Kompetenzzentrum
Digitalisierung und Pflege

Wegweiser für Organisationstyp A (Kleiner ambulanter Pflegedienst)

Cybersicherheitsmaßnahmen planen und priorisieren

Inhaltsverzeichnis

1 Einleitung 3
2 Der Baukasten 7
3 Ihr Weg in vier Etappen 14
4 Dranbleiben: der regelmäßige Zyklus 17
5 Wenn es hakt 20

Dieses Dokument ist die begleitende Regieanweisung für Organisationstyp A (Kleiner ambulanter Pflegedienst). Es beschreibt wie die Dokumente zu benutzen sind, an wen welche Aufgaben delegiert werden können, und gibt Hinweise für die erfolgreiche Umsetzung im Alltag.

1 Einleitung

Jede Organisation braucht Cybersicherheit, jedoch nicht jede Einrichtung braucht die gleiche Cybersicherheit. Was konkret zu tun ist, ist eine sehr individuelle Entscheidung. Sie hängt davon ab, was eine Organisation macht, wie groß sie ist, und wie viele Ressourcen sie hat: eine große vollstationäre Pflegeeinrichtung benötigt etwas anderes als ein kleiner ambulanter Pflegedienst. Diese Individualität ist ein Vorteil, denn ein geringeres Risiko bedeutet in der Praxis auch weniger Aufwand und Kosten für Cybersicherheit, aber dies erfordert eine Planung, was zu welchem Zeitpunkt genau erforderlich ist. Das *klingt* schwierig.

Das vorliegende Material unterstützt Sie genau bei diesen Schritten. Es trifft für Sie eine Vorauswahl, welche Maßnahmen für Sie relevant sind. Es priorisiert diese Maßnahmen, damit Sie mit begrenztem Aufwand den meisten Wert erhalten. Und es nimmt Ihnen diese Planung und Informationssammlung ab, so dass Sie sich um die Umsetzung bei Ihnen vor Ort kümmern können.

Dieses Dokument führt Sie durch den Prozess und das speziell für Ihre Einrichtung angepasste Material: *eine kleine ambulante Pflegeeinrichtung mit wenigen Mitarbeitern, ausgestattet mit einzelnen PCs, Tablets und Mobiltelefonen.*

Die IT muss laufen, läuft aber nebenher! Weil Sie sich neben der Pflege auch um Buchhaltung, Abrechnung, Personal kümmern müssen. Das vorliegende Material legt den Fokus auf Ihre Einrichtung und beschreibt die wichtigsten Maßnahmen und Aktivitäten die für Sie geeignet, wichtig und machbar sind. Es erweitert die Informationen in der Hauptbroschüre, welche die Bedrohungslage, die rechtlichen Anforderungen an Sie, und mögliche Cybersicherheitsvorfälle in der Pflege beleuchtet. Dieses Heft können Sie unabhängig davon abarbeiten.

Was habe ich davon?

Mithilfe des vorliegenden Baukastens erreichen Sie für sich und Ihre Pflegeeinrichtung drei wichtige Ziele:

1. **Besserer Schutz gegen Cyberangriffe.** Die vorbereiteten Maßnahmen schließen häufig ausgenutzte Schwachstellen. Cybersicherheitsmaßnahmen können Angriffe nicht gänzlich ausschließen, jedoch helfen sie Ihnen die Wahrscheinlichkeit, dass Sie von einem Angriff betroffen sind, und die Schäden in einem solchen Fall zu minimieren.

2. **Anforderungen und Nachweise.** Verschiedene gesetzliche Vorgaben schreiben Ihnen den Schutz der Ihnen anvertrauten Daten vor. Das bereitgestellte Material zeigt Ihnen, wie Sie Ihre Daten besser schützen können, und dokumentiert gleichzeitig Ihre Bemühungen zur Erfüllung dieser Aufgaben.

3. **Handlungsfähigkeit.** Viele Ereignisse sind nicht zu 100 Prozent zu vermeiden: mehrere Mitarbeiter fallen gleichzeitig aus, das Dienstauto hat zu Schichtbeginn einen Platten, oder der Computer für die Dokumentation und Abrechnung geht nicht mehr an - alle Daten scheinen verloren. Weil sich diese Ereignisse selbst nicht ausschließen lassen, bereiten Sie sich darauf vor, trotz möglicher Einschränkungen weiter handlungsfähig zu sein, so dass für die Pflegebedürftigen, Ihre Mitarbeiter und Sie alles wie gehabt weiterlaufen kann. Vorsorge für den Ausnahmefall betreiben Sie ohnehin – für die IT haben es die wenigsten getan.

Ist das nicht alles IT-Kram?

Nein, denn Cybersicherheit ist eine ganzheitliche Aufgabe - es geht nicht nur um Technologie, es ist nicht allein ein Thema, welches die IT lösen kann. Lassen beispielsweise Mitarbeiter Akten oder den Dienstlaptop beim Stopp an der Tankstelle kurz unbeaufsichtigt und werden diese aus dem Auto gestohlen, dann ist dies ein Problem, bei dem die IT wenig ausrichten kann. Das Bewusstsein der Mitarbeiter ist hier gefragt. Nutzen Ihre Mitarbeiter ihr privates Handy zur betrieblichen Kommunikation? Dann könnten bei Vertragsende wichtige betriebliche Informationen oder Daten der Pflegebedürftigen auf dem Gerät verbleiben - dies ist ein Thema für das Personalmanagement und den Datenschutz.

Cybersicherheit ist also mehr als IT, es erfordert die aktive Mitarbeit und Mitgestaltung all Ihrer Mitarbeiter. In dem vorliegenden Baukasten werden alle Bereiche Ihrer Einrichtung mitgenommen:

1. Konfigurations-Einstellungen machen Ihre Systeme sicherer gegen unbefugten Zugang von außen
2. Mitarbeiter werden geschult, um ein Bewusstsein für die Thematik zu entwickeln und sich sicher zu verhalten
3. Prozesse werden so angepasst, dass sie automatisch zu mehr Cybersicherheit im Unternehmen beitragen
4. Vorgaben und Richtlinien legen bestimmte Abläufe verbindlich fest und kommunizieren klar die Bedeutung von Cybersicherheit an Ihre Mitarbeiter, damit Sie auch rechtlich besser aufgestellt sind
5. Anschaffungen von Einrichtungsgegenständen, Hard- und Software, die kostengünstig das Sicherheitsniveau Ihrer Einrichtung verbessern

Welche dieser Maßnahmen an wen geht, zeigt Ihnen das nächste Kapitel.

