

NIS2 aus Security-Sicht: technische Maßnahmen in M365

Es gibt zwei Sorten von NIS2-Projekten. Die eine beginnt mit einem Kick-off, an dem vierzehn Personen teilnehmen, von denen elf nicht wissen, warum sie eingeladen wurden. Am Ende steht ein Ordner mit Konzeptpapieren, und im Tenant hat sich exakt nichts verändert. Die andere beginnt mit der Frage, welche Häkchen im Admin Center falsch stehen, und ist nach vier Monaten in einem Zustand, in dem eine Prüfung nicht mehr wehtut.

Dieser Beitrag gehört zur zweiten Sorte. Er behandelt Handlungsfeld E aus der Reihe und beantwortet eine einzige Frage: Welche der gesetzlich geforderten technischen Maßnahmen kannst du in Microsoft 365 abbilden, und wie sieht der Nachweis dafür aus, dass du es getan hast? Die Betroffenheitsfrage streifen wir nur kurz — dafür gibt es offizielle Stellen, und wir sind keine Rechtsberatung.

WICHTIG — Was dieser Beitrag ist und was nicht

Das hier ist eine technische Umsetzungshilfe, keine Rechtsberatung. Ob dein Haus unter das Gesetz fällt, in welche Kategorie es fällt und welche Fristen konkret gelten, klärst du mit dem BSI, mit der Rechtsabteilung oder mit einer Kanzlei — nicht mit einem Fachartikel.

Was du hier bekommst: die Zuordnung von gesetzlichen Anforderungen zu konkreten Funktionen in Microsoft 365, mit dem jeweils passenden Nachweis. Das ist der Teil, den dir keine Kanzlei baut.

Betroffenheit in fünf Minuten geklärt (und dann weiter)

Die NIS2-Richtlinie ist in Deutschland über das NIS2-Umsetzungsgesetz in nationales Recht überführt worden. Das Gesetz wurde Anfang Dezember 2025 verkündet und trat einen Tag später in Kraft; die dreimonatige Registrierungsfrist lief entsprechend bis Anfang März 2026, das BSI hat für die Nachzügler eine Nachfrist bis Ende Juli 2026 eingeräumt. Das BSI geht von rund 29.500 direkt betroffenen Einrichtungen in Deutschland aus — deutlich mehr als unter dem alten KRITIS-Regime, und viele davon haben es bis heute nicht gemerkt.

Die Betroffenheitsprüfung selbst ist keine Kunst: Größe des Unternehmens, Branche, Einordnung als besonders wichtige oder wichtige Einrichtung. Das BSI stellt dafür eine eigene Betroffenheitsprüfung bereit, die Registrierung läuft über das Melde- und Unterrichtsportal. Wenn du diesen Schritt noch nicht gemacht hast, mach ihn, bevor du weiterliest. Er dauert weniger lang als das Meeting, in dem ihr diskutiert, ob ihr ihn machen solltet.

Bemerkenswert ist der Teil, den viele überlesen: Die Verantwortung für die Risikomanagementmaßnahmen liegt ausdrücklich bei der Geschäftsleitung. Sie muss die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Delegieren darf sie die Arbeit, nicht die Haftung. Das ist auch der Grund, warum ein sauberes Berichtswesen kein Nice-to-have ist — dazu später mehr.

FAKTEN — Die Eckdaten in einem Kasten

Rechtsgrundlage in Deutschland: BSIG in der Fassung des NIS2-Umsetzungsgesetzes, in Kraft seit 6. Dezember 2025.

Zehn Mindestmaßnahmen für das Risikomanagement stehen in § 30 BSIG, sie entsprechen Artikel 21 der Richtlinie.

Meldepflichten nach § 32 BSIG: Erstmeldung binnen 24 Stunden ab Kenntnis, Folgemeldung binnen 72 Stunden, Abschlussmeldung spätestens einen Monat nach der 72-Stunden-Meldung.

Betroffen sind nach BSI-Schätzung rund 29.500 Einrichtungen; die Kategorien heißen „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ und unterscheiden sich vor allem in der Aufsichtsintensität und im Bußgeldrahmen.

Die zehn Mindestmaßnahmen aus § 30 BSIG — und wo sie in Microsoft 365 landen

Links das Gesetz, rechts die Technik. Die Zuordnung ist keine Rechtsberatung, sondern eine Arbeitshilfe für die Umsetzung.

1	Risikoanalyse und Sicherheitskonzepte	- Secure Score - Purview Compliance Manager - Risikoregister	6	Wirksamkeit der Maßnahmen bewerten	- Secure Score im Zeitverlauf - Übungen - Red Team
2	Bewältigung von Sicherheitsvorfällen	- Defender XDR - Alert Policies - Meldekette ans BSI	7	Schulung und Sensibilisierung	- Attack Simulation Training - Teilnahmenachweise
3	Aufrechterhaltung des Betriebs, Backup	- Aufbewahrung - Versionierung - M365 Backup	8	Kryptographie und Verschlüsselung	- TLS in Exchange Online - BitLocker - Bezeichnungen
4	Sicherheit der Lieferkette	- Cross-Tenant Access - B2B mit Ablauf - Consent	9	Personalsicherheit, Zugriffskontrolle, Assets	- Entra-Rollen - PIM - Intune-Inventar
5	Erwerb, Entwicklung, Wartung, Schwachstellen	- Vulnerability Management - Intune-Update-Ringe	10	Multi-Faktor- und kontinuierliche Auth.	- Conditional Access - FIDO2 - CAE - Auth-Stärken

Was Microsoft 365 nicht für dich erledigt

Die Betroffenheitsprüfung, die Registrierung beim BSI, die Zuweisung der Geschäftsleitungsverantwortung, die Verträge mit Dienstleistern und die Meldung innerhalb von 24 Stunden. Technik ist der leichtere Teil.

boddenberg.de

Skizze 1: Die zehn Mindestmaßnahmen aus § 30 BSIG und ihre Entsprechung in Microsoft 365. Nicht jede Zeile ist vollständig technisch lösbar — aber jede hat einen technischen Anteil.

