Entra-ID-Überprüfung für Klinik-Tenants: Was sich nach Jahren Wildwuchs findet



Wissen

Alle Beiträge der Serie rund um Kliniken, Klinikverbünde und Microsoft 365:

Microsoft 365 im Krankenhaus

Beratung

Entra-ID-Überprüfung für Ihren Klinik-Tenant: lesend, werkzeuggestützt, mit Maßnahmenplan:

Microsoft-365-Beratung für Krankenhäuser

Schulung

Wissen für IT-Team und Rufbereitschaft, damit der Tenant nach der Prüfung sauber bleibt:

Microsoft-365-Schulung für Krankenhäuser

Jeder Klinik-Tenant hat eine Geschichte. Meist beginnt sie mit einem Pilotprojekt in der Verwaltung, dann kommt eine Pandemie und mit ihr über Nacht Teams für Krisenstab, Hygiene und Pflegedirektion. Danach fusionieren zwei Häuser, ein Hersteller richtet für sein Subsystem eine Schnittstelle ein, eine Agentur baut das neue Intranet, und irgendwann gibt es mehr globale Administratoren als Stationen im Haus. Niemand hat das so geplant. Es ist einfach passiert, zwischen Rufbereitschaft, Zertifizierungsaudit und dem nächsten KIS-Update.

Eine **Entra-ID-Überprüfung im Krankenhaus** bringt diese Geschichte zu Papier. Sie zeigt, welche Konten, Gäste, Anwendungen und Ausnahmen sich über die Jahre angesammelt haben, bewertet sie nach Risiko und übersetzt das Ergebnis in einen Maßnahmenplan, den IT-Leitung, Informationssicherheitsbeauftragte und Geschäftsführung gemeinsam tragen können. Dieser Beitrag beschreibt, was sich in Klinik-Tenants typischerweise findet, wie eine rein lesende, werkzeuggestützte Bestandsaufnahme abläuft und warum das Ergebnis auch für die Nachweise nach § 391 SGB V oder dem BSIG nützlich ist. Er gehört zur Serie Microsoft 365 im Krankenhaus.

Vorweg die Grundhaltung, die sich durch die ganze Serie zieht: Patientendaten gehören ins KIS und seine Subsysteme wie LIS, RIS und PACS. Microsoft 365 ist Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Dass trotzdem in manchem Team eine Excel-Liste mit Patientennamen liegt, wissen alle, die schon einmal einen Klinik-Tenant von innen

gesehen haben. Gerade deshalb ist die Frage, wer überhaupt Zugriff auf diesen Tenant hat, keine akademische.

Fakten: Das Wichtigste in Kürze

- Klinik-Tenants verwildern aus nachvollziehbaren Gründen: Schichtdienst, Honorarkräfte, Leiharbeit, viele Hersteller, mehrere Standorte und Projekte, die unter Zeitdruck entstanden sind.
- Die häufigsten Befunde: aktive Konten ausgeschiedener Ärzte und Mitarbeiter, Gastkonten ohne Ablauf, App-Registrierungen mit weitreichenden Rechten, zu viele globale Administratoren, Legacy-Authentifizierung für Altgeräte, Ausnahmen in Conditional Access und fehlende Notfallkonten.
- Microsoft empfiehlt weniger als fünf globale Administratoren und mindestens zwei reine Cloud-Notfallkonten mit phishingresistenter Anmeldung, deren Funktion mindestens alle 90 Tage geprüft wird.
- Die Überprüfung arbeitet bis zum Maßnahmenplan rein lesend, etwa mit der Rolle Global Reader. Im Tenant wird dabei nichts verändert.
- Anmelde- und Überwachungsprotokolle hält Entra ID mit P1- oder P2-Lizenz nur 30 Tage vor, ohne Premium-Lizenz sieben Tage. Wer sie für die Analyse braucht, sichert sie früh.
- Für die Basisauthentifizierung bei SMTP AUTH in Exchange Online hat Microsoft angekündigt, sie Ende Dezember 2026 für bestehende Tenants standardmäßig abzuschalten. Scanner und Medizintechnik, die per SMTP AUTH Mails versenden, gehören deshalb jetzt auf die Liste.

Warum Klinik-Tenants verwildern

Wildwuchs ist im Krankenhaus kein Zeichen schlechter IT. Er ist die logische Folge eines Betriebs, der rund um die Uhr läuft, in dem ständig Menschen kommen und gehen und in dem die IT selten die Zeit hat, Dinge ordentlich zu Ende zu bringen, bevor das nächste Feuer brennt. Wer einmal versucht hat, am Freitagnachmittag eine Honorarärztin für den Nachtdienst am Wochenende arbeitsfähig zu machen, weiß, dass in diesem Moment niemand an ein Ablaufdatum denkt.

Ein-, Aus- und Umtritte im Schichtbetrieb

Bei festangestellten Ärzten, Pflegekräften und Verwaltungsmitarbeitern ist der Lebenszyklus eines Kontos meist leidlich geregelt: Das Personalsystem kennt Eintritt und Austritt, ein Prozess oder ein Skript legt das Konto im Active Directory an, die Synchronisation trägt es nach Entra ID. Spannend wird es beim Wechsel. Eine Pflegekraft wechselt von der Intensivstation in die Notaufnahme, ein Assistenzarzt rotiert durch drei Fachabteilungen, eine Sekretärin wechselt vom Ärztlichen Direktor zur Pflegedirektion. Neue Gruppen kommen hinzu, die alten bleiben. Nach zehn Jahren hat ein Konto die Rechte einer ganzen Laufbahn.

Noch spannender wird es bei allen, die das Personalsystem gar nicht oder nur am Rand kennt: Honorarkräfte, Leiharbeit, Hospitationen, Famulaturen, Praktika, externe Dozenten der Pflegeschule. Hier entsteht das Konto oft auf Zuruf der Station, und das Ende des Einsatzes meldet niemand, weil die Person einfach nicht mehr kommt.

