KYOS

Securing Heat Pumps in the Age of Bug Bounties

GOhack25 · 6.–8. November 2025

Andy Kutter, Partner/Director Kyos

Agenda

01

Bedrohungslandschaft 2025

Aktuelle Zahlen und Trends im Cyberspace

02

Wärmepumpen & IoT Angriffsfläche Angriffsfläche

Schwachstellen in vernetzten Heizsystemen

03

Verteidigungsstrategien

ZTNA, Verschlüsselung und Monitoring

04

5-Minuten-Checkliste

Praktische Sofortmassnahmen für Betreiber

05

Q&A + Panel-Preview

Diskussion und Ausblick auf die Expertenrunde

Bedrohungslandschaft 2025: Alarmierende Zahlen

28%

Ransomware-Anteil

der gesamten Malware-Fälle laut IBM X-Force 2025 Report

+213%

Anstieg der Opfer

Ransomware-Victims Q1/2025 vs. Q1/2024 (Optiv Studie)

62,594

Schweizer Vorfälle

Cybervorfälle 2024, +28% Zunahme (BACS/SCI)

ENISA identifiziert Ransomware als Top-Bedrohungen für kritische Infrastrukturen.
Die Zahlen zeigen: Cyberkriminelle werden aggressiver und professioneller.

Wärmepumpen & HVAC IoT: Die perfekte Angriffsfläche

Unsichere Remote-Wartung

Fehlende Multi-Faktor-Authentifizierung bei Fernzugriff ermöglicht unauthorisierten Zugang

Unverschlüsselte Protokolle

Modbus, BACnet, MQTT ohne adequate Sicherheitsmassnahmen

Cloud APIs & Mobile Apps

Schwache Authentifizierung bei Endnutzerorientierten Schnittstellen

Lateral Movement Risiken

Kopplung mit PV-Anlagen und Batteriespeichern erweitert Angriffspfade. Die Integration in Smart-Home-Ökosysteme verstärkt die Risiken eines Angriffes erheblich.

Angriffszenarien: Wenn Heizungen zum Ziel werden

DDoS auf Controller

Distributed Denial of Service Attacken führen zu kostspieligen Ausfällen und Betriebsunterbrechungen. Besonders kritisch in Wintermonaten.

Man-in-the-Middle

Manipulation von Sollwerten durch Abfangen der Kommunikation. Resultat: ineffiziente Betriebsführung und potenzielle Geräteschäden.

Ransomware in Gebäudeautomation

Verschlüsselung kritischer Steuerungssysteme führt zu kompletten Ausfällen von Heizung und Warmwasserversorgung.

Datendiebstahl: Nutzungsprofile

Gestohlene Verbrauchsdaten ermöglichen Rückschlüsse auf Anwesenheitszeiten – Privacy-Verletzung und Einbruchsrisiko.

Architektur: Segmentierung & Identitätsmanagement

Warum Segmentierung?

- Reduzierung der Angriffsoberfläche durch Isolation
- Blockierung lateraler Bewegungen im Netzwerk
- Kontrolle und Überwachung des Datenverkehrs
- Compliance mit Sicherheitsstandards

Umsetzungsmethoden

- Netzwerk-Zoning mit VLANs und Firewalls
- Multi-Faktor-Authentifizierung für Remote-Service
- Network Access Control (NAC) und Zero Trust Network Access (ZTNA)
- Mikrosegmentierung auf Application-Ebene

Best Practice: Implementieren Sie eine Defense-in-Depth Strategie mit mehreren Sicherheitsebenen für maximalen Schutz.

Kryptographie & Hardening: Integrität gewährleisten

TLS Everywhere

Verschlüsselung aller Kommunikationskanäle – von Device-to-Cloud bis hin zu internen Protokollen.
Keine Ausnahmen für "interne" Netze.

Firmware-Signierung

Kryptographische Signaturen stellen sicher, dass nur authentische und unveränderte Firmware installiert wird. Schutz vor Supply-Chain-Angriffen.

Secure Boot

Vertrauenskette vom ersten Boot-Vorgang an.
Hardwarebasierte Roots of Trust verhindern das Laden kompromittierter Software.

Software Bill of Materials

SBOM ermöglicht Transparenz über verwendete Komponenten und deren Schwachstellen.
Essentiell für Vulnerability Management.

Das Ziel: Reduzierung von Supply-Chain-Risiken und Gewährleistung der Datenintegrität durch umfassende kryptographische Massnahmen.

