Ransomware im Krankenhaus: Der Weg über Konten und Microsoft 365 und was wirklich hilft



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

BERATUNG
Sicherheitsüberprüfung von Tenant, Active Directory und Dienstleisterzugängen, mit priorisiertem Maßnahmenplan.
› **Beratung für Krankenhäuser**

SCHULUNG
Für IT-Administratoren: privilegierte Konten, bedingter Zugriff und Defender im Klinikbetrieb sicher betreiben.
› **Schulungen für Krankenhäuser**

Es gibt Montage, an denen die Klinik-IT schon beim ersten Kaffee merkt, dass etwas nicht stimmt. Die Dateiablage zeigt Dateien mit seltsamen Endungen, der Druckserver druckt Erpresserbriefe, und auf der Station fragt jemand, warum das KIS so langsam ist. Es ist nicht langsam. Es ist weg. Ab diesem Moment läuft eine Uhr, die mit Patienten, Notaufnahme und Versorgungsauftrag zu tun hat, und die Geschäftsführung stellt Fragen, auf die niemand eine angenehme Antwort hat.

Die gute Nachricht in einem schlechten Thema: Die allermeisten Angriffe mit Ransomware im Krankenhaus beginnen nicht mit einem genialen Hack, sondern mit einem Konto. Ein Kennwort, das per Phishing abgegriffen oder per Passwort-Spray erraten wurde. Ein Fernwartungszugang eines Dienstleisters, der seit Jahren mit derselben Kennung offensteht. Ein Domänen-Administrator, der sich bequem am Stationsrechner angemeldet hat. Wer diese Wege kennt, kann sie verbauen, und zwar meist mit Werkzeugen, die das Haus über Microsoft 365 und Windows Server längst besitzt.

Dieser Beitrag beschreibt, warum Krankenhäuser ein bevorzugtes Ziel sind, wie die Angriffskette über Konten und Microsoft 365 typischerweise verläuft und welche Maßnahmen wirklich helfen, sortiert nach Wirkung und nicht nach Hochglanzfaktor. Er gehört zur Serie Microsoft 365 im Krankenhaus. Deren Grundhaltung gilt auch hier: Patientendaten gehören ins KIS und seine Subsysteme. Microsoft 365 ist Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit, und gerade deshalb ein Einfallstor, das man ernst nehmen muss.

FAKTEN · Das Wichtigste in Kürze

Der häufigste Einstieg ist ein übernommenes Konto oder ein schlecht geschützter Fernzugang, nicht eine exotische Schwachstelle.

Die wirksamsten Maßnahmen in absteigender Reihenfolge: MFA für alle externen Zugänge, Schutz privilegierter Konten mit Tiering, Abschalten der Legacy-Anmeldung, zeitlich begrenzte Dienstleisterzugänge, Defender im lizenzierten Umfang, Sicherung offline und getestet, Segmentierung der Medizintechnik.

Bedingter Zugriff setzt Microsoft Entra ID P1 voraus, das laut Microsoft in Microsoft 365 E3 und E5 enthalten ist. Defender for Identity, das Angriffe im Active Directory erkennt, ist nicht Teil von Microsoft 365 E3.

Rechtlicher Rahmen: § 391 SGB V verlangt Vorkehrungen nach dem Stand der Technik, für Betreiber kritischer Anlagen gelten stattdessen die Pflichten des BSIG. Der B3S „Medizinische Versorgung“ der DKG liegt in Version 1.3.1 vor.

KOMPETENZBEREICH · Microsoft 365 Security bei boddenberg.de

Bedingter Zugriff, Schutz privilegierter Rollen, Defender und die Härtung hybrider Umgebungen sind im Kompetenzbereich Microsoft 365 Security ausführlich beschrieben, unabhängig von der Branche.

Warum Krankenhäuser ein bevorzugtes Ziel sind

Kriminelle Gruppen, die mit Ransomware arbeiten, sind Unternehmer mit schlechter Moral und guter Buchhaltung. Sie suchen Ziele, bei denen der Druck zur Zahlung hoch und der Schutz niedrig ist. Krankenhäuser erfüllen beide Kriterien leider zuverlässiger als die meisten anderen Branchen. Das hat nichts mit schlechter Arbeit der Klinik-IT zu tun, sondern mit drei strukturellen Eigenschaften.

Der Versorgungsauftrag als Druckmittel

Ein Maschinenbauer kann im Ernstfall die Produktion anhalten und eine Woche lang Kunden vertrösten. Ein Krankenhaus kann das nicht. Die Notaufnahme muss sich womöglich von der Notfallversorgung abmelden, geplante Eingriffe werden verschoben, Befunde aus Labor und Radiologie kommen per Bote statt per Schnittstelle. Jede Stunde ohne KIS und Subsysteme kostet nicht nur Geld, sondern bindet Ärzte und Pflegekräfte in Papierprozessen, die im Alltag niemand mehr übt. Genau diesen Druck kalkulieren Angreifer ein.

Dazu kommt die Erpressung mit Daten. Moderne Gruppen verschlüsseln nicht nur, sie kopieren vorher. Wer dann nicht zahlt, findet Teile seiner Daten auf einer Veröffentlichungsseite wieder. Bei Patientendaten ist das für ein Haus ein Reputationsschaden, für die betroffenen Patienten aber vor allem ein Eingriff in ihre Privatsphäre, der sich nicht rückgängig machen lässt.

Eine heterogene Altlandschaft

Kaum eine Branche betreibt so viele Fachanwendungen nebeneinander wie ein Krankenhaus: KIS, LIS, RIS, PACS, Dienstplanung, Küche, Apotheke, CAFM für die Medizintechnik, dazu Geräte mit eingebetteten Betriebssystemen, deren Hersteller Updates nur nach eigener Freigabe erlauben. Ein Teil dieser Anwendungen spricht noch NTLM statt Kerberos, braucht ein Dienstkonto mit Domänen-Administratorrechten oder läuft auf einem Betriebssystem, das schon lange keine Sicherheitsupdates mehr bekommt. Nicht aus Schlamperei, sondern weil eine Zulassung, ein Vertrag oder ein Hersteller daran hängt.

In Klinikverbünden kommt die Geschichte hinzu: Häuser wurden übernommen, Domänen durch Vertrauensstellungen verbunden, und die Altdomäne des vor fünfzehn Jahren eingegliederten Standorts existiert noch, weil dort ein einziges Subsystem hängt. Für Angreifer ist das ein Abenteuerspielplatz. Mehr dazu im Beitrag Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung.

Dienstleisterzugänge und Rufbereitschaft

Hersteller von Medizintechnik, KIS-Anbieter, Dienstleister für Netzwerk und Gebäudetechnik: Alle brauchen Fernzugriff, viele dauerhaft. In der Praxis finden sich VPN-Zugänge mit geteilten Kennungen, Fernwartungswerkzeuge, die auf Servern dauerhaft lauschen, und Konten von Technikern, die das Unternehmen längst verlassen haben. Gleichzeitig muss die eigene IT nachts und am Wochenende in Rufbereitschaft von zu Hause zugreifen können. Jeder dieser Zugänge ist ein Weg ins Haus, und nicht jeder ist so gut bewacht wie die Pforte.

