KYOS

Cybersecurity für Wärmepumpen: Bedrohungen und Lösungsansätze

Andy Kutter, Partner und Direktor von Kyos AG, präsentiert Cybersicherheit für Wärmepumpen. Er beleuchtet Bedrohungen und Lösungen für diese kritische Technologie im IoT-Zeitalter

KYOS

Andy Kutter: Experte für Cybersicherheit

1 **Erfahrung**

Über ein Jahrzehnt in der Cybersicherheitsbranche

2 **Spezialisierung**

Innovative Sicherheitslösungen für kritische Infrastrukturen

3 **Expertise**

Risikobewertung und Schutz von IoT-Systemen

KYOS

Kyos AG: Führend in Cybersicherheit

Spezialisierung

Umfassende Cybersicherheitslösungen für Unternehmen

Dienstleistungen

Sicherheitsberatung, Implementierung von Schutztechnologien, Krisenmanagement und IT-Forensik

Partnerschaften

Zusammenarbeit mit renommierten Partnern wie Microsoft, Google, Thales, Silverfort und Cybereason

KYOS

Einleitung: Wärmepumpen im IoT-Zeitalter

Bedeutung

Wärmepumpen sind wesentlich für energieeffiziente Gebäude. Sie verbessern die Umweltbilanz und senken Energiekosten

