Kompetenzzentrum
Digitalisierung und Pflege

Handlungsempfehlung für Cybersicherheit in der Pflege

Grundlagendokument



Inhaltsverzeichnis

1 **Warum Cybersicherheit?** 3

a. Einleitung 3

b. Cyberangriffe auf den Gesundheitssektor 4

c. Cybersicherheit als unternehmerische Verpflichtung 5

d. Cybersicherheit muss nicht schwierig sein 8

2 **Wie eine E-Mail meinen Betrieb lahmlegte** 9

3 **Cybersicherheit für die Pflege** 15

a. Schutzziele der Cybersicherheit – Was bedeutet das für mich? 15

b. Wenn Schutzziele gegeneinander stehen 21

c. Welcher Organsisationstyp bin ich? 22

d. Übersicht über die Vorgehensweise und große Bausteine des Katalogs 23

e. Wie bringe ich das in meinem Haus zum Laufen? 26

4 **Zusammenfassung** 28

1 Warum Cybersicherheit?

a. Einleitung

Cyberkriminalität ist in Deutschland Alltag geworden. Allein im Jahr 2024 erfasste die Polizei 131.391 Cybercrime-Fälle im Inland sowie weitere 201.877 Straftaten, die aus dem Ausland begangen wurden – zusammen über 333.000 Fälle, im Schnitt einer alle 95 Sekunden[1]. Jeden Tag werden über 280.000 neue Varianten von Schadsoftware entdeckt[2], die Unternehmensdaten ausspionieren oder unbrauchbar machen. Diese große Menge an Cyberangriffen hat unmittelbare Auswirkungen auf Unternehmen: Cyberangriffe werden von Versicherungen[3] mittlerweile als die wichtigste Bedrohung für Unternehmen eingestuft, weit vor „typischen" Auszahlungsgründen wie z.B. Feuer. In einer jährlichen Studie befragt der Branchenverband Bitkom Unternehmen nach erlittenen Schäden durch Cyberkriminalität: im Jahr 2025 betrugen die Verluste deutschlandweit 289 Milliarden Euro[4] – im Schnitt wären dies pro Unternehmen in Deutschland über 82.000 Euro.

Diese Auswirkungen sind auch deswegen so hoch, weil viele Unternehmen nicht vorsorgen. Regelmäßig hört man das Argument: „Ich bin klein und unbedeutend, und habe noch nicht mal eine Webseite – wer soll mich schon angreifen?" Cyberkriminelle hacken nicht nur Webseiten, Schadsoftware verbreitet sich ebenfalls per E-Mail, und selbst ein Besuch von vertrauenswürdigen Webseiten kann zum Problem werden, wenn sich in einer Werbeanzeige Schadsoftware verbirgt.

Durch die Nutzung von Künstlicher Intelligenz und Automatisierung ist es für Kriminelle heute kein Problem mehr, viele Unternehmen gleichzeitig anzugreifen. Selbst wenn Kriminelle von kleinen Unternehmen nur wenige Tausend Euro erpressen können, ist dies multipliziert mit Millionen potentiellen Opfern dennoch lukrativ. Das Ergebnis: 87 % der Unternehmen wurden in den vergangenen 12 Monaten Opfer von Cyberkriminalität[5]. Cyberangriffe sind in der Mitte der Gesellschaft angekommen und treffen klein wie groß. Niemand ist zu klein und unbedeutend.

[1] Bundeskriminalamt: Bundeslagebild Cybercrime 2024. Wiesbaden, Juni 2025

[2] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2025, 2025

[3] Allianz Commercial: Allianz Risk Barometer 2026 – Cyber incidents

[4] Bitkom e. V.: Wirtschaftsschutz 2025. Studienbericht, Berlin, September 2025.

[5] Bitkom e. V.: Wirtschaftsschutz 2025. Studienbericht, Berlin, September 2025.

b. Cyberangriffe auf den Gesundheitssektor

Cyberkriminellen geht es darum, Geld zu verdienen. Warum sollten sie es daher auf den Gesundheitssektor – insbesondere Pflegeeinrichtungen – abgesehen haben? Gibt es nicht in produzierenden Unternehmen viel mehr zu holen?

Überraschenderweise ist Gesundheit mittlerweile zu einem Hauptangriffsziel geworden. Das Bundeskriminalamt nennt den Gesundheitssektor in seinem Lagebild Cybercrime 2024 als eine von vier Branchen im Fokus . Auch die Auswertungen der Europäischen Union bestätigen dies: zwischen 2021 und 2025 ereigneten sich 20 % aller Cyberangriffe europaweit auf den Gesundheitssektor – obwohl dieser nur einer von insgesamt 18 kritischen Sektoren in der Auswertung war[7].

Angriffe auf Gesundheitseinrichtungen sind für Kriminelle lukrativ – auch weil sie ihre Geschäftsmodelle weiterentwickelt haben. Während es beim produzierenden Gewerbe meist um die Verschlüsselung von internen Daten geht und Lösegelder erpresst werden, um diese wieder freizugeben, haben Gesundheitseinrichtungen nicht nur Computer, Drucker und Server, sondern vor allem Daten von Pflegebedürftigen mit sensiblen Informationen in ihrem Besitz. In sogenannten „Triple-Extortion"-Angriffen (Dreifache Erpressung) erpressen Kriminelle dann nicht nur das gehackte Unternehmen, sondern treten auch an Pflegebedürftige und Angehörige heran und drohen mit Veröffentlichung. So können Kriminelle durch einen erfolgreichen Angriff mehrfach abkassieren. Es gibt bereits Zehntausende solcher Fälle, auch bestätigte Fälle, bei denen betroffene Patienten einer gehackten Klinik anschließend Suizid begangen haben[8].

Der Gesundheitssektor ist nicht nur eines der wichtigsten Angriffsziele geworden, Cyberkriminelle haben in den vergangenen Jahren auch gelernt, wie sie Gesundheitseinrichtungen am besten angreifen können. Durch diese Professionalisierung und Spezialisierung steigt das Risiko auch für Pflegeeinrichtungen, die mehr in Cybersicherheit investieren müssen.

---

[6] Bundeskriminalamt: Bundeslagebild Cybercrime 2024. Wiesbaden 2025.

[7] ENISA – European Union Agency for Cybersecurity: ENISA Threat Landscape 2025. Oktober 2025

[8] zum Fall Vastaamo (Finnland, 2020): z. B. Deutsches Ärzteblatt, Vertrauliche Psychotherapiedaten in Finnland gehackt, 26.10.2020

c. Cybersicherheit als unternehmerische Verpflichtung

Cybersicherheit ist sowohl eine ethische Verpflichtung gegenüber Patienten und Mitarbeitern, als auch eine gesetzliche Verpflichtung vorzusorgen. Verschiedene Gesetze und Vorgaben legen Unternehmen auf, ausreichende Maßnahmen gegen Cyberangriffe zu treffen. Kommt ein Unternehmen dieser Pflicht nicht nach, drohen Strafen und Haftung für das Unternehmen und seinen Geschäftsführer sowie möglicherweise auch Schadensersatzforderungen von Betroffenen.

Weil Cyberangriffe heute eine der wesentlichen Schadensquellen für Unternehmen darstellen, sind in den vergangenen Jahren zahlreiche Gesetze und Vorgaben für bessere Cybersicherheit erlassen worden. Im Folgenden stellen wir die wichtigsten aus vier Bereichen kurz vor:

Datenschutz

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-weit geltende Verordnung zum Schutz personenbezogener Daten. Sie legt fest, unter welchen Voraussetzungen Daten von natürlichen Personen verarbeitet, gespeichert und übermittelt werden dürfen. Die DSGVO gibt nicht nur Betroffenen umfangreiche Rechte zur Einsicht, Löschung und Berichtigung von Daten, sie schreibt auch vor, wie mit diesen Daten aus Unternehmensperspektive umgegangen werden muss.

- Art. 24 erfordert geeignete technisch-organisatorische Maßnahmen für die Verarbeitung von Informationen. Hierbei benötigen Gesundheitsdaten mehr Schutz, da Schadensereignisse hier ein hohes Risiko bergen (Erwgr. 75)

  → Die DSGVO gibt Unternehmen die Vorgabe, die Verarbeitung von Daten durch Schutzmaßnahmen abzusichern. Sie müssen sicherstellen, dass die Daten sicher verarbeitet und gespeichert werden, um die Rechte von Betroffenen sicherzustellen. Für besonders sensible Patientendaten gelten erhöhte Anforderungen an Sicherheitsmaßnahmen.

- Art. 32 verlangt, dass die Auswahl an Maßnahmen auf Basis einer objektiven Beurteilung getroffen werden muss. Hierbei müssen der aktuelle Stand der Technik, aber auch die wirtschaftliche Verhältnismäßigkeit abgewogen werden und durch das Unternehmen nachgewiesen werden.

  → Laut Verordnung muss Ihre Unternehmung einen Nachweis darüber führen können, mit welchen Maßnahmen Sie den Schutz der Daten gewährleisten können. Diese Handreichung erspart Ihnen diesen Aufwand und stellt Ihnen auf Ihre Pflegeeinrichtung abgestimmte Maßnahmen vor, mit denen Sie einen guten Schutz realisieren können.

- Art. 32 verpflichtet sowohl Ihr Unternehmen als auch von Ihnen beauftragte Dienstleister entsprechende Maßnahmen zu treffen. Kommt ein Dienstleister dem nicht nach, kann dies eine gesamtschuldnerische Haftung für Sie bedeuten (Art. 82 Rn. 13).

  → Mit Hilfe dieser Handreichung lernen Sie, wie Sie Cybersicherheit von Ihren Geschäftspartnern einfordern und sich absichern, sollte es hier zu einem Vorfall kommen.

Datenschutz oder Datensicherheit – zwei Seiten derselben Medaille

Datenschutz und Datensicherheit werden im Alltag von Pflegeeinrichtungen oft synonym verwendet, dabei beschreiben sie zwei unterschiedliche, aber eng miteinander verwobene Fragestellungen.

Im **Datenschutz** geht es um die Frage: **Dürfen die Daten einer Person überhaupt erhoben, gespeichert und verarbeitet werden?** Im Datenschutz geht es um das Recht auf informationelle Selbstbestimmung von Patienten und Bewohnern, auf Grundlage der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes. Ferner haben Betroffene auf Basis dieser Gesetze Rechte wie z.B. auf Auskunft, Löschung oder Berichtigung ihrer personenbezogenen Daten. Aus Datenschutzsicht muss geklärt werden, welche personenbezogenen Daten durch die Pflegeeinrichtung verwendet werden. Hierfür müssen die entsprechenden Einwilligungen zur Verarbeitung eingeholt, und durch entsprechende Sicherheitsmaßnahmen den Schutz dieser Daten sichergestellt werden.

