ASERCOM Cyber-Security Empfehlung für vernetzte Kälte-Klima Anwendungen

Vorwort

Viele Komponenten in der Kälte- und Klimatechnik wie Verdichter, Ventilatoren oder Regler können heute vernetzt werden. Das kann beispielweise über Bluetooth, WLAN oder LAN erfolgen. In dieser Handlungsempfehlung werden wichtige Schritte beschrieben, wie diese Komponenten sicher mit Smartphones, Computern oder dem Internet vernetzt werden können.
Der Aufbau dieser Handlungsempfehlung folgt dem Lebenszyklus einer Kälte-Klimainstallation: Zu Beginn werden Aspekte der Planungsphase und der Systemarchitektur beschrieben. Daran schließen sich die Installation des Systems im Feld und die Wartungsphase während der Lebensdauer der Komponenten an. Die Empfehlung endet schließlich mit den Außerbetriebnahmen.
In dieser Information werden praktische Empfehlungen gegeben, um Systeme im Feld sicherer zu machen. Diese Schritte können die Angreifbarkeit von Frequenzumrichtern oder Reglern im Feld deutlich reduzieren, sie sind aber keine Alternative zu einem umfassenden, prozessbasierenden Management-System. Insbesondere für größere Installationen und Organisationen sollte unbedingt geprüft werden, ob ein integrierter Management Prozess (information security integrated management system, ISIM), eingeführt werden sollte. Eine gute Hilfe bei dieser Bewertung können Einführungen in die Normen ISO 27001, UL 2900 oder IEC 62443 sein:

https://www.iso.org/isoiec-27001-information-security.html oder https://en.wikipedia.org/wiki/ISO/IEC_27001
https://en.wikipedia.org/wiki/Cyber_security_standards
Kobes, P.: Guideline Industrial Security ISO 62443 is easy; Berlin: VDE Verlag; 2017)

Es wird ausdrücklich empfohlen regelmäßig die lokal gültige Rechtslage zu prüfen. Die Gesetzgebung bezüglich Cyber-Security kann permanent Änderungen unterliegen.

Bild: pixabay

Grundsätzliche Anmerkungen

Cyber-Security Normen wie IEC 62443, VDI/VDE 2182 und andere definieren drei verschiedene Rollen bei einem mit dem Internet vernetzten technischen System:

a) Der Hersteller vernetzbarer Geräte wie zum Beispiel Regler, Frequenzumrichter oder Sensoren (auch als Verkäufer bezeichnet).
b) Der Integrator, der das System mit vernetzbaren Komponenten plant und im Feld installiert (auch als Anlagenbauer bezeichnet).
c) Der Eigentümer oder Betreiber, der technisch und organisatorisch für die Gesamtanlage verantwortlich ist.

Eine sehr wichtige Aufgabe für alle drei Rollen ist die permanente Kommunikation untereinander:
Informationen über die Spezifikation, die Anforderungen, die geplante Nutzung, eventuelle Änderungen, et cetera, müssen zwischen allen drei ausgetauscht werden.

Cyber-Security ist kein statisches Ziel, das ein für alle Mal erreicht werden kann. Es ist wichtig, diese Kommunikation dauerhaft aufrecht zu erhalten und Information, z.B. über verfügbare Updates, während des gesamten Lebenszyklus des Systems im Feld auszutauschen. Das bedeutet, dass es sinnvoll sein kann, einen PDCA-Zyklus (plan-do-check-act Zyklus) während der Lebensdauer zu etablieren.

In den folgenden Abschnitten werden wichtige Empfehlungen für Cyber-Security gegeben. Es ist aber wichtig zu wissen, dass für eine konkrete Anlage auch eine individuelle Risikoanalyse durchgeführt wird, um festzustellen, ob weitergehende und umfangreichere Maßnahmen zum Schutz des Systems notwendig sind. Die in diesem Leitfaden vorgestellten Maßnahmen betreffen hauptsächlich Technologie und Prozesse. Darüber hinaus ist es auch sehr wichtig, die Menschen, die mit der Anlage zu tun haben, zu integrieren. Alle drei oben genannten Gruppen (Hersteller, Integrator und Betreiber/Eigentümer) müssen ihre Mitarbeiterinnen und Mitarbeiter über Cyber-Security schulen und sensibilisieren.

