CyberSicherheitsCheck
für kleine und mittlere Unternehmen (KMU)

Handbuch

für Beratende

Stand 31.10.2024

Baden-Württemberg
MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN

POLIZEI
BADEN-WÜRTTEMBERG
LANDESKRIMINALAMT
BADEN-WÜRTTEMBERG

Hochschule Aalen

CSBW CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

AUTOREN
Prof. Dr. Christoph Karg, Demian Deffner, Miriam Kappe

Unter Mitwirkung von:
Jochen Wellhäußer, Reinhold Hepp

www.csc-kmu.de

Inhalt

1. Einleitung

Dieses Handbuch bezieht sich auf den CyberSicherheitsCheck (fortan im Text CSC genannt) für KMU (www.csc-kmu.de). Es führt in das Beratungskonzept ein, gibt einen Überblick über die Themen und bietet vertieftes Wissen zu den Themen der Beratung. Dieses Handbuch richtet sich an die Beratenden, die den CSC durchführen, sowie an Schulungsanbietende des CSC.

Das Beratungskonzept wurde von 2022 bis 2024 im Rahmen eines Forschungsprojekts an der Hochschule Aalen entwickelt (Projektbezeichnung: Cybersicherheit, Wirtschaftsschutz und Prävention, Abkürzung CyberWuP). Mit dem CSC für kleine und mittlere Unternehmen (KMU) wurde eine Beratungsstruktur entwickelt, die der Geschäftsleitung kleinster und kleiner Unternehmen in einer Stunde einen Überblick über die Cybersicherheit im eigenen Unternehmen sowie über die grundlegenden Aspekte (Basismaßnahmen) von Cybersicherheit geben kann. Sie richtet sich an die Geschäftsleitungen von Unternehmen bis 100 Mitarbeitende. Der wesentliche Anwendungsfall des CSC ist die Beratung der Geschäftsleitung von Unternehmen mit 10 bis ca. 50 Mitarbeitenden.

Der CSC eignet sich jedoch auch für die Beratung von Kleinstunternehmen in einer Größenordnung von unter 10 Mitarbeitenden und in Einzelfällen auch für größere Unternehmen bis ca. 100 Mitarbeitende. Auf die Spezifika der Beratungssituationen von kleinen Unternehmen wird in diesem Handbuch im Kapitel „17.3 Beratung von Kleinst- und Einpersonenunternehmen“ eingegangen.

2. Ausgangssituation

Trotz zahlreicher Materialien und Initiativen sind viele KMU, insbesondere Kleinst- und Kleinunternehmen, beim Thema Cybersicherheit schlecht aufgestellt. Das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg hat deshalb zusammen mit der Hochschule Aalen 2021 das Forschungsprojekt CyberWuP ins Leben gerufen. Das Projekt leistet einen Betrag, um diese Situation zu verbessern. Hierzu wird aus bestehenden Standards, Richtlinien und Empfehlungen ein Maßnahmenkonzept mit reduzierter Komplexität abgeleitet, welches die wichtigsten von KMU umzusetzenden Sicherheitsmaßnahmen in verständlicher Art und Weise beschreibt. Es soll KMU im direkten Austausch vor Ort dazu animieren, sich intensiver mit Cybersicherheit zu beschäftigen, entsprechende Maßnahmen umzusetzen und somit die Risiken von Schäden durch Cyberattacken für das Unternehmen zu reduzieren.

Kleinere und mittlere Unternehmen (KMU) bilden einen Großteil der Unternehmen der deutschen Wirtschaft. Ihre Wirtschaftskraft ist für den Wirtschaftsstandort Deutschland, insbesondere auch Baden-Württemberg, von großer Bedeutung. Mit zunehmender Digitalisierung nutzen viele der KMU Informationssysteme im Rahmen ihrer Geschäftsprozesse. Funktionierende Informationssysteme sind eine der Grundlagen für einen ordnungsgemäßen Geschäftsbetrieb. Cyberattacken gefährden den störungsfreien Geschäftsbetrieb und stellen ein Risiko für die Wirtschaftskraft der KMU dar. Für viele Unternehmen ist die Umsetzung von Maßnahmen im Kontext der Cybersicherheit eine Herausforderung, z. B. mangels Zeit und Ressourcen. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gilt dies insbesondere für Kleinst- (weniger als 10 Mitarbeitende) und Kleinunternehmen (weniger als 50 Mitarbeitende), also für 96,8 % der deutschen Unternehmen (BSI, 2022).

Obwohl die Unternehmen einer großen Anzahl von Cyberangriffen ausgesetzt sind, sind viele der KMU beim Thema Cybersicherheit schlecht aufgestellt. Eine vom Bundesministerium für

Wirtschaft und Klimaschutz (BMWK) in Auftrag gegebene Studie zeigt auf, dass viele KMU keine Kenntnisse über die aktuelle Bedrohungslage, also über aktuelle Gefährdungen durch Cyberattacken, besitzen (BMWK, 2021). Die Studie weist kleinere oder/und inhabergeführte KMU als stärker bedroht aus. Laut den darin befragten IT-Dienstleistern spielen die Entscheider eines Unternehmens bei der Umsetzung von Sicherheitsmaßnahmen eine zentrale Rolle.

Sind Entscheider entsprechend sensibilisiert, dann steigt die Bereitschaft, in IT-Sicherheit zu investieren (BMWK, 2021).

Mit dem CSC wurde ein am Bedarf der KMU ausgerichtetes Konzept erarbeitet, welches der schwierigen Situation für kleine Unternehmen begegnet und mit pragmatischen Lösungsschritten zu einem größeren Bewusstsein für ein Mehr an Cybersicherheit beitragen soll.

2.1 KMU-Cybersicherheitsklassen

KMU sind nicht homogen. Und so sind auch ihre Bedarfe an zusätzlichem Wissen und Fähigkeiten im Bereich Cybersicherheit unterschiedlich. Die Unterscheidung nach Unternehmensgröße reicht nicht aus.

Der CSC eignet sich nach den Forschungsergebnissen, den Ergebnissen aus den Pilotierungen und dem festgestellten Bedarf am besten für:

1. **KMU ohne Cybersicherheit:** Diese KMU nehmen Sicherheitsbedrohungen nicht wahr. Deshalb sehen sie auch keine Notwendigkeit für Sicherheitsmaßnahmen. Es fehlen Sicherheitskompetenz und IT-Fachkräfte. Sie weisen keine Ressourcen für Cybersicherheit zu. Sie haben keine Cybersicherheitsleitlinie.

2. **KMU mit lückenhaften Cybersicherheitsfähigkeiten:** Diese KMU sind sich einiger Bedrohungen und Schwachstellen bewusst. Es fehlt an Überblick und Cybersicherheitskenntnissen. Auch die Verbindung zu Experten, Dritten oder Verbänden zum Austausch von Wissen fehlt. Sie erkennen die Bedeutung von Cybersicherheit. Sie verfügen über eine teilweise ausgearbeitete Cybersicherheitsrichtlinie für einige Bereiche.

Klassifizierung siehe Shojaifar & Järvinen, 2021.

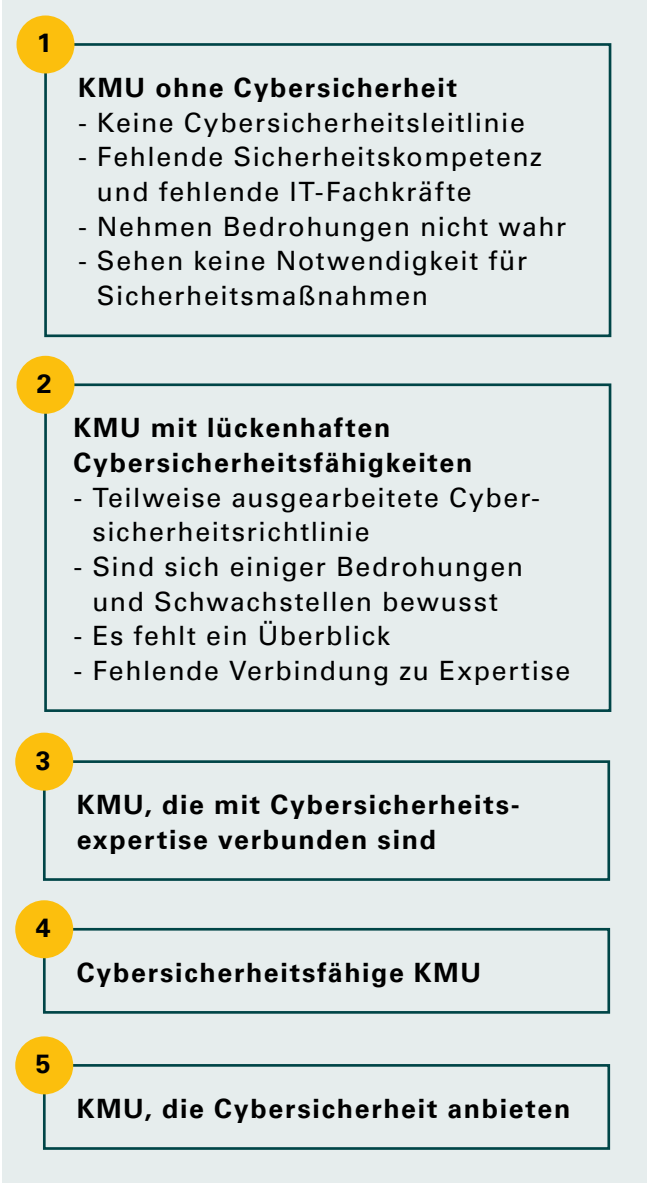


Abbildung 1: 5 Cybersicherheitsklassen von KMU. Eigene Darstellung nach Shojaifar & Järvinen, 2021.

Bei Ersteren liegt die größte Herausforderung in der Ansprache. Da sie in der Regel keine Notwendigkeiten für Sicherheitsmaßnahmen sehen, bedarf es hier extrinsischer Motivation und Überzeugung.

Da vielen Unternehmen häufig das Bewusstsein für Gefahren der Cybersicherheit und für ihre Abhängigkeit von sicher und zuverlässig zur Verfügung stehenden IT-Systemen fehlt, besteht die große Gefahr, dass alles so bleibt, wie es ist, und die dringend gebotenen Schutzmaßnahmen ausbleiben. Genau an diesem psychologischen Punkt setzt das Beratungsmodell CSC an und beabsichtigt, im Rahmen des Dialogs vor Ort die Risiken und Gefahren ein Stück weit begreifbar zu machen und darüber hinaus kleine, Mut machende Lösungsschritte aufzuzeigen und damit den demotivierenden Neutralisationstechniken zum „Nichts-Tun“entgegenzuwirken.

2.2 Bedrohungen: Typische Angriffe und Angriffstechniken

Im Folgenden werden die für KMU besonders relevanten, weit verbreiteten und gefährlichen Angriffsmethoden Phishing, CEO-Fraud und Ransomware-Angriffe erläutert.

2.2.1 Phishing

Phishing bezeichnet den Versuch, vertrauliche Informationen von Personen zu erbeuten, z. B. Zugangsdaten oder Kreditkarteninformationen. Phishing richtet sich in der Regel nicht gezielt an eine Person oder Gruppe, sondern erfolgt nach dem Gießkannenprinzip. Eine Ausnahme davon bildet Spear-Phishing. Dies ist ein gezielter Phishing-Angriff auf eine ausgewählte Zielperson. Ein Phishing-Angriff kann den Anfang eines Ransomware-Angriffs darstellen, an dessen Ende alle Systeme verschlüsselt sind und die Zahlung einer großen Summe Lösegeld erpresst wird. Phishing kann auf viele Arten stattfinden, z. B. per Telefon, SMS oder E-Mail. Neuerdings wurden auch Phishing-Versuche mittels Briefpost beobachtet. Phishing-Schreiben enthalten häufig Links, die zu gefälschten Webseiten führen, auf denen die Daten abgegriffen werden sollen. Die gefälschten E-Mails, Briefe und Webseiten wirken meist professionell und authentisch. Mittels KI werden Phishing-Texte sehr individuell, personenbezogen und in kürzester Zeit erstellt.


IONOS

Wichtige Mitteilung - Bestätigen Sie Ihr E-Mail-Konto

Sehr geehrte Kundin, sehr geehrter Kunde,

Ihr E-Mail-Konto steht kurz vor der Deaktivierung. Um sicherzustellen, dass Sie weiterhin Zugriff auf Ihr Konto haben, bestätigen Sie bitte, dass Sie dieses Konto weiterhin nutzen möchten.

Loggen Sie sich dazu bitte ein und bestätigen Sie die Nutzung.

E-Mail-Konto bestätigen

Wenn Sie innerhalb der nächsten 24 Stunden nicht reagieren, wird Ihr E-Mail-Konto deaktiviert und Sie verlieren den Zugriff auf alle Ihre E-Mails und gespeicherten Daten.

Vielen Dank für Ihre sofortige Aufmerksamkeit und Zusammenarbeit.

Mit freundlichen Grüßen,
Ihr IONOS Team

Abbildung 2: Beispiel einer Phishing-Mail (Verbraucherzentrale, 2024).

Die Methoden der Angreifenden entwickeln sich stetig weiter. Da die Bankkunden inzwischen für die Gefahren von Phishing-Mails sensibilisiert sind und vorsichtiger werden, weiten Angreifende ihre Versuche nun seit einiger Zeit auch auf Briefpost aus (siehe Abbildung 3). Die betroffene Person erhält plötzlich und unerwartet einen Brief mit korrekter postalischer Anschrift und dem Logo und der Anschrift der tatsächlichen Bank.

Beigefügt ist ein QR-Code. Wer den QR-Code scannt und dem Link folgt, landet auf einer gefälschten Banking-Seite im Aussehen der jeweiligen Bank. Dort wird dann ein Einloggen erforderlich sein. Das potenzielle Opfer wird durch die diversen Prozesse geführt und darüber erlangen die Angreifenden schließlich Kenntnis und Zugriff auf das echte Onlinebanking. Auch die Abfrage von sicherheitsrelevanten TANs oder die Bestätigung per TAN-App ist möglich.

Die Angreifenden können auf unterschiedliche Arten an die benötigten Daten für den Versand von Briefpost gelangen. Die Daten können beispielsweise aus einem Hack in der Vergangenheit stammen, wo die Nutzenden z. B. Kunde bei einem Onlineshop mit den entsprechend hinterlegten Daten waren / sind. Wurde der Shop gehackt und gelangen diese Daten in die falschen Hände, können die Angreifenden relativ einfach diese Daten auswerten und entsprechend Mails oder Briefpost personalisieren.

Es ist durchaus möglich, dass das potenzielle Opfer diese Daten in der Vergangenheit selber auf einer Phishing-Seite eingegeben hat (z. B. aufgrund einer früheren gefälschten Paketbenachrichtigung per SMS mit Phishing-Link). Auch die Kombination verschiedener Datenbestände ist denkbar (Landeskriminalamt Niedersachsen, 2024). Im Falle der Zielgruppe KMU sind Adressen in der Regel öffentlich und z. B. über die Firmenwebsite abrufbar. Für groß angelegte Phishing-Angriffe ist der Aufwand des händischen Zusammensuchens von Firmenadressen jedoch zu groß, sodass von den oben genannten Datensammlungen die größere Gefahr ausgeht.

Abbildung 3: Gefälschter Brief im Aussehen der Commerzbank (Landeskriminalamt Niedersachsen, 2024).

2.2.2 CEO-Fraud

Bei dieser Art von Angriffen geben sich Kriminelle fälschlicherweise gegenüber den Mitarbeitenden des Unternehmens z. B. als Geschäftsführer (CEO) aus und versuchen, die Überweisung eines größeren Geldbetrags auf ein ausländisches Bankkonto zu veranlassen. Grundlage für diese Angriffe sind umfangreiche Recherchen von firmeninternen Daten wie E-Mail-Erreichbarkeiten, Organigramm, anstehende Investitionen, bestehende Geschäftsbeziehungen, Dienstreisen der Geschäftsleitung usw.

Wichtige Quellen dieser Recherchen sind: Wirtschaftsberichte, Handelsregister, Unternehmenswebsites, Firmenveröffentlichungen, soziale Netze, in denen Mitarbeitende Informationen zu Funktion oder Tätigkeit preisgeben, usw.

Die Angriffstechnik bei CEO-Fraud ist das oben genannte, gezielte Spear-Phishing. Die Kontaktaufnahme erfolgt via Telefon mit verdeckter Nummer oder Mail mit gefälschte Mailadresse. Die Angreifenden geben sich als leitende Angestellte oder auch Geschäftspartner aus. Gängige Beispiele sind „geänderte Kontoverbindungen“ oder angebliche Investitionen wie z. B. „Maschinenkauf auf einer Messe“. Dabei werden Geldbeträge für vorgeblich erbrachte Leistungen und mit vorgetäuschten Anweisungen der jeweiligen Vorgesetztenebene, meist unter zeitlicher Dringlichkeit, eingefordert. Inzwischen können mittels KI für solche Angriffe problemlos auch gefälschte Stimmen, Bilder und Videos der vermeintlichen Vorgesetzten eingesetzt werden.

2.2.3 Ransomware

Ransomware (engl. ransom = Lösegeld), auch bekannt als Verschlüsselungstrojaner, ist eine der Top-Bedrohungen in der Cybersicherheit. Ransomware-Attacken verfolgen das Ziel, Daten zu verschlüsseln und ein Lösegeld für die Entschlüsselung zu erpressen. Um der Erpressung Nachdruck zu verleihen, wird parallel mit der Veröffentlichung von gestohlenen Geschäftsdaten gedroht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt regelmäßig fest, dass in der angespannten bis kritischen Lage im Cyberraum Ransomware weiterhin die Hauptbedrohung ist. (BSI, 2023a).

In Abbildung 4 werden typische Angriffspfade bei einem Ransomware-Angriff skizziert.
Der erste Zugriff gelingt Angreifenden in der Regel zufällig im Zuge breit gestreuter, ungezielter Angriffe wie Phishing, Schwachstellenscans oder Versand von Malware. Die Erbeutung gültiger Zugangsdaten kann z. B. im Zuge eines breit gestreuten, ungezielten Phishing-Angriffs geschehen, wenn ein Opfer sich täuschen lässt und seine Zugangsdaten auf einer gefälschten Webseite eingibt, oder auch durch das Erraten unsicherer Passwörter (teilweise automatisierte Recherche). Für das „Erraten von Passwörtern“ gibt es zudem Listen mit den häufigsten verwendeten Passwörtern. Auch das Verwenden von Daten, die via Social Hacking ermittelbar sind, wie Geburtsdatum, Name des Haustiers, Wohnort usw., macht Passwörter unter Umständen leicht zu erraten.

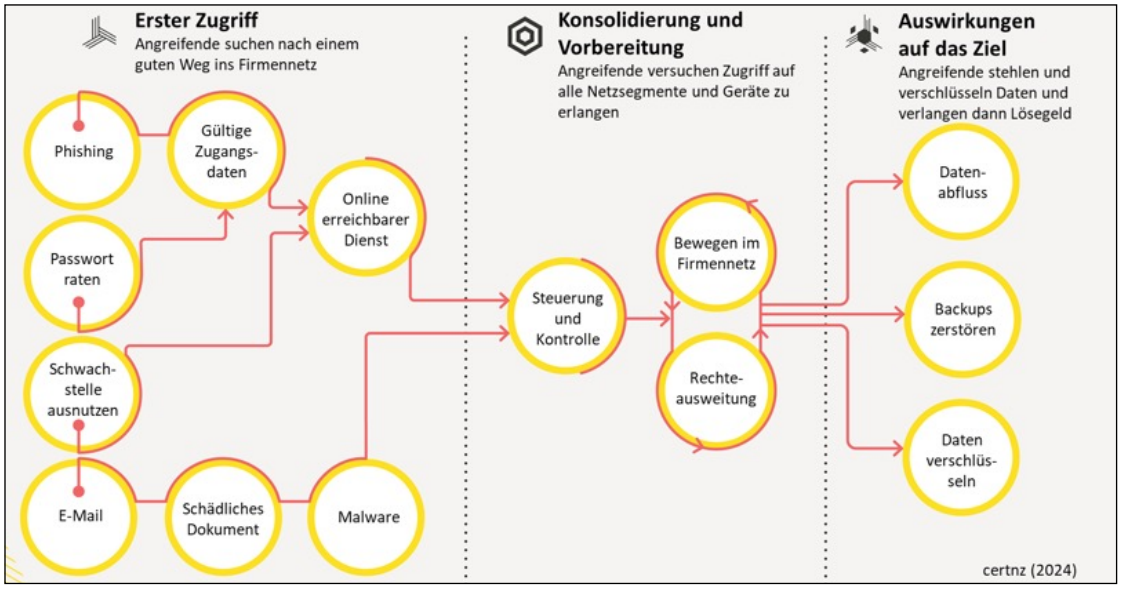


Abbildung 4: Die üblichen Angriffspfade bei einem von Menschen gesteuerten Ransomware-Vorfall.
Quelle: certnz, 2024, übersetzt ins Deutsche.

Mit diesen Zugangsdaten oder durch Ausnutzung offener Schwachstellen kann dann z. B. auf einen online erreichbaren Dienst im Firmennetz Zugriff erlangt werden. Das Einschleusen von Malware, z. B. via E-Mail-Anhang, kann direkt den steuernden Zugriff auf Teile des Firmennetzes ermöglichen.

Von diesem Punkt aus wird versucht, den Zugang zum Firmennetzwerk systematisch auszubauen und zu erweitern (eskalieren). Damit ist der Ransomware-Angriff in seiner zweiten Phase angelangt, der Konsolidierungs- und Vorbereitungsphase.

Das geschieht in einem iterativen Prozess der Rechteausweitung, wo es möglich ist, und der Bewegung im Firmennetz. In dieser Phase wird versucht, administrative Rechte zu bekommen, Zugriff auf relevante Netzbereiche wie Dateiserver, Kundendatenbank und Backup-Systeme zu erlangen und eine Kopie der Firmendaten anzufertigen und zu stehlen. Ebenso wird der Verschlüsselungstrojaner platziert und abschließend ausgeführt.

Die Auswirkungen eines erfolgreichen Ransomware-Angriffs sind üblicherweise:

- Datenabfluss
- Zerstörung der Backups
- Verschlüsselung der Festplatten der Computer
- Kompletter Ausfall der IT-Infrastruktur eines Unternehmens
- Ausfall der Produktion
- Lösegeldforderung, um die Daten zu entschlüsseln bzw. nicht zu veröffentlichen
- Verlust sensibler/vertraulicher Daten, z. B. Konstruktionspläne, Verträge mit Kunden, Personaldaten
- Reputationsverlust

Die Wiederherstellung der Systeme nach einer erfolgreichen Attacke ist sehr aufwendig und kostspielig. Vorsicht ist beim Einspielen der Backups geboten. Diese können pozentiell auch schon infiziert sein: Ransomware-Angriffe erstrecken sich oft über einen längeren Zeitraum. Der große Datenverlust bei der Einspielung älterer Backups muss gegen den Aufwand des Reinigens potenziell infizierter Backups abgewogen werden.

Abbildung 5 zeigt beispielhaft den Sperrbildschirm des Verschlüsselungstrojaners „WannaCry“. Dort steht beschrieben, dass wichtige Daten verschlüsselt worden sind. Es wird die Möglichkeit der Entschlüsselung der Daten versichert, inklusive einer kostenlosen Kostprobe dieser Fähigkeit. Für die vollständige Entschlüsselung wird in diesem Beispiel die Zahlung von 300 $ in Bitcoin gefordert (etwa 275 Euro) und dafür eine Frist von 3 Tagen gesetzt, nach der sich das Lösegeld angeblich verdoppeln werde. Der Ablauf eines Ransomware-Angriffs kann variieren. So kann trotz Lösegeldzahlung der Verkauf der erbeuteten Daten im Darknet stattfinden, die Wiederherstellung der Daten trotz Entschlüsselungssoftware/-key ganz oder größtenteils misslingen, können die Daten in kompromittierter Form zurückgegeben werden und durch möglicherweise fest integrierten Zugang zum Firmennetz erleichterte gleichartige Folgeangriffe (Double bzw. Triple Extortion) durchgeführt werden.

In diesem Handbuch wird gegen Ende, nach der Erläuterung der Beratungskarten, noch mal auf die üblichen Ransomware-Angriffspfade eingegangen und gezeigt, an welchen Stellen die in dieser Beratung enthaltenen Maßnahmen diese Angriffspfade unterbrechen können. Siehe Kapitel „Abwehr von Ransomware-Angriffen“.

Abbildung 5: Ransomware-Beispiel: WannaCry (Seunghwan Hwang, 2017).

3. Beratungsprozess

Aus Sicht der Unternehmen ergibt sich ein Beratungsprozess in vier Schritten, von denen erst der dritte Schritt die Erstberatung darstellt, siehe Abbildung 6. Dies ist kein statisch zu sehender Prozess, sondern soll lediglich eine Orientierung geben, auf welchen Wegen die Beratung des CSC vermittelt und beworben werden kann.

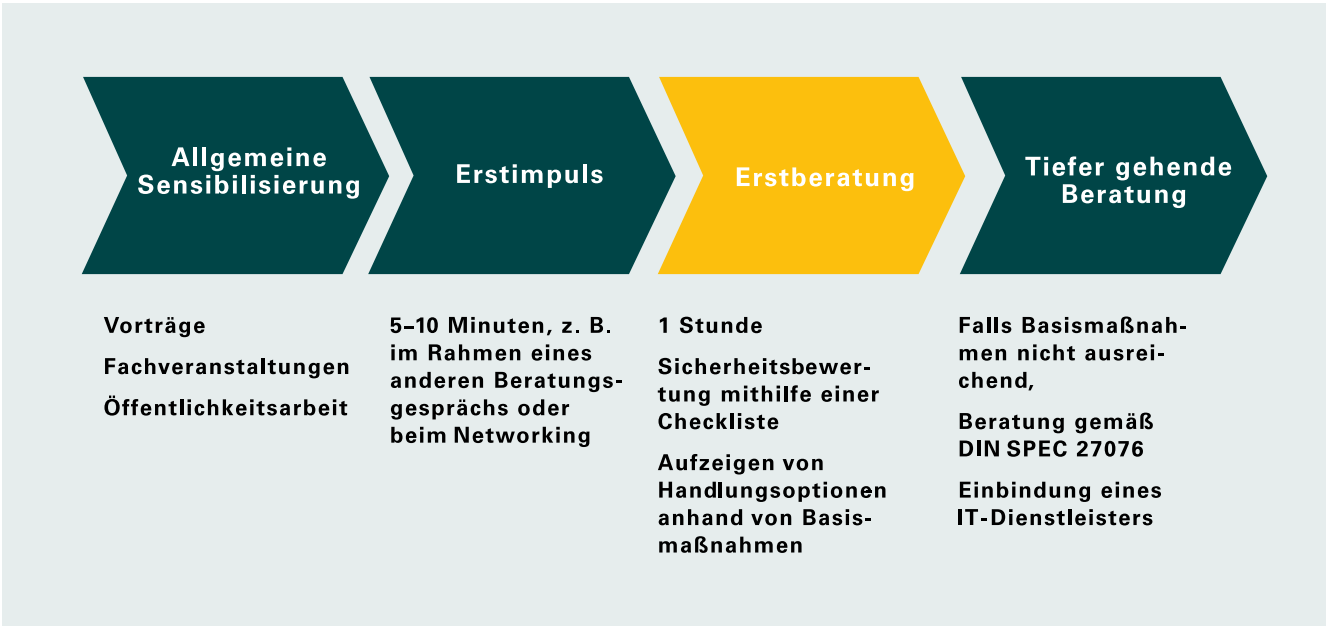


Abbildung 6: Beratungsprozess aus Sicht der Unternehmen, Kundensicht.

Nicht für alle KMU steht das Thema Cybersicherheit bereits auf der Agenda. Detaillierter auf die unterschiedlichen Bedarfe von KMU wurde zuvor bereits im Kapitel „2.1 KMU-Cybersicherheitsklassen“ eingegangen. Im Bereich der allgemeinen Sensibilisierung lassen sich KMU ansprechen, z. B. im Rahmen von Vorträgen, Fachveranstaltungen oder der Öffentlichkeitsarbeit, wo das Beratungsangebot des CSC für KMU beworben und Interesse geweckt werden kann.

Einen Erstimpuls können interessierte oder geeignete KMU z. B. im Rahmen eines anderen Beratungsgesprächs oder beim Networking bekommen, wenn sie hier durch die Beratenden auf das Thema der Cybersicherheit, die Gefahren für das Unternehmen und das Beratungsangebot des CSC für KMU angesprochen werden. Es folgt die Terminkoordination, bei welcher auch sichergestellt werden muss, dass die Beratung tatsächlich mit der Geschäftsleitung stattfindet. Es bietet sich zudem an, gewisse Vorabinformationen zuzusenden, wie beispielsweise einen Hinweis auf die Website www.csc-kmu.de, und insbesondere auch auf die Checkliste zu verweisen, damit sich die Geschäftsleitung auf die Fragen vorbereiten oder zumindest einstellen kann.

