Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale Ersthelfer

Cyber-
Sicherheitsnetzwerk

Version 1.0

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

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Sein reaktives Angebot möchte das BSI vor allem für kleine und mittleres Unternehmen genauso wie für Bürger stärken. Im Zuge dessen wurde das Konzept eines dezentralen Unterstützungsnetzwerks als Anlaufstelle bei Cyberangriffen entworfen – das Cyber-Sicherheitsnetzwerk (CSN).

Mit seinem aufeinander aufsetzenden Eskalationsstufen und einer darüber liegenden Rettungskette möchte es sich an die Struktur und Systematik anderer Rettungskonzepte annähern. Ein einfacher Zugang zu dieser Hilfeleistung soll die Akzeptanz erleichtern und schnell Abhilfe schaffen. Besteht im Laufe der Bearbeitung der Bedarf detaillierterer Hilfestellungen wird über ein entsprechend zur Verfügung stehendes Netzwerk aus Experten, eine kostenpflichtige Hilfe mit eigenständiger Vertragsgestaltung als ergänzendes Angebot bereitgestellt.

Der Digitale Ersthelfer hat die Aufgabe, bei IT-Sicherheitsvorfällen eine qualifizierte Einschätzung des IT-Sicherheitsvorfalls zu treffen und Betroffenen Ersthilfe bei kleineren IT-Störungen und IT-Sicherheitsvorfällen zu leisten sowie erste Handlungsempfehlungen zu geben. Er wird vom Betroffenen, innerhalb seiner beim Cyber-Sicherheitsnetzwerk angegebenen Verfügbarkeitszeiten, telefonisch oder per E-Mail kontaktiert und sollte dann innerhalb kürzester Zeit die entsprechenden Hilfestellungen erarbeiten.

Die Qualifikation zum Digitalen Ersthelfer erfolgt anhand einer Basisschulung, die vom BSI kostenlos als Online-Schulung angeboten wird. Diese Basisschulung für Digitale Ersthelfer befindet sich auf den Web-Seiten des Cyber-Sicherheitsnetzwerks. Als Begleitmaterial zur Basisschulung bietet das Cyber-Sicherheitsnetzwerk als Selbstlernunterlagen den vorliegenden Leitfaden an.

Der vorliegende Leitfaden gibt den Rahmen der Tätigkeit des Digitalen Ersthelfers vor und unterstützt ihn bei der Analyse und den Handlungsempfehlungen. Ist der IT-Sicherheitsvorfall weder mit angemessenem Aufwand noch in einem ersten Gespräch zu beheben, empfiehlt der Digitale Ersthelfer, den Vorfall zur weiterführenden Analyse und Behebung an einen Vorfall-Experten oder einen IT- Sicherheitsdienstleister mit einem Team von Vorfall-Experten weiterzugeben.

Digitale Ersthelfer können sowohl Unternehmen wie IT-Sicherheitsdienstleister oder Computerfirmen als auch Privatpersonen wie Studenten oder IT-affine Nachbarn sein, die ihre Qualifizierung durch eine Online-Schulung sowie einen erfolgreich besuchten Prüfungsworkshop nachgewiesen haben und beim Cyber-Sicherheitsnetzwerk registriert sind.

2 Modul 1 - Grundlagen und IT-Störungen durch technische Defekte

2.1 Einführung

In der heutigen Zeit ist eine funktionierende IT wichtiger denn je. Nahezu jedes Unternehmen und jede Privatperson nutzt Computer, Smartphones und sonstige informationsverarbeitenden Einrichtungen, um die Geschäftsprozesse und seine Kommunikation effektiv und zielgerichtet realisieren zu können und stetig weiter zu optimieren.

Grundlage dafür ist ein möglichst störungsfreier Betrieb der zum Einsatz kommenden IT-Komponenten. Dieser Zustand ist jedoch mehr eine Wunschvorstellung, da IT-Störungen jederzeit auftreten können. IT-Störungen aufgrund von technischen Defekten treten ungeplant und zu ungünstigen Zeitpunkten auf. Die Folge ist meist, dass Prozesse und Verfahren beeinträchtigt oder sogar komplett stillgelegt werden. Aus diesem Grund ist es essenziell angemessen auf IT-Störungen zu reagieren, um einen reibungslosen Betrieb gewährleisten zu können.

Modul 1 beschäftigt sich zunächst mit den Grundlagen und Begrifflichkeiten. Im Anschluss wird eine Auswahl typischer IT-Störungen behandelt. Dabei werden die einzelnen Störungen kurz beschrieben und Handlungsempfehlungen als Lösungsansatz dargestellt. Die Durchführung der einzelnen Handlungsempfehlungen orientiert sich an dem Wissensstand und Möglichkeiten des Betroffenen. Zuletzt werden die wichtigsten Inhalte zusammengefasst und die Wissensvermittlung wird durch Übungsaufgaben gefestigt.

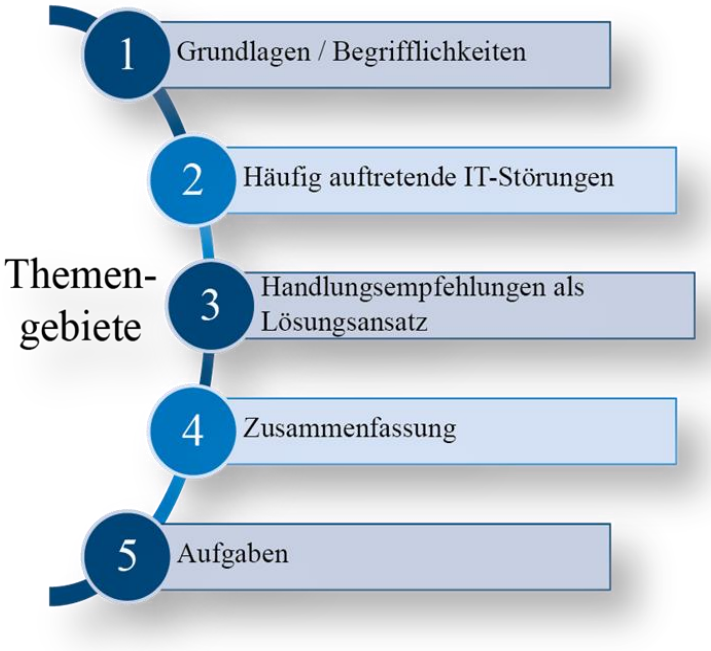

Abbildung 1: Themengebiete Modul 1

2.2 Intention und Lernziele

Das Modul 1 dient als Einstieg in die Thematik. Es behandelt die Grundlagen und beschäftigt sich mit häufig auftretenden IT-Störungen, die durch technische Defekte hervorgerufen werden können. Nach Bewältigung dieses Moduls ist ein allgemeines Verständnis über typische IT-Störungen sowie dessen mögliche Behebungsmethoden vorhanden.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmer dazu in der Lage:

Eine IT-Störung von einem IT-Sicherheitsvorfall zu unterscheiden.

Typische IT-Störungen zu identifizieren.

Betroffene Personen beim Umgang mit IT-Störungen zu unterstützen.

2.3 Begriffsbestimmung – IT-Störung

Unter einer IT-Störung versteht man unerwartet eintretende Ereignisse, die die Funktionsweise des IT-Systems beeinträchtigen oder sogar zu einem kompletten Ausfall führen. Davon kann eine einzelne Komponente im System, das gesamte System oder ein Peripheriegerät betroffen sein. Bei einer IT-Störung kann der Benutzer sein IT-System bzw. einen Dienst nicht mehr ordnungsgemäß nutzen. Die Beeinträchtigung oder der Ausfall sind hierbei grundsätzlich von kurzzeitiger Natur. Die Behandlung von IT-Störungen bewegt sich somit auch im Rahmen der regelmäßigen Störungsbehebung.

Eine Einwirkung von Dritten mit kriminellen Absichten wird bei einer IT-Störung ausgeschlossen. Vielmehr wird bei einer IT-Störung von einem technischen Defekt oder einem versehentlichen fehlerhaften Nutzen des IT-Systems durch den Benutzer selbst ausgegangen.

Abbildung 2: IT-Störung

2.4 Begriffsbestimmung – IT-Sicherheitsvorfall

Als IT-Sicherheitsvorfall wird ein Ereignis bezeichnet, bei dem die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen beeinträchtigt werden und als Folge ein großer Schaden entstehen kann.

Die Vertraulichkeit beschreibt den Schutz von Informationen vor einer unbefugten Preisgabe. Daten dürfen dabei ausschließlich an befugte Personen in der erlaubten Weise zugänglich sein.

Unter dem Begriff Integrität wird die Gewährleistung der Korrektheit von Informationen und die ordnungsgemäße Funktionsweise von Systemen verstanden.

Die Verfügbarkeit von IT-Systemen, IT-Anwendungen oder IT-Netzen sowie auch von Informationen wird sichergestellt, wenn diese von einem berechtigten Nutzer jederzeit wie vorgesehen nutzbar sind.

IT-Sicherheitsvorfälle haben meist ihren Ursprung beispielsweise in einem provozierten Fehlverhalten, einer ausgenutzten Schwachstelle oder einer negativen Einwirkung von außen. Ausschlaggebend ist dabei das Zutun eines Dritten mit kriminellen Absichten. Die Handhabung von IT-Sicherheitsvorfällen ist i. d. R. mit einer umfassenden Behandlung verbunden.

Bei einem IT-Sicherheitsvorfall steht meist das Interesse an den Informationen auf dem System im Vordergrund, nicht das System selbst. Hierbei ist es unerheblich, ob der IT-Sicherheitsvorfall bereits ein unerwünschtes Ergebnis bzw. eine Auswirkung verursacht hat oder nur das Potential dazu hat, Schäden herbeizuführen.

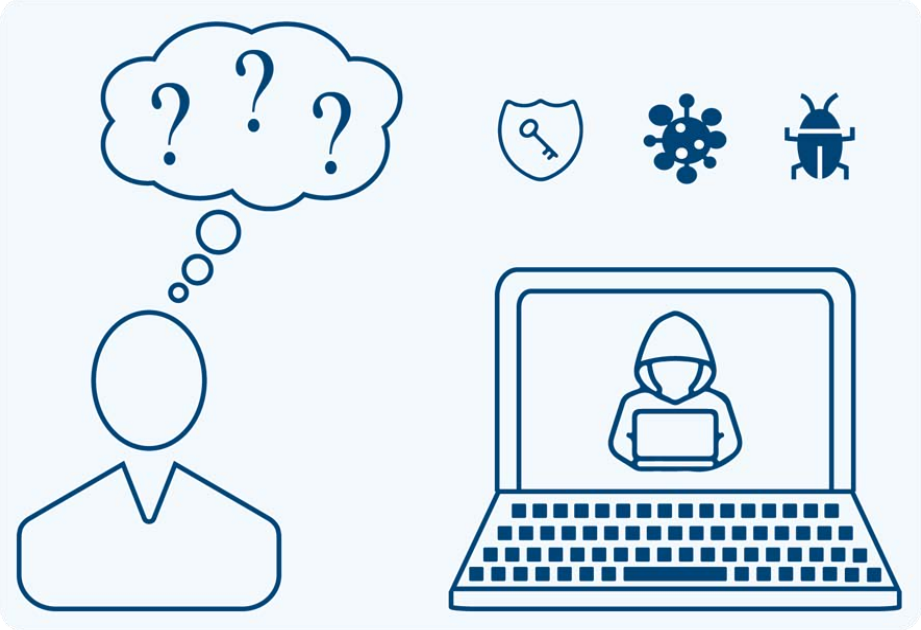

Abbildung 3: IT-Sicherheitsvorfall

2.5 Abgrenzung einer IT-Störung zu einem IT-Sicherheitsvorfall

Die klassische IT-Störung beschreibt eine Störung als Ereignis, das eine Beeinträchtigung oder Nichtverfügbarkeit des IT-Systems zur Folge hat. Dies setzt einen Defekt oder einen Ausfall von Hardware oder Diensten voraus. Die Behandlung von IT-Störungen bewegt sich im Rahmen der regelmäßigen Störungsbehebung.

Analog dieser Definition lässt sich ein IT-Sicherheitsvorfall ebenso als unerwünschtes Ereignis verstehen, das negative Auswirkungen für einen Betroffenen nach sich ziehen kann. In diesem Sinne können die Vertraulichkeit, Integrität und Verfügbarkeit betroffen sein. Anders als bei einer IT-Störung wird ein

IT-Sicherheitsvorfall durch bewusstes Handeln eines Angreifers ausgelöst. Ziel dabei ist es, einen beträchtlichen Schaden anzurichten oder sich Informationen widerrechtlich anzueignen. Im Gegensatz zu der Behandlung einer IT-Störungen im Rahmen der Störungsbehebung ist die Handhabung von IT-Sicherheitsvorfällen grundsätzlich mit einer umfassenden Behandlung verbunden.

Bei einer IT-Störung sind die Auswirkungen immer unmittelbar spürbar. Bei einem IT-Sicherheitsvorfall kann es, neben einer sofortigen Beeinflussung des Systems, möglich sein, dass dieses weiterhin funktionsfähig bleibt. Mögliche Folgen können sich zu einem späteren Zeitpunkt bemerkbar machen. Was auf den ersten Blick eine einfache IT-Störung vermuten lässt, kann auch die Folge eines IT-Sicherheitsvorfalls sein. Somit kann sich eine IT-Störung zu einem IT-Sicherheitsvorfall entwickeln.

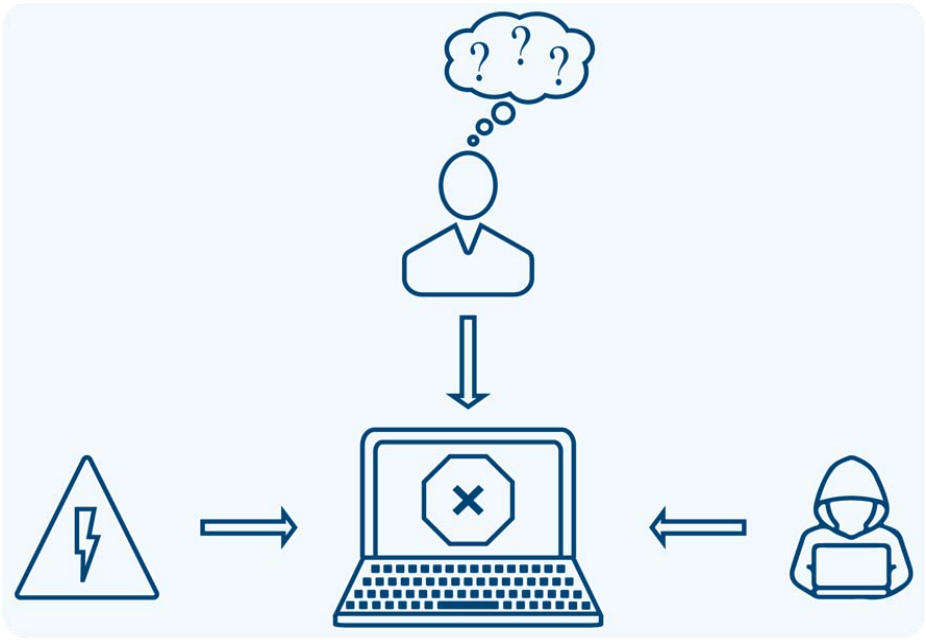

Abbildung 4: Abgrenzung IT-Störung zu IT-Sicherheitsvorfall

Der grundlegende Unterschied zwischen einer IT-Störung und einem IT-Sicherheitsvorfall liegt im Auslöser. Ein IT-Sicherheitsvorfall wird durch einen Cyber-Angriff ausgelöst, wobei eine IT-Störung die Folge von einem technischen Defekt bzw. unbeabsichtigtem Fehlverhalten ist.

Beispiele einer IT-Störung	Beispiele eines IT-Sicherheitsvorfalls
Maus / Tastatur funktioniert nicht	Verschlüsselung von Dateien (Ransomware)
Bildschirm zeigt kein Bild	Identitätsdiebstahl
Probleme mit dem Netzwerk	Manipulation von Daten

Tabelle 1: Beispiele von IT-Störungen und IT-Sicherheitsvorfällen

Merkmale einer IT-Störung	Merkmale eines IT-Sicherheitsvorfalls
Technischer Defekt oder unbeabsichtigtes Fehlverhalten	Kriminelle Cyber-Angriffe
Kurzzeitige(r) Beeinträchtigung / Ausfall	Langwierige(r) Beeinträchtigung / Ausfall
Behandlungsaufwand gering	Behandlungsaufwand i. d R. hoch

Tabelle 2: Unterscheidungsmerkmale einer IT-Störung und eines IT-Sicherheitsvorfalls

2.6 Typische IT-Störungen und Handlungsempfehlungen

In den nachfolgenden Abschnitten werden häufig auftretende IT-Störungen aufgelistet und beschrieben. Darüber hinaus werden Handlungsempfehlungen als Lösungsansatz aufgeführt. Diese zielen darauf ab einen Betroffenen bei der Behebung der zugrundeliegenden Problematik zu unterstützen.