Die Skizze zeigt schon das Grundproblem und die gute Nachricht in einem: Etwa zwei Drittel der geforderten Maßnahmen haben eine unmittelbare Entsprechung in Microsoft 365. Wenn dein Haus ohnehin auf M365 läuft, ist ein erheblicher Teil der technischen Anforderungen mit Bordmitteln abzubilden. Das restliche Drittel — Risikoanalyse, Lieferantenverträge, Krisenorganisation — ist Papier- und Organisationsarbeit, und kein Portal der Welt nimmt sie dir ab.

Identität und Zugriff: MFA ist nicht mehr verhandelbar

Maßnahme zehn im Katalog nennt Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung ausdrücklich beim Namen. Das ist ungewöhnlich konkret für einen Gesetzestext und macht die Sache für dich einfacher: Du musst nicht argumentieren, ob MFA angemessen ist. Du musst zeigen, dass sie greift.

MFA flächendeckend, nicht selektiv

Der klassische Fehler ist die Teilabdeckung: MFA für Administratoren, MFA für die Geschäftsleitung, und der Rest kommt später. Später kommt nie. Nach dem Maßnahmenkatalog geht es um die Sicherheit der Netz- und Informationssysteme insgesamt, nicht um einzelne privilegierte Konten. Ein Sachbearbeiterkonto mit Zugriff auf die Angebotsablage ist ein hervorragender Startpunkt für einen Angriff.

Microsoft hat den Druck erhöht, ohne dich zu fragen: Seit Februar 2025 wird MFA für den Zugriff auf das Microsoft 365 Admin Center erzwungen, seit Oktober 2025 läuft Phase 2 für schreibende Operationen über Azure CLI, Azure PowerShell, Infrastructure-as-Code-Werkzeuge und REST-

Endpunkte. Wer eine Aufschiebung beantragt hatte, ist spätestens seit Juli 2026 auch dabei. Das deckt allerdings nur die administrative Ebene ab — die Fläche musst du selbst erzwingen, über Conditional Access.

Wie du das ohne Aufstand einführest, steht ausführlich in [MFA in Microsoft 365 richtig einführen](#). Die Richtlinienätze, die dahinter stehen, findest du in [Conditional Access: Baselines, die nicht nerven](#). Und wenn du gerade noch überlegst, ob die Security Defaults nicht reichen würden: Für ein Haus im Geltungsbereich reichen sie nicht, weil du mit ihnen weder differenzieren noch etwas nachweisen kannst — die Abwägung steht in [Security Defaults oder Conditional Access?](#).

Legacy Authentication: die Hintertür, die deine MFA aushebelt

Eine MFA-Pflicht, die per IMAP, POP3 oder SMTP AUTH umgangen werden kann, ist keine MFA-Pflicht, sondern eine Formulierung in einem Konzeptpapier. Basic Authentication ist in Exchange Online für die klassischen Protokolle seit Jahren abgeschaltet, aber SMTP AUTH lebt in vielen Häusern weiter, weil das Multifunktionsgerät im dritten Stock sonst nicht mehr scannen kann. Genau dieses Multifunktionsgerät steht dann im Prüfbericht. Der geordnete Rückbau steht in [Legacy Authentication endgültig abschalten](#).

Zugriffskontrolle heißt Rechte wegnehmen, nicht Rechte vergeben

Maßnahme neun verlangt Konzepte für Personalsicherheit, Zugriffskontrolle und Asset Management. In der Praxis scheitert das selten an fehlenden Konzepten, sondern an der Frage, wer den globalen Administrator eigentlich braucht. Die ehrliche Antwort lautet fast immer: weniger Leute als eingetragen sind.

- Rollen statt Personen: Entra-ID-Rollen zuweisen, nicht Berechtigungen an Konten kleben. Für den Alltag reichen Exchange-, SharePoint- oder Security-Administrator — der globale Administrator ist die Ausnahme, nicht der Normalfall.
- Privileged Identity Management für zeitlich begrenzte Erhöhung, wenn du Entra ID P2 beziehungsweise Microsoft 365 E5 im Haus hast. Ohne P2 arbeitest du mit getrennten Administratorkonten und dokumentierter Rechtevergabe.
- Zugriffsüberprüfungen für privilegierte Rollen und für Gruppen mit Zugriff auf sensible Daten. Das ist der Nachweis, dass jemand nachgesehen hat — siehe auch [Tenant-Härtung: die 20 wichtigsten Schrauben](#).
- Break-Glass-Konten außerhalb aller Richtlinien, überwacht und dokumentiert. Wer sie nicht hat, sperrt sich früher oder später selbst aus dem eigenen Tenant aus: [Break-Glass-Konten anlegen und überwachen](#).