Die Erstberatung findet dann im Umfang von einer Stunde statt. Ein Vorschlag für den zeitlichen Ablauf eines solchen Beratungsgesprächs ist in Tabelle 1 zu finden. Der zeitliche Umfang von einer Stunde bildet dabei lediglich einen Richtwert. Mit Blick auf die knappen zeitlichen Ressourcen der Geschäftsleitungen von KMU ist es aber von großem Vorteil, wenn die Beratung üblicherweise nicht länger dauert. Das trägt zur Niederschwelligkeit des Beratungsangebots bei. Im Rahmen der Beratung und zur Vertiefung der Inhalte können die Beratungskarten zu den acht Handlungsfeldern bzw. die Checkliste der Erhebungsfragen ausgehändigt werden.

Phase	Sachinhalt	Methodisch-didaktische Hinweise	Materialien	Zeit (Min.)
Einstieg	Begrüßung, persönliche Vorstellung			2
Beratung erklären	Erklärung des Beratungsablaufs, Checkliste, Auswertung, Beratungskarten	Neugierde wecken, Hemmschwelle abbauen, Vorteile benennen	Mitgebrachtes Material zeigen	2
Sensibilisierung	Fallbeispiel thematisieren: (allgemeiner Fall,) besser „Nachbarschafts“-Fall	Nur kurz: Metaebene	Fall bereithalten	2
Persönliche Sensibilisierung	Zielperson fragen: Sind Sie schon angegriffen worden oder befürchten Sie eine derartige Attacke? Oder: Kennen Sie ein Unternehmen, das angegriffen wurde? /Kennen Sie einen Fall?	Persönliche Betroffenheit herstellen, Bezug zur Lebensrealität aufbauen	Initialfrage bereithalten	4
Gelenkstelle	*Beginn der Arbeitsphase*	*Wechsel zur persönlichen Betroffenheit*		
Checkliste	Stringentes Abarbeiten und Ausfüllen der Fragen des Quick-Checks	Analyse, Sensibilisierung, Risiko aufzeigen, Positives verstärken	**Checkliste/ Excel-Tool**	*ca. 20 Min*
Auswertung	Auswerten – Besprechen – Übergabe des Ergebnisses	Zielperson Überblick verschaffen	PDF zusenden	
Beratungskarten	Die 10 Beratungskarten vorstellen, aushändigen und erläutern	Präzise wichtigste Maßnahmen vermitteln, auf weiterführende Infos der Kartenrückseite verweisen, pragmatische Lösungen aufzeigen, Mut machen zum Handeln	**10 Beratungskarten**	*ca. 25 Min*
Motivationsverstärkung	Hinweis auf Fördergelder u. a. Vorteile, Hinweis auf Gefahren (DSGVO)	Motivation		2
Fazit	Verbindliches Gesprächsergebnis	Zum Handeln ermutigen		2
Verabschiedung				1

Tabelle 1: Ablaufplan und Zeitplan der einstündigen Erstberatung.

Im Anschluss an die Beratung verbleiben die Beratungsmaterialien mit den Beratungsergebnissen bzw. der Auswertung der Antworten im Unternehmen. Üblicherweise hat die Geschäftsleitung mit der Umsetzung der besprochenen und beschriebenen Maßnahmen einiges zu tun. Dennoch ist zur Verstetigung der Cybersicherheit im Unternehmen die kontinuierliche Fortsetzung der Auseinandersetzung äußerst wichtig. In aller Regel ist dafür die Einbindung eines IT-Dienstleisters anzuraten. Dieser übernimmt Aufgaben, für welche dem KMU das Know-how fehlt, und kann auch bei neu aufkommenden Themen beraten. Ergänzend und vertiefend im Sinne einer Analyse kann eine Beratung nach DIN SPEC 27076, ein sogenannter CyberRisikoCheck, empfohlen werden. Aufgesetzt vom BSI, wird diese Beratung von zertifizierten Beratenden privatwirtschaftlich angeboten.

In einem Leitfaden zur Cybersicherheit des irischen National Cyber Security Center ist ein Jahresplan zur Verbesserung der Cyberresilienz erarbeitet worden. Dieser kann interessierten Unternehmen ergänzend ausgehändigt werden zur Strukturierung des Prozesses im Anschluss an die Erstberatung im Rahmen des CSC für KMU (siehe Abbildung 7).

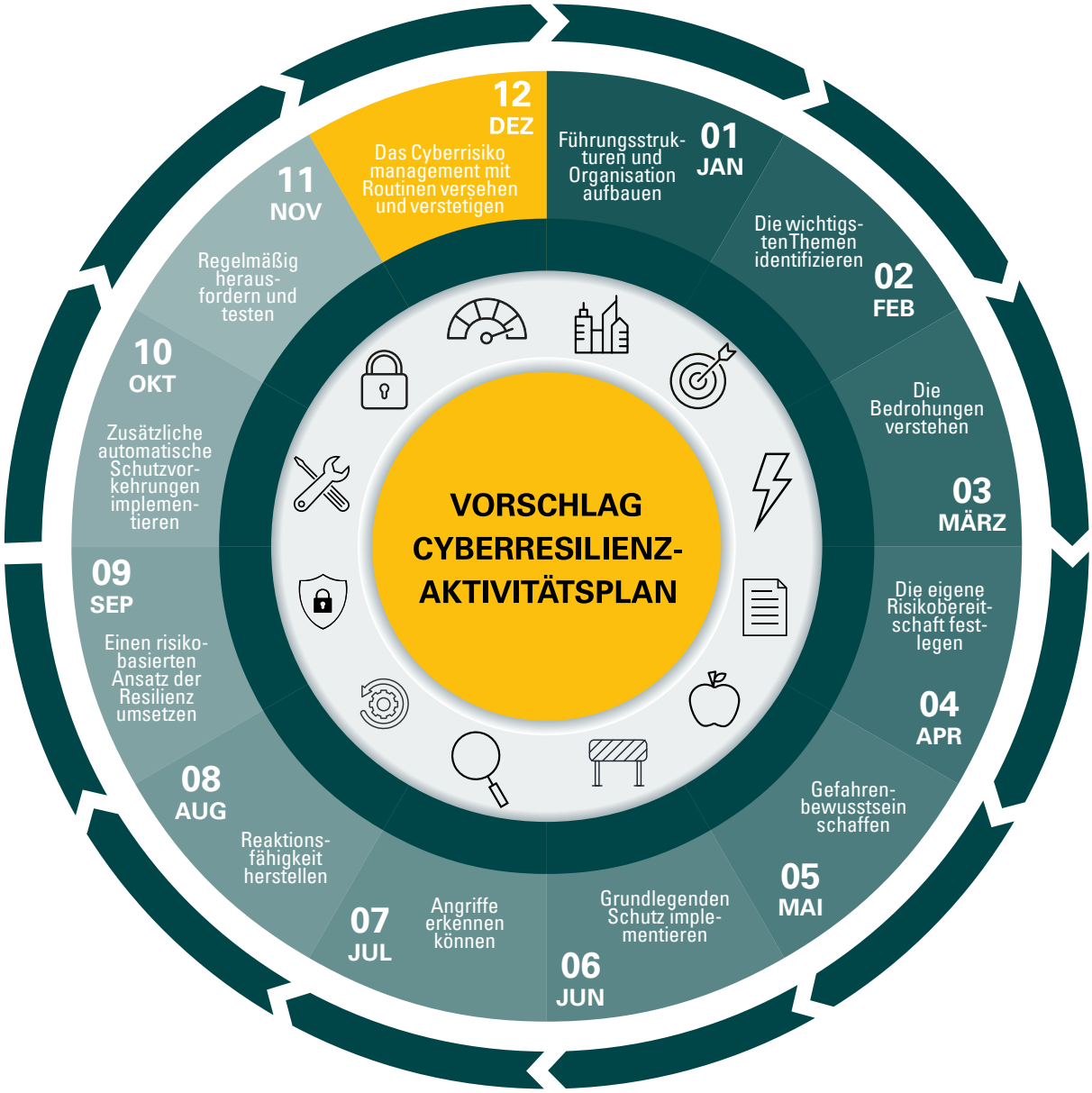


Abbildung 7: Vorschlag eines Cyberresilienz-Aktionsplans.
Quelle: National Cyber Security Center, 2018, übersetzt ins Deutsche.

4. Beratungsmaterialien

Die Beratungsmaterialien des CSC für KMU bestehen aus einer Mappe, in welcher eine Checkliste und 10 Beratungskarten liegen. Diese Materialien werden im Folgenden kurz dargestellt. Die Kerninhalte und die 8 Handlungsfelder der Cybersicherheit für KMU ziehen sich wie ein „roter Faden“ durch die Beratungsmaterialien: Checkliste bzw. Online-Tool mit Auswerteergebnis und Beratungskarten.

4.1 Checkliste

Die Checkliste umfasst 33 Fragen in 8 Abschnitten, mit denen ein grober Überblick über den Stand der Cybersicherheit im Unternehmen erhoben wird. Die Abschnitte sind nach den 8 Basismaßnahmen benannt und gegliedert. Den Einstieg bildet der Abschnitt „Sicherheitslücken schließen“ mit 5 Fragen, was zugleich auch der Titel von Basismaßnahme 1 ist.

Cyber
Sicherheits
Check
für KMU

CHECKLISTE

1 Sicherheitslücken schließen

	Ja	Nein	k. R.*
1.1 Haben Sie einen vollständigen Überblick über alle im Unternehmen eingesetzte Software?	☐	☐	☐
1.2 Existiert für das Einspielen von Softwareaktualisierungen (Updates und Patches) ein definierter Prozess?	☐	☐	☐
1.3 Wird dieser Prozess überwacht (z. B. manuell oder über automatische Benachrichtigungen, die Auskunft über Erfolg/Misserfolg der Maßnahme geben)?	☐	☐	☐

Abbildung 8: Checkliste.

Die Fragen können jeweils mit „Ja“, „Nein“ oder „k. R.“ (keine Relevanz) beantwortet werden. Die Antwort „k. R.“ ist vorgesehen für Situationen, in denen die Frage für das beratene Unternehmen nicht zutrifft. Das Beantworten von Fragen mit „k. R.“ führt dazu, dass diese aus der Auswertung ausgeschlossen werden.

Im Anschluss an die Beantwortung der 33 Fragen wird das Ergebnis errechnet. Zur Erstellung der Auswertung gibt es ein Offline-Tool und den Online-Check auf www.csc-kmu.de. Sowohl mit dem Excel-Tool als auch mit dem Online-Check kann eine grafische Auswertung erstellt werden, die einen schnellen Überblick über die Cybersicherheitssituation im Unternehmen gibt.

Die Checkliste und die Basismaßnahmen sind eng verzahnt. Einerseits sind die Abschnitte der Checkliste nach den einzelnen Basismaßnahmen gegliedert und identisch benannt. Andererseits tauchen auch die Themen der Fragen auf den Vorderseiten der Karten wieder auf.

Frage 1.2 in der Checkliste ist beispielsweise die zur Existenz eines definierten Update-Prozesses. Dieser taucht bei Basismaßnahme 1 wieder auf in Form der Aufforderung, einen Update-Prozess zu definieren und Verantwortliche dafür zu benennen. Für Unternehmen, bei denen alle Punkte und Aufforderungen auf den Vorderseiten der Karten erfüllt sind, können bei der Checkliste alle Fragen mit „Ja“ beantwortet werden.

Die Erhebung mittels der Checkliste dient dazu, insbesondere der Geschäftsleitung einen Überblick über den Stand der Cybersicherheit im Unternehmen zu verschaffen. Im Zuge der Erhebung und der Feststellung des Status quo der Cybersicherheit im Unternehmen wird klar, wo das Unternehmen gut aufgestellt ist und wo es noch Handlungsbedarf gibt.

Das Durchgehen und insbesondere die Auswertung der Checkliste ist ein sensibler Punkt in der Beratung. Leicht kann der Eindruck einer Prüfungssituation entstehen, in welchem Rechtfertigungsdruck aufseiten der Geschäftsleitung entsteht. Hiermit müssen die Beratenden einen guten und vertrauensvollen Umgang entwickeln. Das auszuhändigende Ergebnis des Checks soll der Geschäftsleitung einen Überblick über die Situation im eigenen Unternehmen geben, damit sie handlungsfähig wird in Bezug auf bessere Cybersicherheit. Für die Beratenden macht das Ergebnis keinen Unterschied und hat keine weitere Bedeutung. Es wird empfohlen, das möglichst auch so zu vermitteln. Zudem kann durch Aushändigung der Blanko-Checkliste die Möglichkeit gegeben werden, dass die beratene Person parallel die Antwortfelder mit ankreuzt.

Das Ergebnis des Checks ist zusätzlich auch eine Hilfestellung in der Kommunikation mit und Beauftragung von einem IT-Dienstleistungsunternehmen. In diesem Prozess bietet das Ergebnis des Checks eine Handreichung zur Klärung, welche Aufgaben das IT-Dienstleistungsunternehmen erfüllt und welche Punkte es lösen kann, damit keine Lücken bleiben.

4.2 Excel-Tool

Das Excel-Tool steht zur Auswertung der Checkliste bereit. Es stellt die „alte“ Offline-Lösung dar, insbesondere im Vergleich zum Online-Check, der im nächsten Kapitel erläutert wird. Auf der Website www.csc-kmu.de wird neben den Beratungsmaterialien (Checkliste, Beratungskarten, Mappe) auch das Excel-Tool in einer Excel-Datei zum Download angeboten. Dieses Excel-Tool kann von den Beratenden heruntergeladen und offline mit zu den Beratungsgesprächen genommen werden, wo es auf einem Endgerät im Rahmen der Beratung parallel zur Beantwortung der Checkliste ausgefüllt werden kann. Im Anschluss daran werden die Antwortfelder der 8 Sicherheitskategorien und damit der IT-Sicherheitsstatus als Netzdiagramm sowie Säulendiagramm nach dem Ampelprinzip rot-grün abgebildet und der beratenen Person ausgehändigt.

In dieser Excel-Datei, die ohne Makros auskommt, kann im ersten Tabellenblatt „Sicherheitscheckup“ zu allen 33 Fragen die jeweilige Antwort eingetragen werden.

In Tabellenblatt 2 „Ergebnis“ ist dann die grafische Darstellung des Ergebnisses zu finden (siehe Abbildung 9). Dieses lässt sich z. B. per PDF-Drucker in einem zweiseitigen PDF-Dokument ausgeben.

Auf der ersten Seite wird das Ergebnis aufgeteilt nach den 8 Abschnitten ausgegeben. Auf der zweiten Seite wird das Ergebnis in Form eines Netzdiagramms mit 8 Achsen dargestellt. Die Antwort „Ja“ wertet eine Frage als erfüllt, die Antwort „Nein“ als nicht erfüllt und „k. R.“ wertet eine Frage als nicht relevant und klammert sie aus der Bewertung aus. Sind alle nicht ausgeklammerten Fragen mit „Ja“ beantwortet, so wird auf jeder Achse 100 % Erfüllungsgrad erreicht. Damit ist „der Schutzschirm aufgespannt“ oder der „Fallschirm ohne Löcher“. Gibt es negativ beantwortete Fragen, so zeigt der Schutzschirm Lücken, die sich mit dem Beheben der entsprechenden Punkte schließen lassen.

Die von der beratenen Person parallel zur Erhebung ausgefüllte Checkliste bzw. die ausgefüllte Checkliste des Beratenden sowie das Auswertungsergebnis sollten als Orientierung für die weiteren Schritte im Unternehmen verbleiben.

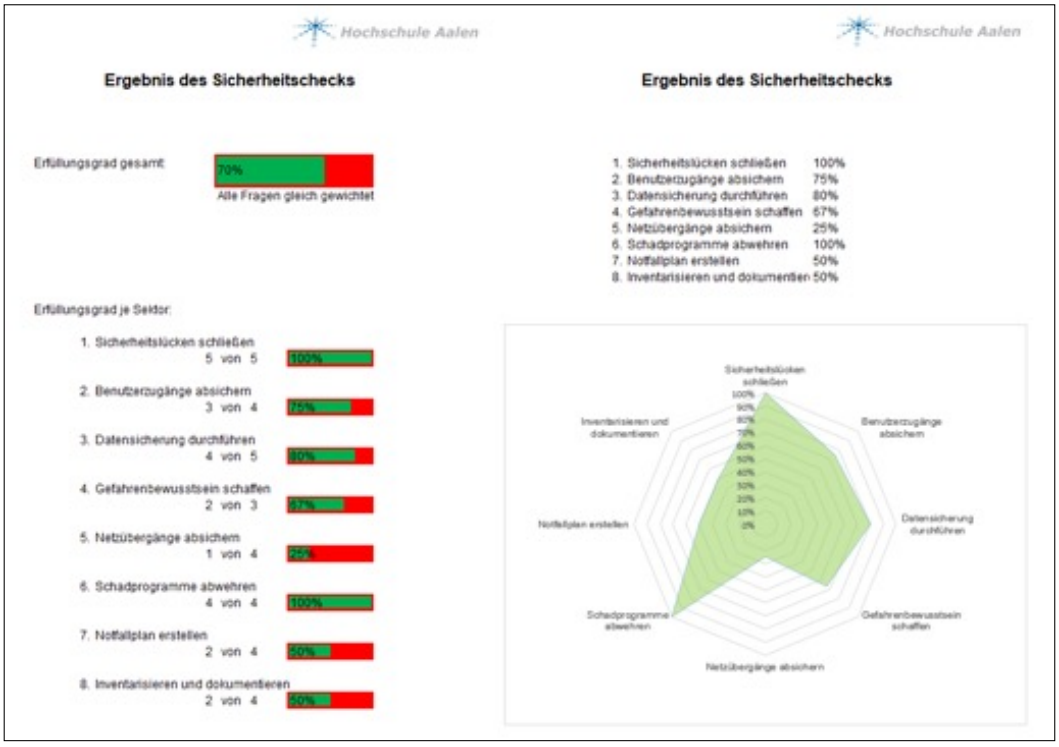


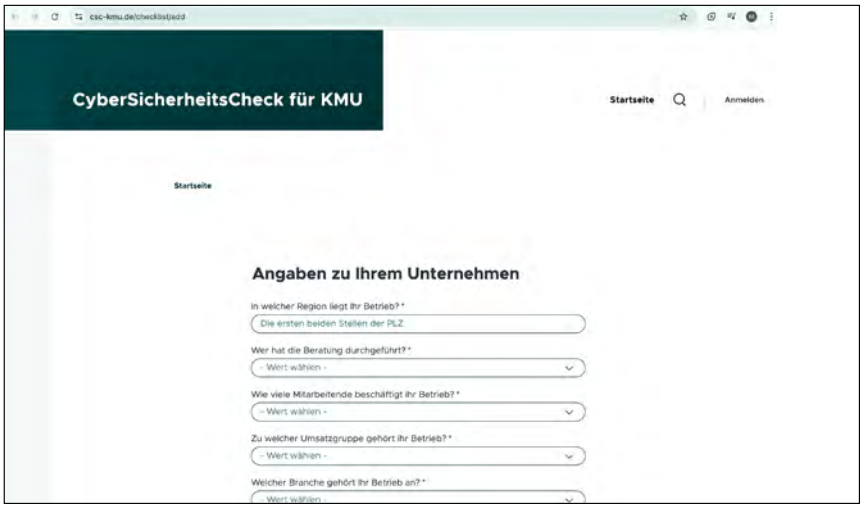
Abbildung 9: Beispielhafte Darstellung eines Ergebnisses des Sicherheitscheckups, das mittels „Excel-Tool“ gewonnen wurde.

4.3 Online-Check

Darüber hinaus wurde die Website www.csc-kmu.de um einen Online-Check erweitert, der das Ausfüllen der Checkliste online ermöglicht und im Anschluss in einem grafisch aufbereiteten Ergebnis die Auswertung der Checkliste ausgibt. Dies lässt sich als PDF herunterladen. Zusätzlich zu den Beratungskarten ist dieses Ergebnis zum Verbleib im Unternehmen gedacht. Es soll der Geschäftsführung einen Überblick über die Situation der Cybersicherheit im eigenen Unternehmen geben und auf offene Punkte und Handlungsbedarfe hinweisen.

Das darin abgebildete Netzdiagramm zeigt die Lücken auf: Wenn alle Fragen mit „Ja“ beantwortet wurden, so ist das Netzdiagramm vollständig gefüllt und damit der „Abwehrschirm umfassend aufgespannt“. Sind einzelne Fragen mit „Nein“ beantwortet, so zeigen sich Lücken in diesem Abwehrschirm. Hier besteht Handlungsbedarf für das Unternehmen.

Werden Fragen mit „k. R.“ (keine Relevanz) beantwortet, so fallen sie aus der Auswertung heraus. Im Extremfall kann dadurch ein Abschnitt mit 5 Fragen zu 100 % erfüllt sein, wenn 4 davon mit „k. R.“ und eine mit „Ja“ beantwortet wurde. In der Regel kommt diese Antwortoption aber insbesondere für Fälle in Betracht, in denen eine Situation abgefragt wird, die im befragten Unternehmen irrelevant, also nicht zutreffend ist.



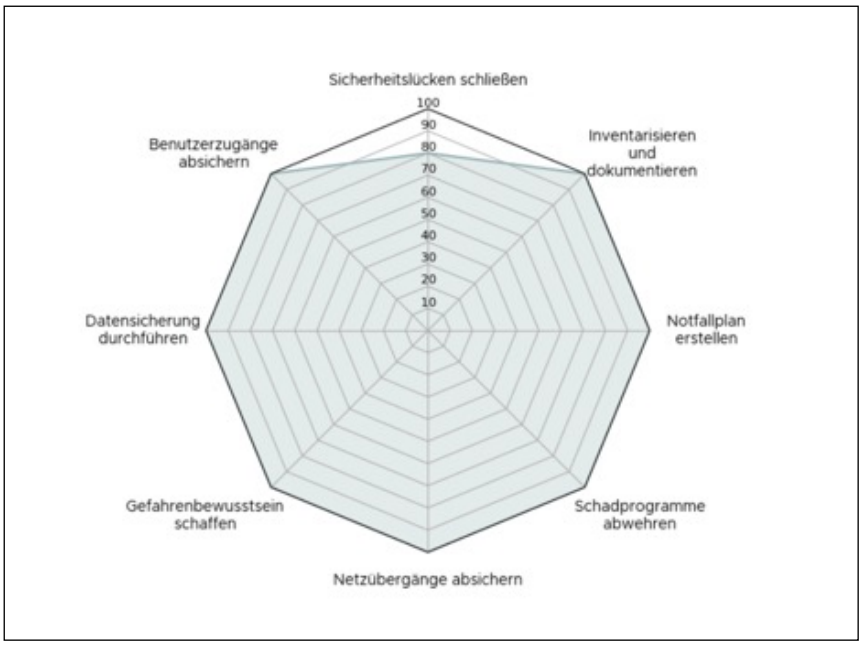


Abbildung 11: Beispiel eines Ergebnisses des Online-Checks.

Anders wäre es, wenn die befragte Person die Antwort nicht weiß. Zu diesen so beantworteten Fragen lässt sich dann auch keine Einschätzung der Cybersicherheitssituation abgeben.

Im Lichte des Risikomanagements betrachtet – und dies liegt dem CSC zugrunde – würde die Antwort bei Unkenntnis bezüglich einer Frage „Nein“ lauten. Die Aussagekraft eines Checks, bei welchem zahlreiche Fragen mit „k. R.“ beantwortet wurden, ist äußerst eingeschränkt.

Werden in einem Abschnitt alle Fragen mit „k. R.“ beantwortet, so taucht auf dem Ergebnis-PDF des Online-Checks ein Hinweis auf, dass in diesem Bereich keine Einschätzung möglich ist und hier der bestehende Handlungsbedarf geprüft werden muss. Kein Abschnitt ist für sich genommen so unwichtig, dass er aus der Betrachtung der Cybersicherheitssituation eines Unternehmens ausgeklammert werden kann.

Manche der Fragen bauen logisch aufeinander auf. Diese Abhängigkeiten sind im Online-Check wie folgt modelliert – diese Logik trifft ebenso für die Excel-Fassung zu, kann allerdings ohne Makros nicht im beschriebenen Sinne technisch abgebildet werden:

- Wenn Frage 1.2 „Haben Sie einen vollständigen Überblick über alle im Unternehmen eingesetzte Software?“ mit „Nein“ oder „k. R.“ beantwortet wird, so wird die anschließende Frage 1.3 „Existiert für das Einspielen von Softwareaktualisierungen (Updates und Patches) ein definierter Prozess?“ auf „k. R.“ gesetzt und für Änderungen gesperrt.

- Wenn Frage 3.1 „Verfügen Sie über eine Datensicherung (Backup) der geschäftskritischen Daten?“ mit „Nein“ oder „k. R.“ beantwortet wird, so sind rein logisch alle weiteren Fragen zum Backup irrelevant. 3.2, 3.3, 3.4 und 3.5 werden in diesem Moment auf „k. R.“ gesetzt und für Änderungen gesperrt.

- Wenn Frage 7.1 „Haben Sie einen Notfallplan für IT-sicherheitsrelevante Ereignisse?“ mit „Nein“ oder „k. R.“ beantwortet wird, so werden die Fragen 7.3 und 7.4, die sich beide auf den Notfallplan beziehen, auf „k. R.“ gesetzt und für Änderungen gesperrt.

- Wenn Frage 8.1 „Verfügen Sie über eine vollständige Übersicht Ihrer IT-Landschaft [...]?“ mit „Nein“ oder „k. R.“ beantwortet wird, so wird die Frage 8.3 „Beinhaltet die Übersicht auch alle relevanten IT-Anwendungen inklusive deren Abhängigkeiten?“ auf „k. R.“ gesetzt und für Änderungen gesperrt.

Abbildung 12: Manche Fragen hängen voneinander ab und werden entsprechend gesperrt, wenn sie aufgrund vorangegangener Antworten nicht relevant sind.

4.4 Beratungskarten

Im Anschluss an die Checkliste und ihre Auswertung (Excel-Tool/Online-Tool) kommen die Beratungskarten zum Einsatz. Davon gibt es 10 Stück, beginnend mit der Einstiegskarte, gefolgt von Basismaßnahme 1–8 und abgeschlossen durch die Zusatzkarte „Weitere Themen". Thematisch lassen sich die 8 Abschnitte der Checkliste in den Basismaßnahmen 1–8 wiederfinden. Werden im Unternehmen alle Punkte umgesetzt, die auf den Vorderseiten der 8 Basismaßnahmen aufgeführt sind, so lassen sich in der Checkliste alle Fragen mit „Ja", ggf. wenige mit „k. R." beantworten. Im Ergebnis wäre der „Abwehrschirm" im Netzdiagramm voll aufgespannt.

Folgende 10 Karten werden bereitgestellt:

Einstiegskarte: Die Einstiegskarte **„Cybersicherheit ist Führungsaufgabe"** steht am Anfang der Beratung. Sie setzt den Rahmen für die Beratung der Geschäftsleitung. Die Themen sind hier Verantwortung für Cybersicherheit, Gefahrenbewusstsein, Zuständigkeiten und IT-Sicherheitsrichtlinie.

Beratungskarte 1:
Sicherheitslücken schließen: Das Schließen von Sicherheitslücken ist eine der wichtigsten Maßnahmen für angemessene Cybersicherheit. Hier geht es vor allem um Softwareaktualisierungen in Form von Updates und Patches.

Beratungskarte 2:
Benutzerzugänge absichern: Ein klares Berechtigungsmanagement und gute Absicherung mittels starker Passwörter oder sogar Zwei-Faktor-Authentifizierung sind die Schwerpunkte dieser Karte.

Beratungskarte 3:
Datensicherungen durchführen: Diese Karte widmet sich ganz dem Thema Datensicherung: Umfang, Frequenz, Speicherorte und Anzahl der Kopien, Testroutinen sind die Bereiche, auf die es hier zu achten gilt.

Beratungskarte 4:
Gefahrenbewusstsein schaffen: Der Wissensstand und das sichere Verhalten der Mitarbeitenden ist ein bedeutender Faktor guter Cybersicherheit. Deshalb geht es in Basismaßnahme 4 darum, wie ein aktueller Informationsstand hergestellt werden kann, sowie um Sensibilisierung und Schulung.

Beratungskarte 5:
Netzübergänge absichern: Klare Netzwerkarchitektur sowie der Einsatz von Firewalls an den richtigen Stellen sind die Themen dieser Basismaßnahme.

Beratungskarte 6:
Schadprogramme abwehren: Hier geht es um den Einsatz von Virenschutzprogrammen, um die Absicherung von Kommunikationswegen und um die Gefahren, die z. B. von Makros ausgehen können.

Beratungskarte 7:
Notfallplan erstellen: Die Absicherung ist nur dann gut und vollständig, wenn sie auch auf den Ernstfall vorbereitet. In dieser Basismaßnahme geht es um die Erstellung eines Notfallplans, um die Festlegung der Verantwortlichkeiten im Ernstfall sowie ums Üben und Bereithalten des Notfallplans.

