Notfallübung für die Klinik-IT: Downtime, Notbetrieb und die Rückkehr zum Papier



WISSEN
Alle Beiträge der Serie zu Microsoft 365 und Klinik-IT an einem Ort.
› **Microsoft 365 im Krankenhaus**

BERATUNG
Moderierte Notfall- und Red-Team-Übung für Ihr Haus, mit Szenario, Auswertung und Maßnahmenplan.
› **Beratung für Krankenhäuser**

SCHULUNG
Für IT-Teams und Krisenstab: Notbetrieb, Rollen, Entscheidungen und Wiederanlauf trainieren.
› **Schulungen für Krankenhäuser**

Jedes Krankenhaus hat einen Notfallplan. Er steht im QM-Handbuch, er wurde im letzten Zertifizierungsaudit wohlwollend durchgeblättert, und er liegt, das ist der Klassiker, als PDF auf genau dem Dateiserver, der im Ernstfall verschlüsselt ist. Ob der Plan trägt, weiß niemand, bis es so weit ist. Und dann ist es Montag, drei Uhr früh, die Rufbereitschaft hat gerade ihren Kaffee verschüttet, und die Frage lautet nicht mehr, ob der Plan gut ist, sondern wo er liegt.

Eine Notfallübung für die IT im Krankenhaus ist das Gegenmittel. Nicht die Brandschutzübung mit Sammelplatz und Strichliste, sondern ein moderiertes Planspiel, in dem Geschäftsführung, Ärztlicher Direktor, Pflegedirektion, IT, Medizintechnik, Datenschutz, Informationssicherheit, Pressestelle und die Vertretung der Belegschaft an einem Tisch sitzen und ein realistisches Szenario durchspielen. Im Kliniktakt, mit Schichtwechsel, Visite und Notaufnahme, die nicht warten, bis die IT fertig ist.

Denn die Erfahrung aus Vorfällen ist ernüchternd eindeutig: **Große Schäden entstehen, weil jemand, der es kann, unter Druck den falschen Knopf drückt, oder weil niemand weiß, wer den Stecker ziehen darf.** Beides lässt sich üben. Dieser Beitrag ist der Abschluss der Serie Microsoft 365 im Krankenhaus. Er beschreibt drei Szenarien, die sich als Planspiel bewährt haben, die Klinikbesonderheiten zwischen Downtime-Konzept und Papierdokumentation und die Frage, wie eine Übung zu Änderungen führt, die im nächsten Ernstfall tatsächlich helfen.

FAKTEN · Das Wichtigste in Kürze

Eine Notfallübung testet nicht die Technik, sondern Entscheidungen: Wer trennt das Netz, wer ruft den Notbetrieb aus, wer meldet die Klinik bei der Rettungsleitstelle ab, wer informiert wen, wenn Mail und Teams ausfallen?

Bewährte Szenarien: Verschlüsselung in der Nacht zum Montag, Ausfall des Identitätsdienstes während der Visite, kompromittiertes Dienstleisterkonto.

§ 391 SGB V verlangt von Krankenhäusern Vorkehrungen nach dem Stand der Technik für Verfügbarkeit, Integrität und Vertraulichkeit sowie Maßnahmen, die das Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter stärken. Für Betreiber kritischer Anlagen gelten stattdessen die Pflichten des BSIG.

Meldepflichten nach § 32 BSIG für wichtige und besonders wichtige Einrichtungen: Frühwarnung spätestens nach 24 Stunden, Meldung nach 72 Stunden, Abschlussmeldung spätestens einen Monat danach. Daneben gelten die Meldepflichten des Datenschutzes.

Ergebnis jeder Übung ist eine Liste von Änderungen an Verfahrensanweisungen, Kontaktlisten und Berechtigungen, nicht ein Teilnahmezertifikat.

Warum Klinik-IT anders üben muss als ein Bürobetrieb

In einem Verwaltungsbetrieb bedeutet ein IT-Ausfall, dass die Arbeit liegen bleibt. Im Krankenhaus bleibt nichts liegen: Patienten werden weiter aufgenommen, versorgt, verlegt und entlassen, Medikamente werden weiter gegeben, Befunde weiter gebraucht. Der Betrieb läuft weiter, nur ohne das Werkzeug, auf das er sich eingestellt hat. Deshalb ist die Kernfrage einer Notfallübung im Krankenhaus nicht „Wann ist die IT wieder da?“, sondern „Wie arbeiten wir sicher, solange sie es nicht ist?“.

Dazu kommt die Verflechtung. Das KIS hängt an Subsystemen wie LIS, RIS und PACS, an Schnittstellen, an Anmeldediensten und an Druckern. Die Medizintechnik hat ihre eigenen Netze, eigene Fernwartungen und eigene Dienstleister. Microsoft 365 ist über Entra ID mit dem lokalen Active Directory verbunden, und die Verwaltung telefoniert vielleicht über Teams, während Station und Zentrale an der Klinik-TK hängen. Ein Ausfall trifft selten genau ein System, und die Übung muss zeigen, welche Abhängigkeiten im Notfallplan fehlen.

Downtime-Konzept und Papierdokumentation

Das Downtime-Konzept beschreibt, wie das Haus ohne KIS arbeitet. In vielen Krankenhäusern existiert es, aber es wurde von der IT geschrieben, und die Stationen kennen es vom Hörensagen. Eine gute Übung prüft deshalb nicht das Dokument, sondern die Praxis: Wo liegen die Papierformulare für Aufnahme, Anforderung, Befund und Verlegung? Wer weiß auf der Station, welche Patienten gerade da sind, wenn die Stationsübersicht dunkel bleibt? Gibt es Notfallrechner, die regelmäßig einen aktuellen Lesestand erhalten, und hat schon einmal jemand im Nachtdienst nachgesehen, ob sie funktionieren?

