Kompetenzzentrum
Digitalisierung und Pflege

Wegweiser für Organisationstyp B (Tagespflege und kleine stationäre Einrichtung)

Cybersicherheitsmaßnahmen planen und priorisieren

Inhaltsverzeichnis

1 Einleitung 3
2 Der Baukasten 7
3 Ihr Weg in vier Etappen 15
4 Dranbleiben: der regelmäßige Zyklus 19
5 Wenn es hakt 23

Dieses Dokument ist die begleitende Regieanweisung für Organisationstyp B (Tagespflege oder kleine stationäre Einrichtung). 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 Tagespflege oder eine kleine stationäre Einrichtung mit ca. 30 Plätzen, mit einem Rechner im Dienstzimmer, der im Schichtbetrieb von wechselnden Personen genutzt wird, Tablets für die Pflegedokumentation, einem eigenen Netz im Haus – und mit einer IT, die extern bereitgestellt wird.* Die IT muss laufen, läuft aber nebenher! Sie haben Dienstplan, Belegung, Angehörige, Qualitätsmanagement und Prüfungen gleichzeitig zu bedienen, und die IT ist formal nicht Ihre Aufgabe. Ausfallen tut sie trotzdem bei Ihnen: Wenn der Rechner im Dienstzimmer morgens nicht startet, hilft es niemandem, dass die Zuständigkeit woanders liegt. 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, der Fahrdienst steht am Morgen nicht zur Verfügung und die Gäste warten zuhause, oder der Rechner im Dienstzimmer startet nicht mehr – und mit ihm hängen Dienstplan, Medikationsübersicht und Übergabe fest. 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. Bleibt beispielsweise die Pflegedokumentation am Wagen im Flur liegen, während alle im Wohnbereich sind, oder steht das Dienstzimmer offen, während Besucher und Handwerker durch das Haus gehen, dann ist das ein Problem, bei dem die IT wenig ausrichten kann. Das Bewusstsein der Mitarbeiter ist hier gefragt – und eine klare Absprache, wer das Dienstzimmer zusperrt. Für beides finden Sie in Ihrem Baukasten eigene Blätter. Nutzen Ihre Mitarbeiter ihr privates Handy zur betrieblichen Kommunikation – etwa einen Dienstgruppen-Chat, in dem die Spätschicht der Frühschicht noch etwas zu einer Bewohnerin schreibt? Dann liegen diese Angaben auf privaten Geräten, und bei Vertragsende verbleiben betriebliche Informationen oder Daten der Pflegebedürftigen dort - 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 Ihrer Einrichtung betrifft, muss die Initiative hierfür zwingend von Ihnen ausgehen. Verantwortlich im Rechtssinne ist Ihr Träger; verantwortlich dafür, dass es im Haus tatsächlich geschieht, sind Sie. Das lässt sich sauber trennen:

- **Bei Ihnen vor Ort liegt**, was mit Menschen und Abläufen zu tun hat – Ihre Mitarbeiter schulen und einbinden, Richtlinien aushändigen und unterschreiben lassen, Prozesse im Schichtbetrieb verankern, Nachweise ablegen.
- **Beim Träger fordern Sie an und nehmen ab**, was Technik, Beschaffung und Verträge betrifft. Sie müssen nicht wissen, wie es gemacht wird. Sie müssen anfordern können, was auf dem Blatt steht, und erkennen, ob es erledigt ist.

