GdW
Die Wohnungswirtschaft
Deutschland

GdW Arbeitshilfe 102

Informations- und IT-Sicherheit in Wohnungsunternehmen

Vorschläge für Mindestmaßnahmen und Umsetzungsempfehlungen

vtw
Die Wohnungswirtschaft
Thüringen

Vorwort

Wohnungsunternehmen verwalten große Mengen sensibler Daten und steuern eine wachsende Zahl digital vernetzter Prozesse und Anlagen – von der Buchhaltung bis zur Heizungs- und Photovoltaikanlage. Sie sind intern auf funktionsfähige digitale Prozesse angewiesen.

Mit der Digitalisierung, die enorme Chancen für Effizienz und Servicequalität bietet, verändern sich zugleich die Risiken. Ein erfolgreicher Angriff auf einzelne Mitarbeiterinnen und Mitarbeiter, eine ausgenutzte Schwachstelle in branchenüblicher Software oder eine unerwartete Betriebsunterbrechung kann spürbare Folgen haben – von ärgerlichen Verzögerungen über Reputationsschäden bis hin zu finanziellen Verlusten. Informationssicherheit ist damit längst keine reine IT-Frage mehr, sondern eine Aufgabe der Unternehmensführung.

Fachlich und methodisch ist dieses Feld gut erschlossen. Mit der ISO-27000-Reihe und dem BSI-Grundschutz stehen bewährte Regelwerke bereit. Auch der Gesetzgeber hat den Rahmen über Jahre geschärft, zuletzt mit der Umsetzung der NIS2-Richtlinie in deutsches Recht Ende 2025.

Wie dringend Maßnahmen in diesem Kontext sind, macht das Bundesamt für Sicherheit in der Informationstechnik in seinem Lagebericht 2025 unmissverständlich deutlich: Nach dem Kosten-Nutzen-Kalkül der Angreifer gebe es keine uninteressanten Ziele mehr. „Jede und jeder ist ein interessantes Ziel." Viele Angreifer agieren rein geschäftlich und dabei sehr professionell. Besonders betroffen sind kleine und mittlere Organisationen, deren Schutzniveau noch nicht ausreicht.

Die eigentliche Herausforderung liegt heute nicht mehr im Mangel an Wissen, sondern darin, das Richtige in der eigenen Organisation tatsächlich umzusetzen – strukturiert, angemessen und mit Augenmaß. Genau hier setzt die vorliegende Arbeitshilfe an. Sie richtet sich an Wohnungsunternehmen aller Größen und unterstützt sie dabei, einen strukturierten und risikobasierten Einstieg in die IT- und Informationssicherheit zu finden. Sie hilft, schnell handlungsfähig zu werden, indem sie einem klaren Prozess folgt und dabei einen realistischen Blick auf die Maßnahmen behält.

Ich bedanke mich für die Erstellung dieser Arbeitshilfe insbesondere bei der AG „IT-Sicherheit" des Fachausschusses IT und Digitalisierung des vtw (Verband Thüringer Wohnungs- und Immobilienwirtschaft e. V.).



Axel Gedaschko
Präsident
GdW Bundesverband deutscher Wohnungs- und Immobilienunternehme

Inhaltsverzeichnis

1	Zielstellung der Anwendungshilfe	1
2	Informationssicherheit und IT-Sicherheit – wo liegt der Unterschied?	1
3	Risikobasierter Ansatz: Schützen, was wirklich wichtig ist	2
4	Ausgangsbasis: Relevante Prozesse und Systeme identifizieren und Auswirkungen analysieren	2
5	Empfohlene Mindestmaßnahmen	3
5.1	M1 Asset-Inventar und Nutzungsregeln	3
5.2	M2 Sicherheitsanforderungen an Lieferanten und Dienstleister	3
5.3	M3 Benutzer- und Zugangsverwaltung	4
5.4	M4 Datensicherung (Backup)	4
5.5	M5 Umgang mit Sicherheitsvorfällen	5
5.6	M6 Aufnahme gesetzlicher und vertraglicher Anforderungen	5
5.7	M7 Schulung und Sensibilisierung der Mitarbeitenden	5
5.8	M8 Protokollierung und Monitoring	6
5.9	M9 Update- und Patchmanagement	6
5.10	M10 Zugangsschutz und Multi-Faktor-Authentifizierung	6
5.11	M11 Systemhärtung und Softwarekontrolle	7
5.12	M12 Business Continuity und Notfallplanung	7
5.13	M13 Viren- und Malwareschutz sowie Firewall	7
5.14	M14 Physisches Zugangsmanagement	8
5.15	M15 Verschlüsselung – E-Mail-Transportweg und sichere Datenspeicher	8
5.16	M16 Cyberversicherung	8
5.17	M17 Penetrationstest und Schwachstellenscan	9
5.18	M18 IT-Netzwerksegmentierung und Netzwerkschutz	9
5.19	M19 Mobile Device Management (MDM)	10
5.20	M20 KI-Nutzungsrichtlinie	10
5.21	M21 Redundanz und Verfügbarkeitssicherung	10
5.22	M22 SIEM – Security Information and Event Management	11
6	Umsetzungsempfehlungen: Prioritäten für Wohnungsunternehmen	11
6.1	Vorschläge für Priorität 1-Maßnahmen: Grundlegendes IT-Sicherheitskonzept	11
6.2	Vorschläge für Priorität 2-Maßnahmen: Praxisorientiertes IT-Sicherheitskonzept	12
6.3	Vorschläge für Priorität 3-Maßnahmen: Ausführliches IT-Sicherheitskonzept	12
6.4	Vorschläge für Priorität 4-Maßnahmen: Erweitertes IT-Sicherheitskonzept	12
Anhang A: Notfallkarte bzw. Notfallsticker der Stadt und Land aus Berlin		14

1 Zielstellung der Anwendungshilfe

Diese Arbeitshilfe hat das Ziel geeignete Maßnahmen zur Informationssicherheit vorzustellen und einen dazu passenden Prozessrahmen aufzuzeigen. Sie richtet sich an Wohnungsunternehmen aller Größenklassen und möchte die hohe Komplexität des Themas durch leicht umsetzbare Arbeitspakete in der Umsetzung vereinfachen und zugänglicher gestalten. Ebenso benennt es nicht nur Maßnahmen, sondern erläutert diese zusätzlich.

