs mit Sicherheit davon ausgegangen werden, dass eine durchgeführte Bereinigung jegliche Schadprogramme entfernen konnte. Sollte der Vorfall-Praktiker oder Vorfall-Experte bei der Wiederherstellung aller Systeme an seine fachlichen und zeitlichen Grenzen stoßen, so sollte er die Vorfall-Bearbeitung an einen registrierten IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten abgeben.

6 Behandlung von speziellen IT-Sicherheitsvorfällen (VP&VE)

6.1 Phishing

6.1.1 Einführung

Beim Phishing versucht ein Angreifender über gefälschte Webseiten oder gefälschte Nachrichten ein oder mehrere Opfer dazu zu bringen, vertrauliche Informationen herauszugeben oder unbewusst schädliche Aktionen durchzuführen. Dabei gibt sich der Angreifende für eine andere Person oder Institution aus und versucht das Vertrauen des Opfers zu erlangen.

6.1.2 Intention und Lernziele

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

Zu erkennen, ob es sich bei dem Problem eines Anrufenden um einen Phishing-Angriff handelt.

Die Folgen eines Phishing-Angriffs zu identifizieren und diese einzudämmen.

Betroffenen präventive Maßnahmen zu vermitteln, wie derartige Angriffe in Zukunft verhindert werden können.

6.1.3 Arten von Phishing

Neben dem herkömmlichen Phishing, bei denen die gleiche Nachricht an viele Empfängerinnen und Empfänger verschickt wird, existieren spezielle Phishing-Varianten. Weitere Informationen zu Maßnahmen und Abwehr von Phishing und Spam werden von der ACS veröffentlicht. Weitere Informationen finden Sie unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_098.pdf?__blob=publicationFile&v=1

6.1.3.1 Spear-Phishing

Eine besondere Form des Phishings ist das Spear-Phishing. Dabei handelt es sich um eine gezielte Phishing-Kampagne gegen eine bestimmte Zielgruppe, beispielsweise Mitarbeitende eines bestimmten Unternehmens, Personen mit gleicher politischer Einstellung, häufige Besucherinnen und Besucher einer Webseite oder eine einzelne Person. Der Angriff ist für den Angreifenden aufwändiger, da zunächst die Mitglieder der Zielgruppe und deren Kontaktdaten ermittelt werden müssen. Je mehr Zeit der Angreifende in die Recherche über die Zielgruppe investiert, desto mehr Informationen erhält dieser und kann eine immer glaubwürdigere Nachricht verfassen. Bei einem Unternehmen wäre dies beispielsweise der allgemeine Schreibstil, die passende Absenderin oder der passende Absender für das Szenario oder das Format der E-Mail-Signatur.

Wurden diese Schritte vom Angreifenden tatsächlich erledigt, bieten Spear-Phishing-Angriffe im Gegenzug eine erhöhte Erfolgschance. Die Ursache dafür ist zum einen, dass die E-Mail in jedem Fall zum Empfangenden passt. Es tritt beispielsweise nicht der Fall ein, dass eine Person eine Phishing-Nachricht erhält, deren vermeintliche Absenderin oder vermeintlicher Absender eine Bank ist, bei der die Person gar kein Kunde ist und den Betrug somit sofort bemerkt. Zum anderen erscheint die E-Mail vertrauenswürdiger, weil auf aktuelle Ereignisse oder bekannte Prozesse oder Namen verwiesen wird.

6.1.3.2 Whaling

Hochrangige Mitarbeitende eines Unternehmens bieten ein besonders attraktives Ziel für Spear-Phishing. Sollte es einem Angreifenden gelingen, die Zugangsdaten eines solchen Mitarbeitenden zu erhalten, so kann er im Namen dieser Person leicht weitere schadhafte Schritte im Unternehmen veranlassen. Stellt sich während des Gesprächs zwischen Vorfall-Praktiker und Betroffenem heraus, dass ein Konto der Geschäftsführerin oder des Geschäftsführers o.ä. Phishing zum Opfer gefallen ist, sollte der Angriff besonders sorgfältig untersucht werden.

6.1.3.3 Emotet / Dynamite Phishing

Bei Emotet handelt es sich um ein professionelles Schadprogramm, welches automatisch die E-Mail-Postfächer infizierter Systeme ausliest, um mit den gewonnenen Informationen weitere Systeme anzugreifen. Die Opfer erhalten dann eine E-Mail, in welcher Bezug auf eine nur wenige Tage alte Mail genommen wird und diese auch an das Ende der betrügerischen Mail angehängt wurde. Dadurch entsteht bei den neuen Opfern ein hohes Maß an Vertrauen, wodurch die Wahrscheinlichkeit hoch ist weitere Systeme zu übernehmen und den Angriff bei deren Kontakten fortzuführen. Aufgrund der extremen Anzahl automatisch generierter Phishing-Mails bei gleichzeitig sehr hoher Erfolgswahrscheinlichkeit des Angriffs wird in diesem Fall auch von *Dynamite Phishing* gesprochen.

Weitere Informationen zu Emotet finden sich unter https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Malware/Emotet/emotet_node.html

6.1.4 Abgrenzung / Einordnung zu verwandten Themen

Phishing ist stets nur ein Schritt in einer Kette von Angriffen, Datendiebstahl und Betrugsfällen. Die durch einen Phishing-Angriff erlangten Informationen können weitere Phishing-Angriffe oder den Einsatz von Verschlüsselungstrojanern ermöglichen.

6.1.4.1 Social Engineering

Beim Social Engineering versucht ein Angreifender ein Opfer zu täuschen und zu verunsichern, damit diese geheimen Informationen preisgibt oder bestimmte Aktionen ausführt. Phishing ist demnach eine Form des Social Engineerings. Social Engineering Angriffe können jedoch zusätzlich persönlich erfolgen, indem ein Angreifender beispielsweise als Handwerkerin oder Handwerker verkleidet, unter Vorwand, um Zugang zu nichtöffentlichen Bereichen eines Gebäudes bittet.

6.1.4.2 Gefälschte Online-Shops

Bei einem gefälschten Online-Shop handelt es sich um eine Webseite, welche vorgibt Produkte zum Kauf anzubieten. Um eine möglichst hohe Besucherzahl zu erreichen, werden besondere Interessen berücksichtigt, die für viele online Einkäuferinnen und Einkäufer ausschlaggebend sind. Ein relevanter Faktor kann beispielsweise der Preis von Produkten sein. Nach der Kaufabwicklung und dem Zahlungseingang erfolgt jedoch kein Versand der Ware an die Käuferin oder dem Käufer. Ein Angreifender kann auch die Webseite eines bekannten Händlers nachbauen und versuchen vorherige Kundinnen und Kunden, die dort in voller Zufriedenheit eingekauft haben, auf die gefälschte Webseite zu locken. Dies kann beispielsweise über eine Phishing-Nachricht erfolgen, die der Angreifende im Namen des vermeintlichen Händlers an die Kundinnen und Kunden sendet, und auf besondere Aktionen oder Rabatte hinweist.

6.1.5 Phishing-Kanäle

Auch wenn Phishing standardgemäß in Form von gefälschten E-Mails auftritt so kann grundsätzlich jeder Kommunikationsweg für Phishing-Angriffe genutzt werden.

6.1.5.1 E-Mail

Durch die weite Verbreitung und kostenlose Nutzung von E-Mails eignen sich diese Kommunikationsdienste besonders gut für Phishing-Angriffe. Der Verfassende der E-Mail kann hier den Absendenden selbstständig wählen, sodass es Angreifenden möglich ist auch im Namen anderer Nutzenden eine E-Mail zu versenden. Zudem ist es möglich beim eigentlichen Inhalt der Nachricht HTML-Code zu verwenden. Dadurch kann bei einem Phishing-Angriff das Logo der vermeintlichen Absenderfirma oder gar deren gesamtes Corporate Design nachgebaut werden, um Nachrichten noch authentischer zu gestalten. Es ergibt sich eine Austauschbeziehung für den Angreifenden zwischen Qualität des nachgeahmten Designs und der dafür investierten Zeit.

6.1.5.2 Anrufe

Potenzielle Opfer können von Angreifenden telefonisch kontaktiert werden, um sie auf gefälschte Webseiten zu leiten und dort ihre Zugangsdaten eingeben zu lassen.

6.1.5.3 SMS und Messenger-Anwendung

Der SMS-Dienst findet bei ehrlichen Unternehmen häufig Anwendung für kurze Mitteilungen an ihre Kundinnen und Kunden, beispielsweise zur Zusendung von Bestätigungscodes oder Neuigkeiten zu Bestellungen und Lieferung. Eine Einbettung von HTML ist nicht möglich, kann und muss von einem Angreifenden somit nicht beachtet werden. Außerdem entfällt aufgrund der kurzen Nachrichtenlänge auch bei ehrlichen Nachrichten oft die Begrüßung und persönliche Anrede der Kundin oder des Kunden. Somit unterscheidet sich eine kurze, unpersönliche Phishing-Nachricht eines Angreifenden optisch nur wenig von einer kurzen, unpersönlichen Nachricht einer ehrlichen Senderin oder eines ehrlichen Senders. Das Fälschen der Absenderrufnummer stellt hierbei jedoch eine größere Schwierigkeit als das Fälschen der Absenderin oder des Absenders einer E-Mail dar. Gleichzeitig erweckt eine zufällige Rufnummer auch nicht viel Misstrauen beim Empfangenden.

6.1.5.4 Social-Media-Kanäle

Profile in Social-Media-Kanälen können in der Regel mit beliebigen Daten angelegt werden, ohne dass diese auf Korrektheit überprüft werden. Dies erlaubt es einem Angreifenden fremde Profile oft mühelos zu imitieren, indem deren Namen, Profilbild und weitere Informationen kopiert und gegebenenfalls nur leicht verändert werden. Kontaktiert der Angreifende andere Nutzerinnen und Nutzer in einem sozialen Netzwerk, können diese in einem Moment der Unachtsamkeit nur auf das Profilbild sowie den Anzeigenamen achten, und den Angreifenden für die tatsächliche Person halten.

6.1.5.5 Typosquatting

Beim Typosquatting versucht ein Angreifender eine Webseiten-Domain zu registrieren, die einer existierenden Webseite sehr ähnlich ist, sich aber durch einen kleinen Tippfehler (beispielsweise einen Buchstabendreher) unterscheidet. Anschließend wird die eigentliche Webseite und deren Anmeldeformular kopiert und der Angreifende wartet, bis sich eine Nutzerin oder ein Nutzer beim Seitenaufruf zufällig auf die richtige Weise vertippt und somit auf der Webseite des Angreifenden landet. Typosquatting-Angriffe sind ungezielt, da zunächst nicht vorausgesagt werden kann, welche Person sich wann vertippen wird. Tritt dieser Fall ein, ist die Erfolgschance jedoch hoch, da die Benutzerin oder der Benutzer keine ungewöhnliche E-Mail o.ä. erhalten hat, die sie oder ihn stutzig werden lassen könnte.

6.1.6 Erkennung von Phishing-Angriffen

Die folgenden Hinweise sollen helfen Phishing-Angriffe zu erkennen. Idealerweise verfügen die Betroffenen selbst über dieses Wissen und Können Angriffe rechtzeitig erkennen und verhindern. Ist dies jedoch nicht möglich, so muss der Vorfall-Praktiker an ihrer Stelle entscheiden, ob es sich um einen Phishing-Angriff, einen anderen Angriff oder nur um eine harmlose Nachricht handelt.

6.1.6.1 Gefälschte Absenderin oder Absender

Noch vor dem Öffnen einer E-Mail kann die Adresse der Absenderin oder des Absenders betrachtet werden. Ist diese nicht Teil der Domain, die mit der eigentlichen Domain des Dienstes übereinstimmt, besteht ein starker Verdacht, dass die E-Mail gefälscht wurde. Neben offensichtlich anderer Adressen greifen Angreifende oftmals auf nur leicht veränderte Domains zurück, in der Hoffnung das Opfer bemerke den Unterschied nicht. Mögliche Variationen, für eine exemplarische Domain *beispiel.de*, sind:

- Fehler in der Second Level Domain, z.B. Buchstabendreher oder -dopplungen wie *beispiell.de*.
- Zusätzliche Präfixe oder Suffixe in der Second Level Domain, etwa *beispiel-online.de* oder *beispiel-kundenservice.de*
- Veränderte Top Level Domain, etwa *beispiel.do* oder *beispiel.biz*

Firmen können die am häufigsten verwendeten Top Level Domains als Alias für ihren Dienst registrieren, sodass sie nicht von einem Angreifenden missbraucht werden können, haben aufgrund der hohen Anzahl an Kombinationen jedoch keine Möglichkeit alle ähnlich aussehenden Domains zu registrieren.

Auf die gleichen Variationen müssen auch die in der Nachricht enthaltenen Links überprüft werden, wenn ermittelt werden soll, ob ein Link zu einer Phishing-Seite führt.

Besonders schwierig zu erkennen sind internationalisierte Domainnamen, bei denen einzelne Buchstaben durch ein ähnlich aussehendes Sonderzeichen ersetzt werden. Beispielsweise ist die Ersetzung eines lateinischen *a* bei der Darstellung nicht von einem kyrillischen *a* unterscheidbar, führt bei einem Link jedoch zu einer völlig anderen Webseite. Um derartige Angriffe zu erkennen, kann der Vorfall-Praktiker beispielsweise mithilfe eines kurzen Python-Befehls die echte Adresse und die Adresse aus einer potenziellen Phishing-Nachricht auf Gleichheit überprüfen.

Auf der anderen Seite können aber auch kryptisch aussehende Links und Adressen von ehrlichen Absenderinnen oder Absendern stammen. So ist beispielsweise info++aazq2oycpzluti@support.beispiel.de ein gültiger Absendende der Domain beispiel.de und sollte nicht zu Misstrauen in die entsprechende Mail führen. Außerdem sollte bedacht werden, dass einige Dienste andere Dienste in Anspruch nehmen, um E-Mails zu versenden. Dies kann dazu führen, dass auch bei einer authentischen Mail die Domain des Absendenden nicht zur Domain des eigentlichen Dienstes passt. Der gleiche Effekt kann bei Mutter- und Tochtergesellschaften auftreten, wenn sie sich eine gemeinsame Infrastruktur teilen.

6.1.6.2 Persönliche Anrede

Während (automatisch versandte) E-Mails ehrlicher Unternehmen der Empfängerin oder den Empfänger oft persönlich ansprechen ("Sehr geehrte Erika Mustermann", "Guten Tag Herr Muster") beginnen Phishing-Nachrichten an Kundinnen und Kunden oftmals mit einer generischen Begrüßung ("Sehr geehrter Kunde", "Sehr geehrte Damen und Herren"). Dies hat zweierlei Gründe: zum einen ist es technisch für den Angreifenden einfacher, die gleiche E-Mail mit dem exakt gleichen Inhalt massenhaft an mehrere potenzielle Opfer zu senden, ohne jedes Mal die Anrede ersetzen zu müssen, zum anderen liegen einem Angreifenden diese Informationen (Name, Geschlecht) oftmals gar nicht vor. Das Fehlen einer persönlichen Anrede ist jedoch keine Garantie, dass es sich um einen Phishing-Angriff handelt, der Absendende kann ebenso den einfacheren Weg einer Massenmail gehen. Gleichzeitig garantiert eine persönliche Anrede nicht die Echtheit der E-Mail, da es plausibel ist, dass der Angreifende auch eine Liste von Namen zu der Liste an E-Mail-Adressen erhalten hat. Die Überprüfung der Anrede kann jedoch in einem Augenblick einen ersten Eindruck über die Echtheit einer Nachricht geben, und sollte somit immer als eines der ersten Merkmale betrachtet werden, solange dadurch kein falsches Vertrauen entsteht.

6.1.6.3 Verunsicherung des Opfers

Da die meisten Phishing-Angriffe im Nachhinein bzw. bei genauem Hinsehen offensichtlich erscheinen versuchen Angreifende dem Opfer keine Zeit zum genauen Nachdenken zu lassen. So wird in Phishing-Nachrichten dem Opfer häufig mit Zeitnot gedroht. Beispiele hierfür sind vermeintliche Gewinnspiele, bei denen

nur die ersten 100 Interessenten Anspruch auf einen Gewinn haben, oder Nachrichten vermeintlicher Banken, die einer Kundin oder einen Kunden über die Sperrung seines Bankkontos informieren, sollte nicht umgehend eine Transaktion bestätigen werden. Durch derartige Versuche handeln die Opfer dann unüberlegt und geben vertrauliche Informationen frei. Daher sollten Vorfall-Praktiker die entsprechende Phishing-Nachricht sorgfältig lesen und auf derartige Formulierungen achten. Auch hierbei ist das Vorhandensein oder Fehlen solcher Formulierungen kein Beweis für Phishing oder Echtheit, kann aber einen zusätzlichen Eindruck in die richtige Richtung vermitteln.

6.1.6.4 Aufruf zu ungewöhnlichen Aktionen

Damit ein Opfer Zugangsdaten auf einer gefälschten Seite eingeben kann, muss ein Angreifender das Opfer zunächst unter Vorwand auf diese Seite locken. Als Begründung wird dabei beispielsweise die Sperrung eines Benutzerkontos oder Probleme bei der Zustellung eines Pakets genannt. Der Vorfall-Praktiker sollte daher selbstständig aus dem Inhalt der Nachricht ermitteln, ob das Opfer zu ungewöhnlichen Aktivitäten aufgerufen wurde. Ist dies aus dem Text nicht ersichtlich, so ist im Dialog mit dem Opfer herausfinden, ob derartige Nachrichten schon früher einmal empfangen wurden, und diese zwar ungewöhnlich, aber dennoch authentisch waren. Nicht jede ungewöhnliche E-Mail ist direkt ein Zeichen für einen Phishing-Angriff. Ist dies jedoch der Fall sollten die anderen Punkte besonders gründlich geprüft werden.

6.1.6.5 Sprachliche Ungenauigkeiten

Da hinter Phishing-Angriffen oftmals ausländische Akteure stehen weisen gefälschte Nachrichten oftmals schwerwiegende Grammatik- und Rechtschreibfehler auf. Bei deutschen Texten sind es insbesondere die Sonderzeichen, die vom Angreifenden nicht korrekt geschrieben werden. Statt Umlaute, wie ä, ö und ü, werden oftmals die Buchstaben a, o und u verwendet, während das Eszett durch ein doppeltes s oder Fragezeichen ersetzt wird. Falsch geschriebene Nachrichten sind ein klares Zeichen für Phishing-Nachrichten, da ehrliche Unternehmen viel Wert auf eine korrekte und professionelle Außenkommunikation legen. Aus diesem Grund sollten derartige Nachrichten stets ein starkes Indiz für den Vorfall-Praktiker für eine Phishing-Nachricht sein, während eine korrekt formulierte Nachricht nicht direkt als Entwarnung gesehen werden kann.

6.1.6.6 Analyse von E-Mail-Headern

Da Phishing-Nachrichten oftmals von ausländischen Angreifenden versandt werden, deutsche Unternehmen ihre Server jedoch meist in Deutschland betreiben, kann ein Blick in die E-Mail-Header einen starken Hinweis auf die Authentizität einer E-Mail liefern.

```
Received: from msx-01.[redacted].de (141.[redacted]) by msx-01.[redacted].de
 (141.[redacted]) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1733.5 via Mailbox
 Transport; Tue, 18 Jun 2019 16:32:23 +0200
Received: from msx-02.[redacted].de (141.[redacted]) by msx-01.[redacted].de
 (141.[redacted]) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1733.5; Tue, 18
 Jun 2019 16:32:23 +0200
Received: from msx-e-01.[redacted].de (141.[redacted]) by msx-02.[redacted].de
 (141.[redacted]) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1733.5 via
 Frontend Transport; Tue, 18 Jun 2019 16:32:23 +0200
Received: from mail.ip.[redacted].ru (77.[redacted]) by msx-e-01.[redacted].de
 (141.[redacted]) with Microsoft SMTP Server id 15.1.1733.5; Tue, 18 Jun 2019
 16:32:22 +0200
Received: from [189.[redacted]] (account [redacted] HELO [127.0.0.1])
  by mail.ip.[redacted].ru (CommuniGate Pro SMTP 5.2.12)
  with ESMTPSA id 257316585 for [redacted].de; Tue, 18 Jun 2019 19:23:57 +0400
```

Abbildung 4: Auszug aus einem E-Mail-Header

Abbildung 4 zeigt einen Auszug aus einem E-Mail-Header. In der vorletzten Zeile ist klar zu erkennen, dass die Mail über einen ausländischen Mailserver (TLD .ru) versandt wurde. Je nach Kontext ist dies ein deutliches Zeichen für einen Phishing-Angriff. Erhält eine Person mit einer E-Mail-Adresse bei einem deutschen Anbieter eine E-Mail von einem vermeintlich deutschen Unternehmen, so kann davon ausgegangen werden, dass alle beteiligten Mailserver in Deutschland stehen, und die Nachricht nicht über ausländische Server versandt wird. Ist der Domain Name der beteiligten Mailserver nicht eindeutig einem Land zuzuordnen (z.B. .com) so kann mithilfe einer Geolocation Software versucht werden, den Standort und somit das Land der IP-Adresse des Mailservers zu ermitteln. Der Vorfall-Praktiker benötigt hierfür unbedingt die originale E-Mail der betroffenen Person. Leitet die betroffene Person die E-Mail an den Vorfall-Praktiker weiter, so führt dies zu einem neuen E-Mail-Header, mit einem Nachrichtenverlauf zwischen dem Mailserver der betroffenen Person und des Vorfall-Praktikers, bzw. Vorfall-Experten. Um dies zu verhindern, kann die betroffene Person jedoch die E-Mail als Datei abspeichern und dann als Anhang in einer E-Mail oder über eine Upload-Möglichkeit dem Vorfall-Praktiker zur Verfügung stellen, ohne dass der E-Mail-Header verloren geht.