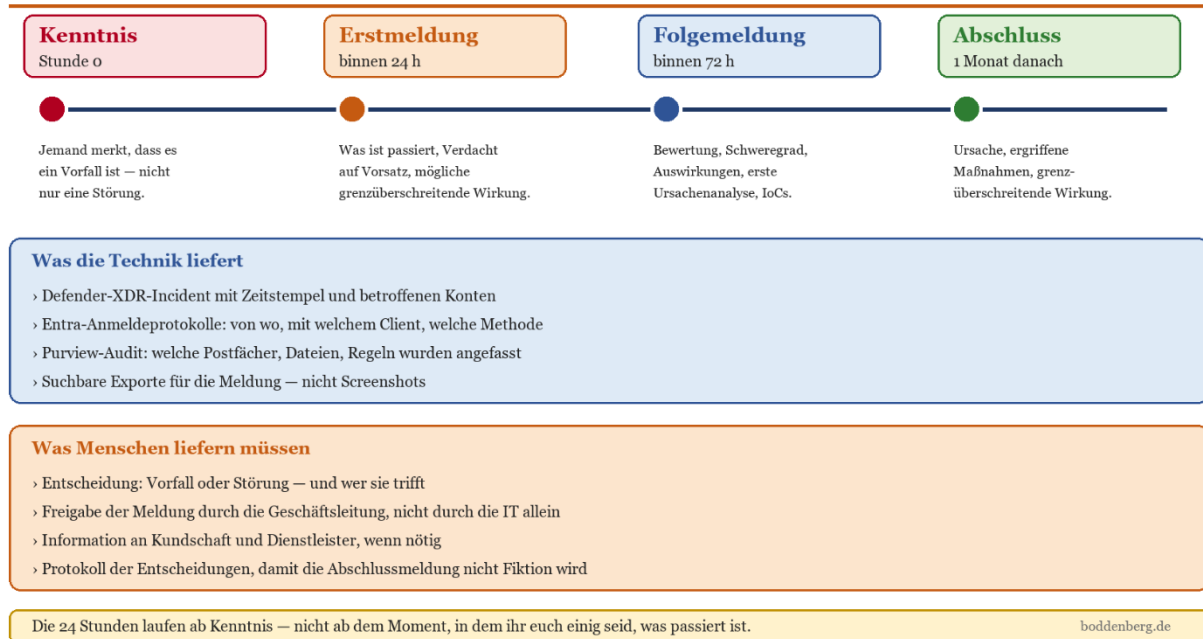
TIPP — Der Satz, der jede Rollendiskussion beendet

Frag nicht, wer den globalen Administrator behalten möchte. Frag, wer bereit ist, namentlich im Prüfbericht zu stehen, falls über dieses Konto etwas passiert. Die Zahl der Kandidaten sinkt in der Regel innerhalb von Sekunden auf ein vertretbares Maß.

Vorfallmanagement: die Uhr läuft ab Kenntnis

Maßnahme zwei verlangt die Bewältigung von Sicherheitsvorfällen. Das ist die harmlose Formulierung. Die unangenehme steht in § 32: 24 Stunden bis zur Erstmeldung, 72 Stunden bis zur Folgemeldung, ein Monat bis zur Abschlussmeldung. Und die 24 Stunden beginnen ab Kenntnis des Vorfalls — nicht ab dem Zeitpunkt, an dem ihr euch intern darauf geeinigt habt, dass es einer war.

Die Meldekette nach § 32 BSIG — und wer im Haus wann etwas tun muss



Skizze 2: Die Meldekette nach § 32 BSIG. Der technische Teil ist der einfachere — die Entscheidungen darüber, ob und wann gemeldet wird, trifft niemand um 3 Uhr morgens spontan gut.

Erkennen: ohne Signal keine Kenntnis

Die Meldefrist setzt voraus, dass jemand überhaupt merkt, dass etwas passiert. In Microsoft 365 sind das im Wesentlichen drei Quellen: die Alert Policies im Purview- und Defender-Portal, die Incidents in Microsoft Defender XDR und — wenn vorhanden — eine SIEM-Anbindung. Die Standard-Alert-Policies sind besser als ihr Ruf, aber voreingestellt landen ihre Benachrichtigungen in einem Postfach, das niemand liest. Wie du das sinnvoll konfigurierst, steht in [Alert Policies und Benachrichtigungen richtig aufsetzen](#); ob eine Sentinel-Anbindung sich lohnt, klärt [Microsoft Sentinel anbinden: wann es sich lohnt](#).

Für die Erkennung selbst sind je nach Lizenz Defender for Office 365, Defender for Endpoint und Defender for Identity die tragenden Bausteine. Insbesondere [Defender for Identity: das Active Directory im Blick](#) ist für Häuser mit lokalem Active Directory relevant, weil ein erheblicher Teil der ernsthaften Angriffe dort beginnt und nicht in der Cloud. Wer sich fragt, wie so etwas praktisch aussieht, findet im [Dossier TerminalFix und der Berlin-Hack](#) einen ausführlich aufgearbeiteten Fall.

Reagieren: der Plan, den es vorher geben muss

Ein Vorfallmanagement ohne schriftlichen Ablauf ist eine Absichtserklärung. Der Katalog verlangt Verfahren, nicht Vorsätze. Praktisch brauchst du: eine Erreichbarkeitskette mit Vertretung, eine Definition dessen, was als Vorfall zählt, eine benannte Person, die die Meldeentscheidung trifft, und Vorlagen für die Meldungen selbst. Der komplette Aufbau steht in [Incident-Response-Plan für Microsoft 365](#) — das ist der Beitrag, den du parallel zu diesem hier brauchst.

Zwei Standardfälle solltest du durchgespielt haben, weil sie statistisch als erstes eintreten: die Übernahme eines Benutzerkontos und ein Verschlüsselungsvorfall. Für den ersten ist [Kompromittiertes Konto erkennen und aufräumen](#) die Arbeitsanweisung, für die ersten sechzig Minuten nach einem Phishing-Treffer [Phishing-Vorfall: die ersten 60 Minuten](#). Und weil ein Plan,

den niemand geübt hat, im Ernstfall etwa so nützlich ist wie ein Feuerlöscher hinter einer verschlossenen Tür: [Feuerwehrübung: Security-Notfälle im Team trainieren](#).

