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



NIS2, § 391 SGB V und B3S: drei Regelwerke, ein Tenant.

Wissen	Beratung	Schulung
Alle Beiträge der Serie im Überblick:	Pflichten einordnen, Tenant prüfen, Maßnahmen priorisieren:	Sensibilisierung und Admin-Wissen für Ihr Haus:
› Microsoft 365 im Krankenhaus	**› Microsoft-365-Beratung für Krankenhäuser**	**› Microsoft-365-Schulung für Krankenhäuser**

Es gibt in der Krankenhaus-IT zwei Sorten von Montagen: solche, an denen das KIS langsam ist, und solche, an denen jemand aus der Geschäftsführung mit einem ausgedruckten Gesetzestext in der Tür steht und fragt, ob „wir das mit NIS2 eigentlich schon haben“. Seit das NIS2-Umsetzungsgesetz am 6. Dezember 2025 in Kraft getreten ist, sind die zweiten Montage deutlich häufiger geworden. Und die ehrliche Antwort lautet fast überall: teilweise. Irgendwo. Wahrscheinlich in einer Excel-Liste des Informationssicherheitsbeauftragten.

Das Problem ist selten mangelnder Wille. Das Problem ist, dass sich die Pflichten überlagern: das neu gefasste BSI-Gesetz (BSIG), der § 391 SGB V, der für Cloud-Dienste einschlägige § 393 SGB V, der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ der Deutschen Krankenhausgesellschaft (B3S), dazu die Medizinprodukte-Betreiberverordnung, die DSGVO und das jeweilige Landesrecht. Jedes Regelwerk hat seine eigene Sprache, seine eigenen Fristen und seine eigenen Fans im Haus. Microsoft 365 sitzt mittendrin – nicht als Patientendatensystem, sondern als das Werkzeug, über das Verwaltung, Gremien, Qualitätsmanagement und Leitungsebene zusammenarbeiten. Und über das sich, wenn man es lässt, ein Angreifer in Ruhe durch den Verbund arbeiten kann.

Dieser Beitrag ist ein Ordnungsartikel. Er sortiert zuerst, welche Pflicht für welches Haus gilt. Dann zeigt er, wo die Anforderungen aus BSIG und B3S konkret in Microsoft 365 ankommen: bei Identitäten und MFA, privilegierten Konten, Protokollierung, Datensicherung, Lieferkette,

Meldepflichten und Schulung. Am Ende steht eine Tabelle, die Sie in die nächste Sitzung mit Geschäftsführung, Informationssicherheitsbeauftragtem und Datenschutzbeauftragtem mitnehmen können. Was er nicht ist: Rechtsberatung. Wo es juristisch wird, sagen wir das.

Auf einen Blick

• NIS2-Umsetzungsgesetz: in Kraft seit 6. Dezember 2025; die Pflichten stehen im neu gefassten BSIG.

• § 391 SGB V (früher § 75c): angemessene Vorkehrungen nach dem Stand der Technik für alle Krankenhäuser, einschließlich verpflichtender Sensibilisierung der Belegschaft – außer für Betreiber kritischer Anlagen, für die das BSIG gilt.

• § 393 SGB V: Sozial- und Gesundheitsdaten in Cloud-Diensten nur mit aktuellem C5-Testat; seit 1. Juli 2025 muss es grundsätzlich ein Typ-2-Testat sein (oder ein gleichwertiges Testat bzw. Zertifikat).

• B3S „Medizinische Versorgung“ der DKG: aktuell Version 1.3.1, redaktionelle Überarbeitung der Version 1.3 vom 10. Oktober 2025; die Eignungsfeststellung des BSI läuft laut BSI bis November 2028.

• Microsoft 365 betrifft vor allem: Identitäten, Admin-Konten, Protokolle, Backup, Lieferkette, Meldeprozess, Schulung.

Der Pflichtendschungel, sortiert: Wer muss eigentlich was?

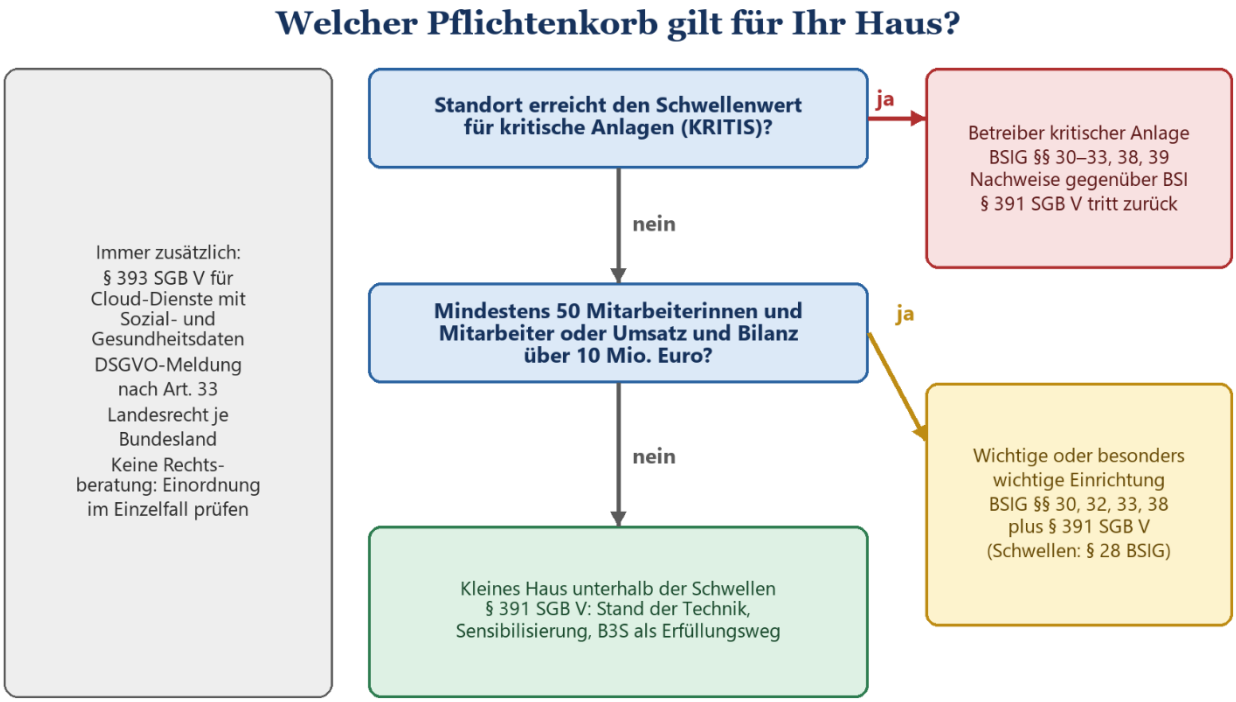
Bevor Sie über Conditional Access diskutieren, lohnt sich eine nüchterne Frage, die erstaunlich oft übersprungen wird: In welchen Pflichtenkorb fällt Ihr Haus? Die Antwort entscheidet darüber, ob Sie dem BSI gegenüber Nachweise führen müssen, ob Ihre Geschäftsführung persönlich in die Pflicht genommen wird und ob Sie einen erheblichen Sicherheitsvorfall binnen 24 Stunden melden müssen. Die technische Antwort im Tenant ist in allen Fällen ähnlich. Die Dokumentationslast und das Haftungsrisiko sind es nicht.