Daraus folgt die einzige zusätzliche Pflicht, die Sie gegenüber einer Einrichtung mit eigener IT haben: Halten Sie fest, was Sie angefordert haben und was daraus geworden ist. Das ist keine Bürokratie, sondern Ihr Nachweis – eine Anforderung, die beim Träger liegt und dokumentiert ist, steht im Prüfungsfall anders da als eine, die nur mündlich fiel. Da Cybersicherheit mehr als nur ein IT-Thema ist, lässt sie sich ohnehin 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. 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 24 Aufgaben. Ihr persönlicher Aufwand für die Leitungsaufgaben der Umsetzung liegt meist bei weniger als einer Stunde pro Aufgabe. Unterscheiden Sie dabei Aufwand und Durchlaufzeit: Bei den technischen Aufgaben kommt der Weg über den Träger hinzu – anfordern, nachfassen, abnehmen. Ihre Arbeitszeit bleibt die knappe Stunde, bis zur Erledigung können aber Wochen vergehen. Planen Sie deshalb nicht Aufgabe für Aufgabe, sondern halten Sie mehrere Anforderungen gleichzeitig bei Ihrer IT-Unterstützung offen und arbeiten Sie in der Zwischenzeit an dem, was bei Ihnen im Haus liegt. 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** nehmen wir das Haus in den Blick: das Netz, die Räume, den Schichtwechsel und die Zusammenarbeit mit Dienstleistern. In der **dritten Etappe** bringen wir die mobilen Geräte 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 Dienstzimmer 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 Tagespflegen und kleine stationäre Einrichtungen, deren IT beim Träger liegt, besteht aus insgesamt 80 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.

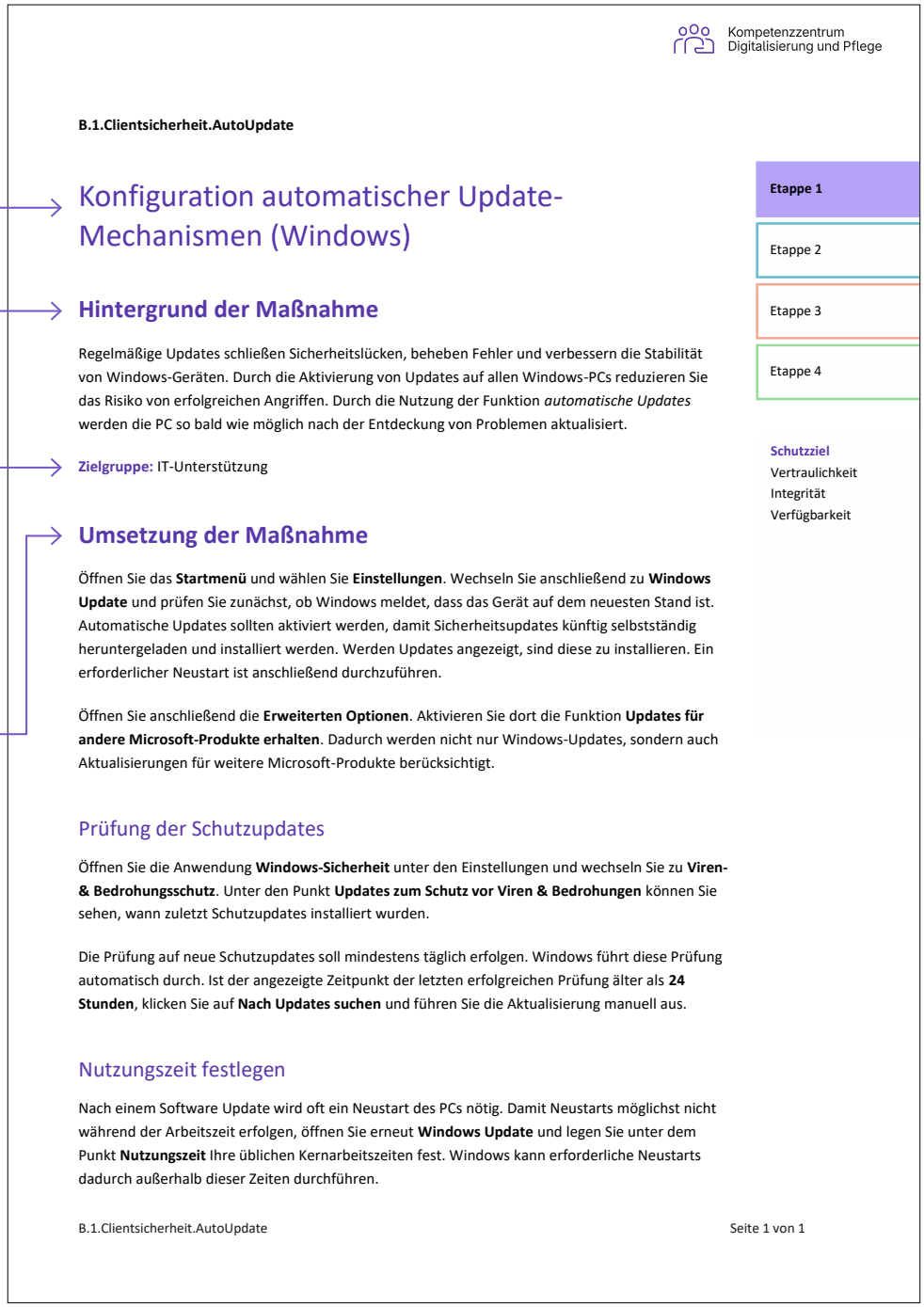
Alle Ihnen vorliegenden Dokumente folgen der gleichen Struktur, nehmen wir das Dokument zur Aktivierung der automatischen Windows Updates als Beispiel:

