Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cyber-Sicherheit für KMU

Die TOP 14 Fragen

Impressum

Herausgeber
Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

Zuständiges Referat
Referat WG 23 –
Cyber-Sicherheit für Kleine und
Mittlere Unternehmen (KMU)

Telefon
+49 (0) 800 2741000

E-Mail
KMU@bsi.bund.de

Internet
www.bsi.bund.de/kmu

Stand
August 2022

Artikelnummer
BSI-BroKMU22/001

Gestaltung
Faktor 3 AG

Druck
Appel & Klinger Druck und Medien GmbH,
Schneckenlohe

Texte und Redaktion
Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Bildnachweis
Titel: AdobeStock © Robert Kneschke; S. 04-05: AdobeStock © sdecoret; S. 05: © BSI; S. 09: © AdobeStock © contrastwerkstatt; S. 10: © AdobeStock © denisismagilov; S. 11: © AdobeStock © doselote (oben); © AdobeStock © Ar_TH (unten); S. 12: © AdobeStock © VideoFlow; S. 15: © AdobeStock © Denys Rudyi; S. 18: © Adobe-Stock © sdecoret; S. 19: © AdobeStock © makibestphoto; S. 20: © AdobeStock © Rawpixel.com; S. 23: © Adobe-Stock © m.mphoto; S. 25: © AdobeStock © kras99; S. 26: © AdobeStock © Anatoliy Karlyuk; S. 28: © AdobeStock © Виталий Сова

Inhaltsverzeichnis

Vorwort

Schon seit längerer Zeit berichten die Medien beinahe jede Woche über mindestens einen großen Cyber-Sicherheitsvorfall. Oftmals sind dabei große Unternehmen, manchmal auch Behörden betroffen. Das heißt aber nicht, dass kleine und mittlere Unternehmen (KMU) ein geringeres Risiko aufweisen, Opfer von Cyber-Vorfällen zu werden. Vorfälle bei KMU schaffen es schlicht nur selten in die überregionalen Nachrichten.

Aber auch rein zahlenmäßig ist die Angriffsfläche von KMU weitaus größer als die von Großunternehmen.

Leider ist das Risiko bei KMU, von einem Cyber-Vorfall betroffen zu werden, höher als bei den großen Unternehmen. Anders als bei diesen fehlt es den kleineren Betrieben meist an Informationssicherheitsteams. Oftmals gibt es dort noch nicht einmal ein dediziertes IT-Team, das sich um den allgemeinen Betrieb der IT-Systeme kümmert. Das Wissen zum Thema Informationssicherheit ist bei KMU daher häufig recht begrenzt und muss extern eingekauft werden.

Mit dieser Broschüre möchten wir KMU einen leicht verständlichen Einstieg bieten, um ihr Cyber-Sicherheitsniveau zu verbessern. Denn Informationssicherheit ist die Voraussetzung für eine sichere Digitalisierung. Im BSI als Cyber-Sicherheitsbehörde des Bundes verstehen wir es als unsere Aufgabe, Ihnen bei dem gemeinsamen Ziel, unsere Wirtschaft vor Cyber-Angriffen zu schützen, ein verlässlicher Partner zu sein.

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

KMU als wichtiger Wirtschaftsfaktor

In Deutschland existieren nach EU-Klassifikation etwa 2,6 Millionen Unternehmen, die dem Bereich der KMU zuzurechnen sind. Das sind 99,4 Prozent aller Unternehmen! Sie beschäftigen 57 Prozent (31 Millionen) der Arbeitnehmerinnen und Arbeitnehmer in Deutschland, stellen 82 Prozent der Ausbildungsplätze und generieren 43 Prozent der Bruttowertschöpfung der deutschen Wirtschaft.

Das Bonner Institut für Mittelstandsforschung (IfM) verwendet eine leicht abweichende KMU-Definition, indem es die Grenze für mittlere Unternehmen nicht bei 249, sondern bei 499 Mitarbeiterinnen und Mitarbeitern zieht, da sich die deutsche Besonderheit der mittelständischen Familienunternehmen damit besser darstellen lässt. Viele dieser familien- bzw. eigentümergeführten Unternehmen zählen zur Gruppe der „Hidden Champions“, die in Deutschland etwa 1.500 Unternehmen umfasst – und damit etwa die Hälfte aller Hidden Champions weltweit ausmacht. Etwa 70 Prozent der deutschen Hidden Champions haben weniger als 250 Beschäftigte, 12 Prozent beschäftigen zwischen 250 und 499 Mitarbeiterinnen und Mitarbeiter.

Einleitung

Sagen wir es ganz offen: Die Situation in Bezug auf Cyber-Sicherheit ist in der überwiegenden Zahl der KMU besorgniserregend.

Viele Unternehmen sind sich dessen sogar bewusst: Sie würden gerne mehr für ihre Cyber-Sicherheit tun. Aber selbst dann, wenn dieser Wunsch vorhanden ist, erscheint den Verantwortlichen die Umsetzung der üblichen Maßnahmen zur Verbesserung der betrieblichen Informationssicherheit (beispielsweise die Umsetzung des IT-Grundschutzes) oftmals als viel zu großes Unterfangen für ihr Unternehmen.

Das BSI ist die Cyber-Sicherheitsbehörde des Bundes und verantwortet bei Staat, Wirtschaft und Gesellschaft Prävention, Detektion und Reaktion im Bereich Informationssicherheit. Seit Herbst 2020 kümmert sich bei uns nun ein neues Referat ausschließlich um die Belange von KMU. Nicht aus dem sprichwörtlichen Elfenbeinturm heraus, sondern auf Augenhöhe. So ist auch diese Broschüre (*) zu verstehen. Vergessen wir einfach einmal für einen Augenblick ISO-Normen und das IT-Grundschutz-Kompendium und fangen mit den wichtigsten Grundlagen der IT-Sicherheit an – kurz und knapp anhand von 14 Fragen. Wenn der erste Schritt gemacht ist, sind die nächsten nicht mehr schwer. Am Ende der Lektüre werden Sie wissen, was Sie im Unternehmen selbst umsetzen können und was Sie extern beauftragen müssen. Das ist übrigens ein wichtiger Punkt: Sie müssen im Bereich IT/IT-Sicherheit nicht alles selbst machen. Wichtig ist nur, DASS das Nötige umgesetzt wird. Putzen Sie die Toiletten in Ihrem Unternehmen selbst? Führen Sie bei Ihren Firmenfahrzeugen selbst den Ölwechsel durch? Erstellen Sie selbst die Steuererklärung? Nein? Dann finden Sie sicher auch einen geeigneten IT-Dienstleister in Ihrer Nähe, für den die Beantwortung der Fragen in dieser Broschüre Routine ist. Und bleiben Fragen offen, dann finden Sie auf Seite 2 Ihren Kontakt zu uns.

Und falls Sie beim Lesen doch einmal denken „Oh, das sind mir jetzt doch zu viele Fachbegriffe!“ – Keine Sorge, Sie müssen nicht wissen, wie die Technik dahinter funktioniert, aber Sie sollten den Begriff zumindest einmal gehört haben. Wer das Wort „Airbag“ nicht kennt, dem wird nicht auffallen, wenn sein Traumauto über keinen verfügt …

* Die Verbesserung der Cyber-Sicherheit von KMU ist kein deutsches Sonderthema. Teile dieser Broschüre haben wir von der *Agence nationale de la sécurité des systèmes d'information (ANSSI)* freundlicherweise übernehmen dürfen und um landesspezifische Fragen und Aspekte ergänzt.

FRAGE 1

Wer ist verantwortlich?