In Microsoft Outlook 2016 kann der Header einer geöffneten E-Mail über die Schaltfläche *Datei → Eigenschaften* eingesehen werden, bei Mozilla Thunderbird v91 über die Schaltfläche *Mehr → Quelltext anzeigen*.

6.1.7 Reaktion auf erfolgreiche Phishing-Attacken

Hat der Vorfall-Praktiker klare Anzeichen für eine Phishing-Attacke gefunden, sollten umgehend die folgenden Maßnahmen umgesetzt werden, um den entstehenden Schaden zu minimieren.

6.1.7.1 Sperren von Benutzerkonten

Wurde ein Benutzerkonto von einem Angreifenden übernommen, hat dieser in der Regel die Möglichkeit im Namen des Opfers Aktivitäten durchzuführen, beispielsweise eine Bestellung bei einem Online-Shop durchzuführen, Nachrichten an andere Personen zu schreiben oder Transaktionen zu veranlassen. Um den Missbrauch so schnell wie möglich zu unterbinden, sollte das Konto daher so schnell wie möglich wieder unter Kontrolle gebracht werden. Sollte der Angreifende das Kennwort des Benutzerkontos nicht geändert haben, kann sich die Benutzerin oder der Benutzer weiterhin anmelden und das Kennwort selbstständig ändern, um den Angreifenden wieder auszusperren. Dabei muss beachtet werden, dass auch alle aktiven Sitzungen beendet werden, da der Angreifende ansonsten über eine bereits bestehende Sitzung weiterhin Zugriff auf den Dienst hat. Hat der Angreifende das Kennwort nach der Übernahme geändert, sollte nicht versucht werden, das Kennwort zu erraten oder mehrere Kennwörter durchprobiert werden. Stattdessen steht bei den meisten Diensten eine "Passwort vergessen?"-Funktion bereit, über die das Kennwort zurückgesetzt und der Zugang wiederhergestellt werden kann. In beiden Fällen ist es essentiell, dass das neue Kennwort nicht dem vorherigen Kennwort entspricht, auch nicht, wenn es leicht variiert wird (beispielsweise durch Anhängen einer Zahlenkombination). Ist eine direkte Wiederherstellung des Benutzerkontos nicht möglich, so sollte zumindest versucht werden, das Konto zu sperren, damit weder der betroffenen Person noch der Angreifende unmittelbar Aktivitäten durchführen kann. Ist das Benutzerkonto erst gesperrt, kann in Ruhe mit dessen Wiederherstellung begonnen werden.

6.1.7.2 Kontaktaufnahme zum Plattform-Betreibenden

Nach der Sperrung des betroffenen Kontos oder um eben diese Sperrung zu erreichen, sollte der Betreibende des entsprechenden Dienstes über den Vorfall alarmiert werden. In der Regel sind diese über ein entsprechendes Formular, eine E-Mail-Adresse, einen Live-Chat oder eine Hotline erreichbar. Die Mitarbeitenden des Dienstes können einen Account dann entweder direkt sperren oder zumindest das weitere Vorgehen erklären. Zudem kann der Betreibende der Plattform besser abschätzen, wie sich die Anzahl der Phishing-Angriffe auf seiner Plattform entwickelt und so andere Benutzerinnen und Benutzer warnen.

6.1.7.3 Ändern der betroffenen Zugangsdaten auf allen Webseiten

Hat ein Angreifender Kenntnis über ein Kennwort erlangt, kann dieses nicht mehr als sicher betrachtet werden. Nachdem das Kennwort beim betroffenen Dienst geändert wurde, ist es nun auch unabdingbar, dieses Kennwort bei allen anderen Diensten zu ändern, bei denen das gleiche Kennwort verwendet wurde. Hierbei sollte für jeden Dienst ein einzigartiges Kennwort gewählt werden und die Passwortänderungen zuerst bei den kritischsten Diensten durchgeführt werden. Alle Benutzerkonten, die das gleiche Kennwort gesetzt hatten, sollten wie im nächsten Punkt beschrieben auf eine Beobachtungsliste gesetzt werden.

6.1.7.4 Achten auf ungewöhnliche Aktivitäten bei den betroffenen Benutzerkonten

Nach einem vermuteten oder erfolgreichen Phishing-Angriff sollten das betroffene Benutzerkonto sowie weitere, mit diesem Konto verbundene Benutzerkonten für mehrere Wochen genau im Auge behalten werden. Dadurch wird sichergestellt, dass der Angreifende durch die oben genannten Maßnahmen tatsächlich ausgesperrt wurde und keine weiteren Benutzerkonten übernehmen konnte.

6.1.7.5 Datenschutzbeauftragten alarmieren

Je nach Art des betroffenen Benutzerkontos (z.B. E-Mail-Postfach) erlangt der Angreifende eine Vielzahl an personenbezogener Daten, die für weitere Attacken missbraucht werden können. Handelt es sich beim Opfer um ein Unternehmen, das über einen Datenschutzbeauftragten verfügt, sollte dieser umgehend prüfen, ob es sich bei dem Angriff um einen meldepflichtigen Vorfall handelt. Ist dies der Fall so beträgt die Meldefrist an die zuständige Aufsichtsbehörde 72 Stunden. Zusätzlich kann der Vorfall freiwillig bei zentralen Stellen[16] gemeldet werden. Der Vorfall- Praktiker muss nicht entscheiden, ob ein Vorfall meldepflichtig ist, sollte der betroffenen Person jedoch auf die Thematik aufmerksam machen.

6.1.7.6 Anzeige bei der Strafverfolgungsbehörde erstatten

Nachdem die unmittelbaren Maßnahmen umgesetzt wurden ist es ratsam, den Vorfall bei einer Strafverfolgungsbehörde zu melden und eine Anzeige zu erstatten. Dies ermöglicht die Erstellung eines Lagebildes um weitere, potenzielle Opfer rechtzeitig vor dem Angriff zu schützen und gewährt gegebenenfalls ein Anrecht auf Schadensersatz, wenn die Täterin oder der Täter gefasst wird.

6.1.8 Schutz gegen Phishing

Die folgenden Maßnahmen können Nutzerinnen und Nutzer vor erfolgreichen Phishing-Angriffen schützen. Sobald sich ein Betroffener an das Cyber-Sicherheitsnetzwerk wendet, ist der Angriff voraussichtlich jedoch bereits erfolgt und die Maßnahmen können keinen weiteren Schaden verhindern. Sie können jedoch die Frage des Betroffenen beantworten, wie solche Angriffe in der Zukunft verhindert werden können.

6.1.8.1 E-Mail-Signaturen

Eine der effektivsten Maßnahmen gegen Phishing ist die Verwendung von kryptographischen E-Mail-Signaturen. Diese dürfen nicht mit den Signaturen am Ende einer E-Mail verwechselt werden, die lediglich Kontaktdaten des Verfassers enthalten.

Vorteile

Digitale Signaturen basieren auf der asymmetrischen Kryptographie. Dabei wird bei jeder verschickten E-Mail in Abhängigkeit der Nachricht mithilfe eines geheimen Schlüssels ein zweiter Teil, die digitale Signatur, mitgeschickt. Die Empfängerin oder der Empfänger kann mit Kenntnis des öffentlichen Schlüssels der Senderin oder des Senders die Signatur auf Gültigkeit überprüfen. Das Verfahren ist so konstruiert, dass ohne Kenntnis des geheimen Schlüssels keine gültige Signatur zu einer Nachricht erzeugt werden kann, und das Manipulieren einer signierten Nachricht die Signatur invalidiert.

[16] z. B. bei der ACS - Allianz für Cyber-Sicherheit

Somit kann sich die Empfängerin oder der Empfänger einer Nachricht sicher sein, dass diese auch garantiert von der angegebenen Absenderin oder dem angegebenen Absender stammt. Die Standards und Programme zur Verschlüsselung von E-Mails S/MIME und PGP sind kostengünstig bzw. kostenlos verfügbar.

Schwierigkeiten

Problematisch bei kryptographischen Signaturen ist, dass das Verfahren die Senderin oder dem Sender und Empfängerin oder Empfänger bekannt sein muss, und die Senderin oder der Sender zunächst die notwendigen Konfigurationen vorgenommen hat. Durch die schwache Verbreitung von Signaturen fällt der Empfängerin oder dem Empfänger häufig die Verwendung, nicht aber das Fehlen einer Signatur, auf. Somit können zwei Geschäftspartnerinnen und Geschäftspartner regelmäßig anhand signierter Nachrichten kommunizieren, empfängt einer der beiden jedoch von einem Angreifenden eine unsignierte Phishing-Mail muss dieser die fehlende Signatur bewusst wahrnehmen, um den Betrug zu erkennen. Zudem schützt eine Signatur nicht vor Angreifenden, welche die Infrastruktur der Senderin oder des Senders korrumpiert haben, und über dessen Mailserver authentische, signierte Phishing-Mails versenden. In diesem Fall kann eine vorhandene digitale Signatur bei Empfängerin oder beim Empfänger ein falsches Gefühl von Sicherheit hervorrufen.

6.1.8.2 Webseiten selbstständig aufrufen, anstatt auf Links zu klicken

Erhält eine Person eine E-Mail, in der sie aufgefordert wird, eine gewisse Aktion zu bestätigen, ist es ratsam nicht auf den in der Nachricht zur Verfügung gestellten Link zu klicken, sondern stattdessen die Webseite des Dienstes selbstständig im Browser aufzurufen. In der Regel kann die ausstehende Aktion dann direkt über die Webseite bestätigt werden, oder es findet sich zumindest ein Hinweis darauf, dass die E-Mail vertrauenswürdig ist. Dies stellt einen kleinen Mehraufwand für die Person da, garantiert jedoch, dass die originale Webseite des Dienstes aufgerufen wird, und Zugangsdaten nicht auf einer Phishing-Seite eingegeben werden.

6.1.8.3 Nachfragen bei vermeintlicher Absenderin oder beim vermeintlichen Absender über zweiten (sicheren) Kanal

Empfängt eine Person eine Nachricht mit zweifelhafter Authentizität so kann sie auf Nummer sichergehen und die Absenderin oder den Absender über einen vertrauenswürdigen Kanal, z.B. Telefon, kontaktieren. Dabei sollten jedoch nicht die in der Nachricht angegebenen Kontaktdaten verwendet werden, sondern Telefonnummern der vermeintlichen Absenderin oder des vermeintlichen Absenders aus dem Adressbuch gewählt oder im Internet recherchiert werden.

6.1.8.4 Grundsätzliches Misstrauen bei Nachrichten mit Anhängen oder Links

Die meiste Gefahr bei Phishing-Nachrichten geht von deren Anhängen oder Links zu weiterführenden Webseiten aus. Daher sollte sich die Empfängerin oder der Empfänger bei Empfang einer Nachricht zunächst die folgenden Gedanken machen, bevor er auf eine Link klickt oder den Anhang öffnet.

- Erwarte ich eine Nachricht mit Anhang / Links?
- Ist für den Inhalt dieser Nachricht ein Anhang / Link notwendig bzw. plausibel?
- Welche Dateiendung hat die Datei im Anhang?
- Auf welche Seite führt der angegebene Link?

Bestehen hierbei Zweifel kann versucht werden, den Anhang zunächst auf eine Art und Weise zu öffnen, bei der kein Schadprogramm ausgeführt wird, beispielsweise durch das Öffnen der Datei mit dem Microsoft Editor.

6.1.8.5 2-Faktor-Authentifizierung

Eine Großzahl an Diensten unterstützt den Einsatz eines zweiten Faktors, als Zusatz neben einem geheimen Kennwort. Dadurch muss beispielsweise bei einer Online-Überweisung mithilfe eines TAN-Generators eine

einmalige Transaktionsnummer generiert werden, welche dann ebenfalls auf der Webseite eingegeben werden muss. Andere Dienste verlangen beim ersten Login auf einem neuen Gerät die Eingabe eines Zahlencodes, der zuvor per SMS an die Besitzerin oder den Besitzer des Benutzerkontos geschickt wurde. Dadurch ist es einem Angreifenden nicht möglich gewisse Aktionen durchzuführen, da er nur die r die Zugangsdaten zu einem bestimmten Benutzerkonto kennt, aber nicht im Besitz des zweiten Faktors ist. Neben diesen Möglichkeiten, besteht auch die weitere Möglichkeit der Identitätsverifizierung durch ein biometrisches Merkmal der Benutzerin oder des Benutzers. Dabei wählt die Benutzerin oder der Benutzer auf einem zweiten registrierten und für die Registrierung vorgesehenen Gerät die Methode der biometrischen Identitätsbestätigung aus. Damit kann beispielsweise mittels der Gesichtserkennung oder dem Fingerabdruck-Scan die eigene Identität verifiziert werden. Diese Methode ist vor allem dadurch effizient, da es für den Angreifenden fast unmöglich ist, in den Besitz des biometrischen Schlüssels zur Authentifizierung zu kommen. Bei legitimen Alltagsgeschäften verursacht die 2-Faktor-Authentifizierung jedoch einen unnötigen Mehraufwand für legitime Benutzerinnen und Benutzer. Außerdem kann der Angreifende unter Umständen auf der gefälschten Webseite zeitgleich nach dem Bestätigungscode des zweiten Faktors fragen und diesen an den eigentlichen Dienst weiterleiten, um sich zu authentisieren.

6.2 Ransomware

6.2.1 Einführung

Als Ransomware, auch Verschlüsselungstrojaner, werden Schadprogramme bezeichnet, welche Dateien auf betroffenen Systemen verschlüsselt und somit für die Besitzerin oder den Besitzer unbrauchbar macht. Angreifende, die einen Ransomware-Angriff praktizieren, fordern für die Entschlüsselung das Zahlen einer Lösegeldsumme von den betroffenen Personen oder Institutionen. Oftmals werden den Opfern eine Frist gesetzt, nach deren Ablauf die Lösegeldforderung steigt oder die Daten nicht mehr vom Angreifenden entschlüsselt werden.
Die Ransomware verschlüsselt in der Regel keine systemrelevanten Dateien, die ein Starten des Systems verhindern würden, sondern beschränkt sich auf gängige Dateiformate von Bildern, Dokumenten, Archiven und Datenbanken. Ein betroffenes Unternehmen kann somit nicht auf Kunden- oder Patientendaten, Rechnungen, Baupläne etc. zugreifen.
Im Gegensatz zu Spionagesoftware ist ein erfolgter Ransomware-Angriff für das Opfer schnell ersichtlich. Da die Angreifenden das Opfer zum Zahlen bewegen möchten, machen sie zusätzlich auf sich aufmerksam, indem sie an offensichtlichen Stellen Textdateien mit einem Hinweis auf den Angriff hinterlegen oder das Hintergrundbild des betroffenen Systems verändern. Als zusätzliches Druckmittel gegen das Opfer kopieren einige Angreifende die Daten vor der Verschlüsselung auf die eigenen Systeme und drohen dem Opfer mit der Veröffentlichung der Daten, sollte dieses nicht dazu bereit sein, das Lösegeld zu bezahlen. Eine derartige Veröffentlichung führt zu einem Datenschutzproblem mit den gestohlenen, meist personenbezogenen Daten, zu einem Reputationsschaden des Unternehmens und im Fall von Betriebsgeheimnissen zu einem Verlust des Wettbewerbsvorteils.

6.2.2 Intention und Lernziele

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer **in der Lage:**

Die Folgen eines Ransomware-Angriffs zu identifizieren und diesen einzudämmen.

Betroffenen Unterstützung bei der Wiederherstellung von verschlüsselten Daten anzubieten.

Betroffenen präventive Maßnahmen zu vermitteln, wie derartige Angriffe in Zukunft verhindert werden können.

6.2.3 Einfallstor

Ransomware kann über viele verschiedene Wege auf ein Zielsystem gelangen. Für eine vollständige Bearbeitung des IT-Sicherheitsvorfalls sollte das Einfallstor identifiziert und geschlossen werden, andernfalls kann der Angreifende das System kurze Zeit nach der Wiederherstellung der Daten erneut angreifen. Problematisch ist aber, dass regelmäßig zwischen Infektion eines Systems und Verschlüsselung der Daten Tage bis Wochen, teilweise sogar Monate liegen. Um den Ablauf nachzuvollziehen, muss daher auf Protokolldateien zurückgegriffen werden.

Häufige Infektionsvektoren sind:

- Spam-Mails mit Office-Dokumenten mit Makros
- Schwache Zugangsdaten für extern erreichbare Systeme
- Extern erreichbare Systeme mit Schwachstellen

6.2.4 Bewältigung des Vorfalls

Nach einem entdeckten Ransomware-Angriff muss zunächst die weitere Ausbreitung des Schadprogramms verhindert werden. Anschließend können die befallenen Systeme bereinigt und mit der Wiederherstellung der Daten begonnen werden.

6.2.4.1 Isolierung betroffener Systeme

Um eine Ausbreitung der Ransomware auf andere Systeme zu verhindern, sollte ein betroffenes System umgehend von den anderen Systemen isoliert werden, beispielsweise durch Ziehen des Netzwerkkabels. Sollte der Verschlüsselungsvorgang noch nicht abgeschlossen sein, kann durch ein schnelles Abschalten des Systems möglicherweise ein Teil der Daten verschont bleiben, es ist jedoch im Regelfall davon auszugehen, dass die Verschlüsselung zum Zeitpunkt der Kontaktaufnahme mit dem Vorfall- Praktiker bereits abgeschlossen wurde. Außerdem gehen beim Ausschalten des Systems alle flüchtigen Daten im Arbeitsspeicher verloren. Um dies zu verhindern, kann das System in den Ruhezustand (Hibernate) versetzt werden. Dabei werden alle Daten aus dem Arbeitsspeicher auf die Festplatte geschrieben und das System anschließend heruntergefahren. Dies erlaubt einer Forensikerin oder einem Forensiker später, die Festplatte zu untersuchen und möglicherweise den Schlüssel, der für die Verschlüsselung der Daten verwendet wurde, aus dem Arbeitsspeicher zu extrahieren (siehe dazu auch 4.5.1 ff. und 10.3.1.) . Um auszuschließen, dass sich das Schadprogramm bereits auf andere Systeme verbreitet hat, sollten auch Systeme genauer untersucht und im Auge behalten werden, die sich unauffällig verhalten. Sollte es unsicher sein, welche Systeme alle betroffen sind, sollten vorsorglich wichtige Systeme (z.B. Backupserver) auch vom Netz getrennt und ggf. vorsorglich heruntergefahren werden.

6.2.4.2 Bereinigung der Systeme

Die Wiederherstellung der Daten sollte nur auf, nicht infizierten Systemen erfolgen, damit die Daten nicht direkt wieder verschlüsselt werden.

Hierfür gibt es zwei Strategien: Entweder sollte versucht werden, infizierte Systeme zu bereinigen, oder die Systeme werden komplett neu aufgesetzt. Beim Bereinigen wird etwa mit Antivirenprogrammen versucht alle Rückstände des Schadprogramms zu entfernen. Hierbei kann jedoch kaum bestätigt werden, dass nicht doch Infektionen oder Hintertüren des Angreifenden zurückbleiben. Daher ist es nachhaltiger, jedoch auch aufwändiger, alle betroffenen Systeme von Grund auf neu zu installieren. Diese Entscheidung muss nicht vom Vorfall- Praktiker getroffen werden, sondern man sollte der Geschäftsführung des betroffenen Unternehmens beide Optionen darlegen, damit diese eine Entscheidungsgrundlage hat. In beiden Fällen sollten alle

auf dem System gespeicherten Kennwörter geändert werden, da diese eventuell im Klartext oder als Hash vom Angreifenden gestohlen wurden und in der Zukunft für einen weiteren Angriff missbraucht werden können.