Beratungskarte 8:
Inventarisieren und dokumentieren: Eine vollständige Inventarisierung der eingesetzten IT-Systeme ist zugleich die Grundlage für viele der Cybersicherheitsmaßnahmen. In Basismaßnahme 8 geht es darum, was dabei beachtet werden muss.

Zusatzkarte:
Weitere Themen: Auf dieser Zusatzkarte sind alle weiteren Themen versammelt, die sich keiner der Basismaßnahmen direkt zuordnen ließen, die aber dennoch wichtig sind oder, je nach Unternehmen, wichtig sein können. Hier werden die Themen Homeoffice und mobiles Arbeiten, physische Sicherheit, Cloud-basierte Lösungen sowie Cyberversicherungen behandelt.

4.5 Aufbau der Karten zu den 8 Basismaßnahmen („roter Faden“)

Die Basismaßnahmen sind nach dem folgenden Schema aufgebaut: Der Titel der Karten bestimmt das Thema. Auf den Vorderseiten sind jeweils Maßnahmen mit Teilaufgaben dargestellt. Sie sind als Handlungsempfehlung formuliert, z. B. „Aktualisieren Sie alle Anwendungen regelmäßig“. Die Punkte der Vorderseiten haben den Anspruch, vollständig die Frage nach dem **„Was“** zu beantworten: Das Schließen von Sicherheitslücken (Basismaßnahme 1) umfasst alle Maßnahmen, die auf der Vorderseite genannt sind.

Auf den Rückseiten befinden sich Fallbeispiele, weitere Informationen z. T. inkl. Links zu digital erreichbaren Quellen mit weiterführenden Informationen. Hier werden erste Hinweise zur Frage nach dem **„Wie“** gegeben. Diese Zusammenstellung erhebt im Gegensatz zur Vorderseite keinen Anspruch auf Vollständigkeit. Vielmehr wurden hier nützliche Hinweise und weiterführende Informationen zusammengetragen, die in einzelnen Punkten weiterhelfen können. Für umzusetzende Maßnahmen, die damit nicht erläutert werden, ist in aller Regel der Einbezug eines IT-Dienstleistungsunternehmens ratsam. Insbesondere kleine Unternehmen dürften in Bezug auf Kompetenz und Zeit bei einigen der aufgeführten Maßnahmen an ihre Grenzen stoßen. Gelingt es, dass durch die Beratung in Zukunft im Bereich IT für alle umfangreicheren oder komplexeren Themen auf ein externes Dienstleistungsunternehmen zurückgegriffen wird, ist für die Sicherheit im Unternehmen zumindest potenziell ebenfalls viel erreicht!

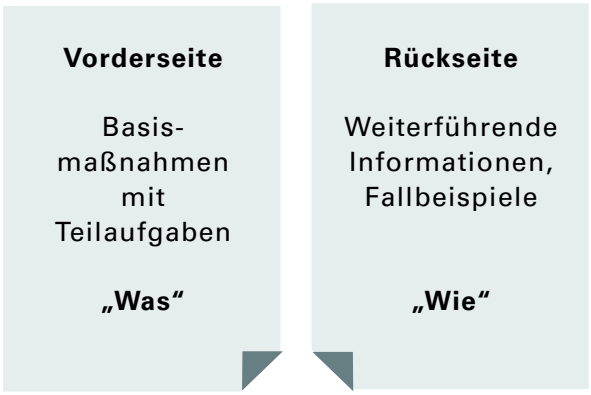


Abbildung 13: Aufbau der Karten.

Die Reihenfolge, in welcher im Folgenden auf die Inhalte der Beratungskarten eingegangen wird, entspricht der Reihenfolge, in welcher die Beratungskarten in der Mappe liegen. Es beginnt mit der Einstiegskarte: Cybersicherheit ist Führungsaufgabe, gefolgt von der Checkliste und daran anschließend die Karten zu den Basismaßnahmen 1–8. Den Abschluss bildet die Zusatzkarte: Weitere Themen. Dies stellt zugleich die Reihenfolge dar, in welcher die Materialien im Laufe des Beratungsgesprächs zum Einsatz kommen.

5. Einstiegskarte

Cybersicherheit ist Führungsaufgabe

5.1 Begründung

Cybersicherheit ist Führungsaufgabe. Nur die Geschäftsleitung kennt die Prozesse im Unternehmen und hat den Überblick, entscheidet über Ressourcen wie Personal, Finanzmittel. Leider scheitern häufig gute und sinnvolle Empfehlungen an der „Kasse“. Dabei gilt zweifelsfrei: Sicherheit kostet Geld. Allerdings kostet die Bewältigung einer Sicherheitskrise noch viel mehr Geld. Die Führung des Unternehmens setzt zudem wichtige Impulse zur Förderung einer Sicherheits- und Vertrauenskultur im Unternehmen. Beide Aspekte können Cyberresilienz nachhaltig unterstützen. Nur die Leitungsebene kann die potenziellen Auswirkungen von Cyberangriffen auf das gesamte Unternehmen abschätzen und die gebotenen Maßnahmen zur Absicherung in die Wege leiten. Keine untergeordnete Stelle in der IT kann für angemessene Cybersicherheit sorgen ohne den Auftrag und die Rückendeckung der Geschäftsleitung. Diese muss die Tragweite der Thematik verstehen, über das angestrebte Niveau der Absicherung entscheiden, dafür ausreichend Ressourcen bereitstellen und dafür sorgen, dass diese Querschnittsaufgabe in die unterschiedlichen Bereiche einfließt und dort zuverlässig erledigt wird.

Cybersicherheit lässt sich nicht ausschließlich durch technische Maßnahmen erreichen. Die

Abbildung 14: Die drei Säulen der Cybersicherheit. Quelle: ENISA, 2021a, S. 28.

Europäische Cybersicherheitsagentur (ENISA) unterscheidet die drei Säulen Mensch – Prozess – Technik, siehe Abbildung 14. Mit anderen Worten: Ein ganzheitlicher Ansatz erfordert die Berücksichtigung von den drei Aspekten Verhalten – Organisation – Technik. Aus sorgfältig gestalteten Prozessen leiten sich technische Maßnahmen genauso ab wie personelle. Gut geschulte Mitarbeitende, ausreichend personelle Ressourcen für den Bereich Cybersicherheit und IT-Infrastruktur sowie die passenden Qualifikationen sind entscheidend.

Die Geschäftsleitung trägt die Verantwortung für den wirtschaftlichen Erfolg ihres Unternehmens. Da Cyberangriffe diesen bedrohen können, liegt auch die Verantwortung für Cybersicherheit bei der Geschäftsleitung.

5.2 Maßnahmen

Abschnitt 1: Verantwortung

Maßnahme: Stellen Sie sich als Unternehmensleitung Ihrer Verantwortung, Cybersicherheit umzusetzen und ihr entsprechende Relevanz einzuräumen.

Begründung: Die Verantwortung für Cybersicherheit liegt bei der Geschäftsleitung. Teilweise wird sie als technische Angelegenheit an untergeordnete Stellen delegiert, denen dann aber die Weisungsbefugnis fehlt, die umfassenden Prozesse strukturiert durchzusetzen. Angemessene Cybersicherheit kann nur hergestellt

werden, wenn die Geschäftsleitung ihr Priorität einräumt und Ressourcen zuweist. Aus diesem Grund richtet sich die Beratung des CSC für KMU auch an die Geschäftsleitungen kleiner und kleinster KMU. Die Leitungsebene ist zudem für den sicherheitsbewussten Umgang mit personenbezogenen, teilweise sehr sensiblen Daten von Kunden verantwortlich sowie für das Handlungsfeld Compliance.

Entscheiden Sie, welches Sicherheitsniveau Sie anstreben und welche Restrisiken gegebenenfalls akzeptabel sind.

Perfekte Sicherheit gibt es nicht. Das herzustellende Absicherungsniveau ist immer ein Kompromiss zwischen Aufwand und Nutzen. Die Konsequenzen, die sich aus dem definierten Sicherheitsniveau ergeben, müssen bekannt sein und akzeptabel: Bei geringer Absicherung drohen möglicherweise schwere, nicht akzeptable Konsequenzen. Die Geschäftsleitung muss die entsprechenden Entscheidungen treffen, da es im Zweifel um den Fortbestand des Unternehmens geht, für welches sie die Verantwortung trägt oder welches ihr gar gehört. Diese Verantwortung lässt sich nicht delegieren.

Stellen Sie ausreichend finanzielle und personelle Ressourcen für die IT-Sicherheit zur Verfügung.

IT-Sicherheit gibt es nicht umsonst. Für gute Absicherung fallen hauptsächlich Personalkosten und Ausgaben für Technik und Dienstleistungen an. Das geht von Schulungs- und Sensibilisierungsmaßnahmen über das Einbinden eines IT-Dienstleisters bis hin zu Hardware wie Firewalls oder einer redundanten Serverstruktur. Gute IT-Sicherheit lässt sich nur erreichen, wenn dafür ausreichend finanzielle und personelle Ressourcen bereitgestellt werden. Dabei braucht es in der Regel nicht die weltbesten Techniken, sondern mit ausreichend personellen Kompetenzen, ggf. auch von extern, sauberen und klaren Prozessen, geordneten Strukturen und aktueller Software ist meist schon viel erreicht.

Seien Sie als Unternehmensleitung ein Vorbild bei der Einhaltung von Sicherheitsregeln.

Der Geschäftsleitung kommt bei der Umsetzung und Anwendung der Sicherheitsregeln eine wichtige Vorbildfunktion zu. Mit gutem Beispiel voranzugehen kann eine wichtige Säule in der Motivation und Sensibilisierung der Mitarbeitenden für angemessene Cybersicherheit sein.

Abschnitt 2: Gefahrenbewusstsein

Seien Sie sich der Gefahr bewusst, dass die Unternehmensleitung ein bevorzugtes Angriffsziel von Cyberkriminellen darstellt.

Die Geschäftsleitung ist ein bedeutendes Angriffsziel. Sie steht in der Öffentlichkeit und ist für Angreifende leicht zu identifizieren. Für sogenannte CEO-Fraud-Angriffe beispielsweise erkunden Angreifende so lange die interne Organisationsstruktur, Aufgabenverteilung, E-Mail-Design und Reisekalender, bis sie in der Lage sind, z. B. der Buchhaltung mittels einer gefälschten Mail vermeintlich von der Geschäftsleitung eine Zahlungsanweisung zukommen zu lassen. Sobald dieses Geld entsprechend überwiesen ist, ist es in der Regel nicht mehr wiederzubekommen.

Sensibilisieren Sie Ihre Führungskräfte für das Thema Cybersicherheit. Setzen Sie es z. B. regelmäßig auf die Tagesordnung von Besprechungen.

Die Führungskräfte müssen ebenfalls über ein entsprechendes Gefahrenbewusstsein verfügen. Es empfiehlt sich, dass das Thema Cybersicherheit bei Besprechungen regelmäßig auf der Tagesordnung steht.

Stellen Sie sicher, dass Ihre Beschäftigten regelmäßig sensibilisiert werden, z. B. durch Schulungen und Newsletter.

Die Beschäftigten müssen in Themen der Cybersicherheit geschult und regelmäßig sensibilisiert werden. Zudem muss die Geschäftsleitung sicherstellen, dass die Handlungsanweisungen zum Thema Cybersicherheit bekannt sind, verstanden wurden und eingehalten werden. Auch bei externen Personen mit Zugang zu den IT-Systemen des Unternehmens muss der Kompetenz- und Schulungsstand sichergestellt werden.

Abschnitt 3: Zuständigkeiten

Legen Sie eindeutig fest, welche Person oder Stelle im Unternehmen für den Bereich der IT-Sicherheit zuständig ist.

Die Geschäftsleitung legt die Zuständigkeiten klar fest, beispielsweise in der IT-Sicherheitsrichtlinie. Die folgenden beiden Zuständigkeiten müssen klar geregelt sein:

- Betrieb des IT-Systems
- IT-Sicherheit

Die entsprechenden Stellen müssen über die passenden Kompetenzen verfügen oder durch Fortbildungen und Schulungen damit ausgestattet werden. Ebenso müssen sie über ausreichend Ressourcen zur Wahrnehmung ihrer Aufgaben verfügen.

Falls Sie mit einem IT-Dienstleister zusammenarbeiten, legen Sie die von ihm übernommenen Aufgaben explizit in einem Dienstleistungsvertrag fest.

Ein IT-Dienstleistungsunternehmen kann bei der Umsetzung von Cybersicherheitsmaßnahmen hilfreich sein. Mit der Beauftragung eines solchen Unternehmens kann Expertise eingekauft werden, die möglicherweise im Unternehmen nicht bereitsteht. Es wird empfohlen, im Dienstleistungsvertrag alle Details klar zu regeln, auch aus Regress- und Haftungsgründen. Insbesondere muss darauf geachtet werden, dass auch die Cybersicherheit und die Aktualisierung aller im Unternehmen verwendeten IT-Systeme eingeschlossen ist. Auch die Reaktionszeit bei Vorfällen sollte bekannt, im Vorfeld abgesprochen und ggf. im Vertrag enthalten sein.

Abschnitt 4: IT-Sicherheitsrichtlinie

Entwickeln Sie für Ihr Unternehmen eine IT-Sicherheitsrichtlinie, in der klare Verhaltensregeln, Anforderungen und Zuständigkeiten festgelegt sind.

In einer IT-Sicherheitsrichtlinie werden die Verhaltensregeln festgelegt, die im Umgang mit IT-Systemen und Daten im Unternehmen gelten. Es wird empfohlen, diese Vorgaben klar zu formulieren. Mit der DIHK-Nutzungsrichtlinie IT-Sicherheit liegt ein Beispiel für eine solche IT-Sicherheitsrichtlinie vor. Quelle: DIHK, 2024, erreichbar unter: https://sl.csc-kmu.de/ek-01.html
Die Erstellung einer solchen IT-Sicherheitsrichtlinie bietet der Geschäftsleitung auch einen Anlass, sich mit dem Thema der Cybersicherheit auseinanderzusetzen. Zugleich bietet die Umsetzung, Durchsetzung und Aktualisierung dieser Richtlinie ein gutes Werkzeug, um die Cybersicherheit sukzessive auszubauen und an dem Thema dranzubleiben.

Halten Sie Ihre IT-Sicherheitsrichtlinie stets aktuell.

Die IT-Sicherheitsrichtlinie ist stets aktuell zu halten. Sobald sich Änderungen an der IT-Infrastruktur ergeben, kann auch eine Anpassung der IT-Sicherheitsrichtlinie notwendig werden.

Kommunizieren Sie die Vorgaben bezüglich Cybersicherheit regelmäßig an Ihre Mitarbeitenden und prüfen Sie deren Einhaltung.

Die IT-Sicherheitsrichtlinie kann erst dann ihre Wirkung entfalten, wenn sie bekannt ist und verbindlich eingehalten werden muss.

Regeln Sie den Zugriff auf IT-Systeme und Dokumente, indem Sie für Ihr Unternehmen ein rollenbasiertes Berechtigungskonzept erstellen.

Und ...

Weisen Sie jeder Rolle nur die Zugriffsberechtigung zu, die sie zur Erfüllung ihrer Aufgaben benötigt (Prinzip der minimalen Rechte).

Um den Zugriff auf IT-Systeme und Dokumente klar zu regeln, empfiehlt sich die Erstellung eines rollenbasierten Berechtigungskonzepts. Darin werden Rollen definiert, denen nur die jeweils notwendigen Zugriffsberechtigungen zugewiesen werden. Dieses „Prinzip der minimalen Rechte“ sorgt dafür, dass alle im Unternehmen nur auf die Systeme und Dokumente Zugriff haben, die für die Ausführung ihrer jeweiligen Rollen notwendig sind. Das kann die Auswirkungen reduzieren, die z. B. durch das sehr häufige Phishing verursacht werden (der Versuch, Zugangsdaten abzugreifen). Ebenso wichtig wie die Erteilung von Berechtigungen an Mitarbeitende bei Übernahme neuer Rollen (z. B. nach einer Einstellung) ist auch der Entzug von Zugriffsberechtigungen und das Sperren von Accounts bei Abgabe der jeweiligen Rollen (z. B. nach einem Weggang/Kündigung). Die Zugriffsrechte sind stets aktuell zu halten.

6. Checkliste

In diesem Kapitel werden die einzelnen Fragen der Checkliste dargestellt und mit zusätzlichen Informationen ergänzt. Die Checkliste enthält 8 Abschnitte mit jeweils 3–5 Fragen, zu jeder der 8 Basismaßnahmen einen. Da die Themen der Checkliste in den Basismaßnahmen wieder auftauchen, sind viele weitere relevante Informationen zu den einzelnen Themen auch in den weiteren Kapiteln dieses Handbuchs zu finden. Wo das der Fall ist, wird entsprechend darauf verwiesen.

Abschnitt 1: Sicherheitslücken schließen

1.1 Haben Sie einen vollständigen Überblick über alle im Unternehmen eingesetzte Software?

Siehe Basismaßnahme 1: Sicherheitslücken schließen.
Zudem: Wenn die Aufgabe der Softwareaktualisierung an ein IT-Dienstleistungsunternehmen übertragen wurde, so ist diese Frage in der Checkliste ebenfalls mit „Ja“ zu beantworten. Für die Beantwortung der Checklistenfragen muss nicht unterschieden werden, wer die Verantwortung für die einzelnen Bereiche trägt. Die beratene Geschäftsführung sollte im Sinne des ganzen Unternehmens antworten. Es spielt keine Rolle, wer die Aufgabe des Schließens von Sicherheitslücken übernimmt. Wichtig ist nur, dass sie zuverlässig erledigt wird. Die Gesamtverantwortung für Cybersicherheit liegt in jedem Fall bei der Geschäftsführung.

1.2 Existiert für das Einspielen von Softwareaktualisierungen (Updates und Patches) ein definierter Prozess?

Siehe Basismaßnahme 1: Sicherheitslücken schließen, insbesondere die Erläuterung zur ersten Maßnahme „Legen Sie einen Update-Prozess fest und benennen Sie einen Verantwortlichen“.

1.3 Wird dieser Prozess überwacht (z. B. manuell oder über automatische Benachrichtigungen, die Auskunft über Erfolg/Misserfolg der Maßnahme geben)?

Siehe Basismaßnahme 1: Sicherheitslücken schließen.

1.4 Ist sichergestellt, dass Softwareaktualisierungen schnellstmöglich nach der Veröffentlichung eingespielt werden?

Siehe Basismaßnahme 1: Sicherheitslücken schließen, insbesondere die Erläuterung zur fünften Maßnahme „Aktualisieren Sie Betriebssysteme und Anwendungssoftware, sobald Sicherheitsupdates vom Hersteller zur Verfügung stehen“.

1.5 Sind Quellen definiert, von denen Sie regelmäßig über neue Sicherheitslücken für die eingesetzten IT-Systeme und Anwendungen informiert werden?

Siehe Basismaßnahme 4: Gefahrenbewusstsein schaffen, insbesondere die Erläuterungen zur ersten Maßnahme „Definieren Sie die Quellen, aus denen man sich regelmäßig über neue Sicherheitslücken informiert“.

Abschnitt 2: Benutzerzugänge absichern

2.1 Erstellen Sie Passwörter gemäß gängigen Empfehlungen, z. B. des BSI, und haben Sie Vorgaben an Ihre Mitarbeitenden kommuniziert, z. B. mittels einer Passwortrichtlinie?

Siehe Basismaßnahme 2: Benutzerzugänge absichern, insbesondere die Erläuterungen im Abschnitt 2 „Passwortsicherheit“.
Zudem: Für Kleinstunternehmen wie z. B. Soloselbstständige genügt es, wenn die entsprechende Person die Kriterien für sichere Passwörter kennt und berücksichtigt. Sobald das Thema auch Mitarbeitende betrifft, empfiehlt sich die Erstellung einer Passwortrichtlinie, mittels der die entsprechenden Vorgaben verbindlich und transparent an die Mitarbeitenden kommuniziert werden können. Gegebenenfalls können auch Empfehlungen des BSI direkt genutzt werden.

2.2 Werden besonders kritische Konten/Zugänge (z. B. solche mit weitreichenden Berechtigungen, Fernzugänge u. a.) zusätzlich mit einer Zwei-Faktor-Authentifizierung (2FA) abgesichert?

Siehe Basismaßnahme 2: Benutzerzugänge absichern, insbesondere die Erläuterungen im Abschnitt 3 „Zwei-Faktor-Authentifizierung“.

2.3 Sind die Mitarbeitenden sensibilisiert, Passwörter geheim zu halten?

Siehe Basismaßnahme 2: Benutzerzugänge absichern, insbesondere die Erläuterungen zur sechsten Maßnahme „Stellen Sie sicher, dass alle Passwörter geheimgehalten werden."

2.4 Existiert eine Zugangssicherung (Passwort, 2FA) für mobile Endgeräte, die auf das Firmennetzwerk zugreifen können?

Siehe Basismaßnahme 2: Benutzerzugänge absichern und Zusatzkarte: Weitere Themen, Abschnitt 1 „Homeoffice und mobiles Arbeiten".

Abschnitt 3: Datensicherung durchführen

3.1 Verfügen Sie über eine Datensicherung (Backup) der geschäftskritischen Daten?

Siehe Basismaßnahme 3: Datensicherungen durchführen.

3.2 Werden Ihre Backups auf mehreren unterschiedlichen Speichermedien gesichert?

Siehe Basismaßnahme 3: Datensicherungen durchführen, insbesondere die Erläuterungen zur dritten Maßnahme „Beachten Sie die 3-2-1-Regel".

3.3 Ist mindestens ein Backup physisch vom Netzwerk getrennt, z. B. über Tapes oder Festplatten, die isoliert gelagert werden, oder durch Sicherung in einem externen Rechenzentrum oder einer Cloud?

Siehe Basismaßnahme 3: Datensicherungen durchführen, insbesondere die Erläuterungen zur dritten Maßnahme „Beachten Sie die 3-2-1-Regel".

3.4 Werden die Funktionsfähigkeit des Backups bzw. der Wiederherstellungsprozess regelmäßig überprüft und geübt?

Siehe Basismaßnahme 3: Datensicherungen durchführen, insbesondere die Erläuterungen zur fünften Maßnahme „Testen und dokumentieren Sie regelmäßig die Wiederherstellung der Daten".

3.5 Ist der Turnus des Backups an die Verarbeitung von geschäftskritischen Daten angepasst (zeitlicher Abstand bzw. Häufigkeit und Umfang der Sicherung)?

Siehe Basismaßnahme 3: Datensicherungen durchführen, insbesondere die Erläuterungen zur zweiten Maßnahme „Orientieren Sie sich beim Turnus des Backups an der Frequenz der anfallenden geschäftskritischen Daten".

Abschnitt 4: Gefahrenbewusstsein schaffen

4.1 Ist sichergestellt, dass Sie zeitnah über die aktuellen Gefahren und gängigen Arten von Cyberangriffen informiert werden?

Siehe Basismaßnahme 4: Gefahrenbewusstsein schaffen, insbesondere die Erläuterungen in Abschnitt 1 „Aktuellen Informationsstand sicherstellen".

4.2 Sind Ihnen und Ihren Mitarbeitenden die aktuellen und gängigen Vorgehensweisen von Cyberkriminellen bekannt?

Siehe Basismaßnahme 4: Gefahrenbewusstsein schaffen.

4.3 Finden regelmäßig Sensibilisierungen zum Thema Cybersicherheit statt, z. B. durch Schulung der Mitarbeitenden?

Siehe Basismaßnahme 4: Gefahrenbewusstsein schaffen, insbesondere die Erläuterungen in Abschnitt 2 „Sensibilisierung und Schulung".

Abschnitt 5: Netzübergänge absichern

5.1 Verfügen Sie an den Übergängen ins Internet über eine dedizierte Firewall und ist diese so konfiguriert, dass nur bestimmte und erwünschte Verbindungen aufgebaut werden können?

Siehe Basismaßnahme 5: Netzübergänge absichern.

Siehe auch 11.3 Exkurs: Rechnernetze.

5.2 Sind besonders kritische IT-Systeme vom restlichen Netz getrennt (wichtig vor allem für Backup oder Produktionsnetze mit veralteten Systemen)?

Siehe Basismaßnahme 5: Netzübergänge absichern.

5.3 Erfolgen Zugriffe von außen auf Ihr System ausschließlich über gesicherte Zugänge, z. B. VPN?

Siehe Basismaßnahme 5: Netzübergänge absichern, insbesondere die Erläuterungen zur letzten Maßnahme „Lassen Sie Zugriffe von außen auf Ihr Firmennetz nur über ein VPN zu".

5.4 Gibt es eine Übersicht aller Zugänge von extern auf Ihr Unternehmensnetzwerk inklusive deren Berechtigungen?

Siehe Basismaßnahme 5: Netzübergänge absichern, insbesondere die Erläuterungen zur sechsten Maßnahme „Identifizieren und dokumentieren Sie alle Netzübergänge".
Siehe auch Basismaßnahme 8: Inventarisieren und dokumentieren.

Abschnitt 6: Schadprogramme abwehren

6.1 Haben Sie die Ausführung von Makros in Ihren Office-Anwendungen technisch deaktiviert?

Siehe Basismaßnahme 6: Schadprogramme abwehren, insbesondere die Erläuterungen im Abschnitt 3 „Makros deaktivieren".

6.2 Sind Ihr E-Mail-Programm und der Server so konfiguriert, dass E-Mails von externen E-Mail-Konten explizit gekennzeichnet werden?

Siehe Basismaßnahme 6: Schadprogramme abwehren, insbesondere die Erläuterungen im Abschnitt 2 „Kommunikationswege absichern".

6.3 Ist Ihr E-Mail-Programm so konfiguriert, dass die tatsächliche E-Mail-Adresse als Absender angezeigt wird (wichtig: vollständige Anzeige aller Absenderinfos)?

Siehe Basismaßnahme 6: Schadprogramme abwehren, insbesondere die Erläuterungen im Abschnitt 2„Kommunikationswege absichern".
Siehe auch 12.3 Exkurs: Kommunikationskanäle absichern.

6.4 Nutzen Sie auf Ihren Endgeräten und Servern eine Antivirenlösung, die regelmäßig aktualisiert wird?

Siehe Basismaßnahme 6: Schadprogramme abwehren, insbesondere die Erläuterungen im Abschnitt 1 „Virenschutzprogramme verwenden".

Abschnitt 7: Notfallplan erstellen

7.1 Haben Sie einen Notfallplan für IT-sicherheitsrelevante Ereignisse?

Siehe Basismaßnahme 7: Notfallplan erstellen, insbesondere die Erläuterungen im Abschnitt 2 „Notfallplan erstellen".

7.2 Wird eine Notfallübung regelmäßig durchgeführt?

Siehe Basismaßnahme 7: Notfallplan erstellen, insbesondere die Erläuterungen im Abschnitt 3 „Üben und bereithalten".

7.3 Enthält der Notfallplan einen Kommunikationsplan mit internen und externen Erreichbarkeiten (z. B. IT-Dienstleister, Polizei, Lieferanten, Kunden, LfDI, CSBW, auch Mobilnummern)?

LfDI steht für Landesbeauftragter für Datenschutz und Informationsfreiheit.
Siehe Basismaßnahme 7: Notfallplan erstellen, insbesondere die Erläuterungen im Abschnitt 2 „Notfallplan erstellen".

7.4 Gibt es eine klar definierte Aufgabenzuweisung der wichtigsten Rollen in diesem Notfallplan?

Siehe Basismaßnahme 7: Notfallplan erstellen, insbesondere die Erläuterungen im Abschnitt 1 „Verantwortlichkeiten festlegen".

Abschnitt 8: Inventarisieren und dokumentieren

8.1 Verfügen Sie über eine vollständig dokumentierte Übersicht Ihrer IT-Landschaft, z. B. IT-Systeme, Verbindungen zwischen Systemen, Außenverbindungen?

Siehe Basismaßnahme 8: Inventarisieren und dokumentieren.

Zudem: Nur wer einen Überblick über sein Netzwerk, seine Systeme und die Verbindungen hat, kann offene Schwachstellen schließen, kritische Lücken finden, fehlende Schutzsysteme nachrüsten etc. Das gilt auch für kleinste Unterneh-

men. Wenn das Firmennetzwerk sehr klein ist und beispielsweise nur aus einem Computer und einem Router besteht, dann ist die Aufgabe der Dokumentation und Inventarisierung allerdings auch schnell erledigt.

Im Ernstfall hilft eine solche Übersicht dabei, Schutzmaßnahmen einzuleiten und den Wiederaufbau zu beschleunigen.

8.2 Ist dokumentiert, welche Zugänge zu den Systemen bestehen (intern & extern)?

Siehe Basismaßnahme 8: Inventarisieren und dokumentieren.

8.3 Beinhaltet die Übersicht auch alle relevanten IT-Anwendungen inklusive deren Abhängigkeiten?

Siehe Basismaßnahme 8: Inventarisieren und dokumentieren.