IoT-Integration

Zunehmende Vernetzung macht Wärmepumpen anfällig für Cyberangriffe

Status Quo: IoT-fähige Wärmepumpen

1

Vorteile

Zentrale Steuerung, Überwachung und Anpassung in Echtzeit möglich

2

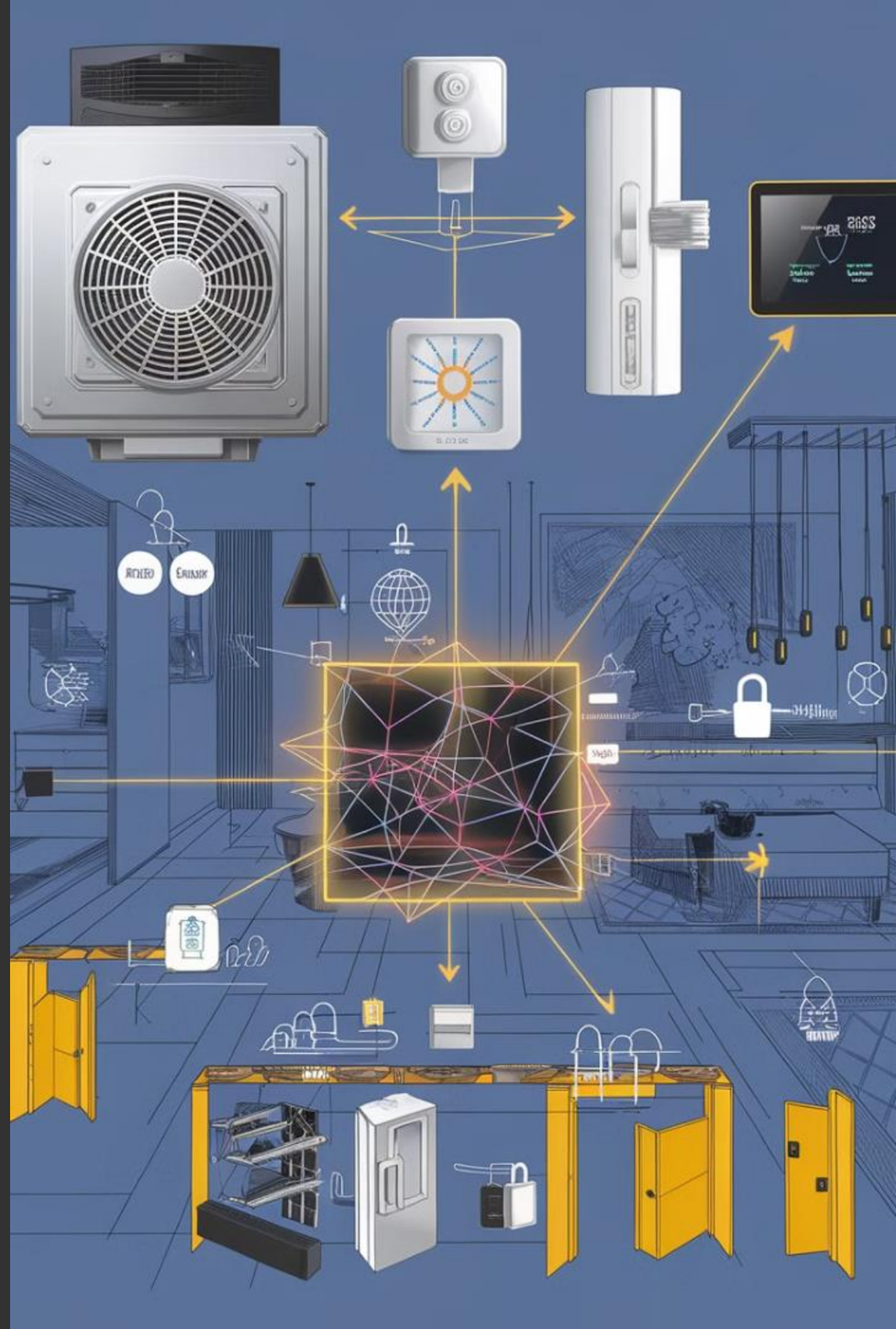
Risiken

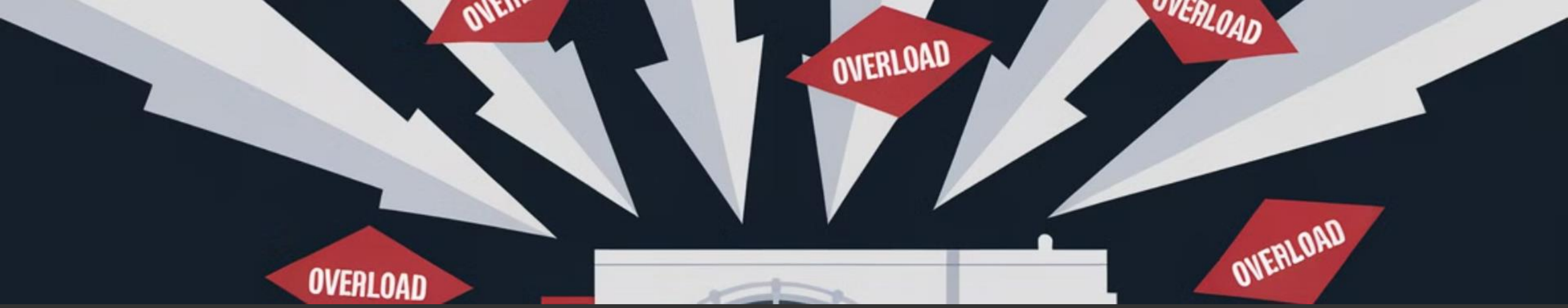
Erhebliche Sicherheitsrisiken durch unzureichende Absicherung von IoT-Geräten

3

Schwachstellen

Unverschlüsselte Kommunikation und unsichere Authentifizierung sind häufige Probleme