Eigenschaft	Warum sie Angreifern hilft	Was daraus folgt
Versorgungsauftrag	Hoher Zahlungsdruck, weil Stillstand Patienten betrifft	Wiederherstellung muss geplant und geübt sein, nicht improvisiert
Viele Subsysteme	Große Angriffsfläche, uneinheitlicher Patchstand	Inventar und Segmentierung statt Einzelfallentscheidungen
Altanwendungen und Medizintechnik	NTLM, alte Betriebssysteme, Dienstkonten mit zu vielen Rechten	Kerberos, getrennte Netze, Rechte der Dienstkonten prüfen
Klinikverbund	Vertrauensstellungen und Altdomänen verbinden Schwachstellen	Domänen konsolidieren, Vertrauensstellungen einschränken
Dienstleisterzugänge	Dauerhaft offen, oft geteilt, selten überwacht	Zugang auf Zeit, eigenes Konto pro Person, MFA, Protokoll
Schichtdienst und Stationsrechner	Gemeinsam genutzte Anmeldungen, Druck zur Bequemlichkeit	Schnelle, aber persönliche Anmeldung statt Sammelkonto

Zur Abgrenzung: Arztpraxen, Pflegeheime und Krankenkassen haben ähnliche Probleme, aber andere Strukturen und andere Rechtsgrundlagen. Dieser Beitrag richtet sich an Akutkrankenhäuser aller Trägerschaften, Klinikverbünde, Fach- und Rehakliniken sowie Universitätsklinika.

HINWEIS · Rechtsrahmen, kurz und ohne Rechtsberatung

§ 391 SGB V verpflichtet Krankenhäuser zu angemessenen organisatorischen und technischen Vorkehrungen nach dem Stand der Technik, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu vermeiden. Dazu gehören ausdrücklich Maßnahmen zur Sensibilisierung der Belegschaft. Die Vorschrift gilt seit dem NIS2-Umsetzungsgesetz vom 6. Dezember 2025 in neuer Fassung. Für Betreiber kritischer Anlagen gelten stattdessen die Pflichten des BSIG.

Den Stand der Technik kann ein Haus insbesondere über einen branchenspezifischen Sicherheitsstandard nachweisen, dessen Eignung das BSI festgestellt hat. Für Krankenhäuser ist das der B3S „Medizinische Versorgung“ der DKG, aktuell in Version 1.3.1 vom 10. Oktober 2025.

Ob Ihr Haus zusätzlich als wichtige oder besonders wichtige Einrichtung im Sinne des BSIG gilt, hängt unter anderem von Größe und Umsatz ab. Das klären Sie mit Ihrer Rechtsabteilung oder externer Rechtsberatung, nicht mit diesem Artikel.

Was das konkret für Microsoft 365 bedeutet, beschreibt der Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten.

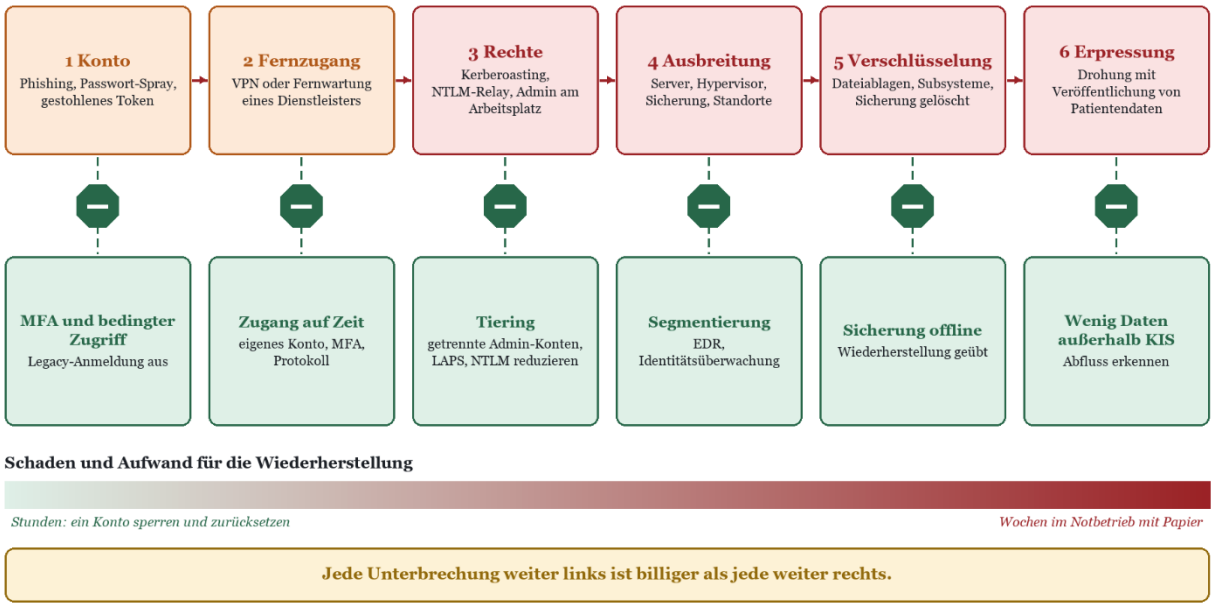
Die Angriffskette: vom Konto zur Erpressung

Kein Angriff gleicht dem anderen im Detail, aber die meisten folgen einem Muster, das sich in sechs Schritte zerlegen lässt. Die Skizze zeigt die Kette und darunter die Stellen, an denen sie sich unterbrechen lässt. Je weiter links die Unterbrechung greift, desto billiger wird der Vorfall. Ein

gesperrtes Konto am Montagmorgen ist ärgerlich. Ein verschlüsseltes Rechenzentrum ist ein Ereignis, über das man noch auf der übernächsten Weihnachtsfeier spricht.

Skizze 1: Die Angriffskette und ihre Unterbrechungspunkte

Oben der Weg des Angreifers, unten die Stelle, an der Sie ihn aufhalten.



Schematische Darstellung eines typischen Ablaufs, kein bestimmter Vorfall.

Schritt 1: Ein Konto wird übernommen

Der Klassiker ist die Phishing-Mail, die täuschend echt aussieht: eine angebliche Freigabe aus SharePoint, eine Sprachnachricht aus Teams, eine Rechnung eines bekannten Lieferanten. Moderne Varianten fangen nicht nur das Kennwort ab, sondern über einen vorgeschalteten Proxy gleich das Sitzungstoken, und umgehen damit klassische MFA per SMS oder Anruf. Daneben steht das Passwort-Spray: Angreifer probieren wenige gängige Kennwörter gegen sehr viele Konten. Gerade in Krankenhäusern mit Kennwortregeln aus dem letzten Jahrzehnt und vielen selten genutzten Konten ist die Trefferquote unangenehm hoch.