8.4 Werden diese Daten regelmäßig aktualisiert?

Siehe Basismaßnahme 8: Inventarisieren und dokumentieren, insbesondere die Erläuterungen zur dritten Maßnahme „Halten Sie die oben genannten Dokumentationen und den Netzwerkplan stets auf dem aktuellen Stand und als physische Kopie (Ausdruck) vor“.

7. Basismaßnahme 1:
Sicherheitslücken schließen

7.1 Begründung

Das Schließen von Sicherheitslücken ist eine der wichtigsten Maßnahmen guter Cybersicherheit. Software ist immer fehleranfällig. Sicherheitslücken, die entdeckt und bekannt gemacht werden, werden durch die Softwarehersteller in der Regel zeitnah durch Updates geschlossen. Sicherheitslücken, die über längere Zeit nicht geschlossen werden, können leicht durch automatisierte Massenangriffe ausgenutzt und ihre Träger somit zum Opfer von Cyberangriffen werden. Software, die stets aktuell gehalten wird, ist eine wichtige Säule guter Cybersicherheit.

7.2 Maßnahmen

Legen Sie einen Update-Prozess fest und benennen Sie einen Verantwortlichen.

Das Aktualisieren der Programme und Systeme ist eine fortlaufende Aufgabe, die eine feste Zuständigkeit braucht. Diese Person muss die nötigen fachlichen Kenntnisse haben oder per Schulung und Trainings bekommen. Ebenso muss sie mit den notwendigen Rechten ausgestattet werden. Sollte diese Aufgabe einem Dienstleistungsunternehmen zukommen, so muss sie in den Dienstleistungsvertrag aufgenommen und dort klar geregelt werden. Das ist wichtig, um Missverständnissen vorzubeugen. Aber auch aus Haftungsgründen ist dies unerlässlich.

Aktualisieren Sie alle Anwendungen regelmäßig.

Je nach Software werden in unterschiedlichen Abständen Updates bereitgestellt. Besonders kritische Komponenten wie z. B. der Browser, die Virendatenbank des Virenschutzprogramms oder das Betriebssystem bekommen täglich bis wöchentlich Aktualisierungen. Es wird empfohlen, für alle Software sicherzustellen, dass in regelmäßigen Abständen nach der Verfügbarkeit von Updates geschaut und diese eingespielt werden. Eine wichtige Grundlage für den Update-Prozess ist, dass Informationen über aktuelle Sicherheitslücken vorliegen. Hierfür gibt es verschiedene Quellen. Es muss sichergestellt werden, dass diese relevanten Informationen an der richtigen Stelle zur Verfügung stehen. In Basismaßnahme 4 wird näher auf dieses Thema eingegangen.

Aktivieren Sie möglichst die automatischen Aktualisierungsfunktionen.

Um diese Aufgabe zu erleichtern, werden oftmals automatische Aktualisierungsfunktionen bereitgestellt. Es wird empfohlen, diese zu aktivieren und zu nutzen. Sie können einen großen Teil der Aufgabe des Updatens übernehmen. Dies gilt insbesondere für die oben genannten Bereiche, für welche häufige Updates die Regel sind: Browser, Virenprogramm, Betriebssystem. Für alle Sicherheitsupdates gilt: Je schneller sie eingespielt und die Sicherheitslücke geschlossen wird, umso besser.
Davon abgrenzen lassen sich Updates, die Softwarefunktionen erweitern und aktualisieren. Diese lassen sich als Funktionsupdates bezeichnen. Tatsächlich ist die Abgrenzung

zwischen Sicherheits- und Funktionsupdate im Alltag nicht immer eindeutig zu ziehen. Bei spezielleren oder stark integrierten Softwarelösungen kann es Gründe geben, Funktionsupdates nicht gleich nach Erscheinen automatisch einspielen zu lassen, um etwaige Fehler in diesen Updates auszulassen. Nach einigen Tagen sind Updates in der Regel nachgereift und können meist problemlos eingespielt werden.

Ermitteln Sie Hard- und Software, die manuell zu aktualisieren sind.

Ein zuverlässiger Update-Prozess basiert auf einer umfassenden Inventarisierung. Es muss klar dokumentiert sein, welche Hardware und welche Software an welcher Stelle eingesetzt wird. Auf das Thema der Inventarisierung wird in Basismaßnahme 8 näher eingegangen. Nur auf dieser Grundlage können diejenigen Komponenten ermittelt werden, die mangels automatischer Aktualisierungsfunktion manuell aktualisiert werden müssen. Auch diese Komponenten müssen regelmäßig aktualisiert werden, am besten, sobald jeweils ein Update zur Verfügung steht.

Aktualisieren Sie Betriebssysteme und Anwendungssoftware, sobald Sicherheitsupdates vom Hersteller zur Verfügung stehen.

Insbesondere im Bereich der Sicherheitsupdates ist es entscheidend, dass diese installiert werden, sobald sie verfügbar sind. Sind Sicherheitsupdates verfügbar, dann sollten diese schnellstmöglich eingespielt werden.
Je schneller eine Sicherheitslücke geschlossen wird, umso kleiner ist die Angriffsfläche, die sich daraus ergibt. Gegebenenfalls muss vor dem Einspielen des Sicherheitsupdates über ein Testsystem die Funktionsfähigkeit des Updates geprüft werden. Die teilweise verfolgte Strategie, Updates einige Zeit liegen zu lassen und auf das Ausbleiben von Fehlerberichten anderer Nutzender zu warten, ist insofern nicht zu empfehlen, als damit das Risiko für Cyberangriffe durch länger offene Sicherheitslücken steigt.

Ersetzen Sie Systeme, die nicht mehr vom Hersteller unterstützt werden (d. h. keine Sicherheitsupdates mehr erhältlich), durch neue Produkte.

Im Bereich der Informationstechnik ist es üblich, dass Produkte einen Lebenszyklus durchlaufen. An die Veröffentlichung schließt sich ein meist mehrere Jahre andauerndes Zeitfenster an, in welchem der Hersteller das Produkt pflegt und die regelmäßige Bereitstellung von Sicherheitsupdates gewährleistet. Oft wird das Produkt nach einigen Jahren durch eine neue Version ersetzt. Nach einer Übergangszeit fällt dann oft das alte Produkt aus dem Support heraus. Es werden dann keine Sicherheitsupdates mehr bereitgestellt. Beispiele hierfür sind das Windows-Betriebssystem oder auch Smartphones. Das betrifft allerdings alle IT-Produkte und -Systeme. Sobald dies der Fall ist, muss das Produkt oder System ersetzt werden.
Meist bietet sich an diesem Punkt ein Upgrade auf eine neuere Version an. Der Einsatz veralteter Hard- und Software stellt ein großes Sicherheitsrisiko dar.

Können Sie das System nicht ersetzen, dann isolieren Sie es (z. B. mittels Firewall).

Sollte sich das betreffende Produkt nicht ersetzen lassen und kann darauf auch nicht verzichtet werden, so muss es im Netzwerk isoliert und ohne Verbindung ins Internet betrieben werden. Eine solche Isolierung, z. B. von Produktionsmaschinen mit veralteter Software/ Steuerung, lässt sich mittels Firewall realisieren. Auch das Kappen des Netzwerkkabels kann eine Möglichkeit darstellen (Stecker ziehen).

8. Basismaßnahme 2:
Benutzerzugänge absichern

8.1 Begründung

Viele Cyberangriffe werden dadurch ermöglicht, dass zu einfache Passwörter oder dieselben Passwörter für verschiedene Dienste verwendet werden. Sichere Passwörter sind bei der Absicherung von Benutzerzugängen von großer Bedeutung. Insgesamt muss die Architektur der Systeme zur Autorisierung (Zugriffskontrolle, Berechtigungen) und zur Authentisierung (Nachweis einer Identität) in den Blick genommen werden. Hierbei gilt das Prinzip der minimalen Rechte: Alle sollten nur die Berechtigungen erhalten, die zur Erledigung der übertragenen Aufgaben notwendig sind. Es empfiehlt sich, das Prinzip der Rollentrennung zu berücksichtigen: Für unterschiedliche Rollen sind unterschiedliche Accounts zu verwenden und jeder Account wird eigenständig abgesichert. Sichere Passwörter, Mehr-Faktor-Authentifizierung und passwortlose Authentifizierung via Passkeys sind die Stichworte, wenn es um die Absicherung von Benutzerzugängen geht.

8.2 Maßnahmen

Abschnitt 1: Trennung von Authentisierungsdaten

Identifizieren Sie Bereiche unterschiedlichen Schutzbedarfs.

Grundlage einer sauberen Rechtevergabe und der Rollentrennung ist, dass es einen Überblick über die unterschiedlich schützenswerten Bereiche gibt. Für alltägliche Aufgaben von IT-Nutzenden (Office, Browser, Mailclient) sind immer einfache Benutzerrechte ausreichend. Andere Bereiche wie z. B. der Dateiserver oder Backup-Laufwerke bedürfen besonderen Schutzes.

Zugänge mit administrativen Rechten sind besonders sparsam zu gewähren, mit sicheren Passwörtern und möglichst einem zweiten Faktor abzusichern (Token, biometrische Merkmale, Einmal-Passwort wie TAN etc.).

Trennen Sie die Konten von Administratoren und anderen Nutzenden.

Es wird empfohlen, Konten mit administrativen Rechten nur zur Administration einzusetzen. Für die normale IT-Nutzung werden Konten mit normalen Benutzerrechten empfohlen. Das führt dazu, dass eine Person je nach auszuführender Rolle unterschiedliche Konten und Zugänge nutzen muss. Eine klare Rollentrennung mindert die Angriffsfläche für Cyberangriffe. Die vergebenen Berechtigungen und Zugänge sollten regelmäßig aktualisiert werden, z. B. für den Fall, dass sich das Aufgabengebiet einer Person ändert, oder wenn eine Person das Unternehmen verlässt.

Vergeben Sie für jedes Konto und jeden Zugang ein eigenes Passwort. Ändern Sie voreingestellte Passwörter ab.

Passwörter sollten niemals mehrfach verwendet werden. Jedes Konto und jeder Zugang muss mit einem eigenen, sicheren Passwort abgesichert werden. Voreingestellte Passwörter sind ebenfalls durch eigene, sichere Passwörter zu ersetzen.

Abschnitt 2: Passwortsicherheit

Bei der Passwortsicherheit sind Länge und Komplexität entscheidend.

Je länger ein Passwort ist und je größer der Zeichenraum, aus welchem es sich zusammensetzt, desto schwerer ist es zu knacken. Ein Passwort, das in den meisten Fällen ausreichend sicher ist, besteht aus min. 12 Zeichen, enthält kleine und große Buchstaben, Zahlen und Sonderzeichen, bedient sich also 4 Zeichenkategorien. Beispiel: KALJe“AO;cNi.
Da solche Passwörter für das menschliche Gehirn schwer zu merken sind, setzt eine zweite Strategie auf schiere Länge: Die Aneinanderreihung von 4–5 beliebig gewählten Worten führt zu Passwörtern, die aufgrund ihrer Länge so schwer zu knacken sind, dass auch sie für die meisten Fälle ausreichend sicher sind. Ein solches Passwort muss mindestens 25 Zeichen enthalten und bedient sich der Zeichen zweier Kategorien: Klein- und Großbuchstaben.
Beispiel: Rasen kehren Straße leeren Ficus
Weitere Details siehe: Empfehlung „Sichere Passwörter erstellen“ des BSI:
https://sl.csc-kmu.de/b2-02.html
Hilfreich kann auch die Verwendung eines Passwortmanagers sein. Ein PW-Manager wird z. B. als lokales Programm installiert. Dort hinein können alle Zugangsdaten gespeichert werden. Er kann sichere Passwörter generieren, die sich dann für die entsprechenden Zugänge mittels Copy + Paste setzen lassen. Auf diese Weise reduziert sich die Anzahl der zu merkenden Passwörter erheblich. Zum Öffnen des Managers bedarf es eines sicheren Passworts.

Es gibt gute, auch kostenlose Passwortmanager wie beispielsweise KeePassXC.

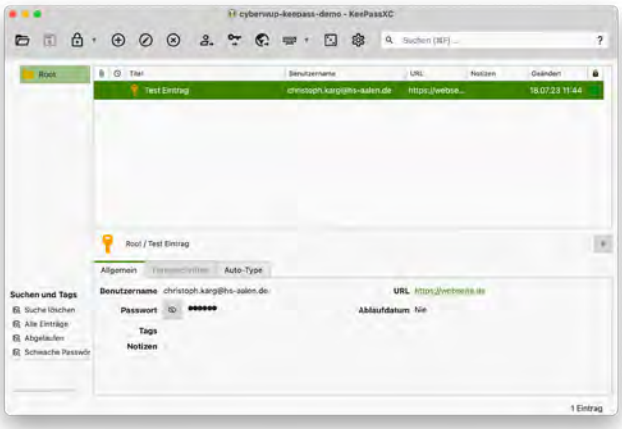


Abbildung 15: KeePassXC.

Legen Sie eine Passwortrichtlinie fest, die von allen Mitarbeitenden einzuhalten ist.

Die Passwortrichtlinie legt alle Kriterien fest, die im Zusammenhang mit der Erstellung und Verwendung von Passwörtern von Bedeutung sind: Passworterstellung mit Länge und Komplexität der Passwörter, Vermeidung von Mehrfachverwendung gleicher Passwörter, Geheimhaltung der Passwörter usw. Eine solche Passwortrichtlinie, die verbindlich von allen Mitarbeitenden eingehalten wird, kann ebenfalls zur Reduktion der Angriffsfläche beitragen.

Stellen Sie sicher, dass alle Passwörter geheimgehalten werden.

Alle Mitarbeitenden müssen dafür sensibilisiert werden, ihre Passwörter geheimzuhalten. Benutzerkonten und Zugänge sollten nicht geteilt genutzt werden. Passwörter dürfen nicht weitergegeben oder offen notiert werden. Klassische Orte wie Notizzettel unter der Tastatur oder der Schreibtischunterlage sind eine Steilvorlage für Angreifende, die sich Zugang zum Gebäude verschaffen und darin dann auch Zugang ins Firmennetz vorfinden können.

Abschnitt 3: Zwei-Faktor-Authentitifizierung

Schützen Sie zumindest kritische Konten und Konten mit weitreichenden Rechten durch die Einrichtung einer Zwei-Faktor-Autentifizierung (2FA).

Die Einrichtung eines zweiten Faktors zur Authentifizierung schützt vor Schaden durch Verlust des Passworts. Derart abgesicherte Zugänge können dann nur durch den Besitz zweier Faktoren genutzt werden.

Ein Beispiel hierfür ist: Passwort (Wissen) und TAN-App (Besitz des Smartphones).
Es gibt verschiedene geeignete Faktoren, deren es zweier aus unterschiedlichen Kategorien bedarf, für eine Zwei-Faktor-Authentifizierung:

- Authentifizierung durch Wissen: Passwort oder PIN
- Authentifizierung durch Besitz: Smartcard, Digitales Zertifikat, USB-Token (z. B. FIDO2), Generator für Einmal-Passwörter (OTP)
- Authentifizierung durch körperliche Eigenschaften: Scan des Fingerabdrucks, Gesichtserkennung, Stimmerkennung, Scan des menschlichen Auges

Mit zwei Faktoren sollten insbesondere kritische Konten wie Zugänge mit Administrationsrechten und Konten für die Fernwartung gesichert werden. Gegebenenfalls hilft hier die professionelle Unterstützung durch ein IT-Dienstleistungsunternehmen weiter. Wo eine 2FA angeboten wird, ist sie auch zu nutzen.

Richten Sie bei Fernzugriffen und VPN möglichst immer eine 2FA ein.

Die Einrichtung eines zweiten Faktors zur Authentifizierung sichert alle entsprechend ausgestatteten Zugänge ab. Da für Cyberangriffe insbesondere Konten mit Zugriffsmöglichkeiten von außerhalb des Firmengeländes von Interesse sind, sollten solche Fernzugriffskonten auch besonders gut abgesichert werden. Eine Zwei-Faktor-Authentifizierung ist hier ratsam.

Grundsätzlich gilt: Wenn von einem Dienstanbieter (E-Mail, soziale Medien usw.) eine 2FA angeboten wird, sollte diese auch genutzt werden.

Teilweise wird vonseiten der Dienste bereits die Nutzung weiterer Faktoren angeboten. Üblich ist das im privaten Bereich beispielsweise beim Onlinebanking, wo zusätzlich zum Kontonamen und dem Passwort in der Regel noch eine TAN eingegeben werden muss. Aber auch Social-Media-Konten und manche anderen Dienste bieten die Einrichtung einer Zwei-Faktor-Authentifizierung an. Wo diese Möglichkeit angeboten wird, sollte sie auch genutzt werden.

9. Basismaßnahme 3:
Datensicherungen durchführen

9.1 Begründung

Das Anfertigen von Backups ist die wichtigste präventive Maßnahme zum Schutz vor dem Verlust geschäftskritischer digitaler Daten. Durch keine noch so gute Absicherung können Cybersicherheitsvorfälle vollständig ausgeschlossen werden. Auch technische Defekte oder Störungen lassen sich nie vollständig ausschließen.

Ursachen für Datenverlust sind beispielsweise:

- Hardware-Defekte
- Umwelteinflüsse wie z. B. Wasserschaden oder Blitzeinschlag
- Fehlbedienung des Computers
- Verlust oder Diebstahl von mobilen Endgeräten
- Cyberattacken

Vollständige, aktuelle und funktionsfähige Backups können Datenverlust verhindern.

9.2 Maßnahmen

Führen Sie eine regelmäßige und automatische Datensicherung durch.

Die regelmäßige und vollständige Datensicherung der Systeme ist eine wichtige Voraussetzung, um im Schadensfall schnell und ohne Datenverlust wieder handlungsfähig zu werden. Die Backups sollten in regelmäßigen Abständen erfolgen. Es lohnt sich, die Möglichkeiten der Automatisierung dieser Backup-Routinen zu prüfen. Durch die stetige Wiederholung der immer gleichen Arbeitsschritte liegt hier großes Automatisierungspotenzial vor.

Bei größeren Systemen kann diese Aufgabe durchaus umfangreich und komplex werden. Wenn mehrere Teilsysteme gesichert werden müssen, ist auch auf die Reihenfolge zu achten, also darauf, welches Teilsystem auf welchem anderen aufbaut.

Orientieren Sie sich beim Turnus des Backups an der Frequenz der anfallenden geschäftskritischen Daten.

Je nach Art der zu sichernden Daten kann eine andere Frequenz der Anfertigung von Sicherungen angemessen sein. Idealerweise werden Backups automatisiert in voreingestellten Zeitintervallen erstellt, z. B. jede Woche freitags um 2:00 Uhr. Je nach zu sicherndem System (Webshop, Fileserver etc.) kann ein kürzeres (z. B. täglich) oder längeres Intervall (z. B. monatlich) passend sein. Die Entscheidung muss unter Berücksichtigung aller Parameter wie Aufwand, Nutzen, Auswirkungen von Datenverlust usw. getroffen werden.

Beachten Sie die 3-2-1-Regel: drei Kopien auf zwei unterschiedlichen Medienträgern und ein Medium physisch von der Arbeitsumgebung getrennt an einem anderen, sicheren Ort aufbewahren.

Eine gute Backup-Strategie sorgt dafür, dass die Daten dreimal vorliegen: Die erste Kopie befindet sich auf der Festplatte des zu sichernden IT-Systems und stellt die Originalversion der Daten dar. Diese unterliegen der täglichen Nutzung. Von dieser Originalversion sind dann zwei weitere Sicherungen anzufertigen. Dabei ist darauf zu achten, dass die insgesamt drei Kopien letztlich auf mindestens zwei unterschiedlichen Medienträgern liegen (interne/externe Festplatte, Wechselplatte, Bandlaufwerk, Cloud-Backup usw.) und dass mindestens eine

der Kopien physisch von der Arbeitsumgebung getrennt an einem anderen, sicheren Ort aufbewahrt wird (Offsite-Backup). Damit wird Gefahren wie der Zerstörung eines Ortes z. B. durch Feuer oder Überflutung, aber auch der Zerstörung der betrieblichen IT-Infrastruktur z. B. durch einen Ransomware-Angriff vorgebeugt. Das heißt, dass diese dritte Kopie nicht nur an einen geografisch anderen Ort verbracht werden muss, sondern, z. B. im Falle der Cloud, diese Kopie auch nicht per Netzwerkverbindung mit dem ursprünglichen System verbunden sein darf. Mit anderen Worten, der entsprechende Cloud-Speicher darf nicht als Laufwerk im System eingebunden sein, wenn er die Funktion des physisch von der Arbeitsumgebung getrennten Medienträgers erfüllen soll.

Verschlüsseln Sie die Datensicherung, insbesondere wenn Daten das Firmengelände verlassen. Der Schlüssel sollte in diesem Fall separat auf einem externen Datenträger und in physischer Form aufbewahrt werden.

Das Verschlüsseln von Daten ist grundsätzlich zu empfehlen. Sobald ein Backup das Firmengelände verlässt, wird es tendenziell schwieriger, unbefugte Zugriffe darauf auszuschließen. Die Verschlüsselung dieser Datensicherung kann hier Abhilfe schaffen. Um jedoch im Ernstfall darauf zugreifen zu können, ist die sichere Aufbewahrung des Schlüssels zu gewährleisten. Es empfiehlt sich, diesen Schlüssel sowohl auf einem separaten Datenträger als auch in physischer Form aufzubewahren. Der Schlüssel wird, wie alle anderen wichtigen Zugangsdaten auch, an einem sicheren Ort aufbewahrt und muss im Ernstfall verfügbar sein. Dabei sollte auch bedacht werden, dass zentrale IT-Systeme im Angriffsfall nicht mehr zur Verfügung stehen könnten. Der Aufbewahrungsort sollte nicht derselbe sein wie der der verschlüsselten Kopie. Doch liegt der Schlüssel bei den beiden anderen Kopien (mutmaßlich auf dem Betriebsgelände), verliert die dritte Kopie ihre Schutzfunktion vor lokaler Zerstörung z. B. durch Feuer oder Überflutung.

Testen und dokumentieren Sie regelmäßig die Wiederherstellung der Daten.

Häufig werden Backups angefertigt, ohne dass sie in ihrer Wiederherstellbarkeit getestet werden. So kann es passieren, dass im Schadensfall die Wiederherstellung der Systeme an defekten, dysfunktionalen oder unvollständigen Backups scheitert. Das Testen der Wiederherstellbarkeit der Datensicherungen ist aufwendig, aber dennoch der unerlässliche letzte Schritt in einer ausgereiften Backup-Strategie. Regelmäßig sollte überprüft und dokumentiert werden, dass die Backups vollständig sind und sich auch wiederherstellen lassen:

Grundlegende Parameter des Backups lassen sich ohne viel Aufwand am Ende der Datensicherung überprüfen: Ist die Backup-Größe im erwarteten Bereich? Falls nein, kann das ein Hinweis auf ein fehlerhaftes Backup sein. Eine solche Integritätsprüfung wird von Backup-Lösungen oft schon automatisch vorgenommen.

Die Funktionsprüfung hingegen ist aufwendiger: Hier wird tatsächlich die Wiederherstellbarkeit der Backups getestet. Dafür muss allerdings eine geeignete Umgebung geschaffen werden, wie z. B. eine Ersatzmaschine oder eine entsprechende virtuelle Umgebung. Dabei wird geprüft, ob sich die Backups einspielen lassen, in welcher Reihenfolge das zu geschehen hat und ob dann der Server und alle Dienste noch funktionieren. Diese Funktionsprüfung ist von entscheidender Bedeutung. Wenn im Ernstfall das Rückspielen der Backups scheitert, weil diese nicht funktionieren, sind trotz Sicherung im Zweifel alle Daten verloren.

10. Basismaßnahme 4: Gefahrenbewusstsein schaffen

10.1 Begründung

Die Mitarbeitenden eines Unternehmens spielen bei der Umsetzung vieler Cybersicherheitsmaßnahmen eine zentrale Rolle. Die besten technischen Sicherheitsvorkehrungen können durch menschliches Fehlverhalten umgangen werden. Phishing, CEO-Fraud und andere Versuche von Cyberkriminellen, Zugang zu Firmennetzwerken zu bekommen, erfolgen meist über den Faktor Mensch. Sind alle beteiligten Personen sensibilisiert und gut geschult, dann sinkt das Risiko von Schäden durch menschliches Fehlverhalten.

10.2 Maßnahmen

Abschnitt 1: Aktuellen Informationsstand sicherstellen

Definieren Sie die Quellen, aus denen man sich regelmäßig über neue Sicherheitslücken informiert.

Um die aktuellen Gefahren zu kennen, ist es wichtig, sich regelmäßig über neue Sicherheitslücken und Bedrohungen zu informieren. Die Erkenntnisse daraus sollten einerseits in die Sensibilisierung der Mitarbeitenden fließen, sind andererseits aber auch für die Aufgabe des Updatens von Bedeutung. Phishing-Maschen ändern sich, Versuche von Cyberkriminellen unterliegen Trends. Es sollten die Quellen definiert werden, anhand derer die verantwortliche Person sich regelmäßig auf dem Laufenden hält.

Abonnieren Sie Newsletter, von denen Sie bzw. die Verantwortlichen regelmäßig automatisch über neue Sicherheitslücken und aktuelle Entwicklungen benachrichtigt werden.

Um auf dem aktuellen Stand zu bleiben, bietet es sich an, Newsletter zu abonnieren, die die Neuigkeiten regelmäßig ins Mailpostfach bringen, und auch einschlägige Infoseiten regelmäßig zu konsultieren. Eine Auswahl solcher Quellen ist auf der Kartenrückseite von Basismaßnahme 4 zu finden. Für alle, bei denen die englische Sprache keine Hürde darstellt, bieten die Infoseiten und Newsletter der amerikanischen Cybersicherheitsagentur CISA einen hervorragenden und umfangreichen Überblick.

Sorgen Sie für die Weitergabe und Umsetzung der Erkenntnisse an Ihre Mitarbeitenden und legen Sie dazu Verantwortlichkeiten fest.

Neuen Entwicklungen, die die eigene Gefährdungslage betreffen, sollte umgehend Rechnung getragen werden. Über die Beachtung der entsprechenden Hinweise im Update-Prozess hinaus ist es von Bedeutung, die Verantwortlichkeit klar festzulegen und auch einen Kommunikationskanal zur Sensibilisierung der Mitarbeitenden zu etablieren. Darüber können relevante Informationen, die im Tagesgeschäft zu beachten sind, geteilt werden (Hinweise auf Phishing-Maschen usw.). Das regelmäßige Erinnern an Cyberbedrohungen führt zu höherer Wachsamkeit und dadurch potenziell zu weniger Fällen menschlichen Fehlverhaltens (auf Link geklickt, Zugangsdaten eingegeben usw.).

Abschnitt 2: Sensibilisierung und Schulung

Stellen Sie Ihr Personal in den Mittelpunkt. Motivieren Sie die Mitarbeitenden durch wirksame Kommunikation und betriebliche Initiativen.

Angemessene Cybersicherheit lässt sich nur unter Einbezug der Mitarbeitenden erreichen. Gut geschultes Personal, das auf dem aktuellen Wissensstand ist und Anlaufstellen kennt, an die es sich im Zweifel wenden kann, ist eine wichtige Säule guter Cybersicherheit. Hierfür sind eine klare und wertschätzende Kommunikation sowie motivierende Initiativen hilfreich.

Versorgen Sie die Mitarbeitenden regelmäßig mit Kurzinformationen.

Morgens im Mailpostfach in regelmäßigen Abständen über einzelne Fälle oder aktuelle Entwicklungen aus dem Bereich Cybersicherheit informiert zu werden, erweitert sukzessive das Wissen der Empfänger und ruft regelmäßig das Thema der Cybersicherheit ins Bewusstsein. Gut geschultes Personal kann sich auf diesem Weg regelmäßig seine Kompetenzen vergegenwärtigen und reagiert im Ernstfall eher souverän und wohlüberlegt auf Cyberangriffe und Sicherheitsvorfälle. Hierfür eignen sich Berichte über Vorfälle, über aktuelle Betrugsmaschen, aber auch Handreichungen mit Handlungsanweisungen, die auch in kleineren Portionen ausgegeben werden können.

Schulen Sie alle Beschäftigten regelmäßig, realitätsnah und abgestimmt auf die speziellen Bedürfnisse. Dies gilt von der Arbeits- bis zur Leitungsebene und auch für den Ausbau der Kompetenzen der Administration.