Als fachliche und gedankliche Ausgangsbasis wurde dafür die Norm ISO/IEC 27001 herangezogen. Konkret geht es um den risikobasierten Ansatz und um Maßnahmen, die auf vorhandenen Risiken wirken. Oftmals starten Vorträge und Erfahrungsberichte sofort bei konkreten Maßnahmen. Dieses Vorgehen ist nicht falsch. Es führt zu schnell messbaren Ergebnissen. Dieses Vorgehen birgt das Risiko, dass weiterhin Schwachstellen in Prozessen und Systemen unerkannt bleiben.

In dieser Arbeitshilfe versuchen wir beide Vorgehensweisen zu kombinieren. Wir stellen Maßnahmenpakete vor, die Wohnungsunternehmen zum Anfang leicht und schnell umsetzen können. Die Komplexität dieser Pakete erhöht sich stetig und sie enthalten anspruchsvollere Aufgaben, sowohl für das Unternehmen, also auch die involvierten Dienstleister. Gleichzeitig integrieren wir Teilaufgaben und Teilbereiche einer umfangreichen Risikoanalyse in die einzelnen Arbeitspakete.

2 Informationssicherheit und IT-Sicherheit – wo liegt der Unterschied?

Beide Begriffe werden im Alltag häufig synonym verwendet. Es lohnt sich jedoch, sie zu unterscheiden, weil sie unterschiedliche Handlungsfelder beschreiben:

Informationssicherheit ist der übergeordnete Begriff. Sie umfasst den Schutz aller Informationen eines Unternehmens – unabhängig davon, ob diese digital oder analog vorliegen. Ziel ist es, drei Grundwerte zu schützen: Vertraulichkeit (nur Befugte haben Zugriff), Integrität (Daten sind korrekt und vollständig) und Verfügbarkeit (Daten und Systeme sind bei Bedarf nutzbar).

IT-Sicherheit ist ein Teilbereich der Informationssicherheit und konzentriert sich auf technische Systeme: Server, Netzwerke, Endgeräte, Software und Cloud-Dienste. Sie beschreibt die konkreten technischen Maßnahmen zum Schutz dieser Systeme.

Diese Arbeitshilfe deckt primär den IT-sicherheitsrelevanten Teil ab, beginnt aber mit Rahmenanforderungen aus der Informationssicherheit.

Oft fällt der Begriff Datenschutz in diesem Kontext und im speziellen die sog. TOMs, oder technisch-organisatorische Maßnahmen. Das führt allerdings oft zu Missverständnissen und fachlichen Irrungen. Datenschutz schützt ausschließlich personenbezogene Daten natürlicher Personen vor unrechtmäßiger Verarbeitung und stützt sich auf gesetzliche Grundlagen wie die DSGVO.

Die Informations- und IT-Sicherheit hingegen schützt Informationen und Systeme eines Unternehmens umfassend – unabhängig davon, ob ein Personenbezug vorliegt oder nicht. Sie

umfasst die o.g. Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Daten, Systemen und Prozessen.

Wird bei jedem Sicherheitsvorfall reflexartig „Datenschutz" gerufen, entstehen Zuständigkeitslücken: Maßnahmen werden falsch priorisiert, Verantwortlichkeiten verwischen, und echte Sicherheitsrisiken bleiben unter Umständen unbehandelt. Eine klare Abgrenzung beider Bereiche ist daher keine bürokratische Formalität, sondern Voraussetzung für ein wirksames Schutzkonzept.

3 Risikobasierter Ansatz: Schützen, was wirklich wichtig ist

Nicht jede Information und nicht jedes System braucht denselben Schutz. Der Schlüssel zu einem effizienten und verhältnismäßigen Sicherheitskonzept ist ein **risikobasierter Ansatz**: Ressourcen werden dort eingesetzt, wo die Risiken am größten sind.

Ein risikobasierter Ansatz folgt vier Grundschritten:

- Relevante Prozesse und Systeme identifizieren – Wo werden schützenswerte Informationen verarbeitet?
- Risiken bewerten – Welche Bedrohungen existieren, und wie wahrscheinlich und folgenreich wären sie?
- Maßnahmen ableiten – Welche Schutzmaßnahmen sind verhältnismäßig und wirksam?
- Überprüfen und anpassen – Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess.

> Beispiel: Ein Wohnungsunternehmen mit 500 Wohneinheiten identifiziert sein ERP-System als hochkritisch (Mieterdaten, Kontodaten, SEPA-Mandate).
> Eine einfache Tabellenkalkulation für die interne Urlaubsplanung hat dagegen einen niedrigen Schutzbedarf. Die gleichen technischen Schutzmaßnahmen für beide anzuwenden wäre unverhältnismäßig und ineffizient.
> Liegen beide Systeme allerdings auf der gleichen technischen Infrastruktur, umfassen die Schutzbedürfnisse im Endeffekt beide Anwendungen. Dem zu Grunde liegt die Logik, dass ein hoher Schutzbedarf über die Hardware-Basis auch an andere Anwendungen „vererbt“ werden kann.

4 Ausgangsbasis: Relevante Prozesse und Systeme identifizieren und Auswirkungen analysieren

Bevor technische Schutzmaßnahmen ergriffen werden können, muss ein Unternehmen wissen, welche Prozesse und Systeme existieren, welche Daten genutzt werden und auf welchen technischen Anlagen diese zum Einsatz kommen oder darauf wirken. Beispiele für typische Prozesse sind:

- Prozesse in der Mieterverwaltung (Personendaten, Bonitätsinformationen)
- Buchhaltung und Finanzsysteme (Bankverbindungen, SEPA-Mandate, Rechnungsdaten)
- Instandhaltungsmanagement (Zugangsdaten zu Liegenschaften, Schlüsselverwaltung)

- Dokumentenmanagement
- Schnittstellen zu externen Dienstleistern, Hausverwaltungssoftware, Behörden
- Betrieb und Wartung von Anlagen der Gebäudetechnik sowie Energieanlagen

> Empfehlung: Stimmen Sie zusammen im Team die wichtigsten Prozesse und Aufgaben ab, ermitteln Sie welche Daten in diesen Prozessen genutzt werden. Definieren Sie zusammen „was passieren würde, wenn" diese Daten für Sie nicht mehr zugänglich wären, nach außen gelangen, gelöscht sind. Diese Überlegungen definieren den sog. Schutzbedarf. Anschließend erstellen Sie eine einfache Liste (Asset-Inventar) aller IT-Systeme und Anwendungen. Das ergibt zusammen eine gute Basis für die Ableitung von Maßnahmen.