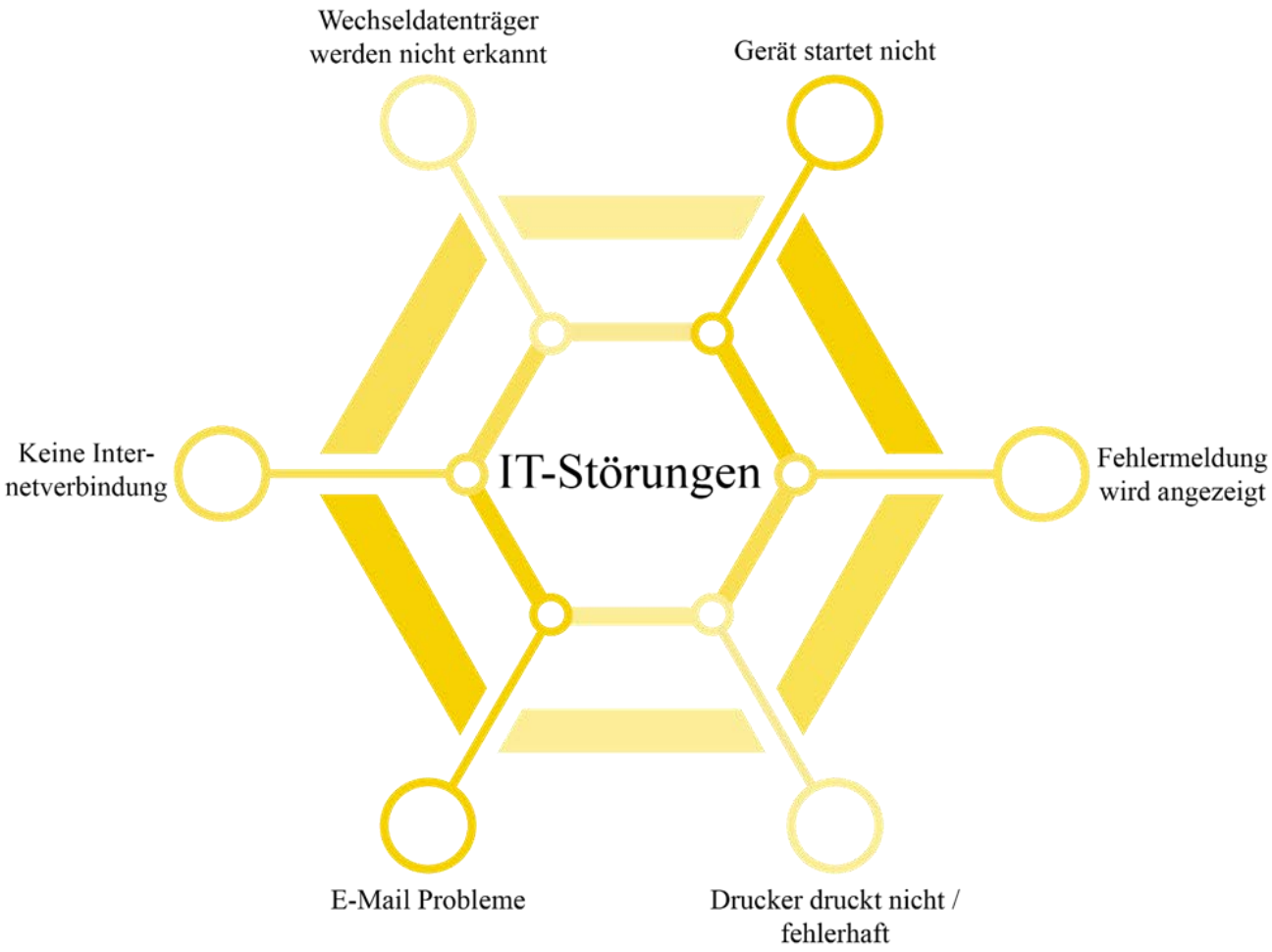

Abbildung 5: Alltägliche IT-Störungen

2.6.1 Gerät startet nicht

Der Versuch das Notebook oder den Desktop-PC einzuschalten bzw. zu starten ist fehlgeschlagen. Beim Betätigen der Einschalttaste zeigt der Computer keine Reaktion. Weder die LEDs leuchten, noch ist der Lüfter angelaufen oder eine arbeitende Festplatte ist zu hören.

Die nachfolgend aufgelisteten Handlungsempfehlungen können bei der vorliegenden Störung als Lösungsansatz ausgesprochen werden. Zu berücksichtigen ist, dass je nach Wissensstand des Betroffenen möglicherweise nicht alle aufgeführten Handlungsempfehlungen realisierbar sind.

Bleiben die nachfolgend aufgeführten Handlungsempfehlungen erfolglos, liegt vermutlich ein Defekt am Gerät vor. Der Betroffene sollte sich an den Verkäufer des Gerätes oder einen IT-Support wenden.

Gerät startet nicht

Mögliche Handlungsempfehlungen zur Behebung:

Netzkabel kontrollieren (ziehen, einstecken, neu starten)
: Das Netzkabel aus der Steckdose sowie dem Gerät ziehen und für 10 Sekunden stromlos machen. Anschließend das Gerät erneut mit Strom verbinden und den Startvorgang wiederholen.

Kontrollschalter am Netzteil kontrollieren (nur bei Stand-PCs)
: An der Rückseite des Stand-PCs i. d. R. in unmittelbarer Nähe zum Netzteil überprüfen, ob der Kontrollschalter umgelegt ist.

Andere Steckdose verwenden
: Das Gerät an eine andere/alternative Steckdose anschließen und den Startvorgang wiederholen.

Netzkabel tauschen
: Sollte ein zweites Netzkabel vorhanden sein, dieses zur Herstellung der Stromversorgung verwenden und den Startvorgang wiederholen.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

2.6.2 Bildschirm zeigt beim Hochfahren eine Fehlermeldung

Nach betätigen der Einschalttaste versucht das Gerät hochzufahren. Dieser Prozess wird nicht korrekt ausgeführt bzw. unterbrochen und eine Fehlermeldung erscheint auf dem Bildschirm bzw. bleibt der Bildschirm schwarz.

Bildschirm zeigt eine Fehlermeldung

Mögliche Handlungsempfehlungen zur Behebung:

Gerät neu starten

Das Gerät kann aufgrund eines Fehlers „hängen geblieben“ sein. Durch längeres Drücken des Ein-/Aus-Schalters kann es manuell bzw. „hart“ ausgeschaltet werden. Anschließend kann das Gerät über ein kurzes Drücken des Ein-/Aus-Schalters wieder eingeschaltet werden.

Gerät stromlos machen

Gerät für 10 Sekunden vom Strom nehmen und anschließend wie gewohnt starten.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

Praxistipp

Hinter dem Start eines Laptops oder Stand-PCs steckt ein komplexer Vorgang, der im Hintergrund von dem Gerät automatisch ausgeführt wird. Im Idealfall wird das System dabei ordnungsgemäß hochgefahren und steht schließlich zur Nutzung zur Verfügung. Doch auch bei diesem Prozess kann es zu Fehlern kommen. Diese machen sich durch das Erscheinen einer Fehlermeldung bemerkbar. Die Folge ist, dass der Startvorgang unterbrochen wird.

Die nachfolgenden Fehler zeigen eine exemplarische Auswahl von Fehlermeldungen, die beim Starten des Gerätes auftreten können.

- BIOS has been reset:
  Standardeinstellungen werden durch Fehler oder Verlust der Spannung geladen
- Boot Device Not Found:
  Die Festplatte, auf der das Betriebssystem installiert ist, wird nicht erkannt.
- Wiederherstellung: Der PC/das Gerät muss repariert werden:
  Wichtige Systemdateien, die zum Starten benötigt werden, wurden beschädigt, verändert oder sind verloren gegangen. Infolgedessen ist die Windows Installation defekt

Bei allen aufgeführten Fehlermeldungen helfen die Handlungsempfehlungen nicht weiter. Somit sollte direkt der entsprechende IT-Support kontaktiert werden.

Die nachfolgenden Abbildungen zeigen wie sich die aufgeführten Fehlermeldungen visuell bemerkbar machen.

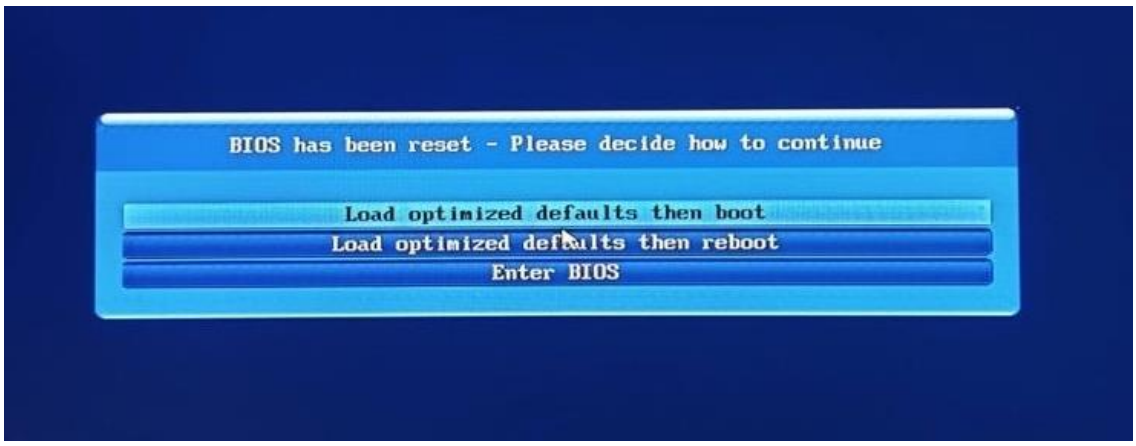

Abbildung 6: Fehlermeldung „Bios has been reset"

Abbildung 7: Fehlermeldung „Boot Device Not Found"

Abbildung 8: Fehlermeldung „Wiederherstellung: Der PC/das Gerät muss repariert werden“

2.6.3 Drucker druckt nicht oder fehlerhaft

Ein Druckauftrag wurde über einen Computer wie gewöhnlich erteilt, doch der Drucker führt diesen jedoch nicht oder fehlerhaft aus.

Drucker druckt nicht

Mögliche Handlungsempfehlungen zur Behebung:

Drucker neu starten
: Den Drucker herunterfahren, für 10 Sekunden vom Strom nehmen und anschließend neu starten. Letztlich den Druckauftrag wiederholen.

Druckziel überprüfen
: Es ist zu überprüfen, ob der richtige Drucker für den Druckauftrag ausgewählt wurde.

Verbindung überprüfen
: Es ist zu überprüfen, ob das Gerät über das Verbindungskabel richtig mit dem Computer verbunden ist bzw. ob eine aktive Netzwerkverbindung besteht.

Verbindungskabel austauschen
: Ist der Drucker direkt mit dem Rechner verbunden, sollte das USB-Verbindungskabel ausgetauscht und der Druckauftrag anschließend wiederholt werden.

Papier auffüllen
: Den Drucker bzw. das richtige Papierfach mit ausreichend Papier auffüllen.

Aktuelle Treiberversion installieren (IT-Kenntnisse erforderlich)
: Neuste Treiberversion des jeweiligen Druckers auf der Herstellerseite herunterladen und installieren.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

Drucker druckt fehlerhaft

Mögliche Handlungsempfehlungen zur Behebung:

Drucker neu starten
: Den Drucker herunterfahren, für 10 Sekunden vom Strom nehmen und anschließend neu starten. Letztlich den Druckauftrag wiederholen.

Toner/Tinte ersetzen
: Die Toner/Tintenpatronen sind durch neue Komponenten auszuwechseln.

Drucker reinigen (IT-Kenntnisse erforderlich)
: Das Reinigungsprogramm des Druckers nach Anleitung der Gebrauchsanweisung durchführen. I. d. R. kann unter den Einstellungen des Druckers ein automatisches Reinigungsprogramm gestartet werden.

Aktuelle Treiberversion installieren (IT-Kenntnisse erforderlich)
: Neuste Treiberversion des jeweiligen Druckers auf der Herstellerseite herunterladen und installieren.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

2.6.4 E-Mails können nicht empfangen oder versendet werden

Es können entweder keine E-Mails empfangen oder versendet werden. E-Mails, die empfangen werden sollten, tauchen dabei nicht im Posteingang auf. Verschickte E-Mails hängen im Postausgang fest bzw. tauchen nicht im Ordner der versendeten E-Mails auf.

E-Mails können nicht empfangen oder versendet werden

Mögliche Handlungsempfehlungen zur Behebung:

Internetverbindung prüfen
: Eine aktive Internetverbindung durch das Aufrufen einer externen Webseite in einem Internetbrowser überprüfen.

Spam Postfach überprüfen
: Im Spam Postfach nach fehlenden E-Mails suchen.

Anwendung / Computer neu starten
: Die Anwendung und/oder das Gerät neu starten.

Speicher leeren
: Nicht mehr benötigte E-Mails entsprechend archivieren, um Speicherplatz zu schaffen. Hierbei ist zu empfehlen, vorab den Spam Ordner sowie den Papierkorb zu leeren.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

2.6.5 Keine Internetverbindung

Der Versuch mit einem gängigen Webbrowser eine Internetseite aufzurufen ist fehlgeschlagen. Die gewünschte Webseite öffnet sich nicht wie erwartet.

Keine Internetverbindung

Mögliche Handlungsempfehlungen zur Behebung:

Netzwerkkabel kontrollieren
: Netzwerkkabel vom Gerät entfernen und erneut einstecken. Anschließend den Aufruf der Webseite wiederholen.

WLAN-Verbindung kontrollieren
: In der Taskleiste oder den Netzwerkeinstellungen überprüfen, ob eine aktive WLAN-Verbindung besteht und ob es sich um das richtige WLAN handelt

Provider prüfen
: Überprüfen, ob der genutzte Provider eine Störungsmeldung veröffentlicht hat (https://www.allestörungen.de).

Router neu starten
: Router für kurze Zeit vom Strom nehmen und anschließend neu starten.

Netzwerkkabel tauschen
: Sollte ein zweites Netzwerkkabel vorhanden sein, dieses verwenden.

WLAN-Adapter/Netzwerkkarte aktivieren (IT-Kenntnisse erforderlich)
: WLAN-Adapter/Netzwerkkarte über die Einstellungen des Gerätes aktivieren.

Beheben die Handlungsempfehlungen die Problematik nicht,

sollte ein IT-Support kontaktiert werden.

Praxistipp

Die nachfolgenden Abbildungen führen zwei Meldungen auf, die bei der Nutzung des Webbrowsers auftreten können. In beiden Fällen ist die Ursache, dass keine aktive Internetverbindung besteht. Die verwendeten Internetbrowser sind in den Beispielen zum einen Microsoft Edge und zum anderen Google Chrome.

Abbildung 9: Meldung bei Microsoft Edge

Abbildung 10: Meldung bei Google Chrome

2.6.6 Mobile Wechseldatenträger werden nicht erkannt

Nach dem Anschließen eines USB-Sticks bzw. einer externen Festplatte oder dem Einlegen einer CD/DVD bzw. Blu-Ray Disc wird der Wechseldatenträger nicht erkannt. Demzufolge ist der Zugriff auf Informationen oder auch das Ausführen von Anwendungen nicht möglich.

Mobile Wechseldatenträger werden nicht erkannt

Mögliche Handlungsempfehlungen zur Behebung:

Verwendung eines anderen USB-Ports
Den USB-Stick bzw. die externe Festplatte an einem anderen Port des Computers anschließen.

Anderes USB-Medium/CD nutzen
Mit einem funktionierenden USB-Medium/CD die Funktionalität des USB-Ports/CD-Laufwerks überprüfen.

USB-Port/CD-Laufwerk aktivieren (IT-Kenntnisse erforderlich)
Über den Geräte-Manager den Port bzw. das Laufwerk für die Nutzung aktivieren.

Treibersoftware des CD-Laufwerks aktualisieren (IT-Kenntnisse erforderlich)
Über den Geräte-Manager die aktuellen Treiber des entsprechenden Laufwerks herunterladen und installieren.

Laufwerkbuchstabe des USB-Mediums ändern (IT-Kenntnisse erforderlich)
In der Datenträgerverwaltung manuell den Laufwerksbuchstaben des USB-Mediums ändern.

Beheben die Handlungsempfehlungen die Problematik nicht,
sollte ein IT-Support kontaktiert werden.

2.7 Zusammenfassung

In Modul 1 wurden die wesentlichen Begriffe „IT-Störung" und „IT-Sicherheitsvorfall" erläutert und zur Verdeutlichung voneinander abgegrenzt. Des Weiteren wurde ein grundlegendes Verständnis bei der Erkennung und Behandlung von typischen IT-Störungen vermittelt. In diesem Sinne ist ein Digitaler Ersthelfer dazu in der Lage, einen minimalen IT-Support zu leisten und anhand von Handlungsempfehlungen einem Hilfesuchenden bei der Behebung der Problematik zu unterstützen.

Das Wichtigste in Kürze

IT-Störung:

- Beeinträchtigung der Funktionsweise oder Ausfall eines IT-Systems durch das Auftreten von unerwarteten Ereignissen.
- Wird nicht durch einen Angreifer ausgelöst.
- Auslöser: technischer Defekt oder unbeabsichtigte menschliche Fehlhandlung.

IT-Sicherheitsvorfall:

- Beeinträchtigung der Vertraulichkeit, Integrität und/oder Verfügbarkeit, sodass ein großer Schaden entstehen kann bzw. zu erwarten ist.
- Wird i. d. R. durch einen Angreifer ausgelöst.
- Auslöser: Cyber-Angriff (kriminelle Absichten).

2.8 Aufgabe

Die nachfolgende Aufgabe dient der Überprüfung des vermittelten Wissens in Modul 1. Dabei soll ein Einblick in die Praxis geliefert, sowie außerdem der überlieferte Kenntnisstand gefestigt werden.

Lesen Sie sich die folgenden Szenarien durch und sprechen Sie Handlungsempfehlungen aus, die einem Betroffenen als Lösungsansatz zur Behebung des Problems gegeben werden können.

Die Lösungen befinden sich im Anhang.

Szenario 1:

Ich habe in Mozilla Firefox versucht Google aufzurufen, jedoch hat sich die Seite nicht geöffnet. Der Versuch eine andere Webseite aufzurufen ist ebenfalls missglückt.

Szenario 2:

Ich habe meine externe Festplatte an meinen Laptop angeschlossen. Die Festplatte wird nicht erkannt und demzufolge kann ich nicht auf die Daten der Festplatte zugreifen.

Szenario 3:

Ich habe einen Druckauftrag abgegeben. Der Drucker fängt normal an zu drucken, jedoch befinden sich auf jeder Seite des Ausdrucks weiße Streifen.

Szenario 4:

Ich habe versucht auf die übliche Weise eine E-Mail zu versenden. Die E-Mail wird mir dauerhaft im Postausgang angezeigt. Als E-Mail-Anwendung benutze ich Microsoft Outlook.

3 Modul 2 – IT-Sicherheitsvorfälle durch Cyber-Angriffe

3.1 Einführung

Jeden Tag werden Firmen, Behörden und Privatpersonen Ziel von unzähligen Cyber-Angriffen. Mittlerweile betrifft die zunehmende Cyber-Kriminalität nahezu jeden Bürger. Nichtsdestotrotz werden die Risiken, die in Verbindung mit Cyber-Angriffen stehen, von den meisten falsch eingeschätzt. Oftmals wird ein erfolgreich durchgeführter Angriff durch einen Hacker erst Monate später oder gar nicht bemerkt. Gerade wenn der Angreifer über einen längeren Zeitraum Zugang zu den Systemen hat, können IT-Sicherheitsvorfälle verheerende Folgen für die Betroffenen haben. Dies spiegelt sich zudem auch häufig in einer Verletzung der Privatsphäre bei Privatpersonen bzw. in Reputationsschäden bei Unternehmen wider.