Unter Umständen passen nicht alle hier beschriebenen Schritte zu allen Installationen und Anlagen im Feld. Es ist daher wichtig, brauchbare und angemessene Schritte aus diesem Leitfaden entsprechend den spezifischen Anforderungen auszuwählen.

Architektur / Planung

Eine gestaffelte Verteidigung schaffen (defense in depth design)

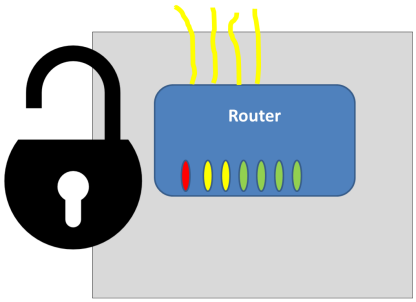
Risiko: Eine einzelne Security-Maßnahme zum Schutz von Kälte- und Klimaanlagen kann Schwächen haben und verletzbar sein.

Lösung: Es ist besser, die Security nicht nur durch eine einzelne Maßnahme, sondern durch mehrere, einander ergänzende Maßnahmen zu erreichen. Wenn ein Angreifer eine erste Schutzschicht durchbrochen hat, muss er trotzdem noch weitere Sicherheitsmaßnahmen überwinden.

IT-Komponenten wie Router sollten in einem verschlossenen Schaltschrank oder Raum gesichert werden

Risiko: Wenn unautorisierte Personen Zugang zu IT-Komponenten wie Routern, Firewall oder SPS haben, können sie Änderungen an den Einstellungen vornehmen und Zugang zur ganzen Installation bekommen. Das gilt insbesondere, wenn USB-Schnittstellen etc. zugänglich sind.

Lösung: IT-Infrastruktur wie Router oder Firewall sollten in einem verschlossenen Schrank oder einem abgeschlossenen Raum platziert werden. Es muss sichergestellt werden, dass nur autorisierte Personen die Türen aufschließen können und dass sie immer abgeschlossen sind, wenn keine autorisierten Personen im Raum sind.



Kälte-Klimaanwendungen sollten von anderen Bereichen des Netzwerks (Büro...) durch Segmentierung (beispielsweise durch eine Firewall), getrennt werden.

Risiko: Wenn die Komponenten von vernetzten Kälte-/Klimaanwendungen im gleichen Netzwerk-Segment wie Büroanwendungen oder Webservern arbeiten, dann können Cyber-Attacken auf einen Bereich schnell auch auf weitere Bereiche übergreifen.

Lösung: Die Installation sollte in logische Abschnitte (Segmente) aufgeteilt werden (siehe dazu auch https://en.wikipedia.org/wiki/Network_segmentation). Das kann zum Beispiel durch eine Firewall zwischen zwei Segmenten erreicht werden.

Installation / Inbetriebnahme

Wechsel der Werkseinstellungen für Passwörter und Login-Namen (Administrator und Nutzer)

Risiko: Komponenten wie Firewalls oder Router aber auch Frequenzumrichter, Regler oder EC-Lüfter mit einem Webinterface haben meistens eine Login-Seite. Meistens gibt es einen Zugang (Nutzername und Passwort) als Werkseinstellung, der auch im Handbuch beschrieben ist. Wenn diese Werkseinstellung nicht geändert wird, kann ein Angreifer einfach in die Komponente eindringen, sobald er die IP-Adresse gefunden hat.

Lösung: Die voreingestellten Zugangsdaten müssen während der Installation geändert werden.

“Installations-Zugänge” müssen nach der Inbetriebnahme wieder gelöscht werden.

Risiko: Während der Installation werden oft besondere Benutzerkonten für Administrator oder Nutzer mit sehr einfachen Passwörtern angelegt, weil das wiederholte Eintippen von langen und sicheren Passwörtern zu umständlich ist.

Lösung: Diese Benutzerkonten müssen nach der Inbetriebnahme wieder gelöscht werden oder mit einem sicheren Passwort geschützt werden.

Passwörter sollten mindestens 8 Zeichen Länge aufweisen und aus Buchstaben, Zahlen und Sonderzeichen bestehen

Bild: pixabay

Risiko: Mit automatisierten Passwort-Crackern wie Medusa (Teil von KALI Linux) ist es einfach, tausende von Passwörtern automatisch auszuprobieren. Solche Tools arbeiten meistens mit Passwortlisten, die bei Angriffen im Netz zusammengestellt wurden. Diese enthalten häufig benutzte Passwörter wie *123456* oder *password*.