„Wer ist in meinem Unternehmen für das Thema Cyber-Sicherheit verantwortlich?“ Diese Frage sollte man sich zuallererst stellen, wenn man sich mit der Sicherheit seines IT-Systems beschäftigen möchte. Die Antwort ist in jedem Unternehmen dieselbe: **die Unternehmensleitung!**

Wenn in einem Unternehmen (beispielsweise aufgrund eines erfolgreichen Ransomware-Angriffs) die Informationstechnik ausfällt, dann steht es danach in den meisten Fällen still. Es wird nichts mehr produziert, Ware wird nicht mehr ausgeliefert, Bestellungen werden nicht mehr entgegengenommen, Kundentermine nicht mehr eingehalten, die Einnahmen fallen aus, die Kosten laufen weiter. Werden (was bei Ransomware-Angriffen mittlerweile fast immer der Fall ist) Kundendaten gestohlen und veröffentlicht, ist oftmals auch noch die Unternehmensreputation dahin. Sprich: Die Lage ist ernst. Kein Thema, das eine verantwortungsvolle Unternehmensleitung nach unten wegdelegieren sollte …

BEWUSSTSEIN BEI DER UNTERNEHMENSLEITUNG SCHAFFEN

Die Unternehmensleitung muss sich natürlich nicht um die Details der Unternehmens-IT kümmern, aber das Thema Informationssicherheit sollte in den Geschäftsleitungsbesprechungen regelmäßig ein Punkt auf der Tagesordnung sein. Vielleicht nicht genauso oft wie die Punkte „Finanzen“ und „Vertrieb“, aber zumindest regelmäßig.

Falls Sie Mitglied der Unternehmensleitung sind: Prima, dann wissen Sie jetzt ja Bescheid! Falls nicht, sorgen Sie dafür, dass Ihre Unternehmensleitung möglichst bald Bescheid weiß!

Falls Sie damit keinen Erfolg haben, regen Sie bei Ihrem Branchenverband oder Ihrer IHK doch einmal an, eine Veranstaltung mit Zielgruppe Unternehmensleitungen zum Thema „Cyber-Sicherheit“ auszurichten. Das KMU-Referat des BSI verbringt einen nicht unerheblichen Teil seiner Zeit damit, genau bei solchen Veranstaltungen Geschäftsführungen mit Vorträgen für das Thema zu sensibilisieren.

DIE ZUSTÄNDIGKEIT FÜR DIE UMSETZUNG VON MASSNAHMEN FESTLEGEN

Es muss klar festgelegt werden, welche Stelle im Unternehmen für den Betrieb des Informationssystems zuständig ist und welche Stelle für den Bereich Informationssicherheit. In kleinen Unternehmen wird dies oftmals dieselbe Person sein, in größeren Unternehmen sind die Zuständigkeiten für die beiden Bereiche aber idealerweise getrennt. Erfahrungsgemäß kann Sicherheit manchmal nur durch Verzicht auf Benutzerkomfort erreicht werden. Aus diesem Grund wird es immer wieder einmal vorkommen, dass IT-Leiterinnen und -Leiter und Informationssicherheitsbeauftragte unterschiedlicher Meinung sind. Daher ist es keine gute Idee, wenn sich diese auf unterschiedlichen Hierarchieebenen befinden. Können sich beide nicht einigen, gilt wieder: **Verantwortlich ist die Unternehmensleitung! Genau dort ist die Entscheidung richtig aufgehoben, welches Sicherheitsniveau angestrebt wird und welche Restrisiken akzeptiert werden.**

WEITERE INFORMATIONEN FINDEN SIE HIER:

1 *https://www.bsi.bund.de/dok/128578*
BSI-Standard 200-1. „Managementsysteme für Informationssicherheit (ISMS)“


1

FRAGE 2

Wie gut kennen Sie Ihre IT-Systeme?

„Kenne ich die IT-Systeme, Apps und die für mein Unternehmen lebenswichtigen Daten?“ **Um sich adäquat zu schützen, muss jedes Unternehmen, selbst ein Einzelunternehmen, seine Hard- und Software sowie die Daten und die Verarbeitungsprozesse, die die Grundlagen seiner Informationswerte bilden und zum Fortbestand des Unternehmens beitragen, inventarisieren.** Aus dieser Bestandsaufnahme lassen sich dann die entsprechenden Schutzmaßnahmen ableiten. Das hört sich nach mehr Arbeit an, als es ist. Bei einem kleinen Unternehmen ist das schnell gemacht.

AUFLISTUNG ALLER VERWENDETEN KOMPONENTEN

Aufzulisten sind: Computer, Smartphones, Tablets, lokale Server, Remote-Server (für Website-Hosting, Kommunikationsdienste, Fachanwendungen usw.). **Außerdem müssen auch alle Peripheriegeräte inventarisiert werden: Drucker, Scanner, Router, Switches, mobile Breitbandmodems usw.** Dadurch wissen Sie, was geschützt werden muss, und können in einer späteren Phase die für die Tätigkeit des Unternehmens kritischen Elemente identifizieren.

AUFLISTUNG DER EINGESETZTEN SOFTWARE

Sie sollten die Art der Software, ihre wesentlichen Funktionen und die jeweilige eingesetzte Version kennen. Wichtig ist auch, dass Sie über gültige Benutzerlizenzen verfügen und die jeweiligen Registrierungscodes im Notfall schnell zur Hand haben (am besten ausgedruckt in einem Aktenordner), denn dies ist für die Wartung und Neuinstallation von Software unerlässlich.

AUFLISTUNG DER DATEN UND DER DATENVERARBEITUNG

Überlegen Sie einmal, was passieren würde, wenn bei Ihnen Daten verloren gingen, verändert oder unbrauchbar würden. Bei welchen Daten würden Sie Gefahr laufen, dass Ihr Geschäftsbetrieb beeinträchtigt oder sogar unterbrochen würde? Gibt es eine Kundendatei? Wo werden die Daten aufbewahrt, beispielsweise die der Buchhaltung? Welche Daten unterliegen gesetzlichen Vorschriften? Die gleiche Frage stellt sich für die Verarbeitung der Daten: Bei Beeinträchtigung welcher Datenverarbeitungsverfahren würde die Geschäftstätigkeit besonders stark beeinträchtigt oder sogar unterbrochen?

AUFLISTUNG ALLER ZUGRIFFSRECHTE

Dabei wird festgelegt, wer das Informationssystem nutzen darf und wie die Bedingungen für den jeweiligen Zugriff aussehen: Kategorie des Zugreifenden (Administratorinnen und Administratoren, Benutzerinnen und Benutzer, Gast und Gästin), Art des Zugriffs (lokale oder Remote-Verbindung) usw. Mit dieser Auflistung kann sichergestellt werden, dass kein unzulässiger Zugriff erfolgen kann (z. B. durch ehemalige Mitarbeiterinnen und Mitarbeiter, die das Unternehmen vielleicht im Streit verlassen haben, oder ehemalige Dienstleister) und somit die Angriffsfläche für Bedrohungen begrenzt wird.

AUFLISTUNG DER IT-VERBINDUNGEN MIT DER AUSSENWELT

Welche Berührungspunkte gibt es zwischen dem Informationssystem Ihres Unternehmens und dem Internet?

Jeder Internetzugang zu einem Provider oder Partner muss ermittelt und in das Bestandsverzeichnis aufgenommen werden. Damit können angemessene Filter- und Überwachungsregeln verknüpft werden.

Diese notwendige Bestandsaufnahme ermöglicht es dem Unternehmen, seinen Bedarf und seine Kapazitäten im digitalen Bereich zu ermitteln. Sie sollte regelmäßig (mindestens zweimal pro Jahr) aktualisiert werden.
Sie hilft auch dabei, für das Unternehmen passende IT-Lösungen auszuwählen, notwendige Sicherheitsmaßnahmen zu identifizieren und gegebenenfalls eine detaillierte Übersicht zu erstellen, die dem beauftragten Dienstleister hilft. Außerdem ist sie für diejenigen Fachleute sehr nützlich, die im Falle einer Cyber-Attacke Gegenmaßnahmen einleiten sollen.

WEITERE INFORMATIONEN FINDEN SIE HIER:

2 *https://www.bsi.bund.de/dok/128640*
BSI-Standard 200-2, IT-Grundschutz-Methodik

3 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein, ORP.4: Identitäts- und Berechtigungsmanagement

2 3

FRAGE 3

Führen Sie regelmäßig eine Datensicherung durch?