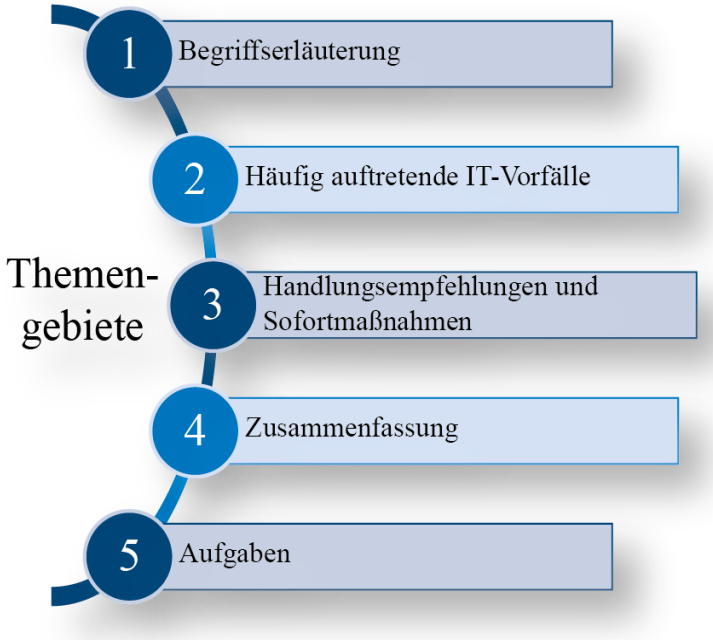

Abbildung 11: Themengebiete Modul 2

3.2 Intention und Lernziele

Das Modul 2 beschäftigt sich mit IT-Sicherheitsvorfällen, die durch Cyber-Angriffe hervorgerufen werden. Zu Beginn wird der Begriff „IT-Sicherheitsvorfall“ erläutert, um die Basis für das Verständnis der weiteren Inhalte zu schaffen. Anschließend werden klassische bzw. typische IT-Sicherheitsvorfälle behandelt, welche das Ergebnis eines Cyber-Angriffs sind. Nach Bewältigung dieses Moduls ist ein grundlegendes Verständnis über häufig auftretende IT-Sicherheitsvorfälle vorhanden.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmer dazu in der Lage:

Einen IT-Sicherheitsvorfall und dessen Merkmale zu beschreiben.

Typische IT-Sicherheitsvorfälle zu identifizieren.

Betroffene Personen bei der Handhabung von IT-Sicherheitsvorfällen zu unterstützen.

3.3 Begriffsbestimmung – IT-Sicherheitsvorfall

Als IT-Sicherheitsvorfall wird ein Ereignis bezeichnet, bei dem die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen beeinträchtigt werden und als Folge ein großer Schaden entstehen kann. Diese Vorfälle haben meist ihren Ursprung beispielsweise in einem provozierten Fehlverhalten, einer ausgenutzten Schwachstelle oder einer negativen Einwirkung von außen. Ausschlaggeben ist dabei das Zutun eines Dritten mit kriminellen Absichten. Die Handhabung von IT-Sicherheitsvorfällen ist i. d. R. mit einer umfassenden Behandlung verbunden.

Bei einem IT-Sicherheitsvorfall steht meist das Interesse an den Informationen auf dem System im Vordergrund, nicht das System selbst. Hierbei ist es unerheblich, ob der Sicherheitsvorfall bereits ein unerwünschtes Ergebnis oder eine Auswirkung verursacht hat oder nur das Potential dazu hat Schäden herbeizuführen.

Merkmale eines IT-Sicherheitsvorfalls
Kriminelle Cyber-Angriffe
Langwierige(r) Beeinträchtigung / Ausfall
Behandlungsaufwand i. d R. hoch

Tabelle 3: Merkmale eines IT-Sicherheitsvorfall

3.4 Typische IT-Sicherheitsvorfälle und Handlungsempfehlungen

Ein IT-Sicherheitsvorfall wirkt sich in jedem Fall negativ auf die Vertraulichkeit, Integrität und/oder Verfügbarkeit aus. Aufgrund der vielfältigen Angriffsmethoden lassen sich IT-Sicherheitsvorfälle nicht immer vermeiden. Demzufolge gilt es diese entsprechend zu erkennen und adäquat darauf zu reagieren.

In den nachfolgenden Abschnitten werden häufig auftretende IT-Sicherheitsvorfälle aufgelistet und beschrieben. Darüber hinaus werden Handlungsempfehlungen bzw. Sofortmaßnahmen aufgeführt. Diese zielen darauf ab, einen Betroffenen bei der Eingrenzung des Schadensausmaß oder Behebung der zugrundeliegenden Problematik zu unterstützen.

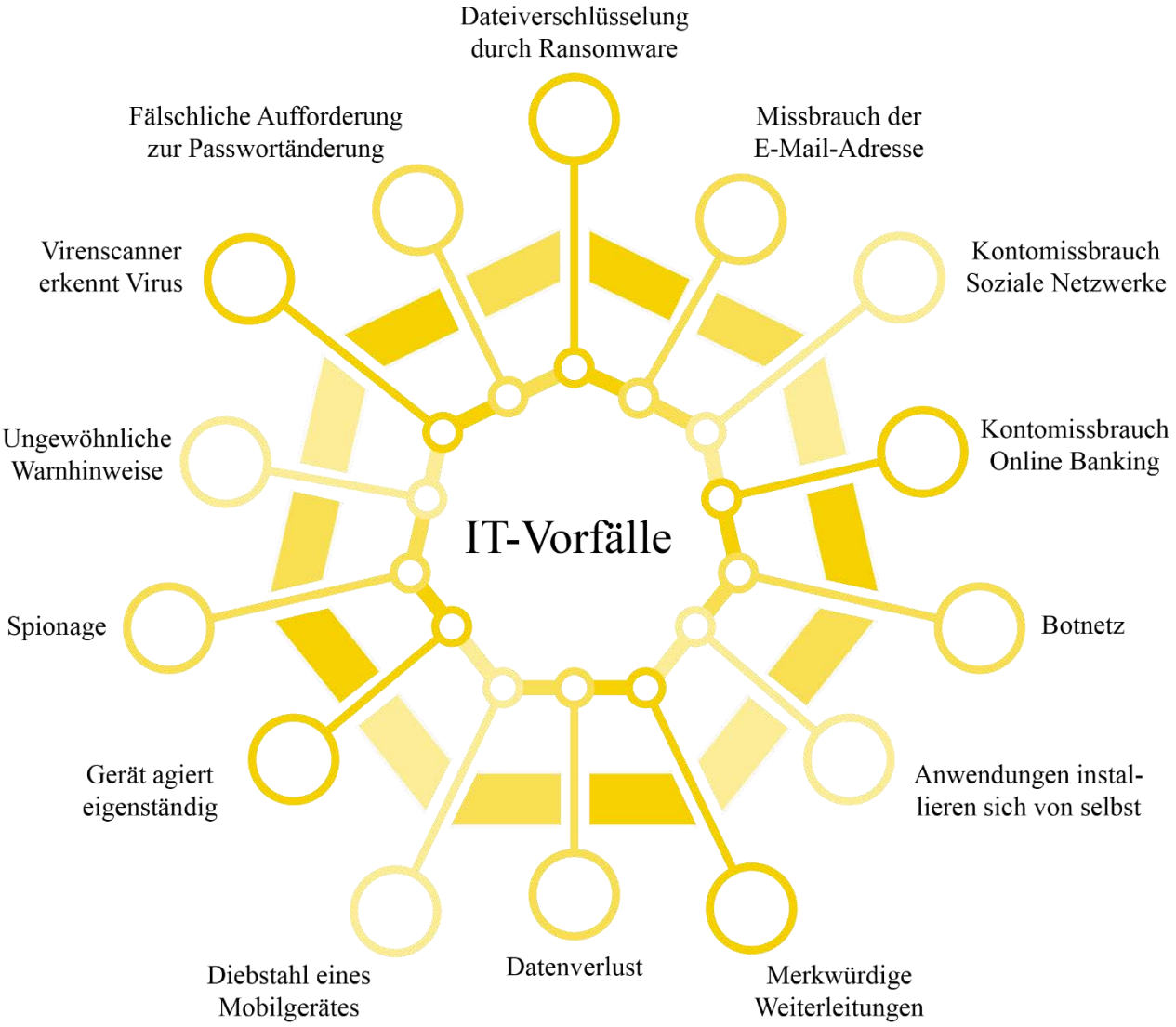

Abbildung 12: Klassische IT-Sicherheitsvorfälle

3.4.1 Missbrauch der E-Mail-Adresse

Ein Angreifer verschickt im Namen des Betroffenen E-Mails an dessen Kontakte. Einerseits ist es dabei möglich, dass das E-Mail-Benutzerkonto gehackt oder infiziert wurde. In diesem Fall werden die Mails direkt von dem entsprechenden Konto unbemerkt an die Kontakte verschickt. Andererseits besteht die Möglichkeit, dass die E-Mail-Adresse des Betroffenen als Absender missbraucht wird. Der Angreifer gibt sich dabei als die betroffene Person aus. Die E-Mails werden dabei nicht von dem Konto des Betroffenen verschickt. In der Regel enthalten diese Mails schadhafte Links, Anhänge oder Aufforderungen – z. B. Daten zu übermitteln oder Zahlungen zu tätigen.

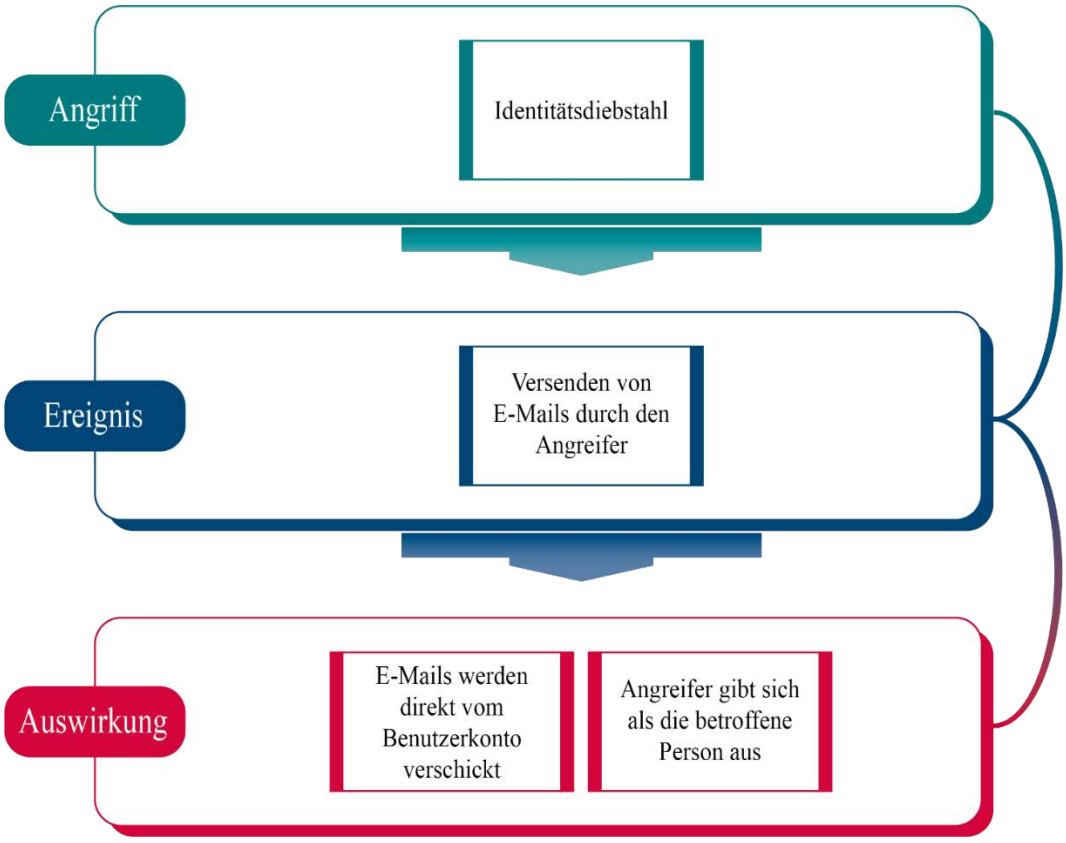

Abbildung 13: E-Mail-Missbrauch

Die nachfolgend aufgelisteten Handlungsempfehlungen können bei dem vorliegenden Sicherheitsvorfall als Lösungsansatz bzw. als Sofortmaßnahmen ausgesprochen werden. Je nach Handlungsempfehlung kann die Problematik behoben, das Schadensausmaß eingegrenzt oder eine Ausbreitung verhindert werden.

Auch wenn anhand der durchgeführten Handlungsempfehlungen der Vorfall auf den ersten Blick beseitigt wurde, kann es durchaus erforderlich sein, dass der Vorfall weiterverfolgt werden muss. Der IT-Sicherheitsvorfall wird durch die aufgeführten Handlungsempfehlungen nicht zwingend vollständig behoben.

Missbrauch der E-Mail-Adresse

Mögliche Handlungsempfehlungen/Sofortmaßnahmen:

Zugangsdaten (Passwort) ändern

Das verwendete Passwort muss umgehend geändert werden. Dabei sollte ein starkes Passwort verwendet und ggf. eine 2-Faktor-Authentifizierung eingerichtet werden. Zudem sollten auch die Zugangsdaten der Benutzerkonten von anderen Plattformen gewechselt werden (**vor allem bei Verwendung des gleichen Passwortes**).

Kontakte informieren

Es sollten möglichst alle Kontakte über den Sachverhalt des Missbrauchs informiert und gewarnt werden, keine Anhänge oder Links zu öffnen oder möglichen Aufforderungen nachzukommen.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt unter dem nachfolgenden Link Ratschläge zur Auswahl eines sicheren Passwortes und zum Umgang mit Passwörtern auf.

Sicherer Umgang mit Passwörtern

3.4.2 Verschlüsselung durch Ransomware

Der Zugriff auf Daten und Systeme wird aufgrund von Ransomware eingeschränkt bzw. unterbunden. Dabei wird zum einen der Systemzugriff gesperrt, wodurch sich Anwendungen nicht mehr ausführen lassen. Zum anderen werden Daten und Informationen verschlüsselt. Demzufolge lassen sich diese nicht aufrufen bzw. öffnen. Der Betroffene erhält i. d. R. eine Aufforderung einen Geldbetrag als Lösegeld zu zahlen (häufig in Form von Kryptowährung[1]). Erst nach erfolgter Zahlung soll die Verschlüsselung aufgehoben werden.

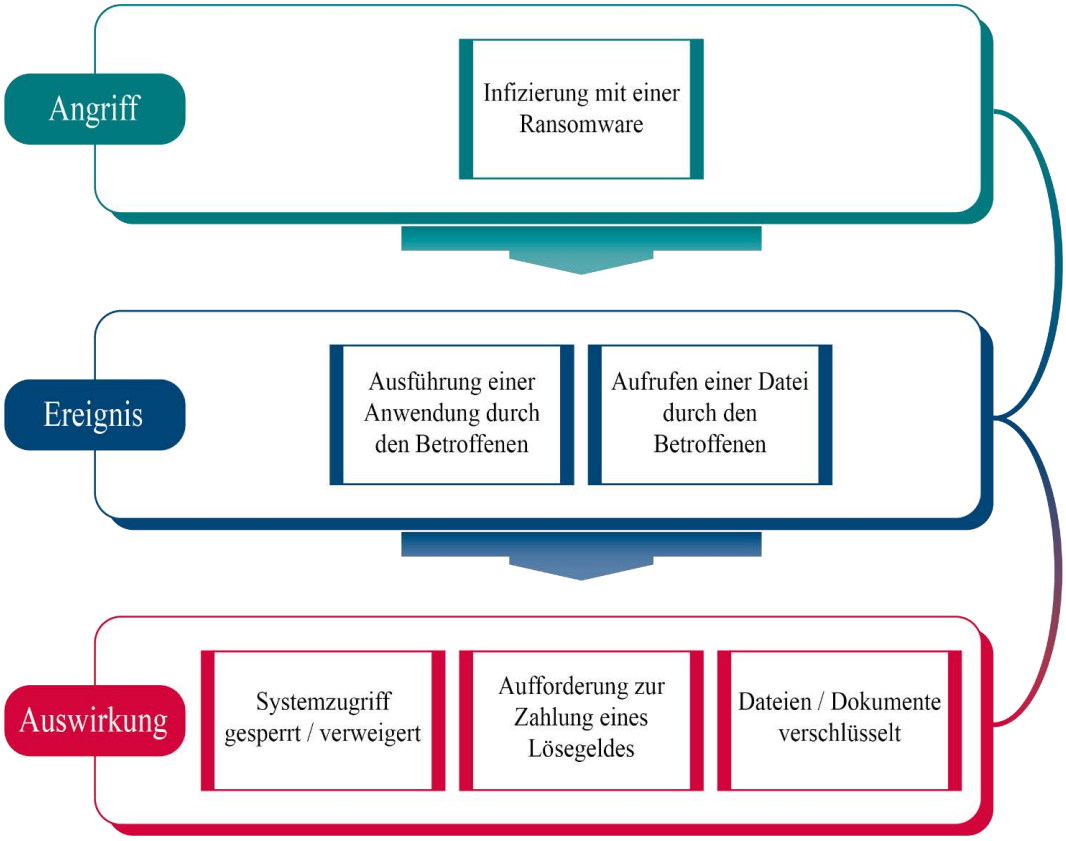

Abbildung 14: Ransomware-Angriff

[1] Eine Kryptowährung beschreibt ein digitales Zahlungsmittel mit einem kryptografisch abgesicherten und dezentralen Zahlungssystem. Eine bekannte Kryptowährung ist der Bitcoin.

Kein Zugriff auf Dateien

Mögliche Handlungsempfehlungen/Sofortmaßnahmen:

Berechtigungen kontrollieren (bei einem Firmennetzwerk)

Die Berechtigungen des entsprechenden Benutzers sollten überprüft werden, da aufgrund fehlender Rechte der Zugriff verweigert werden kann.

Computer vom Netz isolieren

Um die Auswirkungen eines möglichen Ransomware-Befalls möglichst einzudämmen, ist der Computer vom Netz zu isolieren. Dazu sollte die Internetverbindung unterbrochen, eine lokale Verbindung getrennt sowie sonstige Anbindungen entfernt werden.

Zahlungsaufforderung nicht nachkommen.

Möglichen Lösegeldforderungen sollte nicht nachgekommen werden, da es auch nach Zahlung nicht sicher ist, ob der Angreifer die Daten wieder entschlüsselt.

 Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Praxistipp

In den vergangenen Jahren waren zahlreiche Ransomware-Varianten im Umlauf. Somit stellt die Gefahr durch Ransomware eine große Bedrohung im Internet dar. Die nachfolgende Auflistung führt eine beispielhafte Auswahl der namenhaften Arten von Ransomware auf:

- WannaCry:
  Verbreitung durch Ausnutzung einer Sicherheitslücke bzw. Schwachstelle von nicht aktualisierten Systemen
- Ryuk:
  Verbreitung über Backdoor-Malware[2], welche wiederum mit Phishing-Methoden[3] arbeitet
- GandCrab:
  Verbreitung durch Phishing-Methoden per E-Mail
- Stop/DJVU:
  Verbreitung durch eine versteckte Installation bei der Ausführung von klassischen Software-Installern

[2] Eine Backdoor-Malware (deutsch: Hintertür) ermöglicht dem Angreifer einen alternativen Zugriff auf ein System. Dabei werden die üblichen Sicherheitsmechanismen des Systems umgangen.

