

Ergänzungsblatt Bayern

zur GdW-Arbeitshilfe 102 „Informations- und IT-Sicherheit in
Wohnungsunternehmen. Vorschläge für Mindestmaßnahmen und
Umsetzungsempfehlungen“

*Acht Ergänzungen, ein Sofortprogramm für 90 Tage, eine Einordnung nach
Unternehmensgröße und die Melde- und Kontaktwege in Bayern*

Angabe	Inhalt
Herausgeber	VdW Bayern, Verband bayerischer Wohnungsunternehmen e.V. VdW Bayern Digital Solutions GmbH
Zielgruppe	Vorstände, Geschäftsführungen, IT-Verantwortliche und Datenschutzbeauftragte der Mitgliedsunternehmen sowie deren IT-Dienstleister
Stand	31.08.2026 (Kontaktdaten, Fristen und Förderbedingungen mit diesem Stand; bitte vor Nutzung prüfen)
Ansprechpartner	Christian Fischer, Geschäftsführer der VdW Bayern Digital Solutions GmbH christian.fischer@vdwbayern.de, Mobil 0171 2181213
Beilage	Selbstbewertung IT-Sicherheit (Excel-Datei mit Auswertung, 59 Prüffragen zu den 22 Maßnahmen der Arbeitshilfe und den vier Ergänzungen)
Hinweis	Dieses Blatt ergänzt die GdW-Arbeitshilfe 102 und ersetzt sie nicht. Es ersetzt keine Rechtsberatung und keine individuelle Risikoanalyse.

Inhalt

1 Worum es geht.....	3
2 Acht Ergänzungen zur Arbeitshilfe.....	3
2.1 Meldepflichten gehören in jeden Notfallplan (ergänzt M5).....	3
2.2 Prüfen Sie, ob NIS2 für Sie gilt (ergänzt M6).....	4
2.3 Sofortmaßnahmen 2026: Support-Enden und Perimeter (ergänzt M9, M11, M13).....	4
2.4 Backup richtig verstehen (ergänzt M4).....	5
2.5 Erkennung: EDR statt reinem Virenschutz (ergänzt M8, M13, M22).....	5
2.6 E-Mail und Zahlungsverkehr absichern (neu).....	6
2.7 Fernwartungszugänge Ihrer Dienstleister (ergänzt M2, M3).....	6
2.8 Korrigierte Zuordnung zu den Stufen (ergänzt Kapitel 6 der Arbeitshilfe).....	7
3 Sofortprogramm: die ersten 90 Tage.....	7
4 Was die Maßnahmen für Ihr Unternehmen bedeuten.....	10
5 Melde- und Kontaktwege in Bayern.....	14
5.1 Die erste Stunde: was Sie bei einem Verdacht tun.....	14
5.2 Kontakte.....	14
5.3 Melden oder nicht melden?.....	15
6 Weiterführende Angebote.....	15
6.1 Kostenlose Angebote des BSI.....	15
6.2 Förderung: Digitalbonus Bayern.....	15
6.3 Angebote des VdW Bayern.....	16
Anhang: Rechtsgrundlagen und Quellen.....	16

1 Worum es geht

Der GdW hat im August 2026 die Arbeitshilfe 102 „Informations- und IT-Sicherheit in Wohnungsunternehmen“ veröffentlicht. Sie beschreibt 22 Maßnahmen (M1 bis M22) und ordnet sie vier Prioritätsstufen zu. Für den Einstieg in das Thema und für das Gespräch mit Vorstand, Geschäftsführung, Aufsichtsrat und IT-Dienstleister ist sie eine gute Grundlage. Wir empfehlen Ihnen, sie zu lesen und die Stufenlogik als Fahrplan zu verwenden.

Aus der Beratungs- und Prüfungspraxis des VdW Bayern wissen wir aber, dass einige Punkte, die in bayerischen Wohnungsunternehmen regelmäßig den Unterschied machen, in der Arbeitshilfe fehlen oder zu kurz kommen: die Meldepflichten nach einem Vorfall, die Frage, ob NIS2 für Sie gilt, die Support-Enden von Windows 10 und Exchange, der Datenabfluss bei Ransomware, die Erkennung von Angriffen, die Absicherung von E-Mail und Zahlungsverkehr sowie die Fernwartungszugänge Ihrer Dienstleister. Dieses Ergänzungsblatt schließt diese Lücken und ist so aufgebaut, dass Sie es neben die Arbeitshilfe legen können: Die Maßnahmennummern M1 bis M22 und die Stufen 1 bis 4 sind dieselben.

Was Sie hier finden

- **Kapitel 2:** Acht Ergänzungen zur Arbeitshilfe, jeweils mit dem, was Sie konkret tun sollten, und einer korrigierten Zuordnung zu den Stufen.
- **Kapitel 3:** Ein Sofortprogramm für die ersten 90 Tage als abhakbare Liste.
- **Kapitel 4:** Was jede Maßnahme für Ihr Unternehmen bedeutet, je nachdem, ob Sie keine eigene IT, einen IT-Verantwortlichen oder eine IT-Abteilung haben, mit Aufwand und Kostenklasse.
- **Kapitel 5:** Die Melde- und Kontaktwege in Bayern für die erste Stunde nach einem Vorfall.
- **Kapitel 6:** Kostenlose und geförderte Angebote, die Ihnen den Einstieg erleichtern.
- **Beilage:** Eine Selbstbewertung als Excel-Datei mit 59 Prüffragen und automatischer Auswertung nach Maßnahme und Stufe.

Für wen welches Kapitel gedacht ist: Vorstand und Geschäftsführung: Kapitel 1, 2 und 5. IT-Verantwortliche und IT-Dienstleister: Kapitel 2, 3 und 4. Datenschutzbeauftragte: Kapitel 2.1 und 5.

2 Acht Ergänzungen zur Arbeitshilfe

2.1 Meldepflichten gehören in jeden Notfallplan (ergänzt M5)

In einem Wohnungsunternehmen betrifft nahezu jeder Sicherheitsvorfall personenbezogene Daten: Mieter, Mitglieder, Bewerber, Beschäftigte. Die Arbeitshilfe beschreibt in M5, wer intern informiert wird, sagt aber nichts über die gesetzlichen Meldepflichten. Diese laufen ab dem Moment, in dem Sie von einem Vorfall Kenntnis erlangen:

- **Art. 33 DSGVO:** Meldung an das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) innerhalb von 72 Stunden, sobald ein Risiko für die Betroffenen nicht ausgeschlossen werden kann. Auch eine Verschlüsselung durch Ransomware ist eine Datenschutzverletzung (Verlust der Verfügbarkeit), selbst wenn kein Datenabfluss nachgewiesen ist. Eine vorläufige Meldung mit Nachmeldung ist zulässig.
- **Art. 34 DSGVO:** Benachrichtigung der Betroffenen, wenn ein hohes Risiko besteht, zum Beispiel bei Kontodaten, Bonitätsauskünften, Ausweiskopien oder Gesundheitsangaben aus Härtefallanträgen.

