Kompetenzzentrum
Digitalisierung und Pflege

Wegweiser für Organisationstyp D (Stationäre Einrichtung mit externen Dienstleistern)

Cybersicherheitsmaßnahmen planen und priorisieren

Inhaltsverzeichnis

1 Einleitung 3
2 Der Baukasten 8
3 Ihr Weg in vier Etappen 17
4 Dranbleiben: der regelmäßige Zyklus 20
5 Wenn es hakt 25

Dieses Dokument ist die begleitende Regieanweisung für Organisationstyp D (Stationäre Einrichtung mit externen Dienstleistern). 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 stationäre Pflegeeinrichtung ab etwa 60 Beschäftigten, mit mehreren Wohnbereichen und Dienstzimmern im Schichtbetrieb sowie einer IT, die extern betrieben wird, durch einen Dienstleister oder den Träger. Je nach Ausstattung gehören auch Tablets für die Pflegedokumentation, ein eigener Serverraum oder Technikverteiler und eine angeschlossene Telematikinfrastruktur dazu.* Die IT muss laufen, läuft aber nebenher. Sie verantworten Belegung, Dienstplan, Qualitätsmanagement, Prüfungen und Personalführung gleichzeitig, und die IT ist formal nicht Ihre Aufgabe. Ausfallen tut sie trotzdem bei Ihnen - und in einer Einrichtung Ihrer Größe hängen an einem Ausfall nicht einzelne Arbeitsplätze, sondern mehrere Wohnbereiche gleichzeitig. 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, die Rufanlage meldet sich nicht mehr, oder die Pflegedokumentation ist morgens auf keinem Gerät erreichbar - und damit hängen Dienstplan, Medikationsübersicht und die Übergabe in allen Wohnbereichen gleichzeitig 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. Wer im Rechtssinne verantwortlich ist, hängt bei Ihnen von der Konstruktion ab: Gehört Ihre Einrichtung zu einem Träger, liegt die Verantwortung dort. Ist Ihre Einrichtung selbst die juristische Person und hat die IT an einen Dienstleister vergeben, liegt sie bei Ihrer Geschäftsführung - der Dienstleister wird dann für Sie tätig und entlastet Sie nicht. Klären Sie das einmal und schreiben Sie es auf; davon hängen Verträge, Meldepflichten und die Frage ab, wer eine Maßnahme ablehnen darf. Verantwortlich dafür, dass es im Haus tatsächlich geschieht, sind in beiden Fällen 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. In einer Einrichtung Ihrer Größe heißt „bei Ihnen" nicht „bei Ihnen persönlich": Die Pflegedienstleitung, die Wohnbereichsleitungen und das Qualitätsmanagement übernehmen jeweils Teile davon. Legen Sie zu Beginn fest, wer welche Maßnahmenart begleitet - etwa das Qualitätsmanagement die Richtlinien und Nachweise, die Wohnbereichsleitungen die Prozesse im Alltag, die Pflegedienstleitung die Schulungen. Was nicht delegierbar ist: die Entscheidung, eine Maßnahme nicht umzusetzen, und die Abnahme gegenüber der IT. 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 20 Maßnahmenblättern. Ihr persönlicher Aufwand hängt von der Maßnahme, den vorhandenen Vorarbeiten und dem Abstimmungsbedarf ab. Viele Aufgaben lassen sich in einzelnen Terminen bearbeiten; andere benötigen mehrere Abstimmungen und Prüfungen. Unterscheiden Sie dabei Aufwand und Durchlaufzeit: Bei den technischen Aufgaben kommt der Weg über Ihre IT-Unterstützung hinzu - anfordern, nachfassen, abnehmen. Für Anforderung, Abstimmung und Abnahme benötigen Sie eigene Arbeitszeit; bis zur Erledigung können außerdem 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. Rechnen Sie außerdem damit, dass eine Maßnahme in Ihrer Einrichtung nicht an einem Tag ausgerollt ist: Was alle Wohnbereiche und alle Schichten betrifft, braucht mehrere Durchgänge, und die Rückmeldung aus dem letzten Wohnbereich kommt zwei Wochen nach dem ersten. Jede dieser Aufgaben bringt Sie ein Stück näher an eine solide Cybersicherheit, ohne Sie und Ihre Mitarbeiter zu überfordern. Planen Sie die Termine für Etappe 1 gemeinsam mit Ihrer IT-Unterstützung und den Verantwortlichen im Haus anhand der vorhandenen Vorarbeiten und des tatsächlichen Aufwands.