Sollte der Verdacht bestehen, dass Angreifende Zugriff auf den Domain Controller hatten, ist im Idealfall auch dieser neu aufzusetzen. Sollte das nicht möglich sein ist nach der Bereinigung des Domain Controllers das Passwort des KRBTGT-Accounts zweimal zurückzusetzen.

6.2.4.3 Einspielung von Backups

Entdecken die Angreifenden Backup-Systeme in der Infrastruktur des Opfers, wird meist versucht diese ebenfalls zu verschlüsseln, um eine Wiederherstellung der Daten zu verhindern. Liegen jedoch funktionierende, nicht verschlüsselte Backups vor (beispielsweise, weil diese physisch getrennt gelagert wurden) können die verschlüsselten Daten ersetzt und somit wiederhergestellt werden. Dabei ist es essentiell, dass die Backups nicht leichtfertig an infizierte Systeme angeschlossen und somit nachträglich verschlüsselt werden. Um dies zu verhindern, kann der Vorfall- Praktiker an einem garantiert sicheren System zunächst ein Backup der Backups anlegen, und anschließend erst mit der Wiederherstellung der Daten beginnen.

6.2.4.4 Selbstständige Entschlüsselung der Daten

Existiert kein Backup besteht in Einzelfällen die Chance, dass die verschlüsselten Daten eventuell trotzdem entschlüsselt werden können. Dazu kann der Vorfall- Praktiker recherchieren, ob bereits ein kostenloses Entschlüsselungswerkzeug[17] zur Verfügung steht. Dabei muss verhindert werden, aus unseriösen Quellen weitere Schadprogrammeherunterzuladen, die nur vorgibt ein Entschlüsselungswerkzeug zu sein. Im Idealfall werden Entschlüsselungstests mit Kopien der verschlüsselten Daten durchgeführt.

Ist eine Entschlüsselung zum jetzigen Zeitpunkt nicht möglich, können die verschlüsselten Daten dennoch aufbewahrt werden, da mit jedem Tag die Wahrscheinlichkeit steigt, dass ein kostenloses Entschlüsselungswerkzeug veröffentlicht wird. Gleichzeitig verlieren die verschlüsselten Daten auch zunehmend an Wert, daher liegt die Entscheidung, ob die vorhandenen Festplatten aufgehoben oder formatiert und wiederverwendet werden sollen, bei der Geschäftsführung.

6.2.4.5 Analyse von Log-Dateien

Verfügt das Opfer über eine Firewall, die den ein- und ausgehenden Datenverkehr protokolliert, so kann der Vorfall- Praktiker in den Protokolldateien nachsehen, ob es in den Tagen und Wochen vor dem Angriff zu einem ungewöhnlichen hohen Datenverkehr nach Außen kam. Trifft dies zu, ist zu erwarten, dass die Angreifenden Daten aus dem Netzwerk der betroffenen Person oder Institution heruntergeladen hat, und diese möglicherweise veröffentlichen wird. In diesem Fall sollte unbedingt die Datenschutzbeauftragte oder der Datenschutzbeauftragte der betroffenen Person oder Institution, bzw. der zuständige Landesbeauftragte verständigt werden. Sind keine Auffälligkeiten zu beobachten, kann keine Aussage über gestohlene Daten gemacht werden, die Daten könnten auch schon über mehrere Tage vor dem Angriff hinweg in mehreren kleinen Teilen extrahiert worden sein.

6.2.4.6 Bezahlung des Lösegelds

Sollten keine Backups oder kein Entschlüsselungstool verfügbar sein, stellt sich der betroffenen Person oder Institution die Frage, ob Lösegeld als letzte Möglichkeit zur Wiederherstellung der Daten gezahlt werden sollte. Jedoch kann nicht sichergestellt werden, dass die Angreifenden nach Zahlungseingang den verwendeten Schlüssel oder ein entsprechendes Entschlüsselungsprogramm zur Verfügung stellen. Zu beachten ist dabei, dass teilweise die Daten trotz Bezahlung nicht entschlüsselt werden können. Teilweise ist es auch technisch nicht möglich, die Daten überhaupt zu entschlüsseln, da diese bspw. mit Nullen überschrieben wurden, anstatt sie sauber zu verschlüsseln. Eine derartige Vernichtung der Daten kann vom Vorfall-Praktiker mithilfe

[17] https://www.nomoreransom.org/

einer Entropie-Analyse mehrerer Dateien ermittelt werden. Ist die Entropie der untersuchten Dateien gering, ist es naheliegend, dass die Dateien vernichtet oder schlecht verschlüsselt wurden. Zudem sollten folgende Aspekte bedacht werden:

- Die Angreifenden können die Daten dennoch verkaufen oder veröffentlichen.
- Die Angreifenden markieren das Opfer als zahlungswillig, und fokussieren zukünftige Angriffe auf dieses Unternehmen.
- Durch das Lösegeld werden die Angriffe auf die nächsten Unternehmen finanziert.
- Die Systeme müssen dennoch bereinigt bzw. neu installiert werden

Aus diesen Gründen ist das Bezahlen des Lösegelds grundsätzlich nicht zu empfehlen, die Entscheidung liegt jedoch bei der Geschäftsführung. Auch sollte rechtlich geprüft werden, ob sich das Unternehmen durch die Zahlung nicht selbst strafbar macht (Compliance).

Sollte sich trotzdem zur Zahlung entschlossen werden, wird empfohlen die Polizei zu informieren. Diese kann ggf. weiter beraten, den Fluss des Geldes nachvollziehen oder bei der Verhandlung unterstützen.

6.2.5 Kommunikation

Neben der schnellen Wiederherstellung der Systeme spielt auch die interne und externe Kommunikation eine wichtige Rolle, um zusätzliche Hilfe zu erhalten und weitere Schäden zu vermeiden. Aufgabe des Vorfall-Praktiker kann es je nach Auftrag sein, der Geschäftsführung aufzuzeigen, welche Akteure existieren und potenziell über den Vorfall informiert werden sollten. Die eigentliche Kommunikation übernimmt jedoch die Kommunikationsabteilung des betroffenen Unternehmens oder die Geschäftsführung selbst.

6.2.5.1 Interne Mitarbeitende

Als erste Kommunikationsmaßname sollten die eigenen Mitarbeitenden über den Vorfall informiert werden. Hierbei ist auch an die Ehrlichkeit aller Mitarbeitenden zu appellieren, um den Sachverhalt schnell aufzuklären zu können. Damit niemand ein bereits wiederhergestelltes System an ein noch infiziertes System anschließt, sollten die Systeme entsprechend markiert werden, bspw. mit farbigen Klebezetteln, die angeben, ob ein System benutzt werden darf oder nicht.

6.2.5.2 Strafverfolgungsbehörden

Es wird bei Ransomware-Vorfällen generell empfohlen die Strafverfolgungsbehörden zu informieren und Strafanzeige zu erstatten. Durch eine Anzeige bei den Strafverfolgungsbehörden kann eine betroffene Person oder Institution zusätzliche Hilfe erhalten. Aufgrund gesetzlicher Regelungen hat die Polizei besondere Befugnisse die bei der Aufklärung des IT-Sicherheitsvorfalls von Nutzen sein können, die ein Vorfall- Praktiker selbst nicht besitzt, z.B. dem Geldfluss gezahlter Lösegelder zu folgen. Die Polizei kann ebenfalls dabei unterstützen, Beweise zu sichern und ein forensisches Image des betroffenen Systems anzufertigen, damit dieses später genauer analysiert werden kann. Werden die Angreifenden zu einem späteren Zeitpunkt gefasst, hat die betroffene Person oder Institution möglicherweise Anrecht auf Schadensersatz.

6.2.5.3 Versicherungen

Verfügt die betroffene Person oder Institution über eine Cyber-Versicherung, sollte diese ebenfalls zeitnah über den Vorfall alarmiert werden, da dort in der Regel zeitliche Meldefristen vertraglich geregelt sind. Eine zeitnahe Meldung stellt zunächst einen Mehraufwand für die betroffene Person oder Institution dar, jedoch kann er von der Cyber-Versicherung auch weitere Unterstützung oder Ratschläge zur Eindämmung des IT-Sicherheitsvorfalls erhalten. Um möglichst wenig Versicherungsleistung auskehren zu müssen, ist auch die Versicherung an einer schnellen Behebung des Vorfalls interessiert.

6.2.5.4 Geschäftspartnerinnen und Geschäftspartner

Da ein Ransomware-bedingter Betriebsausfall ohnehin schwer vor den Geschäftspartnerinnen und Geschäftspartnern geheim zu halten ist, sollte der IT-Sicherheitsvorfall von Beginn an transparent kommuniziert werden, darauf sollte der Vorfall-Praktiker oder Vorfall-Experte das Unternehmen hinweisen. Dadurch können Angriffe (z.B. anhand gefälschter E-Mails im Namen des betroffenen Unternehmens) auf dessen Geschäftspartnerinnen und Geschäftspartner eingedämmt werden, da diese jede verdächtige Mail besonders überprüfen können. Außerdem können einzelne Geschäftspartnerinnen und Geschäftspartner bei der Wiederherstellung verlorener Daten behilflich sein, z.B. anhand Auftragsbestätigungen, die in den Postfächern der jeweiligen Kundinnen und Kunden vorliegen. Liegen die E-Mail-Adressen aller Geschäftspartnerinnen und Geschäftspartnern vor und ist die Anzahl der Geschäftspartnerinnen und Geschäftspartner gering, können alle Geschäftspartnerinnen und Geschäftspartner mit einer Rundmail über den Vorfall informiert werden. Dabei muss der Versand unbedingt über das BCC Feld erfolgen, damit nicht alle Empfängerinnen und Empfänger die E-Mail-Adressen aller anderen erfahren. In der E-Mail ist es ausreichend, wenn von einem Hackerangriff gesprochen wird, ohne weitere Details zum eigentlichen Angriff nennen. Alternativ oder zusätzlich kann auch ein Warnhinweis auf der Webseite oder den Social-Media-Kanälen des Unternehmens platziert werden. Sind mehrere, gleiche Anfragen der Geschäftspartnerinnen und Geschäftspartner oder der Öffentlichkeit zu erwarten, können häufig gestellte Fragen (FAQ) vorbereitet werden, die kommuniziert werden. Eine entsprechende Frage könnte sein, ob eine Gefahr durch bestehende Fernwartungs- oder VPN-Zugänge besteht.

6.2.5.5 Angreifende

Vorsicht ist bei der Kommunikation mit dem Angreifenden geboten. Für eine entsprechende Kommunikationsstrategie können unter Umständen die Strafverfolgungsbehörden unterstützen. Wendet sich eine betroffene Person oder Institution an die Angreifenden signalisiert dies, dass dieser womöglich auf die Entschlüsselung der Daten durch den Angreifenden angewiesen ist. Hätte die betroffene Person oder Institution eine Sicherheitskopie der Daten, hätte diese sich gar nicht erst an den Angreifenden wenden müssen. Dadurch kann der Angreifende mehr Druck auf die betroffene Person oder Institution ausüben. Gleichzeitig bieten viele Angreifende an, eine Datei kostenlos zu entschlüsseln, um zu beweisen, dass sie die Daten entschlüsseln können. Sendet die betroffene Person oder Institution die wichtigste Datei an den Angreifenden, so kann dieser die Datei veröffentlichen oder missbrauchen. Hat der Angreifende bei seinem Angriff bereits alle Daten des Opfers heruntergeladen, erfährt er nun, welche Datei besonders interessant zu sein scheint und kann diese im Detail untersuchen.

6.2.5.6 Datenschutzbeauftragte und Datenschutzbeauftragter

Im Falle einer Verletzung des Schutzes personenbezogener Daten müssen die Verantwortlichen den Vorfall unverzüglich und möglichst binnen 72 Stunden an die zuständige Datenschutzaufsichtsbehörde melden.[18] Die für ein bestimmtes Bundesland zuständige Aufsichtsbehörde lässt sich der Webseite des BfDI[19] entnehmen. Ob ein Vorfall meldepflichtig ist oder nicht, muss nicht vom Vorfall-Praktiker entschieden werden. Dieser kann lediglich technische Hinweise darlegen, welche auf einen Diebstahl personenbezogener Daten hinweisen oder nicht. Auf dieser Grundlage kann die Geschäftsführung die Datenschutzbeauftragte oder den Datenschutzbeauftragten des Unternehmens alarmieren, sodass dieser die Entscheidung trifft. Verfügt das Unternehmen über keine Datenschutzbeauftragte oder keinen Datenschutzbeauftragten, trifft die Geschäftsführung selbst die Entscheidung. Aufgrund des häufigen Abfluss von Daten wird generell empfohlen den Vorfall zu melden.

[18] https://dejure.org/gesetze/DSGVO/33.html
[19] https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html

6.2.5.7 Juristinnen und Juristen

Entschließt sich die Geschäftsführung dazu, die Lösegeldforderung zu bezahlen, so sollte der Vorfall zunächst von den Juristinnen und Juristen des Unternehmens geprüft werden, ob eine Bezahlung überhaupt strafrechtlich möglich ist (Compliance). Auf Basis dieser Beurteilung kann die Geschäftsführung das Risiko eines Verstoßes bewerten und gegebenenfalls tragen.

6.2.6 Ransomware verhindern

Die folgenden Maßnahmen können bereits erfolgte Ransomware-Angriffe nicht beheben, sie können jedoch die Frage des Betroffenen beantworten, wie solche Angriffe in der Zukunft verhindert werden können.

Grundsätzlich helfen gegen Ransomware-Angriffe die gleichen Maßnahmen, die auch gegen andere Arten von Schadprogrammen helfen, beispielsweise Antivirenscanner, Firewalls, Sicherheitsupdates und Schulungen, um die Mitarbeitenden zu sensibilisieren. Insbesondere gegen Ransomware-Angriffe schützt jedoch ein durchdachtes Backup-Konzept, mit dem der Schaden im Falle eines Falles wie oben beschrieben rückgängig gemacht werden kann. Dazu müssen die Backups jedoch physisch getrennt gelagert werden, damit sie nicht von der Ransomware ebenfalls verschlüsselt wird. Alternativ bieten manche Backup-Systeme oder Cloud-Dienstleister an, dass nur neue Backups hinzugefügt werden, bestehende Backups jedoch nicht überschrieben werden können. Zusätzlich sollten wichtige Dateien nicht lokal auf den Mitarbeitenden-PCs abgelegt werden, sondern auf einem zentralen Netzlaufwerk, damit die Dateien ebenfalls Teil der Backups werden. Wurde ein Backup-System eingerichtet, so sollte die Wiederherstellung eines Backups in einer Übung getestet werden, um sicherzustellen, dass im Ernstfall keine unerwarteten Probleme auftauchen. Auch die Etablierung von ausführlichen Tests der Wiederherstellungsszenarien erweisen sich als zunehmend hilfreich, um die Funktionalität der Backup-Systeme gewährleisten zu können, und mögliche Spätfolgen und Dateninkonsitenz zu verhindern.

Als weitere Maßnahme kann der ausgehende Datenverkehr auf Anfragen zu bekannten Command and Control Servern[20] überwacht werden. Erfolgt eine derartige Anfrage, kann von einer Kompromittierung des Systems ausgegangen und die Verbindung sofort untersucht werden.

[20] https://abuse.ch/

7 Remote-Unterstützung (VP)

7.1 Einführung

Die richtige Reaktion und Vorgehensweise bei einem durch einen Cyber-Kriminellen herbeigeführten IT-Sicherheitsvorfall ist für die Betroffenen von elementarer Bedeutung. Aufgrund möglicherweise fehlender Kompetenzen in diesem Bereich ist es häufig erforderlich, sich an eine Expertin oder einen Experten zu wenden. In der heutigen Zeit ist hierbei die Anwesenheit bei Betroffenen vor Ort nicht zwingend notwendig.

Um Unterstützungsleistungen aus der Ferne in einer angemessenen Weise erbringen zu können, sind jedoch verschiedene Bedingungen zu beachten und zu erfüllen. Dies gilt sowohl auf Seiten des Vorfall- Praktikers als auch auf Seiten der Betroffenen. Der technische Fortschritt bietet hierbei immer mehr Lösungen an, bei denen eine Hilfestellung aus der Ferne effektiv erfolgen kann.

Zudem kann eine Fern- oder Remote-Unterstützung einige Vorteile mit sich bringen, birgt aber andererseits auch gewisse Gefahren und Nachteile.

7.2 Intention und Lernziele

Zunächst wird in diesem Abschnitt eine Abgrenzung zur vor-Ort-Unterstützung vorgenommen. Zudem werden zwei wesentliche Varianten der Remote-Unterstützung erläutert. Im Anschluss werden verschiedene technische Voraussetzungen sowie sonstige Rahmenbedingungen beschrieben, die zu beachten sind. Zuletzt werden Verbindungs- und Zugriffsmöglichkeiten erläutert und die Problematik bei der Datensammlung und -analyse kurz dargestellt.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

- Besonderheiten bei der Remote-Unterstützung widerzuspiegeln und zu beachten.
- Remote-Unterstützung bei der Behandlung eines IT-Sicherheitsvorfalls zu leisten.

7.3 Begriffsbestimmung der Fern- oder Remote-Unterstützung

Der Ausdruck Remote-Unterstützung beschreibt eine Hilfeleistung, die aus der Ferne erbracht wird. Dies bedeutet im Wesentlichen, dass sich die betroffenen Systeme sowie die Hilfesuchenden und der Vorfall-Praktiker dabei an verschiedenen Orten befinden.

In der IT wird oftmals auch der Begriff Fernwartung als Synonym verwendet, welcher jedoch mit der Administration von IT-Systemen in Verbindung steht und von einer Systemadministratorin oder einem Systemadministrator oder Servicepersonal durchgeführt wird. Typische Aufgaben sind dahingehend beispielsweise die Planung, Installation, Konfiguration und Pflege der IT-Infrastruktur.

Im Vergleich zu dem zuvor beschriebenen Begriff einer Fernwartung geht es bei der Remote-Unterstützung im Sinne dieses Leitfadens um eine Hilfeleistung bei der Reaktion auf IT-Sicherheitsvorfälle durch eine Vorfall-Expertin oder einen Vorfall-Praktiker. Infolgedessen werden keine administrativen Unterstützungsleistungen durch die Betroffenen in Anspruch genommen. Vielmehr zielt die Hilfestellung auf die wirksame Behebung des IT-Sicherheitsvorfalls ab.

Im Hinblick auf die Realisierungsmöglichkeiten des Remote-Zugriffs kann zwischen zwei grundlegenden Ansätzen unterschieden werden:

- Passiver Ansatz
- Aktiver Ansatz

Bei dem passiven Ansatz ist der Vorfall-Praktiker in erster Linie als Beobachter tätig. Typischerweise erfolgt die Kommunikation telefonisch und die Betroffenen führen unter Anweisung des Vorfall-Praktiker verschiedene Handlungen durch. Im Regelfall wird im Zuge dessen der Bildschirm der Betroffenen übertragen bzw. gespiegelt, um auf diese Weise die Navigation zu erleichtern. Tastatur- und Mauseingaben werden jedoch ausschließlich durch die Betroffenen realisiert.

Der aktive Ansatz einer Remote-Unterstützung unterscheidet sich von der passiven Variante in dem Punkt, dass die Expertin oder der Experte auch steuernd tätig wird. Es ist ihr oder ihm somit erlaubt, Tastatur- und Mauseingaben eigenständig zu tätigen. Dies ermöglicht dem Vorfall-Praktiker die Systeme der Betroffenen fernzusteuern. Jedoch ist hierbei zu differenzieren, ob die Hilfestellung gemeinsam mit den Betroffenen erfolgt oder der Vorfall-Praktiker sich allein in den Systemen bewegt. In der Praxis fällt die Wahl für gewöhnlich auf die gemeinsame Variante, da hierbei die betroffene Person jederzeit einschreiten kann und zugleich eine Kontrolle über die durchgeführten Handlungen hat.

Um eine Remote-Unterstützung in einer angemessenen Weise wahrnehmen zu können, ist es in der Regel notwendig, auf verschiedene Tools zurückzugreifen.

7.4 Voraussetzungen und Rahmenbedingungen

Um Unterstützungsleistungen hinsichtlich der Reaktion auf IT-Sicherheitsvorfälle über eine Remoteverbindung realisieren zu können, müssen zum einen verschiedene technische Voraussetzungen erfüllt werden und zum anderen ist es erforderlich, zusätzlich die Rahmenbedingungen zu klären. Diese werden in den nachfolgenden Abschnitten genauer erläutert.