Angriffsvektoren: DDoS-Angriffe

Methode

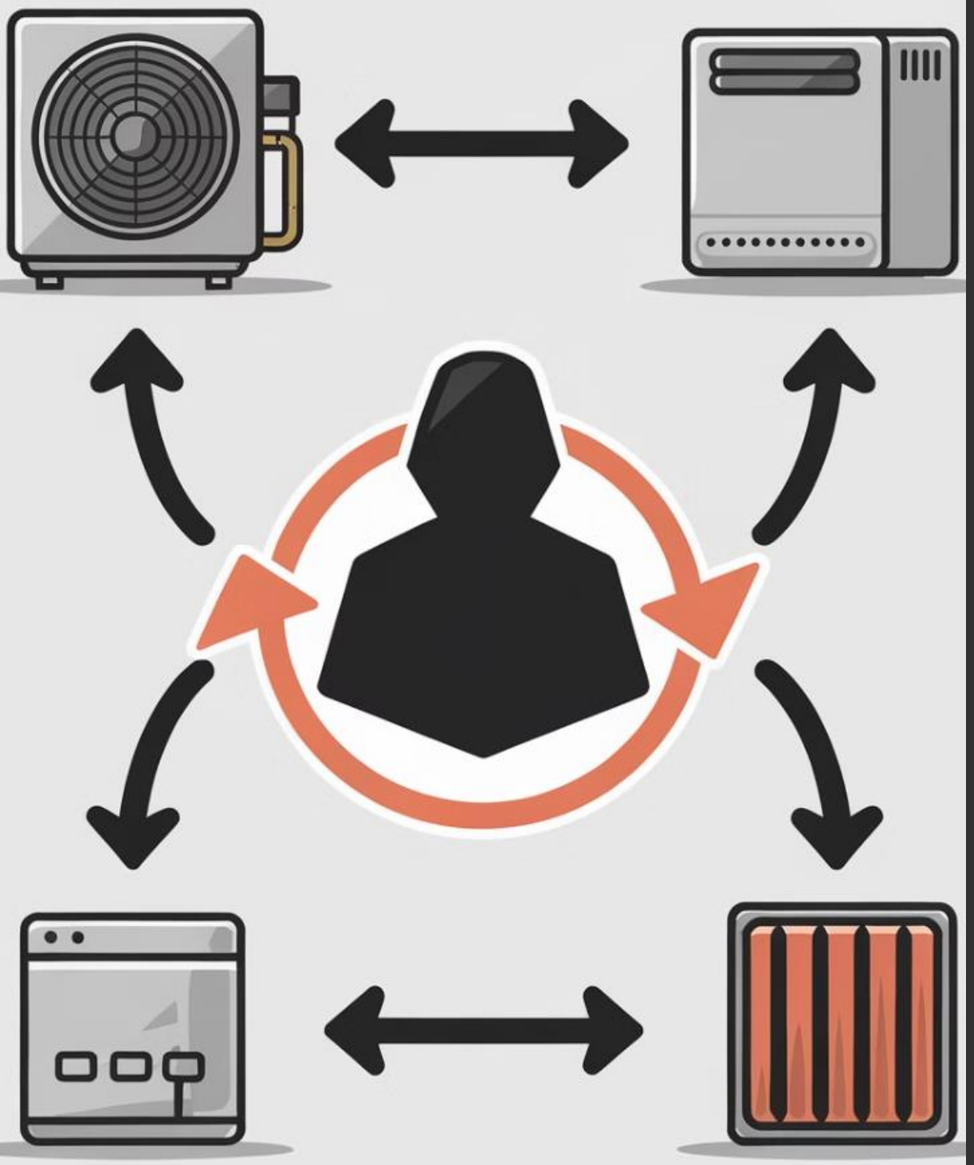
Massenhafte Anfragen überlasten ungesicherte Wärmepumpen

Auswirkung

Systemausfall der Wärmepumpe und mögliche Beeinträchtigung des gesamten Heizungssystems

Gefahr

Potenzielle Unterbrechung der Wärmeversorgung in Gebäuden



Angriffsvektoren: Man-in-the-Middle (MitM) Attacken

1

Eingriff

Angreifer fängt Kommunikation zwischen Steuergerät und Wärmepumpe ab

2

Manipulation

Daten werden verändert oder gefälschte Befehle eingeschleust

3

Folgen

Fehlsteuerung der Wärmepumpe und mögliche Energieverschwendung oder Systemschäden