5 Empfohlene Mindestmaßnahmen

Die folgenden Maßnahmen basieren auf dem international anerkannten Standard ISO 27001 (Annex A). Ihre Auswahl beruht auf Erfahrungswerten, insbesondere aus erfolgten Vorfällen und Maßnahmen bei Wohnungsunternehmen. Sie stellen ein sinnvolles Mindestschutzniveau dar – unabhängig von der Unternehmensgröße. Maßnahmen mit individuell höherem Aufwand können priorisiert anhand des ermittelten Schutzbedarfs umgesetzt werden.

5.1 M1 Asset-Inventar und Nutzungsregeln

Alle informationsverarbeitenden Systeme und Geräte (PCs, Laptops, Smartphones, Server, Drucker, Cloud-Dienste) werden erfasst und mit einem klaren Schutzbedarf versehen. Zusätzlich legen verbindliche Nutzungsregeln fest, wie Mitarbeitende mit diesen Systemen und den darauf gespeicherten Informationen umzugehen haben.

Konkret: Führen Sie eine einfache Tabelle: Gerät/System – Verantwortliche Person – Schutzbedarf – Standort/Cloud. Ergänzen Sie kurze und konkrete Nutzungsregeln, die den Mitarbeitenden möglichst einprägsam und einfach zur Verfügung gestellt werden.

5.2 M2 Sicherheitsanforderungen an Lieferanten und Dienstleister

Wohnungsunternehmen beauftragen häufig externe IT-Dienstleister. Diese Dritten halten und verarbeiten Unternehmensdaten und sind ggf. für die Sicherstellung eines ganzen Prozesses verantwortlich. Insofern müssen ebenfalls angemessene Sicherheitsstandards erfüllt werden.

Konkret: Vereinbaren Sie mit allen IT-Dienstleistern und Software-Anbietern mindestens einen Auftragsverarbeitungsvertrag (AVV nach DSGVO) sowie eine Klausel zu Sicherheitsstandards.

Fragen Sie aktiv nach:

- Gibt es ein Zertifikat (ISO 27001, SOC 2)?
- Wie werden Sicherheitsvorfälle kommuniziert?

- Wie schnell werden kritische Patches eingespielt?
- Vereinbaren Sie Prozesse, um regelmäßig Zertifikate, Auditberichte und Maßnahmenkataloge einzusehen.

Beachten Sie dabei immer den genannten Anwendungsbereich möglicher Sicherheitszertifikate. Der Anwendungsbereich (Scope) beschreibt genau, in welchem Bereich Maßnahmen umgesetzt worden sind und ggf. eine Überprüfung (Audit) stattgefunden hat.

> Beispiel: Ein Wohnungsunternehmen nutzt eine Cloud-basierte Mieterportal-Lösung. Der Anbieter sollte nachweisen können, wo die Daten gespeichert sind, ob geeignete Maßnahmen zur Informationssicherheit umgesetzt sind und wie diese nachgewiesen sind, z.B. über ein Audit. Lassen Sie sich regelmäßig die dazugehörigen Zertifikate und ggf. Auditberichte zusenden.

5.3 M3 Benutzer- und Zugangsverwaltung

Jede Person erhält nur die Zugriffsrechte, die sie für ihre Aufgaben tatsächlich benötigt (Prinzip der minimalen Rechtevergabe). Administratorrechte werden restriktiv vergeben und nicht für alltägliche Aufgaben wie E-Mails lesen oder im Internet surfen genutzt.

Konkret: Prüfen Sie regelmäßig (mindestens jährlich), wer welche Rechte hat – besonders bei Personalwechsel. Richten Sie separate Admin-Konten ein, die nur für Systemverwaltungsaufgaben verwendet werden.

> Beispiel: Die Buchhalterin benötigt vollen Zugriff auf das ERP, aber keinen Zugriff auf die Instandhaltungssoftware. Der Hausmeister braucht Zugriff auf Wartungspläne, aber nicht auf Mieterdaten. Beachten Sie insbesondere die Zugriffrechte für Azubis. Im Rahmen ihrer Ausbildung sammeln sie über die Zeit oft umfangreiche Zugriffsrechte im Unternehmen.

5.4 M4 Datensicherung (Backup)

Regelmäßige Backups sind die wichtigste Schutzmaßnahme gegen Ransomware-Angriffe und Datenverlust durch technische Fehler. Backups müssen getrennt vom Produktivsystem gespeichert werden – sonst werden sie beim Angriff mit verschlüsselt.

Konkret: Tägliche automatische Sicherung aller wichtigen Daten. Aufbewahrung für mindestens drei Monate. Offline- oder Cloud-Backup, das nicht direkt vom Produktivsystem aus erreichbar ist. Regelmäßige Wiederherstellungstests (mindestens einmal jährlich) – ein Backup, das nicht wiederherstellbar ist, ist kein Backup.

> Beispiel: Nach einem Ransomware-Angriff auf das ERP-System kann ein Unternehmen mit täglichen, getrennt gespeicherten Backups den Betrieb innerhalb

von Stunden wiederherstellen. Ein Unternehmen ohne Backup verliert im schlimmsten Fall alle Mieterdaten, Buchungshistorien und Vertragsunterlagen.

5.5 M5 Umgang mit Sicherheitsvorfällen

Ein Sicherheitsvorfall – sei es eine Phishing-E-Mail, ein Datenverlust oder ein verdächtiger Systemzugriff – muss erkannt, bewertet und strukturiert bearbeitet werden. Ohne definierte Prozesse reagieren Unternehmen häufig zu spät oder falsch.