NIS2-Umsetzungsgesetz und BSIG: drei Körbe statt einem

Mit dem NIS2-Umsetzungsgesetz ist das BSIG neu gefasst worden. Statt der alten Zweiteilung „KRITIS oder nicht“ kennt es jetzt Kategorien. **Betreiber kritischer Anlagen** gelten nach § 28 BSIG automatisch als besonders wichtige Einrichtungen. Für alle anderen Einrichtungen aus den gesetzlich gelisteten Sektoren – Krankenhäuser gehören als Gesundheitsdienstleister dazu – entscheiden Größenschwellen: ab 250 Mitarbeiterinnen und Mitarbeitern oder mehr als 50 Mio. Euro Jahresumsatz bei zugleich mehr als 43 Mio. Euro Bilanzsumme „besonders wichtig“, ab 50 Mitarbeiterinnen und Mitarbeitern oder jeweils mehr als 10 Mio. Euro Umsatz und Bilanzsumme „wichtig“. Wer sich die Personalliste eines durchschnittlichen Akutkrankenhauses ansieht, ahnt: Unter 50 bleibt kaum ein Haus. Fach- und Rehakliniken eingeschlossen.

Für die Einordnung als kritische Anlage gilt bei Krankenhäusern seit Jahren ein Schwellenwert von 30.000 vollstationären Fällen pro Jahr, betrachtet je Standort im Sinne der Krankenhausplanung des Landes. Das BMI hat 2026 einen Referentenentwurf für eine neue Verordnung zur Bestimmung kritischer Anlagen vorgelegt; nach der Stellungnahme der DKG soll der Wert für Krankenhäuser dort unverändert bleiben. Prüfen Sie trotzdem vor jeder Entscheidung die dann gültige Fassung – Verordnungen haben die unangenehme Eigenschaft, sich genau dann zu ändern, wenn die Präsentation für den Aufsichtsrat fertig ist.

Für wichtige und besonders wichtige Einrichtungen gelten im Kern: Risikomanagementmaßnahmen nach § 30 BSIG, die Meldepflichten nach § 32, die Registrierung beim BSI nach § 33 und die Pflichten der Geschäftsleitung nach § 38. Betreiber kritischer Anlagen trifft zusätzlich § 31 (unter anderem Systeme zur Angriffserkennung) und die Nachweispflicht nach § 39. Die Registrierungsfrist von drei Monaten nach Eintritt der Betroffenheit ist für die meisten Häuser im Frühjahr 2026 abgelaufen. Wenn bei Ihnen niemand weiß, ob registriert wurde: Das ist der erste Punkt auf der Liste, noch vor jeder Tenant-Einstellung.



Skizze 1: Die Einordnung entscheidet über Nachweise und Haftung, kaum über die Technik.

Kategorie	Typisches Krankenhaus	Rechtsgrundlage	Was das praktisch heißt
Betreiber kritischer Anlage	Großes Haus oder Standort über dem Schwellenwert, häufig Universitätsklinikum oder Maximalversorger	BSIG §§ 28, 30, 31, 32, 33, 38, 39	Nachweise gegenüber dem BSI, Angriffserkennung, Meldepflichten, Haftung und Schulung der Geschäftsleitung. § 391 SGB V tritt zurück.
Besonders wichtige Einrichtung	Akutkrankenhaus oder Klinikverbund ab 250 Mitarbeiterinnen und Mitarbeitern unterhalb des KRITIS-Schwellenwerts	BSIG §§ 28, 30, 32, 33, 38; § 391 SGB V	Risikomanagement, Registrierung, Meldepflichten, Geschäftsleitung in der Pflicht; zusätzlich Stand der Technik und Sensibilisierung nach SGB V.
Wichtige Einrichtung	Kleineres Haus, Fach- oder Rehaklinik ab 50 Mitarbeiterinnen und Mitarbeitern	BSIG §§ 28, 30, 32, 33, 38; § 391 SGB V	Wie oben, mit geringerer Aufsichtsintensität. Die Maßnahmenliste des § 30 BSIG gilt trotzdem vollständig.
Unterhalb der Schwellen	Sehr kleine Einrichtung	§ 391 SGB V	Stand der Technik, Sensibilisierung, B3S als anerkannter Erfüllungsweg.

Keine Rechtsberatung

Ob Ihr Haus eine wichtige oder besonders wichtige Einrichtung ist, hängt an Details: Zurechnung im Konzern oder Klinikverbund, Trägerstruktur, Tochtergesellschaften für Service und IT, Standortbegriff der Landeskrankenhausplanung. Das BSI bietet dafür eine Betroffenheitsprüfung an, die DKG Umsetzungshinweise. Die verbindliche Einordnung gehört in die Hände Ihrer Rechtsabteilung oder einer spezialisierten Kanzlei – nicht in einen Fachartikel und auch nicht in ein Teams-Chat mit der IT.

§ 391 SGB V: die Pflicht, die für alle anderen gilt

§ 391 SGB V ist die Nachfolgeregelung des früheren § 75c und im Zuge der NIS2-Umsetzung neu gefasst worden. Er verlangt von Krankenhäusern angemessene organisatorische und technische Vorkehrungen nach dem Stand der Technik, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse zu vermeiden, soweit diese für den Krankenhausbetrieb und den Schutz der Patientendaten maßgeblich sind. Neu und ausdrücklich: Zu den Vorkehrungen gehören verpflichtende Maßnahmen zur Steigerung des Sicherheitsbewusstseins der Belegschaft. Schulung ist damit keine Kür mehr, sondern Gesetzespflicht.

Angemessen ist eine Vorkehrung, wenn ihr Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder zum Schutzbedarf der Patientendaten steht. Erfüllt werden kann die Pflicht unter anderem über einen branchenspezifischen Sicherheitsstandard, dessen Eignung das BSI nach § 30 Abs. 8 BSIG festgestellt hat – also über den B3S. Und: Die Pflicht gilt für alle Krankenhäuser, ausgenommen Betreiber kritischer Anlagen, die ohnehin den §§ 30, 31 und 39 BSIG unterliegen. Das heißt umgekehrt: Ein Haus, das als wichtige oder besonders wichtige Einrichtung unter das BSIG fällt, aber keine kritische Anlage betreibt, hat beide Regelwerke auf dem Tisch. Die gute Nachricht: Die Maßnahmen überschneiden sich fast vollständig. Wer sauber nach B3S arbeitet, bedient beide.

§ 393 SGB V: Cloud nur mit Testat

Für Microsoft 365 besonders relevant ist § 393 SGB V. Er regelt, unter welchen Bedingungen Sozial- und Gesundheitsdaten in Cloud-Diensten verarbeitet werden dürfen. Neben angemessenen Maßnahmen nach dem Stand der Technik verlangt er ein aktuelles C5-Testat für die eingesetzten Cloud-Systeme, bezogen auf die C5-Basiskriterien, und – das wird gern überlesen – die Umsetzung der im Prüfbericht genannten kundenseitigen Kriterien. Seit dem 1. Juli 2025 gilt grundsätzlich nur noch ein Typ-2-Testat als aktuell; alternativ ein anderes Testat oder Zertifikat, das ein vergleichbares oder höheres Sicherheitsniveau gewährleistet und per Verordnung bestimmt werden kann.