Angriffsvektoren: Ransomware

1 **Vorgehensweise**

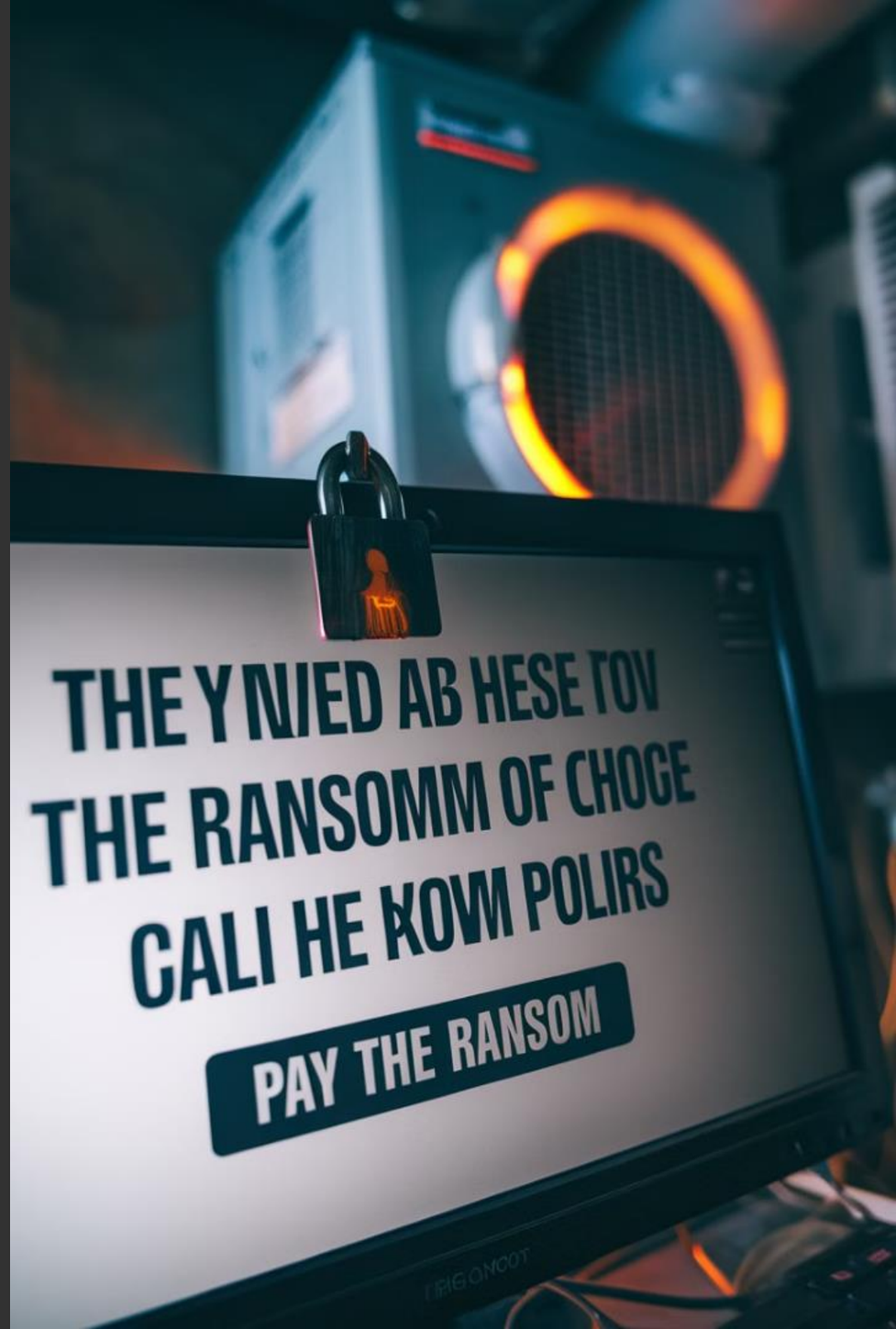
Angreifer verschlüsselt die Steuerungssoftware der Wärmepumpe