WARNUNG — Die Falle bei der 24-Stunden-Frist

Der häufigste Grund für eine verspätete Meldung ist nicht Bosheit, sondern Zuständigkeitsdiffusion. Die IT hält den Vorfall für einen IT-Vorgang, die Geschäftsleitung erfährt am nächsten Werktag davon, und dann ist die Frist um.

Gegenmittel: Eine einzige benannte Person mit Vertretung, die befugt ist, die Erstmeldung ohne Rücksprache abzusetzen. Eine Erstmeldung ist keine Schuldanerkennung und lässt sich in der Folgemeldung korrigieren. Eine versäumte Frist lässt sich nicht korrigieren.

Betrieb, Backup und Lieferkette

Business Continuity: Papierkorb ist kein Backup

Maßnahme drei nennt Backup-Management, Wiederherstellung nach einem Notfall und Krisenmanagement in einem Atemzug. Microsoft 365 bringt dafür mehrere Ebenen mit, die man nicht verwechseln sollte. Versionierung in SharePoint und OneDrive, der zweistufige Papierkorb, Aufbewahrungsrichtlinien aus Purview und seit einiger Zeit Microsoft 365 Backup als eigenständiger, nutzungsabhängig abgerechneter Dienst.

Microsoft 365 Backup ist allgemein verfügbar, kostet rund 0,15 US-Dollar pro geschütztem Gigabyte und Monat über eine Azure-Subscription und arbeitet mit einem Wiederherstellungspunkt-Abstand von zehn Minuten: für Exchange über das gesamte zurückliegende Jahr, für SharePoint und OneDrive über die letzten vierzehn Tage, danach wöchentlich bis zu einem Jahr zurück. Für die Frage, ob das reicht, ist nicht der Preis entscheidend, sondern dein Wiederanlaufziel — und das gehört aufgeschrieben, nicht geschätzt.

Ebene	Deckt ab	Deckt nicht ab	Nachweis
Versionierung	Versehentliche Änderung, einzelne verschlüsselte Dateien	Gelöschte Bibliotheken, gelöschte Tenants, Massenlöschung	Bibliothekseinstellung, Screenshot mit Datum
Papierkorb (2 Stufen)	Gelöschte Dateien bis 93 Tage	Ablauf der Frist, Löschung durch Aufbewahrung	Tenant-Einstellung, Testwiederherstellung
Aufbewahrungsrichtlinien	Beweissicherung, Löschsperre	Schnelle Massenwiederherstellung im Betrieb	Purview-Richtlinie mit Geltungsbereich
Microsoft 365 Backup	Massenwiederherstellung nach Verschlüsselung	Entra-Konfiguration, Teams-Struktur, Intune	Schutzrichtlinie, Restore-Protokoll
Drittanbieter-Backup	Weitere Workloads, Aufbewahrung nach eigenem Plan	Nichts automatisch — Konfiguration entscheidet	Jobprotokolle, Wiederherstellungstest

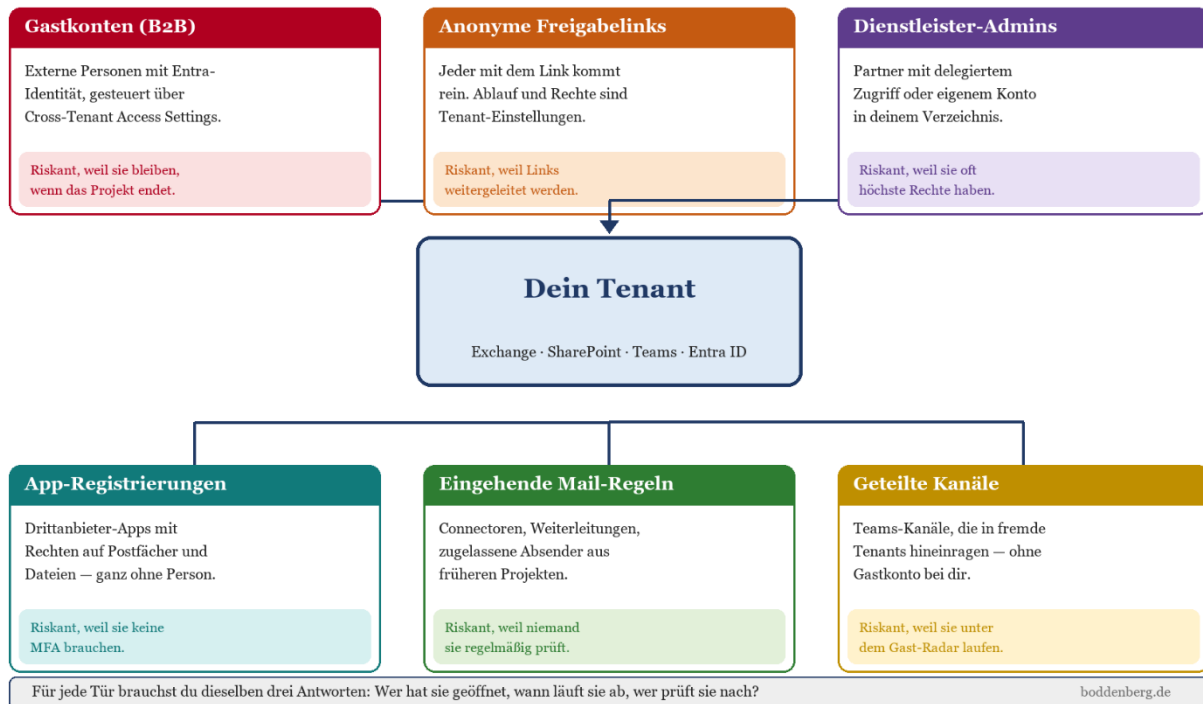
Tabelle 1: Die Ebenen der Wiederherstellbarkeit in Microsoft 365. Keine davon ersetzt eine andere — und keine davon ersetzt einen getesteten Wiederanlauf.