Wenn regelmäßige Datensicherungen (Backups) durchgeführt werden, können die betrieblichen Aktivitäten nach einem Vorfall, gerade auch nach einem Ransomware-Angriff, schneller wieder aufgenommen werden.

IDENTIFIZIEREN SIE DIE DATEN, DIE GESICHERT WERDEN SOLLEN

Um die relevanten Daten zu identifizieren, müssen Sie zunächst alle Ihre Datenverarbeitungssysteme inventarisieren und dann bestimmen, welche Daten von wesentlicher Bedeutung für Ihre Geschäftstätigkeit sind. Dabei kann es sich um organisatorische Daten (z. B. Kundendateien oder Know-how aus der Fertigung), aber vielleicht auch um technische Daten handeln. Letztere können die Konfiguration einzelner Computer oder die gesamte Unternehmensinfrastruktur bzw. einen Teil davon betreffen, zum Beispiel industrielle Produktionsanlagen.

LEGEN SIE FEST, WIE HÄUFIG DATENSICHERUNGEN DURCHGEFÜHRT WERDEN SOLLEN

Das Intervall der Datensicherungen sollte in Abhängigkeit von der Menge der in einem bestimmten Zeitraum anfallenden digitalen Daten festgelegt werden. Beispielsweise reicht es bei Kleinstunternehmen im Handwerksbereich eventuell aus, monatliche Datensicherungen ihrer Rechnungen und ihrer Kundendatei anzulegen. KMU, die über einen Onlineshop Waren oder Dienstleistungen verkaufen, benötigen hingegen wahrscheinlich eine häufigere Datensicherung, beispielsweise wöchentlich oder sogar täglich. Es kann auch eine differenzierte Datensicherung eingerichtet werden, bei der unterschiedliche Sicherungszeitpunkte gelten: täglich oder wöchentlich für geschäftliche Daten und monatlich für technische Daten.

WÄHLEN SIE EIN GEEIGNETES SPEICHERMEDIUM, MIT DEM DIE DATEN GESICHERT WERDEN SOLLEN

Dabei kann es sich um ein physisches Medium wie eine externe Festplatte handeln, die am Ende der Datensicherung vom Informationssystem getrennt werden muss oder um eine Datensicherung in einem Cloud-Dienst. Für Ihre wertvollsten Daten können Sie auch beides

nutzen. Ein physischer Datenträger, der nur für die Zeit der Datensicherung an das Computer-System angeschlossen wird, hat den Vorteil, dass ein Datenzugriff (insbesondere von Ransomware) von außen nicht möglich ist. Aber er kann gestohlen werden, zerstört werden (beispielsweise bei einem Brand oder einer Überschwemmung) oder schlicht einen technischen Defekt aufweisen. Über Cloud-Dienste können Datensicherungen einfach automatisiert werden. Sie sind allerdings ggf. stärker dem Risiko eines unbefugten Zugriffs oder Ausfalls ausgesetzt. **Unabhängig davon, für welche Methode Sie sich entscheiden, müssen alle Datensicherungen, direkt nachdem sie erstellt worden sind, auf ihre Integrität und Funktionsfähigkeit getestet werden. Nur so lässt sich gewährleisten, dass im Ernstfall tatsächlich alle relevanten Daten wiederhergestellt werden können.** Falls Sie eine Cyber-Versicherung abgeschlossen haben, verlangt Ihre Versicherung dies vermutlich sogar von Ihnen. Denn immer wieder kommt es vor, dass Unternehmen nach einem IT-Vorfall Daten aus ihren Backups zurückspielen und dann feststellen müssen, dass alle unbrauchbar sind.

PRÜFEN SIE, WELCHE DATEN VERSCHLÜSSELT WERDEN SOLLEN

Die Verschlüsselung von Daten vor dem Speichern ist eine empfohlene Praxis. Sie ist besonders wichtig bei Daten, die in der Cloud oder auf mobilen Geräten gespeichert werden: Bei einem unberechtigten Zugriff bleiben die Daten geschützt. Die Wahl des Cloud-Betreibers, die Methoden der Datenspeicherung und die Zugangs- und Authentifizierungsvoraussetzungen sind ebenso Punkte, die es zu überprüfen gilt. Aber auch bei lokalen Datensicherungen (externe Festplatte, USB-Stick, Bandlaufwerk) ist eine Datenverschlüsselung ratsam. Wichtig: Wenn Sie Daten verschlüsselt sichern (was immer eine gute Idee ist), dann achten Sie darauf, dass Sie für den Ernstfall auch irgendwo eine Kopie des/der Schlüssel sicher verwahrt haben. In den im Unternehmensumfeld eingesetzten gängigen Betriebssystemen sind Funktionen zum Verschlüsseln von Daten oftmals bereits enthalten, müssen in der Regel jedoch explizit aktiviert werden.

WEITERE INFORMATIONEN FINDEN SIE HIER:

4 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein CON.3: Datensicherungskonzept

5 *https://www.bsi.bund.de/dok/131234*
Datensicherung – wie geht das?

6 *https://www.bsi.bund.de/dok/131240*
Backup: Doppelt gesichert hält besser

4 5 6

FRAGE 4

Spielen Sie regelmäßig Updates ein?

Die meisten Angreifer nutzen öffentliche und dokumentierte Schwachstellen, um in Informationssysteme einzudringen. Um Schaden anzurichten, stützen sie sich entweder auf die Nachlässigkeit von Benutzerinnen und Benutzern und/oder sie nutzen eine Schwachstelle in einem mit dem Internet verbundenen Dienst (z. B. E-Mail-Server, Firewall usw.) aus. **Es ist wichtig, Betriebssysteme und Anwendungssoftware zu aktualisieren, sobald Sicherheitsupdates von den jeweiligen Herstellern zur Verfügung gestellt werden. Sicherheitsupdates kosten kein Geld! Die Aktualisierung zu unterlassen, häufig schon ... Zu spät oder nicht installierte Updates sind einer der häufigsten Gründe für erfolgreiche Cyber-Angriffe auf KMU.**

VERWENDEN SIE AKTUELLE HARDWARE- UND SOFTWARELÖSUNGEN

Aus Gewohnheit, Nachlässigkeit oder um Geld zu sparen, mag es verlockend erscheinen, Hardware oder Software über ihren „Lebenszyklus“ hinaus zu behalten, d. h. länger, als der Hersteller oder der Anbieter die Wartung unter sicheren Bedingungen garantiert. Nicht mehr aktualisierbare Hard- oder Software muss entsorgt oder deinstalliert werden.

AKTIVIEREN SIE AUTOMATISCHE UPDATES

Aktualisierungen des Betriebssystems und aller verwendeten Software sollten durchgeführt werden, sobald von den Herstellern ein Update zur Verfügung gestellt wird. Das gilt vor allem für alle Systeme, die mit dem Internet verbunden sind. **Es wird empfohlen, die von den Anbietern bereitgestellten automatischen Update-Funktionen zu aktivieren.** Zusätzlich zu den regelmäßigen Updates können außerplanmäßige Updates nötig sein, wenn eine Sicherheitslücke entdeckt wird, die so gefährlich ist, dass man nicht mehrere Wochen auf die Bereitstellung eines regulären Updates warten kann. Auch diese Updates sollten so schnell wie möglich eingespielt werden.

LEGEN SIE FEST, WER FÜR DEN UPDATE-PROZESS ZUSTÄNDIG IST

Falls Sie einen IT-Dienstleister beauftragt haben, stellen Sie sicher, dass er die in Ihrem Unternehmen verwendeten IT-Systeme aktualisiert. Verlangen Sie gegebenenfalls, dass dies explizit als Aufgabe in den Dienstleistungsvertrag mit aufgenommen wird. Falls Sie diese Aufgabe nicht auf einen externen Dienstleister übertragen haben, stellen Sie sicher, dass die Aufgabe in Ihrem Unternehmen jemandem eindeutig zugewiesen ist.