Prüfauftrag statt Behauptung

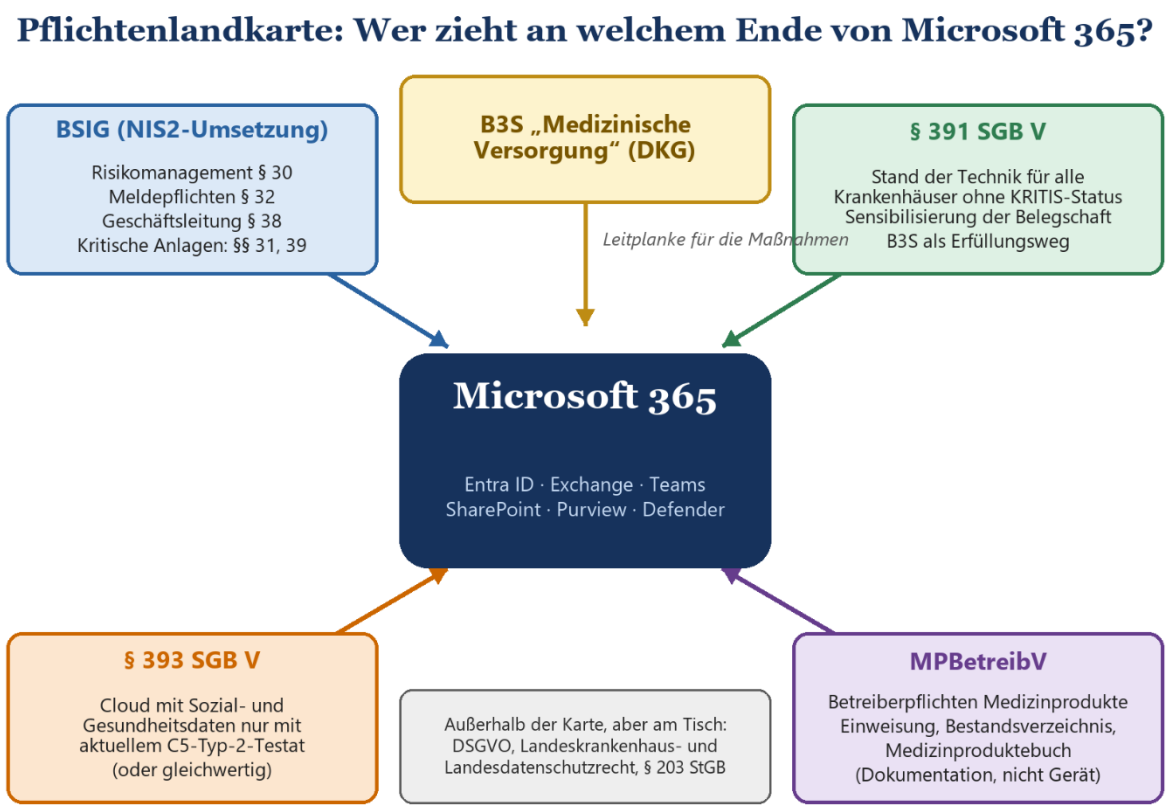
Welche Microsoft-Dienste von welchem C5-Testat welchen Typs in welchem Zeitraum abgedeckt sind, steht im Testat selbst – abrufbar im Microsoft Service Trust Portal. Verlassen Sie sich nicht auf Folien, Vertriebsaussagen oder diesen Artikel. Laden Sie das aktuelle Testat herunter, gleichen Sie den Dienstumfang mit Ihrer tatsächlichen Nutzung ab (Exchange Online, SharePoint, Teams, Copilot, Backup, Defender) und dokumentieren Sie die kundenseitigen Kriterien, die Sie umgesetzt haben. Diese Liste ist Ihr Nachweis, nicht das Testat allein.

Die Details zur Prüfung stehen im Beitrag § 393 SGB V und C5-Testat: Was Krankenhäuser beim Cloud-Einsatz nachweisen müssen.

Und weil die Frage sofort kommt: Ob überhaupt Gesundheitsdaten in Microsoft 365 landen sollen, ist eine Architekturfrage, keine Testatfrage. Unsere Grundhaltung ist eindeutig: Patientendaten gehören ins KIS und seine Subsysteme wie LIS, RIS und PACS. Microsoft 365 ist das Werkzeug für Verwaltung, Organisation, Qualitätsmanagement und Zusammenarbeit. Wo die Grenze verläuft und warum sie in der Praxis trotzdem ständig überschritten wird, beschreibt der Beitrag Patientendaten und Microsoft 365: Wo das KIS endet und das Office anfängt. Zur strafrechtlichen Seite und zum Landesrecht siehe Schweigepflicht und Cloud: § 203 StGB, Landeskrankenhausgesetze und Auftragsverarbeitung.

MPBetreibV und Medizintechnik: der Nachbar am Zaun

Die Medizinprodukte-Betreiberverordnung regelt nicht die IT-Sicherheit von Microsoft 365. Sie gehört trotzdem auf die Landkarte, weil sie im Krankenhaus dieselben Netze, dieselben Konten und oft dieselben Menschen betrifft. Medizintechnik und IT teilen sich Netzsegmente, Fernwartungszugänge und Dienstkonten, und die Dokumentation zu Einweisungen, Bestandsverzeichnis und Medizinproduktebuch landet zunehmend in SharePoint oder einer CAFM-Anwendung. Wer in der Medizintechnik Altgeräte betreibt, die nur NTLM sprechen oder ein Dienstkonto mit nie ablaufendem Kennwort brauchen, weiß, wie schnell eine Betreiberpflicht und eine Härtungsmaßnahme kollidieren. Aus unserer Projekterfahrung in einem Krankenhausverbund mit mehreren Standorten: Die NTLM-Abschaltung scheitert selten an Windows, sondern fast immer an genau diesen Geräten und den zugehörigen Anwendungen. Das ist kein Microsoft-365-Thema im engeren Sinn – aber ein Angreifer, der über ein Cloud-Konto in die lokale Domäne kommt, interessiert sich herzlich wenig für Zuständigkeitsgrenzen.



Skizze 2: Pflichtenlandkarte – Microsoft 365 in der Mitte, der B3S als Leitplanke.

Landesrecht unterscheidet sich

Landeskrankenhausgesetze, Landesdatenschutzgesetze und das Personalvertretungsrecht sind in

jedem Bundesland anders geregelt. Manche Landeskrankenhausgesetze enthalten eigene Vorgaben zur Verarbeitung von Patientendaten durch Dritte, andere verweisen weitgehend auf die DSGVO. Für kirchliche Häuser kommen KDG oder DSG-EKD hinzu. Kein Land ist der Normalfall – prüfen Sie die für Ihren Standort geltende Fassung, im Klinikverbund über Landesgrenzen hinweg gegebenenfalls mehrere.

Der B3S „Medizinische Versorgung“: Übersetzungshilfe zwischen Gesetz und Tenant

Gesetze sagen „Stand der Technik“ und meinen damit alles und nichts. Der branchenspezifische Sicherheitsstandard der DKG ist der Versuch, daraus etwas zu machen, das ein Krankenhaus tatsächlich umsetzen kann. Er beschreibt Anforderungen in Umsetzungsgraden, ordnet sie den kritischen Prozessen der stationären Versorgung zu und liefert über Mapping-Tabellen den Anschluss an die Vorgängerversionen. Das BSI hat die Eignung festgestellt, und genau deshalb ist der B3S für § 391 SGB V ein anerkannter Erfüllungsweg und für Betreiber kritischer Anlagen die naheliegende Prüfgrundlage.