Die Rückkehr zum Papier ist dabei nur die halbe Geschichte. Die andere Hälfte ist die Rückkehr vom Papier: Alles, was während des Notbetriebs handschriftlich dokumentiert wurde, muss nach dem Wiederanlauf ins KIS. Wer nacherfasst, mit welcher Priorität und wie die Stationen dabei entlastet werden, gehört in dieselbe Verfahrensanweisung. Sonst endet der Notbetrieb technisch nach drei Tagen und organisatorisch nach drei Monaten.

TIPP · Der Kugelschreibertest

Bitten Sie im Planspiel die Pflegedirektion, eine Station zu nennen, und fragen Sie dann ganz konkret: Wo liegt dort jetzt, in diesem Moment, der Formularsatz für den Notbetrieb, und wann wurde er zuletzt auf Aktualität geprüft? Die Antwort auf diese eine Frage sagt mehr über die Notfallvorsorge als jedes Konzeptpapier.

Wie Notfallpläne und Standards so abgelegt werden, dass sie auf Station schnell auffindbar sind und trotzdem eine Papierfassung für den Ausfall existiert, beschreibt der Beitrag Hygieneplan,

Pflegestandards, Notfallpläne: Was auf Station in zehn Sekunden auffindbar sein muss.

Abmeldung von der Notfallversorgung und Rettungsleitstelle

Die folgenschwerste Entscheidung in einem IT-Notfall ist oft keine technische: Kann die Notaufnahme weiter Patienten vom Rettungsdienst annehmen, oder muss sich das Haus ganz oder für einzelne Fachbereiche von der Notfallversorgung abmelden? Diese Entscheidung trifft die Klinikleitung mit dem Ärztlichen Direktor, nicht die IT. Die IT liefert aber die Lage, auf der die Entscheidung beruht: Funktionieren Labor, Bildgebung und Befundübermittlung noch, wie lange dauert ein Wiederanlauf realistisch, und was ist mit der Medizintechnik?

Wie die Abmeldung erfolgt, ist nicht bundeseinheitlich geregelt. Rettungsdienst und Leitstellen sind Ländersache, und je nach Bundesland und Rettungsdienstbereich läuft die Abmeldung telefonisch, über ein elektronisches Nachweissystem für Behandlungskapazitäten oder über beides. Das elektronische System ist im IT-Notfall womöglich nicht erreichbar. Die Übung sollte deshalb klären: Wer ruft die Leitstelle an, mit welcher Nummer von welchem Telefon, und wer meldet das Haus nach dem Wiederanlauf wieder an?

WICHTIG · Abmeldung ist keine IT-Entscheidung

Die IT darf und soll eine Empfehlung abgeben, etwa „Laborbefunde frühestens morgen Mittag wieder elektronisch“. Ob sich das Haus deshalb abmeldet, entscheidet die dafür benannte Person der Klinikleitung. Hinterlegen Sie im Notfallplan Name, Vertretung und Erreichbarkeit, auch nachts und am Wochenende.

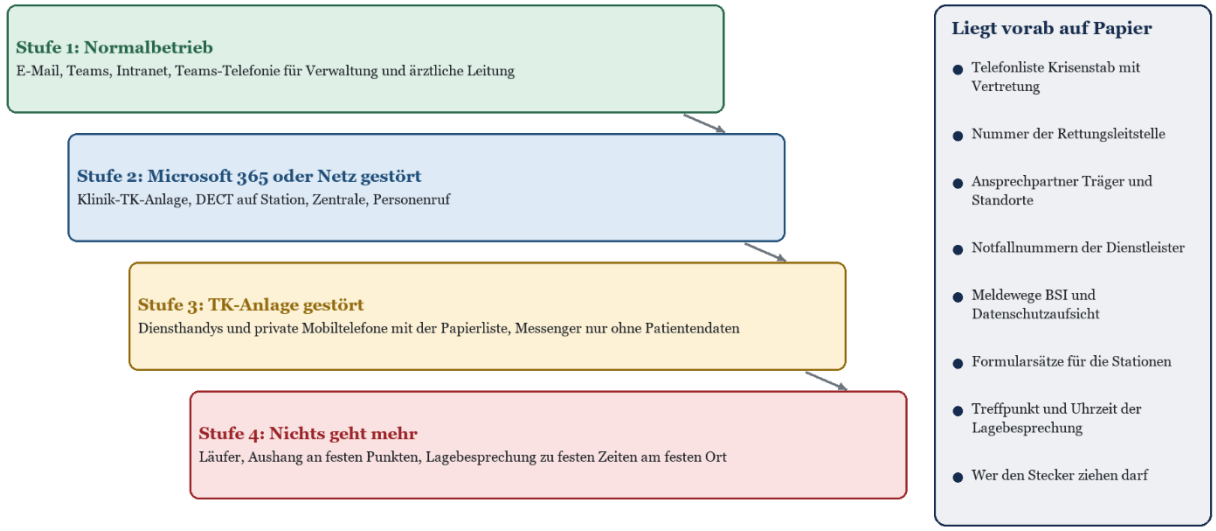
Kommunikation, wenn Mail und Telefonie ausfallen

Der Krisenstab trifft sich, und als Erstes schlägt jemand vor, die Belegschaft per Rundmail zu informieren. Das ist der Moment, in dem die Übung ihren ersten Lacher erntet, und den wichtigsten Befund. Wenn Microsoft 365 nicht verfügbar ist, weil Konten kompromittiert sind oder die Anbindung gekappt wurde, fallen E-Mail, Teams und Intranet gleichzeitig aus. Wenn die Verwaltung und die ärztlichen Leitungspositionen über Teams-Telefonie telefonieren, sind auch diese Apparate still.

Hier zeigt sich, warum Teams-Telefonie im Krankenhaus als Unteranlage hinter der Klinik-TK richtig aufgehoben ist: Station, DECT, Zentrale und Patiententelefone bleiben an der großen Anlage, und die trägt auch dann, wenn die Cloud-Anbindung gestört ist. Wie diese Aufteilung aussieht, beschreibt der Beitrag Teams-Telefonie als Unteranlage im Krankenhaus: Verwaltung und Ärzte an Teams, Station und Patienten an der Klinik-TK. Für die Übung heißt das: Spielen Sie den Abstieg über die Rückfallebenen bewusst durch, bis zur untersten Stufe, auf der Läufer Zettel tragen.