Lösung: Es sollten unbedingt bessere Passwörter benutzt werden, die in keinem Wörterbuch vorkommen oder bei denen ein “l” durch eine “1” oder ein “s” durch eine “5” ersetzt wurde. Um das Risiko von automatisierten Angriffen zu begrenzen, sollte die Länge bei völlig zufälligen Passwörtern mindestens 8 Zeichen betragen. Nicht zufällige Passwörter sollten noch länger sein. Es wird dringend empfohlen, dasselbe Passwort nicht in mehreren Zugängen zu verwenden.

Das System sollte gestärkt werden, indem nicht benutzte Ports, IP-Adressen und Protokolle deaktiviert bzw. geschlossen werden

Risiko: Die IP-Adresse eines Computer kann mit der Adresse eines Hauses verglichen werden und ein Port (z.B. 443) oder ein Protokoll (z.B. https) entspricht dann einer Tür in dieses Haus. Verschiedene internetbasierte Anwendungen wie E-Mail, Dateitransfer oder Webseiten haben verschiedene Protokolle und Ports. Jeder offene oder zugängliche Port ist ein potentielles Einfallstor für einen Hacker.

Lösung: Weil vernetzte Kälte-Klimaanwendungen typischerweise nur mit einem Wartungsserver kommunizieren und nur begrenzte Dienste im Netz verwenden, können die offenen Ports und verfügbaren Protokolle signifikant reduziert werden.

Eine Klimaanlage muss keine Videos auf Youtube streamen oder mit Wikipedia.de kommunizieren.

Datenübertragung sollte verschlüsselt erfolgen (https an Stelle von http, Bluetooth Verschlüsselung, VPN,…)

Risiko: Wenn Daten drahtlos oder über ein Kabel ohne Verschlüsselung übertragen werden, besteht immer das Risiko, dass Dritte die Übertragung belauschen können und zum Beispiel Login-Daten für eine elektronische Komponente oder ein System erfahren.

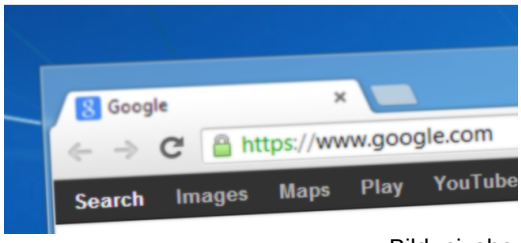


Bild: pixabay

Lösung: Verschlüsselung und Authentifizierung nach dem Stand der Technik sollten immer für die Datenübertragung und Kommunikation eingesetzt werden. Es ist wichtig, dass der beste verfügbare Standard von Zeit zu Zeit wechselt. Dadurch kann die Notwendigkeit entstehen, die Verschlüsselung anzupassen.

Wartung und Pflege während der Lebensdauer des Systems

Alle verfügbaren Updates für Firewall, Router, Smartphones/Tablets, PCs/Laptops…, die in der Installation eingesetzt werden, sollten unbedingt installiert werden.

Risiko: Regelmäßig werden Sicherheitslücken gefunden. Hersteller von Hard- und Software bringen dann Updates und Patches für ihre Produkte auf den Markt, wenn diese betroffen sind. Wenn ein veraltetes Gerät ohne aktuelle Updates in einer Kälte-Klimainstallation eingesetzt wird, dann ist die Installation angreifbar.

Lösung: Es ist wichtig, alle veröffentlichten Updates und Patches zu installieren. Viele Komponenten wie Firewalls oder Router haben die Option, den Nutzer bei neuen verfügbaren Updates über E-Mail oder SMS zu informieren. Das Update kann dann installiert werden. Neben den Geräten, die direkt im System eingebaut sind, ist es auch wichtig, dass alle „Werkzeuge“ wie Smartphones, Laptops oder PCs, die nur zeitweise mit der Anlage verbunden werden, auch mit Updates versorgt werden.

Bluetooth und WLAN deaktivieren, wenn sie aktuell nicht benutzt oder nicht benötigt werden.

Bild: pixabay

Risiko: Es gibt bestimmte Tools und Angriffswege (Exploit), um WLAN- oder Bluetooth-Verbindungen anzugreifen. Im Freifeld kann eine Bluetooth-Verbindung bis zu 50 m – 100 m Entfernung funktionieren. Anders als kabelgebundene Verbindungen können drahtlose Vernetzungen von außerhalb eines umzäunten Geländes oder verschlossenen Gebäudes aufgebaut werden.

