

Cybersecurity-Praxis im Smart Home

Günter Martin, gm@smarthome-deutschland.de, 31.10.2025



Digitale Wohn- und Pflegeumgebungen erzeugen, verarbeiten und übermitteln personenbezogene Daten. Diese Daten bilden die Grundlage für Komfort-, Sicherheits- und Assistenzfunktionen, sind aber zugleich ein Angriffspunkt für Cyberrisiken. Mit der wachsenden Integration von Cloud- und KI-basierten Diensten (z. B. SmartXpedia care) steigt der Bedarf an strukturiertem Datenmanagement und an einem IT-Sicherheitskonzept, das in den Planungsprozess integriert wird.

1	Grundlagen	3
1.1	Regulatorischer Rahmen (2025)	3
1.2	Planungs- und Umsetzungsprinzipien	3
2	Praxisfälle	5
2.1	Praxisfall: Künstliche Intelligenz	5
2.2	Praxisfall: Bot-Netze	6
2.3	Praxisfall: Türsprechanlage mit Kamera	7
2.4	Praxisfall: Mehrfachnutzung von Verbrauchsdaten	8
3	Checkliste und Warnbox	10
3.1	Checkliste	10
3.2	Warnbox: Typische Sicherheitsprobleme	11
4	Weiterführende Quellen	11

1 Grundlagen

1.1 Regulatorischer Rahmen (2025)

Die wichtigsten europäischen Rechtsgrundlagen sind der AI-Act (2024), die RED-Richtlinie, die NIS-2-Richtlinie und der Cyber Resilience Act (CRA). Diese Vorgaben verpflichten Hersteller und Betreiber zu Mindeststandards bei Cybersicherheit, Updatefähigkeit und Datenschutz.

Regelwerk	Kernaussagen	Relevanz für Wohnungswirtschaft
EU-AI-Act (2024/2025)	Regelt Entwicklung, Bereitstellung und Nutzung von KI-Systemen in der EU.	Alle Systeme mit automatisierter Entscheidungslogik (z. B. Sturzerkennung, Zutrittskontrolle, Pflege-Monitoring)
RED-Richtlinie (2024 Erweiterung)	Ursprünglich auf elektromagnetische Verträglichkeit (EMV) und Nutzung des Funkspektrums ausgerichtet, jetzt erweitert um Vorgaben zum Schutz der Privatsphäre und zur Netzresilienz.	Gilt für alle Smart-Home-Geräte mit Funkschnittstellen.
NIS-2 / Cyber-Resilience-Act (CRA)	Sicherheitsanforderungen für alle „Produkte mit digitalen Elementen, die in der Lage sind, mit anderen Produkten zu kommunizieren - Hardware und Software.“ Also tatsächlich alles, was man im SmartHome findet, selbst wenn es nur lokal verbunden ist.	Betreiber und Vermieter gelten als „Betreiber kritischer Dienste“, wenn Pflege- oder Notrufsysteme betroffen sind.
Datenschutz (GDPR/BDSG)	Schutz personenbezogener Daten. Die Wohnung ist Privatsphäre. Alles, was von dort an Daten nach außen dringt, ist privat, selbst wenn sie nicht einer konkreten Person, sondern nur einem Haushalt zugeordnet werden können.	Gilt für alle personenbezogenen und Sensordaten (Bewegung, Gesundheit, Nutzung).

Rechtsgrundlagen Cybersecurity und Datenmanagement für die Wohnungswirtschaft

1.2 Planungs- und Umsetzungsprinzipien

- Security by Design:**
Sicherheitsanforderungen bereits in der Konzeptphase für das Gebäude mit berücksichtigen. (Stakeholder-Map erweitern um IT-Security- und Datenschutzbeauftragte).
- Systembrüche vermeiden:**
Die eingesetzten digitalen Komponenten sollten mit dem gleichen Protokoll arbeiten. Jedes Interface erhöht die Komplexität und steigert das Cyber-Risiko.
- Getrennte Netzsegmente:**
Nicht nur Gebäude- und Verwaltungsnetz sollten getrennt sein, sondern auch innerhalb der

Wohnung sollten IoT-Geräte und private Endgeräte (PC, Notebook, Smartphone) in getrennten Netzsegmenten betrieben werden – beispielsweise über ein Privatnetz für die privaten Endgeräte und ein Gästenetz für die IoT am Router. Dadurch wird verhindert, dass ein kompromittiertes IoT-Gerät (z. B. Kamera, Steckdose, Sprachassistent) auf persönliche Daten oder Arbeitsgeräte zugreifen kann. Die Segmentierung begrenzt Angriffsflächen, erschwert laterale Bewegungen im Netzwerk und erhöht insgesamt die Resilienz des Smart Home gegen Schadsoftware und Botnetze.