Skizze 2: Rückfallebenen der Kommunikation

Jede Stufe tiefer ist langsamer, aber robuster. Üben Sie den Abstieg.



Teams-Telefonie bleibt Unteranlage, die Klinik-TK trägt Station, Zentrale und Patienten.

WARNUNG · Messenger im Notbetrieb

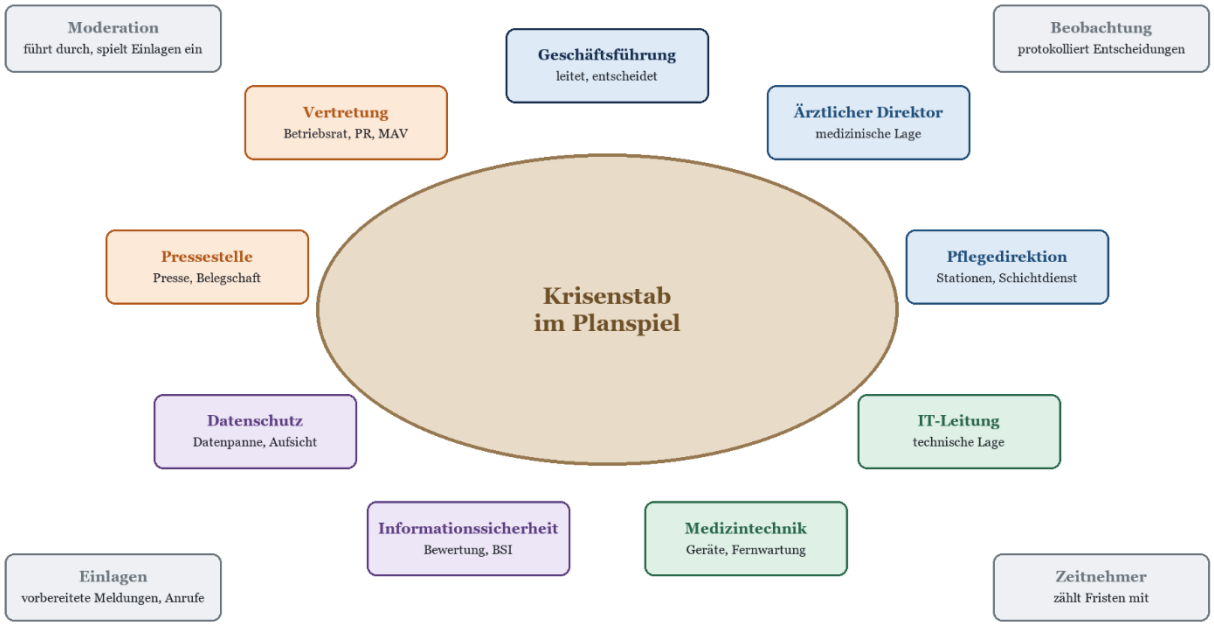
Wenn alles ausfällt, greifen Ärzte und Pflegekräfte zum privaten Smartphone. Das ist menschlich und im ersten Moment kaum zu verhindern. Legen Sie vorab fest, was über solche Kanäle kommuniziert werden darf, nämlich Organisatorisches wie Treffpunkte und Uhrzeiten, und was nicht, nämlich Patientendaten. Eine Regel, die erst im Ernstfall entsteht, wird nicht mehr gelesen.

Wer am Tisch sitzt und warum jeder Platz zählt

Ein Planspiel nur mit der IT ist eine technische Besprechung. Die interessanten Befunde entstehen an den Schnittstellen: wenn die IT-Leitung sagt, sie brauche zwei Stunden für eine Lagebewertung, und die Pflegedirektion antwortet, der Frühdienst beginne in neunzig Minuten. Oder wenn die Pressestelle fragt, was sie der Lokalzeitung sagen soll, und die Informationssicherheit noch nicht weiß, ob Daten abgeflossen sind. Deshalb gehören alle Rollen an den Tisch, die im Ernstfall entscheiden oder informieren müssen.

Skizze 3: Wer beim Planspiel am Tisch sitzt

Innen entscheiden, außen steuern und beobachten.



Neun Plätze, jeder mit benannter Vertretung. Leere Stühle sind ein Befund.

Rolle	Aufgabe im Planspiel	Typische Erkenntnis
Geschäftsführung	leitet den Krisenstab, trifft die Grundsatzentscheidungen	Entscheidungen brauchen eine Lage, und die Lage braucht Zeit
Ärztlicher Direktor	bewertet die medizinische Versorgungslage, Abmeldung von der Notfallversorgung	welche Funktionsbereiche ohne IT wie lange arbeitsfähig sind
Pflegedirektion	Stationen, Schichtdienst, Papierdokumentation	ob die Formulare dort liegen, wo der Plan sie vermutet
IT-Leitung und Rufbereitschaft	technische Lage, Eindämmung, Wiederanlauf	wer nachts was entscheiden darf, ohne jemanden zu wecken
Medizintechnik	Geräte, eigene Netze, Fernwartung der Hersteller	welche Geräte vom Netz getrennt weiterarbeiten und welche nicht
Informationssicherheitsbeauftragter	Bewertung des Vorfalls, Meldung nach BSIG soweit einschlägig	wer die Fristen mitzählt, wenn alle löschen
Datenschutzbeauftragter	Bewertung der Datenschutzverletzung, Meldung an die zuständige Aufsicht	welche Aufsicht zuständig ist, je nach Träger und Land
Pressestelle	Information von Presse, Öffentlichkeit und Belegschaft	vorbereitete Textbausteine sparen die schlimmste Stunde
Betriebsrat, Personalrat oder MAV	Belange der Belegschaft, Mehrarbeit, Schichtplanung, Auswertung von Protokollen	frühe Einbindung verhindert Streit in der Krise

Moderation, Einlagen und Beobachtung

Ein Planspiel braucht eine Moderation, die das Szenario kennt, die Teilnehmer aber nicht bewertet. Sie spielt sogenannte Einlagen ein, also vorbereitete Ereignisse: ein Anruf der Leitstelle, eine Anfrage der Presse, die Nachricht, dass auch die Sicherung betroffen ist. Eine Beobachtung

protokolliert jede Entscheidung mit Uhrzeit und Begründung. Ein Zeitnehmer achtet darauf, dass Fristen im Spiel genauso ablaufen wie im Ernstfall, auch wenn die Übung selbst nur einen halben Tag dauert.