Besonders beliebt sind Konten, die niemand vermisst: das Funktionskonto für den Scanner, das Schulungskonto aus der KIS-Einführung, das Konto der Hospitantin aus dem Jahr 2019, das nie deaktiviert wurde. Was sich in solchen Tenants nach Jahren ansammelt, beschreibt der Beitrag Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet.

Schritt 2: Der Fernzugang eines Dienstleisters

Der zweite große Einstieg führt nicht über Microsoft 365, sondern an ihm vorbei: über VPN-Zugänge und Fernwartungslösungen. Ist ein solcher Zugang nur mit Kennwort geschützt, reicht ein abgegriffenes Kennwort beim Dienstleister. Ist er dauerhaft offen und wird nicht protokolliert, bemerkt niemand, dass sich der „Techniker“ an einem Sonntag um drei Uhr nachts anmeldet. Häufig landen diese Zugänge direkt in einem Servernetz, weil die Medizintechnik oder das Subsystem dort steht.

Schritt 3: Rechteausweitung im Active Directory

Mit einem normalen Benutzerkonto kann ein Angreifer im Active Directory erstaunlich viel lesen: Gruppen, Dienstkonten, Vertrauensstellungen. Von dort aus führen bekannte Wege zu höheren Rechten. Kerberoasting greift Dienstkonten mit schwachen Kennwörtern an. NTLM-Relay nutzt Anmeldungen, die noch über NTLM laufen. Am einfachsten wird es, wenn ein Konto mit Domänen-Administratorrechten sich irgendwann an einem gewöhnlichen Arbeitsplatz angemeldet

hat. Dann liegen dort Anmeldedaten im Speicher, die sich mit frei verfügbaren Werkzeugen auslesen lassen.

Fehlkonfigurierte Zertifikatvorlagen einer internen PKI sind ein weiterer, oft übersehener Weg zu Domänen-Administratorrechten. Wer eine eigene Zertifizierungsstelle betreibt, sollte deren Vorlagen regelmäßig prüfen. Grundlagen dazu im Kompetenzbereich PKI mit ADCS.

Schritt 4: Ausbreitung

Mit hohen Rechten verteilt sich der Angreifer im Netz. Ziel sind die Systeme, die bei der Wiederherstellung helfen würden: die Verwaltung des Hypervisors, der Sicherungsserver, die Domänencontroller aller Standorte. In flachen Netzen, in denen der Arbeitsplatz in der Verwaltung den Sicherungsserver direkt erreicht, geht das beunruhigend schnell. Oft vergehen dabei Tage oder Wochen, in denen nichts auffällt, weil niemand die Anmeldeprotokolle auswertet.

Schritt 5: Verschlüsselung

Die eigentliche Verschlüsselung ist der lauteste und kürzeste Teil. Meist geschieht sie nachts oder am Wochenende, wenn die Rufbereitschaft dünn besetzt ist. Vorher werden Sicherungen gelöscht oder unbrauchbar gemacht und Schattenkopien entfernt. Microsoft 365 selbst ist dabei selten das Hauptziel, aber synchronisierte Ordner auf verschlüsselten Arbeitsplätzen können verschlüsselte Dateien in OneDrive und SharePoint schreiben. Die Versionierung hilft hier, eine Sicherung ersetzt sie nicht.

Schritt 6: Erpressung mit Patientendaten

Zum Schluss kommt die Forderung, verbunden mit der Drohung, kopierte Daten zu veröffentlichen. Hier rächt sich, was in vielen Häusern niemand gern ausspricht: die Excel-Liste mit Patientennamen im Teams-Kanal der Station, der OP-Plan als PDF im Postfach, die Belegungsübersicht auf dem Dateiserver. Solche Listen sind nicht der Normalfall und sollten es nie werden, aber es gibt sie. Je weniger Patientendaten außerhalb von KIS und Subsystemen liegen, desto weniger lässt sich damit erpressen. Wo die Grenze verläuft, beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt.

AUS DER PRAXIS · Aus der Forensik

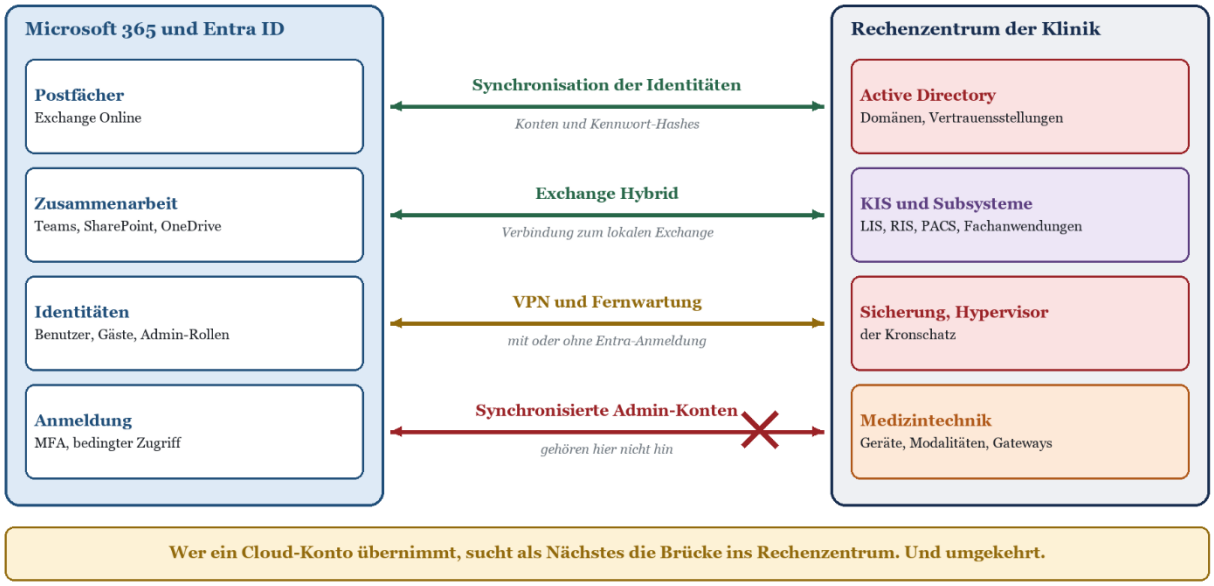
In einer forensischen Untersuchung bei einem Krankenhausverbund mit mehreren Standorten war nicht die Frage „Wie sind sie hereingekommen?“ die schwierigste, sondern „Seit wann sind sie da, und welche Konten kennen sie?“. Die Antwort hängt fast vollständig davon ab, welche Anmelde- und Ereignisprotokolle es gibt, wie lange sie aufbewahrt werden und ob sie außerhalb der betroffenen Domäne liegen. Wer Protokolle erst nach dem Vorfall einschaltet, protokolliert nur noch die eigenen Aufräumarbeiten.