In der **Datensicherheit** – oder besser gesagt der Informationssicherheit, denn diese umfasst auch Informationen auf Papier wie z.B. Patientenakten oder das gesprochene Wort im Behandlungszimmer – geht es hingegen um die Frage: **Wie schützen wir Informationen in unserer Organisation gegen unbefugten Zugriff, Manipulation oder Verlust?** Hieraus leiten sich technische und organisatorische Maßnahmen ab, wie z.B. Verschlüsselung, Firewalls, Zugangsdaten, oder Backups. Die Informationssicherheit schützt alle Informationen einer Einrichtung, nicht nur personenbezogene Patientendaten. Sie bewahrt eine Einrichtung im Idealfall vor einem Cyberangriff und den damit verbundenen Konsequenzen, und erfüllt die rechtlichen Anforderungen an eine Organisation, ihre Leitung und Mitarbeiter.

Pflegeeinrichtungen verarbeiten besonders sensible Daten über ihre Patienten. Die DSGVO stuft Gesundheitsdaten als besonders schutzwürdig ein, für die verschärfte Schutzanforderungen gelten. Ohne die Umsetzung von Informationssicherheit kann eine Einrichtung die Anforderungen des Datenschutzes nicht erfüllen. Gleichzeitig muss die Informationssicherheit auch die Anforderungen an den Datenschutz und die Rechte von Betroffenen berücksichtigen, um effektiv und rechtlich ausreichend zu sein. Datenschutz und Informationssicherheit gehen Hand in Hand als zwei Seiten derselben Medaille.

Berufsrecht

Als medizinischer Leistungserbringer gelten für Sie Verschwiegenheitspflichten (§ 9 MBO-Ä, § 203 StGB). So müssen Sie u.a. Vorkehrungen treffen, damit Unbefugte keinen Zugriff auf Patientengeheimnisse erlangen. Wenn Ihre Einrichtung keine ausreichende Cybersicherheit etabliert hat, kann dies den Vorwurf für ein berufsrechtswidriges Unterlassen begründen. Verschwiegenheitspflichten betreffen nicht nur Ärzte, auch Pflegepersonal (als Angehöriger von Heilberufen mit staatlich geregelter Ausbildung), Auszubildende in einer Einrichtung, aber auch sonstige Mitarbeiter in der Organisation wie z.B. in der Buchhaltung fallen hierunter.

→ Nicht nur medizinische Leistungserbringer wie Ärzte oder Pflegepersonal sind von Verschwiegenheitspflichten betroffen, auch Personen, die mit diesen Daten in Kontakt kommen können (juristisch „Erfüllungsgehilfen"), müssen sich hieran halten. Eine Pflegeeinrichtung muss daher zum Schutz ihrer eigenen Mitarbeiter Sicherheitsmaßnahmen treffen, damit diese die Verschwiegenheitspflichten gewährleisten können.

Gesellschaftsrecht

Je nach Organisationsform ergeben sich weitere Anforderungen aus dem Gesellschaftsrecht. Für GmbHs und gemeinnützige GmbHs stellt das GmbH-Gesetz Anforderungen daran, wie der Geschäftsführer den Betrieb organisieren muss:

‣ § 43 verlangt vom Geschäftsführer einer GmbH, sich mit entsprechender Sorgfalt um die Vermögensinteressen des Unternehmens zu kümmern, andernfalls haftet der Geschäftsführer persönlich gegenüber der Unternehmung. Hierzu zählt auch die Gewährleistung von Datenschutz und Datensicherheit. Hat der Geschäftsführer nicht die notwendigen Kenntnisse hierfür, ist dies bereits eine Sorgfaltswidrigkeit. Fehlende Kenntnisse entlasten nicht von der Verpflichtung.

→ Geschäftsführer sind verpflichtet, Cybersicherheit umzusetzen und sich, wenn nötig Hilfe zu holen. Diese Handreichung stellt Ihnen vor, was Sie machen sollten und welche Möglichkeiten es gibt.

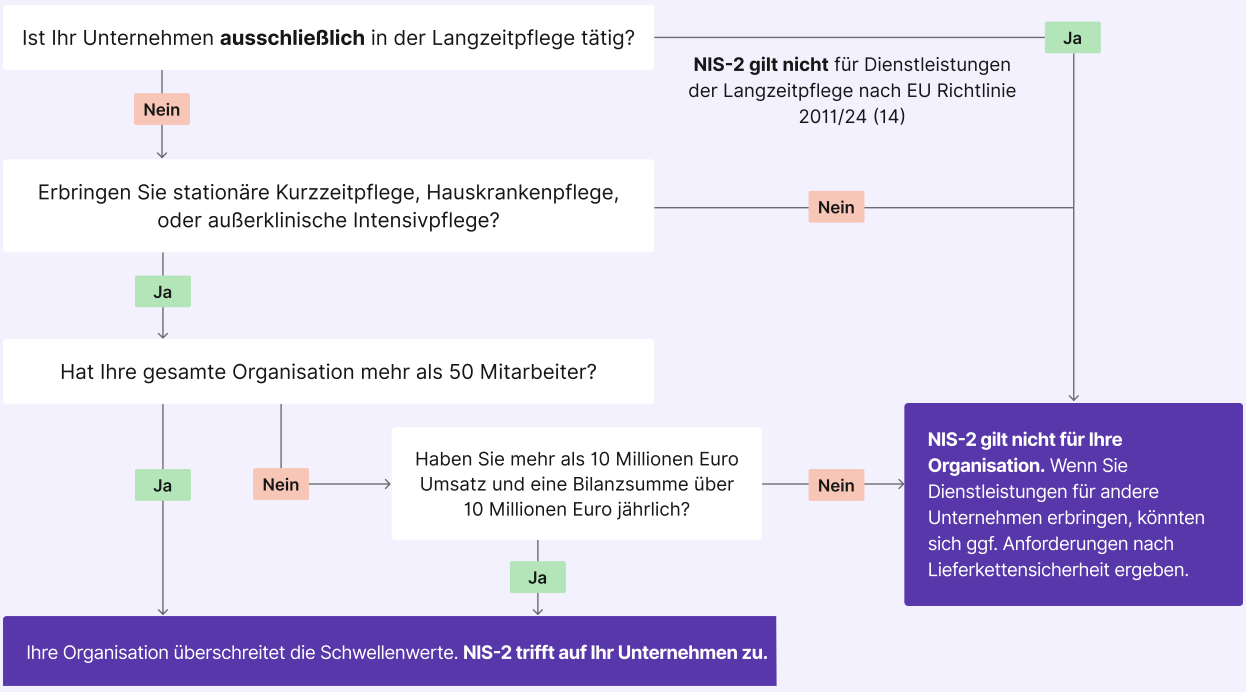
Kritische Sektoren

‣ Die NIS-2-Richtlinie, die Ende 2025 in Deutschland in Kraft getreten ist, reguliert Unternehmen in kritischen Sektoren und verlangt von betroffenen Einrichtungen u.a. die Etablierung eines Risikomanagements, Krisenmanagements, und Meldepflichten. Zwar sind Einrichtungen der Langzeitpflege als Teil des Gesundheitssektors von NIS-2 im ersten Schritt ausgenommen, allerdings gibt es Situationen, in denen Pflegeeinrichtungen dennoch als betroffene Einrichtungen zählen. Dies sind z.B. Komplexträger, aber auch zahlreiche Einrichtungen in der Hauskrankenpflege, außerklinischen Intensivpflege oder stationären Kurzzeitpflege (siehe Kasten).

→ NIS-2 erfordert von betroffenen Einrichtungen eine umfassende Sicherheitskonzeption und Dokumentation. Pflegeeinrichtungen können unter besonderen Umständen von NIS-2 betroffen sein.

Betrifft mich NIS-2?

Die europäische NIS-2 Richtlinie stellt an Unternehmen in kritischen Sektoren, sofern sie eine bestimmten Größe überschreiten, bestimmte Anforderungen an Cybersicherheit. Das folgende Schaubild bereitet den NIS-2 Kriterienkatalog speziell für Pflegeeinrichtungen auf, so dass Sie unmittelbar prüfen können, ob Sie betroffen sind.



Verschiedene Gesetze und Vorgaben verlangen die Umsetzung von Cybersicherheitsmaßnahmen in Pflegeeinrichtungen. Ohne geeignete Maßnahmen drohen erhebliche Strafen für Unternehmen und die Geschäftsführung, nicht nur, wenn ein Angriff eingetreten ist.

Es sollte bei Cybersicherheit aber nicht nur um rechtliche Anforderungen und die Vermeidung von Strafen gehen, denn eine gute Cybersicherheit schützt vor allem Ihre Einrichtung vor einem Vorfall und den damit verbundenen Auswirkungen: nicht funktionierende Computer, Lösegeld-Forderungen von Kriminellen, Überstunden durch nachzutragende Dokumentation, frustrierte Mitarbeiter und verunsicherte Patienten.

d. Cybersicherheit muss nicht schwierig sein

Das Thema Cybersicherheit fühlt sich für die meisten als komplex an. Was genau muss ich tun, was ist sinnvoll und schützt mich? Worauf kann ich verzichten? Produkte, Software und Beratung für Cybersicherheit scheinen auch eine Menge Geld zu kosten. Und zu guter Letzt: wie finde ich hierfür neben meinen anderen Aufgaben überhaupt die Zeit?

Die gute Nachricht ist: Gute Cybersicherheit muss weder teuer noch komplex sein. Vieles lässt sich mit einfachen Schritten schnell und ohne signifikante Anschaffungen verbessern. Gute Cybersicherheit verfolgt einen risiko-basierten Ansatz, der auf die Einrichtung, ihre Größe und Anforderungen abgestimmt ist. Auch der Gesetzgeber sieht dies so vor, denn ein ambulanter Pflegedienst mit wenigen Mitarbeitern benötigt andere Maßnahmen als eine große stationäre Einrichtung.

Da Pflegeeinrichtungen sehr unterschiedlich sind, sind die Handlungsempfehlungen auf die verschiedenen Einrichtungstypen, Größe und Struktur zugeschnitten, so dass Sie nur die Maßnahmen vorgeschlagen bekommen, die für Sie einen echten Mehrwert bieten. Diese werden im Rahmen des Materials Organsisationstypen genannt, Sie können sich im Folgenden anhand weniger Fragen selbst einordnen.

Das vorliegende Material begleitet Sie auf diesem Weg: eine für Sie und zu Ihrer Einrichtung passende Cybersicherheit zu etablieren und langfristig weiter zu entwickeln. Die begleitenden Dokumente geben Ihnen einen nichttechnischen und einfach zu folgenden Einstieg in das Thema. Sie zeigen auf, welche Maßnahmen Sie treffen sollten und wie diese durch Sie oder einen Dienstleister umgesetzt werden können. Und sie geben Ihnen praktische Hilfestellung und vorgefertigte Schablonen, damit Sie Cybersicherheit effizient etablieren und sich auf Ihr Kerngeschäft konzentrieren können – die Pflege.

