Komponenten wie digitale Heizungsregler, Klimasteuerungen, Smart-Home-Zentralen oder vernetzte Wasserzähler können Cyberkriminellen als Einstiegstor in sensible Netzsegmente dienen. Bild: canva.com

TGA: smart, aber auch cybersicher?

Cybersicherheit für vernetzte Sanitär-, Heizungs- und Klimatechnik

Die digitale Vernetzung macht Systeme über ihre Schnittstellen angreifbar. Das gilt auch für die Technische Gebäudeausrüstung (TGA). Bei Cyberattacken sind TGA-Systeme im Sanitärbereich sowie der Heizungs- und Klimatechnik potenzielle Einfallstore in die Gebäudenetzwerke. Mit risikobasierten Prüfungen und einem ganzheitlichen strukturierten Sicherheitskonzept machen Betreiber ihre TGA resilient.

Was lange als rein mechanische oder elektrotechnische Ausrüstung galt, wird im Zuge der Digitalisierung immer mehr zum smarten Alleskönner, damit aber auch zu einer Schwachstelle im Gebäudenetzwerk. Anlagen der Sanitär-, Heizungs- und Klimatechnik (SHK) sind zunehmend digital vernetzt. Sie kommunizieren häufig über funkbasierte Protokolle oder offene Netzwerke wie BACnet, die oft ohne Verschlüsselung oder Zertifikatsprüfung betrieben werden.

Fehlt ein übergreifendes Sicherheitskonzept oder werden die Systeme in unsichere IT-Umgebungen eingebunden, entstehen potenzielle Angriffspunkte für Cyberkriminelle. Diesen können selbst harmlose Komponenten wie digitale Heizungsregler, Klimasteuerungen, Smart-Home-Zentralen oder vernetzte Wasserzähler als Einstiegstor dienen, um sich unautorisiert Zugang zu sensiblen Netzsegmenten zu verschaffen.

Dabei gefährdet eine weitere Entwicklung die Sicherheit der TGA: Im Darknet finden Cyberkriminelle heute auf spezialisierten Plattformen Tools, wie zum Beispiel modulare Schadsoftware, die auf digitale Infrastrukturen abzielt. Dabei werden bekannte Schwachstellen ausgenutzt, etwa veraltete Firmware-Versionen oder mangelhaft segmentierte Netzwerke, um Anlagen zu sabotieren oder unbemerkt zu manipulieren.

VERBORGENE RISIKEN

Angriffe auf SHK-Systeme (anders als bei Produktionsanlagen) bleiben häufig über längere Zeit unbemerkt. Statt sofort abzuschalten, verändern Angreifer schleichend die Systemparameter: Regelkurven werden verschoben, Grenzwerte angepasst oder sicherheitsrelevante (Not-)Funktionen gezielt deaktiviert. Solche Eingriffe zeigen ihre Wirkung oft erst unter extremen Bedingungen – etwa bei außergewöhnlichen Außentemperaturen oder im Störfall. Problematisch ist das

Mit der zunehmenden Vernetzung von TGA-Komponenten steigt auch das Risiko durch unbefugten Zugriff von außen, wie beispielsweise Hackerangriffe.
Bild: BODE Fach-PR, KI-generiert mit LLM

vor allem für kritische Infrastrukturen wie Rechenzentren oder Krankenhäuser, wo Klima- und Kälteanlagen essenzielle Aufgaben übernehmen.

Noch kritischer sind Angriffe auf SHK-Komponenten, die mit Systemen für Notfälle (sicherheitstechnische Gebäudeausrüstung) gekoppelt sind. Im Brandfall übernimmt das Gebäudeleitsystem dann auch sicherheitsrelevante Steuerungsfunktionen: Es schaltet beispielsweise Lüftungsanlagen ab, um die Rauchausbreitung zu verhindern, aktiviert die Schließung von Brandschutzklappen, öffnet gezielt Entrauchungsklappen und steuert die Druckbelüftung auf Flucht- und Rettungswegen. Wird ein solches System kompromittiert, etwa durch einen Cyberangriff, kann dies im Ernstfall gravierende Auswirkungen auf die Personensicherheit haben – bis hin zur Lebensgefahr.