Konkret: Benennen Sie eine verantwortliche Person für IT-Sicherheitsvorfälle. Erstellen Sie einen einfachen Notfallplan (wer informiert wen, welche Systeme werden zuerst abgeschaltet). Veröffentlichen Sie den Notfallplan, machen sie diesen für ihre Mitarbeiter (auch ausgedruckt) zugänglich. Dokumentieren Sie jeden Vorfall, auch wenn er harmlos erscheint.

Beispiel: Eine Mitarbeiterin klickt auf eine Phishing-E-Mail und gibt ihr Passwort ein. Sie meldet es sofort der IT-Verantwortlichen. In unter 30 min wird das Passwort geändert, der Vorfall protokolliert und geprüft, ob Daten abgeflossen sind.

5.6 M6 Aufnahme gesetzlicher und vertraglicher Anforderungen

Wohnungsunternehmen unterliegen ggf. verschiedenen rechtlichen Anforderungen im Kontext der Informationssicherheit. Dazu gehören: DSGVO, Handelsgesetzbuch (Aufbewahrungspflichten), möglicherweise KRITIS-Verordnungen und vertragliche Verpflichtungen gegenüber Kreditgebern oder Versicherungen. Diese Anforderungen gilt es aufzunehmen, zu systematisieren und als Anforderungen für die Maßnahmenauswahl und das Risikomanagement zu nutzen (Beurteilung der eigenen Prozesse und Daten).

5.7 M7 Schulung und Sensibilisierung der Mitarbeitenden

Die meisten erfolgreichen Cyberangriffe beginnen nicht mit technischen Hacks, sondern mit menschlichem Versagen: Phishing-E-Mails, schwache Passwörter, unbedachtes Öffnen von Anhängen. Mitarbeitende sind die erste und wichtigste Verteidigungslinie eines Unternehmens.

Konkret: Führen Sie Schulung zu Informationssicherheit ein – auch für kleine Teams reicht ein halbstündiges internes Briefing mit praxisnahen Beispielen. Neue Mitarbeitende werden direkt beim Onboarding sensibilisiert. Regelmäßige kurze Hinweise (z. B. per E-Mail) zu aktuellen Bedrohungslagen. Eine sehr hilfreiche Maßnahme sind Tests von geplanten Phishing-E-Mails von einem Dienstleister Ihres Vertrauens. Diese Test-Emails sorgen für eine unmittelbare Sensibilisierung und Vergegenwärtigung von Bedrohungen. Diese Maßnahme ist sehr günstig und kann regelmäßig und dauerhaft als Maßnahme verankert werden.

5.8 M8 Protokollierung und Monitoring

Sicherheitsprotokolle (Logs) zeichnen auf, wer wann auf welche Systeme zugegriffen hat und welche Aktionen durchgeführt wurden. Sie sind unverzichtbar, um Angriffe zu erkennen und nach einem Vorfall die Ursache zu rekonstruieren.

Konkret: Aktivieren Sie System-Logs auf kritischen Servern und Anwendungen. Speichern Sie Logs getrennt vom Produktivsystem. Stellen Sie sicher, dass Logs für mindestens 90 Tage aufbewahrt werden. Prüfen Sie Logs regelmäßig auf Auffälligkeiten – bei kleinen Unternehmen reicht ein monatlicher manueller Blick.

> Beispiel: Wenn unbekannte IP-Adressen aus dem Ausland mehrfach versuchen, sich am VPN-Zugang anzumelden, ist das im Log sichtbar. Ohne Logging bleibt dieser Angriffsversuch unbemerkt – und möglicherweise gelingt der nächste Versuch.

5.9 M9 Update- und Patchmanagement

Veraltete Software ist eine der häufigsten Einfallstore für Angreifer. Bekannte Schwachstellen werden in öffentlichen Datenbanken veröffentlicht – und von Angreifern systematisch ausgenutzt, bevor Unternehmen ihre Systeme aktualisieren.

Konkret: Aktivieren Sie automatische Updates für Betriebssysteme und Anwendungen, wo möglich. Kritische Sicherheitsupdates (‚hohes Risiko') sollten innerhalb von 48 Stunden eingespielt werden. Veraltete Software ohne Hersteller-Support (End of Life) ist unverzüglich abzulösen oder zu isolieren.

> Beispiel: Windows 7 wird seit Januar 2020 nicht mehr mit Sicherheitsupdates versorgt. Ein Büro-PC mit Windows 7, der noch an das Netzwerk angeschlossen ist, ist ein offenes Einfallstor – selbst wenn alle anderen Systeme gut gesichert sind. Auch ungepatchte PDF-Reader oder Browser sind typische Schwachstellen.

5.10 M10 Zugangsschutz und Multi-Faktor-Authentifizierung

Ein gestohlenes oder erratenes Passwort genügt häufig, um vollen Zugriff auf Unternehmenssysteme zu erlangen. Multi-Faktor-Authentifizierung (MFA) oder Passkeys erschweren dies erheblich, weil ein zweiter Faktor (z. B. eine App-Bestätigung auf dem Smartphone) zusätzlich zum Passwort nötig ist.

Konkret: MFA oder Passkeys für alle Zugänge (inkl. VPN, Remote Desktop, Cloud-Dienste) einrichten – dies ist heute bei nahezu allen gängigen Systemen technisch einfach möglich. Für interne Systeme mit hochsensiblen Daten (ERP, Buchhaltung) ebenfalls MFA aktivieren. Zugriffsrechte auf das Notwendige beschränken.

5.11 M11 Systemhärtung und Softwarekontrolle

Systeme werden mit einer Vielzahl von vorinstallierten Features und Diensten ausgeliefert, die häufig nicht benötigt werden, aber Angriffsfläche bieten. Systemhärtung bedeutet: alles, was nicht gebraucht wird, wird deaktiviert.

Konkret: Deaktivieren Sie ungenutzte Dienste und Protokolle auf Servern und Clients. Beschränken Sie die Installation von Software auf autorisierte Anwendungen. Deaktivieren Sie unsichere Browser-Features (z. B. Java-Plugins, unsichere Makros in Office-Dokumenten aus externen Quellen). Nutzen Sie aktuelle, unterstützte Betriebssystemversionen. Auch die Nutzung vorhandener Sicherheitsfeatures in oft genutzten MS 365-Umgebungen gehört zur Systemhärtung. Damit verbunden sind Features wie ein Gerätemanagement, White-Listing für Anmeldeversuche aus bestimmten Ländern, die Erweiterung von Exchange-Servern mit No-Spam Proxies.