WEITERE INFORMATIONEN FINDEN SIE HIER:

7 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein OPS.1.1.3: Patch- und Änderungsmanagement

8 *https://www.bsi.bund.de/dok/130994*
Softwareupdates – ein Grundpfeiler der IT-Sicherheit

9 *https://www.bsi.bund.de/dok/130998*
Updates, Browser & Open-Source-Software

7 8 9

FRAGE 5

Haben Sie Makros deaktiviert?

WARUM SOLLTEN SIE MAKROS DEAKTIVIEREN?

Eines der Haupteinfallstore für Ransomware sind Makros, die sich in mit E-Mails verschickten Dateianhängen verbergen. Dieses Einfallstor können Sie schließen – und zwar kostenlos!

Makros sind kleine Programme, die man beispielsweise in Word-, Excel-, PowerPoint- oder PDF-Dateien einbetten kann. Damit lassen sich Vorgänge automatisieren, was für manche Anwendungen durchaus nützlich sein kann. **Leider gilt das aber auch für Angreiferinnen und Angreifer, die Ihr IT-System unter Kontrolle bringen wollen.**

Wenn man eine Datei öffnet, die ein Makro enthält, fragt das öffnende Programm den Nutzer oder die Nutzerin dafür in der Regel um Erlaubnis. Das Problem ist, dass die meisten Nutzerinnen und Nutzer nicht beurteilen können, ob die Datei, die sie da gerade öffnen, legitim ist oder nicht. Cyber-Kriminelle versenden ihre Schadsoftware oftmals über die E-Mail-Adressen von Absendern, die die Empfänger kennen und denen sie vertrauen. Oftmals bezieht sich der Betreff einer Schadcode-E-Mail sogar auf eine bereits bestehende Mailkonversation (was in der Regel heißt, dass der vermeintliche Absender bereits selbst Opfer der Schadsoftware geworden ist).

Überlassen Sie die Entscheidung, ob ein Makro ausgeführt werden darf oder nicht, keinesfalls den Nutzern – denn diese haben schlicht nicht die erforderlichen Kenntnisse, um so eine Entscheidung treffen zu können. Verbieten Sie (zum Beispiel in den Windows-Gruppenrichtlinien) das Ausführen von Makros generell. Die meisten KMU verwenden ohnehin keine Makros. Und falls doch, kann Ihr Administrator die benötigten Makros signieren und ihre Ausführung damit erlauben. Alle anderen Makros bleiben aber weiterhin verboten. Das alles lässt sich mit ein paar Mausklicks erledigen.

WEITERE INFORMATIONEN FINDEN SIE HIER:

10 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein APP.1.1: Office-Produkte

11 *https://allianz-fuer-cybersicherheit.de/dok/462102*
Sichere Konfiguration von Microsoft Office 2013/2016/2019 v1.1

12 *https://allianz-fuer-cybersicherheit.de/dok/462104*
Sichere Konfiguration von Microsoft Access 2013/2016/2019 v1.1

13 *https://allianz-fuer-cybersicherheit.de/dok/462106*
Sichere Konfiguration von Microsoft Excel 2013/2016/2019 v1.1

14 *https://allianz-fuer-cybersicherheit.de/dok/462110*
Sichere Konfiguration von Microsoft PowerPoint 2013/2016/2019 v1.1

15 *https://allianz-fuer-cybersicherheit.de/dok/462114*
Sichere Konfiguration von Microsoft Word 2013/2016/2019 v1.1

16 *https://allianz-fuer-cybersicherheit.de/dok/462108*
Sichere Konfiguration von Microsoft Outlook 2013/2016/2019 v.1.1

17 *https://allianz-fuer-cybersicherheit.de/dok/462112*
Sichere Konfiguration von Microsoft Visio 2013/2016/2019 v1.1

FRAGE 6

Verwenden Sie Virenschutzprogramme?

Virenschutzprogramme sind sehr nützlich zum Schutz von IT-Ressourcen: In vielen Fällen können sie Schadsoftware abwehren und einen Ransomware-Angriff verhindern. **Ein Virenschutzprogramm muss auf allen Systemen installiert werden,** vorrangig auf denen, die mit dem Internet verbunden sind (Arbeitsplatzrechner, Dateiserver usw.). Ein Virenschutzprogramm schützt vor bekannten Bedrohungen, die sich sehr schnell weiterentwickeln: Jeden Tag erscheinen Hunderttausende neue Schadcodevarianten.

Daher muss die Software selbst und ihre Erkennungs-Datenbank immer auf dem neuesten Stand gehalten werden. Diese Datenbank ermöglicht die Identifizierung von Schadprogrammen und -dateien: Wenn sie nicht regelmäßig aktualisiert wird, ist der Virenschutz schnell eingeschränkt.

Die im Handel erhältlichen (teilweise im Betriebssystem bereits enthaltenen) Virenschutzprogramme bieten **automatische Updates** und eine automatische Speicherplatzüberprüfung. Diese Einstellungen müssen unbedingt aktiviert werden.

Darüber hinaus kann es sich gerade bei Kleinstunternehmen je nach Einsatzzweck lohnen, beim Kauf eines Virenschutzprogramms die von vielen Softwareherstellern angebotenen Zusatzfunktionalitäten zu abonnieren, z. B. eine Firewall, einen Webfilter, ein VPN, Anti-Phishing-Tools und Tools zur Verstärkung der Sicherheit von Bankgeschäften.

Vielleicht ist Ihnen aufgefallen, dass die Frage nach den Virenschutzprogrammen nicht Frage Nummer „1“ ist. Das hat seinen Grund: Ein gutes Virenschutzprogramm zu installieren und damit alle IT-Sicherheitssorgen los zu sein – das war einmal … Antivirus-Software ist wichtig, aber die anderen Punkte weiter vorne sind noch wichtiger.

WEITERE INFORMATIONEN FINDEN SIE HIER:

18 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein OPS.1.1.4: Schutz vor Schadprogrammen

19 *https://www.bsi.bund.de/dok/131316*
Virenschutz und falsche Antivirensoftware

18 19

FRAGE 7

Haben Sie eine Richtlinie für sichere Passwörter festgelegt?

WARUM SOLLTE MAN SICHERE PASSWÖRTER WÄHLEN?

Viele Angriffe im Internet werden dadurch ermöglicht, dass zu einfache Passwörter oder dieselben Passwörter für verschiedene Dienste verwendet werden. Es gibt verschiedene Arten von Angriffen auf Passwörter: Brute-Force-Angriffe (der Angreifer probiert so viele Kombinationen wie möglich aus) oder Wörterbuchangriffe (der Angreifer probiert die häufigsten Passwörter aus, zum Beispiel gängige Namen oder einfache Kombinationen wie „qwertz"). Es kann sich bei den Angriffen auch um „Social Engineering" handeln: Dabei probiert der Angreifer persönliche Informationen wie die Vornamen Ihrer Angehörigen oder die Spitznamen Ihrer Haustiere aus, die er zuvor in sozialen Netzwerken ausfindig gemacht hat. Noch einfacher ist es, Passwörter auszuprobieren, die bereits online verfügbar sind. Vielleicht ist Ihr Passwort (mit vielen anderen) einmal bei Dienstleister A abgeflossen, weil er seine Datenbank nicht gut gesichert hatte. Wenn Sie bei Dienstleister B dasselbe Passwort verwenden, machen Sie es einem Angreifer leicht.

Dazu kommt, dass ein Angriff auf Passwörter möglicherweise nicht auf den betroffenen Dienst beschränkt ist, sondern eine Ausbreitung des Angriffs innerhalb des Unternehmens oder auf dessen Partner zur Folge haben kann. Beispielsweise könnte Ihre E-Mail-Adresse vom Angreifer dazu verwendet werden, bösartige E-Mails an Ihre Geschäftskontakte zu senden, um diese zu nachteiligen Aktionen zu verleiten (z. B. auf einen Link zu einer infizierten Website zu klicken, die wie eine völlig legitime Website aussieht – zum Beispiel die Ihrer Bank). Diese Angriffstechnik wird als **Phishing** bezeichnet.

Phishing ist eine der häufigsten Methoden, um an fremde Passwörter zu gelangen.

WAS IST EIN SICHERES PASSWORT?