Microsoft 365 als Brücke ins Rechenzentrum

Kaum ein Krankenhaus betreibt Microsoft 365 isoliert. Identitäten werden aus dem Active Directory synchronisiert, Exchange läuft hybrid, der VPN-Zugang nutzt vielleicht schon die Anmeldung über Entra ID. Das ist sinnvoll und bequem, bedeutet aber: Jede Verbindung zwischen Cloud und Rechenzentrum trägt in beide Richtungen. Wer im lokalen AD Domänen-Administrator wird, kann über synchronisierte Konten oft auch in der Cloud Schaden anrichten. Und wer ein synchronisiertes Konto mit Admin-Rolle in Entra ID übernimmt, hat womöglich gleichzeitig weitreichende Rechte im lokalen Netz.

Skizze 2: Die Brücken zwischen Microsoft 365 und dem Rechenzentrum

Jede Brücke trägt in beide Richtungen, auch den Angreifer.



Vereinfachte Darstellung einer hybriden Klinikumgebung.

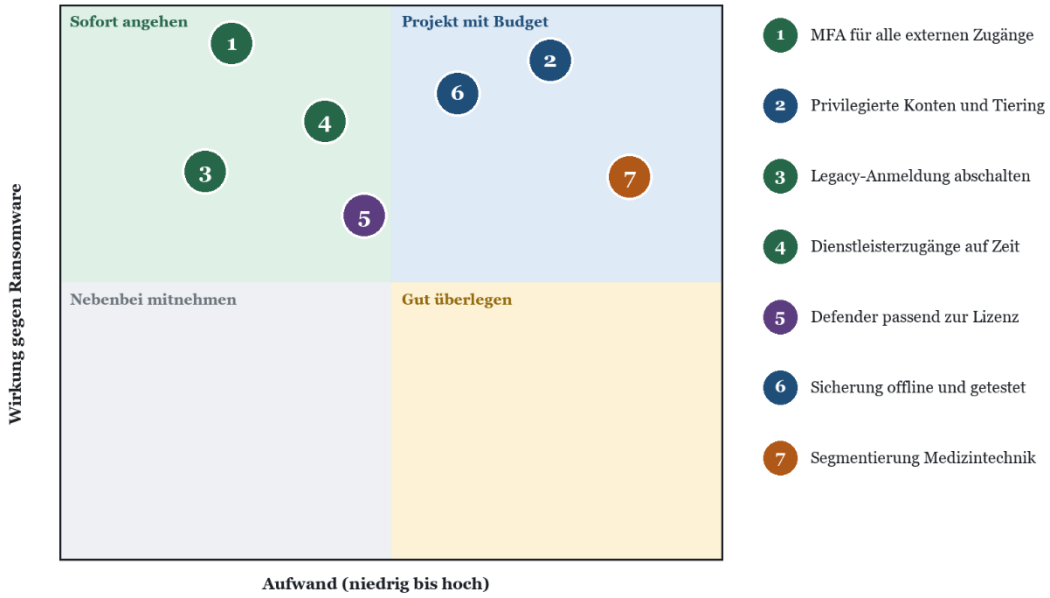
Die wichtigste Konsequenz daraus ist schlicht: Administratorrollen in Microsoft 365 gehören zu reinen Cloud-Konten, die nicht aus dem lokalen AD synchronisiert werden. Und der Server, auf dem die Identitätssynchronisation läuft, ist genauso schützenswert wie ein Domänencontroller. Wie sich ein Tenant im Klinikverbund insgesamt aufstellen lässt, beschreibt der Beitrag Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen.

Maßnahmen nach Wirkung sortiert

Sicherheitskataloge haben die Eigenschaft, alles gleich wichtig erscheinen zu lassen. Die folgende Liste tut das bewusst nicht. Sie ordnet sieben Maßnahmen nach ihrer Wirkung gegen die oben beschriebene Kette. Die Skizze ergänzt den Aufwand, damit Sie sehen, was sich in Wochen und was sich nur in Projekten umsetzen lässt.

Skizze 3: Sieben Maßnahmen nach Wirkung und Aufwand

Grobe Einordnung aus Projekterfahrung, keine Messung. Ihr Haus kann abweichen.



Die Reihenfolge im Text folgt der Wirkung, nicht der Bequemlichkeit.

1. MFA für alle externen Zugänge

Mehrstufige Anmeldung ist die Maßnahme mit dem besten Verhältnis von Wirkung zu Aufwand, und zwar für alle Zugänge von außen: Microsoft 365, VPN, Fernwartung, Citrix-Zugang für die Rufbereitschaft, Webzugänge zu Fachanwendungen. Ein abgegriffenes Kennwort allein reicht dann nicht mehr. In Microsoft 365 setzen Sie das mit Richtlinien für den bedingten Zugriff um. Das setzt Microsoft Entra ID P1 voraus, das laut Microsoft unter anderem in Microsoft 365 E3 und E5 enthalten ist. Wo diese Lizenz fehlt, sind die Sicherheitsstandards von Entra ID die Mindestlösung.

Für Administratoren reicht eine Bestätigung per App auf Dauer nicht. Hier sind phishingresistente Verfahren angebracht, also FIDO2-Sicherheitsschlüssel, Passkeys oder zertifikatbasierte Anmeldung. Sie schützen auch gegen die Proxy-Angriffe, die Sitzungstoken abfangen. Microsoft erzwingt inzwischen ohnehin MFA für die Anmeldung an den eigenen Verwaltungsportalen, etwa dem Azure-Portal und dem Microsoft Entra Admin Center. Darauf sollten Sie sich nicht ausruhen, sondern es als Untergrenze verstehen.

WARNUNG · Die Station ist kein Grund für Ausnahmen ohne Ende

Am Stationsrechner im Schichtdienst ist MFA bei jeder Anmeldung unpraktisch. Das ist ein legitimer Grund für eine durchdachte Lösung, etwa Anmeldung mit Karte, vertrauenswürdige Geräte oder Netze als Bedingung. Es ist kein Grund, ganze Benutzergruppen dauerhaft von MFA auszunehmen. Ausnahmen gehören dokumentiert, begrenzt und regelmäßig überprüft.

Wie die Anmeldung am Stationsarbeitsplatz schnell und trotzdem persönlich bleibt, beschreibt der Beitrag Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel.