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

B.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.

B.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 aber auch im Web-Portal finden können, und welche auf einen Blick kenntlich macht, worum es geht. Aus der Kennung B.1.Clientsicherheit.AutoUpdate können Sie direkt ableiten, dass es eine Maßnahme für eine Tagespflege oder kleine stationäre Einrichtung (B) ist, die Aufgabe der Stufe 1 zugeordnet wurde und sich mit dem Thema Clientsicherheit 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 oder dem Träger stellen. 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 und gehen an Ihre IT-Unterstützung.

Wichtig ist: *Sie müssen nicht verstehen, wie es gemacht wird – Sie müssen anfordern und abnehmen können.* Das Blatt ist dabei Ihre Anforderung; die Rückmeldung darauf ist Ihre Abnahme.

Anschaffung

Für die Verbesserung der Informationssicherheit empfehlen wir ausgewählte Büroeinrichtung, Hard- und Software. Diese begrenzt sich bewusst auf das Nötigste bei möglichst geringen Kosten. Beschafft wird in Ihrer Einrichtung in der Regel über den Träger – die Blätter sind deshalb für Sie vor allem Argumentationshilfe: Sie nennen den Bedarf, die Eigenschaften, auf die es ankommt, und den Grund. Damit begründen Sie den Beschaffungsantrag, ohne selbst Produkte vergleichen zu 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. Klären Sie zuerst, ob Ihr Träger für dieses Thema bereits eine Richtlinie hat. Wenn ja, gilt sie, und Sie prüfen nur, ob sie Ihre Besonderheiten abdeckt. Wenn nein, passen Sie den Vordruck an Ihre Situation an, zum Beispiel durch das Streichen nicht zutreffender Aspekte, und holen Sie vor dem Inkraftsetzen die Freigabe des Trägers ein. Legen Sie die Richtlinie anschließend allen Mitarbeitern und allen Neueinstellungen zur Unterschrift vor – und zwar geplant: Nachtdienst, Wochenenddienst, Aushilfen, Hauswirtschaft, Küche, Fahrdienst, Praktikanten und Ehrenamtliche erreichen Sie nicht, indem Sie das Blatt im Dienstzimmer auslegen.

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 anderer Maßnahmen, um allen den Zweck zu erläutern und zum Mitmachen anzuregen. Rechnen Sie im Schichtbetrieb mit zwei bis drei Durchgängen je Thema zu unterschiedlichen Tageszeiten; für den Nachtdienst braucht es einen eigenen kurzen Durchgang oder eine Nachholung in der Übergabe. Schulungen sollten in regelmäßigen Abständen aufgefrischt werden, um das Wissen präsent zu halten.