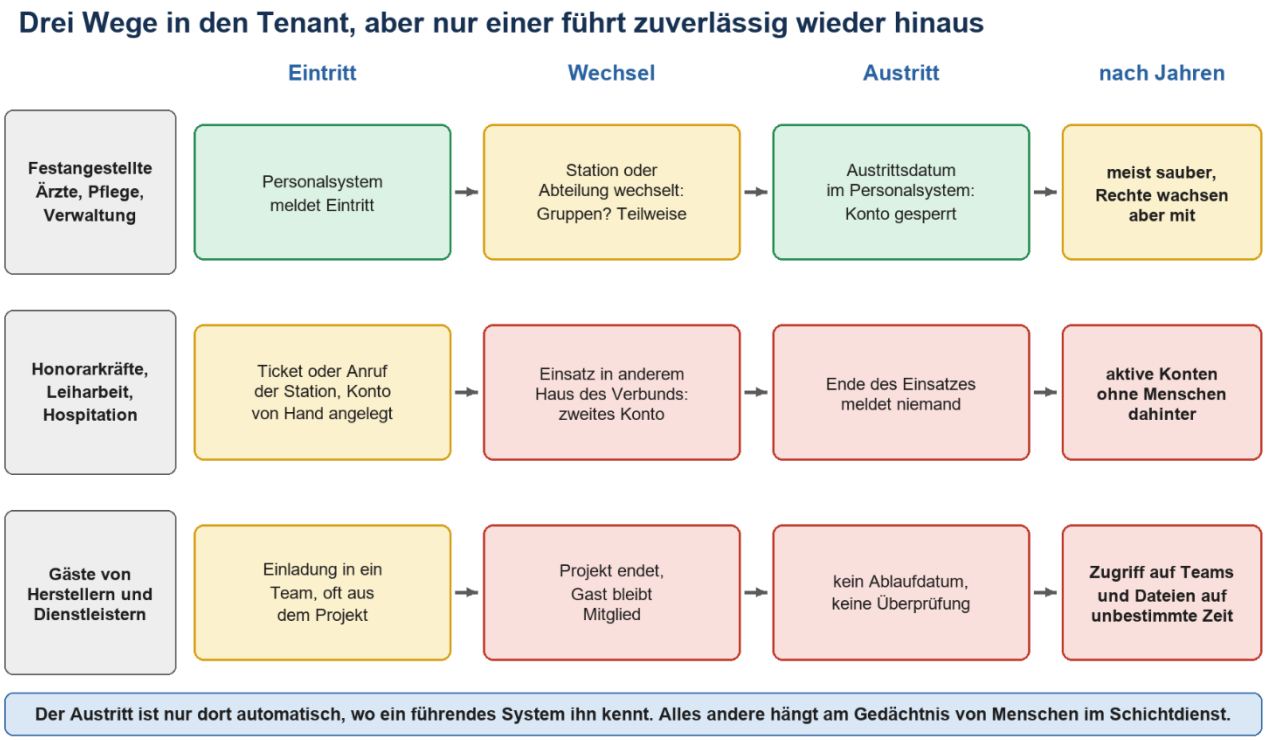


Abbildung 1: Wo ein führendes System den Austritt kennt, verschwinden Konten zuverlässig. Bei Honorarkräften, Leiharbeit und Gästen hängt es am Gedächtnis.

Hersteller, Dienstleister und Projekte

Kaum eine Branche hat so viele Softwarehersteller im Haus wie ein Krankenhaus. KIS, LIS, RIS, PACS, Dokumentationssysteme für Intensiv und OP, Dienstplanung, CAFM, Medizintechnik mit eigener Software, Archiv, Spracherkennung, Küche, Zeiterfassung. Viele davon brauchen inzwischen etwas von Microsoft 365: ein Postfach für den Versand, eine App-Registrierung für die Anmeldung, einen Gastzugang für die Projektzusammenarbeit in Teams. Jedes dieser Dinge ist für sich harmlos. In der Summe ergibt sich eine Landkarte von Berechtigungen, die niemand vollständig kennt, weil jede einzelne von einem anderen Projekt stammt.

Mehrere Standorte, mehrere Köche

Im Klinikverbund kommt eine weitere Zutat hinzu: Zusammengeführte Häuser bringen ihre eigenen Admins, eigene Namenskonventionen und manchmal eigene Altdomänen mit. Wenn der Tenant in einer Fusion schnell gemeinsam nutzbar sein musste, wurden Rechte eher großzügig verteilt, damit die Standort-IT handlungsfähig bleibt. Wie sich das sauber ordnen lässt, beschreibt der Beitrag Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen. Für die Überprüfung heißt das vor allem: Es gibt selten den einen Ansprechpartner, der alles weiß.

Aus der Praxis: Gewachsene Strukturen im Verbund

In der langjährigen Begleitung eines Krankenhausverbunds mit mehreren Standorten ging es um Vertrauensstellungen zwischen Domänen, die NTLM-Abschaltung, Kerberos, den Aufbau und die Härtung der PKI und Exchange Hybrid. Eine Erfahrung aus dieser Arbeit trägt direkt in jede Entra-ID-Überprüfung: Was im lokalen Active Directory gewachsen ist, wird über die Synchronisation in die Cloud getragen. Wer Entra ID aufräumen will, schaut deshalb immer auch auf die Quelle. Mehr dazu im Beitrag Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung.

Die typische Befundlage: acht Fundstücke, die fast immer auftauchen

Jeder Tenant ist anders, aber die Befunde ähneln sich erstaunlich. Die folgende Landkarte zeigt, wo der Wildwuchs typischerweise sitzt. Die Farben geben die häufige Einstufung wieder, nicht die zwingende: Ein einzelnes Gastkonto in einem leeren Team ist etwas anderes als ein Gast mit Zugriff auf die Dateiablage des Krisenstabs.

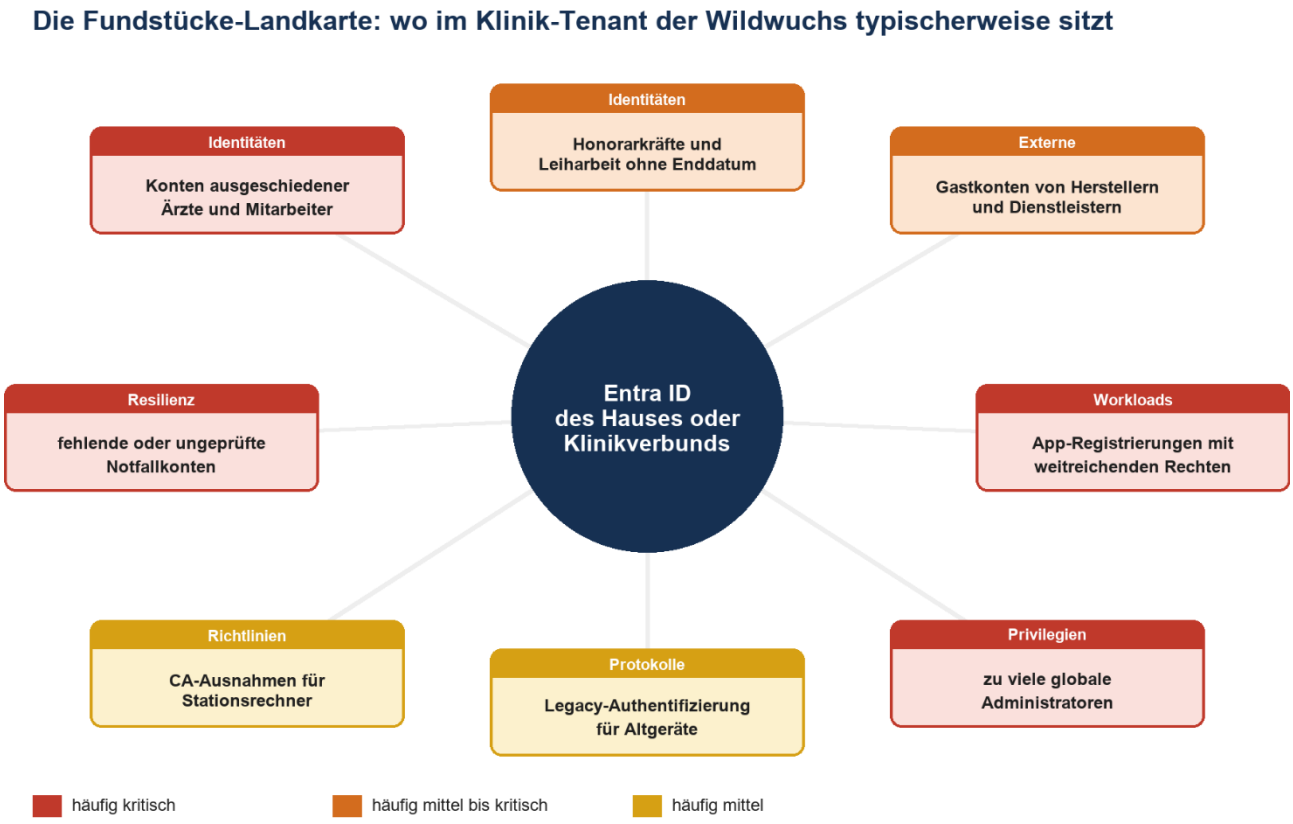


Abbildung 2: Acht typische Fundstücke im Klinik-Tenant, gruppiert nach Identitäten, Externen, Workloads, Privilegien, Protokollen, Richtlinien und Resilienz.