B3S „Medizinische Versorgung“ – Stand

• Herausgeber: Deutsche Krankenhausgesellschaft (DKG).

• Aktuelle Fassung: Version 1.3.1, eine in Abstimmung mit dem BSI erstellte redaktionelle Überarbeitung der Version 1.3 mit Stand 10. Oktober 2025.

• Eignungsfeststellung durch das BSI: für Version 1.3 im November 2025, befristet auf drei Jahre; das BSI führt den B3S Krankenhaus mit Ablauf der Eignungsfeststellung im November 2028.

• Die DKG stellt Reinfassung, Änderungsfassung und eine Mapping-Tabelle zur Vorversion bereit, dazu ein Starter-Paket für § 391 SGB V.

Für Microsoft 365 gilt allerdings: Der B3S ist produktneutral. Er sagt Ihnen, dass Sie Identitäten sicher verwalten, privilegierte Zugänge besonders schützen, Ereignisse protokollieren, Daten sichern und Dienstleister steuern müssen. Er sagt Ihnen nicht, welcher Schalter im Entra Admin Center das erledigt. Das ist auch richtig so – ein Standard, der Produktmenüs beschreibt, wäre nach dem nächsten Portal-Redesign Altpapier. Die Übersetzungsarbeit bleibt beim Haus.

Was der B3S von Microsoft 365 nicht wissen kann

Drei Dinge fallen in Prüfungen regelmäßig auf, weil der B3S sie implizit voraussetzt, die Praxis aber anders aussieht:

- **Geteilte Verantwortung.** Microsoft betreibt die Plattform, das Krankenhaus konfiguriert sie. Für Rechenzentrum, Hypervisor und Dienstverfügbarkeit gibt es Testate. Für die Frage, ob Ihr Globaler Administrator MFA nutzt, gibt es nur Sie.
- **Hybride Identität.** Fast jedes Krankenhaus synchronisiert sein lokales Active Directory nach Entra ID. Ein kompromittiertes On-Premises-Konto mit Cloud-Rechten ist damit eine Brücke in beide Richtungen. Kerberos, NTLM, PKI und Vertrauensstellungen zwischen Altdomänen im Verbund gehören deshalb mit auf die Liste.
- **Schatten-Datenhaltung.** Der B3S geht davon aus, dass Sie wissen, wo schützenswerte Daten liegen. Die Excel-Liste mit Belegungsübersicht und Patientennamen im Teams-Kanal der Station hält sich nicht an diese Annahme.

Ein Mapping, das Prüfer mögen

Legen Sie in Ihrem ISMS eine Zuordnung an: B3S-Anforderung, betroffener Microsoft-365-Dienst, umgesetzte Konfiguration, Nachweisquelle (Bericht, Export, Screenshot mit Datum), verantwortliche Rolle. Microsoft Secure Score und die Empfehlungen im Microsoft Purview-Portal liefern Rohmaterial, ersetzen das Mapping aber nicht. Im QM-Handbuch abgelegt und gelenkt wie jede andere Verfahrensanweisung, besteht das Ding auch das nächste Zertifizierungsaudit.

Wo Microsoft 365 betroffen ist: sieben Pflichtfelder und ihre Bordmittel

Jetzt zum eigentlichen Kern. Die Mindestmaßnahmen des § 30 Abs. 2 BSIG reichen von Risikoanalyse über Bewältigung von Sicherheitsvorfällen, Betriebskontinuität und Backup, Lieferkette, Schwachstellenmanagement, Wirksamkeitsprüfung, Schulung und Kryptografie bis zu Zugriffskontrolle sowie Multi-Faktor-Authentifizierung und gesicherter Notfallkommunikation. Der B3S bricht das für Krankenhäuser herunter. In Microsoft 365 landen davon sieben Felder mit voller Wucht. Für jedes gilt: Die Technik ist meist schon im Tenant, die Organisation drumherum fast nie.

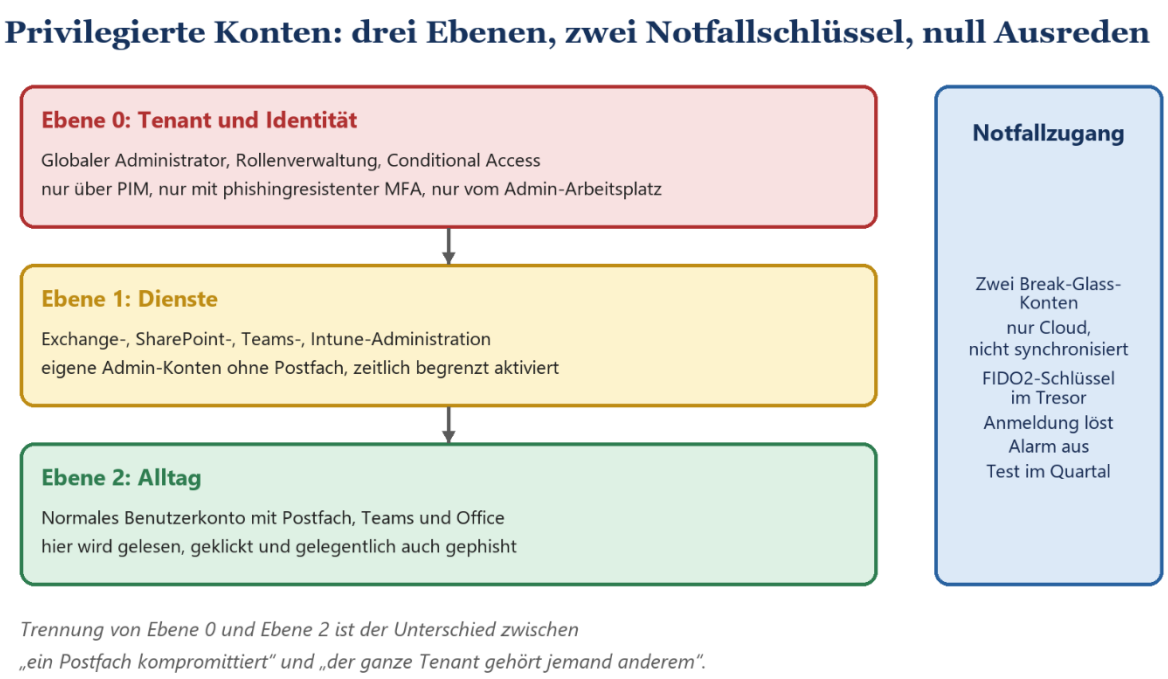
1. Identitäten und MFA

Das Gesetz nennt Multi-Faktor-Authentifizierung ausdrücklich. Das ist bemerkenswert, weil Gesetze selten so konkret werden – und es ist ein Hinweis darauf, wo die meisten Vorfälle beginnen. In Microsoft 365 heißt das: MFA für alle Konten, ohne Ausnahme für „die Chefärzte, die sich beschwert haben“. Die Sicherheitsstandards von Entra ID sind das Minimum ohne Zusatzlizenz; sinnvoll steuerbar wird es erst mit Conditional Access, das eine Entra ID P1 voraussetzt. Damit lassen sich Altprotokolle blockieren, Anmeldungen auf verwaltete Geräte beschränken und Ausnahmen sauber dokumentieren.