2 **Erpressung**

Freigabe der Steuerung nur gegen Lösegeld

3 **Konsequenzen**

Möglicher Ausfall der Heizung und hohe Kosten für Betroffene



KYOS

Angriffsvektoren: Datendiebstahl

Ziel

Diebstahl von Betriebsdaten wie Temperaturverläufe und Nutzungszeiten

Missbrauch

Ableitung von Anwesenheitszeiten und potenzieller Einbruchszeitpunkte

Risiko

Verletzung der Privatsphäre und erhöhte Einbruchsgefahr

Szenario: Angriff auf ein Mehrfamilienhaus

Infiltration

Angreifer kompromittiert die zentrale Wärmepumpensteuerung eines Mehrfamilienhauses

1

Manipulation

Temperatureinstellungen werden verändert, Heizzyklen gestört

2

Auswirkungen

Bewohner leiden unter Komfortverlust und erhöhten Energiekosten

3

Lösungsansatz: Netzwerksicherheit und Segmentierung

Isolation

Wärmepumpen in separate Netzwerke einbinden

Begrenzung

Angriffe auf ein Gerät bleiben lokal begrenzt

Schutz

Erhöhte Sicherheit für das Gesamtsystem

Lösungsansatz: Starke Verschlüsselung

1

Methode

SSL/TLS-Verschlüsselung für Datenübertragungen zwischen Wärmepumpen und Steuerzentralen.