Konten ausgeschiedener Ärzte und Mitarbeiter

Der Klassiker. Das Konto des Oberarztes, der vor Jahren in eine andere Klinik gewechselt ist, ist noch aktiv, hat noch eine Lizenz, ein Postfach und Mitgliedschaften in Teams der Arzneimittelkommission und des Qualitätszirkels. Manchmal wird es sogar noch benutzt, weil seine Sekretärin das Postfach weiter betreut oder weil eine Weiterleitung eingerichtet wurde, an die sich niemand erinnert. Das Konto lebt also weiter, mit mehr Zugriff, als sein Besitzer im Haus je hatte, und ohne dass jemand die Anmeldungen bemerken würde.

Technisch findet man solche Konten über das letzte erfolgreiche Anmeldedatum. In Microsoft Graph liefert die Eigenschaft `signInActivity` diese Information; Microsoft stellt sie nur mit Premium-Lizenzen von Entra ID bereit. Die Zahl allein reicht aber nicht: Ein Konto ohne Anmeldung seit einem Jahr kann der Arzt in Elternzeit sein, und das Konto mit täglicher Anmeldung kann genau das Problem sein. Deshalb gehört der Abgleich mit der Personalabteilung zwingend dazu.

Honorarkräfte und Leiharbeit

Honorarärzte im Bereitschaftsdienst, Pflegekräfte aus der Arbeitnehmerüberlassung, Springer zwischen den Häusern eines Verbunds: Sie halten den Betrieb am Laufen, und sie hinterlassen Konten. Typisch sind Konten ohne Ablaufdatum, Konten mit generischen Namen wie »Honorar-Anästhesie-2«, die über Jahre von wechselnden Personen genutzt werden, und doppelte Konten derselben Person, weil sie in zwei Häusern eingesetzt war. Letzteres ist nicht nur ein Sicherheits-, sondern auch ein Nachvollziehbarkeitsproblem: Wer war es denn nun?

Gastkonten von Herstellern und Dienstleistern

Gäste kommen über Teams in den Tenant, oft auf Einladung eines Projektleiters. Das Projekt endet, die Gäste bleiben. In Klinik-Tenants finden sich regelmäßig Gastkonten von Herstellern, Beratungshäusern, Agenturen und Servicepartnern, die seit Jahren keine Anmeldung mehr hatten, aber noch Mitglied in Teams mit sensiblen Inhalten sind. Besonders unangenehm: Gäste, die über eine private Mailadresse eingeladen wurden, weil die Firmenadresse beim ersten Versuch nicht funktionierte. Ob der Servicetechniker diese Adresse noch nutzt oder ob sie längst jemand anderem gehört, weiß niemand.

> **Warnung: Die Excel-Liste im Gästebereich**
>
> Der unangenehmste Befund ist selten technisch. Es ist die Kombination aus einem Gastkonto ohne Ablauf und einem Team, in dem eine Excel-Liste mit Patientennamen liegt, etwa eine Belegungsübersicht, eine Liste für das Entlassmanagement oder eine Übersicht für eine Studie. Das ist nicht der Normalfall, aber es kommt vor. Die Überprüfung macht solche Konstellationen sichtbar, ohne die Inhalte selbst zu öffnen: Sie zeigt, welche Teams Gäste enthalten und wie die Freigaben aussehen. Ob dort Patientendaten liegen, klären anschließend Datenschutzbeauftragte und Fachbereich. Wo die Grenze zwischen KIS und Office verläuft, beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt.

App-Registrierungen von Subsystem-Herstellern

Hier wird es technisch und oft kritisch. Viele Hersteller nutzen inzwischen Microsoft Graph, um Mails zu versenden, Termine einzutragen, Dateien abzulegen oder Benutzer abzufragen. Dafür legen sie eine App-Registrierung an oder bitten die IT, eine Unternehmensanwendung zu genehmigen. Was in der Installationsanleitung stand, war im Zweifel nicht die minimale, sondern die bequeme Berechtigung: Anwendungsberechtigungen wie `Mail.ReadWrite`, `Sites.ReadWrite.All` oder gar `Directory.ReadWrite.All` erlauben einer Anwendung, ohne angemeldeten Benutzer auf alle Postfächer, alle SharePoint-Websites oder das ganze Verzeichnis zuzugreifen.

Dazu kommen Geheimnisse mit sehr langer Laufzeit, Zertifikate, die irgendwann ablaufen und dann nachts um drei den Befundversand stoppen, und Besitzer, die längst nicht mehr im Haus sind. Die Frage, die in der Überprüfung am häufigsten fällt, lautet: »Wofür war diese App noch mal?« Wenn die Antwort »das hat der Hersteller damals eingerichtet« lautet, ist das ein Befund, kein Schulterzucken.

Microsoft hat die Standardeinstellung für die Zustimmung durch Benutzer inzwischen auf eine von Microsoft verwaltete Richtlinie umgestellt, die für neue Tenants gilt und sich an Microsofts aktuellen Empfehlungen orientiert. Ältere Tenants haben aber oft noch Einstellungen aus der Anfangszeit, in denen jeder Benutzer jeder Anwendung Zugriff auf seine Daten gewähren durfte. Auch das gehört zur Prüfung.

Zu viele globale Administratoren

Microsoft empfiehlt ausdrücklich, die Rolle Global Administrator an weniger als fünf Personen zu vergeben, und blendet im Entra Admin Center einen Hinweis ein, sobald es fünf oder mehr sind. Für privilegierte Rollen insgesamt nennt Microsoft eine Grenze von weniger als zehn Zuweisungen. In Klinik-Tenants ist die Zahl der globalen Administratoren häufig zweistellig. Darunter finden sich Standort-Admins, die eigentlich nur Benutzer anlegen sollten, Dienstleister aus dem Einführungsprojekt, das persönliche Alltagskonto des IT-Leiters, mit dem auch Mails gelesen und Anhänge geöffnet werden, und gelegentlich ein Konto, bei dem niemand mehr weiß, wem es gehört.

Die Gegenstrategie ist bekannt: Rollen nach dem Prinzip der minimalen Rechte, getrennte Admin-Konten ohne Postfach, nur in der Cloud angelegt und nicht aus dem lokalen AD synchronisiert, und zeitlich begrenzte Aktivierung über Privileged Identity Management, das laut Microsoft Entra ID P2 oder Entra ID Governance voraussetzt.

Legacy-Authentifizierung für Altgeräte

Der Multifunktionsdrucker auf Station, der Scans per Mail versendet. Das Blutgasanalysegerät, das Qualitätsberichte an ein Postfach schickt. Die Zeiterfassung, die per SMTP Erinnerungen verschickt. Viele dieser Geräte können nur Benutzername und Kennwort, keine moderne Authentifizierung. Für die Postfachprotokolle hat Microsoft die Basisauthentifizierung in Exchange Online bereits abgeschaltet; übrig geblieben ist vor allem SMTP AUTH. Nach dem aktualisierten Zeitplan vom Januar 2026 bleibt das Verhalten bis Ende Dezember 2026 unverändert; dann wird die Basisauthentifizierung für SMTP AUTH in bestehenden Tenants standardmäßig deaktiviert, Administratoren können sie aber wieder einschalten. Das endgültige Abschaltdatum will Microsoft in der zweiten Jahreshälfte 2027 bekanntgeben.