- **Cyberversicherung:** unverzügliche Meldung an den Versicherer; die Police enthält dafür eine Hotline. Wer zu spät meldet, riskiert den Versicherungsschutz.
- **NIS2 (nur für betroffene Einrichtungen, siehe 2.2):** Erstmeldung an das BSI innerhalb von 24 Stunden, Folgemeldung innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats.
- **Strafanzeige:** keine Pflicht, aber empfohlen. Die Zentrale Ansprechstelle Cybercrime (ZAC) beim Bayerischen Landeskriminalamt berät Unternehmen und nimmt Anzeigen entgegen (Kontakt in Kapitel 5).

Was Sie tun sollten: Binden Sie Ihren Datenschutzbeauftragten sofort ein, nicht erst nach der technischen Bereinigung. Legen Sie fest, wer über die Meldung an das BayLDA entscheidet, und dokumentieren Sie diese Entscheidung auch dann, wenn Sie nicht melden. Nehmen Sie die Meldewege aus Kapitel 5 in Ihren Notfallplan und auf Ihre Notfalkarte auf.

Praxishinweis zu Microsoft 365: Wenn ein Zugangsdatum durch Phishing abgeflissen ist, reicht das Ändern des Passworts nicht. Lassen Sie zusätzlich alle aktiven Sitzungen beenden, die hinterlegten MFA-Methoden prüfen, Postfachregeln (Weiterleitungen) kontrollieren und prüfen, ob der Angreifer eine App-Registrierung angelegt hat. Erst dann ist das Konto wieder sauber.

2.2 Prüfen Sie, ob NIS2 für Sie gilt (ergänzt M6)

Die Arbeitshilfe nennt NIS2 im Vorwort, erklärt aber nicht, dass Wohnungsunternehmen betroffen sein können. Das NIS2-Umsetzungsgesetz ist seit dem 06.12.2025 in Kraft. Die Wohnungswirtschaft ist kein eigener Sektor, aber Wohnungsunternehmen fallen in den Anwendungsbereich, wenn sie eine der folgenden Tätigkeiten ausüben und die Größenschwellen erreichen:

- Betrieb von Energieerzeugungsanlagen, zum Beispiel Photovoltaikanlagen (§ 3 Nr. 18d EnWG), oder Betrieb von Fernwärme- oder Fernkälteversorgung.
- Betrieb öffentlich zugänglicher Ladepunkte für Elektrofahrzeuge.
- Betrieb öffentlicher Telekommunikationsnetze (hier gilt keine Mindestgröße).
- Genossenschaften mit Spareinrichtung, sofern sie Kredite vergeben (Bankensektor).

Die Schwellen für „wichtige Einrichtungen“ liegen bei mindestens 50 Beschäftigten oder mehr als 10 Mio. Euro Umsatz bzw. Bilanzsumme. Das deutsche Gesetz enthält eine Ausnahme für Tätigkeiten, die im Verhältnis zur gesamten Geschäftstätigkeit vernachlässigbar sind; ob Ihre PV-Anlagen oder Ihr Wärmenetz darunter fallen, sollten Sie begründet dokumentieren. Die Registrierungsfrist beim BSI ist am 06.03.2026 abgelaufen; wer betroffen ist und sich noch nicht registriert hat, sollte das umgehend nachholen. Betroffene Einrichtungen müssen ein Risikomanagement nachweisen, Vorfälle melden und ihre Geschäftsleitung schulen; die Geschäftsleitung haftet persönlich für die Umsetzung (§ 38 BSIg).

Was Sie tun sollten: Führen Sie die Betroffenheitsprüfung mit Vorstand oder Geschäftsführung durch, bei Zweifeln mit Rechtsberatung, und halten Sie das Ergebnis schriftlich fest, auch ein negatives. Unsere Mitgliederinformation vom 02.03.2026 auf [vdwbayern.de](https://www.vdwbayern.de) enthält die Details. Unabhängig von NIS2 gilt: Vernetzte Gebäudetechnik (Heizungssteuerung, Wechselrichter, Ladepunkte, Schließsysteme) gehört in ein eigenes Netzsegment (M18), Standardpasswörter sind zu ändern, und Fernzugriffe des Installateurs sind zu regeln (2.7).

2.3 Sofortmaßnahmen 2026: Support-Enden und Perimeter (ergänzt M9, M11, M13)

Die Arbeitshilfe nennt als Beispiel für veraltete Software Windows 7. Die aktuelle Situation ist eine andere: Windows 10, Exchange Server 2016 und 2019 sowie Office 2016 und 2019 erhalten seit dem 14.10.2025 keine regulären Sicherheitsupdates mehr. In vielen Wohnungsunternehmen laufen diese Systeme noch.

Was Sie tun sollten:

- Lassen Sie sich von Ihrem Dienstleister eine Liste aller Geräte und Server mit Betriebssystem und Support-Ende geben (das ist zugleich der Einstieg in M1). Systeme ohne Support werden abgelöst oder, wenn das kurzfristig nicht geht, vom Netz isoliert.
- Ein eigener Exchange-Server ist seit Jahren eines der meistangegriffenen Systeme im Mittelstand. Er darf nicht direkt aus dem Internet erreichbar sein; mittelfristig sollten Sie auf Exchange Server SE migrieren oder zu Exchange Online wechseln.
- Firewall, VPN-Gateway und Switches brauchen Firmware-Updates genauso wie PCs. Laut BSI-Lagebericht 2025 sind ungepatchte, aus dem Internet erreichbare Systeme eines der wichtigsten Einfallstore. Nehmen Sie diese Geräte in den Patch-Rhythmus auf (M9).
- Kein Verwaltungsdienst (Remote Desktop, SMB-Dateifreigaben, Datenbankports) darf aus dem Internet erreichbar sein. Zugriff von außen nur über VPN mit Mehrfaktor-Authentifizierung.
- Die Arbeitshilfe formuliert in M13 „Windows-Firewall oder UTM“. Richtig ist: beides. Die Windows-Firewall schützt das Gerät auch im Homeoffice und innerhalb des Büronetzes, die Firewall am Netzübergang schützt das Netz.