Ein gutes Schulungskonzept ist von großer Bedeutung. Alle Mitarbeitenden müssen für die zugeteilten Aufgaben angemessen geschult werden, auch in Fragen der Cybersicherheit. Die Anforderungen an solche Schulungen unterscheiden sich womöglich zwischen der Arbeits- und der Leitungsebene. Es ist besonders darauf zu achten, dass auf administrativer Ebene die passenden Kompetenzen vorhanden sind oder mittels Schulungen und Fortbildungen aufgebaut werden.
Es gibt Sensibilisierungsangebote, die auf spielerische Weise die Fähigkeiten zum sicheren Umgang mit IT trainieren und die sich gut in den Arbeitsalltag integrieren lassen. Häufig werden auch Programme zum Trainieren von Phishing-Erkennung eingesetzt. Hierzu werden in unregelmäßigen Abständen gefälschte Phishing-Mails im Unternehmen versendet. Das Anklicken der Links darin führt zu einer Website, die über die Gefahren aufklärt, die mit Phishing-Mails verbunden sind. Hier gibt es ein großes Angebot an zahlungspflichtigen Programmen. Aber auch kostenlose Tools stehen zur Verfügung, wie z. B. die Lernspiele des BAKGame-Projekts, erreichbar unter: https://sl.csc-kmu.de/b4-06.html (BAKGame, 2024).

Sensibilisieren Sie Ihre Beschäftigten insbesondere für das Verhalten in sozialen Medien in Form verbindlicher Vorgaben und Aufklärungsmaßnahmen.

Soziale Medien sind potenzielle Recherchequellen, die Cyberkriminelle zur Informationsbeschaffung für gezielte Angriffe nutzen (Social Engineering). Darüber lassen sich teilweise Informationslücken zu Verantwortlichkeiten, Namen, Organisationsstruktur schließen, die dann z. B. einen CEO-Fraud- oder Spear-Phishing-Angriff ermöglichen.

Schärfen Sie das Verantwortungsbewusstsein bei Ihren Beschäftigten, dass Sicherheitsvorfälle und verdächtige Wahrnehmungen gemeldet werden. Definieren Sie entsprechende Meldewege.

Cyberangriffe fangen oft klein an. Gefälschte Mails können die Adressaten zur Preisgabe sensibler Informationen verleiten. Ein erfolgreicher Phishing-Angriff kann zur Übernahme eines Benutzeraccounts führen. Oft gehen diese Schritte nicht gänzlich unbemerkt vonstatten. Sind die Mitarbeitenden sensibilisiert, derartige Vorkommnisse wahrzunehmen, und wissen sie, an wen sie sich mit ihrer Beobachtung wenden können, lassen sich Angriffe schon ganz früh abwehren. Es lohnt sich, in der IT und vielleicht nachgelagert in der Führungsebene Verantwortlichkeiten zur Entgegennahme solcher Hinweise zu definieren und hierfür eine Ansprechperson zur Entgegennahme von Meldungen zu benennen.
Darüber hinaus gilt es, eine Fehlerkultur innerhalb des Unternehmens zu fördern, sodass die Bereitschaft besteht und der Mut aufgebracht wird, auch über evtl. eigenes Fehlverhalten, z. B. unachtsames Anklicken einer Phishing-Mail, zu sprechen und der Ansprechperson im Unternehmen zu melden.

11. Basismaßnahme 5:
Netzübergänge absichern

11.1 Begründung

Eine gute Netzwerkarchitektur ist die Basis für angemessene Cybersicherheit. Klar abgegrenzte Netzwerksegmente mit wenigen, durch Firewalls geschützten Übergängen und insbesondere mit möglichst nur einer durch eine dedizierte Firewall abgesicherten Verbindung zum Internet schaffen die Voraussetzung für eine sichere Umgebung. In einem solchen Netzwerk können Angriffe sich schwerer ausbreiten und betreffen so im Ernstfall nicht die gesamte IT-Infrastruktur.

11.2 Maßnahmen

Abschnitt 1: Firewall einrichten

Nutzen Sie Firewalls zum Schutz aller kritischen Systeme, insbesondere als Schutzmauer zwischen Firmennetzwerk und Internet.

Eine Firewall kontrolliert den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk (z. B. Internet). Eine solche dedizierte Firewall besteht aus Hard- und Software. Sie überprüft beispielsweise anhand der IP-Adresse des Rechners, ob das Datenpaket, das ins Netzwerk hineinwill, überhaupt dazu berechtigt ist. Dazu sind Listen mit erlaubten Sendern (Adressen) in der Firewall hinterlegt.

Eine Personal Firewall ist eine abgespeckte Firewall, eine reine Softwarelösung, die insbesondere im Privatbereich Anwendung findet. Im Gegensatz zu einer dedizierten Firewall, die ganze Netzwerke, bestehend aus vielen Endgeräten, an der Schnittstelle zum Internet schützt, versucht mit einer Personal Firewall ein einzelner PC sich selbst zu schützen. Diese soll aber, ebenso wie die normale Firewall, den Rechner vor Angriffen von außen schützen und auch verhindern, dass bestimmte Programme, z. B. sogenannte Spyware, Kontakt vom Rechner zum Internet aufnimmt.
Quelle: BSI, 2024a.

Sichern Sie möglichst auch alle internen Netzübergänge mit einer Firewall ab.

Eine weitere wichtige Maßnahme ist die Segmentierung des Firmennetzwerks in verschiedene voneinander getrennte Bereiche (siehe Abschnitt 2: Netzübergänge identifizieren und segmentieren). Die Übergänge zwischen diesen Netzsegmenten sollten ebenfalls mit Firewalls abgesichert werden.

Schützen Sie Zugänge zu Netzen und IT-Systemen für Administratoren, vor allem für Fernwartung und Fernadministration.

Besonderes Augenmerk gilt der Absicherung von Zugängen mit Administrationsrechten. Cyberangriffe lassen sich in der Regel erst durch die Erlangung von administrativen Rechten umfangreich eskalieren. Für Angreifende sind insbesondere Zugänge für Fernwartung und Fernadministration von herausragender Bedeutung, da sie die Ausübung administrativer Macht von außerhalb über das Internet ermöglichen. Sind die administrativen Zugänge gut abgesichert ((Zwei-Faktor-Authentifizierung, gut geschulte Administration, Prinzip der minimalen Rechte, Rollentrennung), werden auch Cyberangriffe erschwert.

Achten Sie auf eine strenge Filtereinstellung, die alle nicht zwingend notwendigen Verbindungen blockiert.

Wie bei jeder Software ist die Konfiguration der Firewall entscheidend für die Sicherheit, die sie bietet. Folgende Punkte sind dabei zu beachten:

- Filterregeln so definieren, dass nur die unbedingt notwendigen Zugriffe erlaubt sind
- Einstellungen regelmäßig überprüfen
- Nicht benötigte Ports sperren
- Virenscanner installieren, aktivieren und stets aktuell halten
- Patches sofort nach Bekanntgabe von Sicherheitslücken einspielen
- Protokollierung sicherheitsrelevanter Ereignisse aktivieren und regelmäßig auswerten

Quelle: BSI, 2024a.

Abschnitt 2: Netzübergänge identifizieren und segmentieren

Sorgen Sie für eine Netzwerksegmentierung (z. B. mittels physikalischer Trennung oder VLAN) sowie weitgehende Minimierung externer Netzübergänge.

Damit Firewalls ihre Wirkung entfalten können, ist eine klare und durchdachte Netzarchitektur Voraussetzung. Das Firmennetz sollte, wo möglich und sinnvoll, in einzelne Netzsegmente aufgeteilt werden. Die Übergänge dazwischen sollten minimiert und durch Firewalls geschützt werden. Netzsegmente, die besonders sensibel sind und/oder einen Internetzugang nicht erfordern, sollten möglichst ohne Internetzugang betrieben werden. Bei einem Produktionsnetz, das als Inselsystem nicht mit dem Internet verbunden ist, besteht ein wesentlich geringeres Risiko für Cyberangriffe. Insbesondere Netzübergänge/Verbindungen ins Internet müssen minimiert und hierbei Redundanzen vermieden werden. Diese reduzierte Anzahl an Netzübergängen lässt sich dann auch besser mittels Firewalls schützen.

Identifizieren und dokumentieren Sie alle Netzübergänge.

Wie bereits beschrieben, ist ein besonderes Augenmerk auf alle Netzübergänge, insbesondere diejenigen ins Internet, zu legen. Gewachsene Strukturen, die möglicherweise unterschiedliche DSL-Zugänge beinhalten, bergen größere Risiken. Nicht dokumentierte und von daher unbekannte Internetzugänge bleiben somit potenziell ungeschützt. Eine gute Dokumentation der Netzarchitektur erleichtert im Ernstfall die Sicherungs- und Rettungsmaßnahmen sowie den Wiederaufbau des Firmennetzes.

Überlegen Sie, was am Netz hängen muss und was physikalisch getrennt werden kann. Grundsatz: Trennen Sie alles vom Internet, was nicht erforderlich ist.

Alles, was nicht mit dem Internet verbunden ist, kann in der Regel auch nicht durch Cyberangriffe zerstört werden. Beispielsweise für Produktionsnetze oder Backup-Systeme könnte diese Maßnahme von entscheidender Bedeutung sein.

Lassen Sie Zugriffe von außen auf Ihr Firmennetz nur über ein VPN zu.

Das Firmennetz sollte von außen nur über abgesicherte Netzwerkverbindungen erreichbar sein. Das betrifft beispielsweise VPN, zu welchen im weiteren Verlauf ausführliche Informationen zu finden sind. Auch der Zugriff auf IT-Systeme über Fernzugriffsoftware (z. B. Remote-Shell oder Remote-Desktop) muss entsprechend abgesichert werden. Auf Webseiten, eine Cloud-Anwendung oder eine Webmail-Seite sollte der Zugriff nur über HTTPS-gesicherte Verbindungen möglich sein. Die Verbindungen zu IMAP- und SMTP-Mailservern sollte nur verschlüsselt erfolgen (SSL, TLS).
Bei einem Virtual Private Network, kurz VPN, handelt es sich um ein virtuelles, nicht öffentliches Netzwerk. „Virtuell“ bedeutet, dass die verschiedenen Endgeräte in diesem Netzwerk – anders als z. B. im Firmennetzwerk – nicht direkt physisch miteinander oder mit einem zentralen Router verbunden sind. Eine VPN-Verbindung, umgangssprachlich auch VPN-Tunnel genannt, dient dazu, über das ungeschützte Internet eine geschützte (verschlüsselte) Verbindung zwischen zwei Endpunkten herzustellen.

Hierfür wird eine Verbindung von einem Endgerät – z. B. einem Smartphone – zu einem VPN-Server aufgebaut. Der VPN-Server weist dem Endgerät dann eine neue (interne) IP-Adresse zu. Beim Surfen im Internet ist dann für das Gegenüber (z. B. die besuchte Webseite) statt der Original-IP-Adresse des Geräts die

externe IP-Adresse des VPN-Servers sichtbar. Somit werden der tatsächliche Standort des Geräts sowie die Online-Identität gegenüber Dritten verschleiert. Gleichzeitig werden alle zwischen dem Endgerät und dem VPN-Server übertragenen Daten durch Verschlüsselung vor Zugriffen aus dem restlichen Internet geschützt.

Eine VPN-Verbindung kann für unterschiedliche Anwendungsfälle eingesetzt werden:

- Im Berufsleben dient ein VPN häufig zur **sicheren Anbindung von Homeoffice-Arbeitsplätzen** an das Unternehmensnetzwerk oder dazu, Außendienstmitarbeitern von unterwegs den mobilen Zugriff auf zentrale Anwendungen und Datenbestände im Unternehmen zu ermöglichen – Stichwort mobiles Arbeiten.
- Ein weiteres VPN-Anwendungsfeld betrifft die virtuelle **Vereinigung räumlich getrennter Standortnetze** – was nicht nur für Wirtschaftsunternehmen interessant ist, sondern z. B. auch für Universitäten, staatliche Verwaltungseinrichtungen oder Nichtregierungsorganisationen. Ergänzend zur Verschlüsselung der Datenübertragung kann die Standortanbindung dabei zusätzlich durch einen speziell gehärteten Einwahlknoten (VPN-Gateway) gesichert werden, um einen noch höheren Schutz vor Cyberangriffen zu gewährleisten.
- Bei der Nutzung **öffentlicher WLAN-Hotspots** kann durch eine VPN-Verbindung das Risiko eines unbefugten Zugriffs, Ausspähens oder Abflusses von Daten minimiert werden, da ein VPN sämtliche Daten via Internet in verschlüsselter Form überträgt. Möglichen Ausspähversuchen durch andere Nutzerinnen und Nutzer im öffentlichen WLAN wird somit ein Riegel vorgeschoben.
- Sehr nützlich kann eine VPN-Anbindung auch während eines Auslandsurlaubs sein – z. B., wenn Sie dort einen Beitrag aus der Mediathek eines Fernsehsenders sehen wollen. Denn außerhalb der Landesgrenzen wird das Streaming vieler deutscher Medienangebote aus lizenzrechtlichen Gründen unterbunden. Dieses sogenannte **Geo-Blocking** funktioniert über eine Sperre all jener IP-Adressen, die nicht der Bundesrepublik zugeordnet sind. Mit einer VPN-Software auf Ihrem Tablet oder Notebook funktioniert eine solche IP-Sperre nicht: Sobald Ihre VPN-Verbindung über einen VPN-Server mit Standort in Deutschland aufgebaut wird, erhält Ihr Smartphone oder Tablet auch im Ausland automatisch eine hierzulande nicht blockierte IP-Adresse. Die Geo-Blockade ist somit ausgehebelt (BSI, 2024d).

11.3 Exkurs: Rechnernetze

11.3.1 IP-Adressen

IP-Adressen: IP-Adressen sind die individuellen Adressen, die einzelne Geräte in einem Netzwerk identifizieren. Sie machen Geräte zu Kommunikationszwecken adressierbar und damit erreichbar. IP steht für „Internetprotokoll". IPv4-Adressen reichen von 0.0.0.0 bis 255.255.255.255. Ein Beispiel für eine Adresse aus dem neueren IPv6-Adressraum ist: 2001:0db8:85a3:0000:0000:8a2e:0370:7344.

Die IP-Adresse funktioniert ähnlich einer Postadresse auf einer Briefsendung. Sie sorgt dafür, dass Daten von ihrem Absender zum vorgesehenen Empfänger transportiert werden. Dafür werden Datenpakete mit einer IP-Adresse versehen, die den Empfänger eindeutig identifiziert. Obwohl IP-Adresse, anders als Postadressen nicht an einen bestimmten Ort gebunden sind, können die Router als die Verteilzentren anhand dieser Adressen entscheiden, wohin das Datenpaket weitertransportiert wird (Ernst, Schmidt & Beneken, 2023, S. 322f.).

11.3.2 Host-/Rechnernamen

Numerische IP-Adressen, besonders bei IPv6, sind nicht leicht zu merken und ihre Struktur lässt keine direkten Rückschlüsse auf Ort und Art der Adresse zu. Daher wurde das Domain Name System (DNS) eingeführt, das weltweit jeder IP-Adresse einen eindeutigen Namen zuweist. Das gesamte Netz ist dabei in Teilnetze gegliedert. Die oberste Ebene, die Top-Level Domain (TLD), bestimmt die Endung der Adresse. Diese ist in der Regel ein Ländercode, wie beispielsweise .de für Deutschland, .nl für die Niederlande und .it für Italien.

Als nächste Hierarchiestufe stehen dann Haupt-Domänen, die in der Regel der Name des Providers sind, sowie ggf. Sub-Domänen. Alle Namenskomponenten werden durch Punkte voneinander getrennt. Ein DNS-Name könnte also lauten: firma.provider.de.

Vor der Verbindungsaufnahme muss der DNS-Name in eine IP-Adresse umgewandelt werden. Dazu fordert der Client vor der eigentlichen Herstellung der Verbindung zu dem gewünschten Server bei einem Name-Server (DNS-Server) die zu dem DNS-Namen gehörige IP-Adresse an. Dies läuft in der Regel vom Benutzer verborgen im Anwenderprogramm ab (Ernst, Schmidt & Beneken, 2023, S. 332).

11.3.3 TCP/UDP-Ports

Die IP-Adresse identifiziert in der Regel einen Rechner im Internet. Auf diesem Rechner laufen verschiedene Programme in eigenen Prozessen. Bestimmte Programme bieten Dienste an, die von anderen Rechnern aus benutzt werden können sollen. Beispiele für solche Dienste sind ein Webserver oder ein SSH-/FTP-/Telnet-Dienst. Damit muss ein Programm von außen in der Lage sein, einen bestimmten Prozess oder Dienst auf einem Empfängerrechner zu adressieren. Hierzu werden Ports verwendet bei den Protokollen TCP und UDP. Ein Prozess bzw. Dienst wird damit über die IP-Adresse und den Port angesprochen. Ein Port ist durch eine Nummer zwischen 1 und 65.535 gekennzeichnet, die Ports werden durch das Betriebssystem verwaltet. Für bestimmte Dienste wurden Ports fest definiert, ein solcher Dienst auf einem Rechner sollte an genau diesen Port gebunden sein. Ein Webserver läuft beispielsweise auf Port 80 oder 443 (Ernst, Schmidt & Beneken, 2023, S. 331).

Beispiel: Ein Webbrowser kann während eines laufenden HTTPS-Downloads einen weiteren Download von ein und demselben Webserver starten, weil der Browser dann (Client-seitig) einen weiteren Port öffnet und so eine zusätzliche Verbindung zum selben Port 443 des Servers aufbaut. Der Server antwortet den unterschiedlichen Ports des Browsers mit unterschiedlichen, jeweils zusammengehörigen Inhalten. Für eine Unterscheidung der Verbindungen genügen also verschiedene Portnummern an nur einem der beiden Endpunkte.

12. Basismaßnahme 6:
Schadprogramme abwehren

12.1 Begründung

Jeden Tag erscheinen Hunderttausende neuer Schadcodevarianten. Deshalb muss ein Virenschutzprogramm auf allen Systemen installiert oder aktiviert werden. Zudem müssen das Virenschutzprogramm selbst und seine Erkennungsdatenbank immer auf dem neuesten Stand gehalten werden. Dennoch ist die Installation eines guten Virenschutzprogramms nicht mehr die Lösung, um alle Cybersicherheitssorgen los zu sein. Antivirensoftware ist wichtig, schützt aber nur im Zusammenspiel mit den anderen Maßnahmen in diesen 10 Karten.

12.2 Maßnahmen

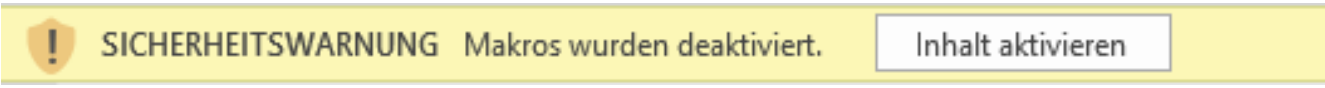


Abbildung 16: Die geschützte Ansicht bei MS Office hindert Makros und andere aktive Elemente an der Ausführung. Quelle: Schwarz & Hahn, 2021.

Abschnitt 1: Makros deaktivieren

Makros sind kleine Programme, mit denen sich Aufgaben z. B. in Excel automatisieren lassen. Makros können sehr hilfreich sein. Mit ihnen lassen sich aufwendige und serielle Aufgaben automatisieren. Doch Makros können auch als Einfallstor für Schadsoftware genutzt werden. Sie können z. B. ganze Programme enthalten. Sobald sie ausgeführt werden, können diese z. B. Schadsoftware unbemerkt aus dem Internet herunterladen. Wenn das verwendete Benutzerkonto zudem ein Administrationskonto ist, kann diese Schadsoftware ungehindert aktiv werden: Rechner verschlüsseln, Keylogger installieren usw.

Verwenden Sie für Dokumente aus externen Quellen eine sichere Darstellungsoption, insbesondere bei E-Mail-Anhängen oder Downloads aus dem Internet. Deaktivieren Sie daher Makros und andere aktive Elemente, die in Ihrer Office-Anwendung nicht benötigt werden.

Dieses Thema betrifft insbesondere Office-Dokumente und -Anwendungen, doch auch PDF-Dateien sind nicht gänzlich vor Schadsoftware sicher. Ein häufiger Angriffsweg ist der Versand von makrohaltigen Dateien als E-Mail-Anhang. Für Office-, aber auch PDF-Dokumente gibt es sichere Darstellungsoptionen, deren Nutzung für die Anzeige von Dokumenten aus externen Quellen unbedingt zu empfehlen ist. Sie können aktive Elemente enthalten, die mit Öffnen des Dokuments aktiv werden und Schadsoftware verbreiten oder Angriffe ermöglichen können.
Es ist deshalb wichtig, für die Anzeige von Dokumenten möglichst immer eine sichere Darstellungsweise zu wählen. Diese sollte zentral für alle Mitarbeitenden auf den Endgeräten und in den jeweiligen Programmen voreingestellt werden. In MS Office z. B. bietet das Trust Center die Option „Alle Makros mit Benachrichtigung deaktivieren“. Wird anschließend ein Dokument geöffnet, welches Makros enthält, erscheint diese Benachrichtigung.

Diese Hinweise sind unbedingt ernst zu nehmen. Bevor Inhalte aktiviert werden, muss die Herkunft der Dateien überprüft und bestätigt sein. Besondere Vorsicht ist angebracht, wenn der Absender unbekannt ist, der Absender gefälscht ist, also z. B. unscheinbare Zeichen enthält, die sich leicht übersehen lassen, oder die erhaltene Datei nicht erwartet wurde. Im Zweifel kann es ratsam sein, mit dem Absender über einen anderen Kommunikationskanal in Verbindung zu treten und sich den Versand des erhaltenen Dokuments bestätigen zu lassen.

Das unbedachte Öffnen von Mailanhängen ist in jedem Fall zu unterlassen.

Zu den gefährlichen Dateitypen gehören unter anderem Dateien mit den Endungen .bat, .exe, .vbs, .com, .ade, .adp, .cpl und .wsc. Einige dieser Typen werden von Mailprogrammen automatisch blockiert. Ein wachsames geschultes Auge schadet hier aber natürlich trotzdem nicht. Denn selbst Virenprogramme erkennen nicht immer alle Schädlinge, die lauern (Schwarz & Hahn, 2021).

Abschnitt 2: Virenschutzprogramme verwenden

Installieren Sie auf allen Geräten zentral verwaltete Virenschutzprogramme und halten Sie diese stets aktuell. Ein mehrstufiger Virenschutz ist sinnvoll.

Zum Schutz von IT-Ressourcen sind Virenschutzprogramme sehr nützlich: 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 neuer Schadcodevarianten (BSI, 2023b).

Mehrstufigkeit: Virenschutzprogramme gibt es nicht nur für Arbeitsplatzrechner, Laptops und Smartphones, also Clients. Der Einsatz von Virenschutzprogrammen auf Servern, beispielsweise Dateiservern, Mailservern, Webservern und Firewalls, ist ebenfalls zu empfehlen.

Dies gilt vor allem bei Homeoffice-Lösungen und Systemen, die mit dem Internet verbunden sind.

Internetzugang und Fernzugriff erhöhen die Angriffsfläche für Cyberangriffe erheblich. Bei Homeoffice-Lösungen sollte ein aktueller Virenschutz stets Bestandteil des Sicherheitskonzepts sein.

Prüfen Sie, ob weitere Sicherheitssysteme erforderlich sind, um Ihre IT-Systeme nach außen zu schützen, z. B. Antivirensoftware auf E-Mail-Servern.

Die Verwendung von Virenschutzprogrammen auf Endgeräten ist wichtig, aber allein nicht ausreichend. Es macht Sinn, zu prüfen, ob weitere Sicherheitssysteme erforderlich sind. Das können beispielsweise Antivirensysteme auf Servern wie E-Mail-Servern oder Fileservern sein, oder weitere Sicherheitssysteme für Webserver. Bei größeren Netzwerken und komplexerer Infrastruktur kann sogar der Einsatz eines Intrusion Detection System hilfreich sein.

Abschnitt 3: Kommunikationswege absichern

Nutzen Sie Filter gegen Spam- und Phishing-E-Mails sowie gegen E-Mails mit Links zu schädlichen Webseiten oder mit schädlichen Dateianhängen.

Die E-Mail ist ein besonders beliebtes Einfallstor für niederschwellige, ungezielte Massenangriffe wie z. B. Phishing. Um die Sicherheit und Funktionalität der Kommunikationswege, z. B. E-Mails, zu erhöhen, bietet es sich an, den eingehenden Mailverkehr mittels Spam-Filter von Spam- und Phishing-Mails zu befreien.

Konfigurieren Sie Ihre E-Mail-Anwendung so, dass:

- E-Mails von extern als solche speziell gekennzeichnet werden, z. B. durch die Voranstellung von „extern“,
- die E-Mail-Adresse angezeigt wird und nicht der E-Mail-Alias (z. B. max.mustermann@email.de anstatt „Max Mustermann“).

Gefälschte Mails kommen in der Regel von externen Absenderadressen. Teilweise versuchen sie, als Absender eine interne Absenderadresse vorzugeben. Markiert das Mailprogramm externe Mails, so kann diese Täuschung leichter auffliegen: Eine Mail, die scheinbar von einem Kollegen kommt, aber das Präfix „extern“ trägt, kann den Empfänger stutzig machen und für

größere Vorsicht im Umgang mit dieser Mail sorgen. Ebenso sollte als Absender die E-Mail-Adresse anstatt des E-Mail-Alias angezeigt werden.

Für die Abwehr von Angriffen über E-Mails und insbesondere E-Mail-Anhänge ist eine zentrale Untersuchung des eingehenden E-Mail-Verkehrs auf Schadprogramme erforderlich.

Neben strengen Filterregeln ist auch die Installation eines Virenschutzprogramms auf dem Mailserver ratsam, welches den eingehenden E-Mail-Verkehr auf Schadprogramme durchsucht.

Sichern Sie auch andere Kommunikationsplattformen ab, z. B. Videochat.

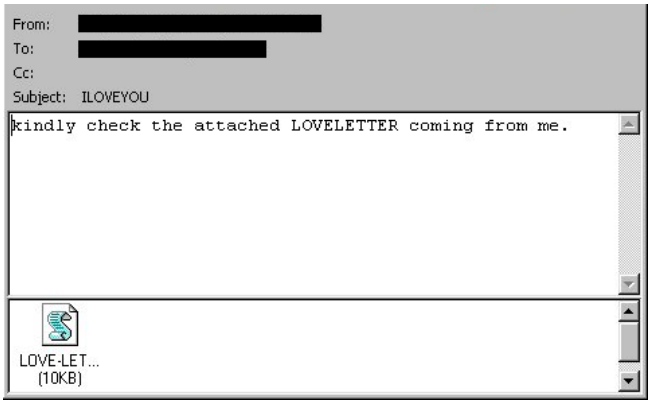
Kommunikationskanäle sind allgemein ein potenzielles Einfallstor für Cyberkriminelle, sei es für Phishing-Versuche, zur Informationsbeschaffung, für Angriffe, die auf sozialer Interaktion beruhen, usw.

Videokonferenzen bieten beispielsweise die Möglichkeit, dass sich Fremde von außerhalb einschalten und mithören. Wer hinter einer ausgeschalteten Kamera sitzt, ist nicht ersichtlich. Die beliebten Screenshots von Videokonferenzen können wertvolle Informationen für Angreifende enthalten: URLs, Meeting-IDs, Namen, Gesichter. Im Falle einer Veröffentlichung sollten diese unkenntlich gemacht werden.

12.3 Exkurs: Kommunikationskanäle absichern

12.3.1 Schadsoftware/Malware

Schadsoftware (Malware) steht für Software, die mit dem Ziel entwickelt wurde, unerwünschte Aktivitäten auf einem Computer meist ohne Kenntnis des Benutzers durchzuführen. Malware wird beispielsweise über Datenträger, E-Mail oder manipulierte Webseiten verbreitet. Malware kann auch in Form eines Makro-Virus in Office-Dokumenten enthalten sein.



Screenshot der ersten Variante des Loveletterwurms.
Quelle: Loveletter-wurm.png, 2024.

Malware nutzt häufig Sicherheitslücken, um den Computer zu „kapern“. Oft werden die Nutzenden mittels Social Engineering zum Ausführen der Malware animiert.

Beispiel: ILOVEYOU-Computerwurm

I-LOVE-YOU (Loveletter) ist ein Computerwurm, der sich im Mai 2000 lawinenartig per E-Mail verbreitete.

Der Wurm agierte in Form eines Kettenbriefs und sorgte für weltweite Störungen in Computernetzwerken und einen Schaden in Milliardenhöhe. Die versendete E-Mail hatte im Betreff den Text „ILOVEYOU“ und als Anhang die Script-Datei LOVE-LETTER-FOR-YOU.TXT.vbs. Nach dem Start (Öffnen des Anhangs) versendete der Wurm eine E-Mail an alle Kontakte des Opfers und zerstörte Dateien auf der Festplatte des Computers.

Der Entwicklers des Wurms war der philippinische Student Onel de Guzmán.