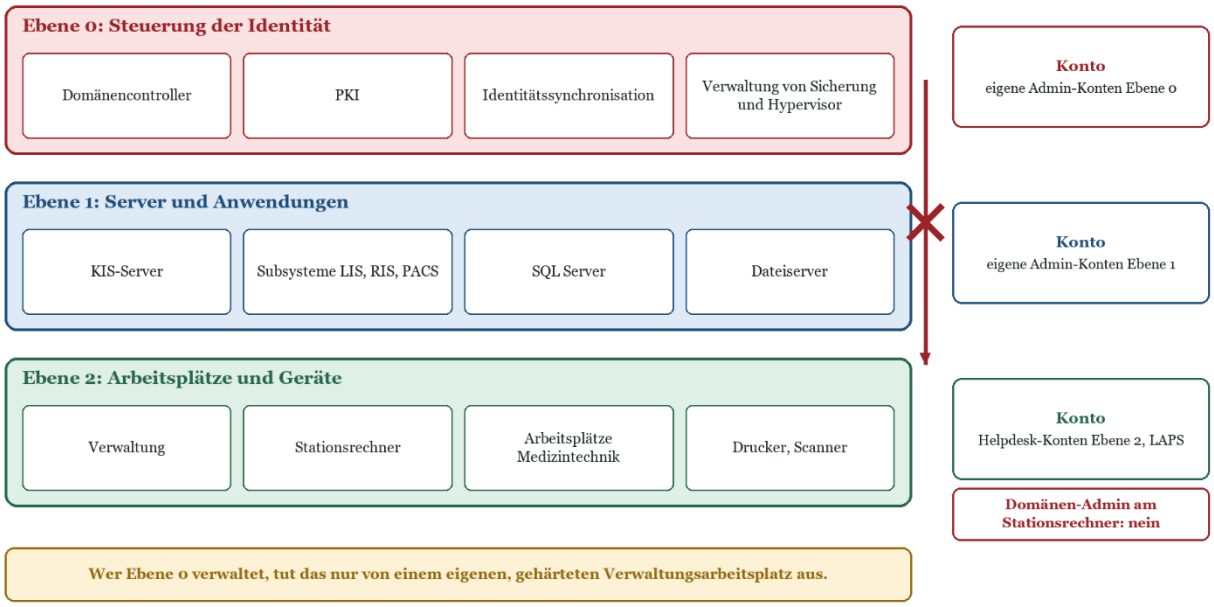
2. Privilegierte Konten schützen und Tiering einführen

Die Rechteausweitung im Active Directory ist der Schritt, an dem aus einem ärgerlichen Vorfall eine Katastrophe wird. Das Ebenenmodell, im Alltag Tiering genannt, setzt genau dort an. Es trennt die Steuerung der Identität (Ebene 0: Domänencontroller, PKI, Identitätssynchronisation, Verwaltung von Sicherung und Hypervisor) von Servern und Anwendungen (Ebene 1) und von

Arbeitsplätzen und Geräten (Ebene 2). Für jede Ebene gibt es eigene Administratorkonten, und kein Konto meldet sich auf einer niedrigeren Ebene an.

Skizze 4: Tiering im Klinikumfeld

Ein Konto, eine Ebene. Höherwertige Konten melden sich nie auf niedrigeren Ebenen an.



Vereinfachte Darstellung nach dem Ebenenmodell für privilegierten Zugriff.

- **Getrennte Konten:** Jeder Administrator hat ein normales Konto für Mail und Teams und je ein eigenes Konto pro Ebene, die er verwaltet. Ja, das sind mehrere Kennwörter. Nein, das ist kein Grund, es zu lassen.
- **Eigene Verwaltungsarbeitsplätze:** Ebene 0 wird nur von gehärteten Rechnern aus verwaltet, auf denen niemand Mails liest oder im Internet surft.
- **Lokale Administratorkennwörter:** Windows LAPS sorgt dafür, dass jedes Gerät ein eigenes, regelmäßig wechselndes lokales Administratorkennwort hat. Ein einziges Kennwort für alle Stationsrechner ist für Angreifer ein Generalschlüssel.
- **Schutzgruppen und Dienstkonten:** Hochprivilegierte Konten gehören in die Gruppe Protected Users, Dienstkonten mit Domänen-Administratorrechten werden auf das Notwendige zurückgeschnitten oder durch gruppenverwaltete Dienstkonten ersetzt.
- **Cloud-Rollen:** Admin-Rollen in Entra ID nur für reine Cloud-Konten, möglichst nicht dauerhaft zugewiesen. Die zeitlich begrenzte Aktivierung über Privileged Identity Management setzt Entra ID P2 voraus, das laut Microsoft in Microsoft 365 E5 enthalten ist.
- **Notfallzugang:** Mindestens zwei Notfallkonten für den Tenant, die vom bedingten Zugriff ausgenommen, aber streng überwacht sind. Sonst sperren Sie sich bei einer falsch konfigurierten Richtlinie selbst aus.

In Klinikverbünden gehört zum Tiering auch ein kritischer Blick auf Vertrauensstellungen. Eine Vertrauensstellung zu einer Altdomäne mit schwacher Pflege ist eine Hintertür in die Ebene 0. Aus der langjährigen Begleitung eines Verbunds mit mehreren Standorten lässt sich sagen: Die Konsolidierung dauert, aber jede abgebaute Vertrauensstellung ist ein Angriffsweg weniger. Kerberos statt NTLM gehört in dasselbe Paket, Grundlagen dazu im Kompetenzbereich Kerberos.

3. Legacy-Authentifizierung abschalten

Alte Anmeldeverfahren kennen keine MFA. Ein Konto, das noch per Basisauthentifizierung erreichbar ist, ist für Passwort-Spray ein offenes Scheunentor. In Exchange Online hat Microsoft die Basisauthentifizierung für die meisten Protokolle abgeschaltet, darunter Exchange ActiveSync,

POP, IMAP, Remote PowerShell und EWS. Für SMTP AUTH, das gern von Multifunktionsgeräten, Scannern und Fachanwendungen zum Mailversand genutzt wird, hat Microsoft die Abschaltung angekündigt und den Zeitplan mehrfach angepasst. Den aktuellen Stand prüfen Sie im Message Center Ihres Tenants.

Unabhängig davon blockieren Sie Legacy-Authentifizierung mit einer Richtlinie für den bedingten Zugriff. Vorher lohnt ein Blick in die Anmeldeprotokolle von Entra ID, welche Geräte und Anwendungen noch alte Verfahren nutzen. Im Krankenhaus ist die Liste meist länger als erwartet, und mindestens ein Eintrag gehört zu einem Gerät, von dem niemand mehr weiß, wo es steht.

Im lokalen Netz ist das Gegenstück NTLM. Microsoft hat NTLMv1 aus Windows 11 Version 24H2 und Windows Server 2025 entfernt und alle NTLM-Versionen als veraltet eingestuft. Wie man NTLM im Krankenhaus schrittweise zurückdrängt, ohne dass die Medizintechnik stehen bleibt, beschreibt der Beitrag NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos.

4. Dienstleisterzugänge zeitlich begrenzen und überwachen

Fernwartung ist im Krankenhaus unverzichtbar, ein dauerhaft offener Zugang ist es nicht. Bewährt hat sich ein einfaches Prinzip: Der Zugang ist standardmäßig geschlossen und wird für einen konkreten Auftrag für ein festes Zeitfenster geöffnet. Jede Person beim Dienstleister hat ein eigenes Konto, nicht ein Konto pro Firma. Die Anmeldung erfolgt mit MFA. Der Zugang führt nur zu den Systemen, die der Auftrag betrifft, und die Sitzung wird protokolliert.