2.4 Backup richtig verstehen (ergänzt M4)

Die Arbeitshilfe nennt Backups die „wichtigste Schutzmaßnahme gegen Ransomware-Angriffe“. Das ist nur die halbe Wahrheit: Ein Backup schützt nicht vor dem Angriff, es ermöglicht die Wiederherstellung. Angreifer ziehen heute vor der Verschlüsselung Daten ab und drohen mit der Veröffentlichung (doppelte Erpressung). Der BSI-Lagebericht 2025 stellt ausdrücklich fest, dass Unternehmen trotz Backup erpressbar bleiben. Für Sie heißt das: Ein Angriff ist auch mit funktionierendem Backup ein Datenschutzvorfall mit Meldepflicht (2.1), und Prävention und Erkennung (2.3, 2.5) bleiben unverzichtbar.

Mindestanforderungen an Ihr Backup, die über M4 hinausgehen:

- 3-2-1-Regel: drei Kopien, auf zwei verschiedenen Medien, eine davon außer Haus.
- Eine Kopie ist offline oder unveränderlich (immutable), das heißt, sie kann auch von einem kompromittierten Administratorkonto nicht gelöscht oder verschlüsselt werden. Das Backup-System hat eine eigene Anmeldung, die nicht dem Domänen-Administrator gehört. Die Arbeitshilfe ordnet das Offline-Backup erst Stufe 4 zu; es gehört in Stufe 1, sonst ist das Backup bei Ransomware wertlos.
- Microsoft 365 einbeziehen: E-Mails, SharePoint, OneDrive und Teams werden von Microsoft nicht als langfristiges Backup vorgehalten. Sie brauchen dafür einen Zusatzdienst oder ein Backup-Produkt.
- Backups verschlüsseln; Wiederherstellungszeit und Wiederanlaufreihenfolge (ERP vor Dokumentenmanagement vor Portal) schriftlich festlegen.
- Wiederherstellung testen: quartalsweise eine Stichprobe (einzelne Dateien, ein Postfach), jährlich ein vollständiger Test mit Protokoll. Das Protokoll ist zugleich ein Nachweis gegenüber Versicherer und Abschlussprüfer.

2.5 Erkennung: EDR statt reinem Virenschutz (ergänzt M8, M13, M22)

Die Arbeitshilfe empfiehlt Virenschutz (M13), einen monatlichen Blick in die Protokolle (M8) und für größere Unternehmen ein SIEM (M22). Der Zwischenschritt, der heute für Unternehmen ohne eigenes Sicherheitsteam der Standard ist, fehlt: Endpoint Detection and Response (EDR). EDR erkennt verdächtiges Verhalten (zum Beispiel ein Programm, das beginnt, massenhaft Dateien zu verschlüsseln), isoliert das Gerät automatisch und meldet den Vorfall zentral. In Microsoft 365

Business Premium ist EDR als „Defender for Business“ bereits enthalten und muss nur eingerichtet werden.

Was Sie tun sollten: EDR auf allen PCs, Laptops und Servern aktivieren und die Alarme an eine Person oder Ihren Dienstleister leiten. Wer niemanden hat, der Alarme rund um die Uhr bearbeitet, beauftragt einen Dienstleister mit „Managed Detection and Response“ (MDR). Ein SIEM ist erst danach sinnvoll. Ersetzen Sie außerdem die monatliche Protokolldurchsicht aus M8 durch Alarme auf fünf Schlüsselereignisse, die Microsoft 365 ohne Zusatzkosten bietet: fehlgeschlagene Anmeldungen in Serie, neue Administratoren, geänderte MFA-Methoden, neue Postfach-Weiterleitungsregeln und Anmeldungen aus untypischen Ländern. Stimmen Sie Protokollierung und Auswertung mit dem Betriebsrat ab, wo es einen gibt (§ 87 Abs. 1 Nr. 6 BetrVG).

2.6 E-Mail und Zahlungsverkehr absichern (neu)

Die Angriffe, die Wohnungsunternehmen am häufigsten unmittelbar Geld kosten, brauchen keine Schadsoftware: gefälschte Rechnungen, angebliche Änderungen der Bankverbindung eines Handwerkers, Zahlungsanweisungen im Namen des Vorstands („CEO-Fraud“) und Schreiben an Mieter mit einer „neuen Bankverbindung für die Miete“. Die Arbeitshilfe behandelt diese Fälle nicht.

Technisch (kostenlos, ein Auftrag an Ihren Dienstleister):

- SPF, DKIM und DMARC für alle E-Mail-Domains des Unternehmens einrichten. Damit können Angreifer nicht mehr unter Ihrer Absenderadresse an Mieter und Lieferanten schreiben. Ziel ist eine DMARC-Richtlinie, die gefälschte Mails abweist.
- Automatische Weiterleitungen an externe Adressen sperren; sie sind das Standardwerkzeug bei übernommenen Postfächern.
- E-Mails von externen Absendern sichtbar kennzeichnen; Anhänge und Links prüfen lassen (in Business Premium enthalten).

Organisatorisch (Buchhaltung und Vorstand):

- Änderungen von Bankverbindungen (Lieferanten, Handwerker, Mieter, Kautionen) nur nach Rückruf über eine bereits bekannte Telefonnummer und im Vier-Augen-Prinzip übernehmen; nie über die Kontaktdaten aus der Änderungsmitteilung selbst.
- Keine Zahlung allein auf Grundlage einer E-Mail, auch nicht vom Vorstand; Freigabegrenzen und Funktionstrennung im ERP nutzen.
- Mieter darüber informieren, wie das Unternehmen kommuniziert (zum Beispiel: Bankverbindungen ändern sich nie per E-Mail oder Brief ohne Rückfragemöglichkeit).

2.7 Fernwartungszugänge Ihrer Dienstleister (ergänzt M2, M3)

Die IT der meisten Mitgliedsunternehmen wird von außen betreut: Systemhaus, ERP-Anbieter, Dokumentenmanagement, Telefonanlage, Gebäudetechnik, Aufzug. Dauerhaft offene Fernwartungszugänge mit geteilten Passwörtern sind ein klassisches Einfallstor, und ein Angriff auf den Dienstleister trifft alle seine Kunden gleichzeitig. Die Arbeitshilfe regelt in M2 die Verträge, nicht aber die Zugänge selbst.

Was Sie tun sollten: Lassen Sie sich alle Fernzugänge auflisten (wer, wohin, welches Werkzeug). Jeder Zugang ist personalisiert, mit Mehrfaktor-Authentifizierung gesichert, wird nur bei Bedarf freigeschaltet und protokolliert. Dauerhaft offene Remote-Desktop- oder TeamViewer-Zugänge aus dem Internet werden abgeschaltet. Prüfen Sie die Dienstleisterkonten quartalsweise. Im Vertrag (M2) sollten stehen: Reaktionszeiten, Meldung von Vorfällen beim Dienstleister an Sie innerhalb von 24 Stunden, Regeln für Subunternehmer, Speicherort der Daten, Datenrückgabe und Kündigung. Der Ausfall des Dienstleisters oder ERP-Anbieters gehört als Szenario in Ihren Notfallplan (M12).