[3] Der Begriff Phishing beschreibt eine gängige Angriffstechnik, bei der eine Person mittels gefälschter Webseiten, E-Mails oder Kurznachrichten getäuscht werden soll. Das verfolgte Ziel dabei ist meist der Diebstahl von persönlichen Daten wie Kennungen und Passwörtern, um letztlich einen Identitätsdiebstahl zu begehen und somit den Personen zu schaden. Gängige Phishing-Methoden sind bspw. „Spear-Phishing“ oder „Pharming.“

Die nachfolgende Abbildung zeigt ein Beispiel einer Lösegeldforderungen, die nach einer Infizierung mit einer Ransomware auf dem Bildschirm des Betroffenen erscheint. Es handelt sich um die Ransomware WannaCry.

Abbildung 15: Lösegeldaufforderung bei der Ransomware „WannaCry“

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet, bezüglich der Gefährdung ausgehend von Ransomware, weiterführende Informationen hinsichtlich der aktuellen Bedrohungslage, einer möglichen Prävention, sowie der Reaktion zum Thema Ransomware an.

Ransomware - Bedrohungslage, Prävention & Reaktion

Einer Ransomware-Attacke zum Opfer gefallenen Person besteht die Möglichkeit, die Schadsoftware über einen Internet-Dienst analysieren zu lassen. Unter dem nachfolgenden Link können Betroffene durch beispielsweise das Hochladen der Lösegeldaufforderung oder einer verschlüsselten Datei die Ransomware automatisch identifizieren lassen. Im Idealfall werden nach einer erfolgten Analyse mögliche Wege aufgezeigt, die Daten zu entschlüsseln.

ID Ransomware

3.4.3 Konto wird missbraucht (Soziale Netzwerke)

Der Betroffene kann sich nicht mehr mit seinen Zugangsdaten auf einer Plattform wie Facebook, Instagram, Twitter o. ä. anmelden. Weitere Hinweise auf einen Angriff können etwa Bilder, Kommentare oder Beiträge sein, die nicht vom Betroffenen selbst veröffentlicht wurden.

Abbildung 16: Kontomissbrauch (Soziale Netzwerke)

Konto wird missbraucht (Soziale Netzwerke)

Mögliche Handlungsempfehlungen/Sofortmaßnahmen:

Aktive Sitzungen kotrollieren

Um einen möglichen Fremdzugriff aufzudecken, sind in den Sicherheitseinstellungen die aktiven Sitzungen zu überprüfen. Dort sind Anmeldungstätigkeiten (z. B. Gerät, Tag, Uhrzeit, Ort) einsehbar.

Zugangsdaten (Passwort) ändern

Das verwendete Passwort muss umgehend geändert werden. Dabei sollte ein starkes Passwort verwendet und ggf. eine 2-Faktor-Authentifizierung eingerichtet werden. Zudem sollten auch die Zugangsdaten der Benutzerkonten von anderen Plattformen gewechselt werden (**vor allem bei Verwendung des gleichen Passwortes**).

Zugangsdaten ändern, wenn Sie sich nicht mehr anmelden können

Setzen Sie Ihr Passwort auf der entsprechenden Plattform zurück („Passwort vergessen“) und ändern dieses anschließend.

Kontakte informieren

Es sollten möglichst alle Kontakte über den Sachverhalt des Missbrauchs informiert und gewarnt werden keine Anhänge oder Links zu öffnen oder möglichen Aufforderungen nachzukommen.

An den Betreiber der Plattform wenden

Bei den meisten Plattformen ist im Impressum des Betreibers eine Mailadresse oder eine Telefonnummer hinterlegt, an die sich in solchen Fällen gewendet werden kann.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt unter dem nachfolgenden Link Ratschläge zur Auswahl eines sicheren Passwortes und zum Umgang mit Passwörtern auf.

Sicherer Umgang mit Passwörtern

3.4.4 Konto wird missbraucht (Online-Banking)

Es wurden Transaktionen durchgeführt, die nicht von dem Betroffenen selbst getätigt wurden. Außerdem kann es sein, dass sich der Betroffene nicht mehr auf der Plattform anmelden kann.

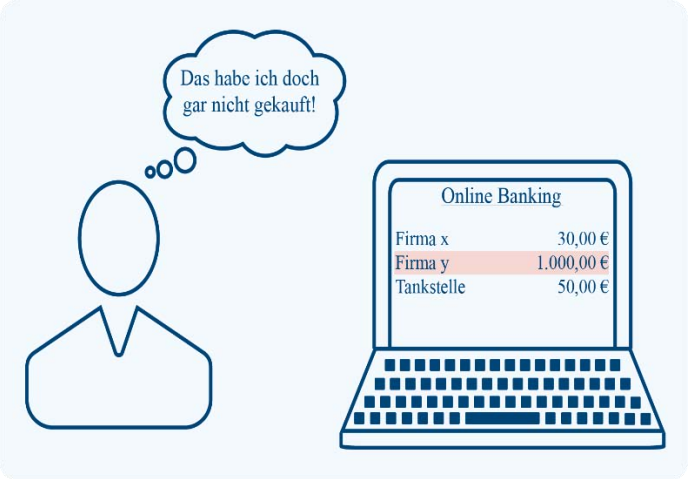

Abbildung 17: Kontomissbrauch (Online-Banking)

Konto wird missbraucht (Online-Banking)

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Zugangsdaten (Passwort) ändern

Das verwendete Passwort muss umgehend geändert werden. Dabei sollte ein starkes Passwort verwendet und ggf. eine 2-Faktor-Authentifizierung eingerichtet werden. Zudem sollten auch die Zugangsdaten der Benutzerkonten von anderen Plattformen gewechselt werden (**vor allem bei Verwendung des gleichen Passwortes**).

Zugangsdaten ändern, wenn Sie sich nicht mehr anmelden können

Setzen Sie Ihr Passwort auf der entsprechenden Plattform zurück („Passwort vergessen“) und ändern dieses anschließend.

An den Betreiber der Plattform wenden

Umgehend telefonisch und per E-Mail den Betreiber der Plattform kontaktieren und die Problematik schildern.

Transaktion widerrufen

Umgehend die getätigten Transaktionen widerrufen. Dies ist oft nur mit Hilfe des Betreibers möglich.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt unter dem nachfolgenden Link Ratschläge zur Auswahl eines sicheren Passwortes und zum Umgang mit Passwörtern auf.

Sicherer Umgang mit Passwörtern

3.4.5 Gerät ist Teil eines Botnetzes

Durch die Infizierung mit einer Schadsoftware wurde das Gerät Teil eines Botnetzes[4]. Infolgedessen erfolgt durch Fernsteuerung ein Missbrauch der Rechenleistung, um bestimmte Aktionen auszuführen. Selbst getätigte Aktionen werden schließlich ungewöhnlich langsam ausgeführt, da die Ressourcenkapazität durch Hintergrundprozesse stark beansprucht werden. Das Gerät reagiert nur noch sehr langsam. Anwendungen oder Dateien lassen sich möglicherweise überhaupt nicht mehr öffnen.

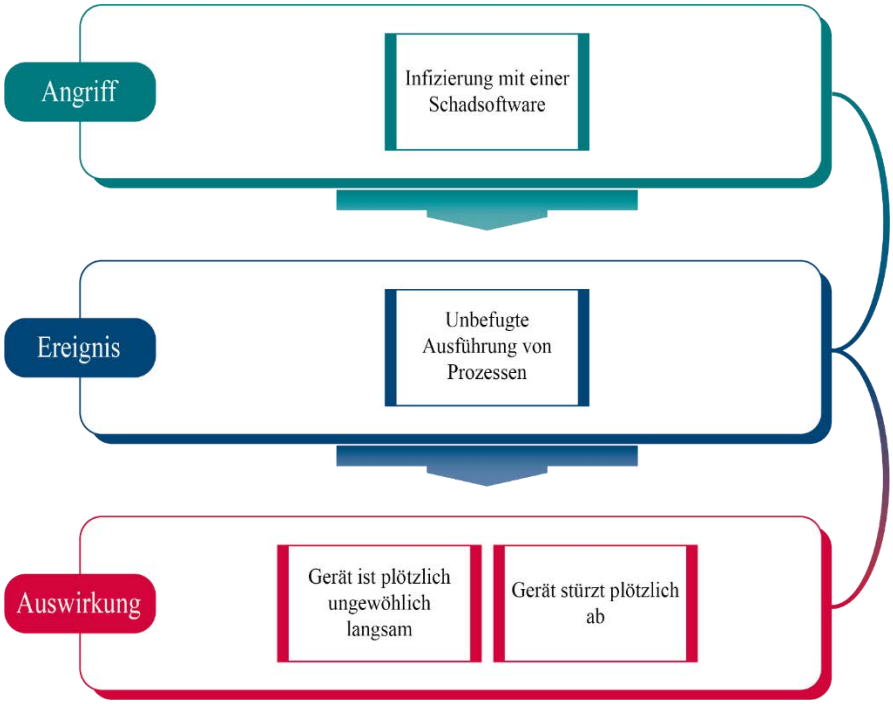

Abbildung 18: Bot-Infektion

Gerät ist Teil eines Botnetzes

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Computer vom Netz nehmen

Um die Auswirkungen möglichst einzudämmen, sollte der Computer vom Netz genommen bzw. die Internetverbindung unterbrochen werden.

Virenscan durchführen

Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, was dringend empfohlen wird, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Internet-Datenverkehr kontrollieren (IT-Kenntnisse erforderlich)

Die versendeten Datenmengen sollten in den Statistiken des Routers überprüft werden. Ungewöhnlich hohe Datenmengen können dabei auf ein Botnetz hinweisen.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

[4] Unter einem Botnetz wird eine Sammlung kompromittierter Geräte (Stand-PC, Laptop, Smartphone) verstanden, die der Angreifer aus der Ferne beliebig steuern kann und für andere Angriffsformen verwendet.

3.4.6 Anwendungen installieren sich von selbst

Dubiose Anwendungen erscheinen auf dem Desktop, obwohl der Betroffene nicht tätig wurde. Die Anwendungen installieren sich dabei im Hintergrund selbst. Dadurch werden die Speicherkapazität sowie die Rechnerleistung beeinträchtigt. Eine Deinstallation der Anwendungen führt nicht zu einer Lösung der Problematik.

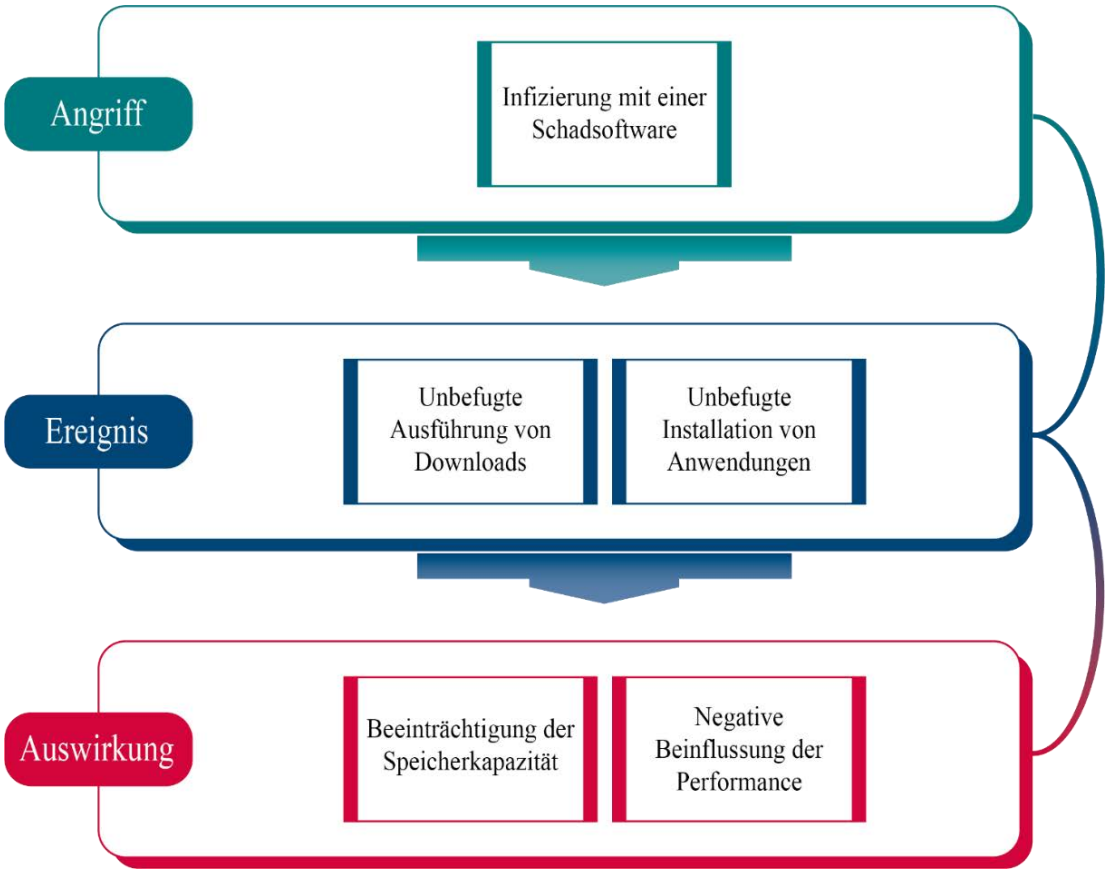

Abbildung 19: Anwendungen installieren sich von selbst

Anwendungen installieren sich von selbst

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Computer vom Netz nehmen

Um die Auswirkungen möglichst einzudämmen und die eigenständigen Installationen zu unterbinden, sollte der Computer vom Netz genommen bzw. die Internetverbindung unterbrochen werden.

Virenscan durchführen

Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, was dringend empfohlen wird, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Computer zurücksetzen

Den Computer mithilfe der integrierten Wiederherstellungsoption zurücksetzen.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Praxistipp

Um Schadsoftware möglichst wirksam und vollständig zu entfernen, kann das Geräte auch zurückgesetzt werden. Oftmals ist dies mit den integrierten Wiederherstellungsoptionen einfach möglich und erfordert kein tiefergehendes Fachwissen.

Unterschieden wird hier zwischen einer zwei grundlegenden Wiederherstellungsvarianten:

1. Persönliche Dateien behalten und Betriebssystem neu installieren
   (Programme und Einstellungen werden zurückgesetzt)
2. Alle Dateien werden entfernt und das Betriebssystem neu installiert
   (Auslieferungszustand wird wiederhergestellt)

Allgemein ist eine vollständige Systemwiederherstellung nur zu empfehlen, wenn zuvor angemessene Datensicherungen durchgeführt wurden oder sich auf dem Gerät keine wichtigen Dateien befinden. Dies spielt vor allem im Unternehmenskontext eine wichtige Rolle und sollte entsprechend berücksichtigt werden.

3.4.7 Umleitung von Suchanfragen / Merkwürdige Weiterleitungen

Nach der Eingabe und Bestätigung zum Öffnen einer Webseite wird der Betroffene auf eine ganz andere Webseite weitergeleitet. Die Eingabe war jedoch korrekt. Zudem besteht die Möglichkeit, dass Suchanfragen in gängigen Suchmaschinen ebenso umgeleitet werden und sich als Ergebnis mehrere Tabs mit verschiedenen, meist ominösen Webseiten öffnen.

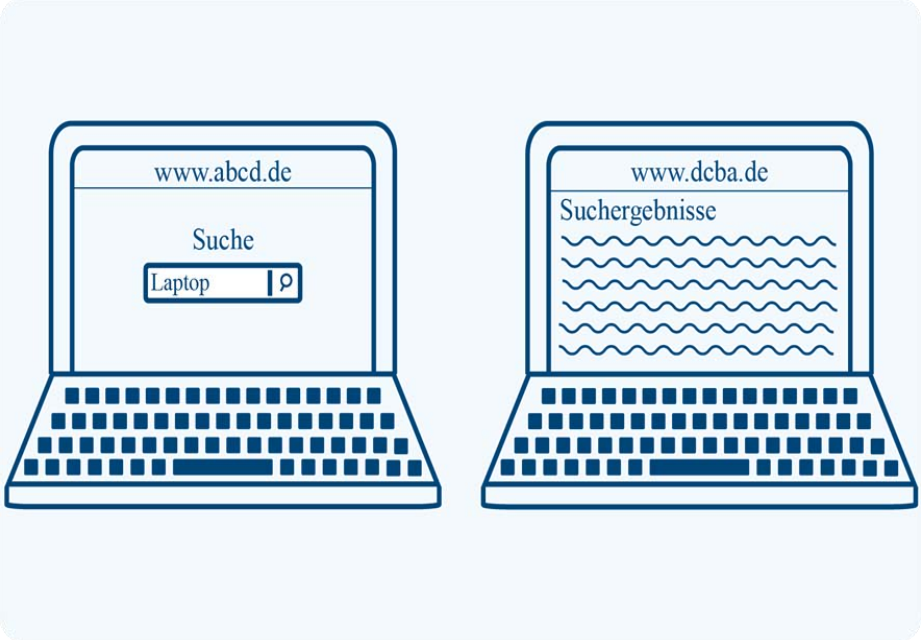

Abbildung 20: Umleitung einer Suchanfrage

Umleitung von Suchanfragen / Merkwürdige Weiterleitungen

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Browser neu starten
: Den genutzten Browser schließen, erneut starten und die Suchanfrage wiederholen.

Alternativen Browser verwenden
: Sollte ein alternativer Internetbrowser auf dem Gerät installiert sein, diesen für die entsprechende Suchanfrage verwenden.

Gerät neu starten
: Das Gerät herunterfahren, stromlos machen, erneut starten und die Suchanfrage wiederholen.

Virenscan durchführen
: Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Browser neu installieren
: Den betroffenen Browser deinstallieren und anschließend eine Neuinstallation anstoßen. Dafür muss die Installationsquelle bzw. ein funktionierender Alternativbrowser vorhanden sein.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Praxistipp

Die übliche Ursache von merkwürdigen Weiterleitungen und Umleitungen der Suchanfragen ist eine sogenannte DNS-Manipulation (DNS-Hijacking[5]). Die Folge einer DNS-Manipulation können Umleitung von Suchanfragen und merkwürdige Weiterleitungen sein.