Können hierbei grundlegende Voraussetzungen nicht erfüllt werden oder kommt es zu Hemmnissen bei den sonstigen Rahmenbedingungen, so kann eine Remote-Unterstützung von einem Vorfall-Praktiker nicht durchgeführt bzw. von Betroffenen nicht in Anspruch genommen werden.

Demzufolge müssen in Abstimmung mit den Betroffenen die technischen Voraussetzungen sowie weitere Anforderungen und ggf. Besonderheiten besprochen sein, bevor eine Remote-Unterstützung durchgeführt werden kann.

Remote-Unterstützung erscheint eine einfache und schnelle Möglichkeit für die Unterstützung von KMU und Bürgerinnen und Bürgern. Allerdings sollte bedacht werden, dass entsprechende Möglichkeiten auch von potenziellen Angreifenden erkannt werden können. Dies kann dazu führen, dass die Angreifenden entsprechende Gegenmaßnahmen einleiten bzw. ihre Spuren verwischen. Weiterhin ist vorstellbar, dass Angreifende den Moment des Remote-Zugriffes dazu nutzen, Systeme und Netze oder Teile davon außer Betrieb zu nehmen („DoS“).

7.4.1 Technische Voraussetzungen

Eine zentrale Anforderung ist das Vorhandensein eines dem Einsatzgebiet entsprechenden Tools, welches dem Vorfall-Praktiker erlaubt, die Oberfläche der Betroffenen darzustellen. Hierbei kann zwischen zwei verschiedenen Arten unterschieden werden. Eine Visualisierung bzw. Spiegelung der Bildschirmoberfläche der Betroffenen erfolgt i. d. R. bei jedem Tool. Der grundlegende Unterschied liegt hier in der Durchführung von Handlungen. Diesbezüglich gewährleisten die meisten Tools jedoch die Möglichkeit der Übergabe der Steuerung an den Vorfall-Praktiker. Eine explizite Zustimmung durch die Betroffenen ist dabei erforderlich.

Neben der Notwendigkeit, einen passiven oder aktiven Ansatz als Unterstützungsleistung auszuwählen, ist es wichtig, dass dabei eingesetzte Betriebssystem zu betrachten. Nicht jedes Tool ist für jedes Betriebssystem geeignet.

Darüber hinaus ist eine wesentliche Voraussetzung eine aktive und funktionierende Internetverbindung, da die Verbindung zu den Systemen über das Internet hergestellt wird.

Neben diesen ausschlaggebenden Bedingungen ist weiterhin notwendig, dass sich Geräte der Betroffenen in einem eingeschalteten Zustand befinden und diese am System eingeloggt sind.

Können die aufgeführten Voraussetzungen erfüllt werden, so ist es in der Regel technisch möglich, eine Remoteverbindung aufzubauen und auf diese Weise Unterstützungsleistungen in Anspruch zu nehmen.

Auch die Möglichkeit des Verbindungstyps sollte diskutiert werden. Das virtuelle private Netzwerke (VPN) ist in diesem Zusammenhang kritisch bzw. muss äußerst sensibel betrachtet werden. Im Zweifel sollte bei der Aufarbeitung und Analyse von IT-Sicherheitsvorfällen immer ein völlig unabhängiger Netz-Zugang zum Internet (z. B. LTE) genutzt werden.

7.4.2 Rahmenbedingungen

Neben den technischen Voraussetzungen gibt es zusätzliche gewisse Rahmenbedingungen und Vorgaben, die zwischen dem Vorfall-Praktiker und den Betroffenen zu klären sind, bevor eine Remote-Unterstützung realisiert werden kann. Die entscheidende Frage ist an dieser Stelle, in welchem Rahmen die Hilfestellung von Betroffenen beansprucht werden soll.

Es gilt, die nachfolgenden Fragestellungen gemeinsam mit den Betroffenen zu klären:

- Wird ein passiver oder aktiver Ansatz verfolgt?
- Ist bereits ein entsprechendes Tool vorhanden?
- Welche Tätigkeiten dürfen auf der Seite des Vorfall-Praktiker durchgeführt werden?
- Wo ist die Grenze der erlaubten Handlungen?
- Ist der Kontakt mit sensiblen/vertraulichen Informationen denkbar?

Unter Berücksichtigung der aufgeführten Fragestellungen ist ein transparentes Vorgehen ein nicht zu vernachlässigender Aspekt, insbesondere dann, wenn steuernde Tätigkeiten ohne Aufsicht getätigt werden können bzw. der Vorfall-Praktiker die Möglichkeit hat, sich allein im System der Betroffenen zu bewegen. Dies sichert vor allem den Vorfall-Praktiker in ihren oder seinen Handlungen ab. Infolgedessen sind die Betroffenen über die nachfolgenden Punkte zu informieren bzw. aufzuklären:

- Darstellung des allgemeinen Vorgehens
- Gleiche Berechtigungen wie die angemeldete Benutzerin oder der angemeldete Benutzer bei Übergabe der Steuerung
- Einsicht in sensible/vertrauliche Daten durch den Vorfall-Praktiker möglich
- Durchführung von Handlungen nach Absprache und Zustimmung durch die Betroffenen
- Dokumentation von Tätigkeiten (idealerweise automatisch und nicht deaktivierbar)

7.5 Verbindungs- und Zugriffsmöglichkeiten

Im Rahmen der Tätigkeiten eines Vorfall-Praktiker bei einer Remote-Unterstützung ist es unter Umständen empfehlenswert oder gar notwendig, dass dieser Zugriff auf die betroffenen IT-Systeme erhält, um wirksam an der Behebung mitwirken zu können.

Je nach Wahl der Verbindungs- und Zugriffsmöglichkeiten sind zum Teil nur eingeschränkte Analysemöglichkeiten gegeben. Dies könnte sich je nach Zielsetzung der Betroffenen negativ auf die Beseitigung auswirken und zu Verzögerungen führen.

Im Nachfolgenden wird zwischen drei grundlegenden Methoden unterschieden:

- Visualisierung der Oberfläche über Konferenztools,
- Visualisierung der Oberfläche und Steuerung über Fernwartungstools,
- Zugriff auf die Infrastruktur über einen VPN-Zugang.

Die verschiedenen Methoden werden beschrieben und zudem potenzielle Probleme ausgeführt.

7.5.1 Konferenztools

Unter dem Einsatz von Konferenztools wird die Visualisierung der Benutzeroberfläche der Betroffenen verstanden. Dies erlaubt auf der einen Seite den Betroffenen, die Problemstellung, gewonnene Erkenntnisse und erkannte Anomalien vorzustellen und auf der anderen Seite dem Vorfall- Praktiker, eine Einsicht in die relevanten Systeme vorzunehmen und somit erste Informationen zu dem vorliegenden Sachverhalt zu sammeln. Die Verbindung muss dabei durch die Betroffenen initiiert werden.

Grundlegende Vorgehensweise ist schließlich die Navigation der Betroffenen zu essentiell wichtigen Bereichen, an denen sich Hinweise und Informationen zu dem IT-Sicherheitsvorfall befinden könnten. Darüber hinaus kann ebenso eine erste Beweissicherung unter Anleitung des Vorfall-Praktiker angestoßen werden. Dabei können jedoch lediglich die lokal zur Verfügung stehenden Bordmittel[21], welche das entsprechende Betriebssystem zur Verfügung stellt, verwendet werden.

Die Nutzung von Konferenztools kommt in der Regel zum Einsatz, wenn es nicht erwünscht ist, dass der Vorfall-Praktiker steuernd in der Systemlandschaft tätig ist oder keine alternativen Möglichkeiten zu Verfügung stehen.

Der wesentliche Vorteil ist die gemeinsame Navigation im System, wobei die Steuerung bei den Betroffenen bleibt und somit die durchzuführenden Handlungen gemäß den Anweisungen des Vorfall-Praktiker implizit akzeptiert werden. Sollten durch gewisse Handlungen Grenzen auf Seiten der Betroffenen überschritten werden, obliegt es diesen, die Aktion zu unterbinden.

Der Nachteil dieser Methode liegt jedoch in der Steuerung durch Betroffene. Je nach Qualifikation und Verständnis kann es hierbei zu Komplikationen bei der Navigation kommen und infolgedessen die Unterstützungsleistung gehemmt werden.

7.5.2 Fernwartungstools

Die Verwendung von Fernwartungstools erlaubt neben der Visualisierung der Benutzeroberfläche der Betroffenen ebenso die Übernahme der Steuerung durch den Vorfall-Praktiker. Die Verbindung muss von den Betroffenen initiiert werden und darüber hinaus ist es teilweise erforderlich, dem Vorfall-Praktiker die Steuerung zu erlauben bzw. zu ermöglichen. Im Anschluss an die explizite Freigabe der Steuerung ist es dem Vorfall-Praktiker möglich, das System für den Zeitraum der Freigabe aus der Ferne zu steuern und sich darin zu bewegen. Der Bewegungsrahmen beschränkt sich dabei auf die Berechtigungen der angemeldeten Benutzerin oder des angemeldeten Benutzers.

Ähnlich wie bei der Nutzung eines Konferenztools ist er jedoch in seinen Möglichkeiten eingeschränkt. Das Verbinden zum System der Betroffenen in Verbindung mit der Übernahme der Steuerung erlaubt es dem Vorfall-Praktiker, sich eigenständig einen Überblick über das Schadensausmaß und das Verhalten der potenziell infizierten Systeme zu verschaffen, sowie eine erste Beweissicherung über die lokal zur Verfügung stehenden Bordmittel anzustoßen. Auf diese Weise können Missverständnisse bei einer Navigation durch Betroffene vermieden werden.

[21] Unter einem Bordmittel wird ein Hilfsprogramm verstanden, welches durch das jeweilige Betriebssystem zur Verfügung gestellt wird. Eine nachträgliche oder zusätzliche Installation ist nicht notwendig.

7.5.3 Virtual Private Network (VPN)

Mit der Bereitstellung eines VPN-Zugangs hat der Vorfalls-Praktiker die Möglichkeit, über das eigene Gerät direkt auf das betroffene Netzwerk zuzugreifen. Mittels der Firewall der Betroffenen lassen sich die Zugriffe auf Netzbereiche oder einzelne Systeme reglementieren. Der Zugriff über das VPN muss in der Regel einmalig auf der Seite der Betroffenen eingerichtet und die Zugangsdaten dem Vorfall-Praktiker übermittelt werden. Darüber hinaus hat der Vorfall-Praktiker den entsprechenden VPN-Client zu installieren. Der Zugriff auf die freigegebenen Netzbereiche und Systeme ist solange möglich, bis die entsprechende Benutzerin oder der entsprechende Benutzer durch die Betroffenen deaktiviert oder gelöscht wird.

Die Nutzung eines VPN-Zugangs erlaubt es dem Vorfall-Praktiker, sich in dem freigegebenen Bereich eigenständig zu bewegen und sich selbstständig einen Überblick über Schadensausmaß und Verhalten der potenziell infizierten Systeme zu verschaffen sowie eine Beweissicherung anzustoßen.

Eine unmittelbare Monitoring-Funktion im Sinne einer gemeinsamen Navigation durch das System im Vergleich zu den Konferenz- und Fernwartungstools ist hierbei nicht gegeben, da die Benutzeroberfläche nicht gespiegelt wird. Gewisse Tätigkeiten werden jedoch im Rahmen der Ereignisprotokollierung der Betroffenen erfasst.

Eine Besonderheit bei der Methodik ist die Möglichkeit, eigene Tools hinsichtlich der Datensammlung und Datenanalyse einzusetzen. Somit ist der Vorfall-Praktiker in diesem Punkt weniger eingeschränkt als in den zuvor beschriebenen Verfahren.

7.6 Datensammlungs- und Analysemöglichkeiten

Die Beweiserhebung in Verbindung mit der Analyse der gesicherten Daten im Rahmen der Ursachenermittlung gestaltet sich bei einer Remote-Unterstützung schwieriger. Grund dafür ist, dass unter Berücksichtigung der Verbindungs- und Zugriffsmöglichkeiten oftmals nur die Bordmittel zur Verfügung stehen. Infolgedessen sind die Möglichkeiten hierbei eingeschränkt, da der Vorfall-Praktiker zunächst keine eigenen Tools und Programme verwenden kann.

An dieser Stelle ist es denkbar, in Abstimmung mit den Betroffenen und im Zuge der Remote-Unterstützung, bestimmte Programme zu installieren. Dabei ist jedoch unter Betrachtung des jeweiligen IT-Sicherheitsvorfalls abzuwägen, welche Tools in Fragen kommen könnten und inwiefern eine Installation sinnvoll ist. Im Kontext einer späteren Installation muss zudem immer bedacht werden, dass dadurch möglicherweise potenzielle Beweise vernichtet werden könnten.

8 Vorfallsbearbeitung bei IT-Systemen „abseits der üblichen Büroanwendung“ (VP&VE)

8.1. Einführung

Bei IT-Sicherheitsvorfällen wird primär an Büroarbeitsplätze und Server für E-Mails, zentrale Datenablagen oder andere IT-Dienste gedacht. Durch die Digitalisierung kommen auch in anderen Bereichen von Unternehmen verschiedenste Systeme zum Einsatz, deren reibungsloser Betrieb gestört werden kann. Beispiele dafür sind Systeme zur Gebäudeautomatisierung oder zur Produktionsplanung, -steuerung und -überwachung, sowie einzelne vernetzte Maschinen oder Geräte. Im Weiteren werden diese Systeme als Operative Technologie (OT) bezeichnet, um diese von der klassischen IT abzugrenzen.

Diese OT-Systeme sind häufig ebenfalls vernetzt, um einen Datenaustausch oder auch Fernzugriff für Wartung und Überwachung zu ermöglichen. Es besteht daher grundsätzlich die Gefahr, dass auch die OT von einem Sicherheitsvorfall betroffen wird oder dieser sich hierauf auswirkt.

8.2 Intention und Lernziele

Dieses Kapitel behandelt die Besonderheiten der OT. Es wird auf die Unterschiede und Besonderheiten eingegangen, die bei einem IT-Sicherheitsvorfall zu berücksichtigen sind. Dazu wird auch in die zuvor beschriebene Vorgehensweise referenziert.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmerin der Lage:

 Den Unterschied zwischen IT und OT zu beschreiben

 Vorfallbehandlung bei OT-Systemen Maßnahmen zu kennen und widerzuspiegeln.

 Grenzen der Analyse zu erkennen.

8.3. Notwendige Basiskenntnisse

Dieser Abschnitt gibt eine Einführung in die Grundlagen der OT. OT wird an dieser Stelle als Sammelbegriff für Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS) und andere gebräuchliche Begriffe aus anderen Branchen verwendet.

Es werden zuerst die Anwendungsgebiete von OT erläutert und danach typische OT-Architekturen vorgestellt. Dazu werden OT-Komponenten und genutzte Kommunikationstechniken beschrieben. Grundlage der Beschreibungen bildet dabei die herstellerunabhängige gängige Praxis der Anwendersicht. Mit Rücksicht auf die Vielzahl unterschiedlicher Anwendungen von OT erfolgt hier eine Betrachtung mit Fokus auf die Cybersicherheit, weshalb die anwendungsspezifischen Details nur generisch angesprochen werden.

Zusätzlich finden Sie unter nachfolgendem Link relevante Informationen zu Absicherung von Fernwartungszugriffen: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_054.pdf?__blob=publicationFile&v=1#:~:text=Sobald%20der%20Fernwartende%20jedoch%20zu,Zugriff%20auf%20das%20System%20erh%C3%A4lt

OT wird überall dort eingesetzt, wo Abläufe automatisiert werden. Dies umfasst das Messen, Steuern, Regeln und Bedienen von industriellen Abläufen.
Beispiele hierfür sind die Verfahrens- und Prozesstechnik, die Fertigungsautomatisierung, die Ver- und Ent-

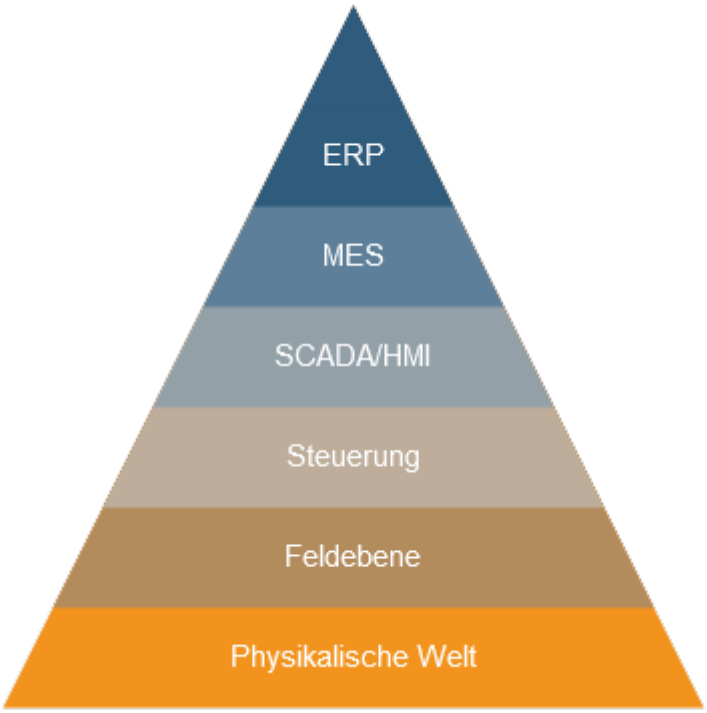


Abbildung 5: Automatisierungspyramiede

sorgungsnetze (z. B. Strom, Wasser, Gas, Fernwärme), die Betriebstechnik (z. B. Schienen- und Straßenverkehr) und die Gebäudeautomation. Die individuellen Anforderungen an OT werden unmittelbar durch die betrieblichen Anforderungen der jeweiligen Prozesse bestimmt.

Die klassische Trennung der Automatisierungsebenen nach dem Vorbild der Automatisierungspyramide (vgl. Abbildung 5) bildet in der Praxis längst nicht mehr die Realität ab. IT-Systeme wie Enterprise-Ressource-Planning (ERP), Manufacturing-Execuction-Systeme (MES) zur Produktionsplanung, SCADA- Systeme zur übergeordneten Steuerung oder Human-Machine-Interfaces (HMI) zur lokalen Steuerung, Speicherprogrammierbare Steuerungen (SPS) oder andere Arten von Kontrollern sowie Feldgeräte in Form von Sensoren und Aktoren verschmelzen zunehmend informationstechnisch mit Office-Anwendungen und Internetdiensten.

8.4 Unterschiede von OT zu Standard-IT

Hier eine Übersicht zu den wesentlichen Unterschieden zwischen IT und OT:

Lebenszyklus
Der Lebenszyklus von IACS wird aus dem der zugehörigen Produktionsanlage abgeleitet. Dieser ist deutlich länger als die in der Office-IT typischerweise anzutreffenden Zeiträume. Die Laufzeit beträgt zehn bis fünfzehn Jahre. Mitunter können es auch 20 Jahre oder mehr sein. In der Office-IT sind es meist nur drei bis fünf Jahre.

Echtzeitverhalten
Automatisierungssysteme werden im Hinblick auf ihr deterministisches Zeitverhalten optimiert. Kommt es aufgrund von (temporären) Modifikationen im Bereich der Software zu Änderungen am Zeitverhalten des IACS, führt dies zu Störungen im materiellen Produktionsprozess. Dies kann z.B. zu mehr Ausschuss führen oder Ausfälle verursachen.

Funktionale Sicherheit
Es gibt viele Anwendungen, in welchen der Betrieb der Anlagen an behördliche Auflagen gebunden ist

(z. B. der Anlagensicherheit oder des Arbeitsschutzes). In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten IACS fallen können, eines dedizierten Genehmigungsprozesses. Dies beeinflusst beispielsweise die Möglichkeiten zur Einspielung von Updates.

Physikalische Trennung
Im Bereich des Aufbaus von ICS ist es üblich, neben logischer Trennung einzelner Teilbereiche auch eine physikalische Trennung von Funktionseinheiten – speziell im Bereich der Infrastruktur – umzusetzen.
Beispiel:
Im Bereich der Office-IT ist es üblich, verschiedene logische Netzwerke auf einem Switch zu betreiben. Im Bereich der ICS ist dies, mit Rücksicht auf mögliche ungewollte Querverbindungen und deren potenzielle Auswirkung, ungebräuchlich. Werden unterschiedliche Netzwerksegmente trotzdem zusammengefasst, so ist dies im Rahmen einer Risikobewertung zu betrachten. Die Auswirkungen auf die Systemintegrität sind in diesen Fällen zu bewerten und zu dokumentieren.

Software
Im Gegensatz zur Office-IT werden ICS über längere Zeiträume mit quasi gleicher Anwendersoftware betrieben. Änderungen finden meist nur im Rahmen vorgeplanter Maßnahmen statt.