Prüffrage	Gute Antwort	Schlechte Antwort
Wer hat Zugang?	Benannte Personen mit eigenem Konto	„Die Firma“ mit einer gemeinsamen Kennung
Wann ist er offen?	Pro Auftrag, mit Ablaufzeit	Immer, seit der Inbetriebnahme
Wie wird angemeldet?	MFA, möglichst über Entra ID oder eigenes Gateway	Kennwort, das seit Jahren gleich ist
Wohin führt er?	Nur zu den betroffenen Systemen	In das gesamte Servernetz
Wer sieht zu?	Protokoll, Alarm bei Anmeldung außerhalb des Fensters	Niemand, bis zur nächsten Rechnung
Wer räumt auf?	Regelmäßige Überprüfung, Ablauf bei Vertragsende	Niemand, das Konto lebt ewig

Externe Personen, die in Microsoft 365 arbeiten, kommen als Gäste in den Tenant und unterliegen dort denselben Richtlinien für den bedingten Zugriff. Zugriffsüberprüfungen helfen, Gastkonten nach Projektende wieder loszuwerden. Wie viele vergessene Gäste und Dienstleisterkonten sich typischerweise finden, zeigt wiederum der Beitrag Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet.

5. Defender im lizenzierten Umfang nutzen

Viele Häuser besitzen mehr Defender, als sie einsetzen, und manche glauben, mehr zu besitzen, als sie lizenziert haben. Beides ist ungünstig. Die folgende Übersicht beruht auf der Servicebeschreibung von Microsoft zum Zeitpunkt dieses Beitrags. Lizenzpakete ändern sich, prüfen Sie den Stand daher vor jeder Entscheidung.

Lizenz	Defender-Bausteine laut Microsoft	Was das im Krankenhaus bedeutet
Microsoft 365 E3	Defender for Endpoint Plan 1, Entra ID P1 für bedingten Zugriff	Gute Basis für Virenschutz und Regeln zur Reduzierung der Angriffsfläche. Keine Erkennung und Reaktion auf Endpunkten (EDR), keine Identitätsüberwachung im AD.

Microsoft 365 E5	Defender for Endpoint Plan 2, Defender for Office 365 Plan 2, Defender for Identity, Defender for Cloud Apps, Entra ID P2	EDR, automatisierte Untersuchung, Erkennung von Angriffen auf das Active Directory, zeitlich begrenzte Admin-Rollen.
Microsoft 365 E3 mit Microsoft Defender Suite	Defender for Endpoint Plan 2, Defender for Office 365 Plan 2, Defender for Identity, Defender for Cloud Apps	Sicherheitsumfang ähnlich E5 ohne kompletten Wechsel. Ob Entra ID P2 enthalten ist, vor dem Kauf prüfen.
Microsoft 365 Business Premium	Defender for Business, Defender for Office 365 Plan 1	Für Organisationen bis 300 Benutzer gedacht und damit für die meisten Krankenhäuser keine Option.
Server	Nicht in den Benutzerlizenzen für Defender for Endpoint enthalten	Für Server braucht es eigene Lizenzen, etwa Defender for Servers oder Defender for Endpoint for Servers. Gerade KIS- und Subsystemserver fallen sonst durchs Raster.

Für den Schutz gegen Ransomware sind zwei Bausteine besonders wertvoll: EDR auf Clients und Servern, weil es die Ausbreitung sichtbar macht, und Defender for Identity, weil es Kerberoasting, verdächtige Replikationsanfragen und seitliche Bewegungen im Active Directory meldet. Wenn das Budget nur für eines reicht, entscheidet Ihre Ausgangslage. Und welche Lizenzen für Pflege und Verwaltung überhaupt sinnvoll sind, beschreibt der Beitrag Lizenzen im Krankenhaus: Frontline für die Pflege, Vollausstattung für die Verwaltung.

WICHTIG · Defender ohne Betrieb ist Dekoration

Ein Alarm, den niemand liest, schützt nicht. Klären Sie vor der Einführung, wer die Meldungen werktags, nachts und am Wochenende sichtet, ob das die eigene IT in Rufbereitschaft oder ein externer Dienstleister übernimmt und welche Maßnahmen automatisch greifen dürfen, etwa das Isolieren eines Geräts. Bei Geräten der Medizintechnik muss die Antwort mit der Medizintechnik abgestimmt sein.

6. Datensicherung offline und getestet

Am Ende entscheidet die Sicherung darüber, ob ein Haus Tage oder Monate im Notbetrieb verbringt. Angreifer wissen das und greifen gezielt den Sicherungsserver an. Daraus folgen drei Anforderungen. Erstens: Mindestens eine Kopie liegt so, dass sie mit den Rechten aus der Domäne nicht gelöscht oder verändert werden kann, also offline oder unveränderlich gespeichert. Zweitens: Die Sicherungsinfrastruktur hängt nicht an derselben Domäne, deren Administratoren gerade kompromittiert sind. Drittens: Die Wiederherstellung wird geübt, und zwar nicht nur für eine einzelne Datei, sondern für Domänencontroller, KIS-Datenbank und ein Subsystem im Zusammenspiel mit dem Hersteller.

Für Microsoft 365 gilt ergänzend: Versionierung, Papierkorb und Aufbewahrungsrichtlinien helfen bei vielen Schäden, sind aber keine unabhängige Sicherung. Ob Sie für Exchange Online, SharePoint und OneDrive eine zusätzliche Sicherung brauchen, hängt davon ab, welche Daten dort liegen und wie schnell Sie sie im Ernstfall zurückbrauchen. Diese Entscheidung sollte bewusst fallen, nicht aus Gewohnheit.

TIPP · Die ehrlichste Kennzahl

Fragen Sie nicht „Haben wir eine Sicherung?“, sondern „Wann haben wir zuletzt einen Domänencontroller und das KIS aus der Sicherung in einer isolierten Umgebung wiederhergestellt, und wie lange hat es gedauert?“. Wenn die Antwort mit „Äh“ beginnt, haben Sie Ihre nächste Übung

gefunden.

7. Netzsegmentierung für Medizintechnik

Medizingeräte lassen sich oft nicht patchen, nicht mit Defender ausstatten und nicht ohne Zustimmung des Herstellers umkonfigurieren. Was sich fast immer tun lässt: sie in eigene Netzsegmente stellen, deren Verbindungen auf das Notwendige beschränkt sind. Das Ultraschallgerät muss das PACS erreichen, aber nicht das Internet und schon gar nicht den Arbeitsplatz in der Buchhaltung. Segmentierung ist die Maßnahme mit dem höchsten Aufwand in dieser Liste, weil sie ein vollständiges Inventar und viele Gespräche mit Medizintechnik, Herstellern und Stationen voraussetzt. Sie ist auch die Maßnahme, die eine Ausbreitung am wirksamsten bremst.