Die folgenden Maßnahmen sind wichtig zum Schutz vor Malware:

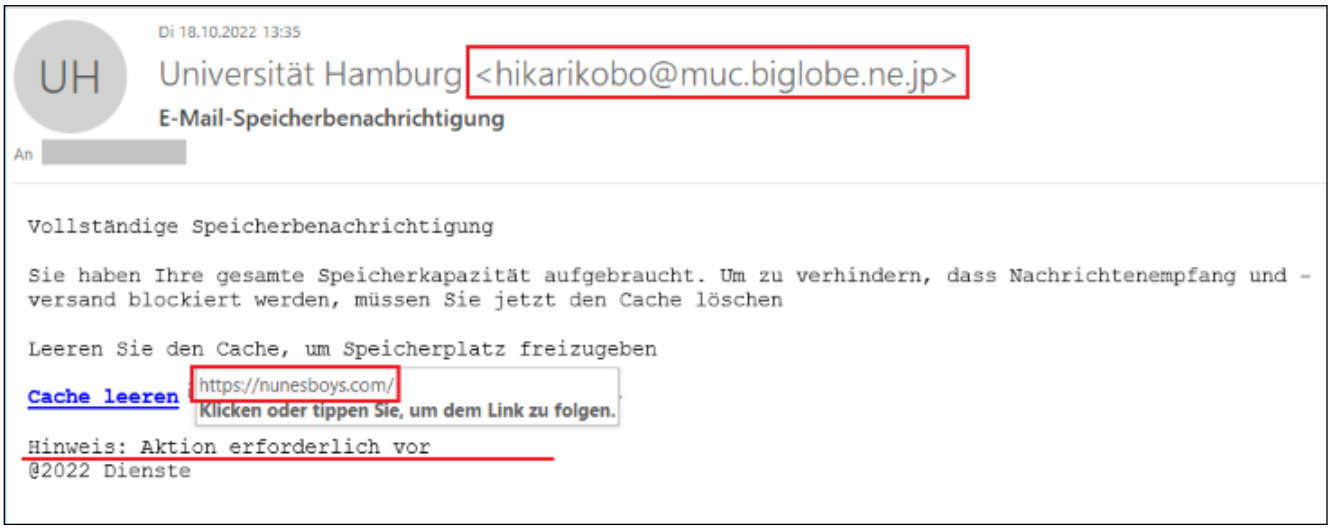
- Einsatz eines namhaften Virenschutzprogramms auf allen Endsystemen und Servern, das seine Virendatenbanken automatisch aktualisiert. Für die Endsysteme (Computer, Laptops usw.) ist die Verwendung der vom Hersteller des Betriebssystems bereitgestellte Antivirenlösung in der Regel zu empfehlen.
- Analyse des eingehenden E-Mail-Verkehrs auf Spam- und Phishing-Mails
- Externe E-Mails explizit als solche kennzeichnen
- Tatsächliche E-Mail-Adresse des Absenders im Mail-Client anzeigen lassen, nicht nur den Anzeigenamen
- Die Ausführung von Makros in Office-Programmen deaktivieren
- Digitale Signaturen in E-Mails einsetzen
- Sensibilisierung der Mitarbeitenden

12.3.2 E-Mail

Anzeigename und Absenderadresse

Es lohnt sich, bei E-Mails besonders genau hinzuschauen, da viele Angriffsversuche hierüber stattfinden (z. B. Phishing, CEO-Fraud). Um den Nutzenden hierbei unter die Arme zu greifen, ist es wichtig, die E-Mail-Clients so zu konfigurieren, dass die Absenderadresse angezeigt wird, nicht nur der Anzeigename.

Stimmt der Anzeigename nicht mit der Mailadresse überein, so kann das ein Anzeichen für eine Phishing-Mail sein. Ist die Absenderadresse unbekannt und deckt sie sich nicht mit dem Inhalt der Nachricht, so kann dies ebenfalls ein Hinweis auf eine gefälschte Mail sein.



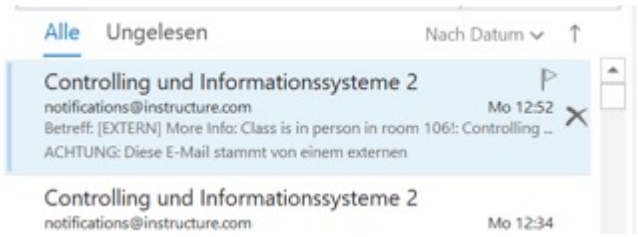
Quelle: Universität Hamburg, 2022.

Es sollte in jedem Unternehmen eine Ansprechperson geben, die bei Zwischenfällen kontaktiert werden kann. Wurde z. B. ein Link in einer Phishing-Mail angeklickt oder spielt der Computer aus anderen Gründen verrückt, so sollte als erste Maßnahme die Netzwerkverbindung getrennt werden (LAN-Kabel ziehen oder/und WLAN-Verbindung ausschalten) und anschließend die Kontaktperson für Sicherheitsvorfälle benachrichtigt werden. Der Aufwand, einen einzelnen Computer neu aufzusetzen oder auch die persönlichen Passwörter zu ändern, ist sehr gering, insbesondere im Vergleich zur Bewältigung eines Angriffs, der im fortgeschrittenen Stadium ganze Teile der IT-Infrastruktur beschädigt und infiziert hat.

Konfiguration von Outlook zur Anzeige der E-Mail-Adresse

Outlook zeigt üblicherweise zu den E-Mails nicht die Absender-Adresse an, sondern nur den Anzeigenamen. Um die Mailadresse zu sehen, muss man mit Mouseover auf den Anzeigenamegehen und das dann erscheinende Menü ausklappen. Um die E-Mail-Adresse standardmäßig anzuzeigen, kann im Reiter „Anzeige“ eine neue Spalte hinzugefügt werden. Diese bekommt z. B. den Namen „E-Mail-Adresse“, als Typ sollte „Formel“ eingestellt werden und die einzutragende Formel lautet: [searchfromemail]. Anschließend noch die Reihenfolge verändern und die neue Spalte z. B. zwischen „von“ und „Betreff“ einsortieren. Zuletzt noch oben die „maximale Anzahl der Zeilen im kom-

primierten Modus“ von 2 auf 3 stellen und mit „OK“ bestätigen. Anschließend wird unter dem Anzeigenamen (Controlling und Informationssysteme 2) die Mailadresse (notifications@instructure.com) zusätzlich angezeigt.



Die ausführliche und bebilderte Anleitung hierzu ist unter folgendem Link zu finden: https://itpcomputersysteme.freshdesk.com/support/solutions/articles/11000096843-im-outlook-die-e-mail-adresse-des-absenders-anzeigen.
Es gibt andere E-Mail-Clients, die diese Thematik von vornherein besser und sicherer lösen. Es kann z. B. der Einsatz von Thunderbird erwogen werden.

Plain-Text-Anzeige

E-Mails enthalten zuweilen grafische Elemente, ausgefallenen Schriften, Bilder und Banner. Diese werden in der Regel nicht direkt mitgeschickt, sondern häufig erst beim Öffnen der Mail von einem Server heruntergeladen. Auf diesem Wege kann auch Malware injiziert werden.
Um das zu verhindern, kann der Anzeigemodus von üblicherweise „HTML“ auf „Nur Text“ geändert werden. Bei Outlook kann das unter Datei → Optionen → Trust Center → Einstellungen für das Trust Center → E-Mail-Sicherheit → Als Nur Text lesen eingestellt werden (Microsoft, 2024).

12.3.3 E-Mail-Server sicher konfigurieren und betreiben

Hierzu ist ggf. die Hinzunahme von fachlich versierter Unterstützung notwendig. Dennoch im Folgenden ein paar Stichworte:

- Der Mailserver darf keine Mails entgegennehmen oder weiterleiten, die nicht für ihn bestimmt sind (Relay-Server). Die internen E-Mail-Server dürfen niemals direkt aus dem Internet erreichbar sein. Nutzen Sie SMTP-Relay-Server („Smarthost“) im Perimeternetzwerk oder bei einem Serviceprovider. Die Verbindung dorthin kann durch IPSec oder SMTPS abgesichert werden (Thimm, 2008).
- Nutzen Sie die Filtermöglichkeiten des Mailsystems aus und richten Sie alle Spam-Schutzfunktionen von der IP-Verbindungsfilterung bis zur Realtime Blackhole List (RBL) ein (Thimm, 2008).
- Richten Sie einen Virenschutz auf dem Mailserver ein.
- Sorgen Sie dafür, dass der eingehende E-Mail-Verkehr auf Spam- und Phishing-Mails untersucht wird.
- Externe E-Mails sollten explizit als solche gekennzeichnet werden, um den Nutzenden eine Stolperstelle zur Erkennung von möglicherweise gefälschten Mails zu bieten.

12.3.4 E-Mail-Verschlüsselung und digitale Signatur

Für den Versand von E-Mails werden unterschiedliche E-Mail-Programme (Clients) verwendet. Die E-Mail-Anbieter nutzen für den Versand der Nachrichten wiederum unterschiedliche Knotenpunkte im Web, an denen die E-Mail navigiert und weitergeleitet wird, bis sie zum empfangenden E-Mail-Programm gelangt. Auf dieser Strecke im – nicht generell verschlüsselten – Internet kann die E-Mail potenziell mitgelesen werden. Um das zu verhindern, sollte die E-Mail verschlüsselt werden. Bei E-Mail-Verschlüsselung gibt es grundsätzlich zwei verschiedene Arten: die Punkt-zu-Punkt- bzw. Transportverschlüsselung und die Ende-zu-Ende-Verschlüsselung.

Transportverschlüsselung

Bei der Transportverschlüsselung wird zwischen dem E-Mail-Programm (Client) und dem E-Mail-Server eine Verbindung aufgebaut und diese z. B. gemäß dem weit verbreiteten Protokoll „Transport Layer Security“ (TLS) verschlüsselt. Dies wird inzwischen von den allermeisten E-Mail-Anbietern unterstützt. Alle Daten, die zwischen dem Client und dem E-Mail-Server ausgetauscht werden, sind damit während des Versands verschlüsselt. E-Mails werden beim Versand allerdings über unterschiedliche Knotenpunkte im Web zwischen den Servern der E-Mail-Anbieter zur Empfängerin oder dem Empfänger weitergeleitet und sind in diesen Punkten nicht verschlüsselt und dazwischen nicht immer. Sowohl beim E-Mail-Anbieter als auch an den Knotenpunkten des Versands liegt die E-Mail im Klartext vor.

Internetkriminelle könnten einen „Man-in-the-Middle-Angriff“ durchführen, der auf diese Punkte ausgerichtet ist. Bei diesem Angriff

platziert sich ein Angreifer „in der Mitte“ der Kommunikation zwischen zwei Kommunikationspartnerinnen oder -partnern und kann ohne deren Wissen Daten (z. B. E-Mails) abfangen, kopieren oder verändern.

Ende-zu-Ende-Verschlüsselung

Im Unterschied zur Transportverschlüsselung werden bei der Ende-zu-Ende-Verschlüsselung nicht die einzelnen Abschnitte des Versandkanals verschlüsselt, sondern die E-Mails selbst. Nur Sender(in) und Empfänger(in) können die E-Mail im Klartext lesen, wenn sie über den notwendigen Schlüssel verfügen. Weder können die beteiligten E-Mail-Anbieter die E-Mail lesen, noch haben potenzielle Angreifer die Möglichkeit, die E-Mails unterwegs zu lesen oder zu manipulieren.

Schlüsselpaare erzeugen und tauschen: Bei dem im Folgenden beschriebenen asymmetrischen Verschlüsselungsverfahren wird ein Paar aus privatem und öffentlichem Schlüssel erzeugt. Dies wird von den meisten E-Mail-Programmen bzw. deren Plug-ins unterstützt. Der private Schlüssel wird nur von dessen Eigentümerin bzw. Eigentümer verwendet und geheimgehalten. Der dazugehörige öffentliche Schlüssel derselben Eigentümerin bzw. desselben Eigentümers wird allen potenziellen Kommunikationspartnern zur Verfügung gestellt. Der öffentliche Schlüssel kann mit einem geöffneten Vorhängeschloss verglichen werden, das von jedermann verschlossen werden kann, sich aber nur von der Besitzerin bzw. dem Besitzer des zugehörigen privaten und geheimen Schlüssels wieder öffnen lässt. Um eine Nachricht sicher zu übermitteln, verschließt die Absenderin oder der Absender die Nachricht mit dem öffentlichen Schlüssel der Empfängerin oder des Empfängers. Diese oder dieser kann die E-Mail dann nur mit dem privaten Schlüssel öffnen und lesen.

Digitale Signatur

Das asymmetrische Verschlüsselungsverfahren kann auch genutzt werden, um die Integrität einer Nachricht sicherzustellen. Dazu wird aus der Nachricht eine Prüfsumme berechnet, die für jede E-Mail eindeutig ist – wie ein Fingerabdruck. Diese Prüfsumme wird mit dem privaten Schlüssel der Absenderin oder des Absenders verschlüsselt und ergibt damit eine digitale Signatur, die mit einer Unterschrift oder einem Siegel verglichen werden kann. Diese Signatur wird an die E-Mail angehängt und verschickt. Die Empfängerin oder der Empfänger entschlüsselt die Signatur mit dem öffentlichen Schlüssel der Senderin oder des Senders und erhält daraus die Prüfsumme der E-Mail. Diese wird mit der zuvor selbst berechneten Prüfsumme verglichen. Stimmen beide Prüfsummen überein, ist sicher, dass die Nachricht unterwegs nicht verfälscht, also die Integrität gewahrt wurde.

Wichtig: Diese Form der Signatur ist nicht zu verwechseln mit einer E-Mail-Signatur, bestehend aus Namen und Webadresse, die an eine E-Mail angehängt werden kann.
Authentizität einer E-Mail: Zum Nachweis, dass ein Dokument wirklich von einer bestimmten Person stammt, wird eine Unterschrift eingesetzt. Damit ist dessen Authentizität bewiesen. Ähnlich kann eine E-Mail mit einer digitalen Unterschrift signiert werden, wie im vorangegangenen Abschnitt zur Integrität beschrieben. Wird das erzeugte Schlüsselpaar einer Besitzerin oder eines Besitzers zusätzlich formell und nachweislich mit einer E-Mail-Adresse verknüpft, ist bei erfolgreicher Integritätsprüfung der Signatur außerdem sichergestellt, dass die Nachricht tatsächlich von der E-Mail-Adresse kommt, zu der das Schlüsselpaar gehört. Auf diese Weise kann auch die Authentizität der Absenderin bzw. des Absenders gewährleistet werden. Somit entspricht eine verschlüsselte und signierte E-Mail einem zugeklebten und versiegelten Brief (BSI, 2024b).

13. Basismaßnahme 7: Notfallplan erstellen

13.1 Begründung

Cyberangriffe laufen inzwischen breit gestreut und oftmals auch weitgehend automatisiert ab. Da zudem die Fallzahlen immer weiter zugenommen haben und auf einem sehr hohen Niveau liegen, stellt sich nicht mehr die Frage, „ob“ ein Unternehmen angegriffen wird, sondern nur noch, „wann“. Um sich auf diesen absehbaren Ernstfall vorzubereiten, ist eine gründliche Notfallplanung unerlässlich. Eine sorgfältige, umfassende, eingeübte, aktualisierte Notfallplanung erleichtert die Bewältigung von Cybersicherheitsvorfällen. Rettungsmaßnahmen, externe Ansprechpersonen zur Unterstützung im Notfall, fortlaufender Geschäftsbetrieb durch redundante Kommunikationssysteme sowie funktionsfähige Backups sind ein paar der Eckpfeiler, die im Ernstfall den Wiederaufbau im Schadensfall wesentlich erleichtern.

13.2 Maßnahmen

Abschnitt 1: Verantwortlichkeiten festlegen

Ihre Planung muss folgende Aspekte umfassen: Definition der technischen und organisatorischen Rollen, Klärung von Verantwortlichkeiten jedes Einzelnen, Festlegung von Zuständigkeiten und die Einbeziehung externer Dienstleister.

Und ...

Bestimmen Sie Beauftragte für die in einem Notfall erforderlichen Aufgabenbereiche (Notfallteam). Eine Konzentration vieler Zuständigkeiten in einer Rolle ist zu vermeiden.

Ein wichtiger erster Schritt für die Notfallplanung ist die Festlegung der Verantwortlichkeiten:

- Welche technischen und organisatorischen Rollen werden gebraucht und wer übernimmt diese im Ernstfall?
- Welche Verantwortlichkeiten kommen jeder und jedem Einzelnen zu?
- Wer ist wofür zuständig?
- Für welche Aufgaben muss ein Dienstleister hinzugezogen werden? Mit welcher Reaktionszeit des Dienstleisters kann im Ernstfall gerechnet werden?

Für die hierbei definierten notwendigen Aufgabenbereiche müssen Beauftragte definiert werden. Dabei ist zu vermeiden, dass sich viele Rollen auf eine Person konzentrieren.

Abschnitt 2: Notfallplan erstellen

Fertigen Sie eine Liste mit allen Ansprechpersonen an und treffen Sie Vorabsprachen mit diesen. Ein Kommunikationsplan sollte auch Handynummern eines Notfallteams und beispielsweise eine eigene Notfall-E-Mail-Erreichbarkeit enthalten, da betriebliche Festnetztelefone und E-Mail-Konten bei Cyberangriffen oft auch betroffen und nicht funktionsfähig sind. Denken Sie außerdem an Kundenadressen.

Als erster Schritt sollte beispielsweise die Notfallkarte des BSI https://sl.csc-kmu.de/b7-02.html ausgefüllt und an mehreren Stellen sichtbar ausgehängt werden. Durch regelmäßige Ansprache sollte jeder Mitarbeitende, der in irgendeiner Weise mit PC-Arbeit zu tun hat, sei es in der Produktion oder Verwaltung, darüber informiert sein.

In einem Notfallplan werden Leitlinien, Rollen und Zuständigkeiten für eine zeitnahe, professionelle und angemessene Reaktion auf alle Sicherheitsvorfälle dokumentiert.

Der Notfallplan muss eine Liste mit allen Ansprechpersonen enthalten, die zudem über ihre Rolle Bescheid wissen. Hier sind Absprachen von großer Bedeutung. Dieser Kommunikationsplan sollte auch Handynummern und beispielsweise eine eigene Notfall-E-Mail-Erreichbarkeit enthalten. Betriebliche Festnetznummern und E-Mail-Konten sind bei einem großen Cyberangriff oftmals mitbetroffen und stehen womöglich nicht zur Verfügung. Zudem sollten auch die wichtigsten Kunden mit Adresse und Erreichbarkeit mitbedacht werden, die im Ernstfall informiert oder kontaktiert werden müssen.

Erstellen Sie einen Notfallplan (Vorfallreaktionsplan), der auflistet, was in der jeweiligen Situation zu tun ist, um so schnell wie möglich wieder handlungsfähig zu sein. Der Notfallplan sollte Kontaktdaten von zu informierenden externen Stellen und bestehende Meldepflichten enthalten (z. B. § 33 DSGVO – möglichst binnen 72 Std.).

Und ...

Dokumentieren Sie Leitlinien, Rollen und Zuständigkeiten für eine zeitnahe, professionelle und angemessene Reaktion auf alle Sicherheitsvorfälle.

Es sind Vorbereitungen zu treffen, um ad hoc einen Krisenstab aufrufen zu können, bei dem alle Teilnehmenden über die eigene Rolle und Aufgabe Bescheid wissen. Zudem sollten Räumlichkeiten und Logistik für den Notfall und die Tätigkeit des Krisenstabes zur Verfügung stehen.

Der Notfallplan sollte ebenfalls die Kontaktdaten von zu informierenden externen Stellen und Informationen zu bestehenden Meldepflichten enthalten (z. B. die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, innerhalb von 72 Stunden, nach § 33 DSGVO).

Dieser zu erstellende Notfallplan, auch Vorfallreaktionsplan genannt, muss zudem auflisten, was getan werden muss, um möglichst schnell wieder handlungsfähig zu sein.
Es gibt hierzu umfangreiche Anleitungen und Vorlagen des BSI und der CSBW:

- BSI – Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle https://sl.csc-kmu.de/b7-01.html
- BSI – IT-Notfallkarte: Verhalten bei IT-Notfällen https://sl.csc-kmu.de/b7-02.html
- BSI – Top-12-Maßnahmen bei Cyberangriffen https://sl.csc-kmu.de/b7-03.html
- CSBW – Factsheet: Erste Hilfe bei einem Cybernotfall https://sl.csc-kmu.de/b7-04.html
- IHK München und Oberbayern: Muster: IT-Notfallplan: https://www.ihk-muenchen.de/de/Service/Digitalisierung/Informationssicherheit/Muster-IT-Notfallplan/#st_text_picture_3

Es gibt auch Notfallrufnummern, die eine erste Orientierung im Angriffsfall bieten können:

- Die Cyber-Ersthilfe der CSBW mit Zuständigkeit in Baden-Württemberg: 0711-137-99999
- Die Nummer der zentralen Ansprechstelle Cybercrime beim LKA BW: 0711-5401-2444

Abschnitt 3: Üben und bereithalten

Halten Sie den Notfallplan und die Kommunikationslisten physisch (ausgedruckt) bereit, damit diese den Beschäftigten auch bei einem IT-Ausfall zur Verfügung stehen.

Denn die beste Notfallplanung nutzt nichts, wenn sie auf einem Laufwerk liegt, auf welches aufgrund des Cyberangriffs nicht mehr zugegriffen werden kann.

Führen Sie regelmäßig Übungen durch, damit Sie im Ernstfall schnell und richtig reagieren können.

Eine gute Notfallplanung entfaltet ihre Wirkung erst dann, wenn sie durch regelmäßige Übungen im Unternehmen bekannt ist. Diese Übungen sollten so intensiv sein und in einer solchen Frequenz stattfinden, dass alle Verantwortlichen sich ihrer Rollen bewusst sind und auch die jeweiligen Aufgaben gut geübt wurden. Diese Vorbereitung hilft, im Ernstfall schnell und richtig reagieren zu können.

Insgesamt trägt ein funktionierendes Notfallmanagement, verbunden mit guter Dokumentation und Inventarisierung des IT-Systems mit Hard- und Software des Unternehmens, mit Netzwerkplänen usw., dazu bei, dass im Falle einer erfolgreichen Cyberattacke die Chaosphase und damit der Schaden deutlich reduziert werden kann.

14. Basismaßnahme 8:
Inventarisieren und dokumentieren

14.1 Begründung

Um sich adäquat zu schützen, muss jedes Unternehmen seine Hard- und Software sowie die Daten und die Verarbeitungsprozesse inventarisieren, welche die Grundlage seiner Informationswerte bilden und zum Fortbestand des Unternehmens beitragen:

Um zu wissen, was man schützen muss, muss man wissen, was man hat.
Außerdem sind eine Inventarisierung und ein Netzplan für Fachleute (z. B. aus der Forensik) sehr nützlich, die im Falle einer Cyberattacke Maßnahmen zum Erhalt der eigenen IT-Systeme einleiten sollen.

14.2 Maßnahmen

Die Inventarisierung und Dokumentation der IT-Systeme des Unternehmens ist die Grundlage für viele Sicherheitsmaßnahmen.
Im Rahmen der Inventarisierung sollten Sie die folgenden Aspekte berücksichtigen:

- Dokumentieren Sie alle verwendeten Hardwarekomponenten.
- Dokumentieren Sie alle eingesetzte Software.
- Dokumentieren Sie alle für den Geschäftsbetrieb wichtigen Daten, einschließlich deren Speicherort.
- Dokumentieren Sie alle Zugriffsrechte.
- Dokumentieren Sie alle IT-Verbindungen mit der Außenwelt.

Durch eine unvollständige Dokumentation entstehen weiße Flecken in der IT-Landschaft. Konsequenz: Die nicht dokumentierten Komponenten werden bei Sicherheitsanalysen nicht berücksichtigt und auch nicht gewartet und aktualisiert.

Klären Sie anhand der Inventarisierung die Frage, ob die erhobene Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist.

Dieser Prozess der Dokumentation bietet zudem die Gelegenheit, die Vielfalt und Komplexität der eingesetzten Systeme zu bewerten. Es sollte dabei geklärt werden, ob die vorliegende Vielfalt an Systemen sicherheitstechnisch und administrativ beherrschbar ist. Der Nutzwert zusätzlicher Systeme kann auch durch die Vergrößerung der Angriffsfläche gemindert werden, sodass das Gesamtsystem und seine Sicherheit stets mitbedacht werden sollten.

Erstellen Sie einen Netzwerkplan.

So wie die Dokumentation aller weiteren oben genannten Aspekte des Firmennetzes ist auch der Netzwerkplan eine Hilfe. Er hilft im Ernstfall bei der Fehlersuche und Koordination der sichernden Maßnahmen. Aber auch für Fragen der Netzsegmentierung und zur Absicherung mittels Firewalls (siehe Beratungskarte 5) ist ein Netzwerkplan unerlässlich.

Halten Sie die oben genannten Dokumentationen und den Netzwerkplan stets auf dem aktuellen Stand und als physische Kopie (Ausdruck) vor.

Die hier beschriebene Dokumentation sollte an einem sicheren Ort auch als physische Kopie vorliegen, da zentrale IT-Systeme im Angriffsfall möglicherweise nicht mehr zur Verfügung stehen.

Die Inventarisierung und Dokumentationen der IT-Systeme müssen regelmäßig aktualisiert werden.

15. Zusatzkarte:
Weitere Themen

15.1 Begründung

Auf den Karten 1–8 werden die wichtigsten Themen für angemessene Cybersicherheit abgebildet. Diese bieten einen guten Einstieg. Dennoch gibt es zusätzliche Themen, die ohne klare Zuordenbarkeit zu den 8 Themen ebenso von großer Wichtigkeit sind. Diese sind in der Zusatzkarte „Weitere Themen“ enthalten. So kommt seit COVID-19 mobiler Arbeit und der Arbeit im Homeoffice eine wesentlich größere Bedeutung zu und auch das Thema Cyberversicherung gewinnt an Bedeutung. Verschiedene weitere Themen wie z. B. Cloud-basierte Lösungen sind je nach Arbeitsweise und Struktur der einzelnen KMU von Bedeutung.

15.2 Maßnahmen

Abschnitt 1: Homeoffice und mobiles Arbeiten: Organisatorisches

Legen Sie die Verhaltensregeln für Homeoffice und mobiles Arbeiten verbindlich fest, z. B. in der IT-Sicherheitsrichtlinie (siehe Einstiegskarte: Cybersicherheit ist Führungsaufgabe).

Die Möglichkeiten mobilen Arbeitens und der Arbeit aus dem Homeoffice sind heute in vielen Bereichen nicht mehr wegzudenken. Zugleich erhöht das Remote-Arbeiten die Angriffsfläche auf das Firmennetz. Es lohnt sich deshalb, dem Thema die notwendige Aufmerksamkeit zu schenken und es organisatorisch sauber aufzusetzen. Dazu gehört beispielsweise, dass die Verhaltensregeln für Homeoffice und mobiles Arbeiten verbindlich und transparent festgelegt werden. Hierfür eignet sich die IT-Sicherheitsrichtlinie, deren Erstellung in der Einstiegskarte „Cybersicherheit ist Führungsaufgabe“ empfohlen und beschrieben wird.

Regeln Sie den Umgang mit betrieblichen Dateien und Dokumenten außerhalb des Firmengeländes.

Auch im Bereich der Informationssicherheit führt das mobile Arbeiten zu einer größeren Angriffsfläche. Um die Abgrenzung zwischen privater Umgebung/privaten Geräten und beruflicher Umgebung/beruflichen Geräten klar zu ziehen, sollte auch für den Umgang mit betrieblichen Dateien und Dokumenten der Umgang außerhalb des Firmengeländes klar geregelt werden.

Verschlüsseln Sie alle Geräte und Datenträger, die für den mobilen Einsatz vorgesehen sind (Laptops, Smartphones, Tablets, Wechselfestplatten, USB-Sticks etc.).

Mobile Geräte unterliegen einem hohen Verlust- und Diebstahlrisiko. Um die Cyber- und Informationssicherheitsgefahren, die von abhandengekommenen oder entwendeten Geräten für das Firmennetz und die betriebliche Informationssicherheit ausgehen, zu minimieren, sollten die Geräte und Datenträger alle verschlüsselt werden.

Planen Sie Vorkehrungen und Prozesse für den Verlust oder den Ausfall mobiler Geräte ein. Geräte sollten aus der Ferne gesperrt und gelöscht werden können. Halten Sie Ersatzgeräte bereit.

Neben der Verschlüsselung sollten mobile Geräte auch aus der Ferne gesperrt und gelöscht werden können. Um einen reibungslosen Betriebsablauf zu gewährleisten, lohnt es sich, ggf. Ersatzgeräte vorzuhalten.

Stellen Sie sicher, dass der Zugriff auf das Unternehmensnetzwerk von außen nur über gesicherte Verbindungen möglich ist, z. B. VPN (siehe Basismaßnahme 5).

Für die mobile Arbeit und die Arbeit im Homeoffice ist der Zugriff auf das Firmennetzwerk oftmals unerlässlich. Zu diesem sollte es jedoch keine offenen Schnittstellen geben. Der Zugriff sollte nur über gesicherte Verbindungen möglich sein wie beispielsweise VPN, welches im Kapitel zur Beratungskarte 5 näher beschrieben wird.