Bei der Wahl eines Passwortes sind Ihrer Kreativität keine Grenzen gesetzt. Wichtig ist, dass Sie sich das Passwort gut merken können. Hierfür gibt es unterschiedliche Hilfsstrategien: Der eine merkt sich einen Satz und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den zweiten oder letzten). Anschließend verwandelt man unter Umständen noch bestimmte Buchstaben in Zahlen oder Sonderzeichen. Die andere nutzt einen ganzen Satz als Passwort oder reiht unterschiedliche Wörter, verbunden durch Sonderzeichen, aneinander. Eine weitere Möglichkeit besteht darin, zufällig fünf bis sechs Worte aus dem Wörterbuch zu wählen und diese miteinander zu verbinden. Dies resultiert in einem leicht zu merkenden, leicht zu tippenden und für Angreifer schwer zu brechenden Passwort.

Grundsätzlich gilt: Je länger, desto besser. Ein gutes Passwort sollte mindestens acht Zeichen lang sein. Idealerweise enthält es auch Sonderzeichen und Ziffern.

Bei Verschlüsselungsverfahren für WLAN wie zum Beispiel WPA2 oder WPA3 sollte das Passwort beispielsweise mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren.

Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, beispielsweise Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...). Manche Anbieter von Onlinediensten machen technische Vorgaben für die verwendbaren bzw. zu verwendenden Zeichen. Wenn Ihr System Umlaute zulässt, bedenken Sie bei Reisen ins Ausland, dass auf landestypischen Tastaturen diese eventuell nicht eingegeben werden können.

Nicht als Passwörter geeignet sind Namen von Familienmitgliedern, des Haustiers, des besten Freundes, des Lieblingsstars, Geburtsdaten und so weiter. Das vollstän-

dige Passwort sollte möglichst nicht in Wörterbüchern vorkommen. Es sollte zudem nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern wie „asdfgh“ oder „1234abcd“ bestehen.

Einfach Ziffern am Ende des Passworts anzuhängen oder eines der üblichen Sonderzeichen $! ? # am Anfang oder Ende eines ansonsten simplen Passworts zu ergänzen, ist nicht empfehlenswert. Das bekommen die gängigen Passwortknackprogramme automatisiert heraus.

WIE SIEHT EINE GUTE RICHTLINIE FÜR PASSWÖRTER AUS?

- **Für jeden Dienst, der eine Authentifizierung erfordert, ist ein anderes Passwort zu verwenden.** Vor allem sollte niemals dasselbe Passwort für die private und die berufliche E-Mail-Adresse verwendet werden.

- Ein Passwort-Manager kann Ihnen helfen, starke Passwörter zu generieren und sich diese nicht merken zu müssen. Mithilfe eines Passwort-Managers können alle Passwörter in einer verschlüsselten Datei gespeichert werden, auf die man nur mit einem einzigen und einzigartigen Passwort zugreift. Und nur dieses eine Passwort müssen Sie sich merken.

- Damit eine gute Passwortrichtlinie Erfolg hat, muss den Benutzern klargemacht werden, welche Risiken die Wahl eines zu leicht zu erratenden Passworts birgt. **Wenn vom Dienstanbieter (E-Mail, Bank usw.) eine Multifaktor-Authentifizierung (MFA/2FA) angeboten wird, sollte diese aktiviert werden.** Zahlreiche Dienste ermöglichen bereits, das Passwort durch eine Zwei-Faktor-Authentifizierung zu verstärken: Dabei muss außer dem Passwort noch ein weiterer Faktor eingegeben werden. Ohne diesen zweiten Faktor nützt es einem Angreifer in der Regel nichts, irgendwie an Ihr Passwort gekommen zu sein. Banken nutzen für die Zwei-Faktor-Authentifizierung beispielsweise das SMS- oder Push-TAN-Verfahren, bei denen ein Sicherheitscode auf dem Handy angezeigt wird. Es wird empfohlen, diese Art von Authentifizierung grundsätzlich immer zu aktivieren, wenn Sie Ihnen angeboten wird.

Multi-Faktor-Authentifizierung (MFA)

Idealerweise sollte eine Multi-Faktor-Authentifizierung mit einem physischen Token (Chipkarte, USB/FIDO2-Token, Personalausweis usw.) implementiert werden, um den Zugang zu vereinfachen.

Kleine und mittlere Unternehmen, die über viele zentralisierte Softwarelösungen (Kommunikationssystem, interne Webdienste usw.) verfügen, können durch die Aktivierung von Single Sign-on (wenn Sie sich einmal eingeloggt haben, gilt dies für alle Dienste, die Sie im Unternehmen nutzen) die Authentifizierungsmechanismen vereinfachen und verstärken.

Um die Anwendung dieser Regeln zu kontrollieren und zu überprüfen, können KMU unter anderem folgende Maßnahmen ergreifen:

- die Sperrung von Konten nach mehreren fehlgeschlagenen Anmeldeversuchen, wobei diese Sperrung temporär oder dauerhaft sein kann,

- die Deaktivierung von anonymen Anmeldeoptionen („Gastkonten“),

- die Einrichtung einer soliden Passwortrichtlinie auf den Authentifizierungsservern (sich „Passwort“ als Passwort auszusuchen, wird eine solche Richtlinie dann beispielsweise verhindern).

WEITERE INFORMATIONEN FINDEN SIE HIER:

20 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein ORP.4: Identitäts- und Berechtigungsmanagement, ORP.4.A8: Regelung des Passwortgebrauchs

21 *https://www.bsi.bund.de/dok/131366*
Sichere Passwörter erstellen

22 *https://www.bsi.bund.de/dok/131350*
Sicherer Umgang mit Passwörtern, Schritt-für-Schritt erklärt

20 21 22

FRAGE 8

Haben Sie eine Firewall eingerichtet?

WARUM SOLLTE DIE LOKALE FIREWALL AKTIVIERT WERDEN?

Diese Software, die (anders als eine zentrale Firewall) auf dem jeweiligen Computer des Benutzers oder der Benutzerin installiert wird, schützt hauptsächlich vor Angriffen aus dem Internet. Sie ermöglicht es aber auch, das Vorgehen eines böswilligen Akteurs, der es geschafft hat, einen der Arbeitsplatzrechner zu hacken, auszubremsen oder zu erschweren. Die Angreifer versuchen häufig, auch in die anderen Arbeitsplatzrechner einzudringen, um vollständige Systemkontrolle zu erlangen und schlussendlich auf die Dokumente der Benutzerinnen und Benutzer zuzugreifen. Die Aktivierung der Firewall erschwert diese Seitwärtsbewegung.

WIE GEHT MAN VOR?

KLEINSTUNTERNEHMEN

Ohne besondere IT-Kenntnisse stellt die Aktivierung einer auf dem Arbeitsplatzrechner vorinstallierten Firewall und deren Standardeinstellung (die alle eingehenden Verbindungen blockiert) eine erste Schutzstufe dar. Eine lokale Firewall ist eine Funktion, die auf den meisten Betriebssystemen verfügbar ist. Firewalls werden auch in Kombination mit Antivirus-Software-Suiten vertrieben.

KLEINE UND MITTLERE UNTERNEHMEN

Eine lokale Firewall (entweder im Betriebssystem integriert oder als Softwarelösung eines Drittanbieters) sollte auf allen Arbeitsplatzrechnern installiert werden. Es wird empfohlen, für einheitliche Konfigurationen und Filterrichtlinien zu sorgen.

Eine strenge Filtereinstellung:

- blockiert alle nicht zwingend notwendigen Verbindungen und
- protokolliert blockierte Verbindungen.

Darüber hinaus sollten auch KMU vorrangig zentrale Firewalls (also spezielle Hardware) einsetzen, um die Verbindung zwischen Informationssystem und Internet zu schützen. Unternehmen, die in puncto Sicherheit besonders sorgfältig sein wollen und/oder über ein großes IT-Netz verfügen, müssen das Unternehmensnetz in Zonen mit unterschiedlichen Sicherheitsebenen hinsichtlich der Anfälligkeit für Bedrohungen unterteilen (Zone für Arbeitsplatzrechner, Zone für interne Server, Zone für mit dem Internet verbundene Server, Zone für Industriesysteme und Produktionsmittel usw.).