Wer ist hierfür verantwortlich?

Cybersicherheit ist eine Aufgabe für jeden in Ihrer Einrichtung, diese fängt aber bei Ihnen selbst an. Gerade weil Cybersicherheit alle Bereiche Ihres Unternehmens betrifft, muss die Initiative hierfür zwingend von Ihnen ausgehen. Als Eigentümer und/oder Geschäftsführer sind Sie der oder die Sicherheitsverantwortliche, denn auch im Falle eines Schadens müssen Sie dafür geradestehen. Da Cybersicherheit mehr als nur ein IT-Thema ist, kann man es nicht komplett an die IT abgeben.

Muss ich das allein und sofort machen ...?

Auch wenn von Ihnen die Initiative für mehr Cybersicherheit in Ihrer Einrichtung ausgehen muss, lassen sich die meisten Aktivitäten delegieren. An Ihre IT-Unterstützung geht der technische Teil, Ihre Mitarbeitenden werden geschult und eingebunden, die Steuerung und Prüfung bleibt bei Ihnen. Ihre Kernaufgabe ist hier insbesondere, den Überblick zu behalten, die Impulse zu setzen und die Umsetzung zu kontrollieren. Um Sie bei diesen Aufgaben zu unterstützen, stellt Ihnen das Kompetenzzentrum Digitalisierung und Pflege kostenlos ein Web-Portal zur Verfügung, mit dem Sie für sich individuell den Prozess begleiten, Aufgaben verteilen und die nächsten Schritte planen können. Eine kurze Übersicht hierzu erhalten Sie in Kapitel 4.

Wie bei jedem Trainingsprogramm geht es hier nicht darum, das Ziel „Cybersicherheit“ in einem Tag zu erreichen. Das vorliegende Paket gruppiert die anstehenden Aufgaben in vier Etappen, jeweils unterteilt in kleine Aufgaben, die sich schnell bearbeiten und abhaken lassen. Etappe 1 besteht aus 20 Aufgaben. Ihr persönlicher Aufwand für die Leitungsaufgaben der Umsetzung liegt meist bei weniger 1h pro Aufgabe. Jede dieser Aufgaben bringt Sie ein Stück näher an eine solide Cybersicherheit, ohne Sie und Ihre Mitarbeiter zu überfordern. So haben Sie innerhalb eines Jahres die Etappe 1 komplett erreicht.

Was bekomme ich an die Hand?

In dem Ihnen vorliegenden Baukasten finden Sie vorgefertigte Dokumente, um Ihnen den Einstieg und den Weg zu besserer Cybersicherheit so einfach wie möglich zu machen. Die Dokumente sind so gestaltet, dass sie ohne Expertenwissen einzusetzen sind, sie leiten Sie jedoch darin an, Ihre Organisation auf ein solides Niveau zu heben. Die beiliegenden Dokumente teilen sich in drei Kategorien ein:

- Konkrete Schritt-für-Schritt Anleitungen, um eine bestimmte Maßnahme vor Ort umzusetzen
- Vordrucke, um wichtige Informationen spezifisch zu Ihrer Einrichtung zu sammeln und zu strukturieren
- Richtlinien und Vorgaben, die Anforderungen für Ihre Mitarbeiter intern und für Geschäftspartner nach außen kommunizieren

Zu jedem dieser Dokumente bekommen Sie eine Einordnung, warum diese Aufgabe nötig ist und worauf geachtet werden muss, zum Beispiel wenn Sie diese weiter delegieren.

Der erste Schritt

Wir laden Sie ein, direkt heute den Weg zu beginnen. Setzen Sie sich einen zwei-wöchentlichen Termin im Kalender, zum Beispiel jeden 1. und 3. Donnerstag im Monat um 13 Uhr, und nehmen Sie sich eine Stunde Zeit, Ihre Pflegeeinrichtung besser vorzubereiten.

2 Der Baukasten

Cybersicherheit für Ihre Pflegeeinrichtung - dies klingt erst einmal nach einer großen Aufgabe. Aber dieser Weg lässt sich gut strukturieren, in kleine Aufgaben, die sich jeweils in weniger als einer Stunde bewältigen lassen. Hieraus ergibt sich der vorliegende Baukasten: er legt einzelne, voneinander gut abgegrenzte Maßnahmen vor, bei der jede von ihnen Sie Ihrem Ziel näherbringen.

Um den Weg noch leichter begehbar zu machen, teilen wir die Aufgaben in Etappen. In der **ersten Etappe** geht es darum, die Angriffsfläche für typische Cyberbedrohungen zu reduzieren und die Grundlage für spätere Handlungsfähigkeit zu legen. In der **zweiten Etappe** verbessern wir die Sicherheit im Umgang mit Geräten, kümmern uns um externe Geschäftsbeziehungen und mobiles Arbeiten. In der **dritten Etappe** verbessern wir die Schnittstellen und Zugriffsrechte. In der **letzten Etappe** lernen Sie den Umgang mit Sicherheitsvorfällen und erreichen einen reibungslosen Weiterbetrieb trotz eines Vorfalls. Die ersten drei Etappen senken das Risiko für einen Cyberangriff deutlich und legen das Fundament für die vierte Etappe, in der Sie lernen Ihre Geschäftskontinuität auch während eines Cyberangriffs aufrecht zu erhalten, um weiterhin für Ihre Kundinnen und Kunden da sein zu können.