Externe Moderation hat einen einfachen Vorteil: Sie darf unbequeme Fragen stellen, ohne am nächsten Morgen wieder mit denselben Menschen in der Kantine zu sitzen. Interne Moderation hat den Vorteil, das Haus zu kennen. Bewährt hat sich eine Mischung, in der externe Moderation das Szenario führt und eine interne Person die Hausbesonderheiten einbringt.

Die Vertretung der Belegschaft gehört dazu

Betriebsrat, Personalrat oder Mitarbeitervertretung sitzen nicht aus Höflichkeit am Tisch. Ein längerer Notbetrieb bedeutet Mehrarbeit, geänderte Schichtpläne und Sonderdienste, und die Auswertung eines Vorfalls greift auf Anmelde- und Zugriffsprotokolle zurück, die Rückschlüsse auf Personen erlauben. Welches Gremium zuständig ist und welche Rechte es hat, hängt von der Trägerschaft ab: Betriebsverfassungsgesetz bei privaten und vielen freigemeinnützigen Häusern, Personalvertretungsrecht des jeweiligen Landes bei öffentlichen Häusern, kirchliches Mitarbeitervertretungsrecht bei kirchlichen Trägern. Die Unterschiede beschreibt der Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

HINWEIS · Keine Rechtsberatung

Ob eine Übung, ihre Auswertung oder die dabei genutzten Protokolle mitbestimmungspflichtig sind, hängt vom Einzelfall, von der Trägerschaft und vom Landesrecht ab. Klären Sie das mit Ihrer Rechtsabteilung und der zuständigen Vertretung, bevor die erste Übung stattfindet. Eine Dienst- oder Betriebsvereinbarung zum Notbetrieb erspart im Ernstfall Diskussionen, für die dann niemand Zeit hat.

Drei Planspiel-Szenarien im Kliniktakt

Gute Szenarien sind realistisch, aber nicht vorhersehbar, und sie zwingen zu Entscheidungen unter Unsicherheit. Die folgenden drei haben sich bewährt, weil sie jeweils einen anderen Teil der Organisation unter Druck setzen: die Nacht und die Rufbereitschaft, den laufenden Stationsbetrieb und die Abhängigkeit von Dienstleistern.

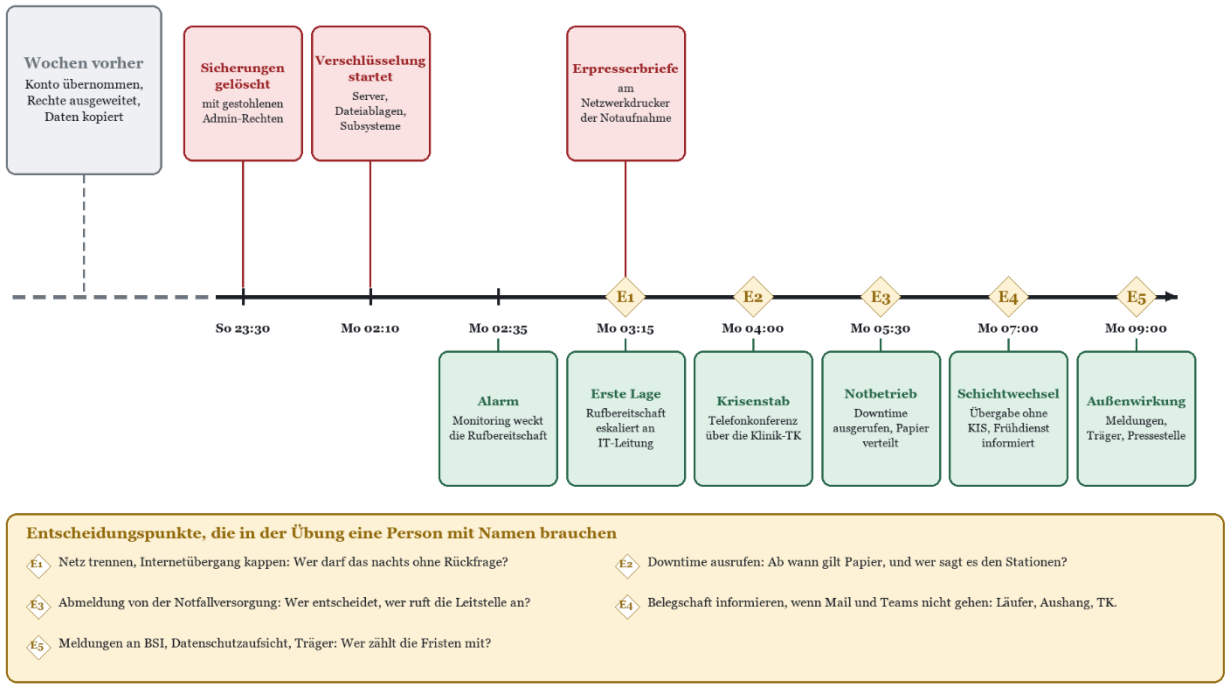
Szenario	Übungsziel	Beteiligte Rollen	Dauer
Verschlüsselung in der Nacht zum Montag	Eskalation aus der Rufbereitschaft, Entscheidung zur Netztrennung, Notbetrieb ausrufen, Abmeldung von der Notfallversorgung, Meldefristen	Geschäftsführung, Ärztlicher Direktor, Pflegedirektion, IT, Medizintechnik, Informationssicherheit, Datenschutz, Pressestelle, Vertretung	halber Tag Planspiel, dazu Vor- und Nachbereitung
Ausfall des Identitätsdienstes während der Visite	Anmeldung an KIS und Stationsrechnern ohne Domäne oder Entra ID, Notfallkonten, Papierdokumentation im laufenden Dienst	Pflegedirektion, Ärztlicher Direktor, IT, Informationssicherheit, Vertretung	zwei bis drei Stunden
Kompromittiertes Dienstleisterkonto	Überblick über Fremdzugänge, Sperrbefugnis, Beweissicherung, Abstimmung mit Hersteller und Medizintechnik	IT, Medizintechnik, Informationssicherheit, Datenschutz, Einkauf oder Vertragsmanagement, Geschäftsführung	zwei bis drei Stunden