Der wunde Punkt ist fast nie das Wiederherstellen einzelner Dateien, sondern die Konfiguration: Conditional-Access-Richtlinien, Entra-Gruppen, Teams-Strukturen, Intune-Profilen. Wer die nur im Kopf hat, hat sie nicht. Ein regelmäßiger Export der Tenant-Konfiguration ist billig und rettet im Ernstfall Tage. Was du sonst noch vorbereitet haben solltest, steht in [Ransomware-Vorsorge in Microsoft 365](#).

Lieferkette: sechs Türen, die nicht dir gehören

Maßnahme vier verlangt Sicherheit der Lieferkette einschließlich der sicherheitsbezogenen Aspekte der Beziehungen zu unmittelbaren Anbietern und Diensteanbietern. Viele Häuser übersetzen das mit „wir schicken den Lieferanten einen Fragebogen“. Das ist der halbe Weg. Die andere Hälfte ist die Frage, wie diese Anbieter technisch in deinen Tenant hineinkommen.

Lieferkette konkret: sechs Türen in deinen Tenant, die nicht dir gehören



Skizze 3: Sechs typische Zugangswege externer Beteiligter in einen Microsoft-365-Tenant. Jeder davon ist legitim — und jeder davon überlebt in der Praxis das Projekt, für das er eingerichtet wurde.

Die Steuerung dafür sitzt an mehreren Stellen: Cross-Tenant Access Settings in Entra ID regeln, mit welchen fremden Tenants eine B2B-Zusammenarbeit überhaupt möglich ist und ob du deren MFA vertraust. Die externen Freigabeeinstellungen in SharePoint entscheiden, ob anonyme Links erzeugt werden dürfen und wann sie ablaufen. Zugriffsüberprüfungen räumen Gastkonten wieder ab. Die vollständige Härtung dieses Bereichs steht in [Gastzugriff und externe Freigaben härten](#).

Ein eigener Punkt sind Anwendungen: App-Registrierungen und erteilte Zustimmungen sind der Zugangsweg, der ohne Person auskommt und deshalb auch ohne MFA funktioniert. Eine App mit Mail.ReadWrite auf Anwendungsebene liest jedes Postfach im Haus, ohne dass sich jemand anmeldet. Wenn du eine einzige Sache aus dem Lieferkettenkapitel mitnimmst, dann diese: Sieh dir an, welche Anwendungen in deinem Tenant Berechtigungen haben und wer sie erteilt hat. Wie du das dauerhaft in den Griff bekommst, steht in [App-Registrierungen und Consent-Governance](#). Für die Sichtbarkeit von Diensten, die niemand beantragt hat, ist [Defender for Cloud Apps im Mittelstand](#) das passende Werkzeug.

TIPP — Die Frage, die im Lieferantenfragebogen fehlt

Fast jeder Fragebogen fragt nach Zertifikaten und nach Verschlüsselung. Kaum einer fragt: „Über welchen technischen Weg greifen Sie auf unsere Systeme zu, mit welchem Konto, und wie erfahren wir, wenn eine Person bei Ihnen ausscheidet?“

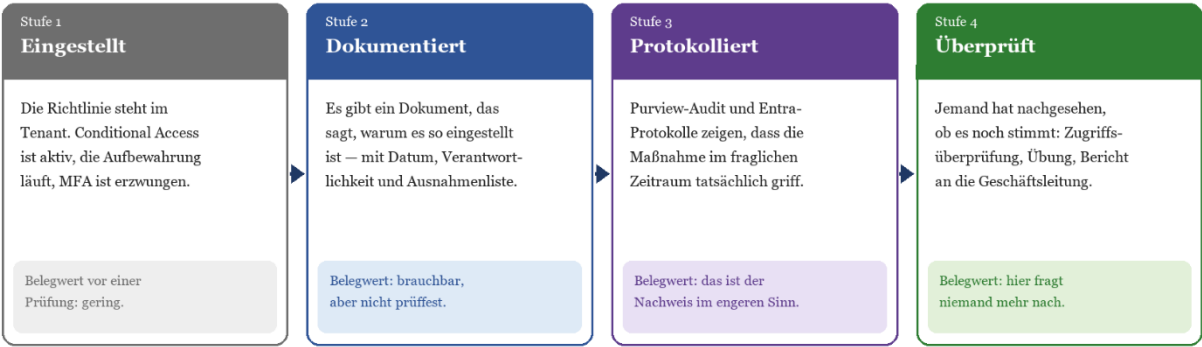
Diese eine Frage bringt mehr als drei Seiten Zertifikatsabfrage — und sie liefert dir die Liste, die du

für die Zugriffsüberprüfung brauchst.

Protokollierung und Nachweis: die Kür, die keine ist

Hier trennt sich das Handlungsfeld von allen anderen. Maßnahme sechs verlangt ausdrücklich Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen. Übersetzt: Du musst nicht nur etwas tun, du musst zeigen können, dass du es getan hast, dass es gewirkt hat, und dass jemand nachgesehen hat.

Vom Häkchen zum Nachweis: die vier Stufen, die eine Prüfung übersteht



Der häufigste Fehler

Häuser bleiben auf Stufe 1 stehen und sind überzeugt, alles getan zu haben. Kommt dann eine Prüfung oder ein Vorfall, gibt es zwar die Einstellung, aber keine Protokolle mehr — weil die Standardaufbewahrung längst abgelaufen ist.