4. **Kabel vor Funk:**

Die Datenübertragung sollte, wo immer möglich, kabelgebunden erfolgen. Kabelverbindungen sind gegenüber Funklösungen weniger stör- und abhöranfällig und bieten höhere Übertragungssicherheit. Sie erfüllen langfristig besser die Anforderungen an Datenschutz, Ausfallsicherheit und EMV-Konformität. Zudem arbeiten Sicherheitsbehörden und Industrie derzeit an sogenannten *Störsende-Systemen* („Jamming Devices“) zur Drohnenabwehr. Solche Systeme unterdrücken gezielt Funkfrequenzen – etwa WLAN, Bluetooth oder ZigBee – und könnten im Ereignisfall auch Smart-Home-Funkverbindungen beeinträchtigen. Kabelgebundene Systeme sind hiervon nicht betroffen und bleiben funktionsfähig.

5. **Edge vor Cloud:**

Wo immer möglich, sollten Daten dezentral – also direkt auf dem Gerät oder im lokalen Netzwerk („Edge“) – verarbeitet werden, statt sie in externe Cloud-Dienste zu übertragen. Das reduziert Abhängigkeiten von Internetverbindungen, verbessert Reaktionszeiten und schützt personenbezogene Daten vor unkontrolliertem Zugriff. Eine Edge-first-Architektur ermöglicht zudem den Weiterbetrieb bei Netzausfällen und erfüllt zentrale Anforderungen des Datenschutzes nach Privacy by Design (Art. 25 DSGVO) sowie des AI-Acts hinsichtlich Transparenz und Nachvollziehbarkeit. Edge-Systeme können zudem lokale Datenschutzverträge vereinfachen, da keine Übermittlung in Drittländer erfolgt. Clouds können langfristig eine Kostenfalle werden, wenn der Anbieter seine Preise unverhältnismäßig erhöht, begründet mit neuen (KI)-Funktionen, die nicht benötigt werden.

6. **Zugriffs- und Rollenmanagement:**

Nutzer-Rechte entsprechend den folgenden Rollen gestalten:

- Mieter (eigene Wohnung)
- Hausverwaltung (Systemstatus)
- Dienstleister (zeitlich beschränkter Zugriff)

7. **Aktualisierbarkeit:**

Firmware-Updates nur signiert; vertraglich gesicherte Updatepflicht des Herstellers.

8. **Bewohner-Fokus:**

Vertrauen und Nutzbarkeit sind entscheidend für die Akzeptanz smarter Technik. Da nur knapp die Hälfte der Bevölkerung über grundlegende digitale Kompetenzen verfügen, sind Einweisung, Dokumentation und leicht verständliche Störungshinweise erforderlich. Empfehlenswert ist eine einfache Kommunikationsstruktur mit Ansprechpartnern im Störfall.

9. **Transparenz:**

Speziell beim AI-Act muss für den Nutzer transparent sein, dass er mit einer KI kommuniziert. Aber auch die anderen Regelwerke verlangen Transparenz: Der Nutzer muss wissen, welche Daten erhoben werden und was mit ihnen passiert.

10. **Dokumentation:**

Risikoklassifizierung nach AI-Act, technisches Verzeichnis der Datenflüsse, Verarbeitungsverzeichnis (GDPR Art. 30).