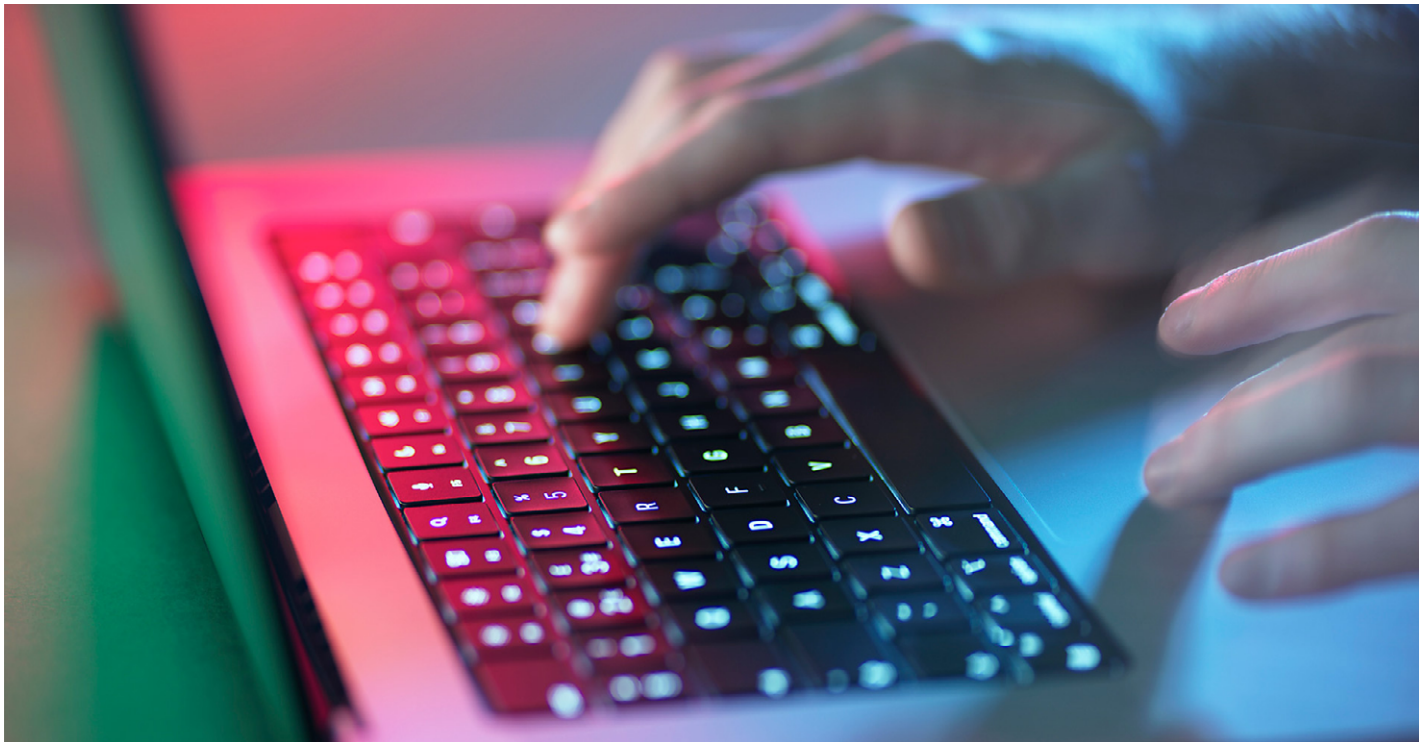
Um Sie bei der praktischen Umsetzung zu unterstützen, bietet Ihnen das Kompetenzzentrum Digitalisierung und Pflege Zugang zu einem kostenlosen Web-Portal, mit dem Sie die Planung und Umsetzung begleiten können und die Dokumentation für Sie zusammenstellt und verwaltet.

2 Wie eine E-Mail meinen Betrieb lahmlegte

Statistiken und Zahlen zeigen die wachsende Bedrohungssituation für Unternehmen auf. Zahlen sagen jedoch wenig darüber aus, wie sich ein Cyberangriff fühlt, wie einfach er ausgelöst werden kann und was die Auswirkungen auf die Einrichtung sind. Deshalb folgen auf den nächsten Seiten vier Geschichten aus sehr unterschiedlichen Einrichtungen.

Sie handeln von typischen Angriffen: Phishing, einer E-Mail mit Anhang, ein mehrfach verwendetes Passwort, oder die Sicherheitslücke bei einem Dienstleister. Die Einrichtungen sind erfunden, die Abläufe nicht – sie sind aus dokumentierten Vorfällen und aus Berichten aus der Praxis zusammengesetzt. Lesen Sie die Fälle deshalb nicht mit der Frage, wer hier einen Fehler gemacht hat, sondern mit der Frage: Was würde das bei uns bedeuten – und woran würde es bei uns hängen?

Antworten auf diese Frage gibt das folgende Kapitel. Zunächst geht es nur darum, einen solchen Vorfall einmal von innen zu sehen.



„Ihr Postfach läuft ab“

Ambulant

Breisgau

8 Mitarbeitende

Es ist Montagvormittag, und die hektischste Zeit im ganzen Monat. Bis morgen müssen alle Abrechnungen an die Kassen versendet sowie die monatlichen Gehälter verbucht sein. Diese Woche muss Monika all dies allein stemmen, ihre Kollegin ist leider krankheitsbedingt ausgefallen. Während Monika am Telefon in der Warteschleife der Bank hängt, geht eine E-Mail im Design von Microsoft 365 ein: „Ihr Speicherplatz ist erschöpft, bitte bestätigen Sie eine kostenlose Erweiterung mit Ihrem Passwort“. Schnell tippt sie mit dem Hörer am Ohr ihr Passwort ein, bestätigen, ok erledigt. Heute keine E-Mails mehr senden zu können, wäre wirklich schlecht gewesen.

Scheinbar ist alles normal. Das E-Mail Postfach lief nach der Erweiterung wie gewohnt weiter, es gab keinen Alarm im Virenscanner, auch keinen schwarzen Bildschirm. Die E-Mail zur Account-Erweiterung kam aber nicht von Microsoft, und seitdem sie Monikas Passwort wissen, lesen Kriminelle die E-Mails des Pflegedienstes mit.



In der darauffolgenden Woche verschicken die Angreifer aus dem echten Postfach gefälschte Rechnungen an Pflegebedürftige und Angehörige über neue Zuzahlungen. Den Briefbogen des Pflegedienstes, die Namen und Adressen von Pflegebedürftigen haben sie aus alten E-Mails gesammelt. In den kommenden zwei Wochen gehen immer mal wieder Telefonate von Angehörigen ein, die über die teils heftigen Zuzahlungen verärgert sind. Sie hätten bereits mehrere E-Mails geschickt, aber nie etwas gehört. Was keiner weiß: Die Kriminellen löschen eingehende Beschwerden sofort aus dem Postfach des Pflegedienstes, damit dort niemand Verdacht schöpft.

Viele der Familien hatten allerdings gezahlt und gehen nun zur Polizei und versuchen, das Geld irgendwie zurückzuerhalten. Nun kommt der Stein ins Rollen: die Polizei befragt Mitarbeiter, sichert Beweise in der Einrichtung. Schnell wird klar, dass im Postfach auch Pflegeberichte, Arztbriefe, und Vollmachten lagen. Neben dem Betrug handelt es sich auch um Datenschutzvorfall. Der Landesdatenschutzbeauftragte schaltet sich ein, es gibt eine verpflichtende Benachrichtigung jedes einzelnen Betroffenen. Insgesamt sind mehr als 25.000 Euro von Betroffenen an die Kriminellen gezahlt worden, diese treten nun mit Schadensersatzforderungen an den Dienst heran. Der Vorfall ist bald in der Regionalzeitung, darüber hinaus kennt man sich: die roten Kleinwagen mit dem charakteristischen Logo der Pflegeeinrichtung sind stadtbekannt, Mitarbeiter werden auf der Straße angesprochen. Der entstandene Vertrauensschaden ist immens und trifft den Pflegedienst im Ort härter als die verlorenen Kunden.

→ Cyberangriffe müssen nicht laut sein, selbst unscheinbare Vorgänge können der Auslöser sein, die schon bald vergessen werden - wie hier das abgefischte Passwort. Auch deshalb dauert es oft in der Praxis lang, bis jemand etwas bemerkt und der laufende Angriff dann auffällt. Andere Angriffe agieren nicht lange im Verborgenen, sondern sind sofort und umfassend präsent.

Ransomware – „Zurück zu Zettel und Stift“

Stationär
Ruhrgebiet
30 Mitarbeitende
80 Bewohner

Kurz nach der Mittagspause geht eine Bewerbung per E-Mail in der Verwaltung ein. Eine Pflegekraft bewirbt sich, sie zieht aus privaten Gründen in die Stadt und sucht eine neue Stelle. Der Lebenslauf im Anhang der E-Mail ist vielversprechend, eine super Ergänzung zum Team. Die Mitarbeiterin leitet die E-Mail noch am Freitagnachmittag an die Pflegedienstleiterin weiter, damit sich diese gleich Montag früh sich die Bewerberin anschauen und Kontakt aufnehmen kann.

Dazu kommt es jedoch nicht mehr: am Sonntagabend rufen Mitarbeiter per Handy die Pflegeleitung an, die Computer gehen nicht mehr, das Telefon auf Station übrigens auch nicht. Am Montagmorgen zeigt sich das wahre Ausmaß, alle Computer-Bildschirme im Haus zeigen eine große rote Warnung: „Ihre Daten wurden verschlüsselt, wir fordern Lösegeld“. Der eilige herbeigerufene Systemadministrator aus dem IT-Systemhaus stellt fest, dass in der Tat alle Daten verschlüsselt worden sind. Die Pflegedokumentation, Briefe, Abrechnungen, selbst die Telefonanlage wurde verschlüsselt. Auf den verschlüsselten PCs findet der Techniker einen Link zu einer Webseite der Cyberkriminellen: die Einrichtung hat 14 Tage Zeit, um insgesamt 75.000 Euro in Kryptowährung zu bezahlen, um ihre Daten wieder zu erhalten. Und nicht nur das: übers Wochenende haben die Täter anscheinend viele sensible Daten der Einrichtung ins Internet kopiert, unter anderem Patientenakten und Gehaltstabellen, und ein Teil dieser Daten steht bereits als Beweis des Hacks auf einer öffentlichen Webseite für alle zu sehen. Nach Ablauf dieser Frist drohen die Kriminellen, alle erbeuteten Daten öffentlich zu machen und die Angehörigen zu kontaktieren. Was tun?