Die vorliegende Struktur in Etappen hat mehrere Gründe. Erstens macht sie den Weg teil- und überschaubarer. Zweitens setzen bestimmte Maßnahmen frühere voraus - eine Zugriffsregelung nützt wenig, wenn alle mit dem gleichen Nutzernamen im Büro arbeiten. Und drittens ordnen wir damit die Maßnahmen so, dass das Verhältnis von Aufwand zu Wirkung am Anfang am besten ist, so erreichen Sie schnell für sich Verbesserungen, die Ihren Betrieb, Ihre Mitarbeiter und Pflegebedürftigen schützen und Sie hoffentlich motivieren, weitere Etappen in Angriff zu nehmen.

Innerhalb einer Etappe können Sie frei wählen, womit Sie anfangen und weitermachen. Alle Maßnahmen können innerhalb der Etappe unabhängig bearbeitet werden, sollte es Synergieeffekte zwischen Maßnahmen geben, stellen wir diese in den Dokumenten dar.

In der Praxis fangen Sie natürlich nicht bei null an. Ein Virenschutz läuft, eine Datensicherung gibt es vermutlich auch. Etappe 1 heißt zu einem guten Teil: prüfen, ob dies bereits gemacht wurde und funktioniert, und abhaken.

Der Baukasten für kleine ambulante Pflegeeinrichtungen mit externer IT besteht aus insgesamt 71 Dokumenten. Inhaltlich decken diese sowohl technische Komponenten wie zum Beispiel die sichere Konfiguration von Arbeitsplatzrechnern, Mobiltelefone und Tablets ab, umfassen aber auch organisatorische Themen wie Personal, die Arbeit mit Cloudanbietern und Dienstleistern, sowie die Vorsorge und der effektive Umgang auf einen Vorfall.

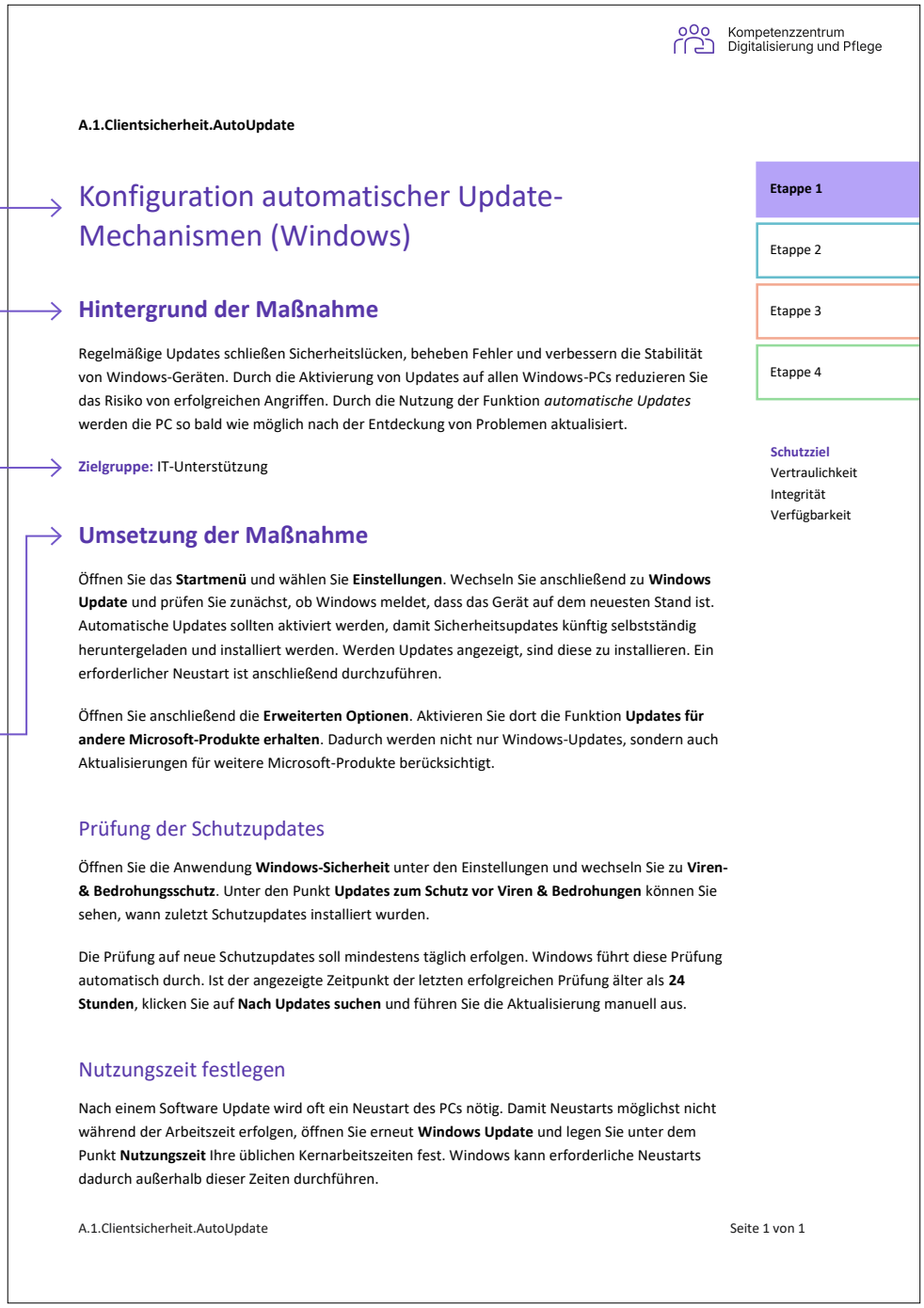
Alle Ihnen vorliegenden Dokumente folgen der gleichen Struktur, nehmen wir das Dokument zur Aktivierung der automatischen Windows Updates als Beispiel:

Titel der Maßnahme zur Orientierung

Bitte lesen Sie dies unbedingt, bevor die die Maßnahme delegieren

Häufig müssen Sie Maßnahmen an Ihre IT-Unterstützung delegieren, einige Maßnahmen liegen aber in Ihrem Verantwortungsbereich

Hier finden sie die detaillierte Beschreibung der Umsetzung der Maßnahme, zur Information für Sie bzw. Ihre IT-Unterstützung.