2 Praxisfälle

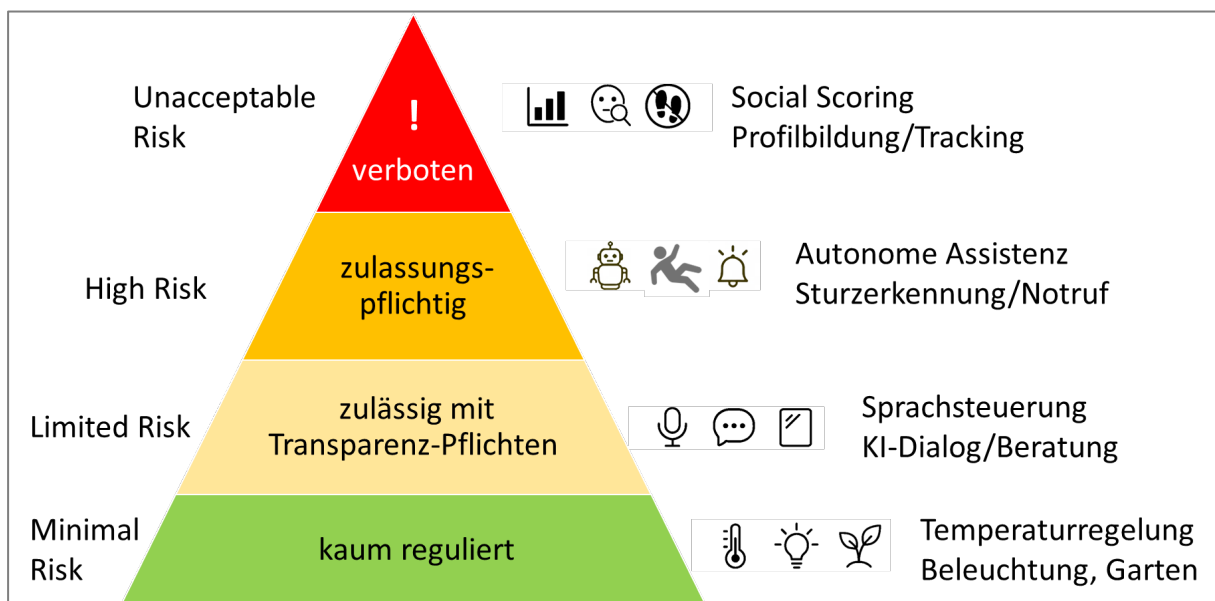
2.1 Praxisfall: Künstliche Intelligenz

Die meisten der in der Tabelle "Rechtsgrundlagen" genannten Regelwerke richten sich primär an den Hersteller/Service-Anbieter (z.B. App) oder Inverkehrbringer. Die Vorgaben und Pflichten für den Betreiber und Endnutzer sind überschaubar. Dagegen bezieht sich der AI-Act auch direkt auf die Betreiber und Nutzer.

Der AI-Act kennt vier Risikostufen (s. Abbildung), aber es geht nicht primär das technische Risiko – etwa durch Hackerangriffe oder Datenlecks. Diese Themen werden bereits durch die anderen Regelwerke abgedeckt. Der AI-Act definiert Risiko im menschenrechtlichen und gesellschaftlichen Sinn: Er fragt, welche Auswirkungen ein KI-System auf die Grundrechte, die Sicherheit und die Würde von Menschen haben kann.

Das Risiko einer KI entsteht nicht nur durch ihre Programmierung, sondern durch ihre Anwendung im konkreten Kontext. Wer etwa einen Gesichtserkennungs-Türöffner, einen Pflege- oder Serviceroboter oder ein selbstlernendes Smart-Home-System betreibt, wird rechtlich zum *Verantwortlichen für den Einsatz der KI*. Er muss sicherstellen, dass das System nur im vorgesehenen Zweck verwendet wird, keine Dritten ohne Einwilligung betrifft und die erforderliche menschliche Aufsicht gewährleistet ist.

Selbst wer die KI nachtrainiert oder Funktionen verändert, gilt bereits als Anbieter eines modifizierten Systems – mit allen Pflichten aus dem AI Act.



Risikostufen des AI-Acts mit Anwendungs-Beispielen im Smart Home

Quelle: SmartHome Deutschland Initiative e.V.

High Risk – zulassungspflichtig: KI wird in sicherheits- oder grundrechtsrelevanten Bereichen eingesetzt, z. B. biometrische Identifizierung oder Medizin. Im SmartHome wird das relevant, wenn es um Gesichts-Erkennung für die Tür-Öffnung geht oder die KI zur Sturzerkennung oder Medikamentenvergabe zum Einsatz kommt. Das ist zulässig, aber nur mit Risikomanagement, menschlicher Aufsicht, Logging, Datenqualitäts- und Bias-Kontrollen. Die Pflichten für High-Risk-Systeme gelten ab Mitte 2026.

Limited Risk – zulässig mit Transparenzpflichten: KI-Systeme, die mit Menschen interagieren, aber ohne gravierende Folgen für deren Rechte oder Sicherheit. Dazu gehören Sprachassistenten, die auf Befehle reagieren und Empfehlungen geben. Nutzer müssen erkennen können, dass sie mit einer KI interagieren. Kein verstecktes Beeinflussen oder Täuschen erlaubt.