Für die Überprüfung heißt das: Die Anmeldeprotokolle zeigen, welche Konten noch mit Legacy-Protokollen arbeiten. Jedes dieser Konten ist meist ein Funktionskonto mit einem Kennwort, das seit der Inbetriebnahme des Geräts nicht geändert wurde und das im Zweifel auf einem Zettel am Gerät klebt. Wer diese Liste hat, kann gemeinsam mit der Medizintechnik planen, statt im Januar von einem Scanner überrascht zu werden, der nicht mehr scannt.

Ausnahmen in Conditional Access für Stationsrechner

Conditional Access ist das Herzstück einer modernen Entra-ID-Absicherung, und genau dort sitzen in Kliniken die meisten Kompromisse. Damit die Anmeldung am Stationsrechner schnell bleibt, wurden Sammelkonten, Gerätegruppen oder ganze IP-Bereiche des Klinikums von der Mehrfaktor-Pflicht ausgenommen. Das war einmal eine bewusste Entscheidung. Heute ist es oft eine Ausnahme ohne Besitzer, ohne Begründung und ohne Ablaufdatum, in die im Lauf der Zeit weitere Konten gerutscht sind, weil »das bei den Stationsrechnern ja auch so ist«.

Die Überprüfung fragt bei jeder Ausnahme: Wer ist ausgenommen, wovon, seit wann, warum, und gibt es heute eine bessere Lösung? Wie die Anmeldung am Stationsarbeitsplatz schnell und trotzdem nachvollziehbar wird, beschreibt der Beitrag Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel. Für gemeinsam genutzte Geräte in der Pflege lohnt zusätzlich ein Blick in Frontline in der Pflege: Gemeinsam genutzte Geräte, Schichtwechsel und Stationsrechner.

Fehlende oder ungeprüfte Notfallkonten

Was passiert, wenn der Föderationsdienst ausfällt, das Mobilfunknetz für die Authenticator-App nicht erreichbar ist oder eine Conditional-Access-Richtlinie versehentlich alle Admins aussperrt? In vielen Klinik-Tenants lautet die ehrliche Antwort: Dann wird es spannend. Microsoft empfiehlt mindestens zwei Notfallkonten, die ausschließlich in der Cloud mit der Domäne onmicrosoft.com

angelegt sind, nicht föderiert und nicht synchronisiert werden, die Rolle Global Administrator dauerhaft aktiv besitzen und mit einer phishingresistenten Methode wie einem Passkey auf FIDO2-Sicherheitsschlüssel oder zertifikatbasierter Authentifizierung angemeldet werden. Jede Nutzung soll einen Alarm auslösen, und die Funktion soll mindestens alle 90 Tage geprüft werden.

Typische Befunde: Es gibt kein Notfallkonto. Es gibt eines, aber es ist synchronisiert und damit vom lokalen AD abhängig. Es gibt zwei, aber beide hängen an der Authenticator-App auf dem Diensthandy des IT-Leiters. Oder es gibt sie, aber seit der Einrichtung hat sich niemand damit angemeldet, und das Kennwort liegt in einem Tresor, dessen Kombination der Vorgänger mitgenommen hat. Notfallübungen kennt jedes Krankenhaus aus Brandschutz und Notaufnahme; für den Tenant fehlen sie erstaunlich oft.

Fakten: Notfallkonten laut Microsoft

- mindestens zwei Konten, nur in der Cloud, Domäne onmicrosoft.com, ohne Abhängigkeit von Föderation oder Synchronisation
- phishingresistente Anmeldung per Passkey (FIDO2) oder zertifikatbasierter Authentifizierung, andere Methode als bei den regulären Admin-Konten
- Rolle Global Administrator dauerhaft aktiv, nicht nur berechtigt
- Ausnahme von Conditional-Access-Richtlinien, die die Anmeldung blockieren oder einschränken
- Alarm bei jeder Anmeldung, Nachbesprechung nach jeder Nutzung, Funktionsprüfung mindestens alle 90 Tage

Befund, Risiko, Sofortmaßnahme im Überblick

Die folgende Tabelle fasst die acht Fundstücke zusammen. Die Sofortmaßnahme ist bewusst klein gehalten: Sie soll das Risiko senken, ohne den Klinikbetrieb zu gefährden. Die eigentliche Bereinigung kommt im Maßnahmenplan.

Befund	Risiko	Sofortmaßnahme
Aktive Konten ausgeschiedener Ärzte und Mitarbeiter	Übernahme unbemerkt, Zugriff auf Postfach, Teams und Dateien; Anmeldungen fallen niemandem auf	Abgleich mit Personalabteilung, Konto sperren statt löschen, Lizenz und Weiterleitungen prüfen
Konten von Honorarkräften und Leiharbeit ohne Enddatum	Konten ohne Menschen dahinter, geteilte Konten, keine Nachvollziehbarkeit	Liste mit Stationen und Personalwesen abgleichen, Ablaufdatum setzen, geteilte Konten beenden
Gastkonten ohne Ablauf und ohne Sponsor	Externe behalten Zugriff auf Teams und Dateien, teils über private Adressen	inaktive Gäste sperren, Gäste ohne Sponsor dem Projektverantwortlichen zuordnen
App-Registrierungen mit weitreichenden Rechten	Zugriff auf alle Postfächer, Websites oder das Verzeichnis ohne Benutzer; lang laufende Geheimnisse	Rechte mit Hersteller klären, ungenutzte Apps deaktivieren, Geheimnisse inventarisieren
Zu viele globale Administratoren	ein kompromittiertes Konto genügt für den ganzen Tenant	Rollen auf das nötige Maß reduzieren, separate Admin-Konten, MFA prüfen
Legacy-	Kennwortangriffe ohne MFA, alte	betroffene Konten und Geräte

Authentifizierung für Altgeräte	Kennwörter an Geräten	inventarisieren, Kennwörter ändern, Ablösung mit Medizintechnik planen
Conditional-Access-Ausnahmen für Stationsrechner	Lücke für alle, die in die Ausnahme gerutscht sind	Ausnahmen dokumentieren, Mitglieder prüfen, fremde Konten entfernen
Fehlende oder ungeprüfte Notfallkonten	Aussperrung bei Störung, keine Handlungsfähigkeit im Notfall	zwei Notfallkonten nach Microsoft-Empfehlung einrichten, Anmeldung testen, Alarm einrichten

Das Vorgehen: lesend erheben, nüchtern bewerten, gemeinsam planen

Eine gute Überprüfung ist langweilig im besten Sinne. Sie verändert nichts, sie bricht nichts, und sie liefert am Ende ein Dokument, mit dem alle Beteiligten arbeiten können. Das ist im Krankenhaus wichtiger als anderswo: Niemand möchte erklären müssen, warum die Befundübermittlung des Labors ausgefallen ist, weil jemand während der Analyse eine App für ungenutzt gehalten hat.