Faustregel: Was du nicht innerhalb von zehn Minuten exportieren kannst, existiert für eine Prüfung nicht.

boddenberg.de

Skizze 4: Die vier Stufen der Nachweisreife. Die meisten Häuser stehen auf Stufe eins und halten sich für fertig.

Aufbewahrungsfristen kennen, bevor sie ablaufen

Das ist der Punkt, an dem regelmäßig Belege verloren gehen, die niemand vermisst hat — bis sie gebraucht werden. Die Standardaufbewahrung von Microsoft Purview Audit liegt bei 180 Tagen für Protokolle, die seit dem 17. Oktober 2023 entstanden sind. Audit (Premium) hebt Exchange-, SharePoint-, OneDrive- und Entra-ID-Datensätze auf ein Jahr; für längere Zeiträume brauchst du die Zehn-Jahre-Zusatzlizenz auf E5-Basis. Die Anmeldeprotokolle in Entra ID selbst sind knapper bemessen: 30 Tage mit P1 oder P2, sieben Tage in der kostenfreien Stufe.

Protokollquelle	Standardaufbewahrung	Verlängerung	Typische Lücke
Purview Audit (Standard)	180 Tage	Audit (Premium) mit E5 bzw. Add-on	Vorfall wird nach 7 Monaten entdeckt
Purview Audit (Premium)	1 Jahr für Exchange, SharePoint, OneDrive, Entra	Zehn-Jahre-Add-on, Optionen 3/5/7/10 Jahre	Andere Aktivitäten bleiben bei 180 Tagen
Entra-Anmeldeprotokolle	30 Tage (P1/P2), 7 Tage kostenfrei	Export nach Log Analytics oder Storage	Niemand hat den Export eingerichtet
Defender XDR, erweiterte Suche	30 Tage	Weiterleitung an Sentinel	Analyse startet am Tag 31
Message Trace	90 Tage historisch, 10 Tage in Echtzeit	Eigener Export	Weiterleitungsregel älter als 90 Tage

Tabelle 2: Aufbewahrungsfristen der wichtigsten Protokollquellen in Microsoft 365. Die rechte Spalte ist die, die in Prüfungen und Vorfällen wehtut.

Der praktische Rat ist unspektakulär: Richte den Export der Entra-Protokolle in einen Log-Analytics-Arbeitsbereich ein, bevor du ihn brauchst, und prüfe einmal, ob deine Audit-Aufbewahrung zu der Zeitspanne passt, in der Vorfälle in deinem Umfeld typischerweise entdeckt werden. Diese Zeitspanne ist in der Praxis deutlich länger als 180 Tage. Zu den Werkzeugen rund um Protokollierung, Aufbewahrung und Nachweisführung gibt es einen eigenen [Kompetenzbereich Microsoft Purview](#).

Die Nachweistabelle: Anforderung, Funktion, Beleg

Das folgende ist der Kern dieses Beitrags. Nimm die Tabelle, geh sie zeilenweise durch und trag in eine vierte Spalte ein, was bei euch tatsächlich existiert. Was leer bleibt, ist deine Aufgabenliste. Das ist unbequemer als ein Reifegradmodell und ungefähr zehnmal so nützlich.

Anforderung (§ 30 BSIG)	M365-Funktion	Nachweis, den du vorlegen kannst
Risikoanalyse und Sicherheitskonzepte	Microsoft Secure Score, Purview Compliance Manager (NIS2-Vorlage als Premium-Assessment)	Score-Verlauf über 12 Monate, Assessment mit dokumentierten Prüfpunkten und hinterlegten Belegen
Bewältigung von Sicherheitsvorfällen	Defender XDR Incidents, Alert Policies, Purview Audit	Incident-Historie mit Zeitstempeln, dokumentierter Meldeweg, Protokoll der getroffenen Entscheidungen
Aufrechterhaltung des Betriebs, Backup	Aufbewahrungsrichtlinien, Versionierung, Microsoft 365 Backup, Konfigurationsexport	Schutzrichtlinien mit Geltungsbereich, Protokoll einer echten Testwiederherstellung mit Datum
Sicherheit der Lieferkette	Cross-Tenant Access Settings, B2B-Gastkonten mit Ablauf, Zugriffsüberprüfungen, Consent-Richtlinien	Liste der Partnertenanten, Ergebnis der letzten Gastkonten-Überprüfung, Liste der Apps mit Anwendungsberechtigungen
Schwachstellen- und Wartungsmanagement	Defender Vulnerability Management, Intune-Update-Ringe, Windows Update for Business	Berichte zur Update-Konformität, offene Empfehlungen mit Fälligkeit und Verantwortlichkeit
Wirksamkeit der Maßnahmen bewerten	Secure Score im Zeitverlauf, Attack Simulation Training, Übungen	Vorher-Nachher-Vergleich, Klickraten je Kampagne, Übungsprotokoll mit Erkenntnissen und Terminen
Schulung und Sensibilisierung	Attack Simulation Training mit Zuweisung, Viva Learning	Teilnahmequote je Abteilung, Nachweis der Schulung der Geschäftsleitung
Kryptographie	TLS-Erzwingung in Exchange Online, BitLocker über Intune, Purview-Vertraulichkeitsbezeichnungen	Connector-Konfiguration, BitLocker-Konformitätsbericht, Bezeichnungsrichtlinie mit Geltungsbereich
Personalsicherheit, Zugriffskontrolle, Assets	Entra-Rollen, PIM, Zugriffsüberprüfungen, Intune-Geräteinventar	Liste der privilegierten Konten mit Begründung, PIM-Aktivierungsprotokoll, Ergebnis der letzten Rollenüberprüfung
Multi-Faktor-Authentifizierung	Conditional Access, Authentifizierungsstärken, FIDO2, Continuous Access Evaluation	Richtlinien im Report-only-Vergleich, Abdeckungsbericht je Benutzergruppe, dokumentierte Ausnahmen mit Ablaufdatum

Tabelle 3: Die Zuordnung von Anforderung, Funktion und Nachweis. Die dritte Spalte ist die, an der Prüfungen scheitern — nicht die zweite.