2.8 Korrigierte Zuordnung zu den Stufen (ergänzt Kapitel 6 der Arbeitshilfe)

Die Stufenlogik der Arbeitshilfe ist richtig, an einigen Stellen aber nicht konsequent. Die folgende Tabelle zeigt, wo wir eine andere Einordnung empfehlen. Alle übrigen Maßnahmen bleiben in der Stufe der Arbeitshilfe.

Maßnahme	Stufe lt. Arbeitshilfe	Empfehlung VdW Bayern	Begründung
Offline- oder unveränderliches Backup (M4)	4	1	Ohne diese Eigenschaft wird das Backup beim Angriff mitverschlüsselt
Notfallkarte, Kontaktliste, Meldewege (M5)	2	1	Kostet nichts und entscheidet in der ersten Stunde
Rechtsrahmen und NIS2-Betroffenheit (M6)	keine Zuordnung	1	Pflichtprüfung mit Fristen
Protokollierung mit Alarmen (M8)	3	2	Ohne Alarme bleibt ein Angriff wochenlang unbemerkt
Makros blockieren, lokale Adminrechte entziehen, Microsoft-365-Grundhärtung (M11)	3	2	Wenige Stunden Aufwand, große Wirkung
EDR auf allen Geräten (M13)	nicht enthalten	2	Stand der Technik, in Business Premium enthalten
Festplattenverschlüsselung mit Schlüsselsicherung (M15)	2	1	In Windows enthalten, schützt bei jedem verlorenen Laptop
Gäste-WLAN und Gebäudetechnik trennen (M18)	3	2	Geringer Aufwand; vollständige Segmentierung bleibt Stufe 3
Mobile Device Management (M19)	3	2	Intune ist in Business Premium enthalten; Diensthandys tragen Mieterdaten
KI-Nutzungsrichtlinie (M20)	3	1	Die Nutzung findet bereits statt; die Richtlinie kostet nichts
Verantwortung und Leitlinie (E1, neu)	nicht enthalten	1	Ohne benannten Verantwortlichen bleibt alles andere liegen
E-Mail-Authentifizierung und sichere Zahlungsprozesse (E2, E3, neu)	nicht enthalten	1	Kostenlos; verhindert die häufigsten Betrugsfälle
Fernwartungszugänge (E4, neu)	nicht enthalten	1	Häufigstes Einfallstor bei extern betreuter IT

3 Sofortprogramm: die ersten 90 Tage

Wenn Sie heute anfangen, sind das die Punkte für die ersten 90 Tage. Sie entsprechen Stufe 1 der Arbeitshilfe mit den Korrekturen aus Kapitel 2. Die meisten Punkte kosten keine Lizenzen, sondern Arbeitszeit, in der Regel bei Ihrem IT-Dienstleister. Nutzen Sie die Liste als Auftrag an den Dienstleister und als Protokoll für Vorstand und Aufsichtsrat. Die beiliegende Excel-Selbstbewertung enthält zu jedem Punkt Prüffragen.

Nr.	Maßnahme	Konkret	Bezug	Erledigt
1	Verantwortung klären	Vorstand oder Geschäftsführung benennt eine verantwortliche Person für Informationssicherheit (bei kleinen Unternehmen kann das ein Vorstandsmitglied sein) und unterschreibt eine Leitlinie von einer Seite: Ziele, Verantwortung, Budget, jährlicher Bericht.	E1	
2	Inventar anlegen	Liste aller Geräte, Server, Cloud-Dienste und Fachanwendungen mit Verantwortlichem, Schutzbedarf, Dienstleister, Support-Ende, Backup ja/nein, MFA ja/nein.	M1	
3	Nutzungsregeln verteilen	Zwei Seiten für alle Beschäftigten: Passwörter, E-Mail, private Nutzung, mobile Geräte, Homeoffice, KI-Tools, Meldung bei Verdacht. Unterschrift oder Bestätigung dokumentieren.	M1, M20	
4	Altsysteme ablösen	Windows 10, Exchange 2016/2019, Office 2016/2019 und andere Systeme ohne Support ablösen oder isolieren; Exchange nicht aus dem Internet erreichbar.	M9	
5	Updates automatisieren	Automatische Updates auf allen Geräten; Firewall, VPN-Gateway und Switches in den Patch-Rhythmus aufnehmen; kritische Updates innerhalb von 48 Stunden (im Dienstleistervertrag festhalten).	M9, M2	
6	Konten aufräumen	Administrator- und Benutzerkonten trennen, lokale Adminrechte entziehen, Dienst- und Dienstleisterkonten auflisten, Austritte am selben Tag sperren, Standardpasswörter ändern.	M3	
7	MFA überall	Mehrfaktor-Authentifizierung für Cloud, E-Mail, VPN, Remote Desktop und alle Administratorkonten; veraltete Anmeldeverfahren abschalten; Passwort-Manager einführen.	M10	
8	Backup absichern	Tägliches Backup, eine Kopie offline oder unveränderlich, eigene Backup-Anmeldung, Microsoft-365-Daten einbeziehen, Wiederherstellung testen und protokollieren.	M4	
9	Endgeräte schützen	EDR auf allen Geräten und Servern aktivieren (in Business Premium: Defender for Business), Windows-Firewall und Firewall am Netzübergang aktiv, keine Verwaltungsdienste aus dem Internet erreichbar.	M13	
10	Grundhärtung	Makros aus dem Internet per Richtlinie blockieren; in Microsoft 365 Sicherheitsstandards oder Conditional Access aktivieren, Gast- und Freigabeeinstellungen prüfen.	M11	
11	E-Mail-Domain absichern	SPF, DKIM und DMARC einrichten; automatische Weiterleitungen nach außen sperren; externe Absender kennzeichnen.	E2	
12	Zahlungsprozesse	Vier-Augen-Prinzip und Rückruf bei Änderung von Bankverbindungen; keine Zahlung allein auf E-Mail-Basis; Buchhaltung sensibilisieren.	E3	
13	Fernwartung regeln	Alle Fernzugänge auflisten, personalisieren, mit MFA sichern, nur bei Bedarf freischalten; dauerhafte Zugänge aus dem Internet abschalten.	E4	