In der folgenden Abbildung ist erkennbar, wie eine klassische DNS-Manipulation funktioniert.

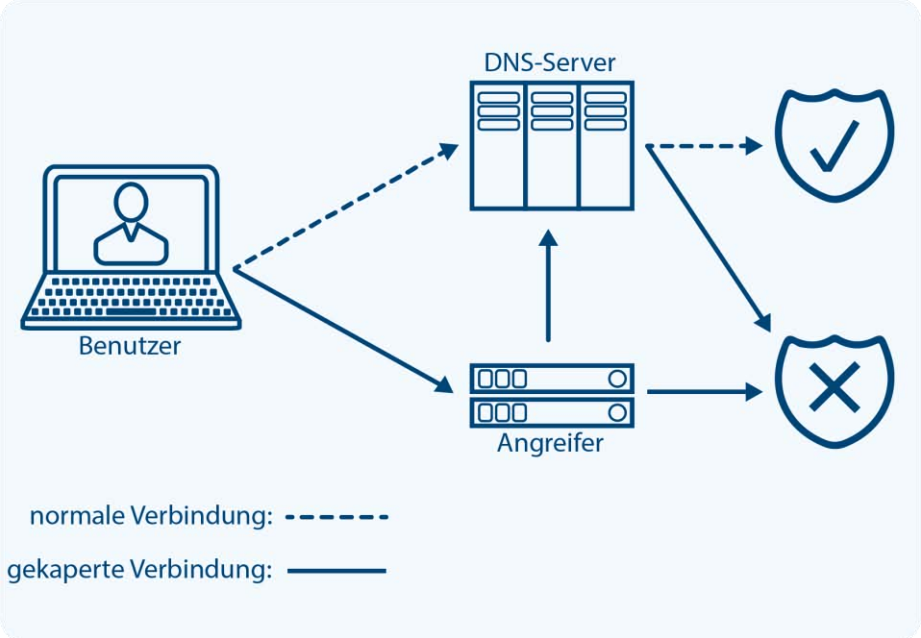

Abbildung 21: Manipulation des DNS-Servers

[5] DNS-Hijacking ist eine Angriffsmethode, bei der die Kommunikation nicht direkt zwischen den beiden Kommunikationspartnern geführt, sondern über einen Dritten geleitet wird.

3.4.8 Datenverlust durch Schadsoftware

Ein Datenverlust durch Schadsoftware kann einerseits zur Folge haben, dass sich Daten nicht mehr an dem entsprechenden Speicherort befinden, da diese von einem Angreifer unbefugt gelöscht und möglicherweise auch gestohlen wurden. Somit hat der Betroffene keinen Zugriff mehr auf seine Daten.

Andererseits besteht die Möglichkeit, dass ein Angreifer Daten gestohlen bzw. unbefugt kopiert hat, diese jedoch nicht gelöscht hat. In diesem Fall hätte der Betroffenen weiterhin Zugriff auf seine Daten.

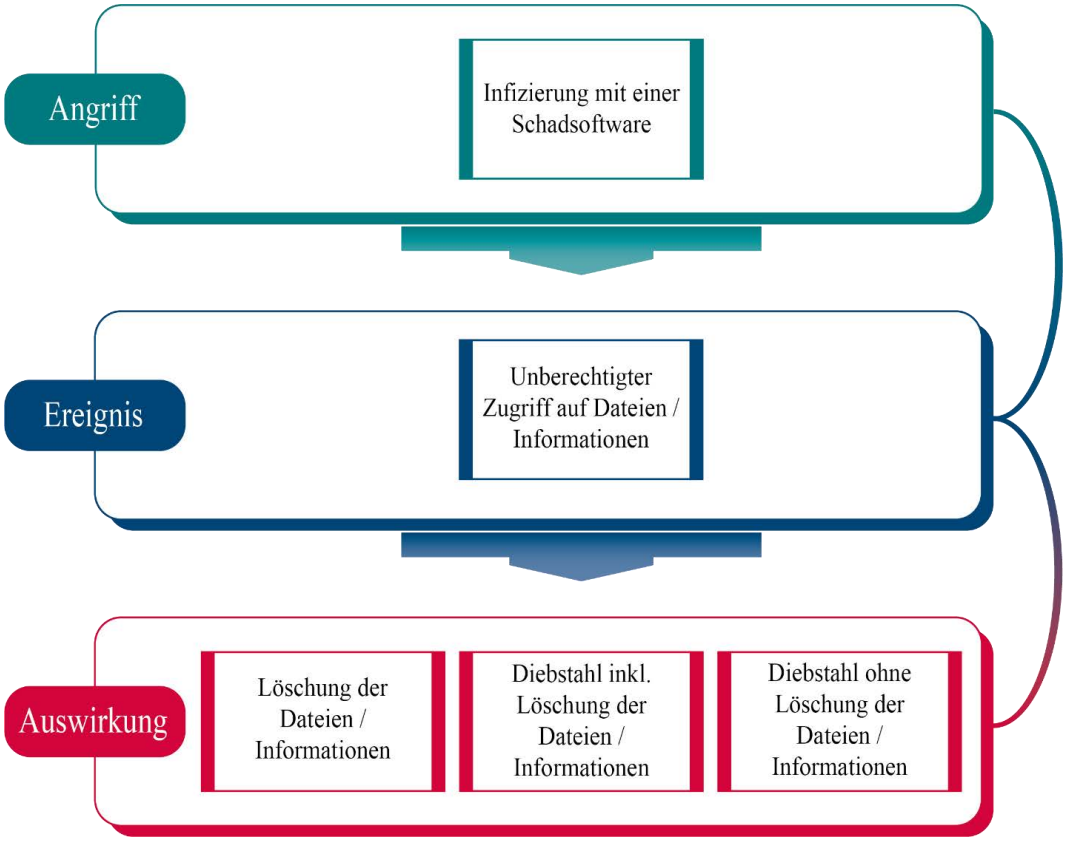

Abbildung 22: Verlust von Daten

Datenverlust durch Schadsoftware

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Computer vom Netz nehmen

Um die Auswirkungen möglichst einzudämmen, sollte der Computer vom Netz genommen bzw. die Internetverbindung unterbrochen werden.

Virenscan durchführen

Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Datensicherung wiederherstellen

Falls eine Datensicherung durchgeführt wurde, können die verlorenen Daten durch das Einspielen der Sicherungskopie wiederhergestellt werden.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.9 Diebstahl eines Mobilgeräts

Bei einem Diebstahl ist das entsprechende Gerät für den Betroffenen nicht mehr verfügbar. Wurden die Daten nicht an einer weiteren Stelle gesichert, ist neben dem finanziellen Schaden auch ein Datenverlust möglich. Je nachdem welche Schutzmaßnahmen auf dem Gerät vorhanden sind, kann der Verlust der Daten auch weitere Folgen, wie z.B. einen Identitätsdiebstahl nach sich ziehen.

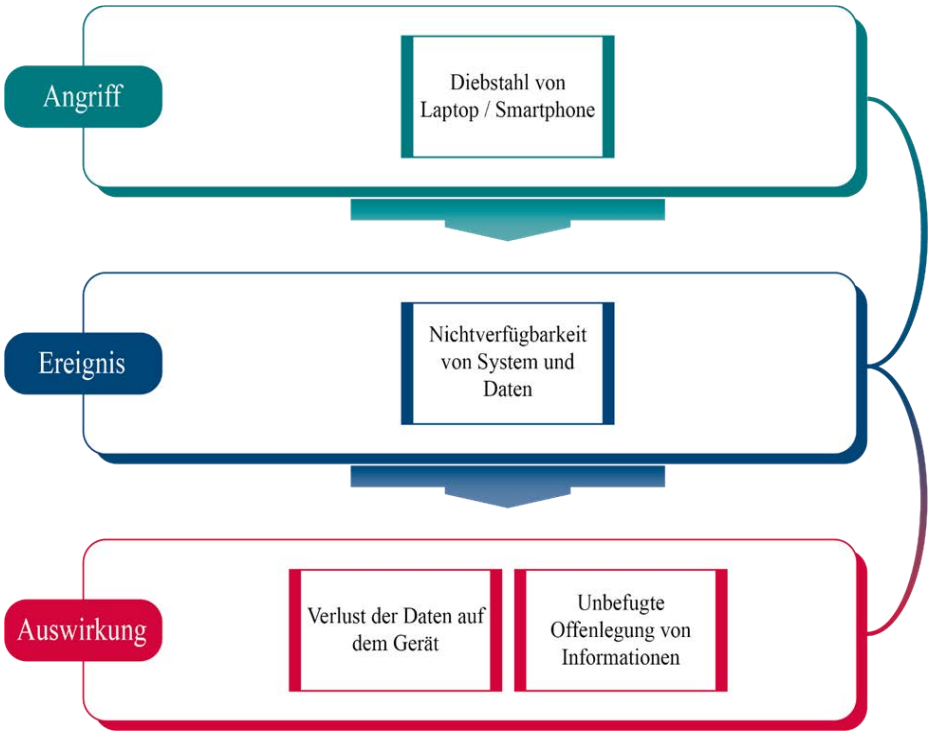

Abbildung 23: Diebstahl eines Mobilgerätes

Datenverlust durch Diebstahl eines Mobilgerätes

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Gerät lokalisieren

Das verlorene Gerät mit Hilfe gegebener Ortungsdienstfunktionalitäten (sofern vorhanden) orten, um den Standort zu ermitteln. Je nach Gerätetyp bzw. Hersteller kann sich die Vorgehensweise unterscheiden. Detaillierte Informationen sind auf den Webseiten der Hersteller zu finden.

SIM-Karte sperren

Der Mobilfunkanbieter sollte kontaktiert und die SIM-Karte gesperrt werden.

Benutzer deaktivieren (bei einem Firmennetzwerk)

Das Benutzerkonto des Betroffenen sollte umgehend deaktiviert bzw. die Zugriffe gesperrt werden.

Daten aus der Ferne löschen

Das gestohlene Gerät mittels gegebener Funktionalität löschen. Dadurch werden die sich darauf befindlichen Daten entfernt und können somit nicht missbraucht werden. Je nach Gerätetyp bzw. Hersteller kann sich die Vorgehensweise unterscheiden. Detaillierte Informationen sind auf den Webseiten der Hersteller zu finden.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.10 Gerät agiert eigenständig

Das Gerät agiert, ohne dass der Betroffene Tätigkeiten ausgeführt hat. Dabei bewegt sich der Mauszeiger eigenständig, Anwendungen, Webseiten oder Ordner öffnen sich ohne Einwirkung des Betroffenen.

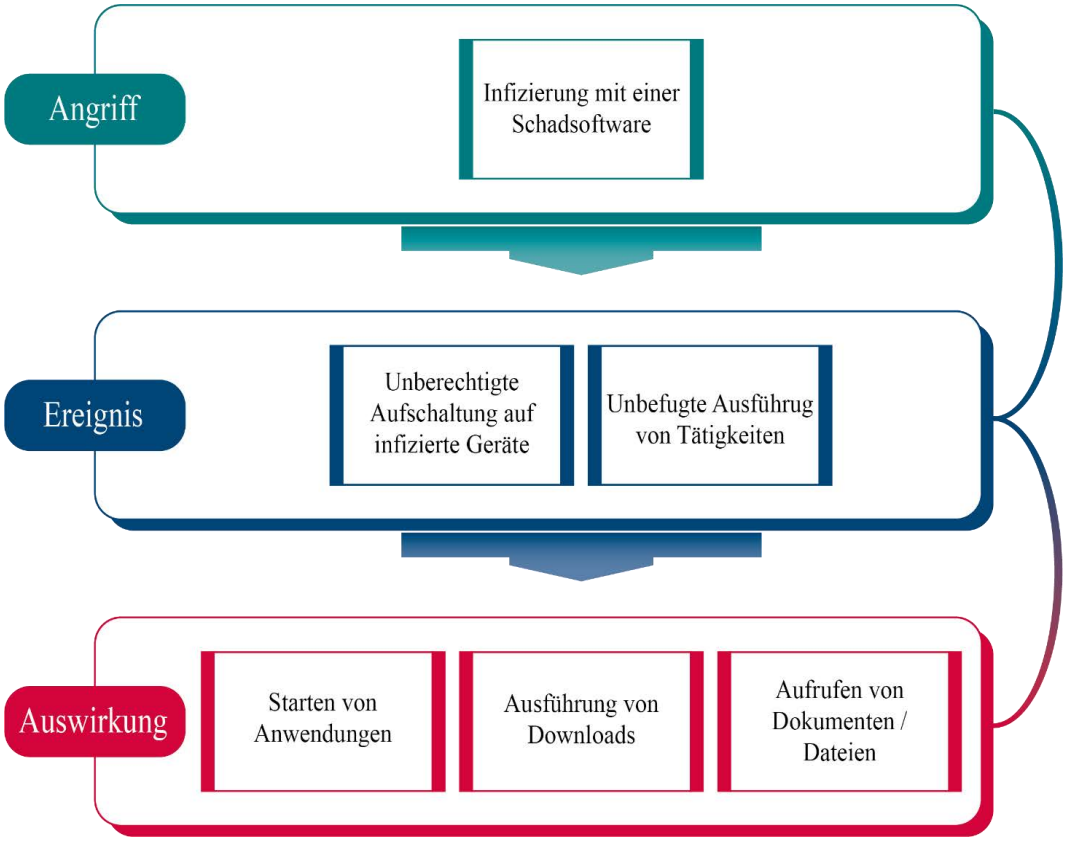

Abbildung 24: Gerät agiert eigenständig

Computer agiert eigenständig

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Computer vom Netz nehmen

Um die Auswirkungen möglichst einzudämmen und die unberechtigten Handlungen zu unterbinden, sollte der Computer vom Netz genommen bzw. die Internetverbindung unterbrochen werden.

Virenscan durchführen

Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.11 Ausspionieren (Mitlesen, Mithören, Mitschauen)

Ein Betroffener wird durch einen unberechtigten Dritten ausspioniert. Dabei ist es denkbar, dass Daten und Informationen (z. B. E-Mails, Dokumente) ohne dessen Wissen oder Zustimmung von einem Angreifer mitgelesen werden. Außerdem kann das Mikrofon des Gerätes unbewusst eingeschaltet und somit das Mithören ermöglicht werden. Zuletzt ist eine Webcam anfällig für Spionageangriffe. Wird diese gekapert, hat ein Angreifer jederzeit die Möglichkeit diese einzuschalten und den Betroffenen auf diese Weise auszuspionieren.

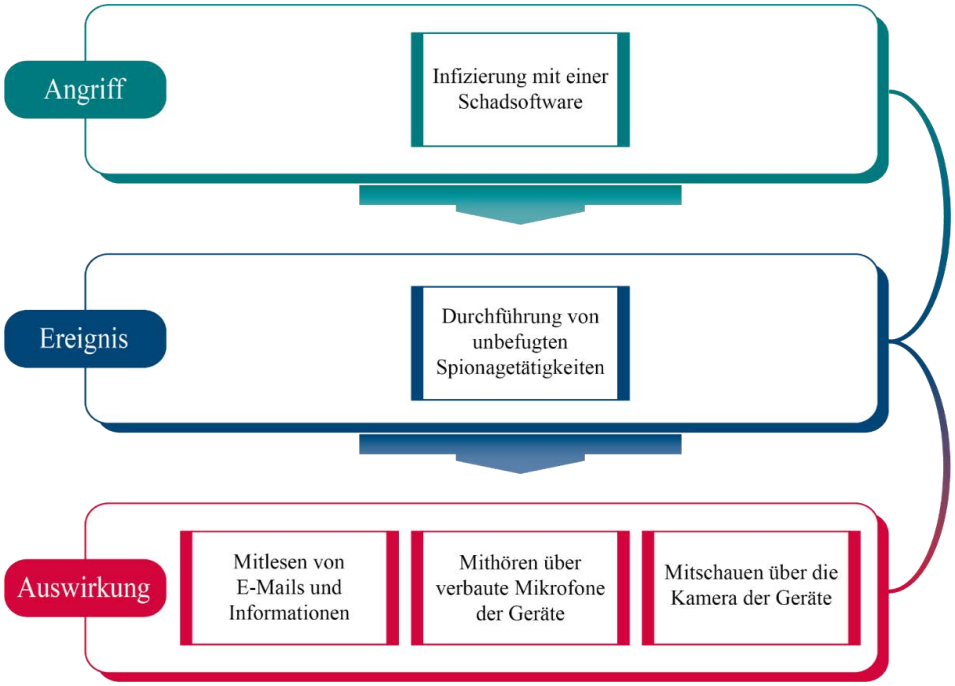

Abbildung 25: Spionagetätigkeiten

Ausspionieren

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Passwortänderung

Sollte der Verdacht bestehen, dass unberechtigte Personen persönliche Informationen mitlesen oder hören, sollte umgehend jedes Passwort zu Diensten oder Portalen, die persönliche Daten enthalten oder über die Passwörter zurückgesetzt werden können, geändert werden.

Sicherheitssoftware kontrollieren

Nach einem Verdacht der Spionage, sollte der Virenscanner und die lokale Firewall auf Aktivität geprüft werden. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Updates installieren

Nachdem die Passwörter geändert wurden, sollten alle Betriebssystem- und Sicherheits-updates auf allen genutzten Geräten installiert werden.

Webcam/Mikrofon deaktivieren oder deinstallieren

Im Gerätemanager sollte die Webcam/ das Mikrofon deaktiviert oder sogar deinstalliert werden, sofern diese selten im Gebrauch sind oder sogar gar nicht benötigt werden.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.12 Ungewöhnliche Warnhinweise auf dem Desktop

Auf dem Desktop des Computers tauchen regelmäßig Warnhinweise auf, die den Betroffenen auf mögliche Gefahren aufmerksam machen möchten. Die Warnhinweise rufen dazu auf, eine bestimmte Software zu installieren oder sogar zu kaufen, um die zugrundeliegende Gefahr zu beseitigen. Die sich öffnenden Fenster können zwar geschlossen werden, öffnen sich jedoch nach einem zufälligen Zeitraum erneut.