> Beispiel: Viele Ransomware-Angriffe nutzen Makros in Office-Dokumenten, die per E-Mail verschickt werden. Ist die Ausführung von Makros aus dem Internet in Office deaktiviert, schlägt dieser Angriffsweg fehl. Diese Einstellung lässt sich in wenigen Minuten in der zentralen Office-Verwaltung umsetzen.

5.12 M12 Business Continuity und Notfallplanung

Was passiert, wenn das IT-System für mehrere Tage ausfällt? Können Mietzahlungen noch verarbeitet werden? Können Handwerker-Aufträge koordiniert werden? Business Continuity bedeutet, diese Fragen im Voraus zu beantworten – nicht erst im Ernstfall.

Konkret: Definieren Sie für kritische Prozesse eine maximale Ausfallzeit und einen Minimalnotbetrieb (z. B. wichtigste Prozesse manuell oder auf Papier). Halten Sie Kontaktlisten und Notfallprozeduren offline verfügbar und testen Sie das Notfallszenario (Tischübungen und technische Übungen).

> Beispiel: Ein Ransomware-Angriff legt alle IT-Systeme für drei Tage lahm. Ein Unternehmen mit Notfallplan weiß: Mieteingang wird manuell auf Papier erfasst, Handwerker-Notfallkontakte sind auf einer Offline-Liste verfügbar, der externe IT-Dienstleister ist informiert und beginnt mit der Wiederherstellung.

5.13 M13 Viren- und Malwareschutz sowie Firewall

Auf allen Endgeräten und Servern muss eine aktuelle Antiviren- bzw. Endpoint-Protection-Software installiert und regelmäßig aktualisiert sein. Ergänzend schützt eine Netzwerk-Firewall den Datenverkehr zwischen dem internen Netz und dem Internet. Beide Maßnahmen bilden die technische Mindestabsicherung und gehören heute zur Grundausstattung jedes Unternehmens.

Konkret: Konkret: Stellen Sie sicher, dass Virenschutz auf allen Geräten aktiv und automatisch aktualisiert wird. Aktivieren Sie die integrierte Windows-Firewall oder nutzen Sie eine

Unified-Threat-Management-Appliance (UTM) am Netzwerkübergang. Prüfen Sie regelmäßig (mindestens quartalsweise), ob alle Geräte geschützt sind – besonders nach der Einrichtung neuer Systeme.

5.14 M14 Physisches Zugangsmanagement

Der physische Zugang zu Serverräumen, Technikräumen und Bürobereichen mit schutzbedürftigen Informationen muss kontrolliert und protokolliert werden. Unbefugte physische Zugriffe können Datenverlust, Manipulation oder Sabotage ermöglichen – selbst wenn alle digitalen Schutzmaßnahmen greifen.

Konkret: Serverräume sind stets abgeschlossen und nur für autorisiertes Personal zugänglich. Nutzen Sie elektronische Zugangssysteme (Chipkarte, PIN) statt einfacher Schlüssel, um Zutritt protokollieren zu können. Installieren Sie eine Gefahrenmeldeanlage (Einbruchmeldung, Brandmeldung). Stellen Sie sicher, dass Unterlagen mit schutzbedürftigen Informationen nicht offen zugänglich herumliegen (Clean-Desk-Policy).

> Beispiel: Ein Wartungstechniker erhält Zutritt zum Serverraum. Durch das elektronische Zugangssystem wird protokolliert, wer wann den Raum betreten hat. Im Fall eines Vorfalls lässt sich der Zugang lückenlos nachvollziehen und die Anzahl der Berechtigten auf ein Minimum begrenzen.

5.15 M15 Verschlüsselung – E-Mail-Transportweg und sichere Datenspeicher

Verschlüsselung schützt Daten sowohl auf dem Übertragungsweg als auch bei der Speicherung. Zwei Bereiche sind für Wohnungsunternehmen besonders relevant: die Verschlüsselung des E-Mail-Transportwegs (TLS) sowie die Festplattenverschlüsselung auf Laptops und mobilen Geräten.

Konkret: Aktivieren Sie Transport Layer Security (TLS) auf Ihrem E-Mail-Server, um E-Mails auf dem Transportweg zwischen Servern zu verschlüsseln – dies ist bei nahezu allen modernen E-Mail-Diensten standardmäßig verfügbar. Aktivieren Sie die Festplattenverschlüsselung (z. B. BitLocker unter Windows) auf allen Laptops und mobilen Geräten. So sind sensible Daten auch bei Gerätediebstahl geschützt.

Für den Datenaustausch, insbesondere mit externen Adressaten, ist es sinnvoll cloudbasierte, sichere Datenspeicher zu nutzen und den zu teilenden Inhalt direkt mit dem Adressaten zu teilen.

5.16 M16 Cyberversicherung

Eine Cyberversicherung deckt finanzielle Schäden ab, die durch Cyberangriffe entstehen – darunter Kosten für die IT-Wiederherstellung, Betriebsunterbrechungen, Benachrichtigungspflichten gegenüber Betroffenen, Anwaltskosten sowie ggf. Lösegeldforderungen. Sie ist kein Ersatz für technische Schutzmaßnahmen, aber eine wichtige Absicherung für den Schadensfall.

Konkret: Prüfen Sie, ob Ihre bestehende Haftpflicht- oder Sachversicherung Cyberrisiken abdeckt – häufig ist dies nicht der Fall. Holen Sie Angebote für eine dedizierte

Cyberversicherung ein und achten Sie auf den Leistungsumfang: Erstattung von Wiederherstellungskosten, Betriebsunterbrechungsschäden und Kosten für Krisenkommunikation. Beachten Sie, dass Versicherer häufig bestimmte Mindeststandards (z. B. MFA, aktuelle Backups) als Voraussetzung fordern.