Nr.	Maßnahme	Konkret	Bezug	Erledigt
14	Notfallkarte und Meldewege	Notfallkarte mit internen und externen Kontakten (Kapitel 5) an jedem Arbeitsplatz; Entscheidung über Meldungen an BayLDA und Versicherer festlegen; Datenschutzbeauftragten einbinden.	M5	
15	NIS2 und Rechtsrahmen	Betroffenheit nach 2.2 prüfen und dokumentieren; Liste der gesetzlichen und vertraglichen Anforderungen (DSGVO, GoBD, BetrVG, Versicherer, Kreditgeber) anlegen.	M6	
16	Laptops verschlüsseln	BitLocker auf allen Laptops, Wiederherstellungsschlüssel zentral sichern (Entra ID oder Active Directory); verschlüsselte USB-Datenträger.	M15	
17	Alle sensibilisieren	Briefing von 60 Minuten für alle Beschäftigten einschließlich Vorstand und Geschäftsführung, Onboarding-Baustein, Teilnahmeliste; Meldekultur ohne Schuldzuweisung.	M7	
18	KI-Richtlinie	Freigegebene KI-Tools festlegen; keine Mieter-, Konto- oder Vertragsdaten in Konsumentenversionen; Beschäftigte informieren (Art. 4 AI Act).	M20	

Danach folgen die Stufen 2 bis 4 der Arbeitshilfe mit den Anpassungen aus Kapitel 2.8. Als Zeitrahmen empfehlen wir: Stufe 2 innerhalb von zwölf Monaten, Stufe 3 innerhalb von 24 Monaten, Stufe 4 bei erhöhtem Risikoprofil oder nach Abschluss der Stufen 1 bis 3.

4 Was die Maßnahmen für Ihr Unternehmen bedeuten

Die Arbeitshilfe richtet sich an Unternehmen aller Größen, sagt aber nicht, was eine Maßnahme für ein kleines Unternehmen ohne eigene IT im Unterschied zu einem Unternehmen mit IT-Abteilung bedeutet. Die folgende Tabelle ordnet jede Maßnahme drei Unternehmenstypen zu und nennt Aufwand und Kostenklasse. Die Typen sind Orientierung, keine feste Grenze:

- **Typ A, ohne eigene IT:** bis etwa 15 Beschäftigte, IT vollständig beim Systemhaus oder beim ERP-Anbieter (Hosting). Ihre Aufgabe ist es, zu beauftragen, sich Nachweise geben zu lassen und die Verantwortung zu behalten; delegieren können Sie die Umsetzung, nicht die Verantwortung.
- **Typ B, mit IT-Verantwortlichem:** etwa 15 bis 60 Beschäftigte, eine Person kümmert sich neben anderen Aufgaben um die IT, ein Dienstleister übernimmt die Technik.
- **Typ C, mit IT-Abteilung:** ab etwa 60 Beschäftigten oder mit mehreren Standorten, eigene IT-Mitarbeitende, Dienstleister für Spezialthemen.
- **Aufwand:** niedrig (bis ein Personentag), mittel (bis fünf Personentage), hoch (Projekt). **Kosten:** keine (mit vorhandenen Lizenzen und Bordmitteln), gering (bis etwa 5.000 Euro), erheblich (darüber). Richtwerte für ein Unternehmen mit 30 Beschäftigten; Dienstleisterstunden nicht eingerechnet.

Nr.	Maßnahme	Typ A: ohne eigene IT	Typ B: mit IT-Verantwortlichem	Typ C: mit IT-Abteilung	Aufwand / Kosten
M1	Asset-Inventar und Nutzungsregeln	Dienstleister liefert die Liste aller Geräte und Dienste; Sie ergänzen Verantwortliche und Schutzbedarf. Nutzungsregeln auf zwei Seiten, von allen bestätigt.	Excel-Inventar mit Support-Ende, Dienstleister, Backup und MFA je System; jährliche Aktualisierung; Nutzungsrichtlinie inkl. Homeoffice und Kl.	Werkzeuggestütztes Inventar (Intune, Netzwerkscan), Klassifizierung der Informationen, Prozess für Neu- und Abgänge.	niedrig bis mittel / keine
M2	Lieferanten und Dienstleister	Vertrag prüfen: Reaktionszeiten, Meldung von Vorfällen binnen 24 Stunden, Fernwartung, Datenrückgabe; AVV; jährlich Zertifikat oder Auditbericht anfordern.	Zusätzlich Dienstleister-Checkliste, Nachweise in einer Akte, Zugänge quartalsweise prüfen.	Lieferantenbewertung, Auditrecht, Exit-Plan, Bewertung des Konzentrationsrisikos (ein Anbieter für alles).	mittel / keine bis gering
M3	Benutzer- und Zugangsverwaltung	Dienstleister trennt Admin- und Benutzerkonten; Austrittsmeldung am selben Tag; jährliche Rechteliste vom Dienstleister anfordern und abzeichnen.	Rollenkonzept im ERP mit Funktionstrennung, Ein- und Austrittscheckliste, Dienstkonten inventarisiert.	Identitätsmanagement, regelmäßige Rezertifizierung der Rechte, besondere Absicherung der Administratoren.	niedrig bis mittel / keine
M4	Datensicherung	Dienstleister bestätigt schriftlich: täglich, eine Kopie offline oder unveränderlich, Microsoft 365 einbezogen, Wiederherstellungstest mit Protokoll.	3-2-1-Regel, eigene Backup-Anmeldung, quartalsweise Stichprobe, jährlicher Volltest, Wiederanlaufreihenfolge dokumentiert.	Unveränderlicher Speicher, Wiederanlaufplan je System, jährlicher Volltest mit Zeitmessung.	mittel / gering