Szenario 1: Verschlüsselung in der Nacht zum Montag

Angreifer haben ein Gespür für Dienstpläne. Die Nacht zum Montag ist beliebt, weil die Besetzung dünn ist und am Morgen alle gleichzeitig merken, dass nichts geht. Das Szenario beginnt mit einem Alarm des Monitorings um halb drei. Die Rufbereitschaft sieht verschlüsselte Dateien auf dem Dateiserver, kurz danach druckt der Netzwerkdrucker in der Notaufnahme Erpresserbriefe. Die Sicherungen, das zeigt sich später, wurden schon Stunden vorher gelöscht.

Skizze 1: Angriff und Reaktion in der Nacht zum Montag

Oben der Angreifer, unten das Krankenhaus, auf der Linie die Entscheidungspunkte.



Fiktives Übungsszenario, Zeiten beispielhaft und nicht maßstäblich.

Die Übung prüft fünf Entscheidungspunkte. Erstens: Darf die Rufbereitschaft den Internetübergang und die Verbindung zu den anderen Standorten sofort trennen, oder muss sie erst jemanden erreichen? Zweitens: Wer ruft den Notbetrieb aus, und wie erfahren die Stationen davon? Drittens: Wer entscheidet über die Abmeldung von der Notfallversorgung? Viertens: Wie wird der Frühdienst um sechs Uhr informiert, wenn Mail und Intranet nicht gehen? Fünftens: Wer beginnt, die Meldefristen zu zählen, und ab welchem Zeitpunkt?

WARNUNG · Der falsche Knopf

Unter Druck tun gute Administratoren, was sie am besten können: reparieren. Server neu starten, Konten löschen, Systeme aus der Sicherung neu aufsetzen. Jede dieser Handlungen kann Spuren vernichten, die für die Frage „Seit wann sind sie da?“ entscheidend sind, und eine zu früh angeschlossene Wiederherstellung kann den Angreifer gleich mit zurückholen. Legen Sie im Notfallplan fest, welche Sofortmaßnahmen erlaubt sind, nämlich trennen und isolieren, und welche erst nach Rücksprache folgen, nämlich löschen, neu aufsetzen und wiederherstellen.

Wie Angreifer typischerweise bis zu diesem Punkt kommen und welche Maßnahmen die Kette vorher unterbrechen, beschreibt der Beitrag Ransomware im Krankenhaus: Der Weg über Konten und Microsoft 365 und was wirklich hilft. Die Notfallübung setzt bewusst dort an, wo diese Maßnahmen versagt haben. Das ist kein Misstrauen gegenüber der eigenen Sicherheitsarbeit, sondern Ehrlichkeit.

Szenario 2: Ausfall des Identitätsdienstes während der Visite

Dienstag, halb zehn, die Visite ist auf den Stationen unterwegs. Plötzlich schlagen Anmeldungen fehl: am Stationsrechner, in der Terminalsitzung, im KIS. Ursache kann ein Ausfall der Domänencontroller sein, eine fehlerhafte Gruppenrichtlinie, ein abgelaufenes Zertifikat oder eine Störung bei Entra ID. Für die Station ist die Ursache zunächst egal. Wer angemeldet ist, bleibt es vielleicht noch eine Weile, wer sich neu anmelden muss, steht vor einem schwarzen Bildschirm.

Dieses Szenario ist besonders lehrreich, weil es keinen Angreifer braucht und trotzdem den ganzen Betrieb trifft. Es prüft, ob es ein Notfallverfahren für die Anmeldung gibt, ob Notfallkonten für Microsoft 365 und Entra ID existieren und funktionieren, und ob die Stationen wissen, ab wann sie auf Papier umstellen. Microsoft empfiehlt, mindestens zwei Notfallzugriffskonten als reine Cloud-Konten einzurichten, die nicht von lokalen Diensten abhängen und deren Anmeldung überwacht wird. Ob diese Konten tatsächlich funktionieren, zeigt erst ein Test, und der gehört in den Übungsplan.

FAKTEN · Was beim Identitätsausfall zu prüfen ist

Notfallkonten für Entra ID: vorhanden, von bedingtem Zugriff korrekt behandelt, Anmeldedaten sicher hinterlegt, Nutzung überwacht, Test dokumentiert.

Lokales Active Directory: Wiederherstellungsverfahren für Domänencontroller beschrieben und geübt, Kennwort für den Wiederherstellungsmodus auffindbar.

Stationsarbeitsplätze: Verhalten bei Anmeldeausfall bekannt, etwa zwischengespeicherte Anmeldungen und laufende Sitzungen.

KIS: lokaler Notfallzugang oder Lesestand auf Notfallrechnern, mit dem Hersteller abgestimmt.

Wie die Anmeldung am Stationsarbeitsplatz aufgebaut ist und wo ihre Abhängigkeiten liegen, beschreibt der Beitrag Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel. Für die technischen Grundlagen von Entra ID, Notfallkonten und bedingtem Zugriff finden Sie Hintergründe im Kompetenzbereich Microsoft Entra ID.