Lösung: In den meisten Fällen muss eine drahtlose Verbindung nicht 24h / 7 Tage aktiviert sein. Häufig kann sie die meiste Zeit deaktiviert werden und nur eingeschaltet werden, wenn Daten übertragen werden sollen. Dadurch kann die Cyber-Security erheblich verbessert werden.

Die Nutzerkonten von Administratoren und Nutzer müssen während der Lebensdauer des Systems gepflegt werden.

Risiko: Mitarbeiter des Betreibers oder Integrators können das Unternehmen während der Betriebsdauer einer Anlage verlassen. Wenn die Nutzerkonten nicht gelöscht werden, dann können diese Mitarbeiterinnen und Mitarbeiter immer noch auf die Anlage zugreifen.

Lösung: Etablieren Sie eine Prozedur, die sicherstellt, dass die Nutzerkonten von ausscheidenden Mitarbeitern sicher gelöscht werden. Eine ähnliche Situation tritt auf, wenn der Betreiber von einem Integrator A zu einem anderen Integrator B wechselt. Wenn in einem System die Möglichkeit besteht, Passwortänderungen regelmäßig zu verlangen, dann sollte diese Option eingeschaltet werden.

Außerbetriebnahme

Alle Komponenten sollten auf die Werkseinstellungen zurückgesetzt werden. Passwörter und Daten sollten gelöscht werden, damit niemand nach der Außerbetriebnahme darauf Zugriff hat. Das ist insbesondere wichtig, wenn Passwörter in mehr als einer Installation verwendet worden sein könnten.

Risiko: Am Lebensende werden Komponenten oder Systeme außer Betrieb genommen. Wenn in den Komponenten dann noch Daten gespeichert sind, beispielsweise auf einer internen Festplatte in einem PC oder einer nichtflüchtigen Speicherkarte in einem Regler, dann können Dritte auf diese Daten Zugriff bekommen.

Lösung: Alle Daten müssen gelöscht und alle Einstellungen auf die Werkseinstellungen zurückgesetzt werden. Besondere Aufmerksamkeit sollte auf Speicherkarten (SD Karten) in einem Kartenleser, USB-Sticks, Cloud-Speicher im Internet und Daten auf Smartphones oder Laptops gelegt werden.

Revision Index

Revision	Change	Date
A	Initial issue	22.03.2018
B	Final approval	18.07.2018
C	German translation	14.08.2018
D	Print version	22.09.2018

Weitere *ASERCOM* Statements und Empfehlungen

- **Kohlenwasserstoff-Kältemittel in Kälteanlagen**
- **Kohlendioxid (CO_2) in Kälte- und Klimaanlagen**
- **Kältemittel mit Temperaturgleit und Auswirkungen auf die Leistungsangaben**
- **Empfehlungen zum Betrieb von Frequenzumrichtern mit Kältemittelverdichtern, die nach dem Verdrängerprinzip arbeiten**
- **Leitlinie für die Auslegung von Verbundsätzen mit frequenzgeregelten Verdichtern**
- **Dimensionierung von thermostatischen Expansionsventilen**
- **R22 Ausstieg**
- **Beurteilung der Energieeffizienz**
- **Empfohlene Filtertrockner für flüssige Kältemittel und Feuchtigkeitsindikatoren für Kälte- und Klimaanlagen mit Fluorkohlenwasserstoffen (HFKWs) als Kältemittel und Polyolester- Kältemaschinenölen**
- **Maschinen-Richtlinie 2006/42/EG**
- **Druckgeräte-Richtlinie (DGR) 2014/68/EU**
- **Richtlinie zur elektromagnetischen Verträglichkeit 2014/30/EC**
- **Dichtheit von Kältemittelverdichtern**

Weitere Informationen finden Sie in *ASERCOM*s technischen Mitteilungen auf www.asercom.org

Über *ASERCOM*

ASERCOM, der Verband der europäischen Hersteller von Komponenten für die Kälte- und Klimatechnik, beschäftigt sich mit wissenschaftlichen und technischen Herausforderungen, so wie mit der Förderung von Leistungs- und Sicherheitsstandards. Weiterhin konzentriert sich der Verband darauf den Umweltschutz zu verbessern. Mit dieser Aufgabe unterstützt *ASERCOM* die gesamte Kälte-Klimabranche und deren Endkunden.

Weitere Informationen erhalten Sie unter: www.*asercom*.org