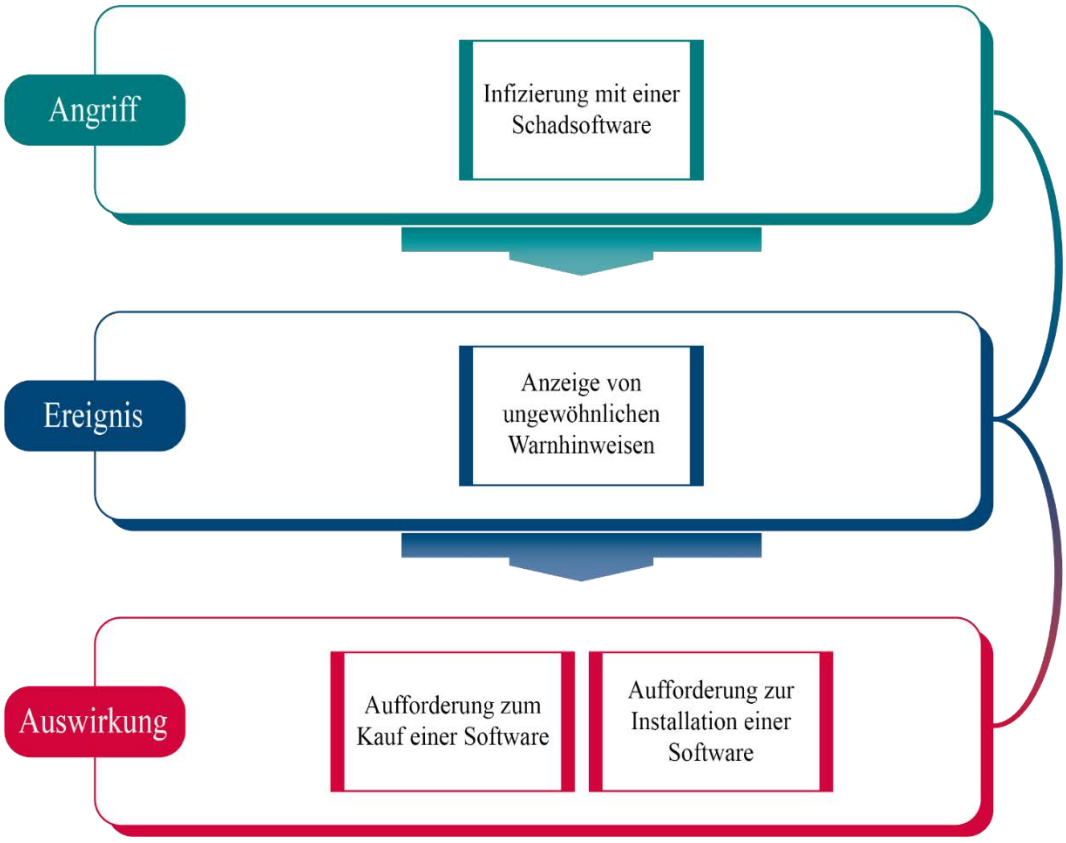

Abbildung 26: Ungewöhnliche Warnhinweise erscheinen

Ungewöhnliche Warnhinweise auf dem Desktop

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Aufforderungen nicht nachkommen

Der Aufforderung ein Programm zu installieren oder gar zu kaufen, sollte nicht nachgekommen werden.

Virenscan durchführen

Falls ein Virenschutzprogramm auf dem Computer vorhanden ist, sollte ein Virenscan manuell gestartet werden. Wurde ein Virus erkannt, lässt sich dieser möglicherweise mit Hilfe des Virenschutzprogrammes direkt bereinigen. Eine lückenlose und vollständige Beseitigung durch das Virenschutzprogramm ist nicht in jedem Fall zu erwarten.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.13 Virenscanner hat einen Virus erkannt

Im Rahmen der gewöhnlichen Nutzung eines Computers öffnet sich plötzlich das installierte Virenschutzprogramm. Grund dafür ist, dass der Virenscanner Alarm schlägt, da der Computer mit einem Virus infiziert bzw. eine Schadsoftware oder unerwünschte Programme erkannt wurden.

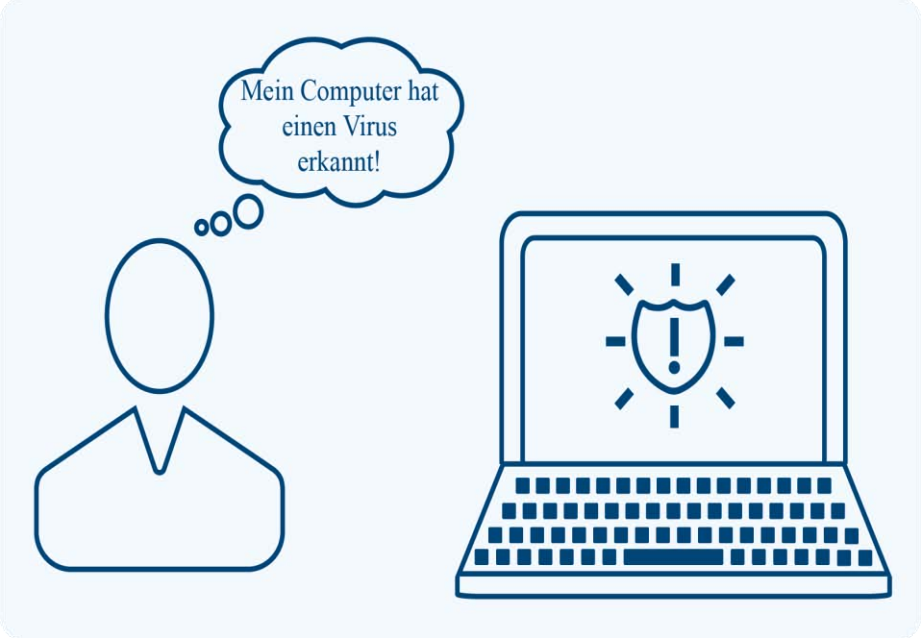

Abbildung 27: Virenscanner schlägt an

Virenscanner hat einen Virus erkannt

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Virenscanner arbeiten lassen

Der automatische durch das Virenschutzprogramm angestoßene Virenscan sollte nicht unterbrochen werden (z.B. Ausschalten). Erkannte Bedrohung können meist von diesem entschärft werden.

Computer vom Netz nehmen

Um die Auswirkungen möglichst einzudämmen und eine weitere Ausbreitung zu unterbinden, sollte der Computer vom Netz genommen bzw. die Internetverbindung unterbrochen werden (Nur durchzuführen, wenn das Virenschutzprogramm die Bedrohung nicht unterbinden konnte).

Dokumente schließen und Programme beenden

Um einen Datenverlust zu vermeiden, sollten alle offenen Dokumente gespeichert und geschlossen werden. Zudem sollten aktive Programme beendet werden.

Weiterführende Überprüfung von Dateien

Um sicher zu gehen, dass keine harmlosen Dateien als Virus erkannt wurden, sollten die als Schadsoftware ermittelten Dateien weiter untersucht werden. Mithilfe des Onlinedienstes der Webseite Virustotal kann die entsprechende Datei überprüft werden.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

3.4.14 Fälschliche Aufforderung einer Passwortänderung per E-Mail

Ein Betroffener erhält eine skurrile E-Mail. In dieser wird vor einer möglichen Kompromittierung des Passwortes gewarnt. Diesbezüglich wird er dazu aufgefordert das Passwort entsprechend zu ändern, um eine unbefugte Nutzung des Benutzerkontos durch einen nicht autorisierten Dritten zu verhindern. Um die Passwortänderung realisieren zu können, ist ein Link hinterlegt. Dieser führt zu einer Webseite, auf der ein Wechsel des Passwortes durchgeführt werden kann. Dabei wird zum einen das alte Passwort abgefragt und zum anderen die Eingabe des neuen Passwortes gefordert.

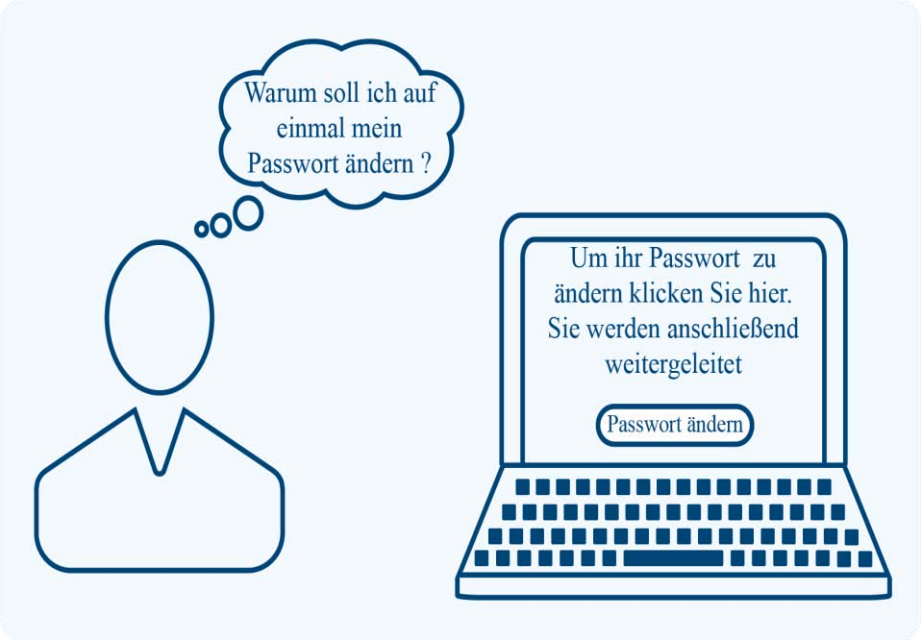

Abbildung 28: Fälschliche Aufforderungen zur Passwortänderung

Fälschliche Aufforderung einer Passwortänderung per E-Mail

Mögliche Handlungsempfehlungen / Sofortmaßnahmen:

Aufforderung nicht nachkommen

Der Aufforderung zur Änderung des Passwortes sollte unter keinen Umständen nachgekommen werden. Zudem sollte vom Klicken auf den Link abgeraten werden.

E-Mail-Absender verifizieren (IT-Kenntnisse erforderlich)

Der tatsächliche Absender einer E-Mail lässt sich über die sog. Header-Information herausfinden. Hierbei ist die Absenderadresse zu prüfen und mit einer unverfälschten E-Mail-Adresse der entsprechenden Plattform zu verifizieren.

Support kontaktieren

Um Aufschluss bzw. Hintergrundinformationen über die erhaltene E-Mail zu erhalten, ist der Kundenservice der entsprechenden Plattform zu kontaktieren.

Zugangsdaten ändern

Über die manuelle Eingabe im jeweiligen Browser die Webseite direkt aufrufen und dort die Zugangsdaten bzw. das Passwort ändern. Dabei sollte ein starkes Passwort verwendet und ggf. eine 2-Faktor-Authentifizierung eingerichtet werden.

Zur weiteren Behandlung des Vorfalls sollte ein Vorfall-Experte kontaktiert werden.

Praxistipp

Jeden Tag werden unzählige Phishing Mails versendet. Auf den ersten Blick sehen diese Mails täuschend echt aus. Anhand der folgenden Merkmale können Phishing-Mails enttarnt werden:

- Rechtschreib- und Grammatikfehler
  Phishing Mails sind oftmals gespickt mit Rechtschreib-, Grammatik- und Zeichensetzungsfehlern.
- Mails in fremder Sprache
  Handelt es sich zum Beispiel um ein deutsches Geldinstitut, werden Sie sicher nicht auf Englisch kontaktiert.
- Anrede nicht mit Ihrem Namen
  Von einer Bank oder einem Geschäftspartner, wie zum Beispiel Online-Zahlungsdiensten, werden Sie in E-Mails grundsätzlich nicht mit „Sehr geehrter Nutzer“ oder „Lieber Kunde“ angeschrieben. Es gibt allerdings auch Täter, die sich die Arbeit machen und Sie mit Ihrem Namen anschreiben.
- Eingabe von Zugangsdaten
  PIN und TAN werden besonders von Geldinstituten niemals telefonisch oder per E-Mail abgefragt.
- Aufforderung zur Öffnung einer Datei
  Bei E-Mails mit Dateianhängen sollten Sie grundsätzlich misstrauisch sein. Diese Dateien könnten Schadsoftware enthalten und Ihr System beim Öffnen der Datei infizieren.
- Aufforderung einen Link zu klicken
  Bei E-Mails mit der Aufforderung einen Link zu klicken, sollten Sie ebenfalls immer misstrauisch sein. Besser ist es die Internetseite selbst aufzurufen, indem Sie diese in das Adressfeld des Browsers eintippen.
- Mailheader prüfen
  Eine Phishing-Mail kann durch das Auslesen des Headers erkannt werden.

Weiterführende Informationen

Der Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. gibt eine detaillierte Übersicht über aktuell im Umlauf befindliche Phishing-Mails.

Phishing-Radar: Aktuelle Warnungen

Darüber hinaus bietet der nachfolgende Link eine Hilfestellung beim Lesen des Mail-Headers. Auf diesem Weg können Phishing-Mails oder sonstige Fake-Mails erkannt werden.

Mail-Header auslesen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt unter dem nachfolgenden Link Ratschläge zur Auswahl eines sicheren Passwortes und zum Umgang mit Passwörtern auf.

Sicherer Umgang mit Passwörtern

3.5 Zusammenfassung

Das Modul 2 befasst sich mit typischen Sicherheitsvorfällen, die durch Cyber-Angriffe herbeigeführt wurden. Zunächst wurde der Begriff „IT-Sicherheitsvorfall“ beschreiben und anhand einer Auflistung von Merkmalen verdeutlicht. Der Digitaler Ersthelfer ist somit in der Lage IT-Sicherheitsvorfälle im Wesentlichen zu identifizieren und nach Möglichkeit Handlungsempfehlungen auszusprechen. Diese können bei der zugrundeliegenden Problematik punktuell einen Lösungsansatz liefern, repräsentieren aber im Wesentlichen Sofortmaßnahmen. Dadurch kann das potenzielle Schadensausmaß eingegrenzt oder eine weitere Ausbreitung verhindert werden. Der IT-Sicherheitsvorfall kann dadurch jedoch nicht abschließend behoben werden. Diesbezüglich ist ein Vorfall-Experte zu konsultieren.

Das Wichtigste in Kürze

IT-Sicherheitsvorfall:

- Ein IT-Sicherheitsvorfall führt i. d. R. zu einer andauernden Beeinträchtigung bzw. einem Ausfall.
- Je nach Art ist mit einem erheblichen Schadensausmaß zu rechnen.
- Auslöser: Cyber-Angriff (kriminelle Absichten).
- Oftmals ist ein IT-Sicherheitsvorfall mit einer Verletzung der Privatsphäre (Privatperson) oder Reputationsschäden (Unternehmen oder der Person) verbunden.

3.6 Aufgabe

Die nachfolgende Aufgabe soll das vermittelte Wissen sowie die erlangten Kenntnisse überprüfen. In diesem Kontext ist die Aufgabe möglichst praxisorientiert. Ziel ist es einen Einblick in die Praxis zu liefern und den erworbenen Kenntnisstand zu festigen. Die Lösungen befinden sich im Anhang.

3.6.1 Aufgabe 1

Lesen Sie sich die folgenden Szenarien durch und sprechen Sie Handlungsempfehlungen aus, die einem Betroffenen als Lösungsansatz zur Behebung des Problems gegeben werden können.

Szenario 1:

Auf dem Desktop des Laptops tauchen Programme auf, die nicht vom Betroffenen selbst installiert wurden. Selbst nach einer Deinstallation werden diese erneut eigenständig installiert.

Szenario 2:

Nach der Ausführung einer Suchanfrage über Google, gelange ich nicht zur gewünschten Ergebnisseite. Es öffnet sich stattdessen eine merkwürdige Seite, welche mir die Suchergebnisse anzeigt.

Szenario 3:

Der Versuch ein Dokument zu öffnen schlägt fehl. Es öffnet sich eine Meldung mit der Aufforderung ein Lösegeld zu bezahlen.

Szenario 4:

Ein Bekannter hat mich auf eine Nachricht angesprochen, die ich ihm per Facebook geschickt habe. Es ging um einen Link für ein Video. Ich bin mir allerdings sicher, dass ich ihn nie über diese Plattform kontaktiert habe.

3.6.2 Aufgabe 2

Nachfolgenden ist eine Reihe von verschiedenen Szenarien aufgelistet. Bestimmen Sie, ob es sich um eine IT-Störung oder einen IT-Sicherheitsvorfall handelt.

1. Maus/Tastatur funktioniert nicht
2. Es besteht keine Internetverbindung
3. Zugangsdaten wurden ausspioniert
4. Diebstahl von mobilen Geräten mit sensiblen Daten
5. Verlust von Daten
6. Programme installieren sich eigenständig
7. Computer startet, aber Bildschirm bleibt schwarz
8. Merkwürdige Weiterleitungen
9. Computer bleibt beim Hochfahren hängen
10. Ungewöhnliche Warnhinweise auf dem Desktop
11. Drucker druckt nicht
12. Fehlermeldung wird auf dem Bildschirm angezeigt
13. Virenscanner hat einen Virus erkannt
14. Geld vom Konto abgebucht
15. USB/CD wird nicht erkannt
16. Computer agieren ohne interne Eingabe
17. Dateien sind plötzlich verschlüsselt
18. Bild auf dem Bildschirm wird nicht richtig angezeigt

4 Modul 3 – Serviceorientiertes Telefongespräch

4.1 Einführung

Wenn Unternehmen oder Privatpersonen aufgrund eines IT-Sicherheitsvorfalls den Kontakt per Telefon suchen, ist es wichtig, dass kompetente und qualifizierte Digitale Ersthelfer die Telefonate entgegennehmen. Neben einer angemessenen Kompetenz und Qualifikation ist jedoch auch das korrekte und kompetente Auftreten nicht zu unterschätzen. Gerade in einem Telefongespräch ist der erste Eindruck ungemein wichtig, da lediglich das Gehörte maßgelblich ist. Es gilt professionelles und lösungsorientiertes Telefonmanagement zu verinnerlichen, um Hilfesuchende angemessen und gezielt zu unterstützen.

Zur Sicherstellung eines fachgerechten und serviceorientieren Auftretens am Telefon, müssen grundlegende Verhaltensweisen eine Selbstverständlichkeit werden. Auf diese Weise können zielgerichtete Telefonate mit Hilfesuchenden geführt werden. Im Wesentlichen geht es neben dem freundlichen Verhalten auch darum, die Problematik möglichst präzise aufzunehmen, um eine entsprechende Eingrenzung schnellstmöglich vornehmen zu können. Darauf aufbauend sollen einem Hilfesuchenden sinnvolle Handlungsempfehlungen an die Hand gegeben werden, die diesen bei der Behebung des IT-Sicherheitsvorfalls unterstützen.

Das Modul 3 behandelt die Durchführung eines fachgerechten und professionellen Telefongesprächs. Diesbezüglich wird dargestellt, wie ein serviceorientiertes Telefonat durchgeführt werden kann. Zu Beginn des Moduls werden dem Digitaler Ersthelfer grundlegende Rahmenbedingungen aufgezeigt, die er während eines Erste-Hilfe-Gespräches berücksichtigen sollte. In diesem Zusammenhang werden der Empfang eines Anrufers und die Aufnahme der Problematik erläutert. Anschließend wird aufgezeigt wie der Sachverhalt entsprechend eingegrenzt und identifiziert werden kann. Letztlich wird beschrieben nach welchen Kriterien es sinnvoll ist Handlungsempfehlungen auszusprechen und auf welche Weise dies erfolgen kann. Im Anschluss werden die wichtigsten Inhalte zusammengefasst.