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 überschaubare Aufgaben, deren Aufwand sich je nach Thema und Ausgangslage unterscheidet. 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 vier Etappen. In Etappe 1 legen Sie mit 20 Maßnahmenblättern das Fundament: die Zusammenarbeit mit der IT, die Beteiligung der Mitarbeitervertretung, sichere Arbeitsplätze und die Pflegeabläufe. Etappe 2 umfasst 14 Maßnahmenblätter zu Netzen, Geräten, Kommunikation und ergänzenden organisatorischen Regeln. In Etappe 3 folgen acht Maßnahmenblätter zu Rollen und Datenablage, Dateiserver, Monitoring, VPN und dem Schutz bei Umzügen und Renovierungen. Etappe 4 umfasst acht Maßnahmenblätter zu Datenschutzmeldungen, Notfallorganisation, mobilem Arbeiten und Homeoffice. Die regelmäßigen Kontrollen aus Kapitel 5 begleiten Sie bereits ab der Umsetzung der jeweiligen Maßnahme.

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.

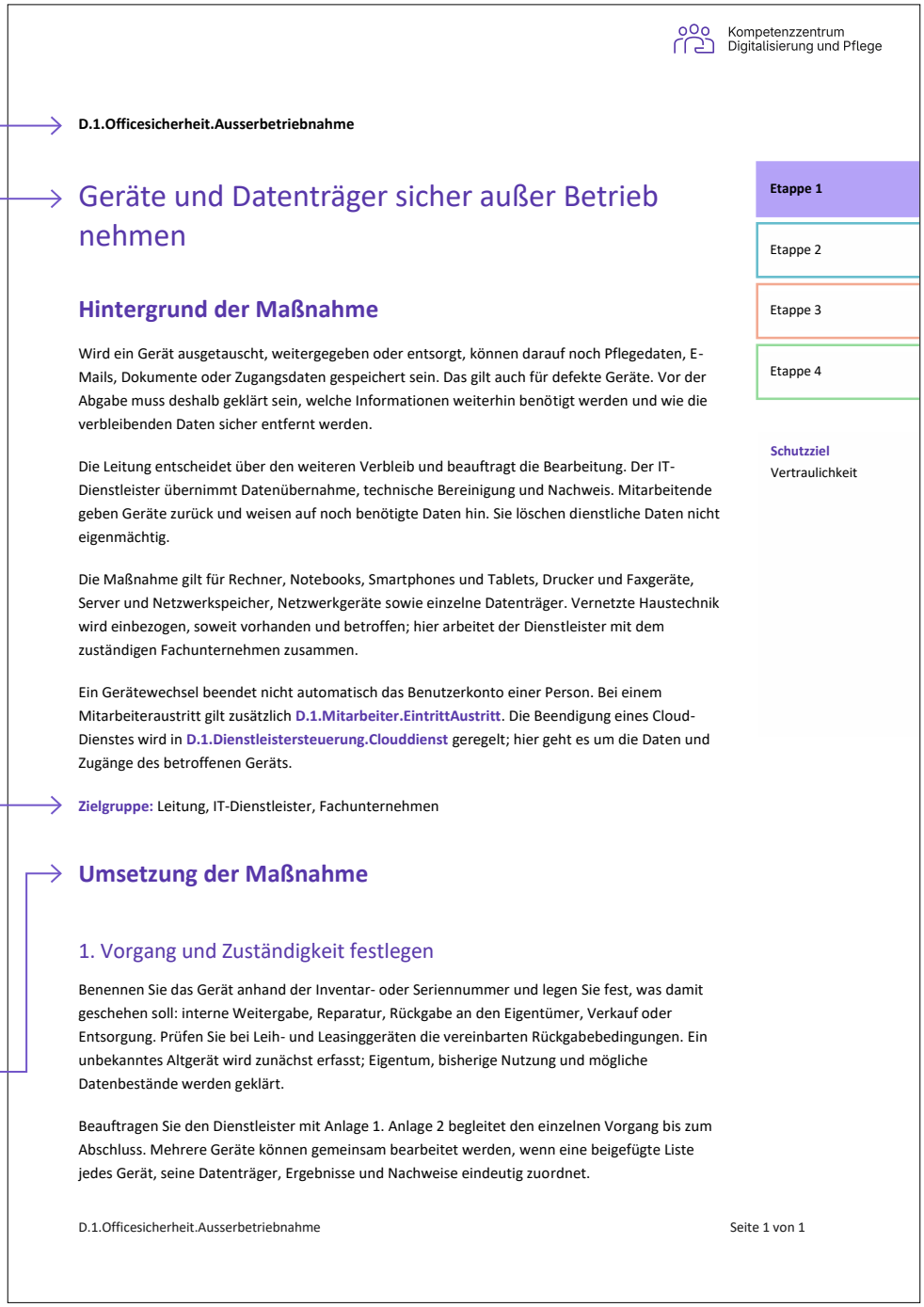
Orientieren Sie sich an der mitgelieferten Bearbeitungsreihenfolge. Vorbereitungen können teilweise parallel erfolgen. Wo eine Maßnahme Ergebnisse aus einem anderen Dokument voraussetzt, müssen diese vor dem jeweiligen Umsetzungsschritt beziehungsweise der Freigabe vorliegen. Die entsprechenden Hinweise finden Sie in den Maßnahmenblättern.