SMARTE TECHNIK SICHER MACHEN

Smart-Home-Technologie automatisiert und steuert die Funktionen eines Gebäudes. Um sie wirksam vor Cyberangriffen zu schützen, dürfen dauerhaft keine werkseitigen Standardzugänge oder unsichere Zugangsdaten verwendet werden. Stattdessen sind starke, individuelle Passwörter zu verwenden und – wo technisch möglich – eine Zwei-Faktor-Authentifizierung (2FA) zu aktivieren. Im laufenden Betrieb gilt: Fernwartungszugriffe dürfen ausschließlich über verschlüsselte, abgesicherte VPN-Verbindungen erfolgen, ide,alerweise über dedizierte Wartungsgeräte oder virtualisierte Umgebungen mit klar definierten Rollen- und Rechtekonzepten. Alle Zugriffe und Änderungen sollten revisionssicher protokolliert und regelmäßig überprüft werden, um jederzeit nachvollziehen zu können, wer wann welche Aktion durchgeführt hat.

Sicherheits- und Firmware-Updates sind zeitnah nach Verfügbarkeit einzuspielen, idealerweise automatisiert oder im Rahmen eines klar definierten Patch-Management-Prozesses. Zuständigkeiten und Eskalationswege müssen dabei eindeutig geregelt sein. Erfolgt die Systemsteuerung über mobile Endgeräte wie Smartphones oder Tablets, sind auch diese umfassend abzusichern – z. B. durch starke Gerätesperren (PIN, biometrisch), Verschlüsselung, Mobile-Device-Management (MDM) und regelmäßige Sicherheitsupdates.

Kann für die Datenverarbeitung und -speicherung kein lokaler Server genutzt werden, sollten nur Cloud-Dienste von DSGVO-konformen Anbietern zum Einsatz kommen, deren Rechenzentren vorzugsweise innerhalb der EU betrieben werden. Ebenso wichtig ist es, bei der Wahl der Smart-Home-Systeme auf vertrauenswürdige Hersteller zu setzen. Sie sind daran zu erkennen, dass sie etablierte Marken vertreiben, Update-Support bieten und zertifiziert sind.

Weiter sollten Smart-Home-Komponenten möglichst vom Hauptnetzwerk getrennt sein: Das bedeutet, dass Steuergeräte für Heizung und Klima in separaten VLANs betrieben werden, getrennt von der klassischen Büro-IT. Diese Trennung reduziert nicht nur die Angriffsfläche, sondern erleichtert auch die Überwachung und Protokollierung. In vielen Fällen ist es sinnvoll, OT-Netze (Operational Technology) vollständig vom Internet zu entkoppeln oder nur gezielt über gehärtete Gateways (Knoten zwischen Netzwerken mit unterschiedlichen Protokollen) anzubinden. Insgesamt sollten unnötige Verbindungen über Bluetooth, WLAN oder ZigBee bei Nichtnutzung abgeschaltet werden. Darüber hinaus ist es sinnvoll, regelmäßig zu prüfen, welche Geräte verbunden sind, und ob Auffälligkeiten eingetreten sind.

SO UNTERSTÜTZEN SACHVERSTÄNDIGE

Für eine fundierte Einschätzung der Cybersicherheitsrisiken von SHK-Anlagen braucht es einen ganzheitlichen Blick auf Technik, Vernetzung und Betriebsumfeld. Dazu sollten qualifizierte Fachkräfte eingebunden werden, die sowohl mit der Anlagentechnik als auch mit den Anforderungen der Cybersicherheit vertraut sind. Prüforganisationen wie TÜV SÜD unterstützen in den folgenden Bereichen:

Sicherheitsanalyse als Basis

Bereits in der Planungsphase werden vulnerable Systembereiche und kritische Schnittstellen identifiziert, Schutzbedarfe definiert und Zuständigkeiten geklärt – etwa von IT-Abteilung, Facility Management oder externen Dienstleistern.