Kompetenzzentrum Digitalisierung und Pflege

A.1.Clientsicherheit.AutoUpdate

Konfiguration automatischer Update-Mechanismen (Windows)

Etappe 1
Etappe 2
Etappe 3
Etappe 4

Hintergrund der Maßnahme

Regelmäßige Updates schließen Sicherheitslücken, beheben Fehler und verbessern die Stabilität von Windows-Geräten. Durch die Aktivierung von Updates auf allen Windows-PCs reduzieren Sie das Risiko von erfolgreichen Angriffen. Durch die Nutzung der Funktion *automatische Updates* werden die PC so bald wie möglich nach der Entdeckung von Problemen aktualisiert.

Zielgruppe: IT-Unterstützung

Schutzziel
Vertraulichkeit
Integrität
Verfügbarkeit

Umsetzung der Maßnahme

Öffnen Sie das **Startmenü** und wählen Sie **Einstellungen**. Wechseln Sie anschließend zu **Windows Update** und prüfen Sie zunächst, ob Windows meldet, dass das Gerät auf dem neuesten Stand ist. Automatische Updates sollten aktiviert werden, damit Sicherheitsupdates künftig selbstständig heruntergeladen und installiert werden. Werden Updates angezeigt, sind diese zu installieren. Ein erforderlicher Neustart ist anschließend durchzuführen.

Öffnen Sie anschließend die **Erweiterten Optionen**. Aktivieren Sie dort die Funktion **Updates für andere Microsoft-Produkte erhalten**. Dadurch werden nicht nur Windows-Updates, sondern auch Aktualisierungen für weitere Microsoft-Produkte berücksichtigt.

Prüfung der Schutzupdates

Öffnen Sie die Anwendung **Windows-Sicherheit** unter den Einstellungen und wechseln Sie zu **Viren- & Bedrohungsschutz**. Unter den Punkt **Updates zum Schutz vor Viren & Bedrohungen** können Sie sehen, wann zuletzt Schutzupdates installiert wurden.

Die Prüfung auf neue Schutzupdates soll mindestens täglich erfolgen. Windows führt diese Prüfung automatisch durch. Ist der angezeigte Zeitpunkt der letzten erfolgreichen Prüfung älter als **24 Stunden**, klicken Sie auf **Nach Updates suchen** und führen Sie die Aktualisierung manuell aus.

Nutzungszeit festlegen

Nach einem Software Update wird oft ein Neustart des PCs nötig. Damit Neustarts möglichst nicht während der Arbeitszeit erfolgen, öffnen Sie erneut **Windows Update** und legen Sie unter dem Punkt **Nutzungszeit** Ihre üblichen Kernarbeitszeiten fest. Windows kann erforderliche Neustarts dadurch außerhalb dieser Zeiten durchführen.

Jedes Dokument beantwortet drei Fragen für Sie:

Warum ist das notwendig? → Es erläutert den Mehrwert für Ihre Einrichtung.

Wann muss das erledigt werden? → Es ist einer Stufe und Themenbereich zugeordnet, denn Maßnahmen bauen aufeinander auf.

Wer macht das? → Es gehört zu einer der fünf Maßnahmenarten, und die sagt Ihnen, an wen das Blatt geht.

Jedes Dokument beginnt mit einer Einordnung für Sie, warum diese Maßnahme hilfreich ist, Ihr Cybersicherheits-Niveau zu verbessern und erläutert den allgemeinen Zweck. Nach dieser Einordnung erhalten Sie auch den Hinweis, wer sich um die Umsetzung dieser Maßnahme kümmern sollte, und an wen Sie die Aufgabe delegieren können. Dies wird gefolgt von der Beschreibung der notwendigen Schritte.

Jedes Dokument verfügt über eine eindeutige Kennung, unter der Sie es auf Ihrem PC finden können, und welche auf einen Blick kenntlich macht, worum es geht.

Aus der Kennung A.1.ClientSicherheit.AutoUpdate können Sie direkt ableiten, dass es eine Maßnahme für eine kleine Pflegeeinrichtung (A) ist, die Aufgabe der Stufe 1 zugeordnet wurde und sich mit dem Thema Client Sicherheit befasst. So haben Sie direkt bei der Bearbeitung immer im Blick, womit Sie sich beschäftigen. Die bereitgestellten Dokumente sind in der Regel zwei bis drei Seiten lang, so dass sie sich gut in einem Stück und begrenzter Zeit bearbeiten lassen.

Das Maßnahmenportfolio deckt die Standard-Prozesse in einer Pflegeeinrichtung sowie die wichtigsten Betriebssysteme von PCs und Mobilgeräten ab. Spezielle Konfigurationsanleitungen für Fachanwendungen können nicht bereitgestellt werden, wenden Sie sich hierzu bitte an den Hersteller Ihrer Fachanwendung.

2.1 Die fünf Maßnahmenarten und ihre Empfänger

In Ihrem Baukasten befinden sich fünf verschiedene Arten von Maßnahmen: Konfigurationen, Schulungen, Prozesse, Richtlinien, und Anschaffungen. Jede von diesen hat einen bestimmten Zweck und eine Zielgruppe:

Konfiguration

Die Handreichungen erläutern, wie ein System konfiguriert sein muss, um seine Cybersicherheit zu erhöhen. Diese Dokumente beinhalten Schritt-für-Schritt Anleitungen und können entweder durch jemand in Ihrem Team oder eine externe IT-Unterstützung (ein lokales Systemhaus, ein IT-affiner Bekannter) umgesetzt werden. Wichtig ist: *Sie müssen nicht verstehen, wie es gemacht wird – Sie müssen beauftragen und abnehmen können.*

Anschaffung

Für die Verbesserung der Informationssicherheit empfehlen wir ausgewählte Büroeinrichtung, Hard- und Software zum Erwerb. Diese begrenzt sich bewusst auf das Nötigste bei möglichst geringen Kosten. Die Dokumente bieten Ihnen hier Einkaufsempfehlungen und zeigen Ihnen auf, worauf Sie bei einem Kauf achten müssen.