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 stationäre Pflegeeinrichtungen mit extern betriebener IT besteht aus insgesamt 50 Maßnahmenblättern. Das ist der größte Katalog der Reihe - und zugleich der mit der kürzesten Leseliste für die Leitung. Wie das zusammengeht, erklärt der übernächste Abschnitt. 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 Cloudan-

bietern und Dienstleistern, sowie die Vorsorge und der effektive Umgang auf einen Vorfall.

Alle Ihnen vorliegenden Dokumente folgen der gleichen Struktur, nehmen wir das Dokument D.1.Clientsicherheit.Baseline für die Absicherung der Arbeitsplatzrechner 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.

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 Etappe 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 D.1.Clientsicherheit.Baseline können Sie direkt ableiten, dass es eine Maßnahme für eine stationäre Pflegeeinrichtung mit externer IT (D) ist. So haben Sie direkt bei der Bearbeitung immer im Blick, womit Sie sich beschäftigen. Der Umfang richtet sich nach dem Thema. Umfangreichere Dokumente gliedern die Umsetzung in einzelne Schritte und enthalten die erforderlichen Anlagen.

In einer Einrichtung Ihrer Größe macht niemand aus der Leitung die Technik selbst. Die Blätter sind deshalb nicht als Klickanleitung für Sie geschrieben, sondern als Anforderung an Ihre IT-Unterstützung. Jedes technische Thema besteht aus zwei Teilen:

- Der **Fließtext** richtet sich an Sie. Er erklärt, worum es geht, was Sie entscheiden müssen und woran Sie erkennen, dass die Maßnahme erledigt ist.
- Das **Sollwertblatt** als Anlage richtet sich an Ihre IT-Unterstützung. Dort stehen die konkreten Einstellungen je Thema, Zeile für Zeile, mit einer Spalte für die Rückmeldung. Dieses Blatt geben Sie weiter, und dieses Blatt kommt ausgefüllt zurück. Das ausgefüllte Blatt bildet zusammen mit den im Maßnahmenblatt geforderten Nachweisen die Grundlage Ihrer Abnahme.