Gefährdungsbeurteilung

Die Risikobewertung erfordert technisches und sicherheitsrelevantes Know-how. Ungeeignete Maßnahmen können neue Schwachstellen erzeugen oder den Betrieb stören.

Risikobasierte Prüfmethoden

Die Sachverständigen klassifizieren Anlagenkomponenten anhand ihrer Kritikalität und legen passende Prüfinhalte und -zyklen fest. So lassen sich Prüfressourcen gezielt einsetzen, ohne Schwachstellen zu übersehen.

Dokumentation und Normen

Ein vollständiges Netzwerkinventar, Topologien und Funktionsbeschreibungen bilden die Grundlage jeder Schwachstellenanalyse. Als praxisnahe Orientierung dienen etablierte Standards wie ISO 27001 (Informationssicherheits-Management), IEC 62443 (Cybersecurity von industriellen Automatisierungssystemen) oder DIN EN 50710 (Anforderungen an Ferndienste für Brandsicherheitsanlagen und Sicherheitsanlagen).

Fachgerechte Sicherheitskonzepte, kontinuierliches Monitoring und risikoorientierte Prüfungen schützen die TGA vor unbefugtem Zugriff. Bild: BODE Fach-PR, KI-generiert mit LLM

IT-SICHERHEIT IM BETRIEB

SHK-Betriebe, die Fernwartung anbieten, müssen die eigene Infrastruktur härten. Dazu zählen Zwei-Faktor-Authentifizierung, segmentierte Netzwerke, dokumentierte Updates sowie Mitarbeiterschulungen. Besonders Techniker benötigen Sensibilisierung für Themen wie Phishing, Passwörter und mobile Sicherheit. Wichtig ist auch eine interne IT-Dokumentation, die klare Zuständigkeiten, Updatezyklen und Kommunikations- sowie Eskalationsprozesse definiert. Nur wenn alle Beteiligten – vom Monteur bis zur Geschäftsleitung – ihre Aufgaben gemäß Sicherheitskonzept kennen und umsetzen, lässt sich das Risiko langfristig und wirksam senken.

VERTRAUEN BEI KUNDEN SCHAFFEN

Endkunden erwarten zunehmend Transparenz bei der Sicherheit ihrer vernetzten SHK-Systeme. SHK-Betriebe sollten fachlich fundierte Antworten geben können – nicht nur zur Funktion, sondern auch zur Absicherung. Unternehmen schaffen Vertrauen, wenn sie ihre Sicherheitsarchitektur transparent darstellen, Daten, wo es möglich ist, lokal speichern, und verschlüsselte Verbindungen (vor allem für Cloud-Services und Fernzugriffe) nutzen.

Zudem entstehen durch die zunehmende Digitalisierung neue Anforderungen an die Vertragsgestaltung: Kunden möchten wissen, wo die Verantwortlichkeiten beginnen und enden, und welche Sicherheitsstandards den Maßnahmen zugrunde liegen. Hier können eine schriftlich dokumentierte Einweisung in das System und seine Sicherheitsfunktionen und eine klare vertragliche Regelung Transparenz schaffen. Nur wer Sicherheitsaspekte frühzeitig berücksichtigt, kann seinen Kunden nachhaltige, rechtssichere und vertrauenswürdige Lösungen bieten – ein klarer Wettbewerbsvorteil in einem zunehmend digitalisierten Markt.

Autor: Dr.-Ing. Stefan Siegfried Veit,
Abteilungsleiter Elektro- und
Gebäudetechnik, TÜV SÜD Industrie Service

tuvsud.com/zues-cybersec

Die wichtigsten Schritte auf dem Weg zu einem wirksamen Schutz der TGA vor Cyberangriffen. Bild: TÜV Süd