Detection & Response: Früherkennung ist entscheidend

Anomalie-Erkennung

ML-basierte Systeme identifizieren in Echtzeit ungewöhnliche Verhaltens-muster bei IoT-Geräten und im Netzwerkverkehr.

Schnelle Eindämmung

Automatisierte Isolation kompromittierter Systeme verhindert die Ausbreitung von Bedrohungen im Netzwerk.

Recovery Testing

Regelmässige Tests der Wieder-herstellungsprozesse stellen sicher, dass im Ernstfall schnell reagiert werden kann.

Technische Umsetzung

- Network Detection & Response (NDR) für IoT-Umgebungen
- Spezialisierte IoT-IDS mit HVAC-Protokoll-Verständnis
- Definierte Incident Response Playbooks
- Automatisierte Key-Rotation bei Kompromittierung
- Failsafe-Modi für kritische Heizungssysteme
- Kontinuierliche Backup-Verifikation

5-Minuten-Checkliste für Betreiber

1. **Segmentierung & Asset-Inventar**

   Erstellen Sie eine vollständige Übersicht aller vernetzten HVAC-Komponenten und isolieren Sie diese in dedizierten Netzwerksegmenten.

2. **MFA für Remote-Zugriff**

   Implementieren Sie Multi-Faktor-Authentifizierung für alle Fernwartungszugänge – keine Ausnahmen für Servicetechniker oder Hersteller.

3. **TLS-Verschlüsselung durchsetzen**

   Stellen Sie sicher, dass alle Kommunikationskanäle verschlüsselt sind. Deaktivieren Sie unverschlüsselte Legacy-Protokolle wo möglich.

4. **Patch-Prozess mit Rollback**

   Etablieren Sie einen strukturierten Update-Prozess mit Rollback-Möglichkeiten und testen Sie Updates zuerst in einer isolierten Umgebung.

5. **Getesteter Incident-Plan**

   Entwickeln Sie Notfallpläne für Cyberangriffe und testen Sie regelmässig die Failover-Modi Ihrer kritischen Heizsysteme.

Wie Kyos Sie unterstützt

Assessments & Architektur-Reviews

Umfassende Sicherheitsbewertungen für IoT-, OT- und Cloud-Umgebungen. Identifikation von Schwachstellen und Verbesserungspotenzialen.

Hardening-Guides & Vendor-Beratung

Entwicklung massgeschneiderter Sicherheitsleitfäden und Beratung von Herstellern bei der sicheren Produktentwicklung.

Zero-Trust Access & MFA

Implementation von Zero-Trust-Architekturen und Multi-Faktor-Authentifizierung für sichere Fernwartungszugänge.

Purple-Teaming & IR-Readiness

Kombinierte Red-/Blue-Team-Übungen zur Verbesserung der Cyberresilienz und Vorbereitung auf Incident Response.

Kyos kombiniert tiefes technisches Verständnis mit praktischer Erfahrung in der Absicherung kritischer Infrastrukturen und IoT-Systeme.

Panel: Energy, IoT, Security

"Energy, IoT, Security – Practice over Perfection"

Gäste & Experten

- Marc Bätschmann (FWS) – Praxiserfahrungen aus der Energiebranche
- Live-Diskussion mit GOhack-Teilnehmern

Diskussionsthemen

- Resilienz vs. Effizienz in der Energiewende
- Sichere Fernwartung bei kritischen Systemen
- Herausforderungen in Vendor-Ökosystemen
- Regulatorische Anforderungen und Standards

Security is not a product

"Sicherheit ist kein Produkt – es ist ein kontinuierlicher Prozess, der Design, Betrieb und Menschen verbindet."

Schlüsselerkenntnisse

- Cybersecurity muss von Anfang an mitgedacht werden
- Menschen und Prozesse sind genauso wichtig wie Technologie
- Kontinuierliche Verbesserung schlägt einmalige "perfekte" Lösungen
- Zusammenarbeit zwischen Herstellern, Betreibern und Security-Experten ist essentiell

Jetzt vernetzen!

Haben Sie Fragen zur Absicherung Ihrer IoT- und Energiesysteme?
Unser Expertenteam steht Ihnen zur Verfügung.

- Andy Kutter – Partner/Director
- andreas.kutter@kyos.ch
- LinkedIn: /in/andykutter
- www.kyos.ch

Nächste Schritte

- Vernetzen Sie sich mit anderen Security-Enthusiasten
- Implementieren Sie die 5-Minuten-Checkliste
- Bleiben Sie am Ball bei Cybersecurity-Trends

GOhack25 Special:
Kostenlose 30-minütige Security-Beratung für alle Teilnehmer!