Updates
Im Bereich der Office-IT werden Systeme nach Bekanntwerden von Fehlern oder Schwachstellen im Idealfall schnellstmöglich (durch die Installation von Patches und Updates) nachgebessert.
Im Anwendungsbereich von ICS sind bei Softwareänderungen, auch während des Änderungsprozesses, neben den Funktionen die vorgegebenen Reaktionszeiten einzuhalten. Darüber hinaus sind grundsätzlich Prüfungen der Gesamtanordnung bestehend aus ICS und einem materiellen Produktionsprozess erforderlich. Die jeweilige Prüftiefe richtet sich nach der jeweiligen Applikation. So sind anwendungsspezifische (z. B. im Bereich der Pharmaproduktion) Prüfungen durchzuführen und zu dokumentieren, deren Abarbeitung eine Produktionsunterbrechung erzwingt. Updates können daher in der Regel nur im Rahmen von Wartungsaktivitäten in größeren Abständen eingebracht werden.

Hardware
Im Gegensatz zur Office-IT werden ICS über längere Zeiträume mit gleicher und häufig unveränderter Hardware (Gerätetypen) betrieben. Das meint, dass die eingesetzten Geräte mitunter das gleiche Alter haben wie die Anlage selbst.

8.5 Weiteres relevantes Fachpersonal

Bei einem IT-Sicherheitsvorfall im Bereich oder mit Bezug zur OT sollte weiteres Fachpersonal neben dem unter Kapitel 1.5 genannten Personen, hinzugezogen werden. Dazu gehören unter anderem:

Verantwortliche für Betrieb der OT-Systeme, sowie für Wartung und Instandhaltung
Unterstützung bei der Bewertung und Umsetzung von Maßnahmen

Sicherheitsbeauftragte für die OT-Anlagen
Unterstützung bei der Bewertung und Kritikalität, um eine Gefahr durch Manipulationen der Systeme für Mensch oder Umgebung auszuschließen

Gesetzliche Vorgaben

Bei einer Betroffenheit von OT können abhängig von der betroffenen OT unterschiedliche gesetzliche Aspekte betroffen sein. An dieser Stelle sollen nur einzelne rechtliche Aspekte herausgegriffen werden:

- Melde- und Registrierungspflichten, sowie die Anforderungen an die eingesetzten Systeme (gemäß BSI-Gesetz)
  Für KRITIS-Unternehmen und Unternehmen im besonderen öffentlichen Interesse gibt es die Verpflichtung zur Meldung von IT-Sicherheitsvorfällen an das BSI.

- Vorgaben zum Arbeitsschutz (Berufsgenossenschaften)
- Störfallverordnung

8.6 Ablauf des Standardvorgehens bei OT

Im Folgenden sollen einige zusätzliche Hinweise gegeben werden, die im Kontext von OT, bei einem IT-Sicherheitsvorfall zu berücksichtigen sind.

8.6.1 Identifikation des Sicherheitsvorfalles

Bei der Identifikation sollte berücksichtigt werden, wie stark die Mitarbeitenden und Verantwortlichen der OT für das Thema IT-Sicherheit sensibilisiert sind.

Es kann vorkommen, dass Beeinträchtigungen, z.B. durch eine Infektion mit einem Schadprogramm, als simple Störung abgetan werden. In der Folge wird ggf. durch einen Neustart der Komponente kurzfristig das Problem gelöst. Aufgrund fehlender Sicherheitsupdates könnte in kurzer Zeit jedoch eine erneute Infektion stattfinden.

Es sollte daher auf gehäufte Fehler oder Störungen geachtet werden.

8.6.2 Eindämmung des Schadensausmaßes

Bei der Umsetzung von Eindämmungsmaßnahmen sollten auch Auswirkungen auf die OT berücksichtigt werden. Beispielsweise kann durch die Trennung von zentralen Netzwerkverbindungen die Überwachung oder Steuerung von (entfernten) Anlagen beeinträchtigt werden. Daher ist eine Abstimmung mit Fachpersonal der OT ratsam.

8.6.3 Beweissicherung & Analyse

Das Sichern von Beweisen kann sich in der OT schwerer gestalten als bei normalen IT-Servern oder Arbeitsplatzsystemen. Gerade bei Steuerungen, Sensoren, Aktoren ist spezielle Software (teilweise auch Hardware) erforderlich, um Daten auszulesen. Es kann auch sein, dass keine Funktionen zum Sichern der notwendigen Informationen (z.B. aus dem Arbeitsspeicher) verfügbar sind, diese vor Zugriff geschützt sind oder das Gerät erst geöffnet werden müsste.

Zudem ist damit zu rechnen, dass eine tiefergehende Analyse mit höheren Aufwänden verbunden ist, da bisher wenige Werkzeuge auf diese Art der Analysen spezialisiert sind.

8.6.4 Wiederherstellung

Bei der Wiederherstellung sollte auf die vorhandenen Wartungs- und Instandhaltungsdienste (intern oder extern) zurückgegriffen werden.

9 Vor-Ort-Unterstützung: Überblick verschaffen (VE)

9.1 Einführung

Aufgrund von fehlenden Voraussetzungen oder Rahmenbedingungen kann es manchmal unumgänglich sein, einen Betroffenen vor Ort zu unterstützen, um einen IT-Sicherheitsvorfall ordnungsgemäß zu behandeln. Jedoch müssen auch bei der Vor-Ort-Unterstützung bestimmte Voraussetzungen erfüllt sein, damit eine reibungslose und gesetzeskonforme Behandlung gewährleistet werden kann. Betroffene sollten dabei bedenken, dass der Vorfall-Experte direkten Zugriff auf organisationsinterne Informationen erhalten kann und muss daher geeignete Rahmenbedingungen festlegen. Um Differenzen über den Leistungsumfang von Beginn an auszuräumen, sollte im Voraus geklärt werden, welche Tätigkeiten vom Vorfall-Experten durchgeführt werden, wo dessen Grenzen sind.

Durch die Anwesenheit des Vorfall-Experten, ergeben sich einige Vorteile, die die Behandlung deutlich erleichtern. Eine direkte Kommunikation zwischen Betroffenen und dem Vorfall-Experten vereinfacht die Abstimmung der Tätigkeiten und kann Missverständnisse vermeiden.

9.2 Intention und Lernziele

Dieses Kapitel des Leitfadens beschäftigt sich mit der Vor-Ort-Unterstützung einer oder eines Betroffenen, die oder der Opfer eines IT-Sicherheitsvorfalls wurde. Ziel dieses Kapitels ist es zu vermitteln, wie sich ein Vorfall-Experte einen Überblick vor Ort verschaffen kann und welche Voraussetzungen für eine erfolgreiche Vor-Ort-Unterstützung gegeben sein müssen. Außerdem werden die allgemeinen Rahmenbedingungen einer Zusammenarbeit von Betroffenen und Vorfall-Experten erläutert.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

 Sicher und kompetent vor Ort aufzutreten.

 Sich einen Überblick über die Gegebenheiten bei Betroffenen zu verschaffen.

9.3 Vorfall-Experte als Krisenmanager etablieren

Das Ziel eines jeden Vorfall-Experten muss immer eine effektive Behandlung und Aufklärung des IT-Sicherheitsvorfalls sein, unabhängig davon, ob es sich um eine Vor-Ort- oder Remote-Unterstützung handelt. Um den IT-Sicherheitsvorfall zur Zufriedenheit aller Beteiligten zu lösen, ist es jedoch besonders bei der Vor-Ort-Unterstützung von essenzieller Bedeutung, dass der Vorfall-Experte für seine Tätigkeit an der richtigen Stelle im Unternehmen etabliert wird.

Bevor die Zusammenarbeit zwischen dem Vorfall-Experten und den Betroffenen beginnt, sollte genau festgelegt werden, wo Unterstützung benötigt wird. Dies ist wichtig für die Aufwandsschätzung seitens des Vorfall-Experten. Zu einem Krisenmanager gehören fundiertes Wissen und ein hoher Erfahrungsschatz. Auch kann so festgestellt werden, ob eventuell weitere Fachkräfte für die Bewältigung des IT-Sicherheitsvorfalls hinzugezogen werden müssen.

Auch der erste Eindruck der Betroffenen vom Vorfall-Experten kann entscheidend sein. Der Vorfall-Experte muss ein selbstbewusstes und sicheres Auftreten sicherstellen. Außerdem ist es wichtig, den Betroffenen gegenüber stets einen kompetenten Eindruck zu vermitteln. Ein unsicheres oder gar hektisches Auftreten kann die Bearbeitung des IT-Sicherheitsvorfalls gefährden.

Die nachfolgenden Abschnitte dienen als Hilfestellung, um ein souveränes Auftreten bei einem Betroffenen vor Ort sicherzustellen.

9.3.1 Erscheinungsbild

Das äußere Erscheinungsbild sollte nicht unterschätzt werden. Für viele Menschen kann der erste Eindruck schon entscheidend dafür sein, ob sie ihr Gegenüber für kompetent halten.

Empfehlenswert	Unratsam
☑ Gepflegtes Äußeres	⊗ Intensive Körpergerüche
☑ Angemessene Kleidung	⊗ Zu lockeres Outfit
☑ Körperhygiene	⊗ Chaotisches Auftreten

Tabelle 2: Hinweise zum Erscheinungsbild

9.3.2 Körpersprache

Eine selbstsichere Körperhaltung hat zum einen Auswirkungen auf die Personen, die sie umgeben, wirkt sich aber auch positiv auf den eigenen Gemütszustand und das Selbstbewusstsein aus.

Empfehlenswert	Unratsam
☑ Ruhiges Auftreten	⊗ Hektische Bewegungen
☑ Positive / freundliche Ausstrahlung	⊗ Auf den Boden schauen
☑ Aufrecht stehen / sitzen	⊗ Die Schultern hängen lassen
☑ Augenkontakt mit Gesprächspartnern	⊗ Fingernägel kauen

Tabelle 3: Hinweise zur Körpersprache

9.3.3 Ausdrucksweise

Eine ordentliche Ausdrucksweise bedeutet, sich gut zu artikulieren, Wörter richtig zu betonen, in einer angemessenen Lautstärke zu sprechen und die eigenen Aussagen mit einer ausdrucksstarken Mimik und Gestik zu unterstreichen. Die sprachlichen Fähigkeiten können zu Hause oder im Berufsalltag trainiert und verbessert werden.

Empfehlenswert	Unratsam
☑ Stilvolle Rhetorik	⊗ Fluchen und Schimpfworte
☑ Deutliche Aussprache	⊗ Rätselhafte & offene Aussagen
☑ Präzise Aussagen	⊗ Umgangssprachliche Wortwahl
☑ Ausdrucksstarke Mimik und Gestik	⊗ Vielzahl von Fachausdrücken

Tabelle 4: Hinweise zur Ausdrucksweise

9.4 Analysefähigkeit des Unternehmens einschätzen

Um einen IT-Sicherheitsvorfall bei einem Betroffenen vor Ort zu bearbeiten, ist es unumgänglich zu klären, welche Ansprechpartnerinnen und Ansprechpartner mit welchen Kompetenzen beim Unternehmen vorhanden sind. Des Weiteren muss sich ein Überblick über die vorhandene IT-Landschaft des Unternehmens verschafft werden.

9.4.1 Personalressourcen und Kompetenzen identifizieren

Zu Beginn der Arbeit vor Ort sollte sich ein Überblick über vorhandene Ansprechpartner sowie deren Kompetenzen und Befugnisse verschafft werden. Es ist beispielsweise ein großer Unterschied, ob man vor Ort mit einem Mitarbeiter aus der Personalabteilung spricht oder mit einem ausgebildeten IT-Administrator mit jahrelanger Berufserfahrung. In jedem Fall kann der Vorfall-Experte schnell feststellen, ob sie oder er allein die Vorfallbearbeitung bewältigen kann oder ein IT-Dienstleister mit einem Team von Vorfall-Experten benötigt wird.

9.4.1.1 Identifikation der Ansprechpartnerinnen und Ansprechpartner

Zunächst wird geprüft, welche und wie viele Ansprechpartnerinnen und Ansprechpartner dem Vorfall-Experten zur Lösung des IT-Sicherheitsvorfalls zur Verfügung gestellt werden. Möglicherweise erwarten die Betroffenen, dass die Expertin oder der Experte den IT-Sicherheitsvorfall löst, ohne eigene Ressourcen zur Verfügung zu stellen. Ist dies der Fall, muss der Vorfall-Experte dem Verantwortlichen darlegen, dass es nötig sein kann, Systeme herunterzufahren oder vom Netz zu trennen. Das kann unter Umständen Folgen für das Unternehmen haben. In einem solchen Fall werden die Ansprechpartner benötigt, die die Befugnis haben, eine solche Entscheidung zu treffen.

9.4.1.2 Kompetenzen der Ansprechpartnerinnen und Ansprechpartner

Der Vorfall-Experte muss analysieren, welche Kompetenzen die verfügbaren Ansprechpartnerinnen und Ansprechpartner haben. Dies ist wichtig, wenn die Aufgaben zur Lösung des IT-Sicherheitsvorfalls verteilt werden. Wenn Ansprechpartnerinnen und Ansprechpartner eine Aufgabe erhalten, für die sie nicht qualifiziert sind, kann es die vollständige Behandlung des IT-Sicherheitsvorfalls verzögern, oder sogar unmöglich machen. Die Kompetenzen der Ansprechpartnerinnen und Ansprechpartner können auf verschiedenen Wegen festgestellt werden, am effektivsten ist jedoch das direkte Gespräch. Bekommt der Vorfall-Experte das Gefühl, die Ansprechpartnerin oder den Ansprechpartner zu überfordern, sollte sie oder er das offen kommunizieren und die jeweilige Situation selbst erneut prüfen. Beginnt man die Behandlung eines IT-Sicherheitsvorfalls mit falschen Informationen, wie beispielsweise mit falschen Kommunikationsverbindungen, Patch-Ständen oder ähnlichem, kann das fatale Folgen für die Vorfallsbehandlung haben.

Im Hinblick auf die Bestimmung der Qualifikation bzw. Kompetenzen der Ansprechpartnerinnen und Ansprechpartner bei der Behandlung von IT-Sicherheitsvorfällen dient die Tabelle 5 als Hilfestellung.

Um als Ansprechpartnerin oder Ansprechpartner in Frage zu kommen, sollten mindestens die Kompetenzen der Nummern 1 bis 3 vorhanden sein, damit eine möglichst akkurate Bearbeitung des IT-Sicherheitsvorfalls sichergestellt werden kann.

Nr.	Qualifikation / Kompetenz
1.	Ansprechpartnerinnen und Ansprechpartner aus der IT
2.	Informations- und kommunikationstechnische Kenntnisse
3.	Fachspezifische IT-Ausbildung / IT-Studium
4.	Weisungsbefugt/Handlungsbefugt
5.	Mehrjährige Berufserfahrung
6.	Erfahrung im Bereich Informationssicherheit
7.	Projekterfahrung bei der Vorfallsbehandlung

Tabelle 5: Kompetenz-Checkliste für Ansprechpartnerinnen und Ansprechpartner

9.4.1.3 Einbindung von externen Dienstleistern

Wenn Dienstleister im Bereich der Informationstechnik und Kommunikationstechnik vorhanden sind, kann es sinnvoll und eventuell auch notwendig sein, diese mit einzubeziehen. Hierbei gilt es zu beachten, welchen Einblick die Dienstleister in die Systeme haben dürfen. Es kann auch notwendig sein, die vorhandenen Dienstleistungs- oder Wartungsverträge zu prüfen oder prüfen zu lassen. Oftmals ist es sinnvoll, ein Team von externen und internen Mitarbeiterinnen und Mitarbeitern aufzubauen, um den IT-Sicherheitsvorfall zu beheben. Der Vorfall-Experte sollte hierbei die Aufgaben für die einzelnen Mitglieder gemeinsam mit dem Verantwortlichen koordinieren.

9.4.2 Analysieren der IT-Infrastruktur des betroffenen Unternehmens

Um den IT-Sicherheitsvorfall schnell analysieren zu können, ist es notwendig, die Analysefähigkeit des Unternehmens einzuschätzen. Dafür müssen einige wichtige Punkte besprochen werden. Die vorhandenen Mittel zur Analyse und die Dokumentation des Unternehmens spielen eine entscheidende Rolle bei der Analyse.

9.4.2.1 Netzwerkdokumentation

Die beste Möglichkeit, sich einen Überblick über den IT-Sicherheitsvorfall zu verschaffen, besteht darin, die Netzwerkdokumentation des Unternehmens zu erfragen und zu sichten. Ist beispielsweise ein ausführlicher Netzwerkstrukturplan vorhanden, lassen sich Rückschlüsse über die Ausbreitung von Viren und das gesamte Schadensausmaß ziehen. Die vorhandene Netzwerkdokumentation sollte natürlich auf einem aktuellen Stand sein und die Gegebenheiten korrekt beschreiben.

Im Netzwerkstrukturplan sollte gezielt geprüft werden, wie die gesamte Netzwerkinfrastruktur des Unternehmens aufgebaut ist. Die folgenden Leitfragen sollten mit einer technischen Ansprechpartnerin oder einem technischen Ansprechpartner besprochen werden, wenn diese nicht bereits im Netzwerkstrukturplan ersichtlich sind:

- Wurde das Netzwerk sinnvoll in Zonen nach Anwendungszweck, Dienst oder ähnlichem eingeteilt?
  - Server-Netz, Client-Netz, Infrastruktur-Netz, VoIP-Netze, Management-Netz, Backup-Netz
- Wie findet die Trennung von Netzwerken statt?
  - Logische Trennung mittels VLAN
  - Physische Trennung mittels getrennter Leitungen und separaten Switches
- Welche Netze dürfen miteinander kommunizieren?
- Durch welches System werden die Netzwerkübergänge abgesichert?
- Wie restriktiv ist dieses System konfiguriert?
- Lassen sich bereits Dienste und Protokolle identifizieren, die am Netzkoppelelement erlaubt sind?
- Sind sämtliche Kommunikationsverbindungen erfasst?

Konnten alle diese Leitfragen beantwortet werden, lassen sich unter Umständen erste Systeme identifizieren, welche potenziell betroffen sein könnten.

Sollte eine solche Dokumentation der Netzwerkinfrastruktur noch nicht im Unternehmen vorhanden sein, sollte der Vorfalls-Experte gemeinsam mit einem oder mehreren IT-Verantwortlichen des Unternehmens einen Netzwerkstrukturplan erstellen. Bei der Erstellung sollten die o.g. Leitfragen berücksichtigt werden.

Eine zentrale Informationsquelle zur Identifikation von Systemen, die miteinander kommunizieren, ist im Regelfall eine Firewall. Diese ist meist in der Lage, IP-Adressen und Protokolle an den Netzübergängen zu erfassen. Um die Kommunikation innerhalb eines Netzes zu analysieren, können Netzwerkanalysetools verwendet werden.

9.4.2.2 Systemdokumentation

Neben dem Netzstrukturplan sollten ggf. weitere vorhandene Dokumentationen geprüft werden. Ein wichtiger Bestandteil ist die Dokumentation des Datensicherungsprozesses. Anhand von dieser Dokumentation

wird im Normalfall ersichtlich, welche Systeme wann und wie oft gesichert werden und ob im Zweifelsfall eine Wiederherstellung möglich ist.

Eine Dokumentation zu den verschiedenen Rollen und Berechtigungen sollten ebenso gesichtet werden, da sich hieraus erste Rückschlüsse über privilegierte Nutzer- und Systemaccounts ziehen lassen. Sofern dokumentierte Informationen zu bestimmten Anwendungen vorhanden sind, sollten diese gleichermaßen Beachtung finden. In ausführlichen Dokumentationen sind meist Verbindungswege zwischen den einzelnen Systemen der Anwendung ersichtlich. Solch eine Dokumentation kann herangezogen werden, wenn die Kommunikationswege nicht eindeutig im Netzwerkstrukturplan ersichtlich sind.

9.4.2.3 Analyse- und Auswertungseinrichtungen

Je nach Unternehmensgröße können verschiedene Anwendungen bei einer Analyse unterstützen. Die dafür am häufigsten zum Einsatz kommenden Systeme sind „Security Information and Event Management Systeme“ (SIEM), zentrale Protokollierungsserver oder auch spezielle Produkte der Antivirus-Hersteller.