2

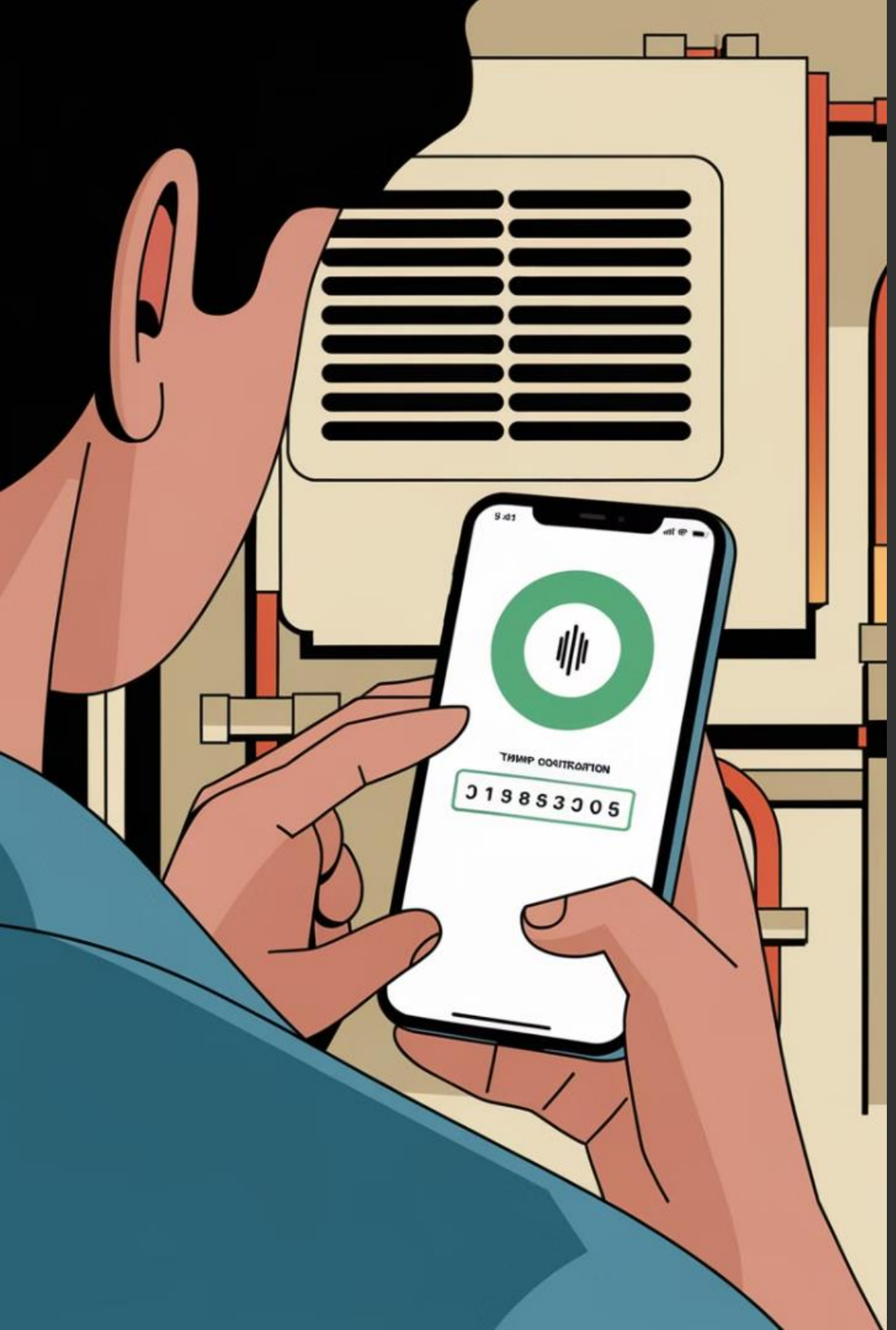
Schutz

Verhinderung von Man-in-the-Middle-Angriffen.

3

Sicherheit

Gewährleistung der Datenintegrität und Vertraulichkeit.



KYOS

Lösungsansatz: Sichere Authentifizierung

1 **Zwei-Faktor-Authentifizierung**

Zusätzliche Sicherheitsebene für den Zugriff auf Wärmepumpensysteme.

2 **Rollenbasierte Zugriffskontrollen**

Beschränkung des Zugriffs auf autorisierte Personen.

3 **Schutz**

Verhinderung unbefugter Zugriffe und Manipulationen.

Lösungsansatz: Firmware-Updates und Patching

1

Regelmässige Updates

Behebung bekannter Sicherheitslücken in Wärmepumpensoftware.