Was die Verbindung mit dem Internet betrifft, so wird diese idealerweise durch die Implementierung einer „demilitarisierten" Zone (DMZ) umgesetzt, die aus Firewalls, aber auch aus Proxy-Diensten besteht – vor allem für die Kommunikation und das Navigieren im Internet.

WEITERE INFORMATIONEN FINDEN SIE HIER:

23 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein NET.3.2: Firewall

24 *https://www.bsi.bund.de/dok/131310*
Firewall – Schutz vor dem Angriff von außen

23 24

FRAGE 9

Wie sichern Sie Ihre Mailaccounts ab?

KLEINSTUNTERNEHMEN
E-Mails sind der häufigste Infektionsvektor am Arbeitsplatzrechner, sei es durch das Öffnen von Anhängen, die schädlichen Code enthalten, oder durch das Klicken auf einen Link, der auf eine schädliche Website umleitet (Phishing).

Ein paar einfache Fragen schützen zumindest teilweise vor Angriffen per E-Mail: Ist der Absender bekannt? Erwarten Sie irgendwelche Informationen von ihm? Steht der vorgeschlagene Link im Zusammenhang mit dem erwähnten Thema? Im Zweifelsfall ist es erforderlich, die Echtheit der Nachricht über einen anderen Kanal (Telefon, SMS usw.) beim Absender zu überprüfen.

Außerdem ist die Umleitung beruflicher Nachrichten an ein persönliches E-Mail-Konto unbedingt zu unterlassen, denn oftmals ist das Unternehmensnetz besser geschützt als das der Mitarbeiter zu Hause.

Manchmal lässt sich beobachten, dass Mitarbeiter verdächtige E-Mails von ihrem privaten E-Mail-Konto an das bei ihrem Arbeitgeber weiterleiten, da sie davon ausgehen, dessen Netzwerk sei perfekt geschützt und werde schädliche E-Mails sicher herausfiltern. Machen Sie Ihrer Belegschaft klar, dass weder das eine noch das andere Verhalten eine tolerierbare Nutzung von IT darstellt.

KLEINE UND MITTLERE UNTERNEHMEN
Egal, ob das Unternehmen sein E-Mail-System selbst betreibt oder betreiben lässt, es muss dafür sorgen:

- dass den Mailboxen der Benutzer ein Virenscanner vorgeschaltet ist, damit infizierte Dateien herausgefiltert werden,
- dass die Transportverschlüsselung der Kommunikation zwischen Mailservern (des Unternehmens oder öffentlicher Server) sowie zwischen den Arbeitsplatzrechnern der Benutzer und den Servern, die die elektronischen Postfächer hosten, aktiviert ist.

Zum Schutz vor bekannten Betrügereien (z. B. betrügerische Aufforderung zu einer Überweisung, die angeblich von einem Vorgesetzten stammt, sogenannter „CEO-Fraud“) müssen organisatorische Maßnahmen (beispielsweise durch Programme zur Mitarbeitersensibilisierung) strikt umgesetzt werden.

WEITERE INFORMATIONEN FINDEN SIE HIER:

25 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein APP.5.3: Allgemeiner E-Mail-Client und -Server

26 *https://www.bsi.bund.de/dok/131822*
Nutzen Sie die E-Mail wirklich sicher?

25 26

FRAGE 10

Wie trennen Sie unterschiedliche IT-Bereiche?

Die Verbindung von IT-Anwendungen mit dem Internet birgt eine Reihe von Risiken, dazu gehören:

- die Datenexfiltration aus dem Unternehmen ins Internet, womit die Vertraulichkeit der Daten nicht mehr gegeben ist und der Ruf des Unternehmens Schaden nimmt, wenn dies öffentlich wird,
- das Eindringen vom Internet aus, um die Integrität oder die Verfügbarkeit des Informationssystems und der Produktionsmittel des Unternehmens zu beeinträchtigen (insbesondere durch Ransomware),
- Identitätsdiebstahl,
- der Missbrauch des Unternehmensinformationssystems für betrügerische oder kriminelle Zwecke.

WIE KANN MAN SICH VOR SOLCHEN BEDROHUNGEN BESSER SCHÜTZEN?

Verwenden Sie keine Gruppenaccounts, sondern für jeden Mitarbeiter und jede Mitarbeiterin ein eigenes Nutzerkonto. Normale Nutzerinnen und Nutzer dürfen nicht über Administratorrechte verfügen. Administratorkonten bleiben Administratorinnen und Administratoren vorbehalten. Dadurch wird das Risiko der Einschleusung von Schadcodes eingeschränkt.

Für das Navigieren im Internet dürfen nur Benutzerkonten genutzt werden: Tatsächlich werden viele Angriffe dadurch verursacht, dass von einem Konto mit Administratorrechten aus gesurft wird, was es einem Angreifer wesentlich einfacher macht, die vollständige Kontrolle über den Computer zu erlangen. Die Administratorkonten dürfen ausschließlich zum Konfigurieren der Systeme oder zum Installieren von Software verwendet werden. **Die Konten und ihre Berechtigungen müssen auf dem neuesten Stand gehalten werden: Wenn oder eine Mitarbeiterin das Unternehmen verlassen, müssen seine Zugriffsrechte ermittelt und widerrufen werden, und zwar so, dass weder er oder sie selbst noch ein Dritter sie wieder nutzen kann.**

Ideal ist es, einen Computer nur für die berufliche Arbeit und weder für persönliche Belange noch in der Familie zu nutzen. Falls dies nicht möglich ist, müssen bei Mehrfachnutzung ein und desselben Geräts auf jeden Fall für

jede zusätzliche Nutzung weitere Benutzerkonten angelegt werden.

Diese Unterteilungen kann auch ein Einzelunternehmer auf seinem eigenen Gerät leicht umzusetzen.

Ähnliches gilt für mobile Endgeräte: **Die Berechtigungen von Apps müssen für jede Nutzungsart eingeschränkt werden, und Apps dürfen ausschließlich von offiziellen Plattformen** oder von der Website der tatsächlichen Herausgeber heruntergeladen werden.

KLEINE UND MITTLERE UNTERNEHMEN
Kleine und mittlere Unternehmen, die eine größere Anzahl von Mitarbeitern und ein IT-Netzwerk mit mehreren Geräten besitzen, sollten die folgenden Maßnahmen ergreifen oder sie von ihrem Dienstleister umsetzen lassen:

- Verbindungen zwischen den Arbeitsplatzrechnern müssen standardmäßig verboten sein. Wenn ein Rechner mit Schadsoftware infiziert ist, verhindert diese Segmentierung, dass die anderen Rechner ebenfalls sofort infiziert werden.
- Zur Administration des Unternehmensnetzes sollten eigens dafür eingerichtete Arbeitsplätze und Administratorkonten genutzt werden.
- Wenn die Ressourcen des Unternehmens es zulassen, sollten die IT-Aktivitäten des Unternehmens durch physische oder virtualisierte Filter in verschiedene Netzwerkzonen unterteilt werden (Zone für interne Server, Zone für mit dem Internet verbundene Server, Zone für Arbeitsplatzrechner, Zone für Administration, Zone für Industriesysteme usw.). Es ist empfehlenswert, sich von IT-Spezialisten beraten zu lassen, damit Sie von einer sicheren und an Ihr Informationssystem und die Art Ihrer Daten angepassten Architektur profitieren.

WEITERE INFORMATIONEN FINDEN SIE HIER:

27 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein OPS.1.1.2: Ordnungsgemäße IT-Administration

28 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein ORP.4: Identitäts- und Berechtigungsmanagement

27 + 28

FRAGE 11

Haben Sie IT-Risiken im Homeoffice und bei Geschäftsreisen im Griff?

Laptops, Smartphones oder Tablets sind praktisch für den Einsatz im Homeoffice und auf Geschäftsreisen. Viele Arbeiten lassen sich so auch unterwegs oder von zu Hause aus erledigen.