Richtlinie

Es gibt wichtige Verhaltensweisen, an die sich Ihre Mitarbeiter halten müssen. Eine Richtlinie kommuniziert zum einen diese Vorgaben, verdeutlicht zum anderen auch die verbindliche notwendigen Einhaltung. Mehrere Dokumente erhalten Vorschläge für grundlegende Richtlinien zur Cybersicherheit, die Ihnen als offene Textdateien bereitgestellt werden. Passen Sie diese Vordrucke an Ihre Situation an, zum Beispiel durch das Streichen von nicht zutreffenden Aspekten, und legen sie diese allen bestehenden Mitarbeitern sowie allen Neueinstellungen zur Unterschrift vor.

Prozess

Cybersicherheit sollte keine permanenten Impulse erfordern, sondern ein guter, durchdachter Prozess regt von sich selbst Menschen zu sicherem Verhalten an. Ein Teil der Dokumente unterbreitet Vorschläge zur Gestaltung von Prozessen in Ihrer Einrichtung, und bietet hierfür unterstützende Dokumente an. Sie verankern diese Prozesse Mithilfe von Richtlinien, in denen Sie Ihre Mitarbeiter beauftragen, diese Vorgehensweisen so umzusetzen. Deshalb nennt jedes Dokument eine hauptverantwortliche Person – bei Richtlinien und Prozessen sind Sie das, auch wenn Ihre Mitarbeitenden es täglich anwenden.

Schulung

Kurze Merkblätter erläutern Ihren Mitarbeitern und Ihnen die wichtigsten Fakten und Fähigkeiten, um sich sicher online zu verhalten. Diese Schulungen laufen parallel mit der Umsetzung von anderen Maßnahmen, um allen den Zweck dieser zu erläutern und zum Mitmachen anzuregen. Schulungen sollten in regelmäßigen Abständen aufgefrischt werden, um das Wissen präsent zu halten.

Maßnahmenart	Geht an	Ihre Aufgabe dabei
Konfiguration	Ihre IT-Unterstützung	beauftragen und abnehmen
Anschaffung	Sie selbst	entscheiden und beschaffen
Richtlinie	Sie passen den Vordruck an, Ihr Team bestätigt	anpassen, unterschreiben, aushändigen, ablegen
Prozess	Sie und Ihr Team	im Arbeitsalltag verankern, Durchführung überwachen
Schulung	Ihr Team	Termin setzen, durchführen, festhalten

Ihr Team wird in den Prozess der Cybersicherheit durch Schulungen, Nutzungsregeln, und verbesserte Prozesse eingebunden. Der Baukasten ist so gestaltet, dass Sie einfach und effektiv einzelne Aufgaben delegieren können. Bei Ihnen verbleibt die Steuerung der Umsetzung, die Ablage der Nachweise, Freigaben, ggf. die Entscheidung über Ausnahmen. Eine Aufgabe bleibt in jeden Fall bei Ihnen: Die Verantwortung für die Umsetzung von Cybersicherheit.

2.2 Zusammenarbeit mit Ihrer IT-Unterstützung

„Die IT“ sieht in Einrichtungen Ihrer Größe sehr unterschiedlich aus, und die Empfehlungen unterscheiden sich:

- Ein Bekannter oder Verwandter, der sich auskennt, und kostenlos oder gegen einen Gefallen Ihre IT macht. Es ist wichtig, hier gute Absprachen zu treffen und um eine gute Dokumentation zu bitten, damit jemand anderes übernehmen kann, sollte Ihr Bekannter gerade nicht verfügbar sein.
- Ein örtlicher IT-Dienstleister im Bedarfsfall. Dieser kommt, wenn etwas installiert oder repariert werden muss, und rechnet jeden Auftrag nach Stunden ab. Um Kosten zu sparen, ist es ratsam die technischen Maßnahmen einer Etappe zu kombinieren und ein ganzes Bündel an Maßnahmen in einem Block umzusetzen.
- Niemand – Sie machen es selbst. Die Steckbriefe der ersten Etappen sind so geschrieben, dass Sie sie allein schaffen. Sobald die Komplexität für Sie steigt, sollten Sie sich für die fortgeschrittenen Aufgaben einen IT-Dienstleister oder ein Systemhaus als weitere Unterstützung suchen.

So beauftragen Sie richtig

Die Maßnahmendokumente sind Ihre gemeinsame Sprache. Sie müssen nicht formulieren, was Sie wollen – Sie geben das Blatt weiter. Darauf steht für den IT-Fachmann, was zu tun ist, und für Sie das warum und wie. Fragen Sie vorher nach dem Aufwand. „Wieviel Zeit veranschlagen Sie hierfür?“ – eine Zahl vorab verhindert die böse Überraschung auf der Rechnung und macht die Entscheidung planbar. Für viele Aufgaben geben wir Ihnen in einer Handreichung eine Einschätzung, damit Sie vorbereitet in ein Gespräch mit Ihrer IT-Unterstützung gehen.

Dokumentation ist essentiell

Im IT-Betrieb und in der Cybersicherheit gilt: alles, was nicht dokumentiert ist, existiert ggf. nicht. Verlangen Sie nach jeder Beauftragung eine kurze Rückmeldung – drei Zeilen genügen:

1. Was wurde gemacht, an welchen Geräten, wann
2. Was wurde nicht gemacht und warum
3. Wenn möglich ein Beleg: ein Bildschirmfoto, ein Ausdruck, ein Protokoll

Das ist kein Misstrauen, sondern genau der Nachweis, den Sie in Ihrer Ablage brauchen. Praktisch: Bitten Sie darum, dass die Rechnung den Steckbrief benennt – dann ist die Zuordnung automatisch dokumentiert.