Szenario 3: Das kompromittierte Dienstleisterkonto

Freitagnachmittag ruft ein Hersteller an: Bei ihm sei eingebrochen worden, möglicherweise seien Zugangsdaten zu Kundensystemen betroffen. Welche, könne man noch nicht sagen. Die Frage an die Klinik-IT lautet jetzt: Welche Zugänge hat dieser Dienstleister bei uns? Ein VPN-Konto, ein Fernwartungswerkzeug, ein Gastkonto in Entra ID, ein Dienstkonto mit Rechten in der Domäne, eine Unternehmensanwendung mit Berechtigungen auf Postfächer? Und wer darf sie sperren, wenn die Sperre die Wartung eines Medizinprodukts unterbricht?

Das Szenario zeigt zuverlässig, ob es einen vollständigen Überblick über Fremdzugänge gibt. In gewachsenen Umgebungen ist das selten der Fall, und genau deshalb lohnt sich vorher eine Bestandsaufnahme. Was sich bei einer solchen Überprüfung typischerweise findet, beschreibt der Beitrag Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet. Für die Übung selbst zählt die Abstimmung: Die IT will sperren, die Medizintechnik fragt nach den Folgen für den Gerätebetrieb, der Einkauf sucht den Vertrag, und die Informationssicherheit möchte Protokolle sichern, bevor irgendjemand etwas ändert.

AUS DER PRAXIS · Lehren aus forensischer Arbeit bei einem Krankenhausverbund

Aus der forensischen Arbeit bei einem Krankenhausverbund mit mehreren Standorten bleiben ohne Details des Falls drei allgemeine Lehren. Erstens: Die Frage „Seit wann und mit welchen Konten?“ lässt sich nur so gut beantworten, wie Anmelde- und Ereignisprotokolle vorhanden, lange genug aufbewahrt und außerhalb der betroffenen Systeme gesichert sind. Zweitens: Vertrauensstellungen

zwischen Domänen vergrößern nicht nur die Angriffsfläche, sondern auch den Bereich, der untersucht werden muss. Drittens: Gut gemeinte Sofortmaßnahmen ohne Absprache erschweren die Aufklärung. Wer übt, wer welche Maßnahme freigibt, spart im Ernstfall Tage.

Wie sich Vertrauensstellungen und Altdomänen im Verbund ordnen lassen, beschreibt der Beitrag Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung.

Wer darf den Stecker ziehen? Befugnisse, Meldepflichten und Wiederanlauf

Die häufigste Lücke, die eine Notfallübung im Krankenhaus aufdeckt, ist keine technische. Es ist die fehlende Antwort auf die Frage, wer was entscheiden darf. Die Rufbereitschaft weiß, wie man den Internetübergang trennt, ist sich aber nicht sicher, ob sie es darf, weil dann auch die Telemedizin-Verbindung und die Fernwartung der Medizintechnik weg sind. Also ruft sie an. Die IT-Leitung ist im Urlaub, die Vertretung hat das Handy lautlos, und die Geschäftsführung wird nachts nicht geweckt, weil das noch nie jemand getan hat. Diese Kette kostet im Ernstfall Stunden, in denen ein Angreifer weiterarbeitet.

Entscheidungsbefugnisse vorab festlegen

Entscheidung	Wer entscheidet	Ohne Rückfrage erlaubt?
Einzelne Systeme vom Netz isolieren	Rufbereitschaft IT	ja, mit Protokollnotiz
Internetübergang und Standortverbindungen trennen	IT-Leitung oder benannte Vertretung	ja, bei klaren Anzeichen eines Angriffs, Information an Geschäftsführung unverzüglich
Konten von Dienstleistern sperren	IT-Leitung mit Medizintechnik	ja, wenn die Patientensicherheit nicht berührt ist
Notbetrieb und Papierdokumentation ausrufen	Geschäftsführung oder benannte Vertretung	nein, aber Bereitschaft vorbereiten
Abmeldung von der Notfallversorgung	benannte Person der Klinikleitung mit Ärztlichem Direktor	nein
Systeme löschen, neu aufsetzen, wiederherstellen	Krisenstab nach Rücksprache mit Informationssicherheit	nein
Kommunikation nach außen	Geschäftsführung mit Pressestelle	nein

Diese Tabelle ist ein Vorschlag, keine Vorschrift. Entscheidend ist, dass es überhaupt eine gibt, dass sie Namen und Vertretungen enthält und dass sie auf Papier im Notfallordner liegt. Ein Krankenhaus ist an Hierarchien gewöhnt. Im IT-Notfall muss die Hierarchie vorher entschieden haben, damit nachts niemand auf sie warten muss.

Meldepflichten mit Fristen

Sobald ein erheblicher Sicherheitsvorfall erkannt ist, laufen Fristen. Für Krankenhäuser, die als wichtige oder besonders wichtige Einrichtung unter das BSIG fallen, regelt § 32 BSIG ein gestuftes Verfahren gegenüber der gemeinsamen Meldestelle von BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: eine Frühwarnung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, eine Meldung innerhalb von 72 Stunden mit erster Bewertung, auf Ersuchen eine Zwischenmeldung und spätestens einen Monat nach der Meldung eine

Abschlussmeldung. Betreiber kritischer Anlagen machen zusätzlich Angaben zur betroffenen Anlage und zur kritischen Dienstleistung.

Unabhängig davon gilt der Datenschutz. Nach Art. 33 DSGVO ist eine Verletzung des Schutzes personenbezogener Daten in der Regel binnen 72 Stunden der zuständigen Aufsichtsbehörde zu melden, und bei hohem Risiko sind nach Art. 34 DSGVO auch die betroffenen Personen zu benachrichtigen. Kirchliche Häuser haben mit dem KDG oder dem DSG-EKD eigene Regelungen und eigene Aufsichten, wie im Beitrag Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch beschrieben. Welche Pflichten Landeskrankenhausgesetze, Landesdatenschutzgesetze oder Vorgaben des Trägers zusätzlich vorsehen, unterscheidet sich je Bundesland und gehört in die Vorbereitung jeder Übung.