Die gerufene Polizei schickt zwei Mitarbeiter, die sich speziell mit solchen Vorfällen auskennen. Diese nehmen den Angriff auf, können aber auch nicht bei der Wiederbeschaffung der Daten helfen. „Mit der Anzeige können Sie Hilfe von der Versicherung bekommen, wenn Sie denn eine haben und diese auch zahlt. Mit den Daten können wir auch nicht helfen, dafür sind die Backups da, aber wir empfehlen Ihnen dringend alle PCs, Server und das ganze Netzwerk neu aufzusetzen - denn oftmals lassen die Kriminellen irgendwo eine Tür in einem System offen, um später ein zweites Mal einzubrechen.“ Mittlerweile sind drei Techniker des Systemhauses vor Ort und berichten, dass auch alle Datenbestände auf den Servern verschlüsselt worden sind. Das letzte Backup vom vergangenen Monat scheint ok zu sein, allerdings enthält dieses nur Teile von dem, was nun gebraucht würde.



Mittlerweile herrscht bei der Pflegedienstleitung und auf den Stationen hektischer Betrieb. Die Pflegedokumentation ist nicht verfügbar, und man probiert nun die Medikationspläne aus Blistern und Erinnerung zu rekonstruieren. Das ist alles zusätzliche Arbeit neben der eigentlichen Versorgung und fehleranfällig - aber Fehler dürfen hier jetzt nicht passieren. Um hier zu helfen und die Mehrarbeit zu schultern, wurden die Mitarbeiter aus den letzten Schichten einbestellt. Alles läuft nun langsamer, und es scheint mindestens eine Pflegekraft pro Schicht und Station mehr nötig, damit alle Aufgaben erledigt werden können. Der Dienstplan der kommenden Woche existiert auch nur noch im Kopf der Pflegedienstleitung, braucht aber ohnehin einen Neuanfang: mit mehr Personal pro Schicht geht dies ohne Mehrarbeit nicht aus, aber mehr Schichten dürfen die Mitarbeiter so nicht machen? Und

wann kamen nochmal Uschi, Frank und Karin aus dem Urlaub zurück? - auch dies wusste der Computer. Durch die Störung der Telefone ist die Einrichtung nicht mehr für Angehörige zu erreichen. Diese machen sich Sorgen und kommen nun vermehrt vorbei, jeder Besuch bindet eine Pflegekraft, um die Situation zu erklären und den Besuch zu beruhigen. Es stellt sich nun heraus, auch die Schwesternrufanlage ist an das Telefon angeschlossen, als erste Lösung bleiben nun alle Türen offen und es werden Trillerpfeifen für Notfälle für die Pflegebedürftigen gekauft und verteilt.
Am Tag 2 des Vorfalls sind zumindest die Medikationspläne auf Papier aufgeschrieben, und ein Block ersetzt die ausgefallene Pflegesoftware. Natürlich müssen die handschriftlichen Notizen irgendwann übertragen werden, aber das ist ein Problem für später - vielleicht können das die Nachtschichten übernehmen? Das Systemhaus hat nun einen besseren Überblick über den Schaden: alle Computer neu aufzusetzen wird wahrscheinlich noch weitere 10 Tage dauern, aber dann beginnt die eigentliche Arbeit: die Fachanwendungen müssen installiert, konfiguriert und der fehlende Datenbestand zum Backup nachgearbeitet werden. Vermutlich wird die Verwaltung noch bis Ende nächsten Monats nicht einsatzbereit sein.

Nach wenigen Tagen scheint der Pflegebetrieb auf den neuen Modus eingeschwungen zu sein, allerdings klagen Mitarbeiter über die Überstunden und extra Schichten. Die Leitung der Einrichtung hat allerdings neue Sorgen: da bis kommendem Monat keine Abrechnung mit den Kassen möglich ist, aber schon bald Gehälter und Betriebsausgaben bezahlt werden müssen, gibt es bald ein dringendes Liquiditätsproblem, eine Insolvenz droht. Die Nachricht über die gestohlenen Unternehmensdaten hat parallel dazu bereits die Runde gemacht: mehrere Mitarbeiter haben schon signalisiert, bald einmal über das Gehalt sprechen zu wollen. Dazu kommen ebenfalls noch offene Meldungen an die Aufsichtsbehörde über die gestohlenen Patientenakten. Die zusehends drängende Frage an den Eigentümer: zahlen oder nicht?

→ Beide bisherigen Fälle haben eines gemeinsam: Der Weg hinein führte durch die Einrichtung selbst – durch ein Postfach, durch einen Menschen, der unter Zeitdruck stand. Getroffen werden kann man jedoch auch, ohne dass im eigenen Haus etwas geschehen ist, denn jedes Unternehmen bezieht Waren und Dienstleistungen von anderen. Dadurch sind Unternehmen miteinander verwoben, und ein Angriff auf einen Geschäftspartner kann so auch zum eigenem Problem werden.

„Wir haben 102 Laptops bestellt?“

Träger
Havelland
120 Mitarbeitende
100 Bewohner

Ein Träger im Havelland: ein Pflegeheim mit 100 Bewohnern und ein ambulanter Dienst, 120 Mitarbeiter. Die IT betreut ein spezialisiertes Systemhaus mit rund neunzig Kunden aus dem Gesundheits- und Sozialbereich.

Das Systemhaus verwaltet die Rechner seiner Kunden über eine Fernwartungssoftware, wie es alle machen: ein Programm auf jedem Gerät, eine zentrale Konsole beim Dienstleister, von dort aus kommt man auf jedes System, ohne hinzufahren. Diese Software hat im Februar eine Schwachstelle, für die es seit zwei Wochen ein Update gibt. Beim Systemhaus ist es noch nicht eingespielt.



Anfang März kommen Fremde über diese Lücke auf die Konsole. Damit haben sie nicht einen Kunden, sondern neunzig. Sie verschlüsseln nichts, sie fordern nichts, sie fallen nicht auf. Sie legen sich in jeder Umgebung einen unauffälligen Zugang an und sehen sich um.
Was sie suchen, findet sich in jeder Pflegeeinrichtung: Kundenkonten bei Lieferanten. Der Träger im Havelland hat elf davon – beim Pflegehilfsmittelhändler, beim Sanitätshaus, beim Küchengroßhandel, beim Bürobedarf, bei einem IT-Händler, bei einem Anbieter für Pflegebetten. Überall hinterlegt: Kundennummer, Ansprechpartner, Lieferung auf Rechnung, Zahlungsziel dreißig Tage. So läuft das seit Jahren, und so soll es auch laufen, denn keine Einrichtung bestellt Verbandmaterial gegen Vorkasse.

Ab der folgenden Woche wird eingekauft. Nicht auffällig viel auf einmal, aber stetig, verteilt über elf Lieferanten und zwei Wochen. Als Lieferadresse ist eine Halle in einem Gewerbegebiet vierzig Kilometer entfernt angegeben, mit dem Zusatz „Zwischenlager Sanierung“. Im folgenden Monat liegt der erste Stapel Rechnungen auf dem Tisch der Verwaltungsleiterin. Zwölf Notebooks und ein Karton Netzwerktechnik, zwei Fernseher. Fünf Patientenlifter und ein Treppensteiger. Küchengeräte. In der Summe 67.000 Euro. Was dann kommt, hat den Träger mehr beschäftigt als der Angriff. Die Lieferanten haben in gutem Glauben an einen langjährigen Kunden geliefert, bestellt aus dessen Mailkonto, unter dessen Kundennummer, mit Rückfrage und Bestätigung. Sie bestehen auf Zahlung. Die Frage, wer das Risiko eines missbrauchten Zugangs trägt, ist juristisch nicht so eindeutig, wie sie sich für den Träger anfühlt.

Bis alles abgeräumt ist, vergehen sieben Monate. Jede einzelne Bestellung muss widerlegt werden, mit Zeitangaben, Protokollen und Stellungnahmen, gegenüber Lieferanten, Inkassobüros und einer Auskunftei. Denn aus den Mahnungen wurden bald Inkassokorderungen, die die Bonität des Unternehmens schädigten - andere Lieferanten wollten dann nur noch begrenzt und gegen Vorkasse liefern. Das macht die Verwaltungsleiterin neben ihrer eigentlichen Arbeit. Sie sagt später, das Schlimmste sei nicht das Geld gewesen, sondern ein halbes Jahr damit zu verbringen, zu beweisen, dass man etwas nicht getan hat.
Und die Frage, die im Haus bleibt: Wer bei uns hätte eigentlich bemerken sollen, dass jemand in unserem Namen einkauft?

→ Bislang ist in diesen Fällen jemand eingebrochen, durch ein Postfach, eine Sicherheitslücke oder via einem Dienstleister. Jede Person und jedes Unternehmen hat jedoch eine Vielzahl an Zugangsdaten, die nicht nur der Nutzer sondern auch der Dienstanbieter schützen muss. Werden diese kompromittiert, meldet sich jemand ganz regulär an und unter einem Namen, den alle kennen und der befugt ist, eine Aktion durchzuführen.

„Um 3:14 Uhr habe ich geschlafen“



Ambulant

Lüneburger Heide

20 Mitarbeitende

Schwester Anja, seit elf Jahren im Team, nutzt für die web-basierte Pflegesoftware dasselbe Passwort wie für alle anderen Online-Zugänge der Pflegeeinrichtung – bequem, man muss sich ja genug merken. Ob Pflegesoftware, Labor, oder Versandshop für Material - mit einem gemeinsamen Zugang haben alle Mitarbeiter Zugriff - praktisch. Einer der Anbieter wird jedoch gehackt und die E-Mail-Adresse für den Zugang und das Passwort landen in einer Liste, die Kriminelle automatisiert bei Tausenden Portalen durchprobieren. Bei drei weiteren Onlineshops sowie bei der web-basierten Pflegesoftware passt es.

Es gibt keinen schwarzen Bildschirm, keine Lösegeldforderung, kein einziges Warnsignal. Im Gegenteil: Alles sieht völlig korrekt aus, denn im System arbeitet ja eine bekannte Mitarbeiterin. Über sechs Wochen werden nachts Akten geöffnet und exportiert – Diagnosen, Medikation, Vollmachten, Versichertennummern, Bankverbindungen aus den Einzugsermächtigungen, sowie Telefonnummern der Angehörigen.

Es fällt erst etwas auf, als Angehörige mit nicht erklärbaren Fällen melden. Ein Sohn ruft an, weil seine 84-jährige Mutter Mahnbescheide für Elektronikartikel bekommt, die sie nie bestellt hat. Zwei Tage später berichtet eine andere Familie von einem Ratenkredit auf den Namen des Vaters. Bei einer dritten Pflegebedürftigen wurde das Konto abgeräumt. Wer könnte hierfür verantwortlich sein?