Nr.	Maßnahme	Typ A: ohne eigene IT	Typ B: mit IT-Verantwortlichem	Typ C: mit IT-Abteilung	Aufwand / Kosten
M5	Sicherheitsvorfälle	Notfallkarte an jedem Arbeitsplatz, Kontaktliste, Meldewege geklärt, Datenschutzbeauftragter eingebunden.	Notfallplan in fünf Schritten (erkennen, isolieren, bewerten und melden, wiederherstellen, nachbereiten), jährliche Tischübung.	Incident-Response-Prozess, Forensik-Dienstleister vorab vereinbart, regelmäßige Übungen, Kommunikationsplan.	niedrig / keine
M6	Rechtsrahmen	NIS2-Betroffenheit prüfen und dokumentieren; DSGVO-Grundpflichten; Verfahrensdokumentation nach GoBD vom ERP-Anbieter anfordern.	Anforderungsliste (Gesetz, Vertrag, Versicherer, Kreditgeber) mit Zuordnung zu Maßnahmen und Nachweisen.	Compliance-Register, jährliche Überprüfung mit Rechtsberatung, Berichterstattung an Aufsichtsrat.	niedrig / keine bis gering
M7	Schulung und Sensibilisierung	Jährliches Briefing von 60 Minuten für alle inkl. Vorstand, Baustein im Onboarding, Teilnahmeliste.	Zusätzlich Phishing-Simulation (mit Betriebsrat abgestimmt), monatliche Kurzhinweise.	Schulungsplattform, rollenspezifische Schulungen, Kennzahlen (Klickrate, Teilnahmequote).	niedrig / keine bis gering
M8	Protokollierung	Dienstleister richtet die Microsoft-365-Alarme ein (fehlgeschlagene Anmeldungen, neue Administratoren, Weiterleitungsregeln) und meldet Auffälligkeiten.	Protokolle 90 Tage zentral, Alarmer an den IT-Verantwortlichen, Zeitsynchronisation geprüft.	Zentrales Logmanagement, definierte Alarmregeln, Vereinbarung mit dem Betriebsrat.	niedrig bis mittel / keine bis gering
M9	Patchmanagement	Automatische Updates; Dienstleister patcht Server, Firewall und VPN monatlich, kritische Updates binnen 48 Stunden (vertraglich); Windows 10 und Exchange 2016/2019 abgelöst.	Patch-Kalender, Testgerät für ERP-Updates, Support-Ende-Spalte im Inventar.	Patchmanagement-Werkzeug, regelmäßiger Schwachstellenscan, Berichterstattung.	mittel / gering bis erheblich (Ablösung von Altsystemen)
M10	Zugangsschutz und MFA	MFA für alle Cloud-Konten, VPN und Remote Desktop; Passwort-Manager; veraltete Anmeldeverfahren abgeschaltet.	Conditional Access, Passkeys für Administratoren, Notfallkonto mit sicher verwahrttem Passwort.	Phishing-resistente MFA (FIDO2) flächendeckend, risikobasierte Zugriffsrichtlinien.	niedrig / keine (in Business Premium enthalten)
M11	Systemhärtung	Makros aus dem Internet blockiert, keine lokalen Adminrechte, Sicherheitsstandards in Microsoft 365 aktiv.	Sicherheits-Baselines, Verwaltung lokaler Admin-Passwörter (LAPS), Freigabeliste für Software.	Application Control, zentrale Softwareverteilung, Konfigurationsmanagement.	niedrig bis mittel / keine

Nr.	Maßnahme	Typ A: ohne eigene IT	Typ B: mit IT-Verantwortlichem	Typ C: mit IT-Abteilung	Aufwand / Kosten
M12	Business Continuity	Maximale Ausfallzeit je Prozess festgelegt, Notbetrieb auf Papier beschrieben, Kontaktliste offline, Ersatzkommunikation (Telefonliste, Messenger).	Notfallhandbuch, Wiederanlaufreihenfolge, jährliche Tischübung, Ausfall des Dienstleisters als Szenario.	BCM-Prozess, technische Übungen, Kommunikationsplan für Mieter und Presse.	mittel / keine
M13	Viren- und Malwareschutz, Firewall	EDR (Defender for Business) auf allen Geräten, Windows-Firewall und Firewall am Netzübergang, DNS-Filter.	Zentrale Konsole, Alarmer werden bearbeitet, Firewall-Regelwerk jährlich geprüft.	MDR-Dienst, Firewall-Review, Erkennung im Netzwerk.	niedrig / keine bis gering
M14	Physischer Zugang	Serverschrank abgeschlossen, Clean Desk, Schlüssel- und Transponderliste, Regeln für Papierakten im Homeoffice.	Zutrittsprotokoll für den Serverraum, Besucherregelung, Multifunktionsgeräte im Blick.	Elektronisches Zutrittssystem, Gefahrenmeldeanlage, Zonenkonzept.	niedrig / keine bis gering
M15	Verschlüsselung	BitLocker auf allen Laptops, Schlüssel in Entra ID gesichert, verschlüsselte USB-Datenträger.	Sicherer Austauschweg für Mieter- und Kontodaten (Portal oder Freigabe), Server- und Backup-Verschlüsselung.	Inhaltsverschlüsselung für E-Mail (S/MIME oder Gateway), Schlüsselmanagement.	niedrig / keine
M16	Cyberversicherung	Angebote einholen, Fragebogen wahrheitsgemäß beantworten, Hotline in die Notfallkarte.	Deckung an Umsatz und Risiken angepasst, Obliegenheiten jährlich geprüft.	Abstimmung mit dem Risikomanagement, Selbstbehalt bewusst gewählt, Forensik-Retainer geprüft.	niedrig / erheblich (Prämie)
M17	Schwachstellenscan und Pentest	Externer Schwachstellenscan quartalsweise durch den Dienstleister; Microsoft Secure Score beachten.	Jährlicher Scan innen und außen, alle zwei bis drei Jahre ein Penetrationstest, Nachtest nach Behebung.	Regelmäßige Penetrationstests, Konfigurationsprüfung der Cloud-Umgebung, Befundverfolgung.	niedrig bis mittel / gering bis erheblich
M18	Netzwerksegmentierung	Gäste-WLAN getrennt, Gebäudetechnik nicht im Büronetz, WLAN mit WPA3 und ohne Gemeinschaftspasswort.	VLANs mit Firewall-Regeln: Büro, Server, Gäste, Gebäudetechnik, Drucker; Netzplan vorhanden.	Zonenkonzept, Netzwerkzugangskontrolle, Management-Netz getrennt.	mittel / gering bis erheblich
M19	Mobile Device Management	Intune für Diensthandy und Laptops (in Business Premium enthalten): PIN, Verschlüsselung, Fernlöschung.	App-Schutz und Container, Regel für private Geräte, Abstimmung mit dem Betriebsrat.	Vollständiges Geräte- und App-Management, Compliance-Richtlinien.	niedrig bis mittel / keine