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 bestehen aus einer Einordnung für Sie und einem Sollwertblatt für Ihre IT-Unterstützung. **Wichtig ist:** *Sie müssen nicht verstehen, wie es gemacht wird - Sie müssen anfordern und abnehmen können.* Das Sollwertblatt ist Ihre Anforderung; das ausgefüllte Blatt bildet zusammen mit den im Maßnahmenblatt geforderten Nachweisen die Grundlage Ihrer 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	Im Haus begleitet von	Ihre Aufgabe dabei
Konfiguration	Ihre IT-Unterstützung	Zu Bennen, Leitung	anfordern und abnehmen
Anschaffung	Den Träger, über den Beschaffungsweg	Verwaltung	Bedarf begründen, beantragen, abnehmen
Richtlinie	Sie prüfen die Richtlinie des Trägers oder passen den Vordruck an, Ihr Team bestätigt	Qualitätsmanagement	abstimmen, anpassen, unterschreiben lassen, aushändigen, ablegen
Prozess	Sie und Ihr Team	Wohnbereichsleitungen	im Schichtbetrieb verankern, Durchführung überwachen
Schulung	Ihr Team	Pflegedienstleitung	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 drei 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.
- **Ein Dienstleister, den Ihre Einrichtung selbst beauftragt hat.** Dann sind Sie Auftraggeberin: Es gibt einen Vertrag, eine Leistungsbeschreibung und eine Rechnung. Fragen Sie hier zusätzlich zum Termin nach dem Aufwand - „Wieviel Zeit veranschlagen Sie hierfür?" -, bündeln Sie technische Maßnahmen einer Etappe zu einem Auftrag, und lassen Sie sich den Steckbrief auf der Rechnung benennen. In dieser Variante gilt außerdem, was bei Träger-IT nicht möglich ist: Die Zugangsdaten zu Ihren eigenen Systemen gehören Ihnen. Lassen Sie sich die Administratorzugänge aushändigen und bewahren Sie sie sicher auf, auch wenn Sie sie nie benutzen.

Im Folgenden sprechen wir von Ihrer IT-Unterstützung, wenn es um die Technik geht - gleich, ob sie beim Träger sitzt, oder von ihm oder Ihnen 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.

Wird Ihre IT vom Träger betrieben oder beauftragt, gilt: 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.

Was Sie vorab 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			
Anschaffung	Einrichtungsleitung begründet	Träger oder Beschaffung, je nach Konstruktion	Einrichtungsleitung

Maßnahmenart	Wer fordert an	Wer führt aus	Wer nimmt ab
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

Fünf 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?
4. Wer im Haus begleitet welche Maßnahmenart? Halten Sie die Zuordnung aus Kapitel 1 fest, damit nicht jede Rückfrage bei der Einrichtungsleitung landet.
5. Besteht eine Mitarbeitervertretung, und welche Ordnung gilt für sie? Davon hängt ab, welche Maßnahmen vor der Beauftragung durch ein Beteiligungsverfahren müssen.

Maßnahmen, die durch die Mitarbeitervertretung müssen

In einer Einrichtung Ihrer Größe besteht in der Regel eine Mitarbeitervertretung - ein Betriebsrat, eine Mitarbeitervertretung nach kirchlichem Recht oder ein Personalrat. Mehrere Maßnahmen dieses Katalogs führen Technik ein, die aufzeichnet, was an einem System geschieht: die Überwachung des Gerätezustands, die Protokollierung, die Verwaltungssoftware auf den Mobilgeräten, das Zugriffsprotokoll der Pflegesoftware. Für die Beteiligung kommt es nicht darauf an, dass Sie damit niemanden kontrollieren wollen, sondern darauf, ob die Technik dazu geeignet wäre.

Klären Sie das, bevor Sie beauftragen, nicht bevor Sie ausrollen - zwischen beidem liegen in der Praxis mehrere Wochen, und nur vorher lässt sich eine Maßnahme noch gestalten. Wie das geht und welche Maßnahmen betroffen sind, steht im Blatt D.1.Mitarbeiter.Mitbestimmung.

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 – Fundament legen

Im ersten Schritt geht es um das Fundament: die häufigsten Einbruchswege schließen, die Zuständigkeiten klären und die Pflegeabläufe absichern. Sie lassen die Arbeitsplatzrechner nach D.1.Clientsicherheit.Baseline absichern, regeln sichere Anmeldungen mit Passwortmanager und Mehrfaktor-Authentisierung und legen die Datensicherung mit Ihrer IT-Unterstützung fest. Für die Pflegesoftware bereiten Sie einen Ersatzablauf vor, damit die Versorgung bei einem Ausfall weiterläuft.