Für alle Krankenhäuser, die nicht als Betreiber kritischer Anlagen den Pflichten des BSIG unterliegen, verlangt § 391 SGB V angemessene Vorkehrungen nach dem Stand der Technik sowie Maßnahmen, die das Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter stärken. Ein moderiertes Planspiel ist genau so eine Maßnahme. Der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ der DKG liegt in Version 1.3.1 vom 10. Oktober 2025 vor; welche Anforderungen er an Notfallmanagement und Übungen stellt, prüfen Sie in der aktuellen Fassung. Den Zusammenhang zwischen NIS2, § 391 SGB V und dem B3S erläutert der Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

HINWEIS · Keine Rechtsberatung

Ob Ihr Haus unter § 391 SGB V oder unter das BSIG fällt, welche Meldungen in welcher Frist an wen gehen und welche Aufsicht zuständig ist, hängt von Größe, Trägerschaft und Bundesland ab. Klären Sie das vorab mit Rechtsabteilung, Datenschutzbeauftragtem und Informationssicherheitsbeauftragtem, legen Sie Meldevorlagen an und drucken Sie sie aus. Im Ernstfall liest niemand mehr Gesetzestexte, und die Frist läuft trotzdem.

Wiederanlauf und Rückkehr vom Papier

Der Wiederanlauf ist eine eigene Übungseinheit. Welche Systeme kommen in welcher Reihenfolge zurück? Erst Identität und Netz, dann KIS, dann die Subsysteme, oder gibt es Abhängigkeiten, die eine andere Reihenfolge erzwingen? Wer gibt ein wiederhergestelltes System frei, und woran erkennt man, dass es sauber ist? Und wer organisiert die Nacherfassung der Papierdokumentation, ohne dass die Stationen neben dem Regelbetrieb auch noch drei Tage Notbetrieb abtippen?

Ergebnis dieser Einheit ist eine Wiederanlaufliste mit Reihenfolge, Abhängigkeiten und Freigabe. Sie gehört als gelenktes Dokument ins QM-Handbuch, mit Prüfdatum und Verantwortung, und als Ausdruck in den Notfallordner. Wie Dokumentenlenkung im Krankenhaus funktioniert, beschreibt der Beitrag QM-Handbuch mit SharePoint: Dokumentenlenkung im Krankenhaus, die im Audit hält.

Skizze 4: Der Übungszyklus

Eine Übung ist erst fertig, wenn sich eine Verfahrensanweisung geändert hat.



Empfehlung: mindestens einmal jährlich ein Planspiel, Szenario wechselnd.

Vom Planspiel zur Red-Team-Übung: So planen Sie Ihre Notfallübung

Nicht jede Übung muss das ganze Haus betreffen. Bewährt hat sich ein Stufenplan, der mit einem Planspiel am Tisch beginnt und sich über praktische Teilübungen bis zu einer technischen Angriffssimulation steigert. Jede Stufe hat ihren Nutzen, und jede setzt die vorherige voraus: Eine Red-Team-Übung in einem Haus, das noch nie geklärt hat, wer den Stecker ziehen darf, findet vor allem diese Lücke.

Übungsform	Was geprüft wird	Aufwand im Betrieb	Geeignet für
Planspiel am Tisch	Entscheidungen, Rollen, Kommunikation, Meldewege	gering, keine Systeme betroffen	Einstieg und jährliche Wiederholung
Downtime-Übung in einem Bereich	Papierdokumentation, Formulare, Übergabe, Nacherfassung	mittel, mit Pflegedirektion und Station abgestimmt	Häuser mit vorhandenem Downtime-Konzept
Technische Wiederherstellungsübung	Sicherung, Wiederanlauf, Notfallkonten, Wiederherstellung des Active Directory in einer isolierten Umgebung	mittel, ohne Eingriff in den Produktivbetrieb	IT-Teams, die ihre Zeiten kennen wollen
Red-Team-Übung	Erkennung und Reaktion auf einen simulierten Angriff unter realistischen Bedingungen	hoch, mit klaren Regeln, Ausschlüssen und Abbruchkriterien	Häuser mit geübtem Krisenstab und Überwachung

WARNUNG · Medizintechnik ist kein Übungsgelände

Bei jeder Übung mit Eingriff in Systeme gilt: Medizinprodukte und Systeme, die unmittelbar der Patientenversorgung dienen, sind ausgeschlossen, solange Medizintechnik und Hersteller nicht ausdrücklich zugestimmt haben. Legen Sie Ausschlüsse, Zeitfenster, Ansprechpartner und ein Abbruchkriterium schriftlich fest. Eine Übung darf die Versorgung nie gefährden.

Was eine Übung vorbereitet braucht

- **Ziel:** eine oder zwei Fragen, die die Übung beantworten soll, etwa „Können wir nachts innerhalb einer Stunde den Notbetrieb ausrufen?“
- **Szenario mit Einlagen:** realistisch für das eigene Haus, mit Uhrzeiten, Anrufen und überraschenden Wendungen
- **Unterlagen:** Notfallplan, Downtime-Konzept, Kontaktlisten, Meldevorlagen, möglichst in der Papierfassung, die es im Ernstfall gäbe
- **Rollen:** alle Plätze am Tisch besetzt, Vertretungen benannt, Moderation und Beobachtung festgelegt
- **Vertraulichkeit:** Übungsbefunde sind sensibel und gehören nicht in einen offenen Teams-Kanal
- **Nachbesprechung:** direkt im Anschluss, ohne Schuldfrage, mit Maßnahmenliste, Verantwortung und Termin

TIPP · Notfall- und Red-Team-Übung mit Begleitung

Sie möchten die erste Übung nicht allein vorbereiten? Unter Microsoft 365 Beratung für Krankenhäuser finden Sie eine moderierte Notfall- und Red-Team-Übung für Krankenhäuser: Szenario passend zu Ihrem Haus, Moderation im Planspiel, Beobachtung, Auswertung und ein priorisierter Maßnahmenplan, der sich in Verfahrensanweisungen und QM-Handbuch übertragen lässt. Grundlage ist Projekterfahrung in Klinikverbünden mit Active Directory, PKI, Exchange Hybrid und Forensik.