Nr.	Maßnahme	Typ A: ohne eigene IT	Typ B: mit IT-Verantwortlichem	Typ C: mit IT-Abteilung	Aufwand / Kosten
M20	KI-Nutzungsrichtlinie	Richtlinie auf zwei Seiten, freigegebene Tools, keine Mieter- und Kontodaten in Konsumentenversionen, Information der Beschäftigten.	Freigabeprozess für neue Tools, Berechtigungsprüfung vor Copilot-Einführung (SharePoint, Teams).	KI-Governance, Datenschutz-Folgenabschätzung bei Mieterdaten, Protokollierung.	niedrig / keine
M21	Redundanz und Verfügbarkeit	Prüfen, ob ein eigener Server noch nötig ist (Hosting); USV an Server und Router; Wartungsverträge.	Zweiter Internetanschluss, Temperaturüberwachung, Ersatzhardware, Alter der Hardware im Inventar.	Redundante Infrastruktur oder Rechenzentrum, Monitoring, Notfallübungen.	mittel / gering bis erheblich
M22	SIEM	Nicht nötig; EDR mit Alarmen reicht.	MDR-Dienst des Dienstleisters statt eigenem SIEM.	SIEM mit definierten Anwendungsfällen und Bereitschaft, oder MDR.	hoch / erheblich
E1	Verantwortung und Leitlinie (neu)	Vorstand oder Geschäftsführung benennt einen Verantwortlichen (kann ein Vorstandsmitglied sein), Leitlinie auf einer Seite.	IT-Verantwortlicher als Sicherheitskoordinator, jährlicher Bericht an die Leitung.	Informationssicherheitsbeauftragter mit Berichtslinie zur Geschäftsführung, Budget, Bericht an den Aufsichtsrat.	niedrig / keine
E2	E-Mail-Authentifizierung (neu)	Dienstleister richtet SPF, DKIM und DMARC ein, Weiterleitungen nach außen gesperrt, externe Absender gekennzeichnet.	DMARC-Berichte ausgewertet, Richtlinie auf „abweisen“ gesetzt.	E-Mail-Gateway mit Sandbox, Überwachung ähnlicher Domains.	niedrig / keine
E3	Sichere Zahlungsprozesse (neu)	Vier-Augen-Prinzip, Rückruf bei Bankverbindungsänderung, Mieter über Kommunikationswege informiert.	Freigabegrenzen im ERP, Stammdatenänderungen protokolliert und geprüft.	Workflow mit Freigaben, automatischer Abgleich von Rechnungsdaten.	niedrig / keine
E4	Fernwartungszugänge (neu)	Liste aller Fernzugänge, personalisiert, mit MFA, Freischaltung nur bei Bedarf.	Protokollierung der Zugriffe, Quartalsprüfung der Dienstleisterkonten.	Zentraler Zugangspunkt (Jump-Host oder PAM), Aufzeichnung der Sitzungen.	niedrig / keine bis gering

5 Melde- und Kontaktwege in Bayern

5.1 Die erste Stunde: was Sie bei einem Verdacht tun

1. **Gerät vom Netz trennen, nicht ausschalten:** WLAN deaktivieren, Netzkabel ziehen. Ausschalten vernichtet Spuren, die der Forensiker braucht, und kann Systeme zusätzlich beschädigen.
2. **Melden:** interne verantwortliche Person und IT-Dienstleister anrufen (Notfallnummer, nicht die allgemeine Hotline). Lieber einmal zu viel melden als einmal zu wenig.
3. **Nichts löschen, nichts bezahlen, nichts antworten:** keine Kommunikation mit Erpressern ohne Abstimmung mit Versicherer, Rechtsbeistand und Polizei. BSI und Strafverfolgungsbehörden raten von Lösegeldzahlungen ab; Zahlungen an sanktionierte Gruppen können strafbar sein.
4. **Datenschutzbeauftragten einbinden:** Die 72-Stunden-Frist für die Meldung an das BayLDA läuft ab Kenntnis.
5. **Versicherer anrufen:** Die Hotline aus der Police vermittelt in der Regel Forensik und Krisenberatung; die Meldung ist Voraussetzung für die Leistung.
6. **Passwörter erst von einem sauberen Gerät ändern:** Sonst liest der Angreifer das neue Passwort gleich mit. Bei Microsoft 365 zusätzlich Sitzungen beenden und MFA-Methoden prüfen (siehe 2.1).
7. **ZAC anrufen:** Die Zentrale Ansprechstelle Cybercrime berät auch, wenn Sie noch keine Anzeige erstatten wollen.
8. **Dokumentieren:** Uhrzeit, wer was beobachtet und getan hat, Screenshots, Erpresserschreiben aufbewahren. Das Protokoll brauchen Sie für Versicherer, Aufsichtsbehörde und Prüfer.

5.2 Kontakte

Tragen Sie die Kontakte in Ihre Notfallkarte und Ihren Notfallplan ein und ergänzen Sie die internen Nummern. Stand der externen Angaben: 31.08.2026, bitte vor Nutzung prüfen.

Anlass	Stelle	Kontakt	Frist / Hinweis
Datenschutzverletzung (Art. 33 DSGVO)	Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Ansbach	Online-Meldeformular: lda.bayern.de/de/datenpanne.html Telefon 0981 180093-0 poststelle@lda.bayern.de	72 Stunden ab Kenntnis; vorläufige Meldung mit Nachmeldung möglich; Betroffene bei hohem Risiko benachrichtigen (Art. 34)
Strafanzeige, Beratung bei Cyberangriffen	Zentrale Ansprechstelle Cybercrime (ZAC) beim Bayerischen Landeskriminalamt	Telefon 089 1212-3300 zac@polizei.bayern.de Online: zac-formular.polizei.bayern.de Im akuten Notfall: 110	Zuständig für alle bayerischen Unternehmen, Verbände und Behörden; berät auch ohne Anzeige
Meldung nach NIS2 (nur betroffene Einrichtungen)	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Meldeportal: mip2.bsi.bund.de Registrierung: portal.bsi.bund.de	Erstmeldung 24 Stunden, Folgemeldung 72 Stunden, Abschlussbericht ein Monat
Verdacht auf Spionage oder Sabotage durch staatliche Akteure	Cyber-Allianz-Zentrum Bayern (CAZ) beim Landesamt für Verfassungsschutz	Telefon 089 31201-222 caz@lfv.bayern.de	Vertrauliche Beratung, keine Strafverfolgungsbehörde

Anlass	Stelle	Kontakt	Frist / Hinweis
Versicherungsfall	Ihr Cyberversicherer	Hotline laut Police (in die Notfallkarte eintragen)	Unverzüglich; Obliegenheit aus dem Vertrag
Zahlungsbetrug	Ihre Hausbank	Betreuer und Sperrnummer der Bank	Sofort; Rückruf und Rückbuchung nur in den ersten Stunden aussichtsreich
Technische Hilfe	Ihr IT-Dienstleister, Ihr ERP-Anbieter	Notfallnummern laut Vertrag (in die Notfallkarte eintragen)	Reaktionszeit laut Vertrag (M2)
Fragen zur Arbeitshilfe, Vermittlung, Vorlagen	VdW Bayern Digital Solutions GmbH	Christian Fischer, Geschäftsführer christian.fischer@vdwbayern.de Mobil 0171 2181213	Keine Notfallstelle; Beratung und Einordnung

5.3 Melden oder nicht melden?

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn Daten vernichtet, verloren, verändert, unbefugt offengelegt oder unbefugt zugänglich werden. Dazu gehören der Datenabfluss nach einem Phishing-Angriff, der verlorene unverschlüsselte Laptop, die E-Mail mit Mieterdaten an den falschen Empfänger und die Verschlüsselung durch Ransomware. Meldepflichtig an das BayLDA ist der Vorfall, wenn ein Risiko für die Betroffenen nicht ausgeschlossen werden kann. Nicht meldepflichtig ist zum Beispiel der Verlust eines vollständig verschlüsselten Laptops, dessen Schlüssel sicher verwahrt ist. Im Zweifel gilt: melden, und zwar vorläufig mit Nachmeldung. Dokumentieren Sie jede Entscheidung, auch die gegen eine Meldung, mit Begründung; das verlangt Art. 33 Abs. 5 DSGVO.