FAKTEN — Nachweise sammeln, ohne ein zweites System zu bauen

Der Purview Compliance Manager kann als Ablage für Nachweise dienen: Jeder Prüfpunkt eines Assessments nimmt Dokumente, Verantwortlichkeiten und Testergebnisse auf. Die NIS2-Vorlage

gehört zu den kostenpflichtigen Premium-Vorlagen; Häuser mit E5, A5 oder G5 dürfen drei davon ohne Aufpreis aktivieren.

Wichtig ist weniger das Werkzeug als die Disziplin: ein Ort, ein Verantwortlicher je Prüfpunkt, ein Datum. Eine gepflegte Tabelle in SharePoint schlägt ein ungepflegtes Compliance-Portal um Längen.

Berichten, weil die Geschäftsleitung haftet

Weil die Verantwortung ausdrücklich bei der Geschäftsleitung liegt, ist das Berichtswesen kein Selbstzweck. Es ist der Mechanismus, über den die Geschäftsleitung ihrer Überwachungspflicht nachkommt — und der Beleg dafür, dass sie es getan hat. Ein Quartalsbericht mit drei Kennzahlen, einer Seite Text und einem Protokollvermerk „zur Kenntnis genommen“ ist in einer Prüfung mehr wert als ein Dashboard, das niemand aufruft. Wie so ein Bericht aussieht, der auch gelesen wird, steht in [Security-Reporting für die Geschäftsführung](#). Und warum der Secure Score dabei eine Kennzahl unter mehreren sein sollte und nicht das Ziel, klärt [Secure Score: sinnvoll nutzen statt Punktejagd](#).

WARNUNG — Monitoring ist mitbestimmungspflichtig

Sobald du Protokolle auswertest, aus denen sich Verhalten oder Leistung einzelner Personen ableiten lässt, bist du im Bereich der Mitbestimmung. Das gilt für Anmeldeprotokolle, für Defender-Warnungen und ganz besonders für Auswertungen aus Attack Simulation Training.

Wer den Betriebsrat erst einbindet, wenn die Auswertung schon läuft, verliert Monate und Vertrauen. Was konkret mitbestimmungspflichtig ist und wie eine tragfähige Betriebsvereinbarung aussieht, steht in [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#).

Was du in den nächsten vier Monaten tust

Wenn du bei null anfängst, hilft dir keine Priorisierungsmatrix, sondern eine Reihenfolge. Diese hier funktioniert in Häusern zwischen 100 und 800 Konten, weil sie mit den Maßnahmen beginnt, die den größten Anteil des Risikos abräumen und gleichzeitig am leichtesten nachzuweisen sind.

Monat	Schwerpunkt	Konkretes Ergebnis
1	Bestandsaufnahme und MFA	Betroffenheit und Registrierung geklärt; MFA-Abdeckung gemessen; Break-Glass-Konten angelegt und überwacht
2	Zugriff und Legacy	Conditional-Access-Grundsatz aktiv, Legacy-Authentifizierung abgeschaltet, privilegierte Rollen reduziert und dokumentiert
3	Vorfall und Meldekette	Incident-Response-Plan schriftlich, Meldeentscheider benannt, Alert Policies auf ein Postfach, das jemand liest
4	Lieferkette und Nachweis	Gastkonten überprüft, App-Berechtigungen gesichtet, Protokollexport eingerichtet, erster Quartalsbericht

Tabelle 4: Eine Reihenfolge, die sich in der Praxis bewährt hat. Sie ist nicht vollständig — sie ist machbar, und das ist wichtiger.

Was in diesen vier Monaten bewusst nicht passiert: keine Ausschreibung für ein SIEM, keine Zielarchitektur mit fünf Ebenen, kein Reifegradmodell. Das kommt danach, wenn es überhaupt kommt. Der komplette Überblick über die Reihe und ihre Handlungsfelder steht auf der Themenseite [Microsoft 365 Security](#). Wenn ihr für die Umsetzung Unterstützung braucht — sei es für die Konfiguration oder für die Nachweisführung — findet ihr die Rahmenbedingungen unter [Microsoft 365 Security Beratung](#); für die Qualifizierung des eigenen Teams gibt es [Schulung Microsoft 365 Security](#).

Häufige Fragen

Reicht Microsoft 365 E3, oder brauche ich zwingend E5?

E3 trägt die technischen Kernanforderungen: Entra ID P1 mit Conditional Access, Purview Audit (Standard) mit 180 Tagen, Aufbewahrungsrichtlinien, Intune, Defender for Office 365 Plan 1 und Defender for Endpoint Plan 1. Was in E3 fehlt, ist im Wesentlichen die Tiefe: Privileged Identity Management, Zugriffsüberprüfungen, Defender for Identity, die erweiterte Suche über alle Signale und die längere Audit-Aufbewahrung. Du kannst mit E3 gesetzeskonform arbeiten, musst dann aber mehr organisatorisch abfangen und mehr manuell dokumentieren. Ob sich E5 rechnet, entscheidet nicht die Compliance, sondern die Frage, wie viel Handarbeit du dauerhaft leisten willst.

Gibt es eine offizielle NIS2-Zertifizierung für Microsoft 365?