Innerhalb des SIEM befinden sich wichtige Hinweise über Filezugriffe, Berechtigungsänderungen, fehlgeschlagene Anmeldeversuche oder Konfigurationsänderungen an Systemen und Netzwerkkomponenten. Beim Einsatz eines Protokollierungsservers, welcher sämtliche Systemereignisse an einer zentralen Stelle speichert, lassen sich Ereignisse identifizieren, die für den weiteren Verlauf der Identifikation und Bereinigung essentiell sein können. Grundlegende Informationen finden sich meist in den Management-Konsolen der Antivirus-Software-Hersteller. Diese Einrichtungen sind in der Lage, sämtliche vom Virenscanner erkannten Aktivitäten zu speichern. Einige Hersteller haben Werkzeuge implementiert, mit denen sich eine Infektionskette nachbilden lässt. Die Auswertung dieser Daten basiert ebenfalls auf Dateizugriffen und Netzwerkkommunikation.

Sollte eines oder mehrere der oben beschriebenen Systeme zum Einsatz kommen, kann dadurch der Prozess der Analyse deutlich beschleunigt werden.

Zusätzlich sollte geprüft werden, ob im Unternehmen forensische Tools im Einsatz sind, die nach Bedarf und Expertise der vor Ort unterstützenden Vorfall-Experten oder des vor Ort unterstützenden Vorfall-Experten benutzt werden können.

9.5 Organisatorische Voraussetzungen ermitteln

Um sich vor Ort einen umfassenden Überblick verschaffen zu können, muss der Vorfall-Experte bestimmte organisatorische Umstände und Voraussetzungen ermitteln. Da Unternehmen verschiedene Vorgehensweisen und Ansätze bevorzugen, müssen diese im ersten Schritt ermittelt werden.

9.5.1 Beschreibung des IT-Sicherheitsvorfalls

Um die Situation richtig bewerten zu können, müssen Informationen zum Verlauf des IT-Sicherheitsvorfalls erfragt werden. Der Vorfall-Experte sollte sich hierbei die Informationen von der betroffenen Person selbst einholen sowie, falls im Unternehmen vorhanden, von der zuständigen Administratorin oder vom zuständigen Administrator. Dabei sollten die Informationen so detailreich wie möglich erfragt werden.

9.5.2 Ermittlung von Notfallplänen

Auf in den meisten Unternehmen existieren bereits etablierte Notfallpläne welche zu erfragen sind. Die dort vorhandenen und getroffenen Vorgaben und Informationen sollten aktuell sein und unbedingt eingehalten werden. In diesen Dokumentationen werden oft Verantwortlichkeiten, Pläne und Verhaltensregeln festgelegt sowie die Reaktion auf Notfallsituationen beschrieben und definiert.

Sofern im Unternehmen noch keine Notfallpläne existieren, sollte eine zentrale Ansprechpartnerin oder ein zentraler Ansprechpartner zur Verfügung stehen, um das weitere Vorgehen mit diesem zu besprechen.

9.5.3 Einbindung von Dienstleistern

Es ist notwendig, bereits im Vorfeld zu ermitteln, ob zusätzliche Dienstleister in den Analyse- und Bereinigungsprozess eingebunden werden dürfen. Gründe für ein Einsatzverbot eines Dienstleisters können unter Umständen aufgrund gesetzlicher oder vertraglicher Regularien bestehen. In einem solchen Fall muss zwingend mit der Stelle im Unternehmen Kontakt aufgenommen werden, welche eine Entscheidung über den Einsatz eines Dienstleisters treffen kann.

Ebenfalls gilt es, bereits im Vorfeld zu klären, ob gewisse IT-Dienstleistungen an einen IT-Dienstleister ausgelagert wurden. In einem solchen Fall sind Kontaktdaten und Ansprechpartner des Dienstleisters erforderlich, da dieser unter Umständen über eine ausführliche Dokumentation der Kundeninfrastruktur verfügt und ggf. wichtige Informationen zum Verlauf des IT-Sicherheitsvorfalls zur Verfügung stellen kann.

9.6 Festlegung von Rahmenbedingungen der Zusammenarbeit

Für eine reibungslose, rechtssichere und vertrauensvolle Zusammenarbeit im Rahmen einer Unterstützung hinsichtlich eines IT-Sicherheitsvorfalls ist es notwendig, verschiedene Rahmenbedingungen vorab festzulegen. Die folgenden Abschnitte beschäftigen sich mit diesen Bedingungen.

9.6.1 Geheimhaltungsvertrag

Die Unterstützung bei einem IT-Sicherheitsvorfall ist eine sensible Tätigkeit, bei welcher nichts Ungewolltes an die Außenwelt gelangen sollte. Der Vorfall-Experte bekommt im Rahmen seiner Unterstützung zumeist Einblicke in sensible Daten und Systeme der oder des Betroffenen. Bei einer Vor-Ort-Unterstützung können zudem weitere, unter Umständen geheimhaltungsbedürftige, Informationen einsehbar sein. Auch sollte selbst die Tatsache, dass ein IT-Sicherheitsvorfall stattgefunden hat, eine interne und absolut vertrauenswürdige Angelegenheit bleiben. Es empfiehlt sich daher, einen Geheimhaltungsvertrag mit der oder dem Betroffenen abzuschließen. Dies ist der Grundstein für eine vertrauensvolle Zusammenarbeit.

Grundlegende Vertragsinhalte eines Geheimhaltungsvertrags sind unter anderem:

- Aufführung der Vertragsparteien
- Definition und Benennung der geheim zuhaltenden Informationen
- Punkte, welche nicht von der Geheimhaltung betroffen sind
- Ggf. Festlegung der Strafzahlung bei Nichteinhaltung der Geheimhaltung
- Dauer der Geheimhaltung

9.6.2 Auftragsverarbeitungsvertrag

Bei der Unterstützung bei einem IT-Sicherheitsvorfall ist es möglich, dass personenbezogene Daten durch den Vorfall-Experten eingesehen werden können oder Daten mit Personenbezug vom IT-Sicherheitsvorfall betroffen sind. Hieraus kann sich eine Verarbeitung im Auftrag gem. Art. 28 DSGVO ergeben. Es empfiehlt sich daher, eine Auftragsverarbeitung zu prüfen und einen Vertrag mit der oder dem Betroffenen zu vereinbaren.

Wichtige Inhalte eines Auftragsverarbeitungsvertrags sind unter anderem:

- Der Gegenstand und die voraussichtliche Dauer des Auftragsverarbeitungsverhältnisses
- Der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung
- Die Art der Daten und der Kreis der Betroffenen
- Die Rückgabe überlassener Daten und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags

Der Auftragsverarbeitungsvertrag kann von einer der beiden Parteien, den Betroffenen oder dem Vorfall-Experten, ausformuliert und bereitgestellt werden. Bei der Art der Daten und dem Kreis der Betroffenen sind allerdings die Betroffenen in der Pflicht, im Detail anzugeben, mit welchen personenbezogenen Daten der Vorfall-Experte in Berührung kommen könnte.

Die erforderlichen Inhalte eines Auftragsverarbeitungsvertrages werden in Art. 28 DSGVO thematisiert.

9.6.3 Kommunikationswege

Eine gute und schnelle Kommunikation zwischen dem Vorfall-Experten, den Betroffenen und den sonstigen beteiligten Parteien ist sehr wichtig. Daher sollten die Kommunikationswege vor Beginn einer Zusammenarbeit eindeutig festgelegt werden. Für den Vorfall-Experten ist es wichtig zu wissen, an welche Personen er sich wenden muss und wie er diese schnellstmöglich erreicht.

Bei der Auswahl der Kommunikationswege sollte die Möglichkeiten einer verschlüsselten Kommunikation berücksichtigt werden. Dies könnte bspw. über LTE-Systeme etabliert werden. Mit einer solchen Maßnahme, wird verhindert, dass der Angreifer Kenntnisse über die Kommunikationsinhalte zwischen Helfenden und Betroffenen erhält und so den Fortschritt der Analyse beobachten kann. Eine besondere Bedeutung kommt diesem Punkt zu, sofern es sich um sensible oder vertrauliche Daten und Informationen handelt und der Austausch über das Internet erfolgt. In erster Linie wird, abgesehen vom telefonischen Kontakt, die Kommunikation per E-Mail zum Einsatz kommen. Demzufolge ist gemeinsam mit den Betroffenen abzuwägen, ob eine Transportverschlüsselung als ausreichend erachtet wird oder ob eine Ende-zu-Ende-Verschlüsselung erforderlich ist.

Zuletzt ist ein möglicher Datenaustausch im Rahmen der Kommunikation zu betrachten. Ist es im Rahmen der Behandlung eines IT-Sicherheitsvorfalls notwendig, beispielsweise Dokumente oder Dateien auszutauschen, so sollte dies unter Berücksichtigung gewisser Sicherheitsaspekte erfolgen, um eine unbefugte Offenlegung zu vermeiden. Eine bewährte Methode ist die Verwendung einer Datenaustauschplattform, die eine verschlüsselte Übertragung gewährleisten kann.

9.6.4 Dokumentation

Ein wichtiger Bestandteil der Aufklärung eines IT-Sicherheitsvorfalls ist die bestmögliche Dokumentation des kompletten Prozesses bis zur Wiederherstellung des Normalzustands.

Die Dokumentation dient den folgenden Zwecken:

- Festhalten aller wichtigen Details rund um den IT-Sicherheitsvorfall.
- Festhalten aller Maßnahmen, welche im Rahmen der Aufklärung und Behebung eines IT-Sicherheitsvorfalls getroffen wurden.
- Nachbereitung eines IT-Sicherheitsvorfalls und Festlegung von Vorbeugemaßnahmen, um einen erneuten Vorfall zu verhindern.

Es empfiehlt sich, dass der Vorfall-Experte und die Betroffenen bereits vor der Zusammenarbeit die Form der Dokumentation abklären. Möglicherweise haben die Betroffenen bereits vorgegebene Formulare für die Dokumentation.

Darüber hinaus sollten bereits vorhandene Dokumente und Berichte berücksichtigt werden. Im Kontext der Vorfallbehandlung sind hierbei u. a. der Bericht von der Kontaktstelle des CSN und, sofern der Kontakt über einen Erst-Helfer erfolgte, dessen Dokumentation zu berücksichtigen.

9.6.5 Was kann nicht geleistet werden?

Vor dem Start einer Unterstützung seitens des Vorfall-Experten bei den Betroffenen sollte genau vereinbart werden, was geleistet werden kann und was nicht. Anhand dessen kann abgeschätzt werden, ob weitere Fachkräfte von Betroffenen oder zusätzlich externe Dienstleister hinzugezogen werden müssen.

10 Vor-Ort-Unterstützung: Vorfallbearbeitung (VE)

10.1 Einführung

Die Folgen eines Cyber-Angriffs können die Handlungsfähigkeit von Organisationen maßgeblich einschränken, indessen Folge ein hoher Schaden entstehen kann. Dieser lässt sich oftmals nur durch die Unterstützung durch Dritte minimieren.

Je nach Auswirkungen und Komplexität eines Cyber-Angriffs ist eine Vor-Ort-Unterstützung durch einen Vorfall-Experten unumgänglich. Somit kann die vor-Ort-Unterstützung bei der Behandlung von IT-Sicherheitsvorfällen eine entscheidende Rolle einnehmen.

10.2 Intention und Lernziele

Dieses Kapitel des Experten-Leitfadens behandelt die Handhabung eines IT-Sicherheitsvorfalls an der Lokation des Betroffenen. Einstiegspunkt ist dabei die Durchführung einer Analyse im Hinblick auf die Ermittlung der Ursache und der Nachvollziehbarkeit des Angriffsweges. Zudem wird die Planung der Vorgehensweise erörtert. Neben der Einrichtung eines Notbetriebes und der Bereinigung der Systeme befasst sich das Kapitel schließlich mit der Wiederherstellung der Systeme. Letztlich wird die Möglichkeit einer Nachbereitung erläutert.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:

 Eine Analyse des IT-Sicherheitsvorfalls durchzuführen.

 Abhängig von den Analyseergebnissen die Vorgehensweise zu planen.

 Die Sinnhaftigkeit eines Notbetriebes zu bewerten.

 Die betroffenen Systeme zu bereinigen und wiederherzustellen.

 Hinweise und Empfehlungen in Bezug auf eine Nachbereitung zu geben.

10.3 Analyse des IT-Sicherheitsvorfalls

Die Bewältigung eines IT-Sicherheitsvorfalls setzt eine genaue Analyse voraus. Die Tiefe der Analyse ist dabei von der Zielsetzung und den Vorgaben des Betroffenen abhängig. Wenn das Hauptziel des Betroffenen eine schnelle Wiederinbetriebnahme der betroffenen Systeme und der Auslöser für den IT-Sicherheitsvorfall bekannt oder nicht von großer Bedeutung ist, kann von einer tiefgründigen Analyse abgesehen werden.

Um angemessene und aussagefähige Analyseergebnisse erzielen zu können, ist es für den Vorfall-Experten von Bedeutung, dass qualifizierte Ansprechpartnerinnen und Ansprechpartner zur Verfügung stehen und unterstützend tätig sind. Diese bilden wiederum das Notfall-Team zur Behandlung des IT-Sicherheitsvorfalls.

10.3.1 Tiefgründige Analyse

Eine tiefgreifende Analyse kann beispielsweise eine Pflichtvorgabe einer abgeschlossenen IT-Sicherheitsrisikoversicherung (siehe auch 6.2.5.3. Versicherungen) sein. Je tiefgründiger die Analyse eines IT-Sicherheitsvorfalls sein soll, umso vorsichtiger muss mit den betroffenen Systemen umgegangen werden.

Die falsche Wahl der Abschaltung eines betroffenen Systems kann den Verlust wichtiger Daten bedeuten, welche für eine forensische Aufklärung notwendig wären. In diesem Zusammenhang wird von flüchtigen und nichtflüchtigen Daten (siehe dazu auch 4.5.1 ff.) gesprochen. Die nichtflüchtigen Daten bleiben auch nach der Abschaltung eines Systems erhalten, da sie sich auf einem Massenspeicher, wie beispielsweise einer Festplatte, befinden. Flüchtige Daten gehen mit der Systemabschaltung verloren, da sie sich u.a. im Arbeitsspeicher oder in Registern des Prozessors bzw. Peripheriegeräten befinden.

Ist eine tiefgreifende Analyse gefordert, sollten diese Bereiche vorab für eine spätere Auswertung gesichert werden. Der Zugriff auf nichtflüchtige Daten sollte dabei nur in einem lesenden Modus erfolgen. Allein durch das Hoch- und Herunterfahren eines Betriebssystems oder Hintergrundvorgänge von Anwendungen und Diensten können wichtige Dateien verändert oder mit einem neuen Zeitstempel versehen werden.

Um das Beschreiben von Datenträgern zu verhindern, empfiehlt sich der Einsatz von Hardwarebasierten Schreibblockern. Ein Schreibblocker filtert die Schreibzugriffe auf Datenträger heraus und lässt lediglich Lesezugriffe zu. Somit ist eine Verfälschung von Daten ausgeschlossen. Es sei aber auch darauf hingewiesen, dass bestimmte Zugriffe Angreifer alarmieren können.

10.3.2 Identifikation betroffener Systeme

Bei der Analyse eines IT-Sicherheitsvorfalls sollten zunächst alle betroffenen Systeme ausfindig gemacht werden. Auch wenn der Betroffene nur von bestimmten Systemen ausgeht, gilt es zu untersuchen, ob eine weitere Verbreitung stattgefunden hat. Alle Auffälligkeiten gilt es zu beobachten und die Beschäftigten beim Betroffenen sollten jede Unregelmäßigkeit melden. Nur wenn alle betroffenen Systeme behandelt werden, kann eine komplette Bereinigung des IT-Sicherheitsvorfalls erfolgen.

10.3.3 Analyse des Auslösers

Für den Betroffenen und Vorfall-Experten ist es gleichermaßen von großer Bedeutung, den Auslöser des IT-Sicherheitsvorfalls möglichst genau zu bestimmen, um im Nachhinein geeignete Maßnahmen festlegen zu können, welche die Gefahr eines ähnlichen IT-Sicherheitsvorfalls für die Zukunft möglichst verhindert.

Typische Auslöser für einen IT-Sicherheitsvorfall:

- Schadprogramme (beispielsweise über E-Mail-Phishing oder sonstige Quellen aus dem Internet)
- Veraltete Betriebssysteme oder Applikationen
- Unzureichend geschützte stationäre oder mobile Geräte
- Unzureichender Netzwerkschutz

Oftmals sind auch die Beschäftigten des Betroffenen in den IT-Sicherheitsvorfall involviert oder der Auslöser des IT-Sicherheitsvorfalls. Von diesen Personen sollte möglichst detailgetreu der Hergang des IT-Sicherheitsvorfalls beschrieben werden.

10.3.4 Schadensfeststellung

Über die Schadensfeststellung soll ermittelt werden, welche negativen Veränderungen der IT-Sicherheitsvorfall auf die IT-Systeme hatte und welche Daten betroffen sind. Hier gilt es, eng mit dem oder den Betroffenen zusammenzuarbeiten, um Abweichungen vom Normalzustand festzustellen.

Mögliche Fragestellungen bei der Schadensfeststellung:

- Sind Daten verloren gegangen?
- Sind Veränderungen am Betriebssystem oder an Applikationen vorgenommen worden?
- Sind bestimmte Dienste nicht mehr funktionstüchtig?
- Ist der Zugriff auf Dateien, Dienste oder Applikationen gesperrt?
- Könnten Kundinnen und Kunden oder sonstige Dritte betroffen sein?
- Ist mit weiteren Folgeschäden zu rechnen?

Alle festgestellten Schäden sind zu dokumentieren. Im Anschluss geht es darum, die finanziellen Auswirkungen möglichst genau zu beleuchten. Diesbezüglich ist es sehr wichtig, potenzielle Schadensketten genauestens zu betrachten, um weitere schädliche Auswirkungen möglichst ausschließen zu können. Werden die finanziellen Auswirkungen schließlich auf die betroffenen Systeme reflektiert, so kann dies einen guten Ansatz hinsichtlich einer Priorisierung der weiteren Tätigkeiten darstellen.

10.4 Planung der Vorgehensweise

Nachdem ein IT-Sicherheitsvorfall eindeutig identifiziert wurde, gilt es die weitere Vorgehensweise detailliert zu planen und gemeinsam mit den Betroffenen eine Strategie festzulegen. Durch eine fehlerhafte Behandlung des IT-Sicherheitsvorfalls kann das Schadensausmaß erhöht werden, anstatt die Auswirkungen einzudämmen. Um das zu verhindern und ungewollte Ereignisse während der Behandlung des IT-Sicherheitsvorfalls zu vermeiden, ist eine gründliche Planung der weiteren Vorgehensweise unabdingbar.

Da die Dauer der Behandlung eines IT-Sicherheitsvorfalls aber ebenfalls ein Indikator für das letztendlich entstandene Schadensausmaß eines Cyberangriffs sein kann, ist es ebenso wichtig abzuwägen, wie viel Zeit in die Planung der Vorgehensweise investiert werden sollte. Mit der richtigen Planung erscheint der zeitliche Aufwand zunächst zwar höher, es können aber potenzielle Probleme, Diskussionen und Unklarheiten während der Behandlung des IT-Sicherheitsvorfalls vermieden oder zumindest reduziert werden.

Es ist nicht möglich pauschal festzulegen, wie viel Aufwand in Planung investiert und wie tief diese Planung sein soll. Das kann sich von Fall zu Fall unterscheiden. Es kommt hierbei unter anderem auf Faktoren wie Umfang und Komplexität des IT-Sicherheitsvorfalls, Intentionen des Betroffenen, aber auch wie konkret die Analyse durchgeführt werden konnte, an.

Die nachstehenden Fragestellungen bieten verschiedene Anhaltspunkte bei der Planung der weiteren Vorgehensweise an und können diesbezüglich sehr hilfreich sein.

Nr.	Fragestellung
1.	Sind die personellen Ressourcen für das Notfall-Team angemessen?
2.	Wie detailliert konnte der Vorfall analysiert werden (Aussagekräftige Ergebnisse; nachvollziehbar, welche Systeme betroffen sind)?
3.	Sind die Intentionen und Zielvorstellungen der Betroffenen geklärt?
4.	Ist die Einrichtung eines Notbetriebes sinnvoll möglich und notwendig?
5.	Ist die Priorisierung der Systeme bzgl. der Bereinigung und Wiederherstellung anhand der Analyseergebnisse hinreichend?
6.	Gibt es Systemabhängigkeiten, welche zu berücksichtigen sind?
7.	Gibt es sonstige Besonderheiten der betroffenen Systemlandschaft?
8.	Werden weitere Personen (z.B. Dienstleister) zur Behandlung des IT-Sicherheitsvorfalls benötigt?