Minimal Risk – kaum reguliert: Funktionale KI, die keine Auswirkungen auf Grundrechte oder Sicherheit hat. Beispiele im Smart Home sind die Temperatur- oder Lichtsteuerung per Mustererkennung (z. B. „lernt“, wann Bewohner nach Hause kommen) sowie die automatische Bewässerung oder Heizungsoptimierung durch einfache Lernalgorithmen.

2.2 Praxisfall: Bot-Netze

Es gibt kaum Fälle, dass SmartHome-Geräte angegriffen, um den Nutzer zu schaden oder zu erpressen. Dieses Risiko besteht vor allem beim PC zu Hause. Trotzdem werden die Geräte durchaus kontinuierlich angegriffen und es wird dabei versucht, eine Schadsoftware zu installieren, z.B. Mirai. Betroffen sind vor allem Web-Cams, NAS-Geräte und Router. Der auf Mirai basierende Raptor Train hat Ende 2024 rund 1,2 Mio. Geräte weltweit infiziert, davon 10% in Deutschland. Dahinter soll eine Staatliche Hackertruppe aus China stecken.

Diese Geräte rufen dann zentral gesteuert gleichzeitig Server auf, z.B. von Amazon, PayPal, Spotify oder Netflix, die dann aufgrund der Masse für Stunden blockiert sind. Bei Raptor Train waren auf US-amerikanische und taiwanesischen Organisationen in den Sektoren Militär, Verwaltung, Bildung, Verteidigung, Telekommunikation und IT das Ziel, die blockiert werden sollten.

Der Benutzer im SmartHome merkt davon nichts, dass seine IoT-Geräte als Waffe missbraucht werden. Bei ihm funktioniert alles unverändert. Juristisch kann er möglicherweise belangt werden. Es gilt der Grundsatz: Keine Strafbarkeit ohne Vorsatz oder Fahrlässigkeit. Sobald Fahrlässigkeit im Spiel ist – z. B. keine Sicherheitsupdates, Standardpasswort belassen, offensichtlich veraltete Firmware – kann ihm Mitverantwortung oder Ordnungswidrigkeit angelastet werden, vor allem bei gewerblichem oder organisatorischem Einsatz.

Um das zu vermeiden, sollten präventiv Maßnahmen ergriffen werden:

- Geräte mit BSI- oder CRA-konformen Sicherheitsfunktionen wählen. IoT-Anbieter sollten das Deutsche IT-Sicherheitskennzeichen des BSI vorweisen können.
- Standardpasswörter sofort ändern
- Regelmäßige Firmware-Updates durchführen
- Segmentierung des IoT-Netzes vom Verwaltungsnetz
- Unnötige Ports und Cloud-Dienste deaktivieren
- Netzwerkmonitoring zur Erkennung ungewöhnlichen Datenverkehrs einsetzen

Durch konsequente Umsetzung dieser Maßnahmen kann das Risiko einer Botnetz-Infektion drastisch reduziert werden. Zudem empfiehlt das BSI, Geräte nur aus vertrauenswürdigen Quellen zu beschaffen und bei unbekannten Herstellern auf regelmäßige Sicherheitsupdates zu achten.

2.3 Praxisfall: Türsprechanlage mit Kamera

Eine **Türsprechanlage mit Kamera** ist zulässig, aber datenschutzrechtlich sensibler als viele denken, weil sie personenbezogene Daten (Gesichter, Verhalten, Ton) verarbeitet. Hier greift die DSGVO, Art. 6 Abs. 1. Folgende Grundsätze sind zwingend einzuhalten:

Aspekt	Anforderung	Praxisempfehlung
Zweckbindung	Nur zur Zutrittskontrolle, nicht zur Dauerüberwachung	Kein Dauerstream oder Aufzeichnung außerhalb des Klingelereignisses
Erforderlichkeit	Nur so viele Daten wie nötig	Nur Bild des Eingangsbereichs, keine öffentlichen Wege oder Nachbargrundstücke
Speicherung	Nur kurzfristig	Livebild oder max. 24–48 h Speicherung (z. B. zur Nachvollziehbarkeit bei Vandalismus)
Zugriffsrechte	Nur für Berechtigte	Passwort-/App-Zugang beschränken, Logs prüfen
Transparenz	Betroffene müssen informiert werden	Betroffene müssen über die Kamera informiert werden, auch wenn sie nur durch Klingeln aktiviert wird. Der Hinweis muss nicht an der Türsprechanlage selbst angebracht sein, sondern gut sichtbar, bevor eine Person den von der Kamera erfassten Bereich betritt – beispielsweise neben der Sprechanlage, am Türrahmen oder am Zugang zum Grundstück. Auf dem vorgelagerten Hinweis sollten zumindest die Videoüberwachung bzw. Video-Türklingel, der Verantwortliche und eine Kontaktmöglichkeit erkennbar sein. Die weitergehenden Informationen nach Art. 13 DSGVO können über eine Webseite oder einen QR-Code bereitgestellt werden, s. Bild unten.
Sicherheit	Daten verschlüsselt, Updates regelmäßig	TLS-Verschlüsselung, sichere Cloud oder lokale Speicherung