2

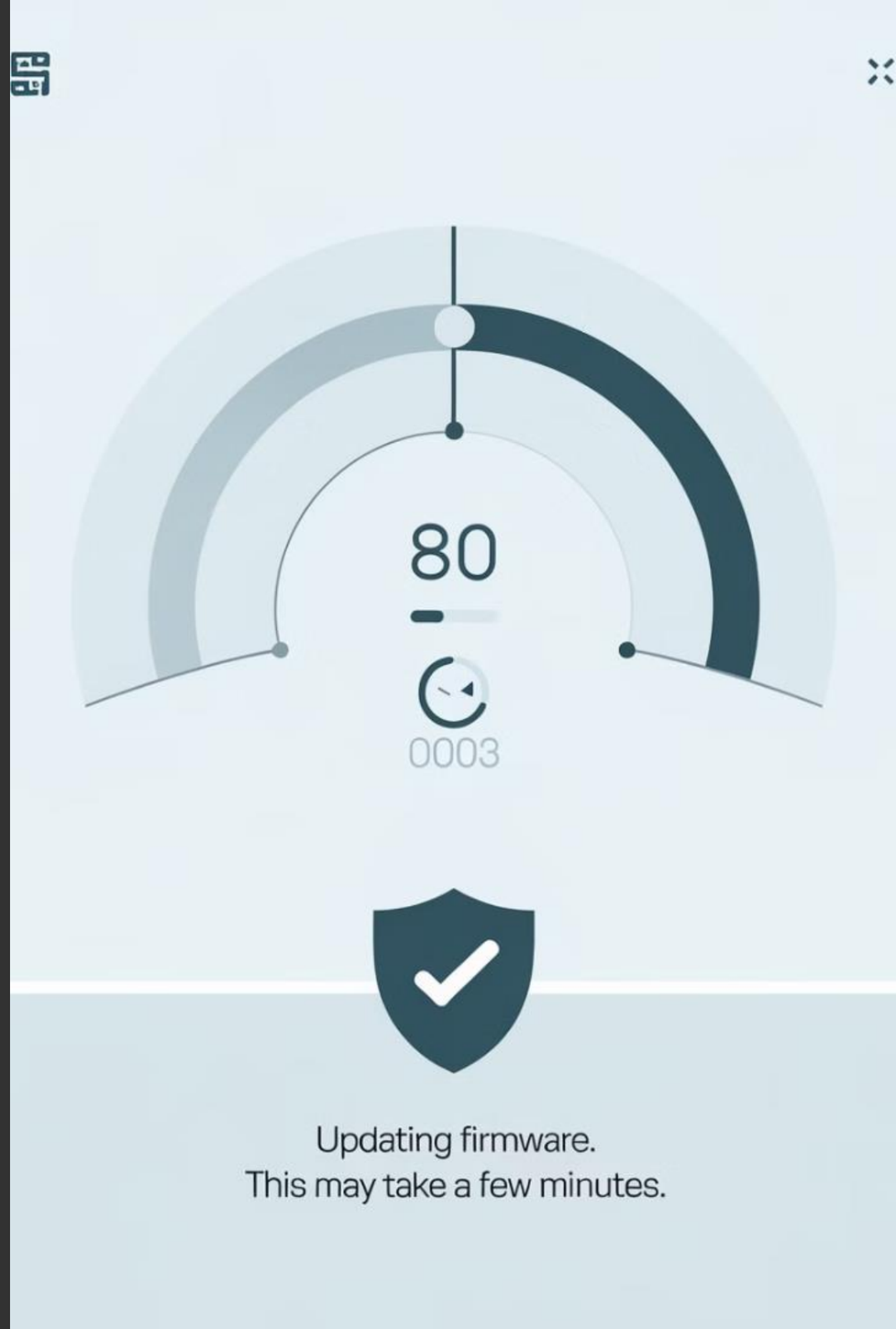
Automatisierung

Implementierung automatischer Update-Prozesse für kontinuierlichen Schutz.

3

Sicherheit

Gewährleistung des aktuellsten Sicherheitsstands für alle Geräte.



Lösungsansatz: IT-Sicherheitsstandards für IoT

IoT Securitycards

Bewertung von Sicherheitsstandards für Wärmepumpen und IoT-Geräte

Früherkennung

Identifikation von Schwachstellen vor möglichen Angriffen

Standardisierung

Etablierung einheitlicher Sicherheitsnormen für IoT-Geräte im Heizungsbereich

Fazit: Präventive Sicherheitsmassnahmen

1 Risikominimierung

Gezielte Massnahmen reduzieren Angriffspotenzial auf Wärmepumpen stark

2 Regelmässige Audits

Notwendigkeit kontinuierlicher Sicherheitsüberprüfungen zur Vorbeugung neuer Bedrohungen

3 Ganzheitlicher Ansatz

Kombination technischer und organisatorischer Massnahmen für umfassenden Schutz

Zukunftsausblick: Sichere IoT-Integration

1

Forschung

Entwicklung fortschrittlicher Sicherheitstechnologien für IoT-Geräte

2

Standardisierung

Etablierung branchenweiter Sicherheitsstandards für vernetzte Heizungssysteme

3

Bewusstsein

Förderung des Sicherheitsbewusstseins bei Herstellern und Nutzern

KYOS

Rolle von Kyos AG in der Cybersicherheit

Beratung

Unterstützung von Unternehmen bei der Implementierung sicherer IoT-Lösungen

Innovation

Entwicklung maßgeschneiderter Sicherheitslösungen für vernetzte Heizungssysteme

Schulung

Angebot von Cybersecurity-Trainings für Fachkräfte im Bereich Gebäudetechnik

Handlungsempfehlungen für Unternehmen

1 Risikoanalyse

Durchführung umfassender Sicherheitsanalysen für IoT-basierte Heizungssysteme

2 Schulungen

Regelmässige Mitarbeiterschulungen zu Cybersicherheit im IoT-Bereich

3 Partnerschaften

Zusammenarbeit mit Cybersecurity-Experten wie Kyos AG für optimalen Schutz

Kontakt und weitere Informationen

KYOS AG

Breitfeldstrasse 13

9015 St. Gallen

Telefon

+41 71/566 70 30

E-Mail

andreas.kutter@kyos.ch

KYOS