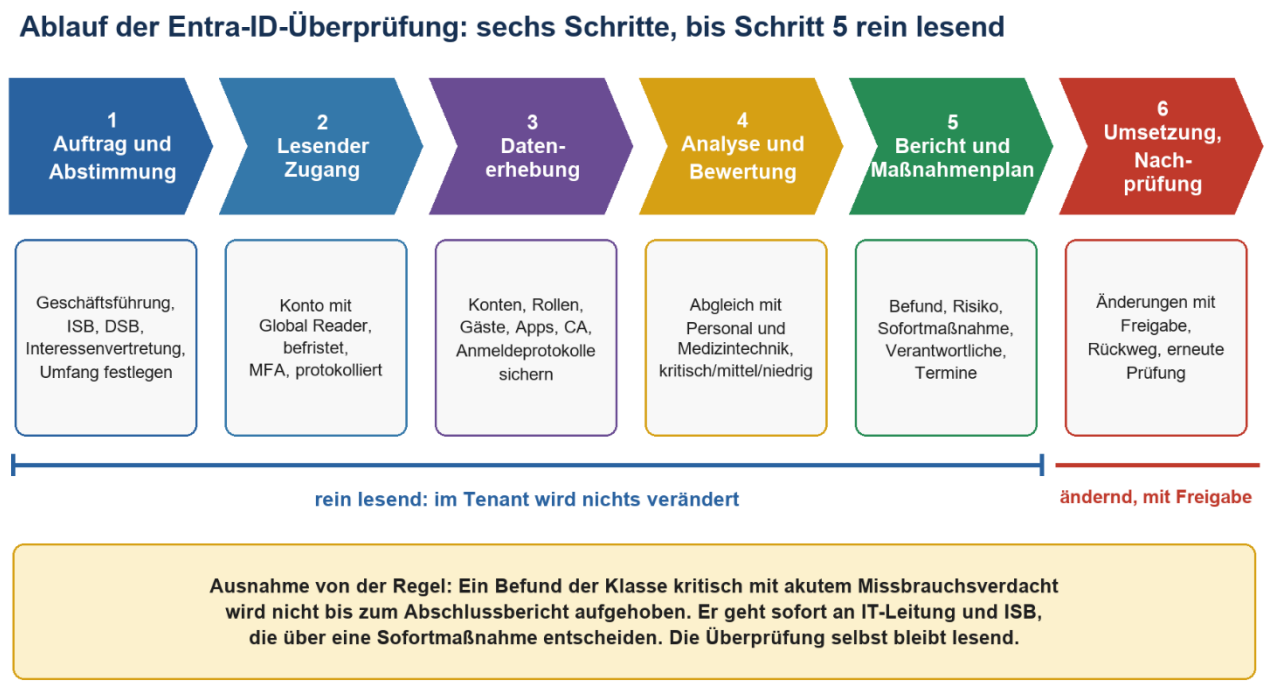


Abbildung 3: Der Ablauf der Entra-ID-Überprüfung. Bis zum Maßnahmenplan wird im Tenant nichts verändert.

Schritt 1: Auftrag und Abstimmung

Bevor ein einziger Befehl läuft, steht der Auftrag: Welcher Tenant, welche Standorte, welche Themen, welcher Zeitraum der Protokolle, wer erhält den Bericht? An den Tisch gehören IT-Leitung, Informationssicherheitsbeauftragte, Datenschutzbeauftragte und, weil Anmeldeprotokolle Rückschlüsse auf das Verhalten einzelner Menschen zulassen, die Interessenvertretung. Das ist kein Formalismus, sondern spart später Ärger.

> **Hinweis: Mitbestimmung und Datenschutz (keine Rechtsberatung)**
>
> Bei der Auswertung von Anmeldeprotokollen geht es nicht um Leistungs- oder

Verhaltenskontrolle, sondern um Sicherheit. Trotzdem können Protokolldaten dazu geeignet sein, und genau darauf kommt es bei der Mitbestimmung an. Welche Regeln gelten, hängt von der Trägerschaft ab: Im privaten und in vielen freigemeinnützigen Häusern ist es das Betriebsverfassungsgesetz, in öffentlichen und kommunalen Häusern das Personalvertretungsrecht des jeweiligen Bundeslandes oder des Bundes, in kirchlichen Häusern das kirchliche Mitarbeitervertretungsrecht. Die Landespersonalvertretungsgesetze unterscheiden sich in Details deutlich. Klären Sie Zweck, Umfang und Löschung der erhobenen Daten vorab mit Datenschutzbeauftragten und Interessenvertretung und lassen Sie die konkrete Rechtslage für Ihr Haus prüfen. Mehr dazu im Beitrag Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

Schritt 2: Lesender Zugang

Für die Erhebung genügt in aller Regel die integrierte Rolle Global Reader, die alles lesen, aber nichts ändern kann. Sie wird befristet einem eigenen Prüfkonto zugewiesen, das mit Mehrfaktor-Authentifizierung angemeldet wird und dessen Aktivitäten im Überwachungsprotokoll erscheinen. Einige Werkzeuge benötigen bei der ersten Ausführung die einmalige Zustimmung eines globalen Administrators zu ihren Graph-Leseberechtigungen; diese Zustimmung erteilt die Klinik-IT selbst und kann sie nach der Prüfung wieder entziehen.

Schritt 3: Datenerhebung mit Werkzeugen

Niemand sollte zweitausend Konten von Hand im Admin Center durchklicken. Die Erhebung läuft werkzeuggestützt, reproduzierbar und mit Zeitstempel, damit die Nachprüfung in einem Jahr dieselben Daten vergleichen kann.

Werkzeug	Was es liefert	Hinweis
Microsoft Graph PowerShell	Konten mit `signInActivity`, Rollenzuweisungen, Gäste, Dienstprinzipale, App-Berechtigungen, Conditional-Access-Richtlinien	flexibel, Ergebnisse als CSV für den Abgleich mit Personalwesen und Medizintechnik
Microsoft Zero Trust Assessment	fertiger Bericht mit Prüfungen zu Identität und Geräten, als HTML	laut Microsoft rein lesend, Verarbeitung lokal; der Bericht enthält sensible Tenant-Informationen und ist entsprechend zu schützen
Entra Admin Center	Anmelde- und Überwachungsprotokolle, Arbeitsmappen zu Legacy-Authentifizierung und Conditional Access, Empfehlungen	Protokolle mit Premium-Lizenz 30 Tage, sonst sieben Tage
Microsoft Secure Score	Bewertung von Einstellungen mit Verbesserungsvorschlägen	gute Ergänzung, ersetzt aber keinen Abgleich mit der Wirklichkeit im Haus
Exchange Online PowerShell	Weiterleitungen, Postfachberechtigungen, Konten mit SMTP AUTH	zeigt, welche Altgeräte über welches Konto senden

Tipp: Protokolle früh sichern

Entra ID hält Anmelde- und Überwachungsprotokolle mit P1- oder P2-Lizenz 30 Tage vor, ohne Premium-Lizenz sieben Tage. Für eine Aussage wie »dieses Gastkonto wurde seit einem Jahr nicht benutzt« reicht das nicht. Die Eigenschaft signInActivity am Konto hilft weiter, für Legacy-Protokolle und Ausnahmen brauchen Sie aber die Protokolle selbst. Wer sie nicht schon in einen Log-Analytics-Arbeitsbereich oder ein SIEM leitet, sollte das vor der Überprüfung einrichten. Das ist auch unabhängig von der Prüfung eine gute Idee, denn im Ernstfall fragt die Forensik genau nach diesen Daten.

Schritt 4: Analyse und Bewertung

Rohdaten sind noch keine Befunde. Erst der Abgleich mit dem Haus macht aus einer Liste inaktiver Konten eine Aussage: Personalabteilung und Personaldienstleister bestätigen Austritte, Medizintechnik und Subsystem-Verantwortliche ordnen App-Registrierungen und Funktionskonten zu, Projektverantwortliche bestätigen oder beenden Gastzugänge. Dann wird bewertet, und zwar nach einem einfachen Raster aus Ausnutzbarkeit und Auswirkung.