Abschnitt 2: Homeoffice und mobiles Arbeiten: Verhaltensregeln

In diesem Abschnitt werden konkrete Verhaltensregeln aufgelistet, die im Bereich mobiles Arbeiten anzuraten sind. Die Festlegung der konkreten Verhaltensregeln wurde bereits eingangs empfohlen, beispielsweise in der IT-Sicherheitsrichtlinie. Die Verhaltensregeln sind wie folgt:

Sperren Sie Geräte wie PCs oder Bediendisplays beim Verlassen des Arbeitsplatzes. Aktivieren Sie die automatische Sperrung auf allen Geräten.

Und ...

Lassen Sie sensible Dokumente nicht unbeaufsichtigt liegen. Lassen Sie Laptops und Smartphones nie unbeaufsichtigt.

Und ...

Bewahren Sie vertrauliche Dokumente und Datenträger in einem verschließbaren Behältnis (z. B. Rollcontainer, Aktenschrank) auf.

Und ...

Stellen Sie sicher, dass dienstliche Geräte ausschließlich von den berechtigten Personen genutzt werden.

Und ...

Übertragen Sie im mobilen Einsatz entstandene Daten (Fotos usw.) zeitnah an Datenspeicher des Unternehmens, um Datenverluste zu vermeiden.

Und ...

Verwenden Sie eine Sichtschutzfolie für Displays, wenn Sie in öffentlichen Räumen arbeiten.

Und ...

Verwenden Sie niemals USB-Sticks, die Sie geschenkt bekommen.

Von mobilen Speichern gehen erhebliche Infektionsrisiken durch Viren und Würmer aus. Das kann unbeabsichtigt sein, wenn ein Speichergerät zuvor an einem infizierten Computer angeschlossen war, wird aber auch für gezielte Angriffe genutzt. Generell ist von der Nutzung fremder USB-Sticks abzuraten.

Untersagen Sie den Anschluss von Geräten Dritter an Ihre eigenen Geräte (USB-Sticks, Presenter, USB-Ladekabel etc.).

Das eben genannte Infektionsrisiko kann auch von anderen USB-Devices ausgehen, denen auf den ersten Blick nicht mal Datenträgereigenschaften zugeordnet werden. Die technische Entwicklung ermöglicht mittlerweile kleinste Datenspeicher, die sich unbemerkt in USB-Ladekabel integrieren lassen und die dann zur Übertragung von Malware genutzt werden können.

Achten Sie bei der Nutzung eines fremden Computers darauf, dass dort keine Zugangsdaten von Ihnen gespeichert werden.

Dieser Punkt ist eigentlich selbsterklärend. Im Falle der Speicherung von persönlichen Zugangsdaten auf einem fremden Rechner ermöglicht das den sonstigen Nutzenden dieses Rechners den Zugriff auf den entsprechenden Account/Zugang. Zusätzlich ist die Nutzung eines fremden Rechners mit der Gefahr behaftet, dass möglicherweise dort installierte Keylogger alle Tastatureingaben mitschreiben, wodurch verwendete Zugangsdaten ebenfalls preisgegeben werden.

Abschnitt 3: Physische IT-Sicherheit

Richten Sie Zugangskontrollen für Serverräume, Schaltschränke usw. ein.

Auch wenn die größten Gefahren im Bereich der Cybersicherheit von ungezielten Massenangriffen ausgehen, gibt es dennoch auch gezielte Angriffe, sowohl im Bereich Cyberkriminalität

als auch im Bereich Spionage und Wirtschaftskriminalität. In diesen Fällen kann es durchaus passieren, dass beispielsweise als IT-Servicekraft getarnte Angreifende sich Zugang zum Firmennetz verschaffen, indem sie in das Firmengelände eindringen und im Falle des Zugangs zu Serverräumen und Schaltschränken usw. durchaus gute Erfolgschancen haben, Zugriff zu erlangen, Schadsoftware einzuschleusen und Daten abzugreifen. Der physische Schutz der IT-Infrastruktur durch abgeschlossene Türen, verschlossene Fenster, wirksame Zugangskontrollen, vor fremdem Zugriff geschützte Passwörter, verschlossen gelagerte sensible Dokumente usw. ist auch für angemessene Cybersicherheit nicht zu vernachlässigen.

Löschen Sie Datenträger vor der Ausmusterung auf sichere Art und Weise. Beachten Sie hierzu die Hinweise des BSI: https://sl.csc-kmu.de/zk-04.html

Auf ausgemusterten Datenträgern können sich noch sensible Informationen befinden, die sich auch nach vollständigem Formatieren oft problemlos wiederherstellen lassen. Bei der normalen Formatierung, der sogenannten High-Level-Formatierung, wird lediglich die Dateisystemstruktur neu angelegt; also das komplette Inhaltsverzeichnis gelöscht und durch ein neues ersetzt. Auch hier liegen die digitalen Daten noch auf dem Datenträger vor (BSI, 2024c). Das Stichwort hierbei ist: Daten einfach oder mehrfach überschreiben. Es gibt spezielle Programme, die diese Funktionalität anbieten.

Vernichten Sie Unterlagen und Datenträger mit vertraulichen oder personenbezogenen Inhalten nach deren Nutzung auf die vorgeschriebene Art und Weise.

Im Umgang mit vertraulichen und personenbezogenen Daten ist allgemein zu großer Sorgfalt zu raten. So sind auch entsprechende Unterlagen nach deren Nutzung auf sichere Art und Weise zu vernichten.

Lassen Sie Service-Personal nie unbeaufsichtigt in die Firmenräume.

Gezielte Angriffe im Bereich Social Engineering können leicht durch als Servicepersonal getarnte Angreifende erfolgen. Es ist ratsam, insbesondere unbekanntes Servicepersonal bei seinem Aufenthalt in den Firmenräumen stets zu beaufsichtigen.

Bewahren Sie Ausdrucke von wichtigen Dokumenten an einem sicheren Ort auf (z. B. Zugangsdaten, Notfallpläne, Serviceverträge, Kontaktdaten von Dienstleistern).

Da im Falle eines Cyberangriffs die Server und Rechner ausgefallen sein können, sind wichtige Dokumente stets auch in ausgedruckter Form vorzuhalten. Damit diese Dokumente vor unbefugtem Zugriff geschützt sind, müssen sie an einem sicheren Ort aufbewahrt werden. Bedenken Sie zudem, dass ein sicherer Aufbewahrungsort auch Gefahren z. B. durch Feuer oder Wasser ausgesetzt ist, sodass auch hier mit einem gewissen Verlustrisiko kalkuliert werden muss.

Abschnitt 4: Cloud-basierte Lösungen

Für die sichere Nutzung von Cloud-Diensten gelten dieselben Empfehlungen wie für die Absicherung der lokalen IT-Infrastruktur.

Auch wenn die Software, der Datenspeicher oder andere Funktionen per Cloud zur Verfügung gestellt werden, gelten dennoch dieselben Empfehlungen wie für die Absicherung der lokalen Infrastruktur (Sicherheitslücken schließen, Benutzerzugänge absichern, Datensicherung durchführen, Gefahrenbewusstsein schaffen, Netzübergänge absichern, Schadprogramme abwehren, Notfallplan erstellen, inventarisieren und dokumentieren).

Planen Sie den Weg in die Cloud sorgfältig. Bedenken Sie von Anfang an auch den Weg aus der Cloud heraus, um nicht zu stark von einem Cloud-Anbieter abhängig zu werden.

Und ...

Machen Sie sich mit den Risiken vertraut, die die Nutzung von Cloud-Computing mit sich bringt.

Und ...

Erstellen Sie eine Cloud-Strategie. Diese muss die Ziele enthalten, die mittels Cloud-Computing erreicht werden sollen.

Und ...

Beachten Sie die Hinweise des BSI zum Thema „Sichere Nutzung von Cloud-Diensten“: https://sl.csc-kmu.de/zk-05.html

Am Anfang sollte die Auseinandersetzung mit der eigenen Cloud-Strategie stehen. Hierbei müssen die Ziele geklärt werden, die mittels Cloud-Computing erreicht werden sollen. Der Weg in die Cloud muss sorgfältig geplant werden. Dabei sollte auch der Weg aus der Cloud heraus mitbedacht werden, um nicht zu stark von einem Cloud-Anbieter abhängig zu werden.

Schlussendlich sollte man sich mit den Risiken vertraut machen, die die Nutzung von Cloud-Computing mit sich bringt. Hierzu gibt es z. B. vom BSI Hinweise, die unter folgendem Link aufgerufen werden können:
https://sl.csc-kmu.de/zk-05.html

Abschnitt 5: Cyberversicherungen

Entwickeln Sie ein Risikobewusstsein für Cyberangriffe und bewerten Sie dieses für Ihr Unternehmen. Prüfen Sie, ob und in welchem Umfang eine Versicherung hilfreich und notwendig ist.

Von manchen Versicherern werden spezielle Cyberversicherungen angeboten, die bei der Bewältigung von Cyberangriffen unterstützen sollen. Ob sich der Abschluss einer solchen Police lohnt, muss im Einzelfall abgewogen werden. Hierfür muss im Unternehmen ein Bewusstsein für das Risiko von Cyberangriffen in Bezug auf das jeweilige Unternehmen entwickelt werden. Darauf aufbauend kann entschieden werden, ob und in welchem Umfang eine Versicherung hilfreich und notwendig ist.

Prüfen Sie, ob sich die jeweiligen Versicherungsklauseln in herkömmliche Versicherungsverträge aufnehmen lassen oder ob eine spezielle Cyberversicherungspolice infrage kommt.

Zuweilen lassen sich die jeweiligen Versicherungsklauseln auch in herkömmliche Versicherungsverträge mit aufnehmen. Zur Frage von Notwendigkeit und Umfang sollte neben den Gesprächen mit den Versicherern auch unabhängige Expertise eingeholt werden.

Beachten Sie, dass Sie nach Abschluss einer solchen Versicherung stets für die Einhaltung der vertraglich vereinbarten Voraussetzungen Sorge tragen müssen, um den vollständigen Versicherungsschutz nicht zu verlieren.

Zu beachten ist schlussendlich, dass das Unternehmen nach Abschluss einer solchen Versicherung stets für die Einhaltung der vertraglich vereinbarten Voraussetzungen Sorge tragen muss, um den vollständigen Versicherungsschutz nicht zu verlieren. Wenn eine Cyberversicherung abgeschlossen wurde, aber nicht alle vertraglich vereinbarten Sicherheitsmaßnahmen umgesetzt wurden, bietet das dem Versicherer Ansatzpunkte, die Regulierung von Schäden abzulehnen. Zur Klärung dieser Fragen kann er auch den Rechtsweg bemühen, wofür er insbesondere bei großen Schadenssummen infolge schwerwiegender Cyberangriffe einen Anreiz hat. Nicht jedes Unternehmen hat die Ressourcen, einen solchen oft langwierigen Prozess durchzustehen.

16. Abwehr von Ransomware-Angriffen

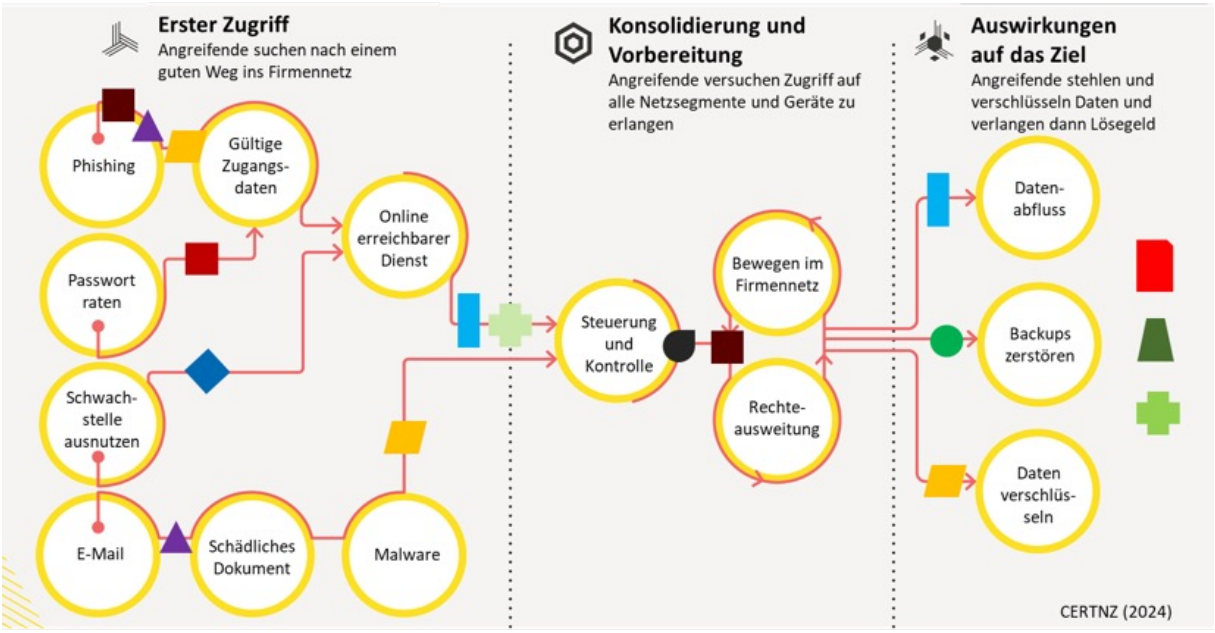
Nachdem nun alle Maßnahmen erläutert wurden, geht es im Folgenden noch mal um das Schema eines Ransomware-Angriffs (siehe Abbildung 17). Darin sind nun die Stellen markiert, an denen die einzelnen Maßnahmen ansetzen und einen Ransomware-Angriff vereiteln oder erschweren können.

Im Bereich des Erstzugriffs tragen zahlreiche Maßnahmen zur Senkung der Cyberrisiken bei: Zur Vereitelung von Phishing-Angriffen helfen beispielsweise die Absicherung von Benutzerzugängen mittels Zwei-Faktor-Authentifizierung, gut geschulte und sensibilisierte Mitarbeitende und die Absicherung von Kommunikationswegen, beispielsweise mittels Spam-Filtern. Gegen das Erraten von Passwörtern helfen ausreichend sichere Passwörter. Ein gutes Update-Management, das zu stets aktueller Software und aktuellen Systemen führt, erschwert das Ausnutzen offener Sicherheitslücken. Gegen E-Mails mit schadhaften Anhängen helfen einerseits gut geschulte und wachsame E-Mail-Nutzende und andererseits auch weitere Stufen zur Abwehr von Malware wie die Installation von Virenscannern auf Servern und Endgeräten und die Deaktivierung aktiver Elemente wie Makros durch die Verwendung sicherer Darstellungsoptionen für Dokumente. Die Angriffsfläche durch online erreichbare Dienste lässt sich ebenfalls verringern, beispielsweise indem nur verschlüsselte Zugriffe von außen auf das Unternehmensnetz zugelassen werden, z. B. mittels VPN aus dem Homeoffice oder beim mobilen Arbeiten.

In die Phase der Konsolidierung und Vorbereitung von Ransomware-Angriffen hinein wirken beispielsweise Maßnahmen der Netzwerkarchitektur und -absicherung wie eine gute Netzsegmentierung und die Absicherung aller Übergänge mittels Firewall. Diese Maßnahmen erschweren die Steuerung und Kontrolle online erreichbarer Dienste sowie das Bewegen im Firmennetz. Ein klares Berechtigungskonzept, das dem Prinzip der minimal notwendigen Rechte folgt und insbesondere administrative Rechte sehr zurückhaltend erteilt, kann ebenfalls der Steuerung und Kontrolle durch Angreifende entgegenwirken. Gut abgesicherte Benutzerzugänge mit sicheren Passwörtern und möglichst einer Zwei-Faktor-Absicherung bremst ebenfalls die Rechteausweitung.

Auch die Auswirkungen eines Ransomware-Angriffs können durch Maßnahmen gemildert werden. Die Absicherung des Netzwerks mittels Firewall kann, je nach Konfiguration, den Abfluss großer Datenmengen verhindern. Aktuelle, vollständige und funktionsfähige Backups können dem Datenverlust durch Verschlüsselung etwas entgegensetzen. Das Aufbewahren einer Kopie der Daten abgetrennt vom Netzwerk und ohne Möglichkeit zum Zugriff aus dem Internet kann der Zerstörung von Backups entgegenwirken. Der Betrieb von Virenschutzprogrammen und weiteren Schutzsystemen kann möglicherweise der Einschleusung und Ausführung des Verschlüsselungstrojaners entgegenwirken. Zusätzlich hilft ein gut ausgearbeiteter, ausgedruckt bereitliegender und eingeübter Notfallplan bei der Bewältigung eines Ransomware-Vorfalls. Eine gute Inventarisierung und Dokumentation erleichtert das Einleiten von Gegenmaßnahmen und den Wiederaufbau der Systeme. Eine Cyberversicherung kann im Ernstfall hilfreich sein zur Übernahme von Lösegeldforderungen und Kosten durch Ausfall und Wiederherstellung.

Das Fazit ist: Die Umsetzung aller empfohlenen Maßnahmen wirkt auch gegen Ransomware.



	Einstiegskarte: IT-Sicherheitsrichtlinie, Berechtigungskonzept
	B1: Sicherheitslücken schließen
	B2, Abschnitt 2: Passwortsicherheit
	B2, Abschnitte 1, 3: Benutzerzugänge absichern, Zwei-Faktor-Authentitifizierung
	B3: Datensicherungen durchführen
	B4: Gefahrenbewusstsein schaffen
	B5: Netzübergänge absichern: Netzsegmentierung und Firewall
	B6: Schadprogramme abwehren: Virenschutzprogramme verwenden, Makros deaktivieren, Kommunikationswege absichern
	B7: Notfallplan erstellen, bereithalten
	B8: Inventarisieren und dokumentieren
	ZK: Homeoffice, mobiles Arbeiten
	ZK: Cyberversicherungen

Abbildung 17: Die üblichen Angriffspfade bei einem von Menschen gesteuerten Ransomware-Vorfall (certnz, 2024), übersetzt ins Deutsche, und darin eingezeichnet die Absicherungsmaßnahmen des CSC für KMU und ihre Ansatzpunkte.

17. Hintergrund-informationen

Cybersicherheit ist ein Thema von großer Bedeutung. Immer mehr Organisationen und Privatpersonen sind von Cyberangriffen betroffen, teils mit erheblichen Auswirkungen. Zugleich sind kleine und mittlere Unternehmen (KMU) in diesem Bereich oft schlecht aufgestellt. Um dieses Problem anzugehen, setzte das Innenministerium Baden-Württemberg zusammen mit der Hochschule Aalen ein Forschungsprojekt auf, welches unter dem Namen CyberWuP von 2022 bis 2024 an der Hochschule Aalen durchgeführt wurde. Zusammen mit zahlreichen Partnern wurde in diesem Projekt unter anderem ein Beratungskonzept zur niederschwelligen Cybersicherheitserstberatung von KMU entwickelt (CSC für KMU). Die IHK Ostwürttemberg hat als Praxispartner die Entwicklung maßgeblich unterstützt. Sie sorgte auch als erster Multiplikator dafür, dass nach Abschluss der Entwicklung diese Beratung als Beratungsangebot der baden-württembergischen IHKen kostenlos für KMU angeboten wird. Daneben gibt es weitere Multiplikatoren, die diese Beratung anbieten oder anbieten werden.

Aufbauend auf Publikationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Europäischen Cybersicherheitsagentur (ENISA) wurde zusammen mit Experten für Cybersicherheit und für KMU im Bereich der Praxisforschung in vielen Workshops diese Beratung entwickelt. Neben dem Zusammentragen und Gliedern der relevanten Themen lag der Fokus auf der Komplexitätsreduktion, um einen Umfang zu erreichen, der sich in einer Stunde Beratung bewältigen lässt, natürlich mit dem Anspruch, nichts Wichtiges wegzulassen (siehe Abbildung 18). Die zeitgleich betriebene empirische Forschung zur Situation der KMU in Bezug auf Cybersicherheit stand beratend zur Seite.

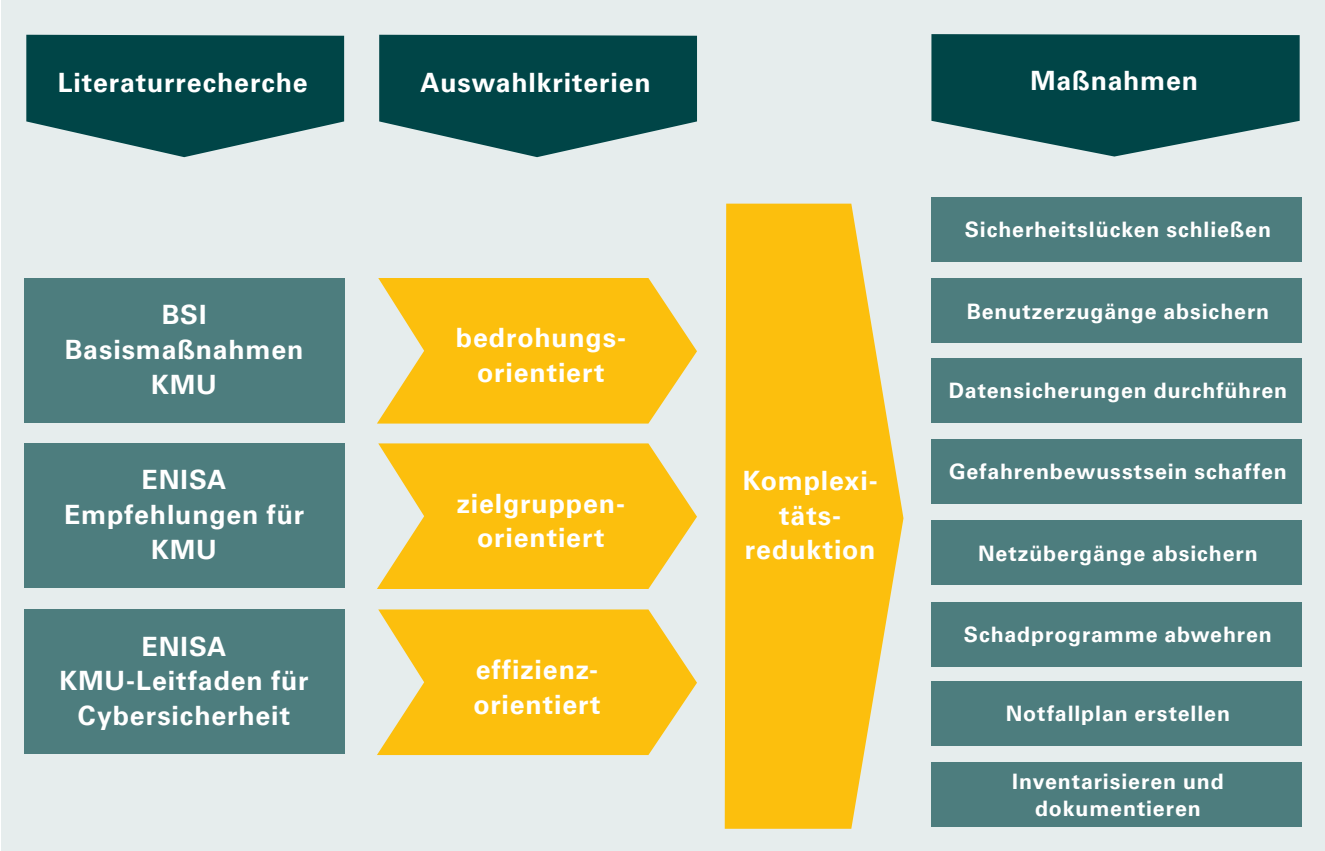


Abbildung 18: In der Entwicklung des Beratungskonzepts des CSC für KMU wurde ein starker Fokus auf die Komplexitätsreduktion gelegt.

Das auf diese Weise entwickelte Beratungskonzept wurde anschließend getestet und pilotiert. In zwei Phasen wurden insgesamt über 60 Beratungen in KMU durchgeführt und evaluiert. Die Ergebnisse flossen in zwei Schleifen in das Beratungskonzept mit ein. Mit Abschluss des Forschungsprojekts liegt ein funktionierendes und getestetes Beratungskonzept im Multiplikatorenmodell vor, welches zur Verbesserung der Cybersicherheit in KMU beitragen kann (CSC für KMU). Die Cybersicherheitsagentur Baden-Württemberg (CSBW) verwaltet und betreut dieses Beratungskonzept, insbesondere mit Blick auf die Multiplikatoren, welche diese Beratung anbieten oder anbieten wollen. Eine Website bietet Zugriff auf die Beratungsunterlagen (www.csc-kmu.de). Dort kann auch die Checkliste als interaktiver Online-Check ausgefüllt werden. Der Durchgang durch die Checkliste bildet den Einstieg in die Beratung. Im Anschluss bietet der Online-Check einen Bericht mit der grafischen Auswertung der Ergebnisse zum Download an.

Zur Zitation: Die Beratungsunterlagen des CSC enthalten Passagen und Inhalte aus Publikationen des BSI und von ENISA.

Dem Format der Beratungskarten geschuldet stehen die Quellenverweise dafür nicht direkt im Text oder in den Fußnoten. Vielmehr werden in Absprache und mit Einwilligung der jeweiligen Herausgebenden die Quellen einleitend genannt. Für den CSC für KMU sind das die Folgenden:

- BSI. (2018). Basismaßnahmen der Cyber-Sicherheit. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI)
- BSI. (2023b). Cyber-Sicherheit für KMU – Die TOP 14 Fragen. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI)
- ENISA. (2021a). Cybersecurity for SMEs-Challenges and Recommendations. European Union Agency for Cybersecurity (ENISA). doi:10.2824/770352
- ENISA. (2021b). KMU-Leitfaden zur Cybersicherheit – 12 Schritte zur Absicherung Ihres Unternehmens. Athen, Heraklion: Agentur der Europäischen Union für Cybersicherheit (ENISA)

Die Quellenverweise in diesem Handbuch erfolgen einheitlich im Text (APA) mit angehängtem Literaturverzeichnis.

17.1 Fallbeispiele für die Sensibilisierung

Im Vorfeld der Beratung und für den Einstieg in die Beratung kann es hilfreich sein, die Cybersicherheitsbedrohungslage für KMU mit einem Beispiel eines Cyberangriffs greifbarer zu machen. Zu diesem Zweck sind im Folgenden ein paar Fallbeispiele aufgeführt, die den Beratenden bei der Vorbereitung auf die Beratungsgespräche helfen sollen.

17.1.1 Varta

Im Februar 2024 wurde der baden-württembergische Batteriehersteller Varta Opfer eines Cyberangriffs. An den drei deutschen Werken in Ellwangen, Dischingen und Nördlingen steht die Produktion still, auch die Standorte in Rumänien und Indonesien sind betroffen. Um größeren Schaden zu vermeiden, werden die internen Systeme nach der Entdeckung des Angriffs sofort abgeschaltet. Der Konzern ist weder per Mail noch per Telefon erreichbar (Süddeutsche Zeitung, 2024). Zur Art des Angriffs hüllt sich der Konzern in Schweigen. Es wird vermutet, dass es sich um einen Ransomware-Angriff handelt (Allgeier Secion, 2024). Es liegt ein für diesen Fall vorbereiteter Notfallplan vor, der die Bearbeitung des Vorfalls erleichtert und die umgehend erforderlichen Maßnahmen enthält (Varta AG, 2024). Die Kriminalpolizei Aalen ermittelt, das Cybercrime-Zentrum Baden-Württemberg, angesiedelt bei der Generalstaatsanwaltschaft in Karlsruhe, leitet die Ermittlungen (SWR, 2024). Den ohnehin kriselnden Konzern trifft dieser Angriff zusätzlich und hart. Die Sanierungspläne aus dem Vorjahr müssen für gescheitert erklärt werden. Der wochenlange Ausfall der Produktion, bedingt durch den Angriff und die Unsicherheit, welche weiteren Gefahren aus den gestohlenen Daten resultieren werden, verschlechtern die Lage zusätzlich. Gegen den Konkurrenzdruck aus Asien hätten Unternehmen wie Varta nur wenige Chancen, zu bestehen (ZDF, 2024).

17.1.2 IHK

Am 3. August 2022 wurden verdächtige Aktivitäten im Netz des IT-Dienstleisters der Industrie- und Handelskammern, dem IHK GfI, entdeckt und 79 Industrie- und Handelskammern, die Auslandshandelskammern, die DIHK sowie IHK DIGITAL vorsorglich vom Netz genommen (IHK zu Essen, 2022). Es handelte sich um einen sogenannten Supply-Chain-Angriff, bei dem die IT-Systeme des bundesweiten IT-Dienstleisters der IHKs, der IHK GfI, angegriffen wurden. Über Wochen waren die betroffenen Einrichtungen offline, zahlreiche Online-Dienste, Telefonleitungen und E-Mail abgeschaltet (CSO, 2022). IT-Forensiker und die Experten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bestätigten, dass extrem professionelle Hacker am Werk waren. Ihre Vorgehensweise deutet auf einen Angriff zum Zweck der Spionage oder Sabotage hin, auch wenn ein finanziell motivierter Hintergrund noch nicht ausgeschlossen werden kann. Der Angriff wurde rechtzeitig gestoppt, es sind keine Daten abgeflossen (IHK Darmstadt, 2024). Die Ergebnisse der forensischen Untersuchung deuten darauf hin, dass der Angriff von langer Hand vorbereitet worden war.