→ Im Protokoll der Pflegesoftware stehen nächtliche Zugriffe und der Export von Daten, doch wer ist hier verantwortlich? Es gibt Gespräche der Geschäftsführung mit allen Mitarbeitern, es gibt Getuschel und Vermutungen im Team. Die Einrichtung wiederum steht vor der Frage, wie sie 40 Familien erklärt, dass die Daten ihrer Angehörigen abgeflossen sind – und wie sie der Aufsichtsbehörde darlegt, warum ein einziges Passwort ausgereicht hat.

3 Cybersicherheit für die Pflege

a. Schutzziele der Cybersicherheit – Was bedeutet das für mich?

In den vier Beispielen des vorigen Kapitels ist jedes Mal etwas verloren gegangen. Einmal war es der Zugriff auf die eigenen Daten. Einmal war es die Gewissheit, dass eine E-Mail wirklich von dem stammt, der darunter steht. Einmal war es die Vertraulichkeit von Akten. Und einmal die Möglichkeit, nachzuweisen, wer etwas getan hat und wer nicht.

So verschieden die vier Angriffe waren – die Liste dessen, was überhaupt verloren gehen kann, ist kurz. Sie umfasst eine Handvoll Punkte, die in der Cybersicherheit Schutzziele genannt werden. Schutzziele bringen Ihnen in der Praxis mehrere Vorteile:

1. Sie zeigen, wo Aufwand nötig ist – und wo nicht. Nicht alles in Ihrem Haus braucht denselben Schutz. Der Medikationsplan muss jederzeit verfügbar sein, das Archiv der Speisepläne von 2019 nicht. Man muss nicht jede Masche der Angreifer kennen – man muss wissen, was in der eigenen Einrichtung geschützt werden muss.

2. Sie legen das Ziel fest, nicht den Weg. Ein Schutzziel beschreibt, was sichergestellt sein muss. Dass der Medikationsplan auch bei einer Störung verfügbar bleibt, lässt sich über einen zweiten Server lösen, über einen täglichen Ausdruck im Dienstzimmer oder über einen Anbieter, der eine verbindliche Wiederanlaufzeit zusichert. Alle drei erfüllen dasselbe Ziel, und sie kosten sehr unterschiedlich viel. Erst wenn das Ziel benannt ist, haben Sie überhaupt die Wahl – und können die Variante nehmen, die zu Ihrer Größe, Ihrem Budget und Ihren Abläufen passt.

3. Sie machen Sicherheit besprechbar, beauftragbar und nachweisbar. Die Anforderung: „Wir hätten gerne mehr Sicherheit“ kann Ihnen niemand anbieten und niemand pauschal ermöglichen. „Die Pflegedokumentation muss innerhalb von vier Stunden wieder verfügbar sein, und jede Änderung an Medikationsdaten muss einer Person zuzuordnen sein“ ist dagegen eine konkrete Anforderung. Sie können sie in einen Vertrag schreiben, zwei Angebote miteinander vergleichen, Ihren Dienstleister daran messen und sie gegenüber Aufsichtsbehörde und Versicherung belegen – Letzteres verlangt die DSGVO in Art. 32 ausdrücklich von Ihnen. Fachbegriffe haben hier dieselbe Funktion wie in der Pflege: „Sie verschluckt sich beim Essen“ und „Dysphagie“ meinen dasselbe, aber nur der zweite Ausdruck sagt allen Beteiligten, was jetzt zu tun ist und wer es tut.

4. Sie verhindern blinde Flecken. Wer an Cybersicherheit denkt, denkt fast immer zuerst an Vertraulichkeit: an Daten, die nicht in falsche Hände geraten sollen. Die teuersten und gefährlichsten Vorfälle in der Pflege entstehen aber regelmäßig dadurch, dass etwas nicht verfügbar ist oder unbemerkt verändert wurde. Die kurze Liste der Schutzziele zwingt dazu, auch danach zu fragen.

Der Begriff Schutzziele klingt technisch, die Sache dahinter ist es nicht – Sie beschäftigen sich mit diesen Zielen implizit jeden Tag, seit es Ihre Einrichtung gibt.

Nehmen wir den Medikationsplan von Frau Weber, 84 Jahre, Wohnbereich 2. Dies ist ein gutes Beispiel, weil an diesem einen Dokument mehrere Anforderungen gleichzeitig verdeutlicht werden können, die inhaltlich wenig miteinander zu tun haben:

Verfügbarkeit - „Ich habe es, wenn ich es brauche“

Das Schutzziel Verfügbarkeit beschreibt, dass eine Information, ein Gerät oder ein Dienst dann nutzbar ist, wenn er gebraucht wird. In der Pflege merken Sie das Fehlen dieses Schutzziels immer im selben Moment: wenn Sie nach etwas greifen und es nicht da ist.

Die Frühschicht will um halb sieben stellen, und der Medikationsplan lässt sich nicht öffnen. Der Verbandwechsel steht an, aber die Wunddokumentation der vergangenen Tage ist nicht einsehbar – man sieht die Wunde, aber nicht ihren Verlauf, und weiß deshalb nicht, ob das, was man sieht, eine Verbesserung ist. In beiden Fällen ist niemand daran gehindert zu pflegen. Man pflegt nur ohne die Grundlage, auf der man es eigentlich tun müsste.

Deutlicher wird es, sobald es schnell gehen muss. Wird Frau Weber mit Verdacht auf einen Schlaganfall in die Klinik verlegt, muss die aktuelle Übersicht über Diagnosen, Medikation, Allergien und Betreuungssituation gemeinsam mit ihr das Haus verlassen – nicht in zwei Stunden, wenn das System wieder läuft, sondern in den fünf Minuten, die der Rettungsdienst im Flur steht. Was jetzt nicht mitgeht, fehlt in der Klinik und wird dort im Zweifel neu erhoben oder geschätzt.

Auf den ersten Blick scheint Verfügbarkeit wie eine Ja/Nein-Frage, sie beinhaltet aber auch eine Zeitfrage: Wie lange komme ich ohne es aus? Die Routine-Arbeit morgendliche Medikation kann ich etwas – vielleicht ein bis zwei Stunden – aufschieben, im Fall der Krankenhausverlegung brauche ich jetzt unmittelbar eine Antwort. Wenn mein Archivzugriff oder die Abrechnung gerade nicht geht, hat dies mehrere Tage Zeit, bevor es drängt. Aus der Beschreibung was brauche ich wann – und wie lange kann ich darauf maximal warten – leitet sich also auch eine Priorisierung ab, die mir in der Cybersicherheitsplanung hilft.

Verfügbarkeit betrifft nicht nur Daten und Akten, sondern auch Geräte und Dienste. Beispiele wären die Rufanlage, der Aufzug oder das Telefon. Und auch hier können wir direkt die Zeitfrage stellen: wie lange können Sie den normalen Ablauf aufrechterhalten, wenn alle Aufzüge gestört sind? Bis wann spätestens muss eine Alternative her? Dies formuliert dann konkrete Anforderungen an ein Schutzziel wie die Verfügbarkeit, und wir nutzen es später

ebenfalls für die Erstellung von Geschäftskontinuitätsplänen, so dass Sie trotz eines Ausfalls handlungsfähig bleiben.

Selbsttest

Wenn morgen früh kein Computer mehr ginge, wie würde der Tag ablaufen? Was wäre zu tun? Schreiben Sie zu fünf Dingen, die Sie täglich brauchen, jeweils eine Zahl auf: Wie lange dürfte es ausfallen, bevor es gefährlich wird? Wenn Sie dabei zögern, ist genau das die Lücke.

Integrität – „Was da steht ist korrekt und aktuell“

Das Schutzziel Integrität ist das am meisten unterschätzte Ziel. Es erfordert, dass Informationen richtig und aktuell sind. Ein Ausfall eines Systems – ein Bruch der Verfügbarkeit – fällt unmittelbar auf und löst eine Reaktion aus, eine verfälschte Information tut dies nicht. Dennoch ist Integrität gerade in Bereichen wie Gesundheit von elementarer Wichtigkeit.

Ist der vorliegende Medikationsplan in der aktuellsten Version, oder wurde die Dosisänderung von gestern eventuell nicht übernommen? In stressigen Momenten können schnell Fehler passieren: eine Dosierung wurde falsch vermerkt oder versehentlich in einer falschen Akte notiert. So kann Integrität unmittelbar Leib und Leben der Pflegebedürftigen betreffen. All dies sind unabsichtliche Versehen, doch absichtliche Handlungen – der Computer in der Pflegestation ist entsperrt, das Programm geöffnet, ein Angehöriger oder ein missgünstiger Kollege – können noch viel drastischere Konsequenzen haben.

Die Notwendigkeit für Integrität beginnt beim Medikationsplan, zieht sich aber durch alle Bereiche in der Einrichtung. Die Abrechnungen an die Kostenträger, die Bankverbindungen für die monatlichen Überweisungen an Angestellte und Lieferanten, die Richtigkeit all dieser Daten muss geschützt werden.

Selbsttest

Woran würden Sie merken, dass ein Eintrag im Medikationsplan verändert wurde? Können Sie nachvollziehen, welche Änderungen wann gemacht worden sind?

Vertraulichkeit - „Nur wer es darf, kann es sehen“

Das Schutzziel Vertraulichkeit beschreibt, dass Informationen nur von denen eingesehen werden können, die hierzu berechtigt sind. Frau Webers Plan verrät mehr als ihre Tabletten. Wer ihn liest, weiß, dass sie ein Antidepressivum bekommt, wogegen sie behandelt wird und oft auch, wie es um sie steht. Der Medikationsplan ist die Diagnose in Listenform.

Vertraulichkeit heißt nicht „geheim“, sondern „nur soweit für die Aufgabe nötig“. Die Küche muss wissen, dass Frau Weber eine Diabeteskost braucht. Sie muss nicht wissen, welches Antidepressivum sie nimmt. Genau diese Unterscheidung ist gemeint. Wenn der Medikationsplan anderen sichtbar wird, wird das Schutzziel Vertraulichkeit verletzt. Dies könnte sein, wenn der Wagen mit Akten im Flur steht, während die Pflegekraft im Zimmer ist, der Bildschirm im Dienstzimmer ungesperrt bleibt, Türen unverschlossen sind oder der Ausdruck auf dem Drucker liegen bleibt.

Anforderungen an Vertraulichkeit gibt es an vielen Stellen in der Einrichtung: die Tourenliste auf dem Beifahrersitz, Vollmachten, oder wenn Informationen über Pflegebedürftige per WhatsApp-Gruppe ausgetauscht werden. Die Umsetzung des Schutzziels in der Einrichtung schützt damit auch Sie und Ihre Mitarbeiter – denn alle Mitarbeiter müssen die Verschwiegenheitspflicht einhalten. Und natürlich müssen auch Informationen Ihrer Mitarbeiter – Personalakten oder Informationen über Gehälter – vertraulich behandelt werden.