Wenn es heißt: „Das ist bei Ihnen nicht nötig"

Nehmen Sie den Einwand zunächst ernst – manchmal stimmt er, dies kann zum Beispiel daran liegen, dass Sie ein bestimmtes Produkt nicht einsetzen oder das Ziel der Maßnahme bereits durch etwas anderes erreicht wird. Fragen Sie aber nach, denn hinter demselben Satz stecken drei sehr verschiedene Aussagen:

1. **„Das trifft auf Ihre Einrichtung nicht zu."** → Kein WLAN, kein Outsourcing, keine Diensthandys. Wenn eine bestimmte Technik bei Ihnen nicht vorkommt, kann eine Maßnahme entfallen. Wichtig ist nur, die Begründung kurz festzuhalten, damit später nachvollziehbar bleibt, dass es eine Entscheidung war und kein versehentliches Vergessen.
2. **„Das ist bei Ihnen schon anders gelöst."** → Lassen Sie sich zeigen oder kurz beschreiben, wie. Dann ist der Zweck der Maßnahme ebenfalls erfüllt und der Nachweis vorhanden.
3. **„Das ist aufwendig / lohnt sich nicht."** → Das ist keine fachliche, sondern eine wirtschaftliche Aussage. Die Entscheidung darüber liegt bei Ihnen, nicht beim IT Dienstleister. Sie müssen den Schaden eines Cyberangriffs tragen, also bleibt dies Ihre Entscheidung.

Die wirksamste Bitte in dieser Situation: **„Können Sie mir das kurz schriftlich begründen? Ich muss es für meine Dokumentation ablegen."** Dies unterstellt nichts und leitet eine konstruktive Diskussion ein, und führt oft dazu, dass die Sache noch einmal genauer angesehen wird. Sind Sie nicht überzeugt? Dann holen Sie sich eine zweite Meinung ein. Wenn Sie überzeugt sind, dass sich der Aufwand in diesem Fall nicht lohnt, dokumentieren Sie diese Entscheidung kurz. Der Gesetzgeber spricht explizit von Abwägungsentscheidungen: eine Maßnahme muss nicht um jeden Preis umgesetzt werden (auch wenn unser Katalog explizit solche auswählt, die preisgünstig zu realisieren sind), wenn sie wirtschaftlich nicht im Verhältnis stehen.

Zugangsdaten zu Ihren eigenen Systemen gehören Ihnen

Wenn nur Ihr Dienstleister die Zugangsdaten zu Ihren Geräten, Ihrem Router, Ihren Cloud-Konten besitzt, kommen Sie im Streitfall, bei Krankheit oder bei Geschäftsaufgabe nicht mehr an Ihre eigenen Systeme. Lassen Sie sich die Zugänge aushändigen und bewahren Sie sie sicher auf – auch wenn Sie sie nie benutzen. Somit halten Sie sich die Möglichkeit offen, sich kurzfristig selbst oder von jemand anderem helfen zu lassen.

3 Ihr Weg in vier Etappen

Die folgenden vier Etappen beschreiben Ihren Weg zu mehr Sicherheit. Sie bauen aufeinander auf, aber jede bringt für sich genommen schon einen spürbaren Zuwachs an Sicherheit – und Sie müssen nicht komplett bis zum Ende gehen, um etwas davon zu haben. Verschaffen Sie sich einen Überblick und arbeiten Sie dann mit der Etappe, die bei Ihnen ansteht.

Etappe 1 – Angriffsfläche verkleinern und Daten sichern

Im ersten Schritt geht es darum, die häufigsten Einbruchswege zu schließen und dafür zu sorgen, dass Sie nach einem Ausfall wieder arbeitsfähig werden können. Sie bringen Ihre Software auf den neuesten Stand, aktivieren den Schutz gegen Schadsoftware, schützen Administrationszugänge und sichern Ihren E-Mail-Verkehr ab, sodass Kriminelle mit schädlichen Anhängen nicht so einfach Ihre Computer übernehmen können. Ferner richten Sie Ihr WLAN sicher ein, und Ihre Mitarbeiter lernen die wichtigsten Grundlagen zum sicheren Umgang mit IT. Nach dieser Etappe ist Ihr Schutz spürbar besser: Die Wege, über die Angriffe üblicherweise beginnen, sind verschlossen. Und mit der Datensicherung liegt die Grundlage dafür, nach einem Ausfall wieder handlungsfähig zu werden.

Parallel hierzu etablieren Sie eine kontinuierliche Datensicherung, die Ihnen die Grundlage für eine möglichst unterbrechungsfreie Weiterarbeit bei einem Ausfall in der Zukunft geben wird. Sie führen mithilfe von Checklisten ein geregeltes Vorgehen für die Einstellung und den Austritt von Mitarbeitern ein, so dass Zugänge entstehen, wenn jemand anfängt, und verschwinden, wenn jemand geht.

Etappe 2 – Sicherheit in den Alltag bringen

Nachdem die Technik im Büro abgesichert ist, nimmt die zweite Etappe alles in den Blick, was Ihr Büro verlässt oder von außen hineinreicht. Sie härten Ihre Systeme weiter ab und schalten für die wichtigsten Zugänge eine Anmeldung mit zweitem Faktor ein, sodass ein gestohlenes Kennwort allein nicht mehr genügt, um hineinzukommen. Sie regeln, wie mobile Geräte eingerichtet, genutzt und beim Ausscheiden wieder eingesammelt werden, und wie unterwegs auf Tour oder von zuhause aus gearbeitet wird.

Sie etablieren Wege wie Auffälligkeiten erkannt und gemeldet werden: Wer eine merkwürdige E-Mail erhält oder ein Gerät verliert, muss wissen, an wen er sich sofort wendet – so dass eine frühe Meldung Schaden verhindert. Schließlich klären Sie die Zusammenarbeit mit Ihren Dienstleistern: wer welche Aufgabe übernimmt, worauf er Zugriff hat und was Sie im Gegenzug an Rückmeldung erwarten. Mit dieser Etappe kommt das zweite Versprechen

hinzu: Richtlinien, Meldewege und die Vereinbarungen mit Ihren Dienstleistern sind genau das, wonach eine Prüfung oder ein Kostenträger fragt. Sie können nun nicht nur sicher arbeiten, sondern es auch belegen.

