Kompetenzzentrum
Digitalisierung und Pflege

Wegweiser für Organisationstyp C (Ambulanter Pflegedienst mit selbstverwalteter IT)

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 21

Dieses Dokument ist die begleitende Regieanweisung für Organisationstyp C (Ambulanter Pflegedienst mit selbstverwalteter IT). 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: *einen ambulanten Pflegedienst mit acht bis sechzehn Mitarbeitern - mehrere Arbeitsplätze im Büro, ein gemeinsamer Dateiserver oder ein Netzlaufwerk, eine eigene E-Mail-Domain, Diensthandys und Tablets auf Tour, und eine IT, die Sie selbst verwalten und für die Sie ein örtliches Systemhaus hinzuziehen.* Die IT muss laufen, läuft aber nebenher. Sie kümmern sich neben der Pflege um Buchhaltung, Abrechnung und Personal - und in einem Betrieb Ihrer Größe ist die IT inzwischen zu groß, um sie nebenbei zu überblicken, aber zu klein für eine eigene Stelle. Genau dafür ist dieses Material gemacht. 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 im Grundlagendokument, 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 Dateiserver, auf dem Dokumentation und Abrechnung liegen, startet nicht mehr – und damit arbeitet nicht ein Arbeitsplatz nicht mehr, sondern das ganze Büro. 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 Mitarbeiter werden geschult und eingebunden, die Steuerung und Prüfung bleibt bei Ihnen. In einem Betrieb Ihrer Größe ist „die IT-Unterstützung" oft zweigeteilt: jemand im Team, der sich auskennt und das Tagesgeschäft macht, und ein Systemhaus für alles, was darüber hinausgeht. Legen Sie einmal fest, wo die Grenze verläuft – sonst bleibt beides am Ende bei Ihnen hängen. Ihre Kernaufgabe ist hier insbesondere, den Überblick zu behalten, die Impulse zu setzen und die Umsetzung zu kontrollieren.

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 23 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** sichern wir das Büro ab: den gemeinsamen Dateiserver, das Netz, die Zugänge von außen und die E-Mail. In der **dritten Etappe** nehmen wir die mobilen Geräte und die übrigen Wege nach außen in den Griff. 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 mittelgroße ambulante Pflegedienste, die ihre IT selbst verwalten, besteht aus insgesamt 83 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.

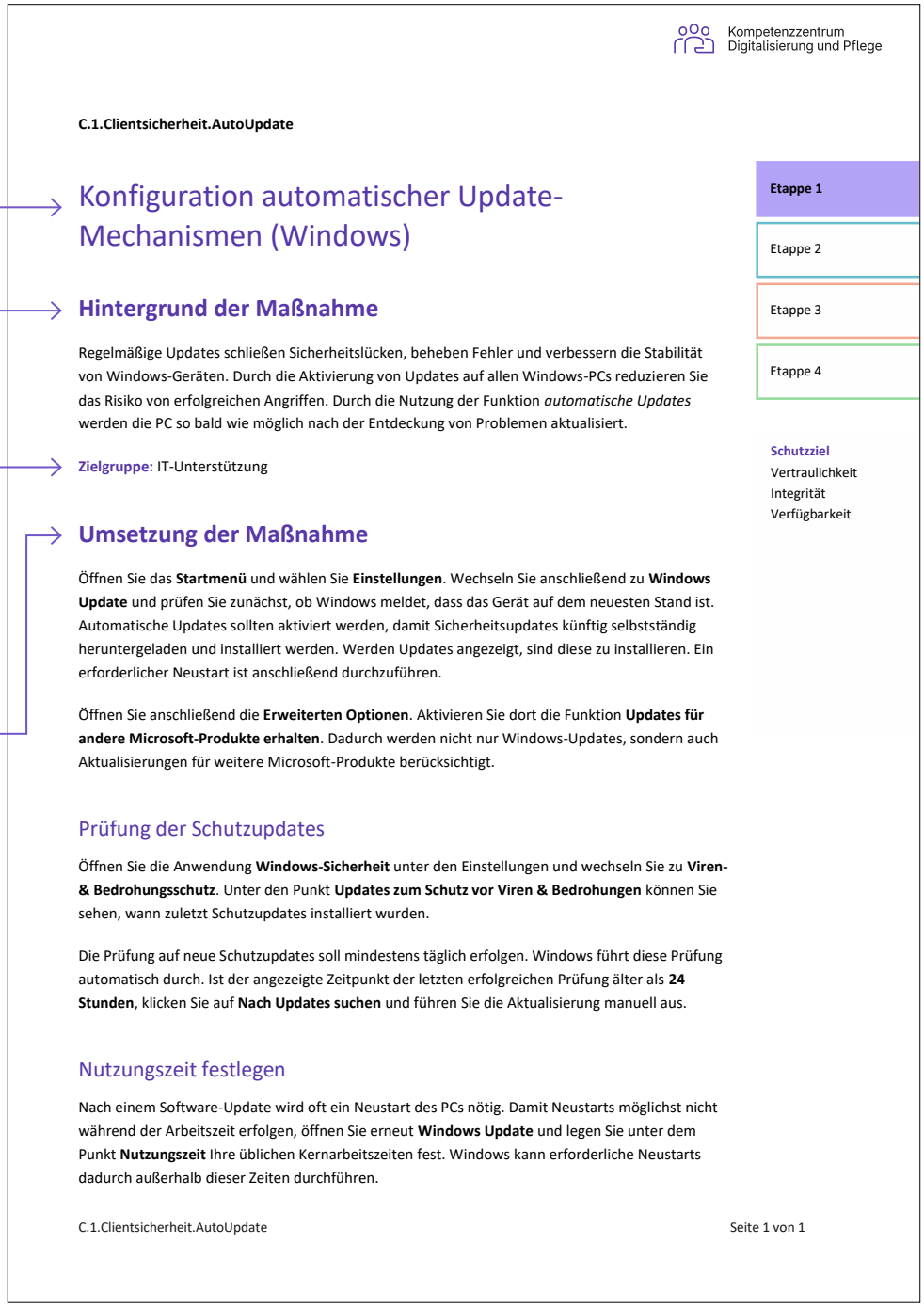
Alle Ihnen vorliegenden Dokumente folgen der gleichen Struktur, nehmen wir das Dokument zur Aktivierung der automatischen Windows Updates als Beispiel:

Titel der Maßnahme zur Orientierung

Bitte lesen Sie dies unbedingt, bevor Sie 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

C.1.Clientsicherheit.AutoUpdate

Konfiguration automatischer Update-Mechanismen (Windows)

Etappe 1
Etappe 2
Etappe 3
Etappe 4

Schutzziel
Vertraulichkeit
Integrität
Verfügbarkeit

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

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.

C.1.Clientsicherheit.AutoUpdate Seite 1 von 1

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 C.1.Clientsicherheit.AutoUpdate können Sie direkt ableiten, dass es eine Maßnahme für einen mittelgroßen ambulanten Pflegedienst (C) 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. Klickanleitungen für einzelne Fachanwendungen können wir nicht bereitstellen, dafür gibt es zu viele Produkte und Versionsstände. Was Sie bekommen, ist die Liste der Anforderungen, die Sie gegenüber dem Hersteller stellen – für die Pflegesoftware liegt dafür ein eigenes Blatt bei. Die Umsetzung bleibt beim Hersteller, die Anforderung und die Abnahme bei Ihnen.

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. Einen Teil davon setzt in Ihrem Betrieb jemand aus dem Team um, den schwierigeren Teil Ihr Systemhaus. Entscheiden Sie das je Blatt und halten Sie es fest – so entsteht nebenbei die Aufgabenteilung, nach der im nächsten Abschnitt gefragt wird. **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	Ihr Team oder Ihr Systemhaus, je nach Blatt	zuordnen, 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 Betrieben Ihrer Größe meist zweigeteilt aus, und für beide Teile gelten eigene Empfehlungen:

- **Jemand im Team, der sich kümmert.** In vielen Pflegediensten ist das die Verwaltungskraft, die Pflegedienstleitung oder ein technisch interessierter Mitarbeiter – meist ohne Stellenanteil dafür. Das funktioniert im Alltag gut und hat ein Risiko: Fällt diese Person aus oder verlässt sie den Betrieb, weiß niemand, wie etwas eingerichtet ist. Bestehen Sie deshalb auf kurzer schriftlicher Dokumentation und darauf, dass die Zugänge nicht nur in einem Kopf liegen. Geben Sie dieser Person außerdem einen festen Zeitanteil; eine Aufgabe, die „nebenbei" erledigt wird, wird in der ersten vollen Woche liegengelassen.
- **Ein örtliches Systemhaus.** Es kommt für das, was darüber hinausgeht - Server, Netz, Fernzugriff, Störungen. Abgerechnet wird meist nach Stunden. Um Kosten zu sparen, ist es ratsam, die technischen Maßnahmen einer Etappe zu bündeln und ein ganzes Paket in einem Block umzusetzen, statt wegen jeder Einstellung einen Termin zu verbrauchen. Prüfen Sie ab dieser Größe, ob sich statt der Abrechnung im Bedarfsfall ein Wartungsvertrag mit fester Reaktionszeit lohnt – Sie haben inzwischen Systeme, deren Ausfall den ganzen Betrieb trifft.

Legen Sie die Grenze zwischen beiden einmal schriftlich fest: Was macht das Team selbst, was geht an das Systemhaus, und wer darf es beauftragen.