Maßnahmenart	Geht an	Ihre Aufgabe dabei
Konfiguration	Ihre IT-Unterstützung	anfordern und abnehmen
Anschaffung	Den Träger, über den Beschaffungsweg	Bedarf begründen, beantragen, abnehmen
Richtlinie	Sie prüfen die Richtlinie des Trägers oder passen den Vordruck an, Ihr Team bestätigt	abstimmen, anpassen, unterschreiben lassen, aushändigen, ablegen
Prozess	Sie und Ihr Team	im Schichtbetrieb verankern, Durchführung überwachen
Schulung	Ihr Team	Termine über alle Schichten 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 bei Einrichtungen in Trägerschaft in zwei Varianten aus, und die Empfehlungen unterscheiden sich:

- **Eine IT-Abteilung des Trägers**. Sie betreut in der Regel mehrere Einrichtungen, arbeitet mit Tickets und hat eigene Planungszyklen. Ihr Hebel ist nicht der Preis, sondern der Termin: Wann wird es gemacht, ist es im Ticket erfasst, steht es auf dem Plan. Bündeln Sie Anforderungen, denn ein Vor-Ort-Termin ist selten und sollte nicht für eine einzelne Einstellung verbraucht werden.
- **Ein Systemhaus, das der Träger beauftragt hat.** Das ist der unangenehmere Fall: Sie sind nicht Auftraggeberin, haben keinen Vertrag und können nicht direkt beauftragen. Jede Anforderung läuft über den Träger. Klären Sie dann einmal verbindlich, ob Sie das Systemhaus im Tagesgeschäft direkt ansprechen dürfen und wo die Grenze liegt – sonst verlieren Sie bei jeder Kleinigkeit eine Woche.

In beiden Fällen gilt: Sie sind nicht die Kundin, die eine Rechnung bezahlt, aber Sie sind diejenige, bei der ein Ausfall ankommt. Das ist der Grund, warum Sie schriftlich anfordern und schriftlich abnehmen. Im Folgenden sprechen wir von Ihrer IT-Unterstützung, wenn es um die Technik geht – gleich, ob sie beim Träger sitzt oder von ihm beauftragt ist. Vom Träger ist die Rede, wenn entschieden, beschafft oder vertraglich geregelt wird.

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 die IT, was zu tun ist, und für Sie das warum und wie. Fragen Sie vorher nach dem Termin. „Bis wann lässt sich das einplanen?" – ein Datum vorab macht die Sache planbar und gibt Ihnen etwas, worauf Sie sich im Kontrolltermin beziehen können. Lassen Sie sich die Ticket- oder Auftragsnummer geben und notieren Sie sie neben der Maßnahmenkennung. 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 das Ticket die Kennung des Steckbriefs im Betreff führt – dann ist die Zuordnung automatisch dokumentiert, und Sie finden den Vorgang später wieder, ohne ihn zu suchen.

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 vier 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, und sie ist nicht von der IT

zu treffen. Entschieden wird sie beim Träger; ausbaden würde den Ausfall Ihre Einrichtung. Genau deshalb gehört Ihre Anforderung und die Begründung der Ablehnung in Ihre Ablage: Damit ist aus einer unterbliebenen Maßnahme eine dokumentierte Abwägung geworden – und zwar eine, die nicht bei Ihnen hängenbleibt.

4. **„Das machen wir trägerweit einheitlich" oder „das kommt mit dem nächsten Rollout."** → Das ist weder falsch noch ablehnend, es ist eine Terminfrage. Fragen Sie nach dem Datum, halten Sie es schriftlich fest und fassen Sie im Kontrolltermin nach. Fragen Sie zusätzlich, was bis dahin gilt: Eine Maßnahme, die in acht Monaten kommt, lässt die acht Monate ungeschützt, und manchmal gibt es eine einfache Zwischenlösung.

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.

Im Notfall erreichbar bleiben

Die Administratorzugänge Ihrer Systeme liegen beim Träger, und das ist richtig so. Der Zweck bleibt aber derselbe: Sie dürfen nicht handlungsunfähig sein, wenn etwas passiert. Klären Sie dafür vier Punkte schriftlich:

1. Wer ist Ihr benannter Ansprechpartner, und wer vertritt ihn im Urlaub und bei Krankheit?

2. Wie erreichen Sie die IT außerhalb der Bürozeiten? Ihre Einrichtung arbeitet nachts, am Wochenende und an Feiertagen, der Träger oft nicht. Gibt es eine Rufbereitschaft, und unter welcher Nummer?