Tabelle 6: Fragestellungen zur Planung der Vorgehensweise

10.5 Notbetrieb

Abhängig von den Auswirkungen eines IT-Sicherheitsvorfalls im Hinblick auf die betroffenen Systeme besteht die Möglichkeit, kurzfristig einen Notbetrieb einzurichten. Unter dem Begriff Notbetrieb wird ein auf die kritischen Geschäftsprozesse eingeschränkter Alternativbetrieb verstanden. Ziel ist es dabei, die Kernprozesse weitestgehend aufrechtzuerhalten, um auf diese Weise einen vollständigen Stillstand zu vermeiden.

Um einen möglichen Notbetrieb sinnvoll zu gestalten, gilt es ein vordefiniertes Mindestniveau zu erfüllen. Das Mindestniveau bezieht sich dabei auf die erforderlichen Ressourcen und Kapazitäten, die für einen vorübergehenden Notbetrieb im Vergleich zum Normalbetrieb mindestens benötigt werden, um diesen sinnvoll gestalten zu können. Dies ist zunächst unabhängig von der Realisierungsform eines Notbetriebes.

Die nachfolgend aufgeführten Ressourcen sind dabei zu berücksichtigen und im Hinblick auf die erforderlichen Mindestvoraussetzungen zu bestimmen:

- Personal
- Informations- und Kommunikationstechnik
- Infrastruktur
- Informationen und Betriebsmittel

Auf der Webseite des BSI können umfangreiche Informationen für den Bereich Notbetrieb gefunden werden.

Für weiterführende Informationen kann zum einen der BSI-Standard 100-4: Notfallmanagement sowie das entsprechende Umsetzungsrahmenwerk zum Notfallmanagement vom BSI herangezogen werden. Darin werden u. a. umfangreiche Informationen zu dem Bereich Notbetrieb behandelt.

Der BSI-Standard 100-4 wird derzeit jedoch vom BSI überarbeitet.

10.5.1 Prüfung

Inwieweit ein Notbetrieb nach einem Cyber-Angriff möglich und auch sinnvoll ist, hängt von dem zugrundeliegenden IT-Sicherheitsvorfall ab. Ausgangspunkt ist hierbei das Ergebnis der Analyse des IT-Sicherheitsvorfalls.

Unter Betrachtung der betroffenen bzw. infizierten Systeme gilt es, gemeinsam mit den Betroffenen zu beurteilen, ob die kritischen Geschäftsprozesse in einem reduzierten Betrieb aufrechterhalten werden können.

Diesbezüglich ist es zunächst erforderlich, für die jeweiligen Kernprozesse die Mindestanforderungen der benötigten Ressourcen in Bezug auf die IT-Systeme zu bestimmen. Anschließend muss auf Basis der Analyseergebnisse ein Abgleich durchgeführt werden, inwiefern die zuvor ermittelten Systeme, welche für den Notbetrieb benötigt werden, von den Auswirkungen des IT-Sicherheitsvorfalls betroffen sind.

Kann hierbei das vordefinierte Mindestniveau erfüllt werden, ist ein Notbetrieb möglich und sollte durch das Notfall-Team des Betroffenen in Abstimmung mit dem Vorfall-Experten eingerichtet werden.

Ist eine Erfüllung der Mindestanforderungen nicht gegeben, sollte von der Einrichtung eines Notbetriebes abgesehen werden, um eine weitere Ausbereitung zu verhindern.

10.5.2 Herstellung des Notbetriebes

Zur Herstellung eines vorübergehenden Notbetriebs aufgrund eines IT-Sicherheitsvorfalls wird im nachfolgenden zwischen zwei grundlegenden Methoden unterschieden:

- Isolierung aller infizierten Systeme aus dem Netzwerk
- Verlagerung der nicht betroffenen Systeme in ein neues Netzwerk

Gemeinsam mit dem Notfall-Team sind die Methoden durchzusprechen, um unter Berücksichtigung des Realisierungsaufwands und des Restrisikos hinsichtlich einer weiteren Ausbreitung eine Entscheidung treffen zu können, ob im Rahmen der Herstellung eines Notbetriebes eher eine Isolierung der infizierten Systeme oder eine Verlagerung der nicht betroffenen Systeme in Frage kommt.

Ein weiterer, nicht zu vernachlässigender Punkt beschäftigt sich mit der Rückführung zum Normal- bzw. Regelbetrieb. Während der Einrichtung eines Notbetriebes sollte immer die Wiederherstellung des Normalbetriebs betrachtet werden, um den Notbetrieb so kurz wie möglich zu gestalten.

Nach Ausarbeitung der Lösungsalternativen bei dem Aufbau eines Notbetriebes ist zur endgültigen Entscheidungsfindung die Geschäftsführung zu beteiligen, bevor die Umsetzung letztlich erfolgt.

In den nachfolgenden Abschnitten werden beide Methoden in Bezug auf die Vorgehensweise bei der Umsetzung näher erläutert.

10.5.2.1 Isolierung

Im Rahmen der Isolierung werden alle Systeme aus dem Produktivnetz selektiert, bei denen der Verdacht besteht, von dem IT-Sicherheitsvorfall betroffen zu sein. Durch die Isolierung wird eine weitere Ausbreitung auf andere Systeme im Netz unterbunden.

Wurden alle potenziell infizierten Systeme vom Produktivnetz separiert, können die übrigen Systeme im Rahmen eines Notbetriebes eingesetzt werden.

10.5.2.2 Verlagerung

Bei der Verlagerung werden im Gegensatz zu der Isolierung alle nicht betroffenen bzw. infizierten Systeme betrachtet. Grundlage dieser Methode ist der Aufbau eines neuen Netzes neben dem eigentlichen Produktivnetz, durch das der Notbetrieb realisiert wird. Wichtig ist, dass die Netze ordnungsgemäß voneinander abgeschottet werden, um eine erneute Ausbreitung zu verhindern.

Letztlich können alle Systeme umgezogen bzw. verlagert werden, bei welchen eine Infizierung zweifelsfrei ausgeschlossen werden kann. Nach erfolgter Verlagerung sind die entsprechenden Systeme innerhalb eines Notbetriebes nutzbar.

Eine Verlagerung stellt im entfernten Sinne eine alternative Möglichkeit der Isolierung dar.

10.6 Bereinigung der Systeme

Die Bereinigung von infizierten Systemen infolge eines Cyber-Angriffs nimmt im Kontext der Reaktion auf IT-Sicherheitsvorfälle eine entscheidende Rolle ein. Hintergrund ist, dass erst nach einer vollständigen Bereinigung eine Wiederherstellung möglich ist und die betroffenen Systeme wieder nahezu gefahrlos verwendet werden können. Die Formulierung „gefahrlos“ ist in diesem Zusammenhang mit Vorsicht zu betrachten, da nicht zweifelsfrei davon ausgegangen werden kann, dass alle Zugangswege ermittelt wurden, welche die Kommunikationswege betreffen oder dass die Infektionen des Schadprogramms (z. B. unerkannte Hintertüren) nicht vollständig beseitigt ist. Je nach Komplexität der Angriffsform besteht hierbei immer ein gewisses Restrisiko.

Neben der Gefahr einer unvollständigen Bereinigung gibt es weitere Gefährdungen, die zu berücksichtigen sind. Darunter fällt beispielsweise die Vernichtung von Beweisen, der Datenverlust oder auch der Ausfall von IT-Systemen.

Grundlage für die Bereinigung sind die Ergebnisse der Vorfallanalyse. Diese dienen einerseits der Rückverfolgung und somit der Bereinigung der Systemlandschaft und andererseits der Anpassung von Abwehrmaßnahmen, um gleichartige Angriffe zukünftig zu vermeiden.

Unter Berücksichtigung der Aussagefähigkeit der Analyseergebnisse hinsichtlich der genauen Ermittlung der Ursache kann die Bereinigung angestoßen werden. Hierbei kann wiederum zwischen zwei grundlegenden Vorgehensweisen unterschieden werden:

- Bereinigung durch Beseitigung des Schadprogramms bzw. schadhafte Dateien
- Bereinigung durch Neuinstallation des Betriebssystems

Die Wahl des Vorgehens ist von dem Resultat der Vorfallsanalyse abhängig. Demzufolge kommt die Bereinigung durch die Beseitigung des Schadprogramms inklusive der Infektionen, Kommunikationswege und Hintertüren ausschließlich dann in Frage, wenn die Ursache bzw. der Angriffsweg in notwendiger Tiefe ermittelt und nachvollzogen werden konnte.

Bestehen bei der Aussagefähigkeit der Analyseergebnisse Bedenken oder konnte die Vorfallsanalyse keine hinreichenden Resultate liefern, sollte die Wahl der Vorgehensweise auf die Bereinigung durch eine Neuinstallation des Betriebssystems fallen.

Letztlich obliegt diese Entscheidung den Betroffenen. Unter Abwägung des zugrundeliegenden IT-Sicherheitsvorfalls sind die verschiedenen Möglichkeiten hinsichtlich der Vor- und Nachteile zusammen mit dem Notfall-Team und der Geschäftsführung durchzusprechen, um dann eine geeignete Entscheidung zu treffen.

10.6.1 Beseitigung des Schadprogramms

Im Rahmen der Beseitigung wird der Ansatz verfolgt, das Schadprogramm von den infizierten bzw. kompromittierten IT-Systeme vollständig und korrekt zu entfernen. Diesbezüglich gilt es, den Einbruchsweg genauestens nachzuvollziehen, um alle schadhaften Dateien wirksam zu löschen sowie die Zugangswege und Kommunikationsmöglichkeiten zu schließen. Darüber hinaus werden potenzielle Hintertüren ausgemacht, um den Angreifenden in letzter Konsequenz auszusperren. Nach abgeschlossener Beseitigung sollte geprüft werden, ob die Systeme optimiert bzw. gehärtet werden können. Zudem sind alle verfügbaren Updates, Patches und Treiber für das Betriebssystem und die verwendete Software zu installieren.

Zusätzlich ist es bei dieser Variante empfehlenswert, die relevanten IT-Systeme gezielt zu überwachen, um die Gefährdung von erkannten Hintertüren zu reduzieren. Die Initiative der Überwachung kann vom Vorfall-

Experten angestoßen werden, ist jedoch durch den Betroffenen zu realisieren. Ein genauer Mindestzeitraum kann dabei nicht pauschalisiert werden. Dies ist abhängig vom vorliegenden IT-Sicherheitsvorfall. Empfehlenswert, auch in Bezug auf präventive Maßnahmen, ist es, eine dauerhafte Lösung zu implementieren, mit welcher die Systemlandschaft wirksam überwacht werden kann.

10.6.2 Neuinstallation des Betriebssystems

Bei der Neuinstallation werden die betroffenen Systeme neu aufgesetzt. In diesem Kontext wird das entsprechende Betriebssystem neu installiert. Dabei werden alle sich auf dem System befindlichen Daten gelöscht und vorgenommene Einstellung zurückgesetzt. Auch hier ist es notwendig, verfügbare Updates und Patches für das Betriebssystem und die Anwendungssoftware unmittelbar im Anschluss zu installieren.

Bevor jedoch die Neuinstallation durchgeführt wird, ist es empfehlenswert zu prüfen, ob eine saubere, integre Datensicherung vorhanden ist. Zudem sollten potenziell wichtige Daten, welche sich auf den betroffenen Systemen befinden, gesichert werden. Diese können jedoch nicht ohne eine weitere Überprüfung verwendet werden, da diese vom Schadprogramm betroffen sein können. Demzufolge sind solche Daten in einer gesicherten Umgebung auf mögliche Veränderungen zu untersuchen, bevor eine Wiederverwendung in Frage kommt. Auf diese Weise kann der Datenverlust möglichst geringgehalten werden.

Im Anschluss kann das System neu aufgesetzt werden. Dadurch kann ein erneuter Befall durch mögliche Hintertüren im Grunde ausgeschlossen werden. Ist die Neuinstallation abgeschlossen, können vorhandene Sicherungskopien des Datenbestands wiederhergestellt werden. Bevor diese wieder eingespielt werden, ist sicherzustellen, dass dadurch keine manipulierten Daten oder Programme auf das neu installierte IT-System übertragen werden.

10.7 Wiederherstellung der Systeme

Nachdem die von dem Cyber-Angriff betroffenen Systeme ordnungsgemäß und erfolgreich bereinigt wurden, können diese wieder in den Produktivbetrieb überführt werden. Diesbezüglich sollte eine geordnete Reihenfolge bestimmt werden, die sich an der Priorität des jeweiligen Systems orientiert. Dabei gilt es zudem, mögliche Systemabhängigkeiten zu beachten, die bei der Wiederherstellung bzw. dem Wiederanlauf eine nicht zu vernachlässigende Rolle spielen. Im Falle einer Nichtbeachtung der richtigen Abfolge beim Hochfahren der Systeme kann es zu Beeinträchtigungen in der Funktionsweise kommen.

Im Falle, dass ein Notbetrieb zeitweise eingerichtet wurde, gilt es die Rückführung in den Normalbetrieb anzustoßen. Wurde der Notbetrieb durch die Isolierung realisiert, so sind die bereinigten Systeme in das Produktivnetz zurückzuführen. Bei einer durchgeführten Verlagerung bietet es sich an, die Systeme in das neu aufgesetzte Netz zu überführen und dieses weiter als Produktivnetz zu nutzen.

10.8 Nachbereitung

Die Nachbereitung eines IT-Sicherheitsvorfalls und dessen Bearbeitung ist ein wichtiger Bestandteil zum Abschluss der Vorfallbearbeitung und dient der Auswertung und Verbesserung. Dazu sollte ein Abschlussgespräch mit den Betroffenen gehalten werden. Somit lassen sich Prozesse rund um die Vorfallbearbeitung optimieren und Abhilfemaßnahmen für potenzielle IT-Sicherheitsvorfälle in der Zukunft treffen. Im Zuge dessen sind alle Handlungen, Entscheidungen und Dokumentationen zu berücksichtigen.

Dies ist zum einen für den Betroffenen wichtig, zum anderen auch für die eigenen Vorgehensweisen als Vorfall-Experte. Mit jedem IT-Sicherheitsvorfall lernen beide Parteien dazu und können die notwendigen Schlussfolgerungen ziehen.

Beispiele für mögliche Fragestellungen:

- Wie schnell wurde der IT-Sicherheitsvorfall erkannt und behoben?
- Haben die Meldewege funktioniert?

- Welche kurz- und langfristigen Maßnahmen müssen ergriffen werden?
- Was ist im Prozess der Vorfallbearbeitung gut gelaufen?
- Wo gibt es Verbesserungsbedarf im Prozess der Vorfallbearbeitung?
- Welche Sicherheitsmaßnahmen könnten verbessert werden?
- Welche Schulungs- und Sensibilisierungsmaßnahmen müssen angestoßen werden?

Die Ergebnisse der Nachbereitung sollten dokumentiert werden.

11 Nach einem Vorfall ist vor einem Vorfall (VP&VE)

11.1 Einführung

Informationstechnik und digitale Infrastrukturen gehören heute in so gut wie allen Geschäftsbereichen zur täglichen Routine. Unabhängig von der Größe einer Institution sind diese auf funktionierende IT-Systeme, cloudbasierte Lösungen und interne, digitale Vernetzung angewiesen. Betriebsstörungen der IT durch Cyber-Angriffe bringen infolgedessen immer unschöne Folgen mit sich und können sogar einen kompletten Stillstand bedeuten.

In Anbetracht der steigenden Abhängigkeit von der Informationstechnik und den zunehmenden Möglichkeiten von Cyber-Kriminellen ist es heutzutage unabdingbar, Strategien zu entwickeln, um Angriffe wirksam zu erkennen und angemessen behandeln zu können.

Eine effiziente Reaktion auf IT-Sicherheitsvorfälle sowie Krisensituationen nimmt unter dem fortschreitenden Stand der Technik eine essenzielle Rolle ein. Eine entscheidende Aufgabe hat diesbezüglich die Implementierung von Vorsorgemaßnahmen.

11.2 Intention und Lernziele

Dieses Kapitel des Leitfadens beschäftigt sich mit dem Aufarbeiten eines vergangenen Vorfalls hinsichtlich der Vorbereitung auf künftige Vorfälle. Es wird darauf abgezielt, Opfer von Cyber-Angriffen für präventive Maßnahmen zu sensibilisieren bzw. den Stellenwert der Prävention darzustellen. Weiterhin wird die Geschäftsprozessanalyse thematisiert und zuletzt die Relevanz sowie der Mehrwert von Übungen dargestellt.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmerinnen und Schulungsteilnehmer in der Lage:


Betroffene über die Bedeutung der Prävention in Bezug auf Cyber-Angriffe aufzuklären.


Präventive Maßnahmen beispielhaft aufzuführen.


Hinweise zur Umsetzung zu geben, welche die Reaktion auf Vorfälle optimieren können.

11.3 Sensibilisierung für Prävention

Die Prävention ist ein entscheidender Tätigkeitsbereich, um über mögliche Cyber-Angriffe und IT-Sicherheitslücken aufzuklären. In Bezug auf die steigenden Anforderungen, die auf eine Organisation und deren IT-Betrieb einwirken, ist es wichtig sich über die unterschiedlichen Angriffsformen und Maßnahmen zu informieren. Mit der Prävention kann so ein tatsächlicher und effektiver Schutz erreicht werden.

Je komplexer der Aufbau der IT-Infrastruktur ist, desto wichtiger ist die Umsetzung von Präventionsmaßnahmen. Die rechtzeitige Entwicklung und folgerichtige Umsetzung einer IT-Security-Strategie durch Vorsorgemaßnahmen ist enorm gewinnbringend, um angemessen auf IT-Sicherheitsvorfälle reagieren und die Auswirkungen frühzeitig eindämmen zu können.

Die Erkenntnis, dass Cyber-Angriffe niemals zu 100 % unterbunden und verhindert werden können, ist in diesem Kontext sehr wichtig und in einem gewissen Maße erforderlich.

Der Aufbau einer wirkungsvollen Sicherheitsstrategie betrachtet dabei zwei grundlegende Bereiche. In erster Linie geht es um die IT-Systemlandschaft hinsichtlich der eingesetzten Hard- und Software. Ein weiterer wichtiger Bereich bzw. Faktor, der oftmals nicht hinreichend berücksichtigt wird, stellen die Mitarbeiter dar.

In den nachfolgenden Abschnitten wird kurz aufgezeigt, inwiefern präventive Maßnahmen sowohl vor als auch nach einem Vorfall umgesetzt werden können. Es handelt sich dabei jedoch nur um einen kleinen Bereich der möglichen Maßnahmen, die bezüglich der Prävention in Betracht gezogen werden können.

Um hierbei einen ganzheitlichen Ansatz zu verfolgen, ist die IT-Grundschutz-Methodik oder auch die DIN ISO/IEC 27001 in Verbindung mit der DIN ISO/IEC 27002 ein bewährtes Mittel.

11.3.1 IT-Systemlandschaft

Da die IT-Systemlandschaft die Basis im Kontext der Realisierung der Geschäftsprozesse darstellt, ist es wichtig die eingesetzte Informationstechnik angemessen abzusichern. Verdeutlicht wird dieser Sachverhalt durch die Tatsache, dass aufgrund der wachsenden Vernetzung jedes System ein potenzielles Angriffsziel und Einfallstor für Cyberkriminelle abbildet.

11.3.2 Systemhärtung

Es ist erforderlich, die IT-Systeme gezielt zu härten. Ziel dabei ist es, mögliche Einfallstore wirksam vor unautorisierte Zugänge und Zugriffe zu schützen sowie eine Ausbreitung im internen Netz zu verhindern oder weitestgehend zu erschweren.

Die Härtung von einzelnen IT-Systemen bis hin zur gesamten IT-Systemlandschaft kann durch eine Vielzahl von Möglichkeiten realisiert werden. Die Auswahl der Maßnahmen ist dabei von den zum Einsatz kommenden Systeme nund dem Aufbau der Netzwerkinfrastruktur abhängig. Zudem sollten die Techniken von Angreifenden bekannt sein und berücksichtigt werden.

Unter Betrachtung der jeweiligen Umgebung gilt es ,die Härtungsmaßnahmen individuell zu wählen und den Gegebenheiten anzupassen. Nachfolgend werden grundlegende Beispiele aufgeführt:

- Segmentierung unterschiedlicher Netzwerkbereiche
- Anpassung des Berechtigungssystems
- Verwendung von Verschlüsselungsmethoden
- Entfernung/Deaktivierung nicht benötigter Software/Dienste
- Absicherung von externen Zugängen

11.3.3 Schwachstellenmanagement

Um sich Zugang zur IT-Infrastruktur zu verschaffen, nutzen Angreifende i. d. R. offene Schwachstellen oder Sicherheitslücken aus, die aufgrund einer mangelnden Absicherung übersehen und nicht beseitigt wurden.