Die Krankenhausrealität macht es nicht einfacher: gemeinsam genutzte Stationsrechner, Schichtdienst, Visite mit dem Tablet, Rufbereitschaft vom privaten Smartphone aus. Für Frontline-Szenarien gibt es eigene Lösungen, für Ärzte in der Rufbereitschaft die Authenticator-App oder FIDO2-Schlüssel. Wichtig ist, dass die Ausnahmen bewusst entschieden und aufgeschrieben werden – nicht, dass es keine gibt. Ein Konto ohne MFA, weil „das Gerät im OP das nicht kann“, ist eine vertretbare Ausnahme, wenn das Konto nichts anderes darf. Es ist ein Einfallstor, wenn es zufällig auch ein Postfach und Lesezugriff auf das Gremien-Team der Geschäftsführung hat.

2. Privilegierte Konten

Wenn es im Tenant eine einzige Maßnahme gibt, die den Unterschied zwischen einem ärgerlichen und einem existenzbedrohenden Vorfall macht, dann ist es die Trennung privilegierter Konten. Admin-Rollen gehören auf eigene Konten ohne Postfach, werden über Privileged Identity Management nur bei Bedarf und zeitlich begrenzt aktiviert und verlangen eine phishingresistente Anmeldung. PIM erfordert Entra ID P2 beziehungsweise eine Lizenz aus Entra ID Governance. Dazu kommen zwei Notfallkonten, die nur in der Cloud existieren, nicht synchronisiert sind und deren Anmeldung einen Alarm auslöst.



Skizze 3: Ebenenmodell für Admin-Konten mit Notfallzugang.

In gewachsenen Klinik-Tenants findet sich bei der ersten Überprüfung fast immer dasselbe Bild: zu viele Globale Administratoren, darunter ein ehemaliger Dienstleister, ein Funktionspostfach und ein Konto, das „nur für die Migration damals" angelegt wurde. Das ist kein Vorwurf, das ist Physik – Berechtigungen wachsen, wenn niemand sie aktiv zurückschneidet. Die Geschäftsführung muss nach § 38 BSIG die Umsetzung der Risikomanagementmaßnahmen überwachen. Eine Liste der aktiven Admin-Rollen, quartalsweise vorgelegt, ist dafür ein erstaunlich wirksames Instrument.

3. Protokollierung

Ohne Protokolle keine Erkennung, ohne Erkennung keine Meldung, ohne Meldung ein Problem mit dem BSI. Microsoft 365 schreibt mit Microsoft Purview Audit (Standard) ein einheitliches Überwachungsprotokoll; seit Oktober 2023 werden diese Einträge standardmäßig 180 Tage aufbewahrt. Audit (Premium) hält Einträge aus Exchange, SharePoint, OneDrive und Entra ID für Benutzer mit E5-Lizenz (oder dem passenden Compliance-Add-on) ein Jahr vor, mit Zusatzlizenz bis zu zehn Jahre. Die Anmeldeprotokolle von Entra ID werden im Portal nur vergleichsweise kurz vorgehalten; wer länger zurückblicken will – und nach einem Vorfall will man das immer –, exportiert sie nach Log Analytics oder Microsoft Sentinel.

Betreiber kritischer Anlagen müssen nach § 31 BSIG Systeme zur Angriffserkennung einsetzen. Microsoft Defender XDR und Sentinel sind dafür im Microsoft-Umfeld die naheliegenden Bausteine, ein bestehendes SIEM oder ein Security-Operations-Dienstleister die andere Variante. Entscheidend ist nicht das Produkt, sondern die Frage, wer um drei Uhr nachts auf den Alarm schaut. Rufbereitschaft kennt das Krankenhaus – für die IT-Sicherheit ist sie erstaunlich oft nicht geregelt.

Protokolle sind auch Leistungsdaten

Audit-Protokolle, Anmeldeprotokolle und die Ergebnisse von Phishing-Simulationen sind technisch geeignet, Verhalten und Leistung von Mitarbeiterinnen und Mitarbeitern zu überwachen. Damit sind je nach Trägerschaft Betriebsrat, Personalrat oder Mitarbeitervertretung zu beteiligen. Regeln Sie Zweck, Zugriff und Auswertung vor der Einführung in einer Dienst- oder Betriebsvereinbarung, sonst steht die Sicherheitsmaßnahme

schneller wieder still, als sie eingeschaltet war.

Mehr dazu: Betriebsrat, Personalrat oder MAV: Mitbestimmung bei Microsoft 365 je nach Trägerschaft.

4. Datensicherung und Wiederherstellung

Microsoft 365 ist hochverfügbar. Das ist nicht dasselbe wie gesichert. Gegen den Ausfall eines Rechenzentrums schützt Microsoft, gegen einen Administrator mit kompromittiertem Konto, der Aufbewahrungsrichtlinien löscht und SharePoint-Bibliotheken leert, schützt nur ein durchdachtes Konzept. Bordmittel sind Aufbewahrungsrichtlinien in Purview, Papierkörbe, Versionierung und Microsoft 365 Backup, das verbrauchsabhängig über ein Azure-Abonnement abgerechnet wird. Daneben gibt es Drittanbieter-Lösungen, die dann allerdings selbst Teil Ihrer Lieferkette und Ihres C5-Prüfauftrags werden.

Der B3S und § 30 BSIG verlangen nicht nur Backup, sondern Notfallwiederherstellung und Krisenmanagement. Die Frage ist also nicht „Haben wir ein Backup?“, sondern „Wie lange dauert es, das QM-Handbuch, die Gremienunterlagen und die Postfächer der Geschäftsführung wiederherzustellen, und wer hat das zuletzt ausprobiert?“ Ein Restore-Test ohne Protokoll ist für den Prüfer ein Gerücht. Und in einem echten Ransomware-Szenario ist Microsoft 365 oft das Erste, was wieder läuft – und damit der Kommunikationskanal für den Notbetrieb. Dafür muss es aber einen Zugangsweg geben, der nicht über die gerade verschlüsselte lokale Domäne führt.