Ein pragmatischer Einstieg ist, mit den Systemen zu beginnen, deren Ausfall am meisten schmerzt, und für jedes Segment festzuhalten, welche Verbindungen erlaubt sind und wer sie verantwortet. Die Medizintechnik ist dabei Partner, nicht Bittsteller: Sie kennt die Geräte, die Herstellerverträge und die Einweisungen.

Die Übersicht: Angriffsschritt, Gegenmaßnahme, Aufwand, Lizenz

Die Tabelle fasst zusammen, welche Maßnahme welchen Schritt der Kette unterbricht. Der Aufwand ist eine grobe Einordnung für ein Haus mittlerer Größe, der Lizenzbedarf nennt die Mindestvoraussetzung laut Microsoft zum Zeitpunkt dieses Beitrags.

Angriffsschritt	Gegenmaßnahme	Aufwand	Lizenzbedarf
1 Konto übernommen	MFA für alle externen Zugänge, phishingresistent für Administratoren, bedingter Zugriff	niedrig bis mittel	Entra ID P1 (in Microsoft 365 E3 und E5)
1 Konto übernommen	Legacy-Authentifizierung blockieren, verwaiste Konten entfernen	niedrig	Entra ID P1 für die Richtlinie, sonst Sicherheitsstandards
2 Fernzugang Dienstleister	Zugang auf Zeit, eigenes Konto pro Person, MFA, Protokoll	mittel	abhängig vom VPN- oder Fernwartungsprodukt; mit Entra-Anmeldung Entra ID P1
3 Rechteausweitung	Tiering, getrennte Admin-Konten, Windows LAPS, Protected Users, NTLM reduzieren	hoch	keine zusätzliche Lizenz, Bordmittel von Windows Server
3 Rechteausweitung	Zeitlich begrenzte Cloud-Admin-Rollen	niedrig	Entra ID P2 (in Microsoft 365 E5)
3 und 4 Rechte und Ausbreitung	Erkennung im Active Directory	mittel	Defender for Identity (z. B. Microsoft 365 E5 oder Defender Suite)
4 Ausbreitung	EDR auf Clients und Servern	mittel	Defender for Endpoint Plan 2; Server separat lizenzieren
4 Ausbreitung	Segmentierung, insbesondere Medizintechnik	hoch	keine Microsoft-Lizenz, Netzinfrastruktur
5 Verschlüsselung	Sicherung offline oder unveränderlich, getrennte Verwaltung, geübte Wiederherstellung	mittel bis hoch	Sicherungsprodukt; keine Microsoft-365-Lizenz erforderlich
6 Erpressung	Patientendaten im KIS halten, Ausleitung erkennen	mittel	Bordmittel; erweiterte Erkennung je nach Purview- und Defender-Umfang

Wenn es trotzdem passiert: Organisation statt Heldentum

Keine Maßnahme verhindert jeden Angriff. Was einen Vorfall beherrschbar macht, ist Vorbereitung: Wer entscheidet, wer meldet, wer spricht mit wem, und wie arbeitet die Station, wenn das KIS nicht da ist. Im Krankenhaus ist das kein IT-Thema allein, sondern eines für Geschäftsführung, Ärztlichen Direktor, Pflegedirektion und Qualitätsmanagement.

Rollen im Ernstfall

Rolle	Aufgabe im Ernstfall	Vorher zu klären
Geschäftsführung	Entscheidet über Notbetrieb, Abmeldung von der Notfallversorgung, externe Hilfe und Kommunikation	Vertretung, Erreichbarkeit, Budgetfreigabe ohne Umweg
IT-Leitung	Eindämmung, Lagebild, Wiederherstellung	Notfallkonten, Offline-Dokumentation, Kontakte zu Dienstleistern
Informationssicherheitsbeauftragter	Bewertung, Meldungen nach BSIG soweit einschlägig, Dokumentation	Meldewege, Vorlagen, Zuständigkeit für die Meldung
Datenschutzbeauftragter	Bewertung der Datenschutzverletzung, Meldung an die zuständige Aufsicht	Welche Aufsicht zuständig ist, je nach Träger und Land
Ärztlicher Direktor und Pflegedirektion	Notbetrieb auf Station und in den Funktionsbereichen	Papierformulare, Ausfallkonzepte, Übung
Qualitätsmanagement	Verfahrensanweisungen für Notbetrieb verfügbar halten	Ausdruck oder Offline-Kopie des QM-Handbuchs für den Ernstfall
Medizintechnik	Bewertung der Geräte, Abstimmung mit Herstellern	Geräteinventar, Ansprechpartner der Hersteller

WARNUNG · Das Notfallhandbuch in SharePoint

Ein Notfallhandbuch, das ausschließlich in SharePoint oder auf dem Dateiserver liegt, ist im Ernstfall möglicherweise nicht erreichbar, etwa weil die Anmeldung über die verschlüsselte Domäne läuft. Halten Sie eine aktuelle Offline-Fassung bereit, mit Telefonnummern auf Papier. Das klingt altmodisch und ist genau deshalb richtig.

Meldepflichten und Zuständigkeiten

Ein Ransomware-Vorfall löst in der Regel mehrere Meldepflichten gleichzeitig aus: gegenüber dem BSI, soweit das Haus unter die Pflichten des BSIG fällt, und gegenüber der Datenschutzaufsicht, wenn personenbezogene Daten betroffen sind. Welche Aufsicht zuständig ist, hängt von Trägerschaft und Bundesland ab. Kommunale und private Häuser unterliegen der staatlichen Datenschutzaufsicht, kirchliche Häuser haben mit KDG oder DSG-EKD eigene Regelungen und Aufsichten. Die Landeskrankenhausgesetze und Landesdatenschutzgesetze enthalten zudem unterschiedliche Vorgaben, ein Bundesland ist hier nicht der Maßstab für alle anderen.

HINWEIS · Keine Rechtsberatung

Fristen, Inhalte und Empfänger von Meldungen ergeben sich aus BSIG, DSGVO, kirchlichem Datenschutzrecht und Landesrecht. Legen Sie die Meldewege vorab mit Ihrer Rechtsabteilung, dem

Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten fest und halten Sie sie offline verfügbar. Im Ernstfall ist keine Zeit, Paragrafen zu lesen.

Besonderheiten kirchlicher Häuser beschreibt der Beitrag Microsoft 365 im kirchlichen Krankenhaus: KDG, DSG-EKD und die MAV am Tisch.