Mobiles Arbeiten erleichtert zwar die durchgängige Geschäftstätigkeit, birgt aber auch bestimmte Risiken.

WAS IST ZU BEACHTEN, WENN SIE BERUFLICH UNTERWEGS SIND?

Sichern Sie Ihre Daten, damit Sie diese im Fall von Verlust oder Diebstahl der Geräte wiederherstellen können.

- Statten Sie Ihre Geräte bei Geschäftsreisen mit Blickschutzfiltern aus.
- Sorgen Sie dafür, dass Ihre Passwörter nicht gespeichert (zum Beispiel im Webbrowser) und automatisch angeboten werden, sondern vom Nutzer oder der Nutzerin eingegeben werden müssen.
- Nutzen Sie Multi-Faktor-Authentisierung (beispielsweise eine Smart-Card oder einen FIDO2-Token).
- Verschlüsseln Sie nach Möglichkeit Ihre sensiblen Daten oder die gesamte Festplatte.
- **Erlauben Sie den Zugriff auf das Unternehmensnetzwerk von außen (beispielsweise aus dem Homeoffice) ausschließlich per VPN** *(Virtual Private Network).* Das gilt auch für Zugriff auf die E-Mail-Konten mittels Webbrowser.

WELCHE VORSICHTSMASSNAHMEN GELTEN WÄHREND DES EINSATZES?

Behalten Sie Ihre Geräte, Speichermedien und Dateien bei sich, auch wenn Sie beispielsweise im Zug nur kurz auf Toilette gehen oder einen Kaffee holen.

- Informieren Sie umgehend Ihr Unternehmen, falls Sie Ihre Hardware verlieren oder sie gestohlen wird.
- Verweigern Sie den Anschluss von Geräten Dritter an Ihre eigenen Geräte (Laptop, USB-Stick, MP3-Player, USB-Ladekabel usw.).

NACH DER RÜCKKEHR

Verwenden Sie niemals USB-Sticks, die Ihnen auf Reisen (Messen, Meetings usw.) geschenkt werden oder die sie irgendwo gefunden haben: Sie können schädliche Programme enthalten.

Falls Sie mit sehr sensiblen Daten arbeiten, einen Grund haben anzunehmen, Sie könnten Opfer von Wirtschafts- oder Industriespionage werden oder in Länder reisen, die im Ruf stehen, Bürgerrechte zu missachten, sollten Sie weitere Dinge beachten:

VOR DER REISE

- Verwenden Sie nur Geräte (Computer, Wechselmedien, Telefon), die für den Einsatz bestimmt sind und nur die notwendigen Daten enthalten.
- Löschen Sie die Anrufliste und den Browserverlauf.
- Kennzeichnen Sie Ihre Geräte, um sicherzustellen, dass sie nicht unbemerkt vertauscht werden.
- Wenn Sie aus der Ferne auf die Informationssysteme des Unternehmens zugreifen müssen, sollten Sie eine VPN-Software installieren, um Ihre Kommunikation zu schützen. Fragen Sie sich, ob Sie wirklich nicht einige Tage auskommen, ohne aus der Ferne Zugriff auf alle Ihre Unternehmensdaten zu haben.

WÄHREND DER REISE

- Bewahren Sie Ihre Geräte, Speichermedien und Dateien sowohl während der Reise als auch während des Aufenthalts bei sich auf (lassen Sie sie auch nicht in einem Hotelsafe liegen).
- Schalten Sie Ihre Geräte aus, falls Sie sie irgendwo abgeben müssen. Bei Handy und Smartphone entfernen Sie außerdem auch die SIM-Karte.
- Informieren Sie Ihr Unternehmen bei Verlust oder Diebstahl oder wenn Ihre Geräte von ausländischen Behörden untersucht oder beschlagnahmt werden.
- Verwenden Sie idealerweise keine Geräte, die man Ihnen zur Nutzung anbietet; geben Sie dort keinesfalls Passwörter ein.
- Verbinden Sie Ihre Hardware nicht mit Geräten, in die Sie kein Vertrauen haben. Wenn Sie während einer Geschäftspräsentation Dokumente austauschen müssen, tauschen Sie diese lieber per E-Mail aus oder verwenden Sie einen nur für diesen Zweck vorgesehenen USB-Stick und löschen Sie die Daten anschließend mit einer sicheren Löschsoftware. Wenn Sie Ihr Mobiltelefon aufladen müssen, schließen Sie es nicht an einen nicht kontrollierten Computer oder an ein fremdes USB-Ladegerät (z. B. an Flughäfen) an.

NACH DER REISE

- Ändern Sie die Passwörter, die Sie während der Reise verwendet haben.
- Lassen Sie, wenn möglich, Ihre Geräte nach der Reise überprüfen. Andernfalls schaffen Sie zusätzliche Geräte an und sondern Sie diese nach der Dienstreise aus.

WEITERE INFORMATIONEN FINDEN SIE HIER:

29 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein INF.9 Mobiler Arbeitsplatz

30 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein CON.7: Informationssicherheit auf Auslandsreisen

31 *https://www.bsi.bund.de/dok/131154*
Sichere Technik, auch auf Reisen

29 + 30

31

FRAGE 12

Wie informieren Sie sich? Wie sensibilisieren Sie Ihre Beschäftigten?

KLEINSTUNTERNEHMEN: SICH INFORMIEREN

Ohne besondere IT-Kenntnisse oder viel Zeit aufwenden zu müssen, ist es möglich, sich über Empfehlungen zu bewährten Verfahren, Warnungen zu aktuellen Bedrohungen und verfügbare Software-Updates zu informieren, indem man die Nachrichten auf der BSI-Webseite www.bsi.bund.de verfolgt. Das BSI bietet auch das Abonnement von kostenlosen Newslettern für verschiedene Zielgruppen an. Darüber hinaus hat das BSI vor einiger Zeit die „Allianz für Cyber-Sicherheit (ACS)“ initiiert, der Unternehmen kostenfrei beitreten können. Auch die ACS bietet eine Vielzahl von Informationen für Unternehmen an.

KLEINERE UND MITTLERE UNTERNEHMEN: INFORMIEREN SIE SICH UND IHRE MITARBEITER

Das BSI betreibt mit dem „Computer Emergency Response Team“ (CERT-Bund) die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen und erfasst in Zusammenarbeit mit dem Nationalen IT-Lagezentrum des BSI auch die technische Entwicklung von Angriffskampagnen und Sicherheitslücken. Es stellt technische Informationen für verschiedene Zielgruppen bereit. Einige davon eignen sich besonders für KMU mit einer IT-Abteilung, andere auch für kleine Unternehmen, die ihre Kenntnisse erweitern wollen.

Darüber hinaus empfiehlt es sich für KMU, eine Kultur der „Computerhygiene“ zu schaffen, indem die Mitarbeiter und Mitarbeiterinnen regelmäßig über gute Sicherheitspraktiken und die wichtigsten Bedrohungen informiert werden, die den Betrieb beeinträchtigen können. Eine IT-Charta kann diese Sensibilisierung erreichen. Diese wird jedem Mitarbeiter ausgehändigt. Sie beschreibt die einzuhaltende IT-Nutzung und das Verfahren zum Melden von Vorfällen. Auf sie sollte regelmäßig hingewiesen werden, beispielsweise durch regelmäßige interne Informationen, bei Sitzungen oder in einem Newsletter.

Das Melden von internen IT-Sicherheitsvorfällen muss gefördert werden, deshalb ist eine zwanglose Vorgehensweise zu bevorzugen. Ziel ist es, das Verantwortungsbewusstsein der Benutzerinnen und Benutzer angesichts der sich entwickelnden Bedrohungen zu wecken und nicht, sie zu bestrafen. Nur so lässt sich erreichen, dass möglichst viele Vorfälle erfasst werden können. Das BSI hat hierzu eine IT-Notfallkarte entwickelt, die Sie sich kostenfrei herunterladen und in Ihrem Unternehmen verwenden können.