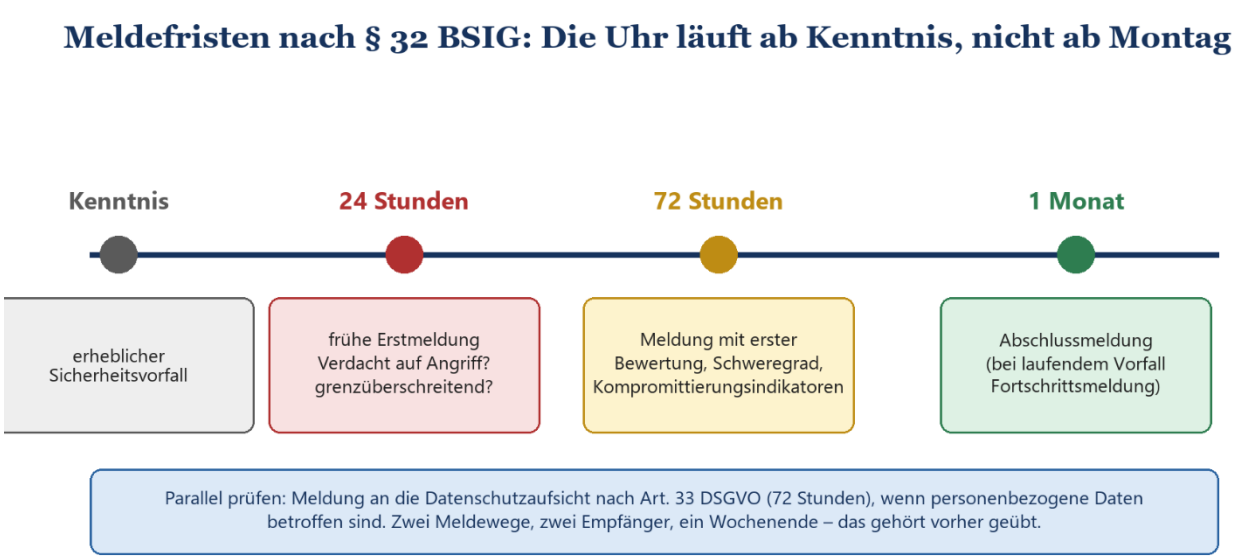
5. Lieferkette

Die Lieferkette eines Krankenhauses ist lang: KIS-Hersteller, Subsystem-Anbieter, Medizintechnik mit Fernwartung, Dienstleister für Netzwerk, Druck und Telefonie, dazu Microsoft selbst. § 30 BSIG verlangt ausdrücklich, sicherheitsbezogene Aspekte in den Beziehungen zu direkten Anbietern und Dienstleistern zu berücksichtigen. Für Microsoft als Lieferanten heißt das: Testate und Berichte aus dem Service Trust Portal sichten, den Auftragsverarbeitungsvertrag (Data Protection Addendum) ablegen, Datenspeicherorte und EU-Datengrenze dokumentieren und den C5-Prüfauftrag nach § 393 SGB V abarbeiten.

Im Tenant selbst ist die Lieferkette greifbarer, als vielen bewusst ist: Gastkonten von Dienstleistern, Enterprise-Apps mit weitreichenden Berechtigungen, die irgendwann jemand per Einwilligung zugelassen hat, Partnerbeziehungen mit delegierten Admin-Rechten. Bordmittel sind die Einstellungen für mandantenübergreifenden Zugriff, die Einschränkung der Benutzereinwilligung für Apps, Zugriffsüberprüfungen (mit Entra ID Governance beziehungsweise P2) und die Überprüfung granularer delegierter Administratorrechte von Partnern. Ein Fernwartungszugang für den KIS-Hersteller gehört nicht in Microsoft 365, sondern in einen eigenen, protokollierten Zugangsweg – aber die E-Mail, mit der der Hersteller das Update ankündigt, landet sehr wohl in Exchange und ist ein beliebtes Phishing-Motiv.

6. Meldepflichten

§ 32 BSIG sieht für erhebliche Sicherheitsvorfälle ein dreistufiges Verfahren an die gemeinsame Meldestelle von BSI und BBK vor: eine frühe Erstmeldung spätestens 24 Stunden nach Kenntnis, eine Meldung mit erster Bewertung spätestens nach 72 Stunden und eine Abschlussmeldung spätestens einen Monat danach. Betreiber kritischer Anlagen machen zusätzlich Angaben zur betroffenen Anlage. Parallel läuft gegebenenfalls die Datenschutzmeldung nach Art. 33 DSGVO.



Skizze 4: Meldefristen nach § 32 BSIG – die Uhr startet mit der Kenntnis.

Microsoft 365 liefert dafür die Erkennung und die Fakten: Vorfälle und Warnungen im Defender-Portal, das Überwachungsprotokoll für die Rekonstruktion, Kompromittierungsindikatoren aus E-Mail und Endpunkt. Was es nicht liefert: die Entscheidung, ob ein Vorfall „erheblich" ist, die Person mit Vertretungsregelung, die die Meldung abgibt, und die Zugangsdaten zum Meldeportal, die nicht im verschlüsselten Passwortsafe auf dem verschlüsselten Server liegen. Unsere Erfahrung aus forensischen Einsätzen: Die ersten 24 Stunden vergehen schneller, als man „Wer hat eigentlich den Schlüssel für den Serverraum?" sagen kann. Notfallkommunikation – das Gesetz nennt sie ausdrücklich – heißt im Krankenhaus auch: Die Klinik-TK-Anlage bleibt für Station, DECT und Zentrale führend, und eine Telefonliste auf Papier hat noch nie ein Kennwort vergessen.

7. Schulung und Sensibilisierung

§ 391 SGB V macht Sensibilisierung der Belegschaft zur Pflicht, § 30 BSIG verlangt grundlegende Schulungen, und § 38 Abs. 3 BSIG verpflichtet die Geschäftsleitung, selbst regelmäßig an Schulungen teilzunehmen. Letzteres ist der Teil, der in Krankenhäusern die meisten Kalender-Einladungen ohne Antwort produziert. Die Geschäftsführung muss Risiken erkennen und bewerten können – das ist kein Grundkurs „Was ist Phishing", sondern ein Format auf Augenhöhe mit Szenarien aus dem eigenen Haus.

Für die Belegschaft bietet Microsoft 365 die Angriffssimulation in Defender for Office 365. Laut Microsoft setzt sie Microsoft 365 E5 oder Defender for Office 365 Plan 2 voraus; E3-Kunden steht nur ein eng begrenzter Testumfang zur Verfügung. Simulationen sind nützlich, wenn sie mit Schulung verbunden und mitbestimmt eingeführt werden, und schädlich, wenn sie als Pranger wahrgenommen werden. Für Pflegekräfte im Schichtdienst funktionieren kurze Lerneinheiten am Stationsrechner oder im Rahmen der Pflichtfortbildung besser als die einstündige Präsenzschulung, zu der wegen Personalmangel niemand kommen kann. Ärzte erreichen Sie am ehesten über konkrete Fälle: die gefälschte Mail der Fachgesellschaft, die vermeintliche Kongresseinladung, die Rechnung eines Medizinprodukte-Lieferanten.

Schulung, die im Schichtplan Platz hat

Bauen Sie Sensibilisierung in vorhandene Formate ein: Pflichtunterweisungen, Einarbeitungskonzept neuer Mitarbeiterinnen und Mitarbeiter, Stationsleitungsrunde, Chefarztkonferenz. Dokumentieren Sie Teilnahme und Inhalte so, wie Sie es von Hygieneschulungen kennen – dann ist der Nachweis für § 391 SGB V und B3S gleich mit erledigt.

Formate für Krankenhäuser finden Sie unter Microsoft-365-Schulung für Krankenhäuser.

Die Übersicht: Anforderung, Bordmittel, Lizenz, Organisation

Die folgende Tabelle fasst die sieben Felder zusammen. Die Lizenzangaben beruhen auf der Dokumentation bei Microsoft Learn zum Stand dieses Artikels. Lizenzpläne ändern sich; prüfen Sie vor einer Beschaffung die aktuelle Dienstbeschreibung. Preise nennen wir bewusst nicht.