Etappe 3 – Mobile Geräte und Wege nach außen

Die dritte Etappe nimmt die Geräte in den Blick, die Ihr Haus verlassen: die Smartphones und Tablets, mit denen Ihre Mitarbeitenden unterwegs dokumentieren und auf E-Mails zugreifen. Sie entscheiden zuerst, ob Sie diese Geräte einzeln einrichten oder über eine zentrale Verwaltung, und richten dann die Einstellungen ein, die ein verlorenes Gerät harmlos machen: Sperrcode, automatische Updates und die Möglichkeit, aus der Ferne zu löschen. Sie prüfen, wie lange der Hersteller noch Sicherheitsupdates liefert – bei älteren Geräten ist dieser Zeitraum häufig abgelaufen –, schalten nicht benötigte Funkschnittstellen ab, erlauben nur freigegebene Apps und erkennen Geräte, an denen die Schutzmechanismen des Betriebssystems ausgehebelt wurden. Eine Nutzungsrichtlinie macht Ihren Mitarbeitenden klar, was auf einem Dienstgerät erlaubt ist.

Dazu kommen die übrigen Wege nach außen. Den Webbrowser stellen Sie so ein, dass er weniger Angriffsfläche bietet, denn er holt täglich fremde Inhalte ins Haus. Externe Personen – Zeitarbeitskräfte, Praktikanten, Wartungsfirmen – erhalten nur die Räume und Zugänge, die sie für ihre Aufgabe benötigen, und geben sie am Ende nachweisbar zurück. Und Sie legen fest, wie bei einem Umzug Geräte und Unterlagen sicher transportiert und wieder angeschlossen werden. Diese Etappe verbessert Ihren Schutz dort, wo Sie am wenigsten unmittelbar eingreifen können: außerhalb Ihrer Räume. Ein Gerät, das gesperrt, verschlüsselt und aus der Ferne löschbar ist, bleibt bei Verlust ein Ärgernis und muss nicht zwangsläufig als Datenschutzvorfall gemeldet werden.

Etappe 4 – Vorfälle beherrschen

Der vierte Schritt bereitet Sie auf den Fall vor, dass trotz aller Vorkehrungen etwas passiert. Sie haben nun Pläne, was in den ersten Stunden zu tun ist: wer benachrichtigt wird, wer entscheidet, welche Geräte sofort vom Netz genommen werden und wie Sie Ihre Touren notfalls auf Papier weiterführen und weiterhin abrechnen können. Auf einem Notfallzettel neben dem Telefon stehen die Nummern, die Sie in diesem Moment brauchen – Ihre IT-Unterstützung, der Anbieter Ihrer Pflegesoftware, Ihre Versicherung.

Dazu gehört, den Wiederanlauf einmal tatsächlich durchzuspielen, statt ihn nur aufzuschreiben: Wie lange dauert es wirklich, bis Ihre Pflegedokumentation aus der Datensicherung wieder verfügbar ist? Wie arbeiten Sie ohne Internet und IT-Unterstützung weiter? Wer das einmal geprobt hat, weiß im Ernstfall, woran er ist, und kann An- und Zugehörigen und Mitarbeitern eine belastbare Auskunft geben. Schließlich beschäftigen Sie sich mit der Sicherheit Ihrer Dienstleister, zum Beispiel der externen IT-Unterstützung, Cloud-Anbietern oder dem Hersteller Ihrer Pflegedokumentation. Diese Etappe hat

die wenigsten Aufgaben, aber die anspruchsvollsten: Hier wird geschrieben und geübt, und Sie erreichen nicht nur Sicherheit, sondern auch Resilienz gegen Cyberangriffe. Diese Etappe löst das Versprechen der Handlungsfähigkeit ein, und zwar belastbar: nicht weil es aufgeschrieben ist, sondern weil Sie es einmal durchgespielt haben und wissen, wie lange es dauert.

4 Dranbleiben: der regelmäßige Zyklus

Maschinen wie ein Auto, ein Aufzug oder ein Flugzeug müssen regelmäßig gewartet werden – so verhält es sich auch mit Cybersicherheit. Auch hier muss man regelmäßig einen Kontrolltermin machen, um sicherzugehen, dass alles in Ordnung ist, weil sich der Betrieb verändert oder eine Software eventuell eine Störung hat. Wer Etappe 1 und 2 erreicht hat, braucht dafür etwa fünf Stunden im Jahr.

Durch regelmäßiges Überprüfen Ihrer Maßnahmen beugen Sie verschiedenen Situationen vor:

- Die Datensicherung lief zwölf Monate zuverlässig und seit Februar nicht mehr. Gemerkt hat es niemand, weil eine Sicherung, die nicht läuft, keinen Lärm macht. Jetzt wo der Computer kaputt ist, brauchen Sie die gesicherten Daten, um weiterzuarbeiten, aber das Backup ist leider veraltet.
- Die Aushilfe vom letzten Sommer hatte noch immer einen Zugang zur Pflegesoftware. Ihr wurde nun ihr Handy gestohlen mit allen Zugangsdaten – sind damit auch die Daten Ihrer Pflegebedürftigen in falsche Hände gelangt?
- Vor zwei Jahren haben Sie alle Laptops verschlüsseln lassen. Das Gerät, das Sie im Frühjahr nachgekauft haben, ist nach zwei Monaten defekt und muss zur Garantiereparatur. Wurde bei dem Neugerät die Festplattenverschlüsselung eingeschaltet, so dass Ihre Daten während der Reparatur vor Zugriffen geschützt sind?

Alle drei Situationen sind beherrschbar, wenn Sie die passenden Maßnahmen etabliert haben – und wenn diese zum Zeitpunkt des Vorfalls noch aktiv sind. Genau das prüft der Kontrolltermin. Die Verschlüsselung Ihrer Geräte schützt Sie eben nur dann, wenn Sie sie nicht nur heute einrichten, sondern bei jeder Neuanschaffung wiederholen. Deshalb braucht es einen festen Termin statt guter Vorsätze.

Einmal im Monat, einmal im Jahr

Bevor ein Pilot den Start vorbereitet, untersucht er kurz den Zustand des Flugzeugs: sind die Reifen intakt, gibt es äußerliche Beschädigungen, die beim nächsten Flug ein Problem werden könnten? Etwa alle ein bis zwei Jahre kommen Flugzeuge zur großen Wartung in den Hangar, bei der alles einmal durchgeschaut wird.