Angrenzend an die Härtung der IT-Systemlandschaft ist es sehr sinnvoll, ein Schwachstellenmanagement aufzubauen. Die Kernaufgabe ist es, die Systeme regelmäßig auf technische Schwachstellen und Sicherheitslücken zu prüfen sowie diese zu erkennen und zu beseitigen – bevor ein Angreifender diese ausnutzen kann.

Dies kann auf der einen Seite manuell durch dafür qualifizierte Personen erfolgen, was sich jedoch unter Betrachtung des Aufwands nur für kleinere Organisationen empfiehlt.

Die andere Möglichkeit erfolgt automatisiert unter Zuhilfenahme eines entsprechenden Tools. Dieses scannt die IT-Systemumgebung und identifiziert offene Schwachstellen und Sicherheitslücken.

Unabhängig davon, ob eine manuelle oder automatisierte Variante gewählt wird, ist es zudem zweckmäßig, sich über geeignete Kanäle Informationen zu aktuellen Schwachstellenmeldungen einzuholen und diese in das IT-Management einfließen zu lassen. Diese können dabei direkt vom Hersteller oder auch speziellen CERTs stammen.

Die Etablierung eines wirksamen Schwachstellenmanagements sollte mit dem Patch- und Änderungsmanagement einhergehen. Während im Rahmen des Schwachstellenmanagements die Komponenten auf Sicherheitslücken und Schwachstellen untersucht werden, sorgt das Patch- und Änderungsmanagement durch die Verteilung von Aktualisierungen und Patches dafür, dass erkannte Lücken gezielt geschlossen werden. Mit dem Patch- und Änderungsmanagement gehen aber auch organisatorische Maßnahmen, wie beispielsweise begleitende und nachhaltige Kontrollen und Protokollierungen, einher.

Neben der regelmäßigen Schwachstellenanalyse kann durch die Realisierung eines Penetrationstests die Sicherheit der IT-Systeme zusätzlich erprobt und ebenso die Wirksamkeit von Härtungsmaßnahmen überprüft werden. Bei einem Penetrationstest werden Techniken und Methoden verwendet, die ein reales Angriffsszenario darstellen, um einen unautorisierten Zugang auf die Unternehmensressourcen zu erlangen. Ziel ist es dabei, ähnlich wie bei einem Schwachstellen-Scan, die Anfälligkeit gegen Cyber-Angriffe zu überprüfen und zu verringern.

11.3.4 Mitarbeitende

Neben dem Einfallstor vorhandener Schwachstellen oder Sicherheitslücken in die IT-Infrastruktur, erhalten Angreifende nicht selten aufgrund einer menschlichen Fehlhandlung Zugang zu den Systemen. Grund dafür ist ein fehlendes Sicherheitsbewusstsein und nicht regelmäßige Sensibilisierungskampagnen rund um Themen der Informationssicherheit bei Mitarbeiterinnen und Mitarbeitern.

Da der Faktor Mensch neben der IT das größte Risiko für die Sicherheit darstellt, ist es erforderlich, die Mitarbeiterinnen und Mitarbeiter für mögliche Bedrohungen und Gefährdungen zu schulen und zu sensibilisieren. Auf diese Weise soll ein angemessenes Sicherheitsbewusstsein geschaffen werden, um potenzielle Bedrohungen frühzeitig zu erkennen und abzuwehren bzw. die Folgen weitestgehend gering zu halten.

Ziel von Schulungs- und Sensibilisierungsmaßnahmen ist es, ein grundlegendes Verständnis rund um die Themen der Informationssicherheit herzustellen. Im Zuge dessen gilt es, die Mitarbeiterinnen und Mitarbeiter über die aktuelle Bedrohungslage, insbesondere durch Cyber-Angriffe, aufzuklären und das erforderliche Wissen zu vermitteln, wie diese sich beim Umgang mit Sicherheitsbedrohungen zu verhalten haben.

Im nachfolgenden wird eine beispielhafte Auswahl von grundlegenden Themen aufgeführt, die Teil einer Schulung sein können:

- Typische Angriffsformen
- Gefahren von und Umgang mit E-Mails
- Gefahren der Internetnutzung
- Umgang mit Passwörtern
- Verhalten bei sicherheitsrelevanten Ereignissen

Die Schulungsinhalte sollten sich dabei immer an der aktuellen Bedrohungslage orientieren.

Bei der Durchführung von Schulungs- und Sensibilisierungsmaßnahmen kann auf verschiedene Methoden zurückgegriffen werden. Die Wesentlichen stellen hierbei einerseits die Präsenzschulung und andererseits die Online-Schulung dar.

11.4 Aufbau eines Sicherheitsbewusstseins

Um die Informationssicherheit wirkungsvoll und gewinnbringend umzusetzen, ist es erforderlich, die Beschäftigten bzw. den „Faktor Mensch“ als bedeutendes Kriterium zu betrachten. Erst wenn die Beschäftigten erkennen, welche wichtige Rolle sie selbst spielen und dazu bereit sind die notwendigen Sicherheitsmaßnahmen wirksam zu unterstützen, kann von einem ganzheitlichen Informationssicherheitsansatz gesprochen werden.

Um dies gewährleisten zu können, ist es erforderlich, ein angemessenes Sicherheitsbewusstsein aufzubauen und auf diese Weise die Sicherheitskultur voranzutreiben. Infolgedessen gilt es, die Mitarbeiterinnen und Mitarbeiter für maßgebliche Gefährdungen zu sensibilisieren, um so eine breite Akzeptanz für die ergriffenen Maßnahmen zu erzielen – auch wenn diese Komfort- oder Funktionseinbußen mit sich bringen.

Der Aufbau eines adäquaten Bewusstseins für Informationssicherheit erfordert gleichermaßen Schulungs- und Sensibilisierungsmaßnahmen. Schulungen zielen dabei auf die grundlegende Wissensvermittlung der nötigen Kenntnisse und Fähigkeiten für ein sicherheitsbewusstes Verhalten ab, wohingegen Sensibilisierungen eine Schärfung der Wahrnehmung für sicherheitsrelevante Situationen und die möglichen Auswirkungen vermitteln.

Ein anhaltend, effizientes Informationssicherheitsniveau ist nur dann möglich, wenn die Beschäftigten die Informationssicherheit als selbstverständlichen Teil des Arbeitsumfelds ansehen und im Arbeitsalltag ohne zusätzliche Aufforderung oder Kontrollen praktizieren. Der Aufbau eines konsistenten Sicherheitsbewusstseins, welches nachhaltige Ergebnisse erzielen soll, setzt einen kontinuierlichen Prozess voraus. Demzufolge ist es erforderlich, ein durchgängiges Schulungs- und Sensibilisierungsprogramm aufzubauen, um für eine Akzeptanz im Bereich der Informationssicherheit zu sorgen.

Das Schulungs- und Sensibilisierungsprogramm ist dabei unter Berücksichtigung bereits vorhandener Maßnahmen auf die Institution zuzuschneiden. Ein entscheidender Punkt ist dabei die Bildung zielgruppenspezifisch geeigneter Inhalte für Sensibilisierungs- und Schulungsmaßnahmen sowie die angemessene Vermittlung dieser Inhalte.

Als Orientierung kann an dieser Stelle auf den IT-Grundschutz-Baustein ORP.3 Sensibilisierung und Schulung sowie den zugehörigen Umsetzungshinweis zum Baustein ORP.3 Sensibilisierung und Schulung zurückgegriffen werden. Der Baustein und die dazugehörenden Umsetzungshinweise behandeln im Wesentlichen die effiziente Gestaltung eines Vorgehens im Bereich der Schulung und Sensibilisierung der Beschäftigten.

11.5 Analyse von Geschäftsprozessen

Die Gewährleistung der Geschäftsprozesse in widrigen Situationen ist für jede Organisation von elementarer Bedeutung. Kommt es aufgrund von Cyber-Angriffen zu Störungen in der IT, kann dies im schlimmsten Fall sämtliche Prozesse und somit den gesamten Betrieb zum Stillstand bringen. Die Folgen sind mit wirtschaftlichen Schäden und mit einem möglichen Reputationsverlust verbunden.

Um einen andauernden Stillstand des Betriebs zu vermeiden, ist es erforderlich, die Geschäftsprozesse hinsichtlich der Kritikalität zu analysieren und zu bewerten. Ziel dabei ist es, die Kernprozesse zu identifizieren, welche zur Erreichung der Geschäftsziele zwingend benötigt werden.

Um eine solche Analyse zielführend durchführen zu können, wird eine möglichst vollständige und aktuelle Übersicht der betrachteten Prozesse benötigt. Anschließend ist es erforderlich, diese im Hinblick auf den Schaden zu untersuchen, der bei einer Unterbrechung entstehen würde. Die Untersuchungsergebnisse können wiederum als Maßstab im Hinblick auf die Bewertung der Kritikalität verwendet und daraus eine Priorisierung abgeleitet werden. Letztlich sollten von ermittelten kritischen Geschäftsprozessen die Verbindung zu den benötigten IT-Systemen hergestellt werden, um hierbei ebenso eine Priorisierung abzuleiten. Ebenfalls dienen die Analyseergebnisse der kritischen Geschäftsprozesse dazu, eine Schutzbedarfsfeststellung und Risiko- sowie Gefährdungsbetrachtung vorzunehmen, um das Informationssicherheitsniveau für die einzelnen Prozesse festzulegen.

Im Rahmen der Vorfallbearbeitung ist es denkbar, dass verschiedene Schritte bezüglich einer Analyse und Bewertung der Geschäftsprozesse bereits durchgeführt wurden. Liegen diesbezüglich bereits dokumentierte Ergebnisse vor, sollten diese nach einem behandelten Vorfall nochmals verifiziert, ggf. angepasst und in die Betriebsdokumentation aufgenommen werden, bzw. für einen erneuten Angriff vorgehalten werden.

11.6 Aufbau eines Sicherheits- und Notfallkonzepts

Sowohl ein Sicherheitskonzept als auch ein Notfallkonzept dienen dazu, dass Informationssicherheitsniveau gewinnbringend zu steigern. Während sich das Sicherheitskonzept im Zuge dessen mit der Darstellung der technischen, organisatorischen und personellen Maßnahmen zur Steigerung der Informationssicherheit beschäftigt, zielt das Notfallkonzept darauf ab, Schäden beim Eintritt von Notfällen wirksam zu minimieren und eine Fortführung der kritischen Geschäftsprozesse zu gewährleisten.

11.6.1 Sicherheitskonzept

Mit einem Sicherheitskonzept soll aufgezeigt werden, inwiefern Sicherheitsprobleme behandelt werden sowie das dadurch angestrebte Sicherheitsniveau hergestellt und sichergestellt wird. Dabei zielt ein systematisches Vorgehen darauf ab, nicht-akzeptable Schwachstellen durch entsprechende Maßnahmen zu vermeiden und auf diese Weise die Ziele der Informationssicherheit zu erreichen. Ein Sicherheitskonzept beschreibt somit primär das Gesamtkonstrukt zur Herstellung eines angemessenen Informationssicherheitsniveaus.

Beim Aufbau kann auf verschiedene Normen und Standards zurückgegriffen werden. Im Wesentlichen gibt es hierbei zwei Standards, die zu nennen sind:

- DIN ISO/IEC 27001
- IT-Grundschutz-Standard (200-1, 200-2 und 200-3)

Beide aufgeführten Normen sind dabei durch eine akkreditierte Zertifizierungsstelle zertifizierungsfähig. Auf diese Weise lässt sich das Informationssicherheitsniveau gegenüber Dritten wirksam nachweisen.

Um detaillierte Einblicke in die IT-Grundschutz-Vorgehensweisen zu erhalten, kann der Online-Kurs: IT-Grundschutz auf der Webseite des BSI genutzt werden. Dieser behandelt alle erforderlichen Schritte bis hin zur Zertifizierung und behandelt auch die Erstellung eines Sicherheitskonzepts.

11.6.2 Notfallkonzept

Um im Falle von IT-Sicherheitsvorfällen und anderen IT-Notfällen angemessen reagieren zu können, sodass die Kernprozesse unbeeinträchtigt fortgeführt sowie mögliche Schäden beim Eintritt weitestgehend reduziert werden können, ist es im Rahmen eines Notfallmanagements erforderlich ein Notfallkonzept zu erstellen.

Das Notfallkonzept übernimmt dabei die Aufgabe einer ordnungsgemäßen Vorbereitung auf potenzielle Vorfälle im Hinblick auf die Minimierung der Auswirkungen und Konsequenzen, und andererseits die Stabilisierung der Geschäftsprozesse, um dadurch den vollständigen Stillstand der Kernprozesse zu vermeiden.

Ein Notfallkonzept lässt sich in zwei grundlegende Komponenten unterteilen:

- Notfallvorsorgekonzept
- Notfallhandbuch

Das Notfallvorsorgekonzept beschäftigt sich mit den Rahmenbedingungen und beinhaltet eine Beschreibung der erforderlichen Maßnahmen und Ressourcen, um Kontinuitätsstrategien umzusetzen. Sowohl präventive als auch reaktive Maßnahmen werden darin behandelt und erläutert.

Das Notfallhandbuch hingegen stellt eine Handlungsanleitung dar, in dem konkrete Informationen und Handlungsanweisungen zur Notfallbewältigung beschrieben werden. Zudem werden wichtige Kontaktinformationen aufgeführt.

Der Aufbau eines Notfallkonzeptes kann ähnlich wie bei einem Sicherheitskonzept unter Zuhilfenahme verschiedener Standards erfolgen. Ein sehr ausführliches Vorgehensmodell bietet hierbei der BSI-Standard 100-4 Notfallmanagement. Auch hierzu gibt es einen Online-Kurs: Notfallmanagement auf der Webseite des BSI, in dem die einzelnen Schritte detailliert behandelt werden.

Darüber hinaus existiert mit dem Baustein DER.4 Notfallmanagement ein entsprechender Baustein im IT-Grundschutz, der das Thema Notfallmanagement und somit auch das Notfallkonzept betrachtet.

11.7 Konzeption von Übungen

Zur Steigerung der grundlegenden Verhaltens- und Vorgehensweise bei einem IT-Sicherheitsvorfall, sowie zur Verbesserung des Sicherheitsbewusstseins, sollten regelmäßig Übungen und Tests durchgeführt werden. Je nach Art der Übung kann die Durchführung dabei mit einem erheblichen Aufwand verbunden sein. Demzufolge ist es entscheidend abzuwägen, welche Art in Frage kommt und sinnvoll ist.

Unterschieden wird hierbei im Wesentlichen zwischen theoretischen und praktischen Übungen.

Bei theoretischen Tests wird die Verhaltens- und Vorgehensweise anhand von ausgedachten Szenarien auf dem Papier bzw. als Planbesprechung durchgespielt. Der Aufwand ist demzufolge eher als gering anzusehen. Praktische Übungen dagegen überprüfen die Wirksamkeit von Verfahren in der Praxis. Der Überprüfungsrahmen kann von einem technischen Test bis hin zu einer praxisgerechten Vollübung gehen. Dies spiegelt sich auch im Aufwand entsprechend wider.

Ungeachtet der Art der Übung sind bei der Durchführung drei grundlegende Schritte zu beachten:

- Konzeption und Planung
- Durchführung
- Auswertung

Das maßgebliche Ziel von Übungen und Test ist es einen möglichen Optimierungsbedarf zu ermitteln, um auf diese Weise Verhaltens- und Vorgehensweise weiterzuentwickeln und zu verbessern. Aus diesem Grund ist es im Kontext der Durchführung wichtig, die getätigten Handlungen möglichst genau zu dokumentieren, da diese die Basis für die Auswertung darstellen.

Ein positiver Nebeneffekt ist zudem die Schärfung des Sicherheitsbewusstseins der Mitarbeitenden sowie die Forderung, immer geordnet und überlegt zu agieren.

12 Anhang

12.1 Übersicht über den Vorfall-Bearbeitungsprozess

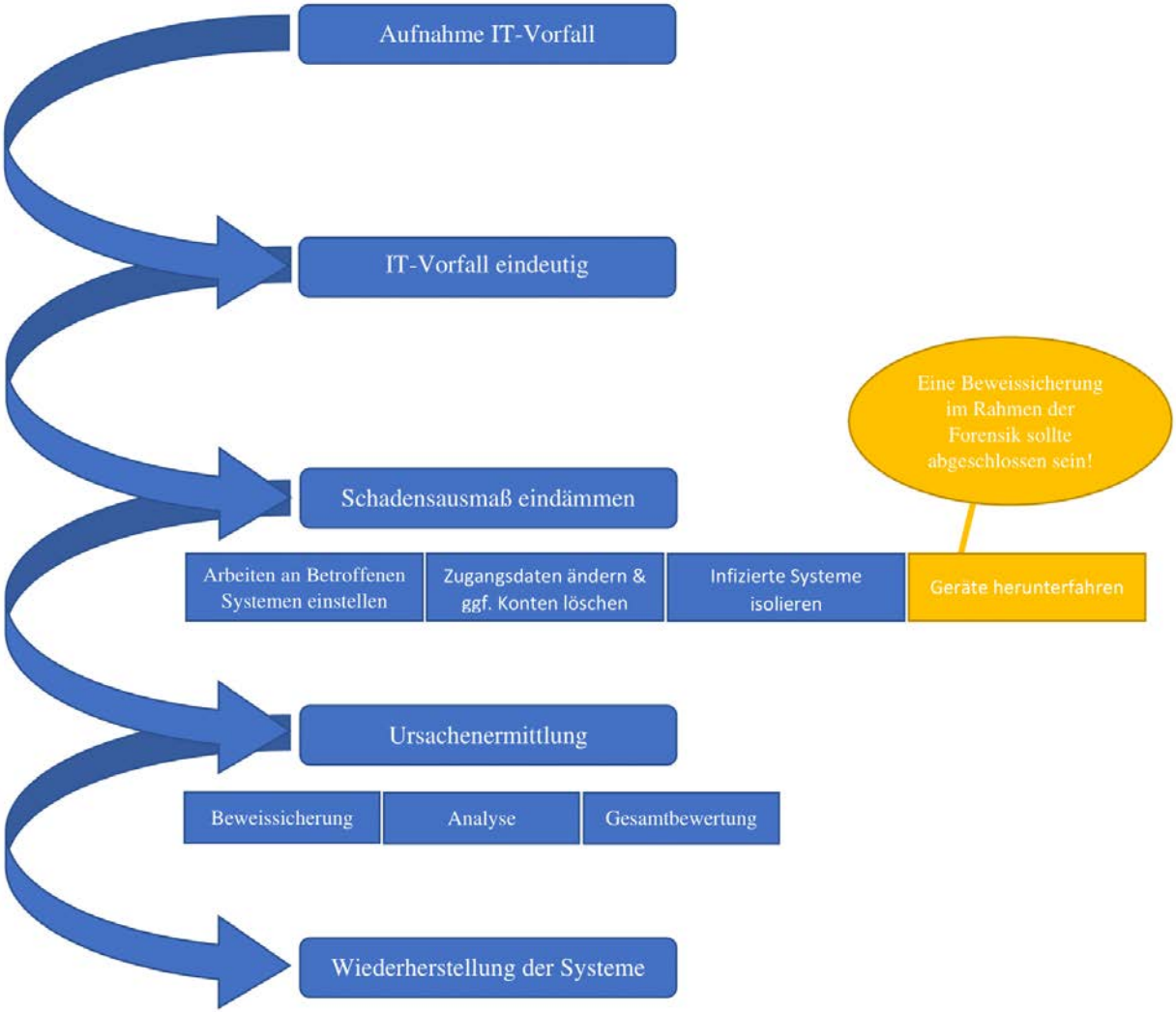


Abbildung 6: Übersicht über den Vorfall-Bearbeitungsprozess

12.2 Checkliste zur IT-Infrastruktur-Analyse

Dokumentation	Kontrolle
Ein Netzwerkstrukturplan ist in detaillierter Form vorhanden.	☐
Eine Inventarisierungsliste mit Informationen über die verarbeitenden Einrichtungen ist vorhanden.	☐
Die Kommunikationsverbindungen (intern und extern) wurden erfasst.	☐
Der Datensicherungsprozess ist dokumentiert.	☐
Es existiert eine Übersicht der Benutzer und deren Berechtigungen.	☐

Tabelle 7: Checkliste zur Dokumentation

Analyse- und Auswertungseinrichtungen	Kontrolle
Sicherheitsrelevante Ereignisse werden in Form eines „Security Information and Event Management Systems“ erfasst.	☐
Ein Protokollierungsserver steht für eine zentrale Auswertung von Protokolldaten zur Verfügung.	☐
Es stehen „Live-Discover“-Anwendungen zur Verfügung, mit der sich Infektionen nachvollziehbar darstellen lassen.	☐
Es sind bereits forensische Tools im Unternehmen im Einsatz.	☐

Tabelle 8: Checkliste zur Analyse- und Auswertungseinrichtungen