> Beispiel: Ein Ransomware-Angriff legt das ERP-System für eine Woche lahm. Die Cyberversicherung übernimmt die Kosten für einen externen IT-Forensiker, die Systemwiederherstellung sowie den Verdienstausfall. Ohne Versicherung können solche Schadenssummen schnell im fünf- bis sechsstelligen Bereich liegen.

5.17 M17 Penetrationstest und Schwachstellenscan

Penetrationstests und Schwachstellenscans helfen dabei, Sicherheitslücken zu identifizieren, die Sensibilisierung der Mitarbeiter zu schärfen und insbesondere Prozesse und Verantwortlichkeiten im Unternehmen zu überprüfen, bevor Angreifer sie ausnutzen.

Ein einfacher Schwachstellenscan prüft automatisiert die von außen sichtbaren Systemen auf bekannte Schwachstellen. Wichtig ist, dass dies oft nur automatisierte Port-Scans sind und einen richtigen Penetrationstests nicht ersetzen können.

Ein ausführlicher Penetrationstest simuliert einen gezielten Angriff – auch von innen – und deckt komplexere Schwachstellen in Prozessen und Konfigurationen auf. Möglich sind auch gezielte physische Penetrationstests die als Service-Teams oder Lieferdienste sich Zutritt zum Unternehmen verschaffen.

Konkret: Führen Sie automatisierte Schwachstellenscan der extern erreichbaren Systeme durch (z. B. über Dienstleister oder BSI-empfohlene Tools).

Für ein ausführlicheres Bild empfiehlt sich alle zwei bis drei Jahre ein professioneller Penetrationstest durch einen zertifizierten Anbieter. Stellen Sie sicher, dass gefundene Schwachstellen systematisch behoben und die Ergebnisse dokumentiert werden.

5.18 M18 IT-Netzwerksegmentierung und Netzwerkschutz

Durch die Aufteilung des Netzwerks in separate Segmente (z. B. Büronetz, Servernetz, Gastnetz, Gebäudetechnik) wird verhindert, dass sich ein Angreifer nach einem ersten Einbruch ungehindert im gesamten Netzwerk ausbreiten kann. Netzwerksegmentierung ist eine der wirksamsten Maßnahmen, um den Schaden bei einem Sicherheitsvorfall zu begrenzen.

Konkret: Trennen Sie das Netzwerk für kritische Server (ERP, Finanzsystem) vom allgemeinen Büronetz. Richten Sie ein separates WLAN für Gäste und Besucher ein. Stellen Sie sicher, dass Gebäudetechnik und IoT-Geräte in einem eigenen Segment betrieben werden und keinen direkten Zugriff auf Bürosysteme haben. Setzen Sie Firewalls oder VLAN-Konfigurationen an den Segmentgrenzen ein.

> Beispiel: Ein Angreifer kompromittiert über eine Phishing-Mail den PC eines Mitarbeitenden. Durch die Netzwerksegmentierung kann er von diesem PC aus

nicht direkt auf den Finanzserver zugreifen. Ohne Segmentierung hätte er sich frei im gesamten Netz bewegen und alle kritischen Systeme angreifen können.

5.19 M19 Mobile Device Management (MDM)

Ein Mobile Device Management-System ermöglicht die zentrale Verwaltung aller mobilen Geräte (Smartphones, Tablets, Laptops) im Unternehmen. Es erlaubt die Durchsetzung von Sicherheitsrichtlinien, die Fernlöschung von Daten bei Verlust oder Diebstahl sowie die Kontrolle installierter Apps und Konfigurationen.

Konkret: Setzen Sie eine MDM-Lösung ein (z. B. Microsoft Intune, Jamf), um alle dienstlichen Mobilgeräte zentral zu verwalten. Erzwingen Sie Geräteverschlüsselung, PIN-Schutz und automatische Bildschirmsperrung. Ermöglichen Sie Remote-Wipe für verloren gegangene Geräte. Definieren Sie, welche privaten Apps auf dienstlichen Geräten erlaubt sind, und trennen Sie private und dienstliche Daten (Container-Lösung).

Beispiel: Ein Mitarbeitender meldet sein Diensthandy als gestohlen. Über das MDM-System kann die IT-Abteilung das Gerät sofort aus der Ferne sperren und alle Unternehmensdaten löschen – bevor ein Dritter Zugriff auf dienstliche E-Mails, Dokumente oder Zugangsdaten erlangt.

5.20 M20 KI-Nutzungsrichtlinie

KI-Tools (z. B. ChatGPT, Microsoft Copilot, Google Gemini) werden zunehmend im Arbeitsalltag eingesetzt. Ohne klare Richtlinien besteht die Gefahr, dass Mitarbeitende unwissentlich vertrauliche Unternehmensdaten, Mieterdaten oder interne Dokumente in externe KI-Dienste hochladen, wo diese zur Modellverbesserung genutzt oder gespeichert werden können.

Konkret: Erarbeiten Sie eine verbindliche Richtlinie zur Nutzung von KI-Tools. Legen Sie fest, welche Daten keinesfalls in externe KI-Dienste eingegeben werden dürfen (insbesondere personenbezogene Daten, Kontodaten, Vertragsinhalte). Definieren Sie, welche KI-Tools genehmigt sind (z. B. Unternehmensversion mit Datenschutzgarantie vs. kostenlose Konsumentenversionen). Sensibilisieren Sie Mitarbeitende regelmäßig zu diesem Thema.

5.21 M21 Redundanz und Verfügbarkeitssicherung

Redundante Systeme und Infrastruktur stellen sicher, dass kritische Prozesse auch bei einem Ausfall einzelner Komponenten weiterbetrieben werden können. Dazu zählen unterbrechungsfreie Stromversorgung (USV), redundante Internetanbindung sowie eine ausreichende Klimatisierung und Brandschutz im Serverraum.

Konkret: Statten Sie den Serverraum mit einer USV aus, die bei Stromausfall eine geordnete Abschaltung oder Überbrückung ermöglicht. Prüfen Sie die Möglichkeit eines zweiten Internetanschlusses bei einem anderen Anbieter für unternehmenskritische Prozesse. Stellen Sie sicher, dass der Serverraum ausreichend klimatisiert ist und eine funktionsfähige

Brandschutzanlage (z. B. Brandfrüherkennungssystem, CO_2-Löschanlage) vorhanden ist. Dokumentieren Sie die physische IT-Infrastruktur im Rahmen des Asset-Inventars (M1).

