

## **GdW Arbeitshilfe 102**

# **Informations- und IT-Sicherheit in Wohnungsunternehmen**

Vorschläge für Mindestmaßnahmen und Umsetzungsempfehlungen

## 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 Immobilienunternehmen

## 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 |