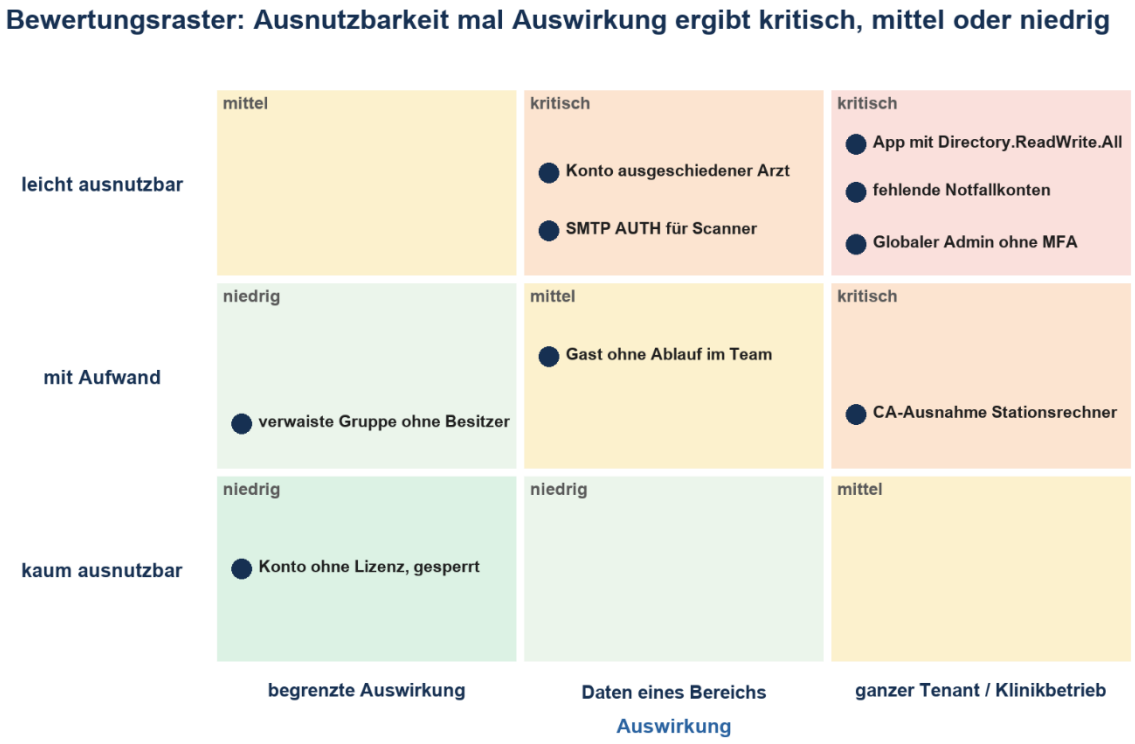


Abbildung 4: Bewertungsraster mit Beispielen. Die Einordnung im konkreten Tenant hängt von Rechten, Inhalten und vorhandenen Schutzmaßnahmen ab.

Stufe	Kriterien	Erwartung an die Umsetzung
kritisch	leicht ausnutzbar und Auswirkung auf den ganzen Tenant oder den Klinikbetrieb, etwa globale Rechte ohne starke Anmeldung, Apps mit Verzeichnis-Schreibrechten, fehlende Notfallkonten	sofort, innerhalb von Tagen; bei akutem Verdacht sofortige Meldung an IT-Leitung und ISB
mittel	mit Aufwand ausnutzbar oder auf einen Bereich begrenzt, etwa inaktive Gäste in Projekt-Teams, Legacy-Authentifizierung einzelner Funktionskonten, breite	geplant, innerhalb weniger Wochen bis Monate, mit Abstimmung der

	CA-Ausnahmen	Betroffenen
niedrig	kaum ausnutzbar oder geringe Auswirkung, etwa gesperrte Konten ohne Lizenz, verwaiste Gruppen ohne Inhalt, uneinheitliche Namen	im Regelbetrieb, bei Gelegenheit oder mit der nächsten Aufräumrunde

Schritt 5: Bericht und Maßnahmenplan

Der Bericht hat zwei Leserschaften. Die Geschäftsführung braucht eine Seite: Wie steht der Tenant da, wo liegen die kritischen Punkte, was kostet die Behebung an Zeit und Aufmerksamkeit? Die IT braucht die Details: Jeder Befund mit Fundstelle, Risiko, Einstufung, Sofortmaßnahme, Verantwortlichen und Termin. Ein guter Maßnahmenplan ist so konkret, dass er sich in das Ticketsystem übertragen lässt, und so realistisch, dass er den Rufbereitschaftsplan überlebt.

Schritt 6: Umsetzung und Nachprüfung

Erst jetzt wird etwas geändert, und zwar mit Freigabe, Rückweg und einem Termin, der nicht in die Übergabe, nicht vor die Visite und nicht auf Freitag um 15 Uhr fällt. Konten werden zuerst gesperrt und erst nach einer Karenzzeit gelöscht. App-Rechte werden nach Absprache mit dem Hersteller reduziert, nicht im Alleingang. Nach einigen Monaten folgt eine kurze Nachprüfung mit denselben Werkzeugen: Sind die Befunde behoben, und ist Neues nachgewachsen?

Beratung: Entra-ID-Überprüfung für Ihren Klinik-Tenant

Wir führen die Überprüfung für Ihr Haus oder Ihren Klinikverbund durch: rein lesend, werkzeuggestützt, mit Abgleich gegen Personalwesen und Medizintechnik, mit Bewertung nach kritisch, mittel und niedrig und einem Maßnahmenplan, den Ihre IT umsetzen kann. Die Ergebnisse sind so aufbereitet, dass Geschäftsführung, Informationssicherheit und Datenschutz damit arbeiten können. Alle Informationen finden Sie auf der Seite Microsoft-365-Beratung für Krankenhäuser.

Was die Überprüfung für die Nachweise nach § 391 SGB V und BSIG bringt

Die IT-Sicherheit in Krankenhäusern regelt § 391 SGB V, der frühere § 75c, seit dem NIS2-Umsetzungsgesetz vom 6. Dezember 2025 in neuer Fassung. Krankenhäuser müssen danach nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen treffen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme zu vermeiden. Maßnahmen zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter zählen ausdrücklich dazu. Die Pflichten können über einen branchenspezifischen Sicherheitsstandard erfüllt werden, dessen Eignung das BSI festgestellt hat; für die medizinische Versorgung ist das der B3S der Deutschen Krankenhausgesellschaft, aktuell in Version 1.3.1 vom 10. Oktober 2025.

Für Krankenhäuser, die als Betreiber kritischer Anlagen gelten, greift § 391 SGB V nicht; sie unterliegen den Pflichten des BSIG. Dazu gehört nach § 39 BSIG die Pflicht, die Umsetzung der Anforderungen alle drei Jahre durch Audits, Prüfungen oder Zertifizierungen gegenüber dem BSI nachzuweisen, einschließlich der dabei aufgedeckten Sicherheitsmängel. Was das im Einzelnen für Microsoft 365 bedeutet, ordnet der Beitrag NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten ein.

Hinweis: Keine Rechtsberatung

Ob Ihr Haus unter § 391 SGB V oder unter das BSIG fällt, welche Nachweise konkret verlangt werden und wie ein Prüfer eine Entra-ID-Überprüfung würdigt, ist eine Frage des Einzelfalls und gehört in die Hände Ihrer Rechtsabteilung oder entsprechender Fachleute. Dieser Beitrag beschreibt, welche technischen Ergebnisse eine Überprüfung liefert und wie sie sich in ein bestehendes Informationssicherheitsmanagement einfügen.