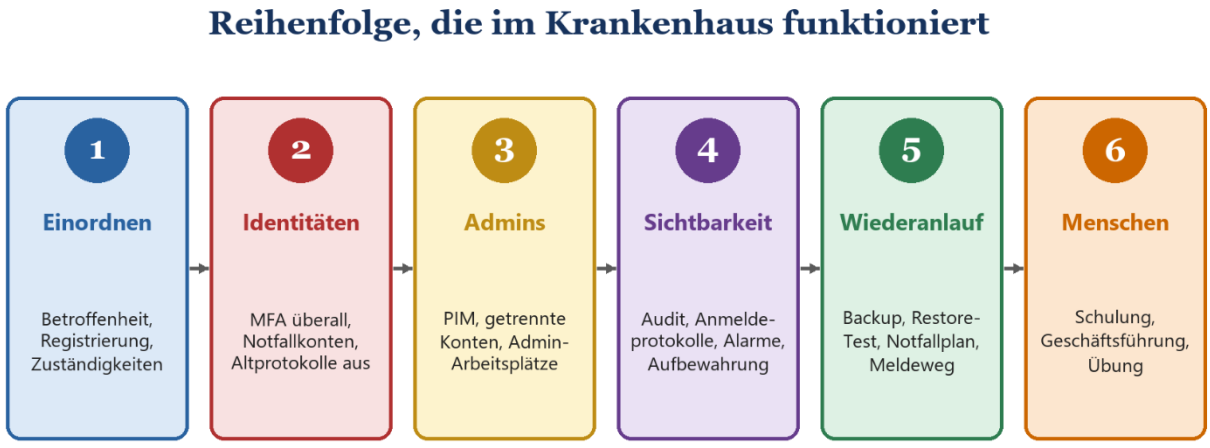
Anforderung (BSIG / B3S)	Microsoft-365-Bordmittel	Lizenzbedarf	Organisatorischer Anteil
Identitäten und MFA	Entra-ID-Sicherheitsstandards, Conditional Access, Authentifizierungsmethoden (Authenticator, FIDO2, Windows Hello), Blockade von Altprotokollen	Sicherheitsstandards ohne Zusatzlizenz; Conditional Access ab Entra ID P1 (z. B. in Microsoft 365 E3 und Business Premium)	Ausnahmeregelung für Stationsrechner und Medizintechnik, Rufbereitschaft, Registrierungsprozess, Verfahrensanweisung
Privilegierte Konten	Getrennte Admin-Konten, Privileged Identity Management, Rollen mit minimalen Rechten, Notfallkonten mit Alarm	PIM mit Entra ID P2 bzw. Entra ID Governance (z. B. in Microsoft 365 E5)	Rollenkonzept, Freigabeprozess, quartalsweise Überprüfung, Vorlage an die Geschäftsführung
Protokollierung und Erkennung	Purview Audit, Entra-Anmeldeprotokolle, Defender XDR, optional Microsoft Sentinel	Audit (Standard) mit 180 Tagen Aufbewahrung; Audit (Premium) mit einem Jahr für E5-Benutzer, bis zehn Jahre mit Add-on; Sentinel verbrauchsabhängig	Wer sichtet Alarme, auch nachts? Mitbestimmung bei Auswertung, Löschkonzept für Protokolle
Datensicherung und Wiederanlauf	Aufbewahrungsrichtlinien, Versionierung, Papierkorb, Microsoft 365 Backup	Aufbewahrung je nach Plan; Microsoft 365 Backup verbrauchsabhängig über Azure	Restore-Tests mit Protokoll, Notfallhandbuch, Zugangsweg unabhängig von der lokalen Domäne
Lieferkette	Service Trust Portal, mandantenübergreifende Zugriffseinstellungen, App-Einwilligung, Zugriffsüberprüfungen, GDAP-Überprüfung	Zugriffsüberprüfungen mit Entra ID P2 bzw. Governance; übrige Einstellungen ohne Zusatzlizenz	Lieferantenverzeichnis, C5-Prüfauftrag nach § 393 SGB V, Vertragsprüfung, Gastkonten-Lebenszyklus
Meldepflichten	Vorfälle und Warnungen im Defender-Portal, Überwachungsprotokoll, Untersuchungswerkzeuge	Umfang der Erkennung hängt an Defender-Plänen (Office 365, Endpoint, Identity)	Meldeprozess 24 h / 72 h / 1 Monat, Erheblichkeitsbewertung, Vertretung, Zugang zum Meldeportal, Datenschutzmeldung
Schulung und Sensibilisierung	Angriffssimulation und Schulungskampagnen in Defender for Office 365	Microsoft 365 E5 oder Defender for Office 365 Plan 2; für E3 nur eingeschränkter Testumfang	Schulungskonzept je Berufsgruppe, Schulung der Geschäftsleitung nach § 38 BSIG, Mitbestimmung, Nachweisführung

Die Excel-Liste im Stationskanal

Sie existiert. Belegungsübersicht, OP-Planung, Übergabeliste – mit Namen, Geburtsdaten und gelegentlich Diagnosen, angelegt aus guter Absicht, weil das KIS die Sicht nicht hergibt, die die Station braucht. Diese Liste ist kein Normalfall und darf keiner werden. Sie ist aber ein Signal: Entweder fehlt eine Funktion im KIS, oder es fehlt eine Regel im Haus. Purview kann solche Dateien mit vertraulichen Informationstypen und Vertraulichkeitsbezeichnungen aufspüren und kennzeichnen. Die Ursache beseitigen muss das Haus – mit der Pflegedirektion, nicht gegen sie.

Vom Pflichtenpapier zur Umsetzung: eine Reihenfolge, die im Haus funktioniert

Die Versuchung ist groß, mit dem spannendsten Teil anzufangen: Sentinel, Automatisierung, schöne Dashboards. Die Erfahrung sagt: Fangen Sie mit dem langweiligsten an. Erst die Einordnung und die Zuständigkeiten, dann die Identitäten, dann die Admins, dann die Sichtbarkeit, dann der Wiederanlauf, und die Menschen von Anfang an mitnehmen. Diese Reihenfolge ist nicht originell, aber sie überlebt den Realitätskontakt mit einem Krankenhaus, in dem die IT nebenbei noch das KIS-Update, die Medizintechnik-Migration und die Rufbereitschaft stemmt.



Skizze 5: Umsetzungsreihenfolge vom Einordnen bis zur Schulung.

Wer im Haus was verantwortet

Rolle	Aufgabe im Kontext NIS2 / § 391 / B3S	Berührung mit Microsoft 365
Geschäftsführung	Lässt Risikomanagementmaßnahmen umsetzen und überwacht sie, nimmt an Schulungen teil, trägt die Haftung	Entscheidet über Lizenzen, Budget, Ausnahmen; erhält quartalsweise Bericht
Informationssicherheitsbeauftragter	ISMS, B3S-Mapping, Risikoanalyse, Meldeprozess	Nachweisquellen aus Secure Score, Audit, Defender
IT-Leitung und Administration	Technische Umsetzung, Betrieb, Erkennung, Wiederherstellung	Konfiguration von Entra ID, Purview, Defender, Backup
Datenschutzbeauftragter	Datenschutzfolgenabschätzung,	Prüft Datenflüsse,

	Auftragsverarbeitung, Art.-33-Meldung	Speicherorte, Protokollzwecke
QMB	Lenkung der Verfahrensanweisungen und Nachweise	Ablage des Mappings und der Verfahrensanweisungen in SharePoint
Medizintechnik	Betreiberpflichten nach MPBetreibV, Fernwartung, Geräteintegration	Dienstkonten, Netzsegmente, Ausnahmen bei MFA und NTLM
Betriebsrat, Personalrat oder MAV	Mitbestimmung bei technischen Einrichtungen zur Verhaltens- und Leistungskontrolle	Protokollierung, Phishing-Simulation, Auswertungen

Für die technische Seite – Conditional-Access-Richtlinien, PIM-Konfiguration, Audit-Aufbewahrung, Defender-Einstellungen – haben wir einen eigenen, ausführlichen Leitfaden geschrieben: NIS2 technisch umsetzen mit Microsoft 365. Der Überblick über Härtung, Erkennung und Reaktion im Microsoft-Umfeld steht im Kompetenzbereich Microsoft 365 Security.