3. Welchen Weg nehmen Sie, wenn niemand reagiert? Ein Eskalationsweg mit Namen und Zeitgrenze, nicht „dann melde ich mich nochmal".

4. Sind die Daten Ihrer Einrichtung in der Datensicherung des Trägers tatsächlich enthalten? Lassen Sie sich das einmal bestätigen, mit Angabe, was gesichert wird und wie lange es dauert, es zurückzuholen.

Diese vier Antworten gehören auf den Notfallzettel im Dienstzimmer.

2.3 Was Sie mit Ihrem Träger klären müssen

Bevor Sie mit Etappe 1 beginnen, klären Sie einmal die Arbeitsteilung. Das ist schnell abgestimmt und erspart Ihnen bei jeder einzelnen Maßnahme die Frage, wer eigentlich dran ist. Halten Sie das Ergebnis schriftlich fest – eine Seite genügt.

Maßnahmenart	Wer fordert an	Wer führt aus	Wer nimmt ab
Konfiguration	Einrichtungsleitung	Ihre IT-Unterstützung	Einrichtungsleitung
Anschaffung	Einrichtungsleitung begründet	Beschaffung des Trägers	Einrichtungsleitung
Richtlinie	Träger oder Einrichtung, je nach Regelung	Einrichtungsleitung	Einrichtungsleitung, Freigabe beim Träger
Prozess	Einrichtungsleitung	Einrichtung	Einrichtungsleitung
Schulung	Einrichtungsleitung	Einrichtung, bei technischen Themen mit der IT	Einrichtungsleitung

Drei Fragen gehören in dasselbe Gespräch:

1. **Darf die Einrichtung eigene Richtlinien erlassen,** oder gelten die des Trägers?
2. **Ist ein Auftragsverarbeitungsvertrag nötig?** Gehört die Einrichtung zur selben juristischen Person wie der Träger, ist kein Vertrag erforderlich, sondern eine interne Abgrenzung der Aufgaben und Verantwortlichkeiten. Liegt der IT-Betrieb in einer eigenen Service-Gesellschaft oder bei einem Verbundpartner, ist es eine Auftragsverarbeitung und braucht einen Vertrag. Fragen Sie das ab, bevor Sie das Falsche suchen.
3. **Wie kommt Ihre IT-Unterstützung an Ihre Nachweise** – arbeitet sie im Web-Portal mit, oder tragen Sie deren Rückmeldungen selbst ein?

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 und stellen Office so ein, dass ein Anhang nicht mehr ungefragt ausgeführt wird. Sie richten das WLAN sicher ein und regeln den Umgang mit USB-Sticks und externen Datenträgern.

Zwei Dinge kommen hinzu, die auf den ersten Blick nicht nach IT aussehen und für Ihre Einrichtung die größte Wirkung haben. Erstens das Dienstzimmer: Der Rechner, an dem die Schicht arbeitet, die Unterlagen und der Schlüssel dazu gehören in einen Raum, der zugeht, wenn alle im Wohnbereich sind. Zweitens der Meldeweg: Wer eine merkwürdige E-Mail bekommt oder ein Gerät vermisst, muss wissen, an wen er sich sofort wendet – auch nachts, auch am Wochenende. Eine frühe Meldung verhindert Schaden, und sie kommt nur, wenn klar ist, dass niemand dafür belangt wird.

Parallel etablieren Sie die Datensicherung. In Ihrer Konstellation heißt das meist nicht, sie selbst einzurichten, sondern sich bestätigen zu lassen, was der Träger sichert, wie oft, und wie lange es dauert, die Daten zurückzuholen. Dazu kommen Eintritts- und Austrittschecklisten, damit Zugänge entstehen, wenn jemand anfängt, und verschwinden, wenn jemand geht – bei Aushilfen, Praktikanten und Ehrenamtlichen genauso wie bei Festangestellten. Die Vertraulichkeitserklärung gehört in denselben Vorgang.