5.22 M22 SIEM – Security Information and Event Management

Ein SIEM-System sammelt Sicherheitsprotokolle aller IT-Systeme an zentraler Stelle, korreliert Ereignisse und erkennt Angriffsmuster automatisch. Es geht damit deutlich über das einfache Logging (M8) hinaus: Statt einzelne Logs manuell zu prüfen, analysiert ein SIEM kontinuierlich alle Daten und schlägt bei verdächtigen Mustern Alarm.

Konkret: Für kleine Wohnungsunternehmen genügt zunächst das in M8 beschriebene manuelle Logging. Wächst das Unternehmen oder erhöht sich das Risikoprofil, ist der Einsatz eines SIEM-Systems zu erwägen. Viele Cloud-Plattformen (z. B. Microsoft Sentinel, Azure) bieten SIEM-Funktionen bereits zu überschaubaren Kosten an. Definieren Sie gemeinsam mit einem IT-Dienstleister, welche Ereignisse als kritisch gelten und welche Alarmierungsprozesse etabliert werden sollen.

> Beispiel: Innerhalb weniger Minuten versuchen 500 verschiedene IP-Adressen sich über das VPN anzumelden – ein klassisches Brute-Force-Angriffsmuster. Das SIEM erkennt dieses Muster sofort und schlägt Alarm, sodass die IT innerhalb von Minuten reagieren kann. Ohne SIEM bliebe dieser Angriff möglicherweise wochenlang unbemerkt.

6 Umsetzungsempfehlungen: Prioritäten für Wohnungsunternehmen

Die folgende Prioritätenliste bietet Wohnungsunternehmen jeder Größe einen praxisorientierten Einstieg. Anstatt alle Maßnahmen gleichzeitig anzugehen, empfiehlt es sich, die Maßnahmen schrittweise nach Dringlichkeit umzusetzen. Die vier Prioritätsstufen orientieren sich an der Erfahrung der AG „IT-Sicherheit“ des FA IT und Digitalisierung des vtw und wurden für den typischen Kontext von Wohnungsunternehmen entwickelt.

Der Fokus liegt auf der internen Absicherung des Unternehmens und Geschäftssitzes. Themen rund um die Sicherheit von Wohngebäuden (z. B. smarte Gebäudetechnik, vernetzte Heizungsanlagen) sind nicht Gegenstand dieser Empfehlungen.

6.1 Vorschläge für Priorität 1-Maßnahmen: Grundlegendes IT-Sicherheitskonzept

Ohne diese Maßnahmen ist ein Wohnungsunternehmen einem erheblichen und unmittelbaren Risiko ausgesetzt. Sie sind schnell umsetzbar, kostengünstig und bilden das unverzichtbare Fundament jeder IT-Sicherheit. Beginnen Sie hier – auch wenn Sie sich erst ins Thema einarbeiten.

- Struktur, Bestandsaufnahme und IT-Richtlinie / Nutzungsregeln → M1
- Trennung von Admin- und Benutzerkonten → M3
- Datensicherung (Backup) → M4
- Führungskräftesensibilisierung → M7
- Update- und Patchmanagement → M9

- Passwortrichtlinie (komplexe, einmalige Passwörter, Passwort-Manager, Multi-Faktor-Authentifizierung) → M10
- Viren- und Malwareschutz (inkl. Firewall) → M13

6.2 Vorschläge für Priorität 2-Maßnahmen: Praxisorientiertes IT-Sicherheitskonzept

Mit diesen Maßnahmen wird das IT-Sicherheitsniveau deutlich angehoben und entspricht einem soliden, praxisnahen Standard für Wohnungsunternehmen. Sie bauen auf Priorität 1 auf und sollten zeitnah, idealerweise innerhalb des ersten Jahres nach Abschluss von Priorität 1, umgesetzt werden.

- Sicherheitsanforderungen an Lieferanten und Dienstleister → M2
- Digitales Identitäts- und Zugriffsmanagement, Rollenkonzept → M3
- Benutzereintritt und -austritt, Abteilungswechsel (On- und Offboarding) → M3
- Notfallhandbuch inkl. wichtiger Kontaktdaten → M5, M12
- Mitarbeitersensibilisierung (Schulung, Phishing-Simulation) → M7
- Physisches Zugangsmanagement (Serverraum, Büro, Gefahrenmeldeanlage) → M14
- E-Mail-Verschlüsselung des Transportwegs und sicherer Datenaustausch (TLS) → M15
- Festplattenverschlüsselung (z. B. BitLocker) → M15
- Cyberversicherung → M16
- Einfacher Penetrationstest (automatischer Schwachstellenscan, externer Angriff) → M17
- Risikoanalyse der physischen IT-Infrastruktur (Klimatisierung, Stromversorgung, Brandschutz, USV) → M21

6.3 Vorschläge für Priorität 3-Maßnahmen: Ausführliches IT-Sicherheitskonzept

Diese Maßnahmen führen zu einem ausführlichen und reifen IT-Sicherheitskonzept. Sie erfordern mehr Aufwand und ggf. spezialisiertes Know-how oder externe Unterstützung, bieten aber einen erheblichen Sicherheitsgewinn – insbesondere für Unternehmen mit größerer IT-Infrastruktur oder erhöhtem Risikoprofil.