Für IT-Teams und Krisenstabsmitglieder, die Notbetrieb, Rollen und Wiederanlauf trainieren wollen, gibt es passende Inhalte unter Microsoft 365 Schulung für Krankenhäuser.

Wer die technischen Grundlagen der Absicherung von Microsoft 365 vertiefen möchte, findet sie im Kompetenzbereich Microsoft 365 Security. Die branchenübergreifende Umsetzung der NIS2-Anforderungen beschreibt NIS2 technisch umsetzen mit Microsoft 365.

Häufige Fragen zur Notfallübung für die Klinik-IT

Wie oft sollte ein Krankenhaus eine IT-Notfallübung durchführen?

Eine feste, für alle Häuser geltende Frequenz gibt es nicht. Bewährt hat sich ein Planspiel mindestens einmal im Jahr mit wechselndem Szenario, ergänzt um Downtime-Übungen in einzelnen Bereichen und technische Wiederherstellungstests. Wer den B3S anwendet oder als Betreiber kritischer Anlagen geprüft wird, sollte die Übungsplanung mit den dortigen Anforderungen abgleichen.

Können wir eine Notfallübung im laufenden Betrieb machen?

Ein Planspiel am Tisch ja, es berührt keine Systeme. Praktische Übungen auf Station oder in der IT sind möglich, wenn sie sorgfältig vorbereitet, zeitlich begrenzt und mit Pflegedirektion, Ärztlichem Direktor und Medizintechnik abgestimmt sind. Die Patientenversorgung hat immer Vorrang, und jede Übung braucht ein Abbruchkriterium.

Was gehört in ein Downtime-Konzept?

Mindestens: wer den Notbetrieb ausruft, welche Formulare wo liegen, wie Aufnahme, Anforderung, Befundübermittlung und Verlegung ohne KIS laufen, welche Notfallrechner oder Lesestände es gibt, wie kommuniziert wird, wenn Mail und Telefon ausfallen, und wie nach dem Wiederanlauf nacherfasst wird. Das Konzept gehört als gelenktes Dokument ins QM-Handbuch und als Papierfassung auf jede Station.

Was unterscheidet eine Red-Team-Übung von einem Penetrationstest?

Ein Penetrationstest sucht möglichst viele Schwachstellen in einem abgegrenzten Bereich. Eine Red-Team-Übung simuliert einen zielgerichteten Angriff und prüft, ob und wie schnell die Organisation ihn erkennt und darauf reagiert. Sie testet also auch Rufbereitschaft, Eskalation und Krisenstab. Beides braucht eine schriftliche Beauftragung mit Regeln, Ausschlüssen und Ansprechpartnern.

Was ist, wenn Microsoft 365 selbst ausfällt?

Dann fallen E-Mail, Teams, Intranet auf SharePoint und gegebenenfalls die Teams-Telefonie der Verwaltung aus, das KIS und die Klinik-TK aber nicht zwingend. Das ist ein gutes Planspiel-Szenario für sich: Es zeigt, wie viel Organisation inzwischen über Teams läuft und welche Notfallpläne nur noch digital existieren. Patientendaten gehören auch deshalb ins KIS und nicht in Excel-Listen in Teams, wie der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt erläutert.

Gehört die Notfallübung ins Qualitätsmanagement?

Ja. Übungsplan, Protokolle, Maßnahmenlisten und die daraus geänderten Verfahrensanweisungen sind Nachweise, die in einem Zertifizierungsaudit nach KTQ oder ISO 9001 und in Prüfungen der Informationssicherheit gefragt sein können. Sie gehören gelenkt abgelegt, mit Freigabe und Prüfdatum.

Wer sollte moderieren, intern oder extern?

Eine externe Moderation kann unbequeme Fragen stellen, ohne in der Hierarchie des Hauses zu stehen, und bringt Erfahrung aus anderen Umgebungen mit. Eine interne Begleitung kennt Abläufe und Menschen. Für die erste Übung hat sich die Kombination bewährt, für Wiederholungen kann ein geschultes internes Team die Moderation übernehmen.

Fazit: Üben, solange es nur ein Spiel ist

Eine Notfallübung für die IT im Krankenhaus ist unbequem, und genau darin liegt ihr Wert. Sie zeigt, dass der Notfallplan auf dem verschlüsselten Server liegt, dass die Formulare auf Station seit Jahren niemand angefasst hat, dass die Leitstelle eine Nummer hat, die nur im Intranet steht, und dass niemand genau weiß, wer nachts den Stecker ziehen darf. Jede dieser Erkenntnisse ist im Planspiel billig und im Ernstfall teuer.

Fangen Sie mit einem Planspiel an, mit allen Rollen am Tisch und einem Szenario, das zum Haus passt. Machen Sie aus jedem Befund eine Maßnahme mit Verantwortung und Termin, übertragen Sie die Ergebnisse in Verfahrensanweisungen und Notfallordner, und üben Sie im nächsten Jahr wieder, mit neuem Szenario. Die Krankenhaus-IT hat schon so manchen Montag überstanden. Mit Übung übersteht sie auch den, an dem die Erpresserbriefe aus dem Drucker kommen, und die Station merkt davon vor allem, dass der Kugelschreiber bereitlag.

WEITERLESEN · Weiterlesen

› Ransomware im Krankenhaus: Der Weg über Konten und Microsoft 365 und was wirklich hilft
› Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet
› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten
› Teams-Telefonie als Unteranlage im Krankenhaus: Verwaltung und Ärzte an Teams, Station und Patienten an der Klinik-TK
› Hygieneplan, Pflegestandards, Notfallpläne: Was auf Station in zehn Sekunden auffindbar sein muss
› Microsoft 365 Beratung für Krankenhäuser

› Microsoft 365 Schulung für Krankenhäuser