Am Anfang stehen die Vereinbarung mit Ihrer IT-Unterstützung, die erforderliche Beteiligung der Mitarbeitervertretung vor der Beauftragung und die Festlegungen zu Cloud-Diensten. Klären Sie, wer welche Aufgabe übernimmt, worauf die IT-Unterstützung Zugriff hat, was Sie an Rückmeldung erwarten und wie Sie sie außerhalb der Bürozeiten erreichen. Dazu kommen der geregelte Fernzugriff des Dienstleisters, die Richtlinien für den Arbeitsalltag sowie Eintritt und Austritt, Vertraulichkeit und die sichere Außerbetriebnahme von Geräten.

Im Haus sichern Sie die Dienstzimmer und legen fest, wie gemeinsam genutzte Rechner beim Schichtwechsel übergeben werden. Die Blätter zur Pflegesoftware und zum Schichtwechsel enthalten außerdem Hinweise für den Fall, dass dabei Smartphones oder Tablets eingesetzt werden: Dann müssen die erforderlichen Schutzmaßnahmen aus Etappe 2 bereits vor deren Einsatz berücksichtigt und umgesetzt werden.

Schließlich zwei Dinge, die den Rest tragen: der Meldeweg, damit eine Auffälligkeit gemeldet wird, solange sie klein ist - auch aus dem Nachtdienst, auch am Wochenende -, und das Basiswissen für alle Mitarbeiter. Beides ist die Voraussetzung dafür, dass die technischen Maßnahmen der folgenden Etappen im Alltag überhaupt wirken.

Nach dieser Etappe sind die grundlegenden Schutzmaßnahmen und Pflegeabläufe geregelt, die Datensicherung geplant und die Zusammenarbeit mit der IT vereinbart. Die internen und externen Meldewege helfen Ihnen, Auffälligkeiten früh weiterzugeben. Den laufenden Sicherungsbetrieb und die Wiederherstellungstests konkretisieren Sie in Etappe 2.

Etappe 2 – Netze, Geräte und Kommunikation ordnen

Die zweite Etappe ordnet Netze, Geräte und Kommunikation. Sie vereinbaren mit Ihrer IT-Unterstützung den Sicherungsbetrieb und einen angemessenen Plan für Wiederherstellungstests. Außerdem regeln Sie die Beschaffung und erfassen nicht freigegebene Geräte und Anwendungen, damit diese geprüft und in geregelte Verfahren überführt werden können.

Im Netz trennen Sie, was nicht zusammengehört: das Dienstnetz vom Besucher- und Bewohner-WLAN. Sie lassen Netzwerkdosen aufnehmen und ungenutzte oder frei zugängliche Anschlüsse absichern. Die E-Mail-Domain wird gegen gefälschte Absender geschützt, die Filterung unerwünschter und schädlicher E-Mails geregelt und die Sicherung wichtiger E-Mails geklärt. Auch Messenger und Multifunktionsgeräte erhalten klare Regeln.

Die mobilen Geräte bekommen ihre Grundordnung nach D.2.Mobilesecurity. Geraeteverwaltung: sichere Anmeldung, automatische Sperre, Verschlüsselung, zentral gesteuerte Updates sowie Verfahren für Verlust und Fernlöschung. Die zugehörigen Nutzungsregeln stehen in D.2.Mobilesecurity. Nutzungsrichtlinie. Ihre IT-Unterstützung setzt die technischen Anforderungen um; Sie weisen die Mitarbeiter in die Regeln ein.

Organisatorisch kommen der Umgang mit Besuchern und die Einbindung externer Mitarbeiter hinzu. Die Beteiligung der Mitarbeitervertretung wird bereits in Etappe 1 geklärt und bei den hier betroffenen Maßnahmen vor der Beauftragung berücksichtigt.

Nach dieser Etappe sind die eingesetzten Netze, Geräte und Kommunikationswege geordnet. Für die Datensicherung sind Überwachung und Wiederherstellungstests vereinbart und die vorgesehenen Nachweise vorhanden.

Etappe 3 – Rollen, Datenablage und Betrieb regeln

In der dritten Etappe legen Sie mit dem Rollenkonzept fest, welche Aufgaben welche Zugriffe benötigen. Darauf baut die Datenablage mit ihrer Berechtigungsmatrix auf. Erst anschließend planen Sie mit Ihrer IT-Unterstützung, ob und wie ein lokaler Dateiserver benötigt wird. Einrichtung und Betrieb folgen auf Grundlage der freigegebenen Planung.