- Elektronisches Gerätemanagement (vollständiges Asset-Inventar) → M1
- Monitoring der IT-Infrastruktur (Verfügbarkeit, Performance, Anomalien) → M8
- Softwareverteilung und zentrale Softwarekontrolle → M11
- Ausführlicher Penetrationstest (investigativer Angriff von innen, durch zertifizierten Dienstleister) → M17
- IT-Netzwerksegmentierung (Trennung Büro, Server, Gäste, Gebäudetechnik) → M18
- Mobile Device Management (MDM) für Smartphones, Tablets und Laptops → M19
- KI-Nutzungsrichtlinie für den sicheren Einsatz von KI-Tools → M20

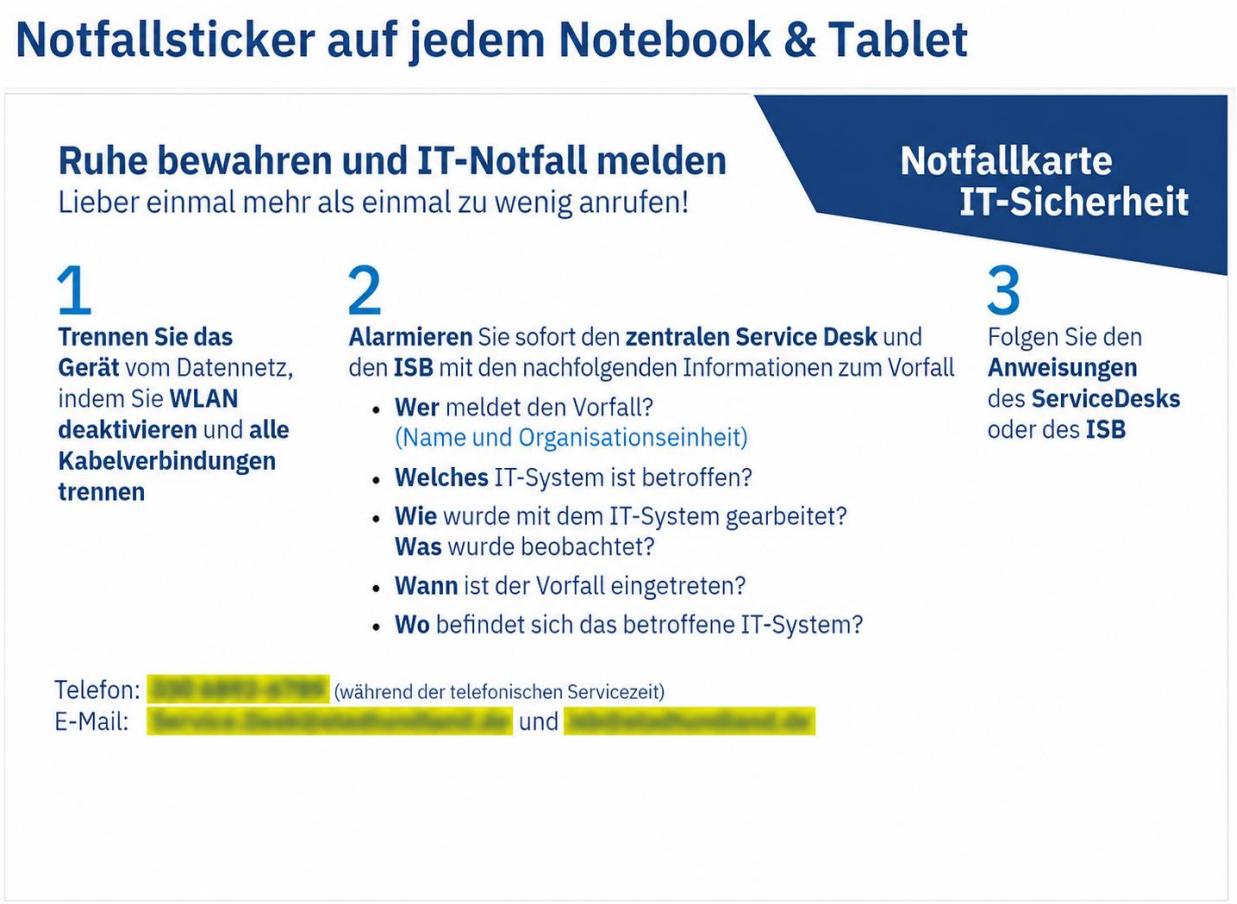
6.4 Vorschläge für Priorität 4-Maßnahmen: Erweitertes IT-Sicherheitskonzept

Diese Maßnahmen erhöhen das Schutzniveau weiter und adressieren spezifische Risiken rund um Verfügbarkeit, Angriffserkennung und administrative Sicherheit. Sie sind besonders relevant für Unternehmen mit komplexerer IT-Infrastruktur, erhöhten regulatorischen Anforderungen oder nach abgeschlossener Umsetzung der Prioritäten 1 bis 3.

- Umsetzung eines Risikomanagements, insbesondere Risikoanalyse und grundlegende Einführung eines ISMS
- Trennung von administrativen Rollen (z. B. System-Admin, Netz-Admin, Security-Admin) → M3
- Redundanz für Backup und Internetzugriff (zweiter Provider, Offline-Backup) → M4, M21
- System zur frühzeitigen Erkennung von Sicherheitsbedrohungen (SIEM) → M22

Hinweis: Die Prioritätenliste ist als Orientierung zu verstehen, nicht als starre Vorgabe. Unternehmen mit spezifischen Risiken (z. B. KRITIS-Nähe, Cloud-first-Strategie, große Außenstellen) können die Reihenfolge anpassen. Maßgeblich bleibt die individuelle Risikoanalyse gemäß Kapitel 3 dieser Arbeitshilfe.

Anhang A: Notfallkarte bzw. Notfallsticker der Stadt und Land aus Berlin



Impressum

Herausgeber:
GdW Bundesverband
deutscher Wohnungs- und
Immobilienunternehmen e.V.
Klingelhöferstraße 5
10785 Berlin

Telefon: +49 (0)30 82403-0
Telefax: +49 (0)30 82403-199

Brüsseler Büro des GdW
3, rue du Luxembourg
1000 Bruxelles

Telefon: +32 2 5 50 16 11
Telefax: +32 2 5 03 56 07

E-Mail: mail@gdw.de
Internet: http://www.gdw.de

@ GdW 2026

Der GdW Bundesverband deutscher Wohnungs- und Immobilienunternehmen e.V. ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung eingetragen und übt seine Interessenvertretung auf der Grundlage des Verhaltenskodex für Interessenvertreterinnen und Interessenvertreter im Rahmen des Lobbyregistergesetzes aus

Diese Broschüre ist als PDF zum Preis
von 15,00 EUR zu beziehen beim
GdW Bundesverband deutscher Wohnungs-
Und Immobilienunternehmen e.V.
Postfach 301573
10749 Berlin
Telefon: +49(0)30 82403-182
E-Mail: bestellung@gdw.de