Ein Blatt in dieser Etappe ist anders als die übrigen: das Sammelblatt zur Grundkonfiguration. Es fasst die Einstellungen zusammen, die sich ohne besondere Technik von Hand setzen lassen, und ersetzt für diese Punkte die Einzelblätter. Nutzen Sie es, wenn jemand die Geräte ohnehin in der Hand hat; die Einzelblätter bleiben für den Fall, dass eine Einstellung streitig ist oder nachgewiesen werden muss.

Nach dieser Etappe ist Ihr Schutz spürbar besser: Die Wege, über die Angriffe üblicherweise beginnen, sind verschlossen, die Daten sind gesichert, und mit dem Meldeweg ist das erste Stück Handlungsfähigkeit eingelöst – Sie erfahren von einem Vorfall, während er noch klein ist.

Etappe 2 – Sicherheit in den Alltag bringen

Die zweite Etappe nimmt das Haus in den Blick: alles, was hinein- und hinausreicht. Sie härten die Rechner weiter ab, verschlüsseln die Festplatten und schalten für die wichtigsten Zugänge eine Anmeldung mit zweitem Faktor ein, sodass ein gestohlenes Kennwort allein nicht mehr genügt.

Den größeren Teil macht aber das Netz aus, und zwar ganz handfest: Das Dienstnetz wird vom Gäste- und Besucher-WLAN getrennt, damit das Tablet eines Angehörigen nicht im selben Netz hängt wie die Pflegedokumentation. Die Netzwerkdosen in Fluren, Aufenthaltsräumen und Gruppenräumen werden aufgenommen und abgeschaltet oder zugeordnet – eine offene Dose im Flur ist ein Zugang ins Haus, an dem niemand vorbeigehen muss. Dasselbe gilt für das Multifunktionsgerät und den Router, die beide eigene Zugänge und eigene Updates haben.

Dazu kommen zwei Abläufe, die es nur bei Ihnen gibt. Der Schichtwechsel: Wie wird der gemeinsam genutzte Rechner übergeben, wer meldet sich ab, was passiert mit dem offenen Bildschirm während der Übergabe. Und der Besucherverkehr: Angehörige, Handwerker, Therapeuten, Praktikanten und Ehrenamtliche gehen durch das Haus; geregelt gehört, wer begleitet wird, wer sich anmeldet und wo die Grenze des öffentlichen Bereichs liegt.

Schließlich klären Sie, was nach außen geht: Sie prüfen Ihre Dienstleister auf Eignung, regeln die Nutzung von Cloud-Diensten, legen in der Maßnahmenkarte fest, welche Geräte, Zugänge und Verträge es überhaupt gibt, und halten in einem Beschaffungsblatt fest, worauf bei neuer Technik zu achten ist. Mit den Meldepflichten im Datenschutz wissen Sie außerdem, was im Ernstfall binnen 72 Stunden zu geschehen hat und wer es tut – Sie oder der Träger.

Mit dieser Etappe kommt das zweite Versprechen hinzu: Richtlinien, Übersichten und die Vereinbarungen mit Ihren Dienstleistern sind genau das, wonach eine Prüfung, die Heimaufsicht 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 hat einen klaren Schwerpunkt: die Tablets und Diensthandys, mit denen in der Pflege dokumentiert, telefoniert und organisiert wird. Sie sind das einzige Betriebsmittel, das Ihr Haus täglich verlässt oder in fremde Hände geraten kann, und sie sind deshalb ein eigener Abschnitt wert.

Sie legen fest, wie ein Gerät eingerichtet wird, bevor es in Betrieb geht: Sperrcode, automatische Updates, Verschlüsselung, Abschalten der Schnittstellen, die niemand braucht, und die Möglichkeit, ein verlorenes Gerät aus der Ferne zu sperren und zu löschen. Sie entscheiden, ob die Geräte einzeln von Hand eingerichtet werden oder über eine Geräteverwaltung – ab etwa zehn Geräten lohnt sich die Verwaltung, darunter ist die händische Umsetzung schneller. Für beide Wege liegt ein Blatt bei.