Ein weiterer Schwerpunkt ist das Monitoring. Sie vereinbaren mit Ihrer IT-Unterstützung, welche Systeme überwacht werden, wer Auffälligkeiten erhält und wie darauf reagiert wird. So ergänzen Sie die vorhandenen Schutzmaßnahmen um einen geregelten Umgang mit technischen Warnungen.

Außerdem bereiten Sie den VPN-Zugang für eigene Mitarbeiter technisch vor und regeln den Schutz bei Umzügen und Renovierungen. Die Freigabe der mobilen Nutzung erfolgt erst, wenn die erforderlichen Festlegungen aus D.4.Richtlinie.MobilesArbeiten und gegebenenfalls D.4.Richtlinie.Homeoffice vorliegen. Diese Richtlinien bearbeiten Sie in Etappe 4; die technische Vorbereitung kann bereits vorher erfolgen.

Nach dieser Etappe sind Rollen und Datenablage geregelt, ein gegebenenfalls benötigter Dateiserver ist geordnet eingerichtet und sein Betrieb festgelegt. Technische Auffälligkeiten erreichen die vereinbarten Ansprechpartner.

Etappe 4 – Notfälle vorbereiten und Arbeiten außerhalb regeln

In dieser Etappe vervollständigen Sie die Notfallorganisation und regeln mobiles Arbeiten und Homeoffice. Sie erproben die vorgesehenen Abläufe und halten die erforderlichen Nachweise fest.

Sie legen fest, wie mögliche Datenschutzverletzungen bewertet und gemeldet werden, und bearbeiten Notfallvorsorge, Notfallhandbuch, Spurensicherung und Notfallbewältigung. Der in Etappe 1 vorbereitete Ersatzablauf für die Pflegesoftware fließt in diese Planung ein. Mit Ihrer IT-Unterstützung klären Sie, welche Systeme und Arbeitsabläufe für die Versorgung zuerst wieder verfügbar sein müssen.

Sie erproben die Ersatzabläufe und den Wiederanlauf im vereinbarten Umfang. Wiederherstellungstests richten sich nach dem Testplan aus D.2.Officesicherheit.Backup.BetriebTest und den Möglichkeiten des jeweiligen Betriebsmodells. Stimmen Sie bei gehosteten Anwendungen die erforderlichen Nachweise und Übungen mit dem Anbieter ab. Halten Sie Ergebnisse, benötigte Zeiten und Verbesserungen fest.

Für mobiles Arbeiten und Homeoffice legen Sie die organisatorischen Regeln fest und prüfen den vorgesehenen Arbeitsplatz anhand der Homeoffice-Karte. Erst wenn die erforderlichen Festlegungen vorliegen und die Schutzmaßnahmen umgesetzt sind, geben Sie die Nutzung frei. Die technische Vorbereitung aus Etappe 3 können Sie dafür verwenden.

Etappe 4 umfasst wie Etappe 3 acht Maßnahmenblätter. Die regelmäßigen Kontrollen aus Kapitel 5 führen Sie für alle bereits umgesetzten Maßnahmen fort; sie beginnen nicht erst mit dieser letzten Etappe.

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. Beginnen Sie mit regelmäßigen Kontrollen, sobald eine Maßnahme umgesetzt ist. Planen Sie dafür einen kurzen monatlichen Kontrolltermin und eine ausführlichere Jahresprüfung ein. Nach Umsetzung des Rollenkonzepts in Etappe 3 kommt der halbjährliche Kontenabgleich hinzu. Der Aufwand hängt von der Zahl der Personen, den eingesetzten Systemen und dem Stand der Nachweise ab. Das ist mehr als in einer kleinen Einrichtung, und der Grund ist nicht die Technik, sondern die Zahl der Personen: Jeder Eintritt, Austritt und Bereichswechsel muss sich in den Konten wiederfinden. Ein Teil davon lässt sich delegieren - der monatliche Blick an das Qualitätsmanagement, der Kontenabgleich an die Verwaltung.