Mitbestimmung bei Überwachungswerkzeugen

Anmeldeprotokolle, Defender-Alarme und Sitzungsaufzeichnungen bei Fernwartung sind technische Einrichtungen, die geeignet sind, Verhalten und Leistung der Mitarbeiterinnen und Mitarbeiter zu überwachen. Damit sind Betriebsrat, Personalrat oder Mitarbeitervertretung je nach Trägerschaft zu beteiligen. Das ist kein Hindernis, sondern eine Chance: Eine Vereinbarung, die klar regelt, dass Sicherheitsprotokolle der Abwehr von Angriffen dienen und nicht der Leistungskontrolle, schafft Vertrauen und beschleunigt die Einführung. Wie sich die Mitbestimmung je nach Träger unterscheidet, beschreibt der Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

Ein Fahrplan für die ersten 90 Tage

Zeitraum	Maßnahmen	Ergebnis
Woche 1 bis 2	Bestandsaufnahme: externe Zugänge, Admin-Konten, Legacy-Anmeldungen, Dienstleisterkonten, Lizenzstand	Liste mit Risiken und Verantwortlichen
Woche 3 bis 6	MFA für alle externen Zugänge, Legacy-Authentifizierung blockieren, Notfallkonten, Cloud-Admins als reine Cloud-Konten	Die häufigsten Einstiege sind verbaut
Woche 4 bis 8	Dienstleisterzugänge auf Zeit umstellen, verwaiste Konten entfernen, Windows LAPS	Weniger dauerhaft offene Türen
Woche 6 bis 12	Tiering-Konzept, getrennte Admin-Konten für Ebene 0, Test der Wiederherstellung, Defender-Betrieb klären	Grundlage für die Projekte der nächsten Monate
danach	Segmentierung der Medizintechnik, NTLM zurückdrängen, Vertrauensstellungen abbauen	Ausbreitung wird schwer

Wenn Sie diesen Weg nicht allein gehen möchten, finden Sie unter Microsoft 365 Beratung für Krankenhäuser eine Sicherheitsüberprüfung mit priorisiertem Maßnahmenplan. Für das Team, das die Maßnahmen danach im Alltag betreibt, gibt es passende Inhalte unter Microsoft 365 Schulung für Krankenhäuser. Wer die technischen Anforderungen aus NIS2 branchenübergreifend betrachten möchte, findet sie unter NIS2 technisch umsetzen mit Microsoft 365.

Häufige Fragen zu Ransomware im Krankenhaus

Ist Microsoft 365 selbst das Ziel von Ransomware?

Selten das Hauptziel, aber häufig der Einstieg. Übernommene Konten in Microsoft 365 dienen dazu, weitere Phishing-Mails aus einem echten Postfach zu verschicken, Daten abzugreifen und den Weg ins Rechenzentrum zu finden. Die Verschlüsselung trifft meist die lokalen Server. Synchronisierte Ordner können verschlüsselte Dateien allerdings auch in OneDrive und SharePoint tragen.

Reicht MFA per Authenticator-App aus?

Für die meisten Benutzer ist sie ein großer Fortschritt gegenüber reinem Kennwort. Für Administratoren und besonders exponierte Konten sollten Sie phishingresistente Verfahren wie

FIDO2-Schlüssel, Passkeys oder zertifikatbasierte Anmeldung einsetzen, weil sie auch gegen Angriffe helfen, die Sitzungstoken abfangen.

Brauchen wir Microsoft 365 E5, um sicher zu sein?

Nein. Die wirksamsten Maßnahmen dieses Beitrags, MFA, Tiering, Abschalten der Legacy-Anmeldung, Dienstleisterzugänge auf Zeit und eine getestete Offline-Sicherung, lassen sich mit Microsoft 365 E3 und Bordmitteln von Windows Server umsetzen. E5 oder ein Sicherheitszusatz bringt vor allem Erkennung: EDR, Identitätsüberwachung im Active Directory und zeitlich begrenzte Admin-Rollen. Das ist wertvoll, ersetzt aber keine Grundhygiene.

Was ist mit Stationsrechnern und Sammelkonten?

Sammelkonten sind für Angreifer attraktiv, weil niemand ihre Nutzung einer Person zuordnen kann und ihre Kennwörter selten wechseln. Ziel ist eine schnelle, persönliche Anmeldung, etwa mit Karte und schnellem Benutzerwechsel. Wo ein Sammelkonto vorübergehend bleibt, gehört es auf das Nötigste beschränkt, ohne Postfach und ohne Zugriff auf Microsoft 365 von außen.

Wie gehen wir mit Medizingeräten um, die nur NTLM können?

Erst inventarisieren, dann segmentieren, dann mit dem Hersteller über Kerberos sprechen. NTLM lässt sich über Überwachung und Ausnahmelisten schrittweise zurückdrängen, ohne Geräte auf einen Schlag lahmzulegen. Das Vorgehen beschreibt der Beitrag NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos.

Deckt das C5-Testat von Microsoft die Ransomware-Abwehr ab?

Nein, das ist eine andere Frage. Ein C5-Testat bewertet die Sicherheit des Cloud-Anbieters, nicht die Konfiguration Ihres Tenants und schon gar nicht Ihr lokales Active Directory. Welche Microsoft-Dienste von welchem Testat abgedeckt sind, prüfen Sie im Service Trust Portal von Microsoft. Hintergrund dazu im Beitrag § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen.

Sollen wir im Ernstfall zahlen?

Das ist eine Entscheidung der Geschäftsführung mit rechtlichen, ethischen und praktischen Aspekten, die dieser Beitrag nicht beantworten kann. Behörden raten grundsätzlich davon ab. Praktisch gilt: Eine Zahlung garantiert weder funktionierende Schlüssel noch die Löschung kopierter Daten. Die beste Grundlage für diese Entscheidung ist eine Sicherung, die sie überflüssig macht.

Fazit: Konten schützen, Wege verbauen, Wiederherstellung üben

Ransomware im Krankenhaus ist kein Naturereignis, sondern ein Geschäftsmodell, das auf vorhersehbaren Schwächen aufbaut: übernommene Konten, offene Dienstleisterzugänge, zu mächtige Administratoren an zu gewöhnlichen Rechnern, flache Netze und Sicherungen, die mit denselben Rechten gelöscht werden können wie alles andere. Gegen jede dieser Schwächen gibt es eine Maßnahme, und die wirksamsten davon sind weder neu noch teuer.

Fangen Sie links in der Kette an: MFA für alle externen Zugänge, Legacy-Anmeldung aus, Dienstleister auf Zeit. Dann die Mitte: Tiering, getrennte Admin-Konten, Erkennung im Active Directory. Und parallel das Ende: eine Sicherung, die den Angriff überlebt, und eine Wiederherstellung, die jemand schon einmal gemacht hat. Der Rest ist Ausdauer. Krankenhaus-IT hat davon erfahrungsgemäß reichlich, sie hat schließlich auch schon das letzte KIS-Update überlebt.

WEITERLESEN · Weiterlesen

› Microsoft 365 im Krankenhaus

› Kompetenzbereich Microsoft 365 Security
› Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet
› NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos
› Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung
› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten
› Kompetenzbereich Microsoft Entra ID
› Microsoft 365 Beratung für Krankenhäuser