DSGVO-Grundsätze bezogen auf Türsprechanlagen mit Kameras



Hinweis-Schild auf Video-Überwachung. Die vollständigen DSGVO-Informationen (z. B. Speicherdauer, Rechtsgrundlage, Rechte der Betroffenen, Auftragsverarbeiter) dürfen auf Anfrage oder in digitaler Form bereitgestellt werden. Der QR-Code zur Datenschutzerklärung wird aktuell von Aufsichtsbehörden empfohlen.

Typische Fehler sind zu vermeiden:

- Dauerhafte Aufzeichnung oder Streaming (z. B. zur Handy-App ohne Anlass)
- Erfassung öffentlicher Bereiche oder Nachbargrundstücke
- Nutzung unsicherer Cloud-Systeme mit Sitz außerhalb der EU
- Kein Hinweis oder unklare Verantwortlichkeit
- Standardpasswörter / offene Ports. Sonst wird die Kamera schnell zum Teil eines kriminellen Bot-Netzes

2.4 Praxisfall: Mehrfachnutzung von Verbrauchsdaten

Verbrauchsdaten, etwa aus Heizungs-, Warmwasser- oder Stromzählern, gelten als personenbezogene Daten im Sinne der DSGVO, da sie einem konkreten Haushalt oder Nutzer zugeordnet werden können. Ihre Erhebung ist gesetzlich (z. B. nach Heizkostenverordnung) zur Abrechnung erforderlich. Eine weitere Nutzung – etwa zur vorbeugenden Wartung, Energieoptimierung oder baulichen Analyse – ist nur unter bestimmten Bedingungen zulässig. Dabei gelten folgende Grundprinzipien

- **Zweckbindung** (Art. 5 Abs. 1 b DSGVO): Daten dürfen nur für den ursprünglichen Zweck (Abrechnung) genutzt werden.
- **Zweckänderung:** Weitere Nutzungen sind erlaubt, wenn eine Rechtsgrundlage (z. B. berechtigtes Interesse, Art. 6 Abs. 1 f DSGVO) oder eine Anonymisierung besteht.
- **Transparenzpflicht:** Mieter müssen über jede zusätzliche Verwendung informiert werden.
- **Datensparsamkeit:** Nur notwendige und technisch gesicherte Daten verarbeiten.

„Bei gemeinsamer Nutzung durch Messdienstleister ist ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO erforderlich.“

Nutzung	Zulässigkeit	Rechtsgrundlage / Voraussetzung
Heizkostenabrechnung	erlaubt	Gesetzliche Pflicht (§ 6 HeizkostenV)
Vorbeugende Wartung (Leckage, unregelmäßiger Verbrauch)	erlaubt, wenn anonymisiert oder mit Vertrag	Berechtigtes Interesse oder AV-Vertrag
Hinweis an Mieter (hoher Verbrauch)	nur mit Einwilligung	Art. 6 Abs. 1 a DSGVO
Bauliche oder energetische Analyse	erlaubt, wenn anonymisiert	Keine Personenbezüge
Benchmarking, Forschung	mit anonymisierten oder pseudonymisierten Daten	Art. 89 DSGVO
Profiling einzelner Mieter (Verhaltensanalyse)	unzulässig	Verstoß gegen Zweckbindung und Art. 22 DSGVO