Nein. Es gibt kein Häkchen, keinen Prüfbericht von Microsoft und kein Testat, das deinen Tenant für konform erklärt. Microsoft liefert Funktionen und Nachweismöglichkeiten; die Konformität stellt deine Einrichtung her, und zwar einschließlich aller Systeme außerhalb von M365. Wer dir eine „NIS2-Zertifizierung für Microsoft 365“ verkaufen will, verkauft dir eine Beratungsleistung mit irreführendem Namen.

Wir sind selbst nicht betroffen, aber unsere Kundschaft fragt trotzdem. Was tun?

Das ist der Regelfall, und er hat einen Namen: Lieferkettenwirkung. Betroffene Einrichtungen müssen die Sicherheit ihrer unmittelbaren Anbieter berücksichtigen, also reichen sie Anforderungen weiter. Praktisch bedeutet das, dass du dieselben Fragen beantworten musst wie ein direkt betroffenes Haus, nur ohne Meldepflicht ans BSI. Die Tabelle in diesem Beitrag ist auch dafür brauchbar — sie ist im Kern eine Liste dessen, was ein vernünftiger Auftraggeber fragen wird.

Müssen wir jeden Sicherheitsvorfall melden?

Nein, sondern erhebliche Sicherheitsvorfälle im Sinne des Gesetzes. Der Unterschied ist nicht trivial, und die Abgrenzung solltest du vorher schriftlich festlegen — nicht während des Vorfalls. Eine geblockte Phishingmail ist kein meldepflichtiger Vorgang. Eine Kontoübernahme mit anschließendem Datenabfluss sehr wohl. Für den Graubereich dazwischen brauchst du eine benannte Person mit Entscheidungsbefugnis und die Bereitschaft, im Zweifel zu melden statt zu diskutieren.

Wie lange müssen wir Protokolle aufbewahren?

Das Gesetz nennt keine pauschale Frist für Protokolldaten, sondern verlangt angemessene Maßnahmen — und die Abschlussmeldung einen Monat nach der 72-Stunden-Meldung setzt voraus, dass du die Ursache noch rekonstruieren kannst. Praktisch heißt das: Die 180 Tage von Purview Audit (Standard) sind die Untergrenze, ein Jahr ist die vernünftige Zielgröße, und die 30 Tage der Entra-Anmeldeprotokolle solltest du per Export verlängern. Beachte dabei die Löschfristen aus dem Datenschutz — beide Anforderungen gelten gleichzeitig, und die Auflösung gehört in die Betriebsvereinbarung.

Wer haftet, wenn wir die Fristen reißen?

Die Geschäftsleitung. Sie muss die Risikomanagementmaßnahmen billigen und ihre Umsetzung überwachen; der Bußgeldrahmen orientiert sich an der Einstufung als besonders wichtige oder wichtige Einrichtung. Für dich in der IT ist das weniger eine Drohung als ein Hebel: Es ist der Grund, warum ein Sicherheitsbudget in diesem Jahr besser durchgeht als im letzten. Die konkrete Haftungsfrage beantwortet allerdings eine Kanzlei, nicht dieser Beitrag.

Fazit

NIS2 ist unangenehmer in der Ankündigung als in der Umsetzung — jedenfalls für den technischen Teil. Wer Microsoft 365 im Haus hat, besitzt für die Mehrzahl der geforderten Maßnahmen bereits die Werkzeuge und muss sie vor allem einschalten, zuweisen und belegen. Die Arbeit steckt nicht in der Beschaffung, sondern in der Ordnung: Wer darf was, wer merkt es, wer entscheidet, und wo liegt der Beweis.

Der Unterschied zwischen einem Haus, das die Prüfung übersteht, und einem, das sie nicht übersteht, ist selten die Technik. Es ist die dritte Spalte der großen Tabelle — der Nachweis. Häkchen im Portal sind schnell gesetzt und noch schneller wieder verändert. Protokolle, Berichte und Überprüfungen mit Datum überleben auch den Kollegen, der im Herbst kündigt.

Und falls dich das alles nach viel Aufwand für ein Gesetz klingt: Es ist im Kern dieselbe Liste, die du auch ohne Gesetz abarbeiten würdest, um nicht in der Lokalzeitung zu landen. Der Gesetzgeber hat sie nur verbindlich gemacht und ein Datum drangeschrieben. Das ist, ehrlich gesagt, die effektivste Priorisierungshilfe, die die IT-Sicherheit in den letzten zwanzig Jahren bekommen hat.

WEITER — Passend zu diesem Beitrag

- › [Incident-Response-Plan für Microsoft 365](#) — der Plan, ohne den die 24-Stunden-Frist nicht zu halten ist
- › [Security-Reporting für die Geschäftsführung](#) — weil die Geschäftsleitung haftet und deshalb berichtet werden muss
- › [Kompetenzbereich Microsoft Purview](#) — Nachweise, Audit und Aufbewahrung im Zusammenhang
- › [MFA in Microsoft 365 richtig einführen](#) und [Legacy Authentication endgültig abschalten](#) — Maßnahme zehn, praktisch umgesetzt
- › [Gastzugriff und externe Freigaben härten](#) und [App-Registrierungen und Consent-Governance](#) — die Lieferkette an der technischen Tür
- › [Ransomware-Vorsorge in Microsoft 365](#) und [Feuerwehrrübung: Security-Notfälle im Team trainieren](#) — Betriebsfortführung, geübt statt geplant
- › [Security-Monitoring und Betriebsrat: was mitbestimmungspflichtig ist](#) — bevor die erste Auswertung läuft
- › [Microsoft 365 Security Beratung](#) und [Schulung Microsoft 365 Security](#) — wenn Unterstützung sinnvoll ist