Unabhängig von der rechtlichen Einordnung gilt: Wer nachweisen muss, dass Zugriffe angemessen geregelt sind, braucht eine belastbare Bestandsaufnahme. Eine Entra-ID-Überprüfung liefert dafür mehrere Bausteine, die sich in ein ISMS, in die Unterlagen zum B3S oder in ein Audit nach BSIG einbringen lassen.

Ergebnis der Überprüfung	Nutzen für Nachweise und ISMS
Datierte Bestandsaufnahme aller Konten, Gäste, Rollen und Apps	belegt, dass Berechtigungen bekannt sind und regelmäßig überprüft werden
Bewertung nach kritisch, mittel, niedrig	Grundlage für die Risikobehandlung und die Priorisierung im ISMS
Maßnahmenplan mit Verantwortlichen und Terminen	zeigt den Umgang mit festgestellten Mängeln, wie ihn auch § 39 BSIG für Betreiber kritischer Anlagen vorsieht
Nachprüfung nach Umsetzung	dokumentiert die Wirksamkeit der Maßnahmen
Notfallkonten mit Testprotokoll	Baustein für Notfallmanagement und Wiederanlauf
Prozessbeschreibung für Ein- und Austritt, Gäste und Apps	kann als Verfahrensanweisung in das QM-Handbuch und das ISMS übernommen werden

Ein Nebenaspekt, der in diesem Zusammenhang oft auftaucht: § 393 SGB V verlangt seit dem 1. Juli 2025 für die Verarbeitung von Sozial- und Gesundheitsdaten in Cloud-Diensten ein aktuelles C5-Testat vom Typ 2 oder ein nach der zugehörigen Verordnung gleichwertiges Testat oder Zertifikat. Welche Microsoft-Dienste von welchem Testat erfasst sind, ist ein Prüfauftrag: Die aktuellen Berichte stehen im Service Trust Portal von Microsoft und sind gegen die tatsächlich genutzten Dienste abzugleichen. Das ist nicht Teil der Entra-ID-Überprüfung, gehört aber in dieselbe Mappe. Details im Beitrag § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen.

Wichtig: Überprüfung ist kein Penetrationstest

Eine Entra-ID-Überprüfung prüft Konfiguration und Bestand, sie greift nichts an. Sie ersetzt weder einen Penetrationstest noch ein Audit nach BSIG oder eine Prüfung gegen den B3S. Sie ist aber die Grundlage, auf der diese Prüfungen deutlich weniger Überraschungen bringen.

Vom Bericht zum Regelbetrieb: der Maßnahmenplan

Der Bericht ist der Anfang, nicht das Ende. Erfahrungsgemäß lassen sich die Maßnahmen in drei Horizonte ordnen, die sich auch gegenüber der Geschäftsführung gut erklären lassen.

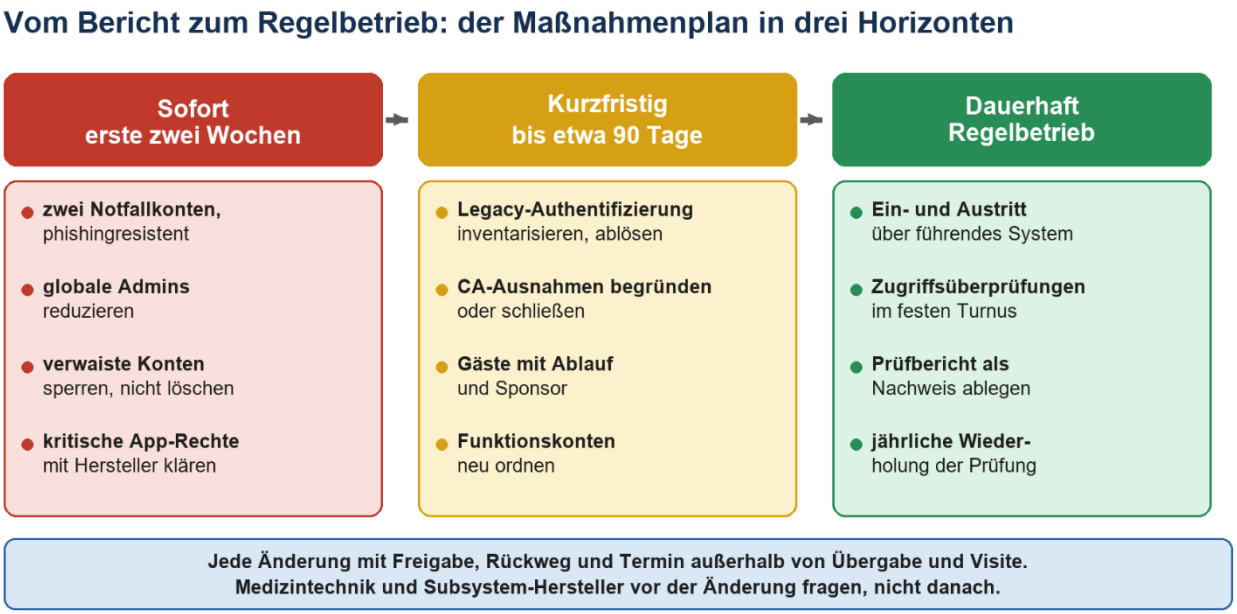


Abbildung 5: Der Maßnahmenplan in drei Horizonten. Die Zeiträume sind Richtwerte und hängen von Größe und Personalausstattung der Klinik-IT ab.

Sofort: die kritischen Punkte

In den ersten Tagen geht es um das, was ein einzelner Angreifer ausnutzen könnte, um den ganzen Tenant zu übernehmen, und um die Fähigkeit, im Notfall handlungsfähig zu bleiben. Zwei Notfallkonten nach Microsoft-Empfehlung, getestet und mit Alarm. Die Zahl der globalen Administratoren auf das Nötige reduziert, alle Admin-Konten mit starker Anmeldung. Konten ausgeschiedener Personen gesperrt. App-Registrierungen mit Verzeichnis- oder Postfach-Vollzugriff mit dem Hersteller besprochen und, wo möglich, auf die tatsächlich benötigten Rechte zurückgeschnitten.

Kurzfristig: die mittleren Punkte

In den folgenden Wochen kommen die Themen, die Abstimmung brauchen. Legacy-Authentifizierung wird gemeinsam mit Medizintechnik und Haustechnik abgelöst, Gerät für Gerät, mit Blick auf das Ende der Basisauthentifizierung bei SMTP AUTH. Ausnahmen in Conditional Access bekommen eine Begründung, einen Besitzer und ein Ablaufdatum, oder sie verschwinden. Gastkonten bekommen einen Sponsor im Haus und eine Befristung. Wo NTLM und Kerberos im lokalen Netz eine Rolle spielen, hilft der Beitrag NTLM abschalten im Krankenhaus: Medizingeräte, Altanwendungen und Kerberos.