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. Die nachfolgenden Termine unterstützen Ihre regelmäßige Kontrolle. Die in den Maßnahmenblättern festgelegten Überwachungen, Prüfungen und Fristen gelten zusätzlich:

Einmal im Monat überprüfen Sie, ob wichtige Punkte für Ihre Cybersicherheit noch wie erwartet funktionieren und aktuell sind:

- **Datensicherung:** Ihre IT-Unterstützung überwacht jeden geplanten Sicherungslauf auf Erfolg, Vollständigkeit und Auffälligkeiten. Lassen Sie sich die verständliche Statusmeldung im vereinbarten Turnus geben, beispielsweise wöchentlich, und legen Sie sie ab. Im monatlichen Kontrolltermin prüfen Sie, ob die Meldungen vorliegen und erkannte Probleme bearbeitet werden. Vereinbaren Sie Umfang, Turnus, Termine und Beteiligte der Wiederherstellungstests nach D.2.Officesicherheit. Backup.BetriebTest. Der Plan berücksichtigt die Bedeutung der Daten, zulässige Ausfallzeiten und die Komplexität der Wiederherstellung. Er umfasst den erstmaligen Nachweis nach der Einrichtung sowie die vorgesehenen Tests einzelner Daten und des Wiederanlaufs wichtiger Systeme oder Arbeitsabläufe.
- **Updates:** Ihre IT-Unterstützung steuert die Updates zentral und prüft deren erfolgreiche Installation. Lassen Sie sich den dokumentierten Prüfstand und offene Abweichungen nach D.1.Clientsicherheit.Baseline beziehungsweise D.2.Mobilesecurity.Geraeteverwaltung vorlegen. Entscheidend ist, ob die erforderlichen Sicherheitsupdates innerhalb der vereinbarten, nach Dringlichkeit festgelegten Fristen installiert wurden. Ein Datum allein genügt dafür nicht. Vorführungen an ausgewählten Geräten ergänzen die technischen Nachweise für den gesamten Gerätebestand; sie ersetzen diese nicht.

Für den kurzen Kontrolltermin können Sie zunächst etwa eine Viertelstunde einplanen. Offene Probleme und fehlende Nachweise benötigen gegebenenfalls zusätzliche Bearbeitungszeit. Tipp: Koppeln Sie diese Überprüfung an etwas, das ohnehin monatlich passiert - die Leitungsrunde, die Belegungsmeldung oder den Termin des Qualitätsmanagements.

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** – Der eigentliche Abgleich findet halbjährlich statt, gegen das Rollenkonzept (siehe Etappe 3). Im Jahrestermin prüfen Sie nur, ob er stattgefunden hat und ob die gemeldeten Differenzen erledigt sind.

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 und Technik** – Schließen Dienstzimmer, Serverraum und Netzverteiler zuverlässig, und ist klar, wer Schlüssel hat? Sind seit dem letzten Termin Netzwerkdosen in Fluren oder Aufenthaltsbereichen hinzugekommen oder wieder in Betrieb genommen worden?

10. **Beteiligung** – Sind seit dem letzten Termin Maßnahmen hinzugekommen, die durch die Mitarbeitervertretung müssen? Deckt die bestehende Vereinbarung die tatsächlich eingesetzte Systemkonfiguration noch ab?

11. **Übung** – Wann wurde der Wiederanlauf zuletzt tatsächlich durchgespielt, und wie lange hat er gedauert? Ist die gemessene Zeit noch die, mit der Ihr Notfallkonzept rechnet?

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.

Planen Sie für eine solche Jahresprüfung mehrere Stunden ein. Der tatsächliche Aufwand hängt von Ihrer Einrichtung und den offenen Punkten ab. Die Prüfung 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
Mitarbeiter verlässt den Betrieb	Offboarding: Zugänge sperren, Geräte und Schlüssel zurück
Mitarbeiter wechselt den Wohnbereich oder die Funktion	Rolle im Rollenkonzept ändern – nicht Rechte einzeln ergänzen
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
Neues System oder neue Funktion mit Protokollierung	Beteiligung der Mitarbeitervertretung prüfen, bevor beauftragt wird
Fremdfirma arbeitet länger im Haus	Besucher und Fremdfirmen, Zugang zu Technikräumen, Vertraulichkeit
Anbau, Sanierung oder neuer Wohnbereich	Netzwerkdosen, Netztrennung, physischer Schutz, Rufanlage

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 wie-

der 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 Ihre IT-Unterstützung beziehungsweise Ihr Träger. 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