6 Weiterführende Angebote

6.1 Kostenlose Angebote des BSI

- **CyberRisikoCheck nach DIN SPEC 27076:** für Unternehmen mit weniger als 50 Beschäftigten. Ein vom BSI geschulter IT-Dienstleister führt ein ein- bis zweistündiges Interview, prüft 27 Anforderungen aus sechs Themenbereichen und erstellt einen Bericht mit Punktzahl und nach Dringlichkeit geordneten Empfehlungen. Der Bericht nennt auch passende Förderprogramme. Es ist keine Zertifizierung, aber ein guter Einstieg, der sich mit Stufe 1 der Arbeitshilfe deckt. Anfallen kann nur das Honorar des Dienstleisters; Dienstleister finden Sie über die Karte auf bsi.bund.de (Suchbegriff CyberRisikoCheck).
- **Allianz für Cybersicherheit:** kostenlose Teilnahme für Unternehmen; Warnmeldungen, Webinare, Checklisten und Erfahrungsaustausch.
- **Veröffentlichungen:** „Ransomware: Bedrohungslage, Prävention und Reaktion“, „Top-Maßnahmen bei Cyber-Angriffen“ und „Die Lage der IT-Sicherheit in Deutschland 2025“ (alle auf bsi.bund.de).

6.2 Förderung: Digitalbonus Bayern

Der Digitalbonus Bayern fördert bis zum 31.12.2027 unter anderem die „Einführung oder Verbesserung von Prozessen der IT-Sicherheit“ mit 50 Prozent der Kosten, bis zu 7.500 Euro

(Digitalbonus Standard). Antragsberechtigt sind kleine Unternehmen der gewerblichen Wirtschaft mit weniger als 50 Beschäftigten und höchstens 10 Mio. Euro Umsatz oder Bilanzsumme und einer Betriebsstätte in Bayern. Ausgeschlossen sind gewerbesteuerbefreite Unternehmen (das betrifft die meisten Vermietungsgenossenschaften nach § 5 Abs. 1 Nr. 10 GewStG) und Unternehmen mit öffentlicher Beteiligung (kommunale Gesellschaften). Für kleine private Wohnungsunternehmen kann die Förderung interessant sein. Der Antrag wird online bei der zuständigen Bezirksregierung gestellt, vor Beginn der Maßnahme. Details: digitalbonus.bayern.

6.3 Angebote des VdW Bayern

Der Verband unterstützt seine Mitgliedsunternehmen mit Beratung zur Einordnung und Priorisierung, mit Seminaren und Webinaren zu IT-Sicherheit und zum Einsatz von KI, mit einem verbandseigenen KI-Angebot mit vertraglich geregelter Datenschutz, das sich als freigegebenes Tool im Sinne von M20 eignet, und mit einem Vorlagenpaket, das in Vorbereitung ist: Asset-Inventar, Notfallkarte, Gliederung für den Notfallplan, Nutzungsrichtlinie, KI-Richtlinie und Dienstleister-Checkliste. Die Selbstbewertung als Excel-Datei liegt diesem Blatt bereits bei. Wenn Sie den Einstieg gemeinsam mit anderen Mitgliedsunternehmen angehen wollen, etwa mit einem gemeinsamen Termin für den CyberRisikoCheck, vermitteln wir gern.

Ansprechpartner: Christian Fischer, Geschäftsführer der VdW Bayern Digital Solutions GmbH, christian.fischer@vdwbayern.de, Mobil 0171 2181213.

Anhang: Rechtsgrundlagen und Quellen

- GdW Arbeitshilfe 102 „Informations- und IT-Sicherheit in Wohnungsunternehmen. Vorschläge für Mindestmaßnahmen und Umsetzungsempfehlungen“, GdW Bundesverband deutscher Wohnungs- und Immobilienunternehmen e.V., August 2026.
- DSGVO Art. 28 (Auftragsverarbeitung), Art. 32 (Sicherheit der Verarbeitung), Art. 33 und 34 (Melde- und Benachrichtigungspflichten); BayLDA, Meldung einer Datenpanne: lda.bayern.de/de/datenpanne.html.
- NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), in Kraft seit 06.12.2025, insbesondere §§ 28, 30, 32, 33 und 38 BSI; BSI, Informationen für regulierte Unternehmen: bsi.bund.de; Meldeportal: mip2.bsi.bund.de. VdW Bayern, Mitgliederinformation „NIS-2 Registrierungspflicht läuft am 06.03.2026 ab“ vom 02.03.2026, vdwbayern.de.
- BSI, „Die Lage der IT-Sicherheit in Deutschland 2025“, vorgestellt am 14.11.2025; BSI, CyberRisikoCheck nach DIN SPEC 27076: bsi.bund.de.
- Bayerische Polizei, Zentrale Ansprechstelle Cybercrime: zac.polizei.bayern.de; Cyber-Allianz-Zentrum Bayern: lfv.bayern.de.
- Digitalbonus Bayern, Förderprogramm: digitalbonus.bayern (Laufzeit 01.07.2024 bis 31.12.2027).
- Microsoft, Produktlebenszyklus: Support-Ende für Windows 10, Exchange Server 2016 und 2019 sowie Office 2016 und 2019 am 14.10.2025.
- Verordnung (EU) 2024/1689 (KI-Verordnung) Art. 4 (KI-Kompetenz); § 87 Abs. 1 Nr. 6 BetrVG (Mitbestimmung bei technischen Überwachungseinrichtungen); GoBD (BMF-Schreiben), § 147 AO, § 257 HGB; § 34 GenG, § 43 GmbHG (Sorgfaltspflichten); § 5 Abs. 1 Nr. 10 GewStG (Vermietungsgenossenschaften).