Vertraulichkeit betrifft übrigens mehr als Datenschutz. Im Datenschutz geht es um den Schutz von personenbezogenen Daten, während die Vertraulichkeit alle Daten im Unternehmen, zum Beispiel den Kontostand des Unternehmens, betrifft. Umgekehrt regelt der Datenschutz mehr als nur Vertraulichkeit – etwa, ob Sie eine Information überhaupt erheben und wie lange Sie sie aufbewahren dürfen.

Selbsttest

Gehen Sie einmal an einem normalen Nachmittag durch Ihr Haus. Welche Bildschirme sind offen? Was liegt am Drucker? Welche Türen stehen auf? Welche Unterlagen liegen im Flur?

Neben diesen grundlegenden Anforderungen an Informationen, gibt es auch noch sogenannte erweiterte Ziele, die den Umgang mit Daten beschreiben:

Authentifizierung – „Wer bist du?“

Die Entscheidung, ob jemand berechtigt ist, eine Information zu sehen oder zu verändern, erfordert erst einmal Klarheit darüber, wer einen Zugriff machen möchte. Hierzu nutzt man in der Praxis Nutzernamen und Passwörter, aber auch (Zwei-Faktor-)Token.

Spät abends wird Frau Webers Plan geöffnet und es soll eine Änderung in der Dosis gespeichert werden. Wer hat dies beauftragt? Wenn alle mit dem gleichen Konto und dem geteilten Passwort „Pflege1“ arbeiten, lautet die Antwort „die Pflege“, und dies ermöglicht keine Authentifizierung. Die Dokumentation von Aktionen, die Nachvollziehbarkeit von Änderungen, und Vertraulichkeit brauchen eine klare Aussage, wer die Person ist.

Selbsttest

Können Sie sagen, welche Mitarbeiter gerade in der Pflegedokumentation angemeldet sind?

Autorisierung – „Was darfst du?“

Mit der Möglichkeit, Personen eindeutig zu authentifizieren, können auch andere Schutzziele umgesetzt werden. Eine Autorisierung steuert, wer bestimmte Aktionen ausführen darf, z.B. wer bestimmte Informationen lesen oder schreiben kann.

Auch dies leben Sie bereits jeden Tag. Ändern darf den Plan nur der behandelnde Arzt, die Pflegekraft verabreicht und dokumentiert. Die Küche sieht die Kostform, nicht den Wirkstoff. Drei Rollen, ein Dokument, drei verschiedene Rechte. Diese Rechte werden im Rahmen der Autorisierung und zugeordneten Berechtigungen digital abgebildet und auf Informationen angewendet.

Autorisierungen müssen mittels einer Berechtigungsverwaltung aktiv verwaltet werden. Die Kollegin, die vor zwei Jahren von Wohnbereich 2 nach 4 gewechselt ist, sieht Frau Webers Plan immer noch. Nicht aus bösem Willen – es hat nur nie jemand die Rechtevergabe angepasst.

Selbsttest

Welche Daten kann eine Pflegekraft in Ihrem Haus sehen?

Authentizität – „Ist das echt?“

Für wichtige Handlungen reicht es nicht, nur die Identität des Gegenübers zu kennen. Wir müssen auch sicher sein, dass eine Information tatsächlich von dem stammt, der als Absender oder Urheber auftritt. Ist der Anruf und die telefonische Anordnung, die Dosis zu verdoppeln, wirklich vom behandelnden Arzt?

Auch sonst ist Authentizität Grundvoraussetzung für sicheres Handeln: Ist die Mail vom Sanitätshaus echt? Ist der Anrufer wirklich vom Prüfdienst? Ist die geänderte Bankverbindung wirklich vom Lieferanten?

Selbsttest

Wie prüft die Stationsleitung, ob der Anrufer wirklich der behandelnde Arzt ist? Gibt es hierfür eine etablierte Regel, oder entscheidet jeder für sich?

Nicht-Abstreitbarkeit – „Wer war es – und kann er das später bestreiten?“

Kurze Zeit später stellt sich raus, dass die Dosis schädlich war, der Arzt erklärt, er habe das nie angeordnet. Bei dem Schutzziel Nicht-Abstreitbarkeit geht es nicht mehr darum, ob der Anruf echt war, sondern zu beweisen, von wem die Information kam. Diese Frage schützt nicht den Empfänger vor einer falschen Information oder Aktion wie der Fehlhandlung, sondern die Beteiligten in einer Auseinandersetzung mit Dritten.

Nicht-Abstreitbarkeit ist damit keine per-se technische Frage, sondern insbesondere eine juristische. Wer hat eine Aktion wann und wie aufgetragen und ausgeführt? In der Pflege ist die Pflegedokumentation der zentrale Beleg, und das Schutzziel Nicht-Abstreitbarkeit bedeutet, dass Sie nachvollziehen können, wer eine wichtige Aktion durchgeführt hat. Wenn Sie Authentifizierung und Autorisierung konsequent umsetzen, schützt es Sie und den einzelnen Mitarbeiter, und verschafft Handlungsfähigkeit. Wer hat diesen Schritt ausgeführt und warum? Wenn alle unter demselben Konto arbeiten, lässt sich keine Eintragung einer Person zuordnen.

Selbsttest

Nehmen Sie einen Eintrag in der Pflegedokumentation der letzten Woche. Können Sie zweifelsfrei sagen, wer ihn gemacht hat und ob und durch wen er danach geändert wurde?

Hiermit haben Sie die sieben Ziele an einem einzigen Dokument kennengelernt: Frau Webers Medikationsplan muss verfügbar sein, er muss stimmen, er darf nicht jeder Person einsichtig sein, ändern darf ihn nur der Arzt, seine Anordnungen müssen echt sein, und seine Einträge müssen sich einer Person zuordnen lassen.

Nicht immer und nicht überall haben die Ziele dasselbe Gewicht. Beim Medikationsplan steht Integrität vorn, im Notfall Verfügbarkeit, bei Personalakten Vertraulichkeit. Der vorliegende Maßnahmenkatalog begegnet dem durch einen risiko-basierten Ansatz, in dem er die Maßnahmen für die jeweils wichtigsten Schutzziele in einer Situation priorisiert.

b. Wenn Schutzziele gegeneinander stehen

Die Schutzziele sind nicht unabhängig voneinander, und sie ziehen nicht immer in dieselbe Richtung. Wer eines konsequent durchsetzt, beschädigt regelmäßig ein anderes – aus diesem Grund scheitert Cybersicherheit oft in der Praxis.

Das bekannteste Beispiel ist der Rechner, der am Medikamentenwagen mitfährt – bei Ihnen vielleicht ein Tablet oder ein Notebook auf der Ablage, an dem gestellt und gleich dokumentiert wird. Der Wagen steht dabei im Flur, während die Pflegekraft im Zimmer ist. Aus Sicht der Vertraulichkeit ist es deshalb genau richtig, dass sich der Bildschirm nach zwei Minuten sperrt: Andernfalls steht Frau Webers Medikationsplan für jeden lesbar im Gang – für Besucher, für Handwerker, für andere Bewohner.

Aus Sicht der Frühschicht bedeutet dieselbe Regel, sich auf einer Runde vierzehnmal neu anzumelden, mit Handschuhen, unter Zeitdruck, während im Zimmer jemand ruft. Was dann passiert, kennt jede Einrichtung: Das Passwort wandert auf einen Zettel am Wagen, die Anmeldung bleibt offen, oder alle arbeiten mit demselben Konto. Die Maßnahme, die die Vertraulichkeit erhöhen sollte, hat sie am Ende gesenkt – und die Nachvollziehbarkeit gleich mit. Das gleiche Prinzip erlebt die Pflegekraft im ambulanten Dienst mit dem Tourenhandy, welches jedes Mal neu entsperrt werden muss.

Daraus folgt eine Regel, die für alle vorgestellten Maßnahmen gilt: Eine Sicherheitsmaßnahme, die den Arbeitsablauf blockiert, wird umgangen. Und danach ist die Lage nicht so gut wie vorher, sondern schlechter – denn die Umgehung steht in keiner Dokumentation, und alle Beteiligten glauben, das Problem sei geregelt. Das ist kein Disziplinproblem und kein Grund, Ihren Mitarbeitern zu misstrauen. Es ist ein Konstruktionsfehler der Maßnahme.

Für Sie heißt das dreierlei:

1. Konflikte müssen entschieden werden, nicht ignoriert. Wenn Sie sich bewusst gegen die Zwei-Minuten-Sperre und für fünfzehn Minuten entscheiden, weil die Mitarbeiter sonst nicht arbeitsfähig sind, ist das eine legitime, risikobasierte Entscheidung – sofern Sie sie treffen, begründen und aufschreiben. Genau diesen Nachweis verlangt die DSGVO ohnehin von Ihnen.

2. Oft gibt es einen dritten Weg, der beide Ziele bedient. Eine Anmeldung per Chipkarte oder Ausweis ist schneller als ein Passwort und trotzdem persönlich. Ein Notfallzugang, der im Ernstfall alles freigibt, dabei aber protokolliert und im Nachhinein geprüft wird, sichert Verfügbarkeit und Nachvollziehbarkeit zugleich. Solche Lösungen finden Sie nur, wenn Sie den Konflikt vorher benannt haben.

3. Maßnahmen müssen zur Rolle passen. Was für die Verwaltung sinnvoll ist, kann in der Nachtwache unbrauchbar sein. Deshalb sind die Maßnahmen für die verschiedenen Anwendungsbereiche und Notwendigkeiten, aber auch die Größe und Möglichkeiten der verschiedenen Einrichtungen zugeschnitten.

C. Welcher Organsisationstyp bin ich?

Pflegeeinrichtungen sind sehr verschieden. Ein großer Träger mit mehreren stationären Häusern und ein kleiner ambulanter Pflegedienst unterscheiden sich nicht nur in Größe und Budget, sondern auch darin, welche Art von Maßnahmen sie am dringendsten brauchen. Was für das eine Haus die wichtigste Aufgabe der ersten Wochen ist, spielt im anderen kaum eine Rolle.

Damit für Sie die richtigen Maßnahmen ausgewählt und auf Ihre Einrichtung zugeschnitten werden können, arbeitet dieser Katalog mit sogenannten Organsisationstypen: exemplarischen Einrichtungen, die in den relevanten Merkmalen – Größe, Struktur, Versorgungsform und technische Ausstattung – miteinander vergleichbar sind. Sie müssen sich also nicht durch alle Maßnahmen arbeiten und selbst entscheiden, was auf Sie zutrifft. Sie ordnen sich einmal ein, und der Katalog trifft die Vorauswahl und die Priorisierung für Sie.