Nach diesem Vorgehen organisieren auch Sie Ihre Kontrolltermine. Einmal im Monat überprüfen Sie, ob wichtige Punkte für Ihre Cybersicherheit noch wie erwartet funktionieren und aktuell sind:

- **Datensicherung:** Überprüfen Sie, ob das Backup weiterhin im eingestellten Rhythmus läuft und komplett durchläuft. Ein Backup ist jedoch nur nützlich, wenn sich Daten daraus wiederherstellen lassen und bei so manchem Vorfall gab es dann ein böses Erwachen. Probieren Sie, ob Sie eine einzelne Datei aus der Datensicherung erfolgreich zurückholen können.
- **Updates:** Überprüfen Sie für alle Ihre Geräte, ob diese weiterhin automatisch nach Updates suchen und diese installieren. Der letzte Überprüfungsversuch sollte nicht länger als 2 Tage zurückliegen. Damit stellen Sie sicher, dass im Hintergrund keine Schwachstelle lauert, über die Kriminelle einbrechen können.

Beides zusammen dauert nicht länger als 10 Minuten. Tipp: Koppeln Sie diese Überprüfung an etwas, das ohnehin monatlich passiert – dies könnte die Abrechnung zum Monatsende sein.

Einmal im Jahr folgt dann die große Prüfung. In diesem Termin überprüfen Sie die wichtigsten Punkte Ihrer Cybersicherheit:

1. **Datensicherung** – einmal vollständig prüfen: Werden wirklich alle wichtigen Daten erfasst? Ist noch Platz? Läuft es auf allen Geräten?
2. **Zugänge** – Wer hat noch Zugriff worauf? Alle Konten von Ausgeschiedenen entfernen.
3. **Geräte** – Welche Geräte sind im Einsatz, welche liegen ungenutzt herum, welche fehlen? Ungenutzte sicher löschen.
4. **Mitarbeiter** – Kurze Auffrischung für alle, Nachschulung für alle, die neu dazugekommen sind.
5. **Notfallzettel** – Stimmen die Nummern noch? Ist der Zettel dort, wo er hingehört?
6. **IT-Unterstützung** – Ist die Zusammenarbeit noch geregelt? Liegen die Administratorzugänge bei Ihnen? Gibt es einen gültigen Auftragsverarbeitungsvertrag?
7. **Richtlinien** – Sind diese noch aktuell, und von allen unterschrieben, die seither dazugekommen sind?
8. **Dokumentation** – Sind die Dokumentationen auf dem aktuellsten Stand?

Hängen Sie auch hier den Termin an etwas Bestehendes – die jährlichen Pflichtunterweisungen Ihrer Mitarbeiter oder den Jahresabschluss. Ein zusätzlicher, freistehender Termin wird verschoben; ein angehängter nicht.

Eine solche Jahresprüfung kostet Sie etwa drei Stunden, spart Ihnen aber viel Zeit, indem Sie einen Cyberangriff vermeiden können bzw. schneller wieder arbeitsfähig werden.

Jede Jahresrunde dokumentieren Sie als ein datiertes und unterschriebenes Blatt in der Ablage. Das kostet Sie eine Minute und ist genau das, was im Ernstfall zeigt, dass Sie Ihrer Sorgfaltspflicht nachgekommen sind – gegenüber Prüfern, gegenüber Ihrer Versicherung, gegenüber An- und Zugehörigen.

Und wenn Sie eine Überprüfungsrunde verpasst haben? Das passiert. Fangen Sie nicht von vorn an – nehmen Sie sich drei Punkte vor: Holen Sie testweise eine Datei aus der Sicherung zurück, gehen Sie die Zugänge durch und überprüfen Sie kurz die Geräte. Damit haben Sie die typischen Risiken abgeräumt, die in der Zwischenzeit gewachsen sind. Der Rest kann bis zum nächsten Termin warten.

Was nicht auf den Jahrestermin warten kann

Manche Ereignisse rufen eine Maßnahme sofort auf. Dies passiert am häufigsten bei einem Personalwechsel, und jeder Wechsel berührt gleich mehrere Maßnahmen. Auch ein neues Gerät, eine Reparatur oder eine neue Software sind Anlässe, einmal über die wesentlichen Punkte zu schauen.

Wenn das passiert …	… holen Sie das hervor
Neuer Mitarbeiter	Onboarding, Richtlinien aushändigen und unterschreiben lassen, Schulung
Mitarbeiter verlässt den Betrieb	Offboarding: Zugänge sperren, Geräte und Schlüssel zurück
Neues Gerät kommt ins Haus	Grundeinrichtung, in die Geräteliste, in die Datensicherung
Gerät wird ausgemustert oder verkauft	Sicheres Löschen
Gerät geht verloren oder wird gestohlen	Sofort: sperren, Kennwörter ändern, Meldepflichten prüfen
Neue Software oder neuer Cloud-Dienst	Wer hat Zugriff, wo liegen die Daten, Vertrag prüfen
Wechsel der IT-Unterstützung	Zugänge übernehmen, Vertrag neu, Notfallnummer aktualisieren
Umzug oder neue Räume	WLAN neu einrichten, physischer Schutz der Geräte
Verdacht auf einen Vorfall	Notfallzettel

Damit diese Punkte automatisch passieren, betten wir sie in Prozesse ein. Eine Einstellungs- und Austrittscheckliste sorgt dafür, dass zur Einstellung Richtlinien unterschrieben werden und bei Verlassen Zugänge auch wieder gelöscht werden. Die Inventarisierung bei Kauf hilft Ihnen jederzeit den Überblick zu behalten.

5 Wenn es hakt

Die vorliegenden Dokumente wurden vor Ort mit Einrichtungen getestet, und Ihre IT-Unterstützung sollte Sie Mithilfe der vorliegenden Informationen gut betreuen können. Nichtsdestotrotz können sich in besonderen Situationen Fragen ergeben, die durch die vorliegenden Dokumente nicht abgedeckt werden. Das Kompetenzzentrum Digitalisierung und Pflege stehen Ihnen als Kontakt zur Verfügung:

Kompetenzzentrum Digitalisierung und Pflege
des GKV Spitzenverbands

www.kompetenzzentrum-pflege.digital

kontakt@kompetenzzentrum-pflege.digital

VPN
0100
1010