Zulässige und unzulässige Nutzungen von Verbrauchsdaten

3 Checkliste und Warnbox

3.1 Checkliste

Prüffrage	Verantwortlich	Status
Ist ein IT-Sicherheitsbeauftragter benannt? Er sollte die nachfolgenden Punkte der Checkliste managen	Geschäftsführung / Datenschutzbeauftragter	☐
Sind Datenflüsse (Sensor → Gateway → Cloud) dokumentiert?	Systemintegrator	☐
Sind Mieterdaten pseudonymisiert oder nur lokal gespeichert?	Datenschutzbeauftragter	☐
Gibt es eine Meldepflichtregelung bei Cybervorfällen (NIS-2)?	Geschäftsführung	☐
Liegt für KI-Systeme eine aktuelle Risikoklassifizierung nach AI-Act vor?	Projektleiter / Systemintegrator	☐
Besteht ein Notfall-/ Backup-Konzept?	Betreiber	☐
Sind die eingesetzten IoT-Geräte aus vertrauenswürdigen Quellen, möglichst mit dem freiwilligen IT-Sicherheitskennzeichen des BSI?	Projektleiter / Systemintegrator	☐
Werden Firmware-Updates signiert / automatisiert verteilt?	Hersteller / Integrator	☐
Sind Wartungs-Zugänge protokolliert und zeitlich limitiert?	IT-Dienstleister	☐
Wurden Cyber-Schulungen für Hausmeister / Technikpersonal durchgeführt?	WG / Hausverwaltung	☐
Wird der Mieter über Datennutzung verständlich informiert?	Vermieter / Hausverwaltung	☐
Gibt es im Mietvertrag eine Anlage Datenschutz und ist diese auf aktuellem Stand?	Vermieter / Hausverwaltung	☐
Ist sichergestellt, dass bei Mieterwechsel oder Vertragsbeendigung auch digitale Zugänge (Credentials) zurückgesetzt werden?	Vermieter / Hausverwaltung	☐

Checkliste Cybersecurity und Datenmanagement

3.2 Warnbox: Typische Sicherheitsprobleme

Die nachfolgende Warnbox zeigt typische, technisch-praktische Schwachstellen, die in der Bau- und Wohnungswirtschaft häufig vorkommen und vom BSI, ENISA und in Security-Audits regelmäßig dokumentiert werden.

Problem / Schwachstelle	Risiko / Auswirkung	Empfohlene Maßnahme
Veraltete Firmware oder Standardpasswörter auf Gateways und Controllern	Unautorisierte Zugriffe, Einbindung in IoT-Botnetze (z. B. Mirai), Manipulation von Steuerdaten	Automatische Updateprozesse einrichten, sichere Passwortrichtlinien, Geräte mit BSI-/CRA-Zertifizierung verwenden
Fehlende Segmentierung von Mieter-, Verwaltungs- und Servicenetzen	Schadsoftware kann sich seitlich ausbreiten, Daten- und Funktionsverlust	VLAN- oder Subnetztrennung, separates WLAN/IoT-Gastnetz, Firewalls zwischen Segmenten
Offene Cloud-Konten ohne Multi-Faktor-Authentifizierung (MFA)	Kontoübernahme, Manipulation oder Missbrauch von Smart-Home-Diensten	MFA aktivieren, starke Passwörter, regelmäßige Kontenprüfung und Auditierung
Unverschlüsselte Kommunikation über MQTT, Modbus oder HTTP	Abhören oder Manipulation von Sensordaten und Steuerbefehlen	TLS-/VPN-Verschlüsselung aktivieren, nur sichere Protokolle zulassen, Edge-first-Architektur bevorzugen
Ransomware-Angriffe auf Gebäudeleittechnik (BMS)	Ausfall von Heizungs-, Aufzugs- oder Zugangssystemen, Betriebsunterbrechung	Regelmäßige Backups, Netzwerkisolierung, Notfall- und Wiederanlaufkonzept, Offline-Fallback
Fehlende Zugriffstrennung bei Dienstleistern oder Wartungspartnern	Unbefugter Zugriff, Datenabfluss, Manipulation von Systemen	Individuelle Accounts mit Rollenrechten, zeitlich begrenzte Freigaben, Zugriff protokollieren
Fehlende Notfallübung oder fehlend Incident-Response-Prozesse	Verzögerte Reaktion bei Cyberfällen	Regelmäßige Notfalltests, klare Meldewege nach NIS-2.

Typische Sicherheitsprobleme in der Bau- und Wohnungswirtschaft

4 Weiterführende Quellen

- EU AI Act (2024): <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689>
- BSI Deutsches IT-Sicherheitskennzeichen: <https://www.bsi.bund.de>
- Botnetze: (BSI): „Die Lage der IT-Sicherheit in Deutschland 2024“: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html>
- Cyber Resilience Act: <https://digital-strategy.ec.europa.eu>
- SmartHome Deutschland e.V.: <https://www.smarthome-deutschland.de>
- BSI-Warnung zu IoT-Botnetzen (Mirai): <https://www.bsi.bund.de>