Das Ziel der Attacke sei Spionage oder Sabotage gewesen, allerdings könne auch ein finanziell motivierter Hintergrund noch nicht ausgeschlossen werden. Neben der schwierigen Aufgabe der Wiederherstellung aller Systeme gehe zusätzliche Gefahr von Trittbrettfahrern aus, warnt der angegriffene IT-Dienstleister IHK GfI: Da der Vorfall für große Aufmerksamkeit sorgte, rufe er mit sehr hoher Wahrscheinlichkeit weitere Kriminelle auf den Plan, die mithilfe von Phishing oder Social Engineering versuchen könnten, persönliche Daten zu stehlen oder Endgeräte zu kompromittieren (CSO, 2022). Die IHK zu Essen berichte über das Krisenmanagement, dass ein Krisenstab gegründet wurde, der sich jeden Morgen traf, um die Abläufe im Haus zu koordinieren. Die Priorisierung der ersten Maßnahmen (Aufsetzen der verschiedenen Kommunikationsmittel und Umstellung auf analoge Prozesse) wurde durch den sukzessiven Wiederanlauf der verschiedenen Services unterstützt und laufend aktualisiert (IHK zu Essen, 2022).

Einen Monat nach dem Angriff gibt es immer noch Einschränkungen. Zwar seien die Webseiten der meisten IHKen wieder online und auch 47 der 79 IHKen am 6.9. telefonisch wieder erreichbar, doch bis alle IHKs wieder voll funktionsfähig arbeiten können, würden noch weitere Wochen ins Land gehen, so der IT-Dienstleister IHK GfI. Der am 3. August entdeckte Angriff habe zwar durch das Trennen aller IHKs vom Internet abgewehrt werden können, die Softwareanwendungen und IT-Systeme der IHKs würden aber nur nach intensiver Prüfung schrittweise hochgefahren, erklärte die IHK GfI. Grund ist die Sorge vor weiteren Attacken (Süddeutsche Zeitung, 2022).

17.1.3 Ausführlicher Erfahrungsbericht der fiktiven Fischer GmbH

Unternehmen, die von Cyberkriminalität betroffen sind oder waren, geben selten und ungern ausführliche Einblicke in die erlebten Vorfälle. Ein KMU mit 20 Mitarbeitenden hat das gegenüber der Neuen Zürcher Zeitung (NZZ) getan. In einem längeren Bericht werden umfangreiche Einblicke in einen Ransomware-Angriff aus unternehmerischer Betroffenenperspektive gegeben. Für das Unternehmen wird das Pseudonym „Fischer GmbH“ verwendet: https://www.nzz.ch/technologie/die-erpressung-landet-im-spam-ordner-tausende-von-kundenadressen-im-darknet-der-manager-in-der-ohnmacht-ein-kleinunternehmen-gibt-einen-seltenen-einblick-in-einen-hack-ld.1712713

17.2 Cyberangriffe erkennen und richtig reagieren

Swisscom, ein großer Schweizer Dienstleister der Telekommunikation und Informationstechnologie, der selbst Cybersicherheitsdienstleistungen anbietet, hat in einem Artikel mit dem Titel „So erkennen Sie Cyberattacken – und reagieren richtig“ folgende Punkte zusammengestellt (Swisscom, 2024). Weitere Informationen finden sich auch auf dem CSBW-Factsheet „Informationssicherheitsvorfall erkennen“, erreichbar unter: https://sl.csc-kmu.de/b7-05.html

Cyberangriffe im Alltag erkennen

- Obwohl Sie den Computer keiner großen Belastung aussetzen, läuft er langsam, die Lüfter sind laut.
- Das System verhält sich ungewöhnlich. Zugriffe auf lokale Systeme wie ein Server oder NAS sind langsam. Es tauchen häufig Fehlermeldungen auf.
- Die Internetverbindung ist ungewöhnlich langsam. Im Router ist ein ungewöhnlich hoher ausgehender Datenverkehr dargestellt.
- Der Computer „macht sich selbstständig“. Fenster öffnen und schließen sich von alleine, der Mauszeiger bewegt sich ohne Zutun.
- Das Antivirenprogramm meldet den Fund und die Blockade einer oder mehrerer verdächtiger Dateien. Fehlermeldungen des Antivirenprogramms besagen, dass es deaktiviert sei.
- Sie erhalten Warnmails über ungewöhnliche Anmeldeaktivitäten in Ihren Konten und Zugängen.
- Sie erhalten Zweitfaktoren wie Codes per SMS oder die Aufforderung, sich mittels Mobil-ID zu verifizieren, ohne dass die entsprechenden Anmeldeversuche auf Sie zurückzuführen sind.
- Ihre Passwörter funktionieren nicht mehr. Die Startseite des Browsers hat sich ohne Ihr Zutun verändert.

Cyberangriffe als Admin erkennen:

- In den Logdateien von Servern und NAS tauchen Meldungen auf, die auf viele fehlerhafte Zugriffsversuche hinweisen, oder sie enthalten erfolgreiche Zugriffe von Admins, die sich nicht erklären lassen (Zeit, Ort etc.).
- Es laufen Hintergrundprozesse mit ungewöhnlichen, oft kryptischen Namen.
- Windows-Schattenkopien (Volume Shadow Copies) wurden gelöscht.
- Es gibt unerklärbare Veränderungen an Backups oder den Backup-Einstellungen.
- Hohe Prozessor-, Speicher- und Netzwerklast ohne erklärbaren Grund.
- Der verfügbare Speicherplatz verändert sich markant oder Speichermedien sind plötzlich voll.

Richtig auf einen Cyberangriff reagieren:

- Ruhig bleiben, klaren Kopf behalten. Nicht überhastet reagieren.
- Gegebenenfalls die Netzwerkverbindung ins Internet trennen, am besten in Absprache mit Cybersicherheitsfachleuten. Ohne Internetverbindung sind die Angreifenden oft ihrer Handlungsmöglichkeiten beraubt.
- Krisen- und Notfallplan aktivieren.
- So schnell wie möglich Cybersicherheitsfachleute hinzuziehen.
- Polizei informieren.

Die Folgen einer Cyberattacke beheben:

- Isolieren kompromittierter Systeme, um weitere Ausbreitung zu verhindern. Geräte vom Netz nehmen, ohne sie auszuschalten, um keine Spuren zu verwischen.
- Forensische Beweissicherung auf den befallenen Geräten.
- Systeme bereinigen. Gegebenenfalls Backup wiederherstellen. Die Möglichkeit kompromittierter Backups beachten.
- Admin-Passwörter ändern, Zwei-Faktor-Authentifizierung aktivieren.
- Datenverlust personenbezogener Daten prüfen und ggf. beim Landesdatenschutzbeauftragten anzeigen.
- Anzeige erstatten.
- Vorfall beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei der Zentralen Aufklärungsstelle Cybercrime Ihrer Landespolizeibehörde (ZAC) melden. Sie unterstützen damit generell die Bekämpfung von Cyberkriminalität.

Denken Sie daran, im Falle eines Cyberangriffes unmittelbar die Polizei einzubinden. Nur dadurch ist es den Strafverfolgungsbehörden möglich, Cyberkriminelle zu ermitteln, weitere potenzielle Opfer zu identifizieren und vor einem bevorstehenden Angriff zu warnen sowie die Strukturen der Cyberkriminellen nachhaltig zu zerschlagen.

Durch die Einbindung der Polizei leisten Sie jedoch nicht nur einen Beitrag zur ganzheitlichen Cybercrimebekämpfung. Als geschädigtes Unternehmen profitieren Sie auch direkt und auf vielfältige Weise von exklusiven Befugnissen der Polizei. So kann beispielsweise die Veröffentlichung von Daten, die bei Ihnen ausgespäht wurden, durch die polizeiliche Beschlagnahme von Servern der Täter, auf denen diese von den Tätern gespeichert wurden, verhindert werden.

Wirtschaftsunternehmen und Behörden können sich hierzu an die 24/7 erreichbaren Zentralen Ansprechstellen Cybercrime (ZAC) bei den jeweiligen Landeskriminalämtern wenden[1].

Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Baden-Württemberg für Unternehmen und Behörden innerhalb dieses Landes:

Hotline[2] BW: **+ 49 (0)711 5401-2444**
Erreichbarkeit: **24/7**
E-Mail: **cybercrime@polizei.bwl.de**
PGP-Key: **lka-bw.de/zac**

Bei den Zentralen Ansprechstellen Cybercrime sind ausgewiesene Cybercrime-Experten beschäftigt, die Ihnen bereits beim ersten Telefonat wichtige Informationen zur Vorfallbehandlung, wie beispielsweise Erkenntnisse zur Vorgehensweise der Tätergruppierungen, geben können. In enger Abstimmung mit Ihnen werden von dort alle weiteren polizeilichen Maßnahmen veranlasst. Diese werden in kooperativer Zusammenarbeit mit Ihnen und eingebundenen externen Dienstleistern durchgeführt und haben stets Ihre Interessen als geschädigtes Unternehmen im Blick.

Das niedrigschwellige Angebot des CSC ist ganz bewusst so gehalten, dass nicht die Gefahr einer wirtschaftlichen Tätigkeit entsteht und durch die kostenneutrale Beratung wettbewerbsrechtliche Punkte tangiert würden. Der CSC bleibt in der sensibilisierenden, Awareness-orientierten Beratung und bietet keine operativen Lösungen an, wie es beispielsweise die IT-Dienstleistungsunternehmen tun. So geht es z. B. nicht um die Konfiguration einer Firewall, Vorschläge zur Segmentierung einzelner Netzbereiche usw., es geht nicht um Proto-kollauswertung und daraus resultierende Ableitungen, sondern es geht lediglich darum, durch sinnvoll installierte Firewalls und durch logisch aufgebaute Netzwerksegmentierung größtmöglichen Schutz zu bieten.

17.3 Beratung von Kleinst- und Einpersonenunternehmen

Der CSC für KMU wurde zur Anwendung in KMU bis 100 Mitarbeitende konzipiert. Der Kern-Anwendungsfall ist ein Unternehmen mit 10 bis 50 Mitarbeitenden.

Ist ein Unternehmen besonders klein, besteht vielleicht sogar nur aus einer oder zwei Personen ohne Mitarbeitende, so ist selbst der reduzierte Themenumfang in den Beratungsmaterialien an manchen Punkten zu umfangreich.

Dennoch bietet das Beratungsmaterial eine gewisse Flexibilität, die es den Beratenden ermöglicht, auf die unterschiedlichsten Beratungskontexte individuell einzugehen. Insbesondere wenn Beratende mit den behandelten Themen und den Materialien gut vertraut sind, können sie diese Flexibilität voll ausschöpfen. Dieses Handbuch deckt viele der Themen ab, zu denen in besonderen Beratungssituationen Fragen aufkommen können.

[1] Die Erreichbarkeit der für Sie zuständigen Zentralen Ansprechstelle Cybercrime finden Sie unter: www.polizei.de/zac
[2] Diese Hotline ist nur für Baden-Württemberg zuständig. Für andere Bundesländer bitte die Nummer im Netz erfragen.

Die Checkliste und damit auch der Online-Check auf www.csc-kmu.de bietet durch die Antwortoption „k. R." (keine Relevanz) die Möglichkeit, nicht relevante Fragen auszuklammern. Diese werden dann in der Auswertung auch nicht berücksichtigt. Für Kleinstunternehmen, in denen z. B. das Firmennetzwerk aus einem Computer, einem Cloud-Speicher und einem Router besteht, sind möglicherweise die Fragen im Bereich der Absicherung der Netzübergänge zu umfangreich. Auch die Fragen zur Absicherung mobiler Endgeräte mit Zugriff aufs Firmennetzwerk können irrelevant sein, wenn die verwendeten Mobilgeräte diese Zugriffsmöglichkeiten gar nicht aufweisen. In diesen Fällen können die entsprechenden Fragen durch Angabe von „k. R." aus dem Check herausgenommen werden und es kann somit individuell auf die vorgefundene Unternehmenssituation eingegangen werden.

Die Beratungskarten bieten diese Flexibilität prinzipiell ebenfalls. Maßnahmen, die auf den Kartenvorderseiten zur Umsetzung empfohlen werden, die aber ggf. nicht vorhandene Mobilgeräte oder nicht vorhandene Mitarbeitende betreffen, können in der Umsetzung einfach ausgelassen werden. Auch Dokumentationsempfehlungen von Netzwerkstrukturen, Hardware- und Softwarebeständen können in besonders kleinen Unternehmen sinnlos erscheinen. Nichtsdestotrotz sind die allermeisten der angesprochenen Themen auch für kleinste Unternehmen von Bedeutung, wenngleich sich deren Umsetzungsumfang in diesen Fällen eher klein ausgestalten wird. Auch Soloselbstständige sollten wissen, wo sie ihre wichtigsten Datenbestände gespeichert haben, ob die Backups funktionieren, welche Personen im Ernstfall zu kontaktieren sind und wie die eigenen Kunden bei einem Ausfall des Computers oder Smartphones noch erreicht werden können.

17.4 Umgang mit Dienstleister-/Produktempfehlungen in der Beratungssituation

In der Beratung kann es an verschiedenen Stellen passieren, dass die beratenen Geschäftsführungen die Beratenden um konkrete Empfehlungen bitten, sei es z. B. für Programme wie Virenschutzprogramme oder Passwortmanager oder auch für IT-Dienstleistungsunternehmen. Es ist schwierig, im Rahmen der Beratungsmaterialien oder auch der Schulungsunterlagen oder des Handbuchs verlässliche Empfehlungen zu diesen Punkten zu erarbeiten. Einerseits, weil sich die Empfehlungen im Laufe der Zeit verändern, einmal verschriftlichte Empfehlungen also möglicherweise schlecht altern. Andererseits, weil aber auch ganz zentral die Gefahr besteht, mit solchen Empfehlungen in Wettbewerbsprozesse einzugreifen. Der CSC für KMU ist unabhängig von wirtschaftlichen Interessen und wird kostenlos zur Verfügung gestellt. Aus diesem Grund können auch keine Empfehlungen gegeben werden. Im Zweifel kann dem beratenen Unternehmen empfohlen werden, sich mit diesen Fragen an den eigenen IT-Dienstleister zu wenden, ggf. nach dessen Beauftragung, so noch keine Geschäftsbeziehung zu einem IT-Dienstleistungsunternehmen besteht.

17.5 Abgrenzung zum CyberRisikoCheck nach DIN SPEC 27076

Während der Projektlaufzeit von CyberWuP wurde mit der DIN SPEC 27076 ein weiteres Beratungskonzept für eine IT-Sicherheitsberatung für Klein- und Kleinstunternehmen veröffentlicht. Diese Beratung wurde in ihren Zielen und ihrem Umfang in der DIN SPEC 27076 definiert und kann, darauf aufbauend, durch zertifizierte IT-Beratende privatwirtschaftlich und kostenpflichtig angeboten werden.

Mit der Beratung werden ähnliche Ziele verfolgt wie mit dem CSC:

- Ermittlung des IST-Zustands der Informationssicherheit des Unternehmens und Sichtbarmachung der wichtigsten Sicherheitsrisiken, Generierung eines Risikostatus
- Unterbreitung von Handlungsempfehlungen, zudem Hinweis auf mögliche Fördermaßnahmen
- Sensibilisierung für gängige Gefahren

Jedoch sieht die Beratung gemäß DIN SPEC 27076 eine im Vergleich zum CSC tiefer gehende Analyse der IT-Infrastruktur des Unternehmens vor. Das zeigt sich schon am zeitlichen Umfang. Bei der DIN SPEC 27076 gibt es zwe i Beratungstermine im Umfang von insgesamt mindestens vier Stunden. Der Ablauf dieser Beratung ist wie folgt vorgesehen:

1. Erstinformation des zu beratenden Unternehmens (Anbahnung)
2. Durchführung des Gesprächs zur Erhebung des IST-Zustands
3. Auswertung und Erstellung des Ergebnisberichts
4. Präsentation des Ergebnisberichts und Hinweis auf umzusetzende Handlungsempfehlungen

Damit unterscheidet sich das Beratungsangebot nach DIN SPEC 27076 insbesondere in den folgenden Punkten vom CSC für KMU:

- Die Beratung nach DIN SPEC 27076 sieht eine tiefer gehende Analyse der IT-Infrastruktur des Unternehmens vor.
- Der zeitliche Aufwand ist mit zwei Terminen und min. vier Stunden größer,
- DIN-SPEC-27076-Beratungen dürfen nur durch zertifizierte IT-Sicherheitsberatende durchgeführt werden,
- DIN-SPEC-27076-Beratungen sind nicht kostenlos.

Der CSC und die Beratung nach DIN SPEC 27076 ergänzen sich gut, indem ein kostenloser CSC den Einstieg ins Thema Cybersicherheit bieten kann und die anschließende Umsetzung der Cybersicherheitsmaßnahmen, neben der Inanspruchnahme von IT-Dienstleistern, durch regelmäßige DIN SPEC 27076-Beratungen begleitet werden kann.

Abbildung 19: Der CyberRisikoCheck nach DIN SPEC 27076 ist zeitaufwendiger als der CSC für KMU. Er eignet sich gut als weitergehendes Beratungsangebot für kleine Unternehmen, die mit dem CSC für KMU einen guten Einstieg ins Thema Cybersicherheit gefunden haben.
Quelle: https://www.bsi.bund.de/dok/crc

17.6 Abgleich mit den Empfehlungen des BSI

CyberSicherheitsCheck für KMU	BSI-Empfehlungen (TOP-14-Fragen)													
	1. Verantwortlichkeit	2. Kenntnis IT-Systeme	3. Daten-sicherung	4. Updates	5. Datenaktivierung Makros	6. Virenschutz	7. Passwort-richtlinie	8. Firewall	9. Absicherung Mailaccounts	10. Trennung IT-Bereiche	11. Homeoffice und mobiles Arbeiten	12. Information der Beschäftigten	13. Versicherung für Cyberrisiken	14. Reaktion auf Cyberangriff
EK: Cybersicherheit ist Führungsaufgabe	✓												✓	
B1: Sicherheitslücken schließen				✓										
B2: Benutzerzugänge absichern							✓		✓	✓				
B3: Datensicherungen durchführen			✓											
B4: Gefahrenbewusst-sein schaffen												✓		
B5: Netzwerkübergänge absichern								✓		✓				
B6: Schadprogramme abwehren					✓	✓								
B7: Notfallplan erstellen														✓
B8: Inventarisieren und dokumentieren		✓												
ZK: Weitere Themen											✓			

Abbildung 20: Alle BSI-Empfehlungen der TOP-14-Fragen in Bezug auf Cybersicherheit für KMU werden auch in den Beratungskarten des CSC für KMU behandelt.

Zum Thema Cybersicherheit für KMU gibt das BSI unter anderem eine Broschüre mit dem Titel „Cybersicherheit für KMU – Die TOP-14-Fragen“ heraus (BSI, 2023b). Der Abgleich des vorliegenden CSC mit diesen BSI-Empfehlungen zeigt eine vollständige Deckung (siehe Abbildung 20). Das bedeutet, alle Themen, von welchen das BSI es für wichtig erachtet, dass sie im Rahmen der TOP 14 Fragen in Bezug auf Cybersicherheit für KMU aufgeführt werden, werden auch in den 10 Beratungskarten des CSC für KMU behandelt.

18. Glossar

Cybersicherheit	Cybersicherheit beschreibt den Schutz von Computersystemen und Netzwerken vor Cyberangriffen.
CISO	Chief Information Security Officer: die Person, die für die Sicherheit der Informationen und Systeme in einer Organisation zuständig ist
Informationssicherheit	Informationssicherheit umfasst alle Maßnahmen, die zum Schutz von Informationen ergriffen werden.
IT-Sicherheit	IT-Sicherheit soll IT-Systeme schützen, sodass Angreifende keine Daten und Informationen ausspähen, manipulieren, kopieren oder zerstören können.
Malware	„Malicious software“: Viren, Würmer, die in Computersysteme eindringen und dort Störungen oder Schäden verursachen
Phishing	Beschaffung persönlicher Daten anderer Personen, z. B. mittels gefälschter E-Mails oder Websites, die zur Dateneingabe der entsprechenden Daten auffordern (Passwörter, Kreditkartendaten)
Ransomware	Verschlüsselungstrojaner, Erpressungssoftware
Spam	Unerwünschte, massenhaft z. B. per E-Mail verteilte Nachrichten
Trojaner	Tarnt sich als nützliche Anwendung, erfüllt im Hintergrund aber unbemerkt andere, meist schädigende Funktionen
Virus	Sich selbst verbreitendes und reproduzierendes, schädigendes Programm, nutzt dazu die Bootbereiche von Datenträgern, Dateien oder Makros
Wurm	Bildet eine Unterklasse der Viren, beschreibt ebenfalls sich selbst verbreitende, schädigende Programme

Literaturverzeichnis

Allgeier Secion. (2024). Deutscher Batteriehersteller Varta gehackt – Allgeier secion. Abgerufen am 05.09.2024 von www.secion.de: https://www.secion.de/de/blog/blog-details/deutscher-batteriehersteller-varta-gehackt-allgeier-secion

BAKGame. (2024). IT-Sicherheit in der Wirtschaft – Bedrohungsanalyse für KMU. (Technische Akademie für berufliche Bildung Schwäbisch Gmünd e. V.; Hochschule Aalen.) Abgerufen am 16.10.2024 von BAKGame – Bedrohung, Analyse, KMU: https://baksecure.de/spiele/

BMWK. (2021). IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland. Bundesministerium für Wirtschaft und Energie (BMWK). Abgerufen am 29.08.2024 von https://www.bmwk.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.pdf?__blob=publicationFile&v=1

BSI. (2022). BSI-Lagebericht 2022: Gefährdungslage im Cyber-Raum hoch wie nie. Abgerufen am 29.08.2024 von Bundesministerium des Inneren und für Heimat: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/10/bsi-lagebericht.html

BSI. (2023a). Die Lage der IT-Sicherheit in Deutschland 2023. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI)

BSI. (2023b). Cyber-Sicherheit für KMU – Die TOP 14 Fragen. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI)

BSI. (2024a). Firewall – Schutz vor dem Angriff von außen. Abgerufen am 16.10.2024 von Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/dok/504484

BSI. (2024b). E-Mail-Verschlüsselung. Abgerufen am 16.10.2024 von Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html

BSI. (2024c). Daten auf Festplatten und Smartphones endgültig löschen. Abgerufen am 15.05.2024 von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/dok/6599236

BSI. (2024d). Wie funktioniert ein Virtual Private Network (VPN)? Abgerufen am 16.10.2024 von Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/dok/504116

certnz. (2024). How ransomware happens and how to stop it. Abgerufen am 18.07.2024 von www.cert.govt.nz: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

CSO. (2022). Deutschlandweite Cyberattacke auf die IHK. Abgerufen am 05.09.2024 von www.csoonline.com: https://www.csoonline.com/de/a/ihk-faehrt-deutschlandweit-die-it-systeme-herunter,3674080

DIHK. (2024). Nutzungsrichtlinie IT-Sicherheit. Abgerufen am 16.10.2024 von graphassets.com: https://media.graphassets.com/627IVmszTvuQi5e4cAAA

ENISA. (2021a). Cybersecurity for SMEs – Challenges and Recommendations. European Union Agency for Cybersecurity (ENISA). doi:10.2824/770352

ENISA. (2021b). 12 Schritte zur Absicherung Ihres Unternehmens. Abgerufen am 29.10.2024 von KMU-Leitfaden zur Cybersicherheit: https://www.enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_de.pdf

Ernst, H., Schmidt, J., & Beneken, G. (2023). Grundkurs Informatik. Wiesbaden: Springer Fachmedien

IHK Darmstadt. (2024). Cyberattacke trifft IHK-Organisation. Abgerufen am 05.09.2024 von www.ihk.de/darmstadt: https://www.ihk.de/darmstadt/servicemarken/ueber-uns/ihk-finanzen/geschaeftsbericht2022/cyberattacke-5846774

IHK zu Essen. (2022). Deutschlandweiter Cyberangriff und IT-Sicherheit im Fokus. Abgerufen am 05.09.2024 von www.ihk.de/meo: https://www.ihk.de/meo/standortpolitik/jahresbericht2022/cyberangriff2-5786646

Landeskriminalamt Niedersachsen. (2024). Gefälschte Briefpost im Namen von diversen Banken mit QR-Code. Abgerufen am 07.08.2024 von www.polizei-praevention.de: https://www.polizei-praevention.de/aktuelles/gefaelschte-briefpost-im-namen-von-diversen-banken-mit-qr-code.html

Loveletter-wurm.png. (2024). Abgerufen am 16.10.2024 von wikimedia.org: https://upload.wikimedia.org/wikipedia/commons/f/ff/Loveletter-wurm.png

Microsoft. (2024). Lesen von E-Mail-Nachrichten im Nur-Text-Format. Abgerufen am 16.10.2024 von Microsoft: https://support.microsoft.com/de-de/office/lesen-von-e-mail-nachrichten-im-nur-text-format-16dfe54a-fadc-4261-b2ce-19ad072ed7e3

National Cyber Security Center. (2018). 12 Steps to Cyber Security. Dublin: Government of Ireland

Schwarz, L., & Hahn, J. (2021). Makros – Kleines Wort, großes Risiko. Abgerufen am 16.10.2024 von RWTH Aachen University, IT Center Blog: https://blog.rwth-aachen.de/itc/2021/03/10/makros/

Seunghwan Hwang. (2017). Abgerufen am 15.05.2024 von https://de.wikipedia.org/wiki/WannaCry#/media/Datei:%EA%B0%90%EC%97%BC%EC%82%AC%EC%A7%84.png

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. The 16th International Conference on Availability, Reliability and Security (ARES 2021)

Süddeutsche Zeitung. (2022). Cyberangriff auf IHK: noch immer Einschränkungen. Abgerufen am 05.09.2024 von www.sueddeutsche.de: https://www.sueddeutsche.de/wirtschaft/internet-cyberangriff-auf-ihk-noch-immer-einschraenkungen-dpa.urn-newsml-dpa-com-20090101-220908-99-678925

Süddeutsche Zeitung. (2024). Hackerangriff auf Batteriehersteller Varta. Abgerufen am 05. 09 2024 von www.sueddeutsche.de: https://www.sueddeutsche.de/wirtschaft/varta-batterie-hacker-angriff-apple-1.6359994

Swisscom. (2024). So erkennen Sie Cyberattacken – und reagieren richtig. Abgerufen am 05.09.2024 von www.swisscom.ch: https://www.swisscom.ch/de/b2bmag/sicherheit/cyberattacken-erkennen-reagieren/

SWR. (2024). Cyberattacke: Weiter Auswirkungen auf Ellwanger Batteriehersteller VARTA. Abgerufen am 05.09.2024 von www.swr.de: https://www.swr.de/swraktuell/baden-wuerttemberg/ulm/cyberangriffe-wie-auf-varta-ellwangen-arbeitsplaetze-in-gefahr-ihk-ost-wuerttemberg-100.html

Thimm, S. (2008). E-Mail-Server richtig konfigurieren – Zehn kritische Fehler beim Einrichten eines E-Mail-Servers. Abgerufen am 16.10.2024 von Computerwoche Tec Workshop: https://www.tecchannel.de/a/zehn-kritische-fehler-beim-einrichten-eines-e-mail-servers,1750499

Universität Hamburg. (2022). ACHTUNG! Phishing-Mails mit dem Betreff „E-Mail-Speicherbenachrichtigung“. Abgerufen am 16.10.2024 von UHH – Aktuelle Meldungen: https://www.rrz.uni-hamburg.de/ueber-uns/aktuell/2022/2022-10-19-sicherheitswarnung-phishing-speicherbenachrichtigung.html

Varta AG. (2024). VARTA von Cyberangriff betroffen. Abgerufen am 05.09.2024 von www.varta-ag.com: https://www.varta-ag.com/fileadmin/varta_ag/publications/ad-hoc_announcements/20240213_VARTA_AG_Ad_hoc_Cyberangriff_DE.pdf

Verbraucherzentrale. (2024). 11-12.06.2024.png. Abgerufen am 16.10.2024 von www.verbraucherzentrale.de: https://www.verbraucherzentrale.de/sites/default/files/inline-images/11-12.06.2024.png

Wilson, M., & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. Information Security Journal: A Global Perspective

ZDF. (2024). Varta geht der Saft aus. Abgerufen am 05.09.2024 von www.zdf.de: https://www.zdf.de/nachrichten/wirtschaft/unternehmen/varta-batterie-hersteller-krise-100.html

www.csc-kmu.de
Zielgruppe: Beratende
Erstellt von Prof. Dr. Christoph Karg,
Demian Deffner, Miriam Kappe
Unter Mitwirkung von:
Jochen Wellhäußer, Reinhold Hepp