Welcher Organsisationstyp Ihrer Einrichtung entspricht, ermitteln Sie mit den folgenden vier Fragen:

Frage 1 – Wie ist Ihre Organisation aufgestellt?

- Wir sind eine Einrichtung an einem Standort → Frage 2
- Wir sind ein Träger mit mehreren Einrichtungen oder Standorten → Frage 3

Frage 2 – Was beschreibt Ihre Tätigkeit?

- Wir sind eine Tagespflege oder eine kleine stationäre Einrichtung mit bis zu 30 Betten → Organsisationstyp B
- Wir sind eine kleine ambulante Pflegeeinrichtung mit bis zu fünf Mitarbeiter, ein bis zwei Rechner, keine eigenen Server → Organsisationstyp A
- Alle anderen, weiter mit Frage 3

Frage 3 – Wer kümmert sich um Ihre IT?

- Wir betreiben eigene Server und Anwendungen im Haus und holen bei Bedarf ein lokales IT-Haus dazu → Organsisationstyp C
- Unsere IT wird dauerhaft von einem Dienstleister betreut, die meisten Anwendungen laufen in der Cloud → Organsisationstyp D

Frage 4 – Wie einheitlich ist Ihre IT über die Standorte hinweg?

- Historisch gewachsen: je Einrichtung unterschiedlich, Insellösungen, keine durchgängige Benutzer- und Geräteverwaltung → Organsisationstyp E
- Zentral gesteuert: einheitliche Benutzerverwaltung, zentralverwaltete Geräte, mehrere Dienstleister werden intern koordiniert → Organsisationstyp F

Was folgt aus Ihrer Einordnung?

Jede Maßnahme im Katalog trägt eine eindeutige Kennung, aus der Sie sofort ablesen können, für wen sie gedacht ist und wo sie hingehört. Die Maßnahme A.1.ClientSicherheit. Browser richtet sich beispielsweise an Organsisationstyp A, gehört zur ersten Etappe, betrifft den Themenbereich Client-Sicherheit und behandelt darin die Absicherung des Webbrowsers. Die Kennung setzt sich also aus vier Teilen zusammen:

- A – der Organsisationstyp, an den sich die Maßnahme richtet
- 1 – die Etappe, in der sie bearbeitet wird
- ClientSicherheit – der Themenbereich
- Browser – die konkrete Aufgabe

Für jeden Organsisationstyp ist ein eigener Maßnahmenkatalog zusammengestellt, den Sie als Ganzes herunterladen können. Und auch das Web-Portal kennt Ihre Zuordnung: Es legt Ihnen nur die Maßnahmen vor, die für Ihre Einrichtung tatsächlich relevant sind, in der für Sie sinnvollen Reihenfolge.

Wenn die Einordnung nicht eindeutig ist

Manche Träger lassen sich nicht auf einen einzigen Organsisationstyp festlegen – etwa, wenn unter einem Dach ein Pflegeheim, eine Tagespflege und ein ambulanter Dienst betrieben werden. In diesem Fall gilt eine einfache Regel: Ordnen Sie sich dem anspruchsvolleren Organsisationstyp zu, d.h. nehmen Sie den Buchstaben weiter im Alphabet. Sie enthält in der Regel alle Maßnahmen der kleineren und geht an den Stellen darüber hinaus, an denen Ihre zusätzliche Größe oder Struktur es erfordert. Alternativ können Sie für jeden Bereich getrennt vorgehen, wenn dieser über eigene Systeme und eigene Abläufe verfügt.

Und unabhängig davon: Der Organsisationstyp trifft eine Vorauswahl, sie schließt nichts aus. Wenn Sie beim Durchsehen auf eine Maßnahme aus einem anderen Katalog stoßen, die zu Ihrer Situation passt, setzen Sie sie um. Die Einordnung soll Ihnen Arbeit ersparen, nicht Ihre Möglichkeiten begrenzen.

d. Übersicht über die Vorgehensweise und große Bausteine des Katalogs

Cybersicherheit lässt sich nicht in einem Schritt herstellen. Der Versuch, alles auf einmal anzugehen, ist erfahrungsgemäß der häufigste Grund dafür, dass am Ende gar nichts passiert. Der vorliegende Katalog teilt den Weg deshalb in mehrere Etappen auf.

Jede Etappe verfolgt ein größeres Zwischenziel – etwa die Absicherung der häufigsten Einfallstore, die Begrenzung und Trennung von Zugriffsrechten oder den Aufbau eines Notfallprogramms. Die Etappen sind dabei so geschnitten, dass Sie mit jedem einzelnen Schritt die Sicherheit Ihrer Einrichtung tatsächlich verbessern. Sie müssen eine Etappe nicht vollständig abgeschlossen haben, um einen Nutzen davon zu haben.

Die Aufteilung hat zwei Gründe. Zum einen sortiert sie Abhängigkeiten: Manche Maßnahmen entfalten ihre Wirkung erst, wenn eine andere bereits umgesetzt ist – Rechte lassen sich zum Beispiel erst dann sinnvoll vergeben, wenn jede Person ein eigenes Benutzerkonto hat. Zum anderen sorgt die Reihenfolge dafür, dass der größte Zugewinn an Sicherheit möglichst früh entsteht. Sie beginnen mit dem, was am meisten bringt und am wenigsten kostet.

Innerhalb einer Etappe ist die Reihenfolge Ihnen überlassen. Die Aufgaben sind bewusst so zugeschnitten, dass sie unabhängig voneinander bearbeitet und in Ihrer Organisation verteilt werden können. Es ist ausdrücklich nicht vorgesehen, dass alles bei einer Person landet: Manches gehört in die Verwaltung, manches zur Pflegedienstleitung, manches zur Haustechnik – und manches beauftragen Sie bei Ihrem Dienstleister.



Organisationstyp A –
Kleiner ambulanter Pflegeservice

Etappe 1: Basisschutz
Etappe 2: Grundlegende Sicherheitsvorkehrungen
Etappe 3: Segmentierung & Zugriffssteuerung
Etappe 4: Vorfallsmanagement



Organisationstyp B –
Tagespflege und kleine stationäre Einrichtung

Etappe 1: Grundlegende Sicherheitsvorkehrungen
Etappe 2: Segmentierung & Zugriffssteuerung
Etappe 3: Erweiterte Maßnahmen
Etappe 4: Vorfallsmanagement



Organisationstyp C –
Ambulanter Pflegedienst mit selbstverwalteter IT

Etappe 1: Grundlegende Sicherheitsvorkehrungen
Etappe 2: Schnittstellen und Reaktionsfähigkeit
Etappe 3: Planung und Resilienz
Etappe 4: Gesteuerte Weiterentwicklung



Organisationstyp D –
Stationäre Einrichtung mit externen Dienstleistern

Etappe 1: Grundlegende Sicherheitsvorkehrungen
Etappe 2: Externe Abhängigkeiten
Etappe 3: Planung und Resilienz
Etappe 4: Gesteuerte Weiterentwicklung



Organisationstyp E –
Träger mit mehreren Standorten und dezentraler Struktur

Diese Einrichtungen verfügen in der Regel über ein bestehendes Management-system. Die Handlungsempfehlung stellt Ihnen Checklisten zur Verfügung, um die Abdeckung nach Maßnahmen zu überprüfen. Die Kataloge der vorherigen Organi-sationstyps stehen Ihnen als Ressourcen zusätzlich zur Verfügung.



Organisationstyp F –
Träger mit mehreren Standorten und zentraler Organisation

Diese Einrichtungen verfügen in der Regel über ein bestehendes Management-system. Die Handlungsempfehlung stellt Ihnen Checklisten zur Verfügung, um die Abdeckung nach Maßnahmen zu überprüfen. Die Kataloge der vorherigen Organi-sationstypen stehen Ihnen als Ressourcen zusätzlich zur Verfügung.

Die Maßnahmen selbst sind unterschiedlicher Natur. Sie finden Anleitungen zur Konfiguration von Systemen im laufenden Betrieb, Empfehlungen für die bessere Gestaltung von Abläufen, Richtlinien zur Kommunikation und zur rechtlichen Absicherung, Schulungsinhalte für Ihre Mitarbeiter sowie Vorschläge für Anschaffungen, die die Sicherheit Ihrer Einrichtung verbessern. Dazu kommen Vorlagen und Schablonen: vorformulierte Texte, Musterschreiben und Checklisten, die Sie nur noch an Ihre Einrichtung anpassen müssen.

So ist eine Maßnahme aufgebaut

Jede Maßnahme ist ein eigenständiges Dokument von ein bis drei Seiten. Dieser Umfang ist bewusst gewählt: Eine Maßnahme soll sich in höchstens einer Stunde umsetzen lassen, meist geht es deutlich schneller. Was mehr Zeit beanspruchen würde, ist in mehrere Maßnahmen zerlegt.

Jedes Maßnahmendokument enthält:

- Das Schutzziel, das abgesichert wird. Damit können Sie jede Maßnahme in das einordnen, was Sie im vorigen Abschnitt kennengelernt haben – und selbst entscheiden, wie wichtig sie für Ihre Einrichtung ist.
- Wer sie umsetzt: Sie selbst, Ihr Dienstleister, oder beide gemeinsam. Bei Maßnahmen, die ein Dienstleister übernehmen muss, finden Sie eine fertige Formulierung, die Sie unverändert weiterleiten können.
- Voraussetzungen, falls eine andere Maßnahme vorher erledigt sein sollte.
- Eine Schätzung von Aufwand und Kosten, sofern externe Ausgaben anfallen.
- Was Sie dokumentieren sollten. Diese Angaben sind zugleich Ihr Nachweis gegenüber Aufsichtsbehörde und Versicherung, dass Sie die Maßnahme getroffen haben – und ersparen Ihnen später die Rekonstruktion aus dem Gedächtnis.
- Anhänge mit vorformulierten Texten, die Sie für Ihren eigenen Zweck nur anpassen müssen.

Für die Organsisationstypens A bis D steht Ihnen darüber hinaus ein eigenes Begleitdokument zur Verfügung, das Sie Schritt für Schritt durch diesen Prozess führt.

e. Wie bringe ich das in meinem Haus zum Laufen?

Am Anfang steht eine Standortbestimmung

Bevor Sie die erste Maßnahme umsetzen, sollten Sie wissen, was Sie überhaupt haben. Welche Systeme sind im Einsatz, welche Geräte hängen am Netz, welche Dienstleister arbeiten für Sie, und wer hat Zugang zu Ihren Daten? Ohne diese Liste lässt sich nichts priorisieren, denn Sie können nicht entscheiden, was besonders geschützt werden muss, solange Sie nicht wissen, was es gibt. Was ich nicht kenne, kann ich nicht schützen.