Dazu kommen drei Themen, die daneben stehen: Der Webbrowser wird so eingestellt, dass er weniger Angriffsfläche bietet. Die Uhrzeit der Geräte wird auf eine verlässliche Quelle gestellt – unscheinbar, aber ohne sie ist nach einem Vorfall keine Spur mehr zeitlich zuzuordnen. Und Sie regeln, welchen Zugriff Externe bekommen: Honorarkräfte, Therapeuten, Mitarbeiter eines ambulanten Dienstes, die bei Ihnen dokumentieren.

Zum Schluss ein Thema, an das man erst denkt, wenn es zu spät ist: der Umzug. Wird ein Wohnbereich umgebaut, ein Gruppenraum neu belegt oder die Verwaltung verlegt, stehen Rechner und Unterlagen für einige Tage dort, wo sie nicht hingehören. Dafür gibt es ein eigenes Blatt.

Nach dieser Etappe gilt für Ihre mobilen Geräte dasselbe wie für die Rechner im Haus: Sie wissen, welche es gibt, wie sie eingerichtet sind, und was passiert, wenn eines verschwindet.

Etappe 4 – Vorfälle beherrschen und von außen arbeiten

Die vierte Etappe bereitet Sie auf den Fall vor, dass trotz aller Vorkehrungen etwas passiert. Sie halten fest, was in den ersten Stunden zu tun ist: wer benachrichtigt wird, wer entscheidet, welche Geräte sofort vom Netz genommen werden – und wie Sie weiterarbeiten, solange die Technik steht. Dienstplan, Medikationsübersicht, Übergabe und Pflegedokumentation müssen für ein bis zwei Tage auf Papier laufen können; in der Tagespflege gehören die Anwesenheitsnachweise der Gäste dazu, weil davon die Abrechnung abhängt.

Ein Punkt ist in Ihrer Konstellation schärfer als anderswo: Fällt die Anbindung an den Träger aus, ist unter Umständen auch die Pflegedokumentation nicht erreichbar, weil sie dort liegt. Klären Sie deshalb vorab, was ohne diese Verbindung im Haus noch funktioniert, und was Sie dann tun. Das ist die Frage, die in der Vorsorge zuerst beantwortet werden muss.

Auf einem Notfallzettel im Dienstzimmer stehen die Nummern, die in diesem Moment gebraucht werden – und zwar so hinterlegt, dass auch der Nachtdienst sie findet: Ihre IT-Unterstützung mit ihrer Rufbereitschaft, der Hersteller Ihrer Pflegesoftware, der Datenschutzbeauftragte des Trägers, und die Heimaufsicht für meldepflichtige Ereignisse.

Dazu gehört, den Wiederanlauf einmal tatsächlich durchzuspielen, statt ihn nur aufzuschreiben: Wie lange dauert es wirklich, bis die Pflegedokumentation aus der Datensicherung wieder verfügbar ist? Fragen Sie das nicht nur ab, sondern vereinbaren Sie dafür einen Termin mit Ihrer IT-Unterstützung. Wer das einmal geprobt hat, weiß im Ernstfall, woran er ist, und kann Angehörigen und Mitarbeitern eine belastbare Auskunft geben.

In dieselbe Etappe gehört das Arbeiten von zuhause: Wer Dienstpläne, Abrechnung 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 sieben bis acht Stunden im Jahr: rund eine Viertelstunde im Monat für die kurze Kontrolle und vier bis fünf Stunden für den Jahrestermin. Der Unterschied zu einer Einrichtung mit eigener IT liegt nicht in der Zahl der Punkte, sondern darin, dass Sie für einen Teil davon eine Rückmeldung des Trägers einholen und ablegen müssen.