Weiterlesen und vertiefen

› NIS2 technisch umsetzen mit Microsoft 365

› Microsoft 365 Security

› Microsoft Entra ID

› Microsoft Purview

› Kerberos

› PKI mit ADCS

› Microsoft 365 im Krankenhaus: Warum die Klinik anders tickt als Verwaltung und Mittelstand

Wenn Sie die Einordnung, das B3S-Mapping oder eine Überprüfung Ihres Tenants nicht allein stemmen wollen, unterstützen wir Sie mit der Microsoft-365-Beratung für Krankenhäuser – vom Workshop mit Geschäftsführung und Informationssicherheitsbeauftragtem bis zur technischen Prüfung.

FAQ: NIS2 im Krankenhaus und Microsoft 365

Fällt mein Krankenhaus unter NIS2?

Sehr wahrscheinlich ja. Krankenhäuser gehören als Gesundheitsdienstleister zu den im BSIG gelisteten Einrichtungsarten. Ab 50 Mitarbeiterinnen und Mitarbeitern oder mehr als 10 Mio. Euro Umsatz und Bilanzsumme ist ein Haus mindestens wichtige Einrichtung, ab 250 Mitarbeiterinnen und Mitarbeitern oder entsprechendem Umsatz und Bilanzsumme besonders wichtige. Betreiber kritischer Anlagen sind immer besonders wichtig. Die verbindliche Einordnung, insbesondere im Klinikverbund, sollte rechtlich geprüft werden.

Gilt § 391 SGB V zusätzlich zum BSIG?

Für Betreiber kritischer Anlagen nicht – für sie gelten die Pflichten aus dem BSIG. Für alle anderen Krankenhäuser gilt § 391 SGB V, und zwar auch dann, wenn sie als wichtige oder besonders wichtige Einrichtung zusätzlich unter das BSIG fallen. In der Praxis überschneiden sich die Maßnahmen weitgehend; der B3S bedient beide.

Muss ich den B3S anwenden?

Nein, aber es ist der naheliegende Weg. § 391 SGB V nennt den vom BSI als geeignet festgestellten branchenspezifischen Standard ausdrücklich als Möglichkeit, die Pflichten zu erfüllen. Wer einen anderen Weg geht, muss die Angemessenheit selbst begründen.

Welche B3S-Version ist aktuell?

Die DKG stellt den B3S „Medizinische Versorgung“ in Version 1.3.1 bereit, einer redaktionellen Überarbeitung der Version 1.3 mit Stand 10. Oktober 2025. Prüfen Sie vor Audits auf den Seiten der DKG und des BSI, ob eine neuere Fassung vorliegt.

Ist Microsoft 365 nach § 393 SGB V überhaupt zulässig?

Das hängt davon ab, welche Daten Sie dort verarbeiten und ob für die genutzten Dienste ein aktuelles C5-Testat vom geforderten Typ vorliegt. Welche Dienste abgedeckt sind, prüfen Sie im Service Trust Portal – nicht in Werbeunterlagen. Hinzu kommen die kundenseitigen Kriterien aus dem Prüfbericht, die Sie selbst umsetzen müssen.

Reicht Microsoft 365 E3 für NIS2?

Für die Grundlagen – MFA, Conditional Access, Audit (Standard), Aufbewahrung – liefert E3 viel. PIM, längere Audit-Aufbewahrung und die vollständige Angriffssimulation setzen E5 oder entsprechende Zusatzlizenzen voraus. „Reicht“ ist allerdings keine Lizenzfrage, sondern eine Frage der Risikoanalyse: Was fehlt, muss anders abgedeckt oder bewusst als Restrisiko getragen werden.

Was muss die Geschäftsführung persönlich tun?

Nach § 38 BSIG die Risikomanagementmaßnahmen umsetzen lassen und ihre Umsetzung überwachen sowie regelmäßig an Schulungen teilnehmen. Bei schuldhafter Pflichtverletzung droht Haftung nach den für die Rechtsform geltenden Regeln. Delegieren lässt sich die Arbeit, nicht die Verantwortung.

Wer meldet einen Sicherheitsvorfall, wenn er am Wochenende passiert?

Wer im Meldeprozess dafür benannt ist – und dessen Vertretung. Die 24-Stunden-Frist kennt kein Wochenende. Legen Sie fest, wer die Erheblichkeit bewertet, wer meldet, wo die Zugangsdaten liegen und wie die Datenschutzmeldung parallel läuft. Und üben Sie das, bevor es ernst wird.

Dürfen wir Phishing-Simulationen ohne Betriebsrat, Personalrat oder MAV durchführen?

In aller Regel nicht. Simulationen und ihre Auswertung sind geeignet, Verhalten zu überwachen, und damit mitbestimmungspflichtig – nach Betriebsverfassungsgesetz, Personalvertretungsrecht des Bundes oder Landes oder kirchlichem Mitarbeitervertretungsrecht. Eine Vereinbarung, die Zweck und anonymisierte Auswertung regelt, ist der übliche Weg.

Fazit: Weniger Dschungel, mehr Liste

NIS2, § 391 SGB V und der B3S sind keine drei verschiedenen Projekte. Sie sind drei Blickwinkel auf dieselbe Aufgabe: Ein Krankenhaus muss seine IT so betreiben, dass Versorgung und Patientendaten auch an einem schlechten Tag geschützt sind. Das BSIG regelt, wer meldet, nachweist und haftet. § 391 SGB V sorgt dafür, dass auch Häuser unterhalb der KRITIS-Schwelle nicht durchs Raster fallen und die Belegschaft geschult wird. § 393 SGB V setzt die Leitplanke für Cloud-Dienste. Und der B3S übersetzt das Ganze in eine Sprache, mit der eine Klinik arbeiten kann.

Microsoft 365 ist in dieser Landkarte nicht das Problem, sondern ein Teil der Lösung – wenn die Identitäten geschützt, die Admin-Konten getrennt, die Protokolle aufbewahrt, die Wiederherstellung geübt, die Lieferanten bekannt, der Meldeweg geklärt und die Menschen geschult sind. Die Bordmittel dafür liegen größtenteils schon im Tenant. Was fehlt, ist meistens die Viertelstunde, in der jemand entscheidet, wer sich darum kümmert. Nehmen Sie sich diese Viertelstunde. Der nächste Montag mit Gesetzestext in der Tür kommt bestimmt.