Diese Bestandsaufnahme ist deshalb nicht nur eine Vorbereitung, sondern bereits die erste Maßnahme. In vielen Einrichtungen ist die fehlende Übersicht selbst die größte Schwachstelle. Fast immer tauchen dabei Dinge auf, von denen niemand mehr wusste: ein Fernwartungszugang aus einem alten Wartungsvertrag, ein Benutzerkonto eines längst ausgeschiedenen Mitarbeiters, ein Gerät in der Haustechnik, das seit Jahren am Internet hängt, oder eine Abhängigkeit von einem Dienstleister, die nie jemand ausgesprochen hat.

Ebenso wichtig ist die andere Blickrichtung: Keine Einrichtung fängt bei null an. Sie haben mit hoher Wahrscheinlichkeit bereits einen Virenschutz, eine Datensicherung, Verschwiegenheitserklärungen, eine Schließanlage und einen Vertrag mit einem IT-Dienstleister. Vieles davon lässt sich übernehmen und weiterführen. Auch das gehört zur Standortbestimmung – und es erspart Ihnen doppelte Arbeit.

Nehmen Sie sich Zeit für Cybersicherheit – regelmäßig

Cybersicherheit scheitert selten am Wollen. Sie scheitert am Kalender. Sie ist wichtig, aber nie die dringendste Aufgabe an einem Tag, und damit verliert sie jeden Tag gegen alles, was gerade brennt.

Das Gegenmittel kennen Sie aus Ihrem eigenen Betrieb. Auch Hygienebegehung, Brandschutzunterweisung und Pflegevisite wären ohne feste Termine längst untergegangen. Behandeln Sie Cybersicherheit genauso: ein fester Termin im Monat, ein bis zwei Stunden, im Kalender wie jeder andere Pflichttermin.

Setzen Sie sich dabei realistische Ziele. Zwei bis vier Maßnahmen pro Monat sind neben dem Tagesgeschäft machbar – und bringen Sie innerhalb eines halben Jahres ein erhebliches Stück voran. Wer sich zu viel vornimmt, hört erfahrungsgemäß schnell wieder auf.

Nachdem Sie die Maßnahmen umgesetzt haben, geht es in den Erhalt: denn Cybersicherheit ist eine wiederkehrende Aufgabe. Prüfen Sie den Stand einmal jährlich, und zusätzlich immer dann, wenn sich etwas ändert: neue Software, ein neuer Dienstleister, ein neuer Standort – oder nachdem etwas passiert ist.

Bei der Planung, der Zuordnung von Aufgaben an Ihre Mitarbeiter und der Verfolgung Ihres Fortschritts unterstützt Sie das begleitende Web-Portal.

Dokumentation pflegen

Neben Planung und Umsetzung ist die Dokumentation der dritte, oft vergessene Teil. Erst wenn ein Vorgang nach seiner Durchführung festgehalten wird, können alle darauf vertrauen, dass er auch wirklich stattgefunden hat. Das ist bei der Konfiguration eines Virenscanners nicht anders als bei der Gabe eines Medikaments.

Dokumentation bedeutet dabei keine Aktenordner voller Papier. Zu den meisten Maßnahmen genügt eine kurze Notiz: wer hat wann etwas umgesetzt, und mit welchem Ergebnis wurde es geprüft. An den relevanten Stellen finden Sie in den Anhängen der Maßnahmen fertige Vorlagen dafür. Mit diesen können Sie bei einer Prüfung oder gegenüber Ihrer Versicherung belegen, dass Sie sich um das Thema

gekümmert haben – und zwar nachweisbar und nicht nur aus der Erinnerung.

Noch einfacher geht es über das Web-Portal: Dort verwalten Sie nicht nur Aufgaben und Zuständigkeiten, sondern lassen sich die Nachweise über die umgesetzten Maßnahmen auch direkt erzeugen.

Wenn etwas nicht geht

Nicht jede Maßnahme passt in jede Einrichtung. Manches lässt sich mit Ihren Abläufen, Ihrer Technik oder Ihrem Personalstand nicht sinnvoll umsetzen. Das ist kein Scheitern – vorausgesetzt, Sie gehen bewusst damit um.

Entscheiden Sie ausdrücklich, dass Sie eine Maßnahme nicht oder nicht in dieser Form umsetzen. Halten Sie fest, warum. Und überlegen Sie, was Sie stattdessen tun, um dasselbe Schutzziel wenigstens teilweise zu erreichen. Eine begründete, dokumentierte Abweichung ist etwas völlig anderes als eine übersehene Maßnahme – und genau diese Abwägung verlangt die DSGVO in Art. 32 von Ihnen.

Wo geht es heute los?

- Wählen Sie drei Maßnahmen aus, die sofort wirken, und weisen Sie sie den zuständigen Mitarbeitern zu.
- Tragen Sie sich den nächsten Termin ein, bevor Sie dieses Kapitel zuklappen.

4 Zusammenfassung

Cybersicherheit ist heute essenziell für jedes Unternehmen. Denn:

1. **Auch Ihre Einrichtung ist ein Ziel:** Der häufigste Einwand lautet, man sei zu klein und zu unbedeutend, um jemanden zu interessieren. Das war einmal richtig. Heute laufen Angriffe automatisiert und massenhaft; die Täter suchen keine bestimmte Einrichtung, sondern eine offene Tür. In den vergangenen zwölf Monaten waren 87 Prozent der Unternehmen in Deutschland betroffen – vom Einzelunternehmen bis zum Konzern.

2. **Der Gesundheitsbereich steht besonders im Fokus:** Das Bundeskriminalamt führt ihn als eine von vier Schwerpunktbranchen, europaweit entfällt jeder fünfte Angriff auf kritische Einrichtungen auf das Gesundheitswesen. Der Grund ist einfach: Pflegeeinrichtungen besitzen nicht nur Computer, sondern Patientenakten. Kriminelle erpressen deshalb längst nicht mehr nur die Einrichtung, sondern treten auch an Pflegebedürftige und Angehörige heran.

3. **Der Schaden ist selten ein IT-Schaden:** Die vier Beispiele in diesem Dokument zeigen, was tatsächlich passiert: Medikationspläne, die zur Stellzeit nicht verfügbar sind. Angehörige, die auf gefälschte Rechnungen zahlen und danach der Einrichtung nicht mehr vertrauen. Wochen an Nachdokumentation. Ausbleibende Abrechnungen und daraus ein Liquiditätsproblem. Und Mitarbeiter, die unter Verdacht geraten, weil niemand nachvollziehen kann, wer was getan hat. Getroffen wird immer der Betrieb, nicht die Technik.

4. **Vorsorge ist auch eine Pflicht – mit persönlicher Verantwortung:** Datenschutzrecht, Berufsrecht und Gesellschaftsrecht verlangen von Ihnen angemessene Schutzmaßnahmen und den Nachweis darüber. Fehlende Kenntnisse entlasten die Geschäftsführung dabei ausdrücklich nicht. Umsetzen kann die Aufgabe jemand anders – verantwortlich bleibt die Leitung.

5. **Sicherheit ist beherrschbar, weil sie aus wenigen Zielen besteht:** Sie müssen nicht wissen, wie Angriffe funktionieren. Sie müssen wissen, was in Ihrem Haus geschützt werden muss: dass Informationen verfügbar sind, wenn sie gebraucht werden; dass sie stimmen; dass nur die Befugten sie sehen; und dass nachvollziehbar bleibt, wer was getan hat. Mit diesen grundlegenden Aspekte leitet sich alles Weitere ab.

6. **Sicherheit muss weder teuer noch kompliziert sein:** Ein erheblicher Teil der wirksamsten Maßnahmen kostet kein Geld, sondern eine Entscheidung und etwas Zeit. Entscheidend ist nicht, alles gleich stark zu schützen, sondern zu wissen, was wie stark geschützt werden muss.

Was Sie jetzt tun können

Sie brauchen für die Umsetzung von Cybersicherheit keinen Projektplan, keine teure Beratung oder eine komplett neue IT. Sie brauchen für den Start einen Nachmittag:

- Verschaffen Sie sich einen Überblick: Welche Systeme, Geräte, Dienstleister und Zugänge gibt es in Ihrer Einrichtung? Was Sie nicht kennen, können Sie nicht schützen – und diese Liste fehlt in den meisten Häusern.
- Wählen Sie drei Maßnahmen aus, die sofort wirken, und weisen Sie sie den zuständigen Personen zu. Jede einzelne Maßnahme in diesem Katalog ist so zugeschnitten, dass sie in höchstens einer Stunde umgesetzt werden kann.
- Tragen Sie sich den nächsten Termin ein. Cybersicherheit scheitert selten am Wollen, sondern am Kalender. Behandeln Sie sie wie die Hygienebegehung oder die Brandschutzunterweisung: ein fester Termin, regelmäßig, im Kalender wie jeder andere Pflichttermin.

Was daraus wird

Wenn Sie zwei bis vier Maßnahmen im Monat umsetzen – mehr ist neben dem Tagesgeschäft nicht realistisch –, haben Sie nach einem Vierteljahr die häufigsten Einfallstore geschlossen. Nach einem Jahr haben Sie geordnete Zugriffsrechte, wissen, von welchen Dienstleistern Sie abhängen, und verfügen über ein Notfallkonzept, das Sie handlungsfähig hält, wenn doch etwas passiert. Und Sie können jederzeit belegen, was Sie getan haben – gegenüber der Aufsichtsbehörde, Ihrer Versicherung und Ihren Bewohnern.

Damit ist Ihre Einrichtung nicht unangreifbar. Aber sie ist kein leichtes Ziel mehr und steht im Ernstfall nicht ohne Plan da. Damit stellen Sie sicher, dass der Pflegebetrieb weiterläuft, Patienten versorgt und Ihre Mitarbeiter bezahlt werden können.

Wie es weitergeht

Der auf Ihren Organsisationstyp zugeschnittene Maßnahmenkatalog steht Ihnen zum Download bereit, ergänzt um ein Begleitdokument, das Sie durch die Etappen führt. Einen Anfang zu machen ist das Schwerste. Danach ist jede weitere Verbesserung nur noch ein kleiner Schritt.

Bildnachweise

In diesem Abschnitt sind die im Dokument verwendeten Bilder und Grafiken mit den zugehörigen Quellen- und Urheberangaben aufgeführt.

- Seite 9: © Andrew Brookes / Westend61
- Seite 10: © Krakenimages.com / stock.adobe.com
- Seite 11: © mapo / stock.adobe.com
- Seite 13: © Velocitystock777 / stock.adobe.com
- Seite 14: © Pixel-Shot / stock.adobe.com
- Seite 24: © highwaystarz / stock.adobe.com
- Seite 24: © BusinessClass / cocoon studio
- Seite 24: © Westend61 / Maskot
- Seite 24: © Westend61 / Javier de la Torre


VPN
0100
1010