Informationen erhalten Sie ebenfalls über eine kostenlose Mitgliedschaft in der durch das BSI initiierten Public-Private-Partnership „Allianz für Cyber-Sicherheit“.

WEITERE INFORMATIONEN FINDEN SIE HIER:

32 *https://www.allianz-fuer-cybersicherheit.de/*
Allianz für Cybersicherheit

33 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein ORP.3:
Sensibilisierung und Schulung zur Informationssicherheit

34 *https://www.bsi.bund.de/dok/520180*
BSI-Newsletter und Sicherheitshinweise

35 *https://www.bsi.bund.de/dok/523422*
IT-Notfallkarte – Ihr Einstieg ins Notfallmanagement

FRAGE 13

Deckt Ihre Versicherungspolice auch Cyber-Risiken ab?

Versicherungsunternehmen bieten zunehmend Produkte an, um Unternehmen zu unterstützen, die Opfer von Malware oder Cyber-Angriffen werden. Im Schadensfall bietet die Versicherung finanzielle Deckung für den Schaden sowie oftmals auch Rechtsbeistand an. Manchmal werden durch die Versicherung bzw. einen von ihr beauftragten Dienstleister im Bedarfsfall sogar die Abwehrmaßnahmen gegen einen akuten Cyber-Angriff übernommen.

Es gibt verschiedene Absicherungsarten, u. a. gegen Identitätsdiebstahl, Garantien gegen Betriebsausfälle, Rechtsberatung bei der Meldung einer Verletzung des Schutzes personenbezogener Daten und technische Unterstützung bei der Wiederherstellung des Informationssystems nach einem Cyber-Angriff.

Die jeweiligen Versicherungsklauseln können in herkömmliche Versicherungsverträge aufgenommen werden oder die Form einer speziellen „Cyber"-Versicherungspolice annehmen, wobei sich der letztgenannte Markt gerade erst entwickelt. Auf jeden Fall muss sichergestellt werden, dass die für den Fortbestand des Unternehmens bedeutendsten Risiken abgedeckt sind.

FRAGE 14

Wissen Sie, wie Sie bei einem Cyber-Angriff reagieren müssen?

BEREITEN SIE SICH AUF EINEN VORFALL VOR

KMU sollten in Erwartung, dass es irgendwann zu einem ernsten IT-Sicherheitsvorfall kommen wird, bereits im Voraus Dienstleister ausfindig machen, die auf die Bekämpfung von Sicherheitsvorfällen spezialisiert sind. Das BSI hält dazu unter www.bsi.bund.de eine Liste qualifizierter IT-Dienstleister bereit.

IM FALL EINES NACHGEWIESENEN VORFALLS

Bei einem Vorfall in einem Informationssystem sollten Sie als Erstes Ihre Geräte oder das Informationssystem Ihres Unternehmens vom Internet trennen. Für einzelne Geräte kann dies bedeuten, den Netzwerkstecker zu ziehen oder WLAN-Dienste zu deaktivieren. Für das Informationssystem eines Unternehmens kann dies an den Netzwerkkomponenten oder der Unternehmens-Firewall durchgeführt werden. Dadurch wird der Angreifer daran gehindert, seinen Angriff wie z. B. eine Ransomware zu steuern, und es wird eine mögliche Datenexfiltration verhindert.

Schalten Sie die vom Angriff betroffenen Computer und Geräte nicht aus und verändern Sie sie nicht, um die Arbeit der hinzuzuziehenden IT-Forensiker/Ermittler nicht zu behindern.

Wenn Lösegeld gefordert wird, gehen Sie niemals darauf ein. Erstens ist nicht sichergestellt, dass Sie nach Zahlung des Lösegeldes tatsächlich einen Entschlüsselungsschlüssel erhalten. Zweitens müssen Sie ohnehin erst herausfinden, wie die Angreifer Zugriff auf Ihr System erlangt haben, und diesen Zugang schließen. Andernfalls werden Ihre Daten sonst unter Umständen wieder verschlüsselt („Wer einmal gezahlt hat, zahlt auch ein zweites Mal!“). Und Drittens, haben Sie spätestens nach Lesen der Frage 3 in dieser Broschüre dafür gesorgt, dass alle Ihre wichtigen Daten gesichert sind. Zwar sind Opfer von Ransomware-Angriffen häufig mit dem Problem konfrontiert, dass Daten vor der Verschlüsselung von den Angreifern ausgeleitet/gestohlen werden. Aber bei einer vorhandenen Datensicherung kann ein Unternehmen nach Schließen des durch die Angreifer genutzten Einfallstors immerhin die Backups zurückspielen und den normalen Geschäftsbetrieb wieder aufnehmen.

Es wird empfohlen, ein Logbuch zu erstellen, um Aktionen und Ereignisse im Zusammenhang mit dem Vorfall zu verfolgen. Jeder Eintrag dieses Dokuments sollte mindestens die folgenden Angaben enthalten:

- die Uhrzeit und das Datum der Aktion und des Ereignisses,
- den Namen der Person, die die Aktion vorgenommen hat oder über das Ereignis informiert wurde, sowie
- die Beschreibung der Aktion oder des Ereignisses.

Ein Logbuch, das während des gesamten Vorfalls regelmäßig aktualisiert wird, erleichtert das Eingreifen des Dienstanbieters und die Behebung des Problems erheblich.

Zusätzlich muss ein KMU unbedingt ein Konzept für die interne und externe Kommunikation entwickeln, das im Falle eines Angriffes unverzüglich umgesetzt werden kann.

Außerdem können die Mitarbeiter über die IT-Charta informiert werden, wie sie sich im Fall eines nachgewiesenen Vorfalls zu verhalten haben.

RECHTLICHE ASPEKTE

Unternehmen, die personenbezogene Daten verarbeiten und der Datenschutz-Grundverordnung unterliegen, müssen die Anforderungen dieser Verordnung einhalten. Bei einem Vorfall müssen sie zudem die zuständigen Datenschutzbeauftragen und ihre Kunden informieren.

Es sollte unbedingt Anzeige erstattet werden. Gute Ansprechpartner dafür sind die „Zentralen Ansprechstellen Cybercrime (ZAC)“ der zuständigen Polizeien.

WEITERE INFORMATIONEN FINDEN SIE HIER:

36 *https://www.bsi.bund.de/dok/531534*
BSI IT-Grundschutz-Baustein DER.2.1:
Behandlung von Sicherheitsvorfällen

37 *https://www.bsi.bund.de/dok/133680*
Einen Vorfall bewältigen, melden, sich informieren, vorbeugen

38 *https://www.bsi.bund.de/dok/409044*
Dokument „Ransomware:
Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“

39 *https://www.bsi.bund.de/dok/128152*
Zertifizierung und Anerkennung durch das BSI

40 *https://www.bsi.bund.de/dok/128816*
Qualifizierte Dienstleister

41 *https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/Infoblatt_Datenschutzverstoesse.pdf*
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit; Infoblatt „Meldung von Datenschutzverstößen“

42 *https://www.bsi.bund.de/dok/128672*
Cyber-Sicherheitsnetzwerk

43 *https://www.bsi.bund.de/dok/519246*
Zusammenarbeit mit der Polizei

36 37 38 39 40 41 42 43

Wer nicht vorbereitet ist, hat bei einem Vorfall das Nachsehen.

Warten Sie nicht, bis der Ernstfall eintritt.

Schützen Sie sich jetzt!

In diesem Leitfaden werden anhand von **14 Fragen** verständliche Maßnahmen zum Schutz des Unternehmens vorgestellt.

Einige Empfehlungen beruhen auf einfach umsetzbaren Vorgehensweisen, andere erfordern etwas mehr Aufwand. Wenn Sie diese Empfehlungen befolgen, erhöhen Sie Ihr Sicherheitsniveau und schärfen das Bewusstsein Ihrer Teams für die richtigen Maßnahmen. Es liegt an Ihnen, das Thema aufzugreifen und Ihr Unternehmen sowie Ihre Mitarbeiterinnen und Mitarbeiter zu schützen.

www.bsi.bund.de