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. Das gilt auch nach innen: Wenn nur ein Mitarbeiter die Kennwörter zum Dateiserver, zum Router und zu den Cloud-Konten kennt, haben Sie dasselbe Problem wie bei einem Dienstleister, der nicht herausrückt - nur mit mehr Verlegenheit. Ein Passwortmanager mit einem Notfallzugang für die Leitung löst das; ein Blatt dazu liegt in Etappe 1.

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. Sie bringen die Software auf den aktuellen Stand, aktivieren den Schutz gegen Schadsoftware, sichern den E-Mail-Verkehr ab, stellen Office so ein, dass ein Anhang nicht mehr ungefragt ausgeführt wird, und regeln den Umgang mit USB-Sticks und externen Datenträgern. Für die Grundeinstellungen liegt ein Sammelblatt bei, das die Einzelblätter zusammenfasst, wenn jemand die Geräte ohnehin in der Hand hat.

Zwei Themen sind in einem Betrieb Ihrer Größe neu gegenüber einem Ein-Personen-Büro. Erstens die gemeinsame Datenablage: Wo liegen die Dateien, wer legt wo ab, und was hat auf einem lokalen Desktop nichts verloren? Ohne diese Festlegung nützt die beste Sicherung wenig, weil sie die Hälfte der Daten nicht erfasst. Zweitens die Kennwörter: Bei acht bis sechzehn Personen lassen sie sich nicht mehr im Kopf oder auf einem Zettel verwalten – ein Passwortmanager ist ab hier Grundausstattung, nicht Kür.

Dazu kommen die Themen, die mit Menschen zu tun haben: Checklisten für Eintritt und Austritt, damit Zugänge entstehen, wenn jemand anfängt, und verschwinden, wenn jemand geht; die Vertraulichkeitserklärung; und zwei Richtlinien, die festhalten, was im Betrieb gilt – für die Benutzung der Geräte und für das Büro. Auch die Pflegesoftware und der dienstlich genutzte Messenger bekommen in dieser Etappe ihre Grundregeln.

Parallel etablieren Sie die Datensicherung: planen, einrichten, und – der Punkt, an dem die meisten scheitern – einmal prüfen, ob sich daraus tatsächlich etwas zurückholen lässt.

Nach dieser Etappe sind die üblichen Einbruchswege verschlossen, die Daten liegen geordnet und gesichert, und es ist geregelt, wer im Betrieb worauf Zugriff bekommt.

Etappe 2 – Sicherheit in den Alltag bringen

Die zweite Etappe nimmt die Technik in den Blick, die allen gemeinsam gehört. Im Mittelpunkt steht der Dateiserver: Sie planen ihn, richten ihn ein und legen fest, wer welche Ordner sieht. Das ist der größte Einzelschritt dieses Katalogs und zugleich der mit der größten Wirkung, denn hier liegen Pflegedokumentation, Abrechnung und Personalunterlagen nebeneinander.

Um ihn herum sichern Sie die Wege ab, über die von außen zugegriffen wird: ein Zugang per VPN statt offener Fernwartung, eine Anmeldung mit zweitem Faktor für die wichtigsten Zugänge, und klare Regeln für die Fernunterstützung durch Ihr Systemhaus. Das Netz wird getrennt, sodass Gäste und Privatgeräte nicht dort hängen, wo die Fachanwendungen arbeiten, und Router, Multifunktionsgerät und WLAN bekommen ihre eigenen Einstellungen und Updates – Geräte, an die niemand denkt und die jeder im Haus erreichen kann.

Bei der E-Mail geht es ab dieser Größe nicht mehr nur um den Posteingang: Sie schützen Ihre eigene Domain davor, dass in Ihrem Namen geschrieben wird, und schalten einen professionellen Spam- und Schadsoftwarefilter vor. Dazu härten Sie die Rechner weiter ab, verschlüsseln die Festplatten und stellen den Webbrowser enger.

Organisatorisch kommen drei Dinge hinzu: der Meldeweg für Auffälligkeiten – wer eine merkwürdige E-Mail bekommt oder ein Gerät verliert, muss wissen, an wen er sich sofort wendet –, die Meldepflichten im Datenschutz mit ihren 72 Stunden, und die Beschaffungsregeln, damit das nächste Gerät nicht wieder einzeln eingerichtet werden muss.