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:** Die Sicherung läuft nicht bei Ihnen, sondern bei Ihrer IT-Unterstützung, die Bestätigung gehört trotzdem zu Ihnen. Lassen Sie sich monatlich den Statusbericht oder eine kurze Bestätigung geben, dass die Sicherung Ihrer Einrichtung vollständig durchgelaufen ist, und legen Sie sie ab. Ein Backup ist außerdem nur nützlich, wenn sich Daten daraus zurückholen lassen, und bei so manchem Vorfall gab es dann ein böses Erwachen: Vereinbaren Sie einmal im Jahr einen Termin mit Ihrer IT-Unterstützung, bei dem eine einzelne Datei testweise zurückgeholt wird. Notieren Sie dabei, wie lange es gedauert hat. Genau das ist der Punkt, an dem sich eine IT-Unterstützung gern auf „läuft" zurückzieht – und an dem Sie einen Beleg brauchen.
- **Updates:** Die Geräte, die bei Ihnen im Haus stehen und die Sie aufklappen können – der Rechner im Dienstzimmer, die Tablets –, sehen Sie selbst nach: Der letzte Überprüfungsversuch sollte nicht länger als zwei Tage zurückliegen. Für alles Übrige fragen Sie den Statusbericht bei Ihrer IT-Unterstützung ab. Wenn es keinen gibt, ist das die erste Anforderung, die Sie stellen sollten.

Beides zusammen dauert nicht länger als eine Viertelstunde. Tipp: Koppeln Sie diese Überprüfung an etwas, das ohnehin monatlich passiert – den Monatsdienstplan, die Belegungsmeldung oder die monatliche Dienstbesprechung.

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** – Kontenliste bei Ihrer IT-Unterstützung anfordern und neben die Beschäftigtenliste legen, in beide Richtungen durchgehen. Aushilfen, Praktikanten, Ehrenamtliche und Leihkräfte ausdrücklich mit. Differenzen schriftlich melden.
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. Im Schichtbetrieb heißt das zwei bis drei Durchgänge oder die Einbindung in die Pflichtunterweisung.

5. **Notfallzettel** – Stimmen die Nummern noch? Ist der Zettel dort, wo er hingehört?

6. **Zusammenarbeit mit dem Träger** – Stimmen Ansprechpartner, Stellvertretung und die Nummer für außerhalb der Regelarbeitszeit? Ist die Aufgabenteilung noch zutreffend? Ein Auftragsverarbeitungsvertrag ist nur nötig, wenn der IT-Betrieb bei einer anderen juristischen Person liegt.

7. **Richtlinien** – Sind diese noch aktuell, und von allen unterschrieben, die seither dazugekommen sind?

8. **Dokumentation** – Sind die Dokumentationen auf dem aktuellsten Stand?

9. **Räume** – Schließen Dienstzimmer und Schränke zuverlässig, und weiß jede Schicht, wer zusperrt? Sind neue Netzwerkdosen in Fluren oder Aufenthaltsbereichen dazugekommen?

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 vier bis fünf 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: Lassen Sie sich die aktuelle Bestätigung der Datensicherung geben, 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

Wenn das passiert ...	... holen Sie das hervor
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
Umbau, neuer Wohnbereich oder Gruppenraum geht in Betrieb	Netzwerkdosen prüfen, Netztrennung, physischer Schutz der Geräte
Wechsel des Ansprechpartners beim Träger oder der betreuenden IT	Neuen Ansprechpartner und Eskalationsweg schriftlich bestätigen lassen, Notfallzettel aktualisieren, Aufgabenteilung neu bestätigen
Verdacht auf einen Vorfall	Notfallzettel
Neue Gruppe Besucher, Praktikanten oder Ehrenamtliche	Besucherverkehr, Vertraulichkeitserklärung, kurze Einweisung
Neuer Gast oder Bewohner mit eigenem Gerät im Haus	Gäste-WLAN statt Dienstnetz, Netzwerkdosen

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 mit diesen Informationen gut arbeiten können. Erste Anlaufstelle bei fachlichen Rückfragen ist deshalb der Träger selbst. 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