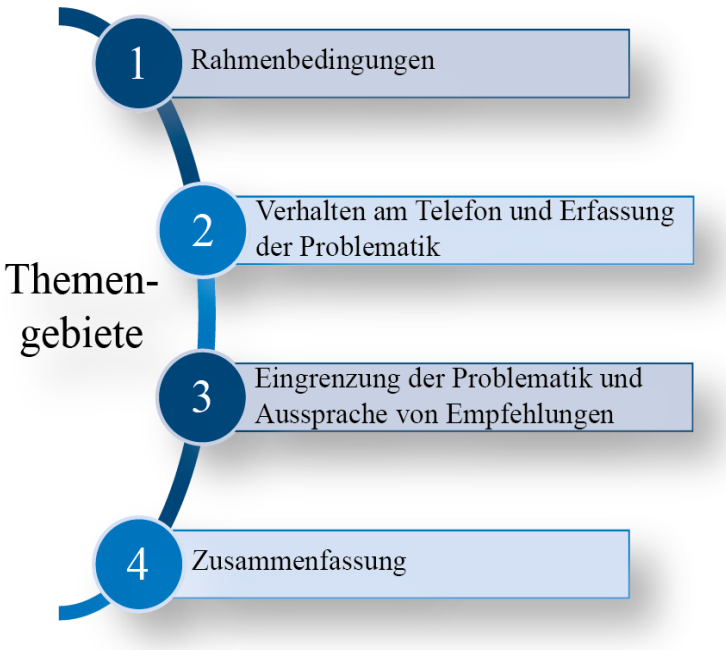

Abbildung 29: Themengebiete Modul 3

4.2 Intention und Lernziele

Modul 3 setzt sich mit dem korrekten Verhalten eines Digitalen Ersthelfers am Telefon auseinander. Grundlegend für ein erfolgreiches Gespräch ist neben der Beachtung von verschiedenen Rahmenbedingungen das professionelle Auftreten des Digitaler Ersthelfers. Weiterhin ist die sorgfältige Aufnahme des Sachverhaltes im ersten Schritt des Telefonats die Grundlage für die weitere Behandlung und essenziell für ein serviceorientiertes Telefongespräch. Diesbezüglich werden gezielte Fragen behandelt, welche bei der Aufnahme essenziell sind. Auf dieser Basis wird anschließend dargestellt, wie die Problematik entsprechend eingegrenzt bzw. identifiziert werden kann. Letztlich wird aufgezeigt, inwiefern die Aussprache von Handlungsempfehlungen möglich bzw. sinnvoll ist und wie dies zu erfolgen hat.

Nach Bewältigung dieses Moduls ist ein potenzieller Digitaler Ersthelfer dazu in Lage, Telefongespräche entgegenzunehmen und einen Betroffen bei der Behebung der entsprechenden Problematik zu unterstützen.

Nach Abschluss dieses Moduls sind die Schulungsteilnehmer dazu in der Lage:

 Einen IT-Sicherheitsvorfall und dessen Merkmale zu beschreiben,

 Typische IT-Sicherheitsvorfälle zu identifizieren,

 Betroffene bei der Handhabung von IT-Sicherheitsvorfällen zu unterstützen.

4.3 Digitale Rettungskette

Unter der Digitalen Rettungskette wird eine Methodik verstanden, die KMU sowie Privatpersonen bei der Reaktion auf IT-Sicherheitsvorfälle durch Cyber-Angriffe unterstützen sollen. Um für jeden Betroffenen die passende Unterstützungsleistung anbieten zu können, besteht die Digitale Rettungskette aus mehreren Eskalationsstufen. Sie erlaubt es Betroffenen, mit ihren IT-Sicherheitsvorfällen an einem beliebigen Glied einzusteigen, aber auch aktiv an das nächste Glied in der Kette zu eskalieren, sollte die momentane Stufe nicht in der Lage sein, den Vorfall zu bekämpfen. Dabei reichen die Stufen der Digitalen Rettungskette von schriftlichen Leitfäden über eine telefonische Unterstützung, bis hin zu einem Team von Experten, das vor Ort tätig werden kann.

Die nachfolgende Abbildung stellt den Aufbau der Digitalen Rettungskette dar.

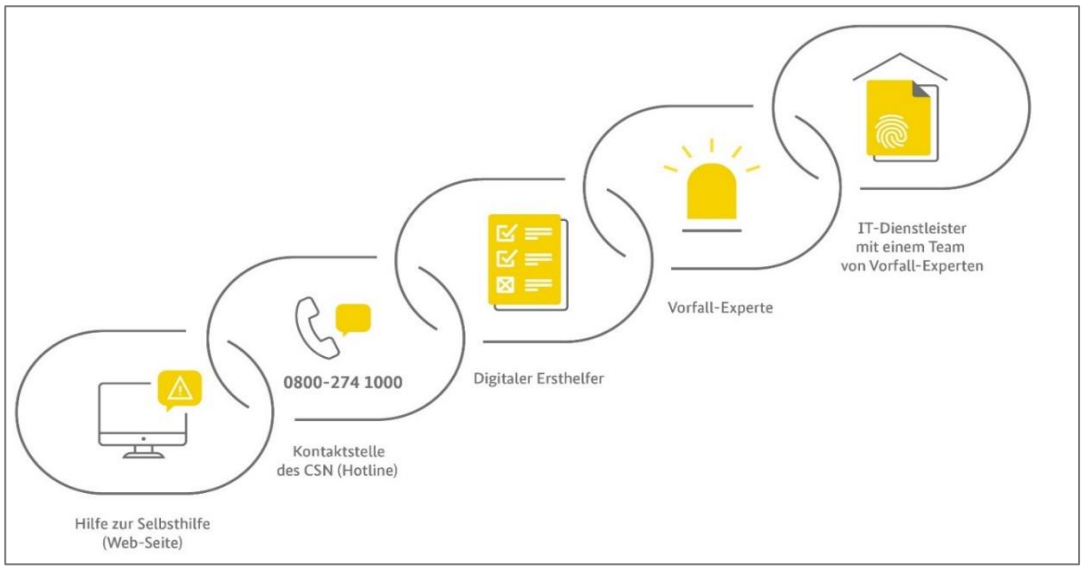

Abbildung 30: Digitale Rettungskette

4.3.1 Überblick über die Digitale Rettungskette

Mit dem Konzept einer Digitalen Rettungskette arbeiten Digitale Ersthelfer, Vorfall-Experten und IT-Sicherheitsdienstleister aufeinander abgestimmt. Sie bilden ein übergreifendes Komplettsystem, welches, beginnend mit der Identifizierung und über Hilfestellung, bis hin zur umfassenden Lösungsbetreuung und Vorfallklärung, eine Kette unterschiedlicher reaktiver Hilfsangebote etabliert. Mit diesem bundesweit einheitlichen Rahmen der Vorfallbearbeitung wird Verständlichkeit und Akzeptanz bei den Zielgruppen der kleinen und mittelständigen Unternehmen, genauso wie bei den Bürgern, erreicht.

4.3.2 Eskalation in der Digitalen Rettungskette

Bei der Digitalen Rettungskette stehen die folgenden Eskalationsschritte eines IT-Sicherheitsvorfalls in einer aufeinander abgestimmten Reihenfolge:

1. Hilfe zur Selbsthilfe
2. Anruf bei der Kontaktstelle (Hotline) des Cyber-Sicherheitsnetzwerks abgeben
3. telefonische Ersthilfe durch Digitalen Ersthelfer
4. Analyse durch den Vorfall-Experten
5. Unterstützung durch einen IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten.

Jeder dieser Schritte stellt hierbei eine Eskalation des IT-Sicherheitsvorfalls in eine höhere Stufe dar. Es können, je nach Eskalation, auch einzelne Glieder der Kette in jede Richtung übersprungen werden.

4.3.3 Kontaktstelle des Cyber-Sicherheitsnetzwerks

Die erste persönliche Anlaufstelle des Cyber-Sicherheitsnetzwerks ist entweder die Webseite des Cyber-Sicherheitsnetzwerk oder die Kontaktstelle (zentrale Hotline), die dem Betroffenen hilft, den IT-Sicherheitsvorfall einzuschätzen und auf die Liste der Digitalen Ersthelfer verweist.

Betroffene eines IT-Sicherheitsvorfalls entscheiden selbstständig, ob Sie zunächst eigenständig die Erste-Hilfe-Maßnahmen anhand der Informationen der Webseite in Anspruch nehmen oder sich sofort an die Kontaktstelle des Cyber-Sicherheitsnetzwerks (Hotline) wenden. Die Kontaktstelle ist über eine kostenfreie Telefonnummer 0800-274 1000 zu erreichen und hilft den betroffenen Personen den IT-Sicherheitsvorfall einzuschätzen sowie bei der Entscheidung das entsprechende Glied der Digitalen Rettungskette zu kontaktieren. Am Ende eines Gespräches erhalten die Betroffenen eine Liste von regionalen Experten der

gewählten Eskalationsstufe. Dabei kann es sich um regionale Digitale Ersthelfer oder zertifizierte Vorfall-Experten bzw. IT-Dienstleister handeln.

Die Kontaktaufnahme mit Experten beruht auf freiwilliger Basis. Es steht allen Betroffenen jeder Zeit frei zu entscheiden, ob sie eine Unterstützungsleistung seitens des Cyber-Sicherheitsnetzwerkes nutzen möchte oder nicht.

4.3.4 Überblick über die Aufgaben des Digitalen Ersthelfers

Für die First-Level-Unterstützung sind im Cyber-Sicherheitsnetzwerk Digitale Ersthelfer registriert, die schnell telefonische Ersthilfe durchführen. Sie bieten telefonische Ersthilfe zur Behebung von kleineren IT-Störungen- und IT-Sicherheitsvorfällen an. Anhand des vorliegenden Leitfadens versuchen sie das IT-Sicherheitsproblem innerhalb kürzester Zeit zu lösen und dem Betroffenen Handlungsempfehlungen an die Hand zu geben. Sollten Digitale Ersthelfer ein Problem nicht lösen können, so empfehlen sie dem Betroffenen je nach Schadensumfang, sich an einen Vorfall-Experten oder IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten zu wenden.

Ein Digitaler Ersthelfer führt in der Regel noch keinen Vor-Ort-Service durch, sondern bietet die Ersthilfe vorwiegend per Telefon oder in Einzelfällen auch per E-Mail o.ä. digitalen Kommunikationswegen an.

Der „Leitfaden zur Reaktion auf IT-Sicherheitsvorfälle für Digitale-Ersthelfer“ gibt einen Rahmen für die Tätigkeit als Digitaler Ersthelfer vor und unterstützt ihn bei der Analyse und den Handlungsempfehlungen. Die kostenfreie Basisausbildung zum Digitalen Ersthelfer steht allen interessierten und EDV-affinen Personen offen. Es handelt sich hierbei um ein Erste-Hilfe-Programm, welches in einem Onlinekurs vermittelt wird. Erst danach können sie sich bei Interesse im Cyber-Sicherheitsnetzwerk registrieren lassen und die Vorfall-Bearbeitungsleistung anbieten.

Ist der Vorfall weder mit angemessenem Aufwand noch in einem ersten Gespräch zu beheben, empfiehlt der Digitale Ersthelfer, den Vorfall zur weiterführenden Analyse und Behebung an einen Vorfall-Experten oder einen IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten zu kontaktieren. Die Erkenntnisse und Maßnahmen, die zur Behebung des Vorfalls durchgeführt wurden, werden fortlaufend in einem Vorfallbericht dokumentiert. So hat der im Nachgang mit dem Vorfall beschäftigte Vorfall-Experte einen Überblick über bereits erfolgte Maßnahmen und Analysen. Dieser Bericht wird ausschließlich dem Betroffenen nach Beendigung des Gespräches digital übermittelt, so dass der Betroffene jederzeit die Datenhoheit behält.

4.3.5 Aufgaben des Vorfall-Experten

Die Aufgabe des Vorfall-Experten ist es, nach einer ersten Analyse des Digitalen Ersthelfers, ein ergänzendes, weiteres Unterstützungsangebot zur Reaktion auf IT-Sicherheitsvorfälle anzubieten. Das Unterstützungsangebot basiert auf der Grundlage der Ersteinschätzung der Hotline oder der Analyse des Digitalen Ersthelfers. Im Gegensatz zu Digitalen Ersthelfern handelt es sich bei Vorfall-Experten um ausgebildete IT-Fachleute mit spezifischer Berufserfahrung, die sich zusätzlich im Rahmen einer Aufbauschulung für das Cyber-Sicherheitsnetzwerk qualifizieren müssen. Die Unterstützung durch einen Vorfall-Experten ist für den Betroffenen in der Regel kostenpflichtig, als Grundlage hierfür dient ein Dienstleistungsvertrag. Dieser wird selbständig und individuell zwischen beiden Parteien geschlossen.

Vorfall-Experten sind meist selbständige Experten oder regionale kleinere IT-Sicherheitsdienstleister, die den Betroffenen sowohl telefonisch als auch Vor-Ort bei einem IT-Sicherheitsvorfall unterstützen. Für die Tätigkeit im Cyber-Sicherheitsnetzwerk ist der Nachweis der Personenzertifizierung beim BSI und eine Registrierung bei der Geschäftsstelle des Cyber-Sicherheitsnetzwerks erforderlich.

Die kostenpflichtige dreitägige Aufbauschulung der Vorfall-Experten bei einem registrierten IT-Schulungsanbieter des Cyber-Sicherheitsnetzwerks basiert auf einem Curriculum, dessen Themen in einem "Leitfaden zur Reaktion auf IT-Sicherheitsvorfällen- für Vorfall-Experten" aufbereitet sind. 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. Erst nach erfolgreicher Zertifizierung können sich Vorfall-Experten bei Interesse im Cyber-Sicherheitsnetzwerk registrieren lassen.

Der IT-Sicherheitsvorfall wird an die Vorfall-Experten abgegeben, wenn zur Analyse und Behebung oder, zusätzlich Untersuchung, ein Team unterschiedlicher Spezialisten erforderlich ist, dass über einen gewissen Zeitraum vor Ort den Betroffenen Unterstützungsleistung anbietet.

4.3.6 Grenzen des Digitalen Ersthelfer

Der Digitale Ersthelfer orientiert sich an den Handlungsempfehlungen des Leitfadens. Die Unterstützung bei der Reaktion auf einen vorliegenden IT-Sicherheitsvorfall erfordert situationsabhängig unterschiedliches Fachwissen aus den entsprechenden Bereichen. Ist hier eine Grenze erreicht, bei der die zur Beseitigung erforderliche Expertise die Kompetenzen des Digitalen Ersthelfers gemäß Leitfaden übersteigt. Der IT-Sicherheitsvorfall sollte dann an einen Vorfall-Experten oder registrierten IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten weitergegeben werden. Eine weitere Grenze der Unterstützung ist erreicht, wenn die Bearbeitung des Vorfalls über den Umfang der Beauftragung hinausgeht. Um Missverständnisse zu vermeiden ist es wichtig zu Beginn eines Telefongesprächs über grundlegende Rahmenbedingungen im Hinblick auf die Durchführung des Telefonats aufzuklären.

4.4 Arbeitsweise des Digitalen Ersthelfers

Die Bearbeitung eines IT Sicherheitsvorfalls beginnt in dem Moment der Kontaktaufnahme des Betroffenen mit dem Digitalen Ersthelfer und dessen Zustimmung zur Bearbeitung des IT-Sicherheitsvorfalls. Der Ablauf der Vorfallbearbeitung lässt sich in folgende Stufen einteilen.

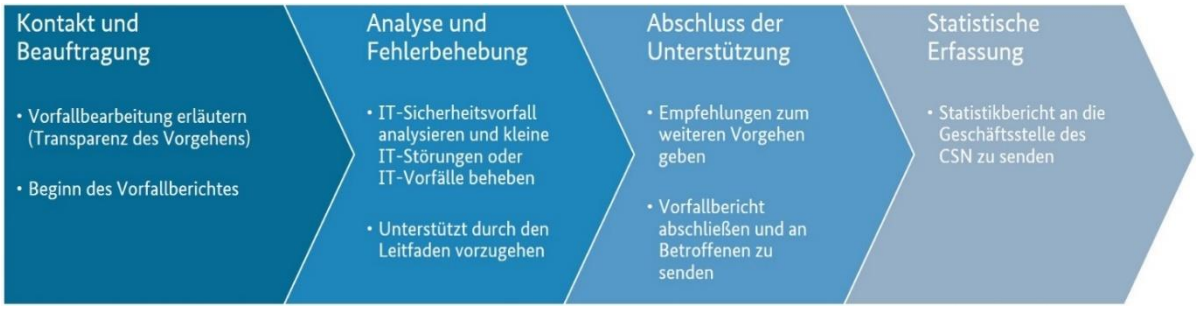

Abbildung 31: Ablauf der Vorfallbearbeitung durch den Digitalen Ersthelfer

4.4.1 Kontakt und Beauftragung

Innerhalb seiner Verfügbarkeitszeiten steht der Digitaler Ersthelfer für die Ersthilfe in der Digitalen Rettungskette des Cyber-Sicherheitsnetzwerks zur Verfügung. Die Kontaktaufnahme erfolgt direkt durch den Betroffenen eines IT-Sicherheitsvorfalls. Der Digitale Ersthelfer beginnt mit dem Vorfallbericht und generiert eine eindeutige Vorfallnummer.

Sollte sich schon zu Beginn herausstellen, dass es sich bei dem Anliegen des Betroffenen um keine IT-Störung oder keinen IT-Sicherheitsvorfall handelt, wird das Gespräch beendet. Es erfolgt aber eine statistische Rückmeldung an das Cyber-Sicherheitsnetzwerk.

Als nächstes informiert der Digitaler Ersthelfer den Betroffenen über den Ablauf der Vorfallbearbeitung (insbes. zur Erhebung von personenbezogenen Daten) und zur Frage der Haftung. Der Digitaler Ersthelfer holt sich dessen Zustimmung für die nähere Analyse des Vorfalls.

4.4.2 Analyse und Fehlerbehebung

Der Digitaler Ersthelfer analysiert unterstützt durch den vorliegenden Leitfaden den IT-Sicherheitsvorfall. Er erfasst in einem Vorfallbericht alle notwendigen Daten zur Bearbeitung des Vorfalls, analysiert den Vorfall und erarbeitet Lösungsvorschläge.