Mit dieser Etappe kommt das zweite Versprechen hinzu: Richtlinien, Meldewege und die Übersicht über Ihre Arbeitsplätze 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 Büro verlassen: die Smartphones und Tablets, mit denen Ihre Mitarbeiter unterwegs dokumentieren und auf E-Mails zugreifen. Sie entscheiden zuerst, ob Sie diese Geräte einzeln einrichten oder über eine zentrale Verwaltung – bei acht bis sechzehn Mitarbeitern ist das die Schwelle, ab der sich die Verwaltung rechnet; für beide Wege liegt ein Blatt bei. Dann richten Sie die Einstellungen ein, die ein verlorenes Gerät harmlos machen: Sperrcode, automatische Updates, Verschlüsselung und die Möglichkeit, aus der Ferne zu löschen. Sie prüfen, wie lange der Hersteller noch Sicherheitsupdates liefert, schalten nicht benötigte Funkschnittstellen ab, erlauben nur freigegebene Apps und erkennen Geräte, an denen die Schutzmechanismen des Betriebssystems ausgehebelt wurden. Eine Nutzungsrichtlinie macht Ihren Mitarbeitern klar, was auf einem Dienstgerät erlaubt ist.

Dazu kommt, wie auf Tour und von unterwegs gearbeitet wird – der Zugriff aus dem Auto, aus der Wohnung eines Patienten, aus dem fremden WLAN –, und die Regeln dafür.

Schließlich die Wege nach außen, die keine Geräte sind: Externe Personen – Zeitarbeitskräfte, Praktikanten, Wartungsfirmen – erhalten nur die Räume und Zugänge, die sie für ihre Aufgabe benötigen, und geben sie am Ende nachweisbar zurück. Sie klären die Zusammenarbeit mit Ihren Dienstleistern und Cloud-Anbietern: wer welche Aufgabe übernimmt, worauf er Zugriff hat, was Sie an Rückmeldung erwarten. Sie regeln den laufenden Betrieb des Dateiservers, halten fest, wie bei einem Umzug Geräte und Unterlagen sicher transportiert werden, und sorgen dafür, dass nach einem Vorfall überhaupt Spuren da sind, an denen sich nachvollziehen lässt, was geschehen ist.

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 – Ihr Systemhaus, 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? Bei einem eigenen Dateiserver ist diese Frage schärfer als bei einzelnen Rechnern – fällt er aus, steht das ganze Büro, und die Antwort entscheidet, ob Sie einen Tag oder eine Woche auf Papier arbeiten.

In dieselbe Etappe gehört das Arbeiten von zuhause: Wer Abrechnung, Dienstplanung oder Verwaltung zeitweise von zuhause erledigt, braucht einen eingerichteten Arbeitsplatz, eine Absprache darüber, was dort liegen darf, und eine Richtlinie, die beides verbindlich macht.

Diese Etappe hat die wenigsten Aufgaben, aber die anspruchsvollsten: Hier wird geschrieben und geübt. Sie 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 acht bis zehn Stunden im Jahr: rund eine Viertelstunde im Monat für die kurze Kontrolle, und fünf bis sechs Stunden für den Jahrestermin. Der Unterschied zu einem kleinen Pflegedienst sind nicht mehr Punkte, sondern mehr Personen und der Dateiserver: Zugänge ändern sich häufiger, und die Prüfung der Sicherung betrifft nicht mehr einzelne Rechner, sondern den Bestand, von dem alle arbeiten.

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. Prüfen Sie dabei ausdrücklich, ob die Sicherung den Dateiserver vollständig erfasst und ob sie auch die Daten einschließt, die noch auf einzelnen Rechnern liegen. Die Rückholprobe machen Sie einmal im Quartal mit einer Datei vom Server, nicht nur mit einer vom eigenen Arbeitsplatz.
- 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? Gehen Sie dabei die Ordner auf dem Dateiserver durch, nicht nur die Benutzerkonten: Die Konten sind meist richtig, die Freigaben wachsen still mit. Alle Konten von Ausgeschiedenen entfernen, Zeitarbeitskräfte und Praktikanten ausdrücklich mit.
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, und stimmt die Grenze zwischen dem, was das Team macht, und dem,

was das Systemhaus macht? Liegen die Administratorzugänge bei Ihnen, und zwar nicht nur bei einer einzelnen Person? 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?

9. **Dateiserver** – Läuft er noch auf einem unterstützten Stand, ist genug Platz da, und stimmen die Freigaben noch mit der Aufgabenverteilung im Betrieb überein?

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, Freigaben auf dem Dateiserver prüfen, Geräte und Schlüssel zurück
Neues Gerät kommt ins Haus	Grundeinrichtung, in die Geräteliste, in die Datensicherung
Gerät wird ausgemustert oder verkauft	Sicheres Löschen

Wenn das passiert ...	... holen Sie das hervor
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
Zeitarbeitskraft oder Praktikant fängt an	Externe: befristeter Zugang, Vertraulichkeit, Rückgabe terminieren
Die Person, die sich um die IT kümmert, fällt aus oder geht	Zugänge und Dokumentation übernehmen, Systemhaus informieren, Notfallnummern aktualisieren
Neuer Ordner oder neue Freigabe auf dem Dateiserver	Wer darf hinein, gehört er in die Sicherung

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