Dauerhaft: damit es nicht wieder wächst

Der wichtigste Teil ist der unsichtbare. Ein Tenant, der einmal aufgeräumt ist, verwildert wieder, wenn die Prozesse dahinter bleiben, wie sie waren. Deshalb gehören in den Maßnahmenplan auch organisatorische Punkte: ein Eintritts- und Austrittsprozess, der Honorarkräfte und Leiharbeit einschließt; eine Regel, dass Gäste immer einen Sponsor und ein Enddatum haben; eine Freigabe für neue App-Registrierungen, bei der jemand die Berechtigungen liest; regelmäßige Zugriffsüberprüfungen, die laut Microsoft Entra ID Governance oder die Entra Suite voraussetzen, oder als Alternative ein dokumentierter manueller Turnus. Wer das als Verfahrensanweisung im

QM-Handbuch verankert, hat zugleich einen Nachweis für das nächste Zertifizierungsaudit nach KTQ oder ISO 9001.

Rolle im Haus	Beitrag zur Überprüfung und zum Maßnahmenplan
Geschäftsführung	Auftrag, Priorität, Freigabe des Maßnahmenplans
IT-Leitung und Administration	Zugang, technische Zuordnung, Umsetzung
Informationssicherheitsbeauftragte	Bewertung, Einbindung in ISMS und B3S-Unterlagen
Datenschutzbeauftragte	Zweckbindung und Löschung der Prüfdaten, Bewertung von Teams mit Gästen
Personalabteilung	Abgleich von Ein- und Austritten, Honorarkräften und Leiharbeit
Medizintechnik und Subsystem-Verantwortliche	Zuordnung von Funktionskonten, Altgeräten und App-Registrierungen
Qualitätsmanagementbeauftragte	Überführung der Prozesse in Verfahrensanweisungen
Betriebsrat, Personalrat oder MAV	Beteiligung bei Auswertung von Protokolldaten und bei neuen Kontrollprozessen

Fachliche Vertiefung zu Identitäten, Rollen und Conditional Access gibt es im Kompetenzbereich Microsoft Entra ID und im Kompetenzbereich Microsoft 365 Security. Wer das Thema NIS2 breiter technisch angehen will, findet den Überblick unter NIS2 technisch umsetzen mit Microsoft 365. Damit das eigene Team die Ergebnisse im Alltag halten kann, lohnt eine Microsoft-365-Schulung für Krankenhäuser für Administration und Rufbereitschaft.

Häufige Fragen zur Entra-ID-Überprüfung im Krankenhaus

Verändert die Überprüfung etwas in unserem Tenant?

Nein. Bis zum Maßnahmenplan wird ausschließlich gelesen, typischerweise mit der Rolle Global Reader. Einzige Ausnahme kann die einmalige Zustimmung zu Leseberechtigungen eines Prüfwerkzeugs sein, die Ihre IT selbst erteilt und wieder entziehen kann. Änderungen erfolgen erst nach Freigabe des Maßnahmenplans.

Wie lange dauert eine Überprüfung?

Das hängt von Größe, Zahl der Standorte und vor allem davon ab, wie schnell Personalwesen und Medizintechnik beim Abgleich helfen können. Die technische Erhebung ist meist schnell erledigt; die Zuordnung im Haus braucht die meiste Zeit. Planen Sie die Termine nicht in die Hochphase eines Zertifizierungsaudits oder einer KIS-Umstellung.

Brauchen wir dafür bestimmte Lizenzen?

Für die Erhebung selbst nicht unbedingt. Einige Informationen, etwa das letzte Anmeldedatum per Graph oder Protokolle über 30 Tage, setzen laut Microsoft Premium-Lizenzen von Entra ID voraus. Für die dauerhaften Maßnahmen wie Privileged Identity Management oder automatisierte Zugriffsüberprüfungen nennt Microsoft Entra ID P2 beziehungsweise Entra ID Governance. Welche Lizenzen Sie tatsächlich haben, ist Teil der Bestandsaufnahme.

Sehen Sie bei der Prüfung Patientendaten?

Die Überprüfung betrachtet Konten, Rollen, Gäste, Anwendungen, Richtlinien und Protokolle, nicht Inhalte. Postfächer, Dateien und Chats werden nicht geöffnet. Wo der Bericht auf Teams mit Gästen und sensiblen Freigaben hinweist, klären Datenschutzbeauftragte und Fachbereich, was dort liegt.

Müssen wir die Interessenvertretung beteiligen?

Das hängt von Trägerschaft, Bundesland und Ausgestaltung ab und ist keine Frage, die dieser Beitrag rechtsverbindlich beantworten kann. Weil Anmeldeprotokolle Rückschlüsse auf einzelne Menschen zulassen, ist eine frühe Information von Betriebsrat, Personalrat oder Mitarbeitervertretung in jedem Fall sinnvoll.

Warum nicht einfach alle inaktiven Konten löschen?

Weil inaktiv nicht gleich überflüssig ist. Hinter einem inaktiven Konto kann eine Ärztin in Elternzeit stehen, ein Funktionskonto für ein Gerät, das nur einmal im Quartal sendet, oder ein Postfach, das aus Aufbewahrungsgründen erhalten bleiben muss. Deshalb wird erst abgeglichen, dann gesperrt, und erst nach einer Karenzzeit gelöscht.

Gilt das auch für Rehakliniken und Universitätsklinika?

Ja. Die Befunde ähneln sich über alle Trägerschaften und Versorgungsformen hinweg. Universitätsklinika haben zusätzlich oft Verflechtungen mit dem Tenant der Hochschule, Rehakliniken häufig besonders viele externe Dienstleister. Arztpraxen, Pflegeheime und ambulante Dienste haben andere Rahmenbedingungen und sind nicht Gegenstand dieses Beitrags.

Wie oft sollten wir die Überprüfung wiederholen?

Eine vollständige Überprüfung einmal im Jahr hat sich bewährt, dazu die laufenden Prüfungen aus dem Maßnahmenplan, etwa die Funktionsprüfung der Notfallkonten, die Microsoft mindestens alle 90 Tage empfiehlt. Nach Fusionen, Trägerwechseln oder großen Projekten lohnt eine zusätzliche Runde.

Fazit: Wildwuchs ist normal, ihn zu ignorieren nicht

Kein Klinik-Tenant ist nach Jahren im Betrieb sauber, und das ist keine Schande. Die Konten ausgeschiedener Ärzte, die Gäste aus dem Pandemieprojekt, die App des Subsystem-Herstellers und die Ausnahme für die Stationsrechner haben alle eine Geschichte, die zu ihrer Zeit vernünftig war. Problematisch wird es, wenn niemand mehr weiß, dass es sie gibt.

Eine Entra-ID-Überprüfung schafft dieses Wissen. Sie arbeitet rein lesend, stützt sich auf Werkzeuge statt auf Klickarbeit, bewertet nüchtern nach kritisch, mittel und niedrig und endet in einem Maßnahmenplan, den die Klinik-IT umsetzen und die Geschäftsführung verantworten kann. Nebenbei entsteht genau die Art von Dokumentation, die bei Nachweisen nach § 391 SGB V, gegenüber dem BSI oder im nächsten Zertifizierungsaudit hilft. Und mit etwas Glück findet sich dabei auch das Notfallkonto, bevor man es braucht.

Weiter im Thema

› Microsoft 365 im Krankenhaus

› Microsoft-365-Beratung für Krankenhäuser

› Klinikverbund und Tenant-Strategie: Ein Mandant, mehrere Häuser, gewachsene Domänen

› Anmeldung am Stationsarbeitsplatz: Citrix, Entra ID, Karte und schneller Benutzerwechsel

› NIS2, § 391 SGB V und B3S: Was die Sicherheitspflichten für Microsoft 365 bedeuten

› Active Directory im Klinikverbund: Vertrauensstellungen, Altdomänen und der Weg zur Konsolidierung

› Kompetenzbereich Microsoft Entra ID