Der Betroffene führt nun die vom Digitaler Ersthelfer vorgeschlagenen Handlungsempfehlungen in Eigenregie aus und der Digitaler Ersthelfer trägt alle getroffenen Maßnahmen und das jeweilige Ergebnis im Vorfallbericht ein.

Dabei liegt es im Ermessen der Digitalen Ersthelfer welchem Zeitrahmen er für die Bearbeitung festlegt, um dem Betroffenen Handlungsempfehlungen an die Hand zu geben zu können.

4.4.2.1 Aufnahme der Problematik

Eine effiziente und genaue Erfassung des zugrundeliegenden Sachverhalts ist unabdingbar, um die Probleme der Hilfesuchenden so schnell und effektiv wie möglich zu lösen bzw. diese bei der Behebung entsprechend zu unterstützen. Demzufolge gilt es den IT-Sicherheitsvorfall durch gezielte Fragen möglichst sorgfältig aufzunehmen.

Im Zuge der Problemerfassung wird schließlich die Rückmeldung des Hilfesuchenden aufgenommen. Hierbei ist zu empfehlen dies angemessen zu dokumentieren, um den Überblick über den Sachverhalt zu bewahren.

Die nachfolgenden Fragestellungen dienen als Orientierung bei der Aufnahme der Problematik. Zur Sicherstellung einer möglichst präzisen Erfassung sollten dabei alle Fragen gestellt werden. Je nach Wissenstand des Hilfesuchenden ist es denkbar, dass vereinzelt eine Beantwortung der Frage nicht möglich ist.

 Wer ruft an? In welchem Umfeld wird sich bewegt? (KMU oder Privat)

 Was ist geschehen? Welche Auswirkungen sind spürbar?

 Welche IT-Systeme bzw. welche Prozesse sind betroffen?

 Sind externe bzw. Dritte von dem IT-Sicherheitsvorfall betroffen? (z.B. Partner, Kunden)

 Wie ist das Problem aufgetreten? Welche Tätigkeiten wurden ausgeführt? Welche Unregelmäßigkeiten konnten beobachtet werden?

 Wann ist die Begebenheit aufgetreten? (vor Wochen, seit Tagen, gerade eben)

 Wo befindet sich das betroffene IT-System? (Gebäude, Raum, Arbeitsplatz, häuslicher Umgebung)

 Wurden schon Maßnahmen getroffen? Wenn ja, welche?

4.4.2.2 Eingrenzung der Problematik

Um die Problematik eingrenzen zu können, ist es notwendig, das Problem des Anrufenden möglichst detailliert zu erfassen und zu identifizieren, um die entsprechenden Handlungsempfehlungen aussprechen zu können. Dabei ist im ersten Schritt zu überprüfen, ob es sich dabei im Rahmen der Behebung um eine IT-Störung oder einen IT-Sicherheitsvorfalls handelt.

Ein Entscheidungskriterium hierfür ist die Ermittlung des verletzten Schutzziels (Vertraulichkeit, Integrität oder Verfügbarkeit). Durch die Bestimmung der betroffenen Schutzziele ist es möglich herauszufinden, ob die Problematik eine IT-Störung oder einen IT-Sicherheitsvorfall darstellt.

- Eine Verletzung der Vertraulichkeit liegt vor, wenn ein unautorisierter Informationsgewinn vorliegt. Das bedeutet beispielweise, dass eine Person unbefugt an Informationen gelangt, die nicht für diese Person bestimmt waren oder, dass sensible Informationen im Internet veröffentlicht werden.
- Die Integrität wird verletzt, wenn die Korrektheit der Daten nicht mehr gegeben ist oder das System nicht mehr richtig funktioniert. Als Beispiel ist hier im Wesentlichen die Manipulation von Daten durch unbefugtes Verändern oder Einfügen aufzuführen.
- Eine Verletzung der Verfügbarkeit tritt ein, wenn die Funktionalität des Systems nicht mehr gegeben ist oder Informationen nicht mehr zur Verfügung stehen. Ein Verfügbarkeitsverlust macht sich z.-B. durch den kompletten Ausfall des Systems oder einen Verlust von Daten bemerkbar.

Sind lediglich die Schutzziele der Vertraulichkeit oder Integrität betroffen ist der Verdacht eines IT-Sicherheitsvorfalls nicht mehr auszuschließen. Ist die Verfügbarkeit betroffen, kann es sich sowohl um eine IT-Störung als auch um einen IT-Sicherheitsvorfall handeln.

Anschließend wird bewertet, ob ein bekanntes IT-Problem (siehe Kapitel 2 und 3) identifiziert werden konnte. In diesem Fall können schließlich gezielte Handlungsempfehlungen ausgesprochen werden, die im Idealfall die Problematik beseitigen.

Eine Weiterleitung an ein beliebig höheres Glied der Digitalen Rettungskette ist notwendig, wenn die ausgesprochenen Handlungsempfehlungen die Problematik nicht lösen konnten oder keine eindeutige Bestimmung des Sachverhaltes nicht möglich ist.

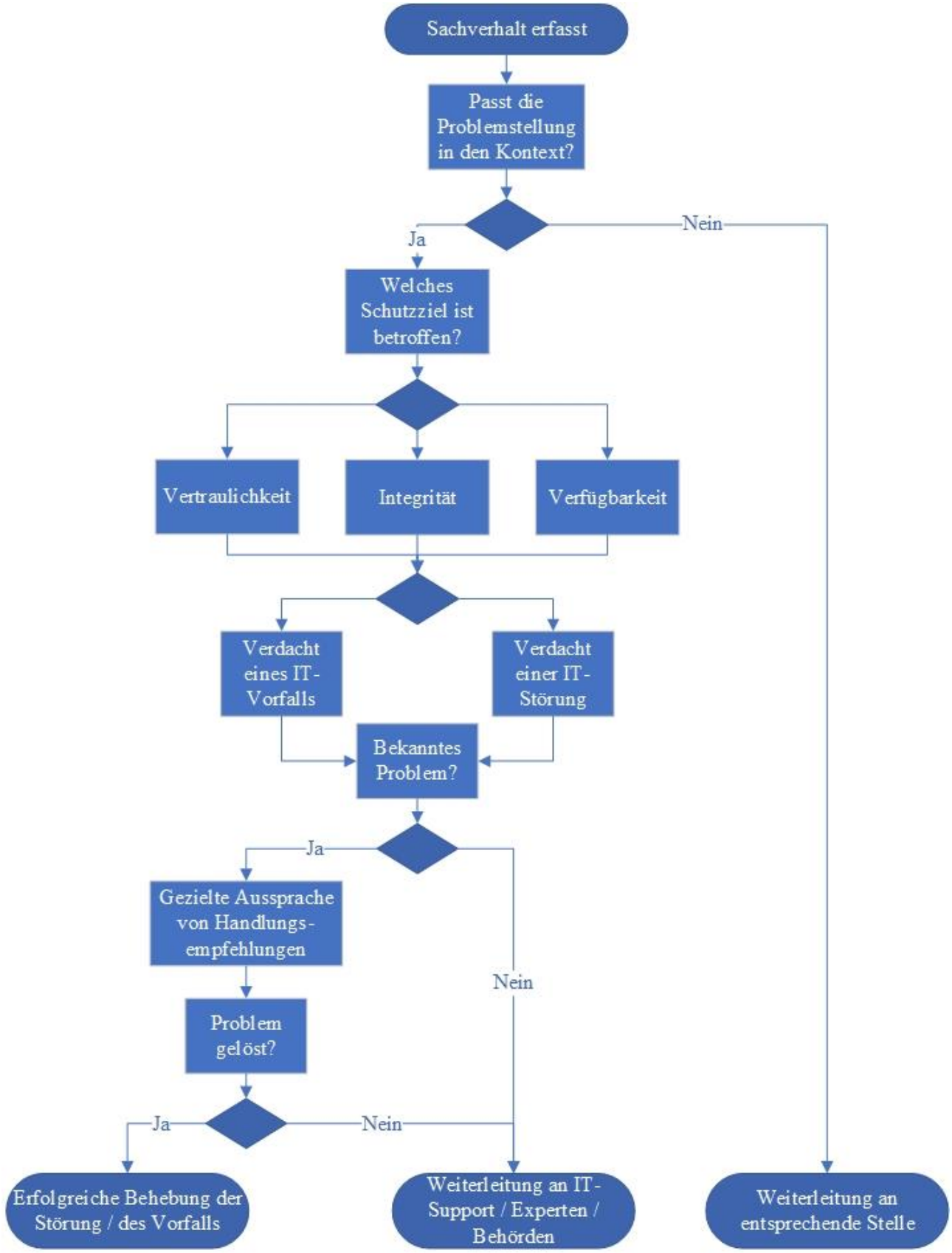

Abbildung 32: Entscheidungsmatrix

4.4.3 Abschluss der Unterstützung durch den Digitalen Ersthelfer

Der Digitaler Ersthelfer informiert am Ende des Gespräches den Betroffen über die weiteren Maßnahmen und Möglichkeiten. Zum Abschluss des Gespräches übersendet der Digitaler Ersthelfer dem Betroffenen per E-Mail den Vorfallbericht inkl. aller Analysen, umgesetzten Maßnahmen und Ergebnisse.

Der Abschlussbericht dient dabei als Unterstützungsnachweis und Dokumentation der Vorfallbearbeitung sowie als möglicher zukünftiger Lösungsansatz bei erneutem Auftreten des Sicherheitsvorfalles.

Konnte der Vorfall nicht behoben werden, wird der Betroffene darauf hingewiesen, dass er innerhalb des Cyber-Sicherheitsnetzwerks das nächste oder auch ein beliebiges höheres Glied in der Digitalen Rettungskette kontaktieren kann. Alle notwendigen Informationen zur weiteren Vorfall-Bearbeitung sind im Vorfallbericht dokumentiert, den der Betroffen an den Vorfall-Experten bzw. IT-Sicherheitsdienstleister mit einem Team von Vorfall-Experten zur Unterstützung weiterreicht.

Zusätzlich wird der Betroffene darauf hingewiesen, dass die Möglichkeit besteht, einen beliebigen anderen IT-Spezialisten außerhalb des Cyber-Sicherheitsnetzwerks zu kontaktieren und zu beauftragen. Die Weitergabe des Erfassungsformulars ist ihm dabei freigestellt.

Im Vorfallbericht gekennzeichnete Felder werden vom Digitaler Ersthelfer in einem Statistikbericht zusammengefasst und unabhängig von der Fehlerbehebung an das Cyber-Sicherheitsnetzwerk gesandt. Der Digitaler Ersthelfer weist den Betroffenen explizit darauf hin, dass der Sicherheitsvorfall anonymisiert in einer Statistik erfasst wird.

4.4.4 Statistische Erfassung der Vorfallbearbeitung

Für jeden IT-Sicherheitsvorfall füllt der Digitaler Ersthelfer nach Abschluss seiner eigenen Tätigkeiten einen Statistikbericht aus. Der Statistikbericht ist Teil des Vorfallberichtes. Die Felder des Vorfallberichtes, die in den Statistikbericht übernommen werden sind für den Betroffenen transparent dargestellt.

Der Statistikbericht wird vom Digitaler Ersthelfer per E-Mail an die CSN-Geschäftsstelle geschickt und die Statistikinformationen ausgewertet[6].

4.5 Orientierungshilfe: 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 formales 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 ein Anrufer entsprechend in Empfang zu nehmen ist und welche grundlegenden Fragen im Zuge der Aufnahme zu klären sind.

Anschließend werden Methoden und Verfahren dargelegt, wie die Problematik eingegrenzt und möglichst genau identifiziert werden kann. Dabei werden gezielte Fragestellungen, die eine Eingrenzung ermöglichen, formuliert.

Im letzten Schritt wird aufgezeigt, in welcher Form Handlungsempfehlungen ausgesprochen werden können. Hierbei wird vor allem berücksichtigt, wann es sinnvoll ist, zielgerichtet Handlungsempfehlungen als Lösungsansatz auszusprechen.

[6] Sollte der IT-Sicherheitsvorfall von einem Vorfall-Experten oder von einem IT-Dienstleister mit Team von Vorfall-Experten weiterbearbeitet werden, so wird auch dort nach Abschluss der Tätigkeit ein weiterer Statistikbericht erstellt. Die Vorfall-Nummer verhindert eine doppelte Erfassung der statistischen Daten.

4.5.1 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, mit wem spricht. Stellen Sie sich nicht mit möglichen Titeln wie Prof. oder Dr. vor. Um den Anrufer 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.

4.5.2 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 Anrufer den vermeintlichen IT-Sicherheitsvorfall mit den ausgesprochenen Handlungsempfehlungen nicht abschließend beheben kann. In diesem Falle verweist der Digitaler Ersthelfer den Anrufer an einen Vorfall-Experten und spricht daher lediglich generelle Verhaltensregeln aus:

- 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-Experten kontaktieren.
- Weitere Maßnahmen erst nach Rücksprache mit dem entsprechenden IT-Support oder einem Vorfall-Experten einleiten bzw. umsetzen.

4.6 Zusammenfassung

Das dritte Modul beschäftigt sich mit Themen rund um die Führung eines serviceorientierten Telefongesprächs. Neben der Auflistung von Rahmenbedingungen und der Verhaltensweise am Telefon, behandelt der Kern des Moduls die Aufnahme und Eingrenzung der Problematik sowie zuletzt die Aussprache von Handlungsempfehlungen.

Ziel des Erste-Hilfe-Gesprächs ist die die Behebung des Problems. Nicht immer ist jedoch eine abschließende Lösung das Resultat, da Digitale Ersthelfer nur im Rahmen ihrer Möglichkeiten handeln können. In diesen Fällen ist ein Vorfall-Experte zu kontaktieren. Trotz alledem ist die Einhaltung der Verhaltensregeln von essenzieller Bedeutung, um dem Anrufenden Hilfe anbieten zu können und um den zu erwartenden Schaden weitestgehend reduzieren zu können.

Das Wichtigste in Kürze

Serviceorientiertes Telefongespräch

- Ordnungsgemäße Berücksichtigung der Rahmenbedingungen für die Durchführung eines Erste-Hilfe-Gesprächs.
- Professionelles Verhalten am Telefon steigert die Chance das Gespräch lösungsorientiert und produktiv zu gestalten.
- Die detaillierte Aufnahme des Sachverhalts ist die Basis für die Eingrenzung bzw. Identifizierung der Problematik und der Aussprache von Handlungsempfehlungen.
- Die Aussprache von gezielten Handlungsempfehlungen ist nur bei einer zweifelsfreien Identifizierung des Problems sinnvoll.
- Um eine angemessene Reaktion auf IT-Sicherheitsvorfälle zu gewährleisten, ist die Einhaltung der Verhaltensregeln wichtig.

5 Anhang

5.1 Lösungen Modul 1

Szenario 1

- Netzwerkkabel kontrollieren (ziehen, einstecken, neu starten)
- Netzwerkkabel tauschen
- Router neu starten
- WLAN-Adapter / Netzwerkkarte aktivieren
- Provider prüfen
- Switch austauschen

Szenario 2

- Verwendung eines anderen USB-Ports
- Anderes USB-Medium / CD nutzen
- USB-Port / CD-Laufwerk aktivieren
- Treibersoftware des CD-Laufwerks aktualisieren
- Laufwerkbuchstabe des USB-Medium ändern

Szenario 3

- Toner / Tinte ersetzen
- Drucker / Druckkopf reinigen

Szenario 4

- Spam Postfach überprüfen
- Internetverbindung herstellen
- Anwendung / Client neu starten
- Anwendung neu installieren
- Speicher leeren

5.2 Lösungen Modul 2

5.2.1 Lösungen zu Aufgabe 1

Szenario 1

- Client vom Netz nehmen
- Virenscan durchführen
- Client zurücksetzen

Szenario 2

- Browser neu starten
- Alternativen Browser verwenden
- Gerät neustarten
- Browser neu installieren
- Virenscan durchführen

Szenario 3

- Client vom Netz nehmen
- Zahlungsaufforderung nicht nachkommen.
- Ransomware analysieren

Szenario 4

- Zugangsdaten (Passwort) ändern
- Zugangsdaten ändern, wenn Sie sich nicht mehr anmelden können
- Kontakte informieren
- An den Betreiber der Plattform wenden

5.2.2 Lösung zu Aufgabe 2

IT-Störung	IT-Sicherheitsvorfall
1. Maus/Tastatur funktioniert nicht	3. Zugangsdaten wurden ausspioniert
2. Es besteht keine Internetverbindung	4. Diebstahl von mobilen Geräten mit sensiblen Daten
7. Client startet, aber Bildschirm bleibt schwarz	5. Verlust von Daten
9. Client bleibt beim Hochfahren hängen	6. Programme installieren sich eigenständig
11. Drucker druckt nicht	8. Merkwürdige Weiterleitungen
12. Fehlermeldung wird auf dem Bildschirm angezeigt	10. Rechner überlastet
16. USB/CD wird nicht erkannt	11. Ungewöhnliche Warnhinweise auf dem Desktop
19. Bild auf dem Bildschirm wird nicht richtig angezeigt	14. Virenscanner hat einen Virus erkannt
	15. Geld vom Konto abgebucht
	17. Computer agieren ohne interne Eingabe
	18. Dateien sind plötzlich verschlüsselt

Tabelle 4: Lösungen zu Aufgabe 2

5.3 Checkliste: Verhaltensregeln nach einem IT-Sicherheitsvorfall

Um den Schaden von IT-Sicherheitsvorfällen möglichst auf ein Minimum zu reduzieren oder auch die eine weitere Ausbreitung weitestgehend zu verhindern, ist das korrekte Verhalten nach dem Auftreten von essenzieller Bedeutung.

Allgemeine Verhaltensregeln
 Ruhe bewahren und nicht in Panik geraten.
 Weitere Arbeiten mit bzw. an dem IT-System einstellen.
 Das betroffenen IT-System vom Netzwerk isolieren.
 Alle bisher durchgeführten Schritte und Unregelmäßigkeiten dokumentieren, sowie Beobachtungen ggf. in Form von Screenshots festhalten.
 Keine weiteren Maßnahmen eigenständig umsetzen, um das Problem zu beheben.
 Handelt es sich um eine IT-Störung, die nicht behoben werden kann, ist der Kontakt zu dem entsprechenden IT-Support aufzunehmen.
 Handelt es sich um einen IT-Sicherheitsvorfall, der nicht behoben werden kann, ist der Kontakt zu einem Vorfall-Experten aufzunehmen.
 Weitere Maßnahmen erst nach Rücksprache mit dem entsprechenden IT-Support oder einem Vorfall-Experten einleiten bzw. umsetzen.

Tabelle 5: Checkliste - Verhaltensregeln nach einem IT-Sicherheitsvorfall