Clipping aus: Die Kälte 9/2011
Erscheinungsdatum: September 2011
Referenz Pressemeldung: Sicherheit bei der Datenfernübertragung von Kälteanlagen

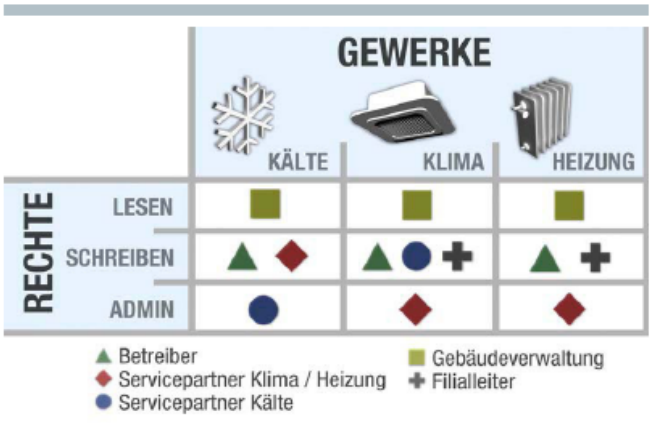
SICHERHEIT BEI DER DATENFERNÜBERWACHUNG VON KÄLTEANLAGEN

Absolut verlässlicher Betrieb gewünscht

In den letzten Monaten häufen sich Meldungen über Datenmissbrauch und gehackte Netzwerke. Da es sich meist um Angriffe auf Datenbanken handelt, kommt es nicht zu einem direkten Schaden. Gelingt es Eindringlingen allerdings in Steuerungsprozesse einzugreifen, kann das verheerende Folgen haben. Dies gilt auch für die Datenfernüberwachung kältetechnischer Anlagen in Lebensmittelmärkten, bei der täglich große Datenmengen auf externe Server übertragen werden. Bei nicht ausreichenden Sicherheitsvorkehrungen können die sensiblen Temperatur- und Energiedaten an unbefugte Dritte gelangen, im schlimmsten Fall kann sogar auf das Regelungssystem Einfluss genommen werden. Der potenzielle Warenverlust bei Filialbetrieben liegt dann schnell im Millionenbereich.

Gianluca di Lieto und Karsten Vossberg, Remscheid

Die heutige Datenfernüberwachung von kälte- und klimatechnischen Anlagen bringt besonders großen Lebensmittelmärkten und Handelsketten mit großen Filialnetzen viele Vorteile: Die Daten aller angeschlossenen Anlagen für Kühlung, Heizung, Lüftung oder Beleuchtung können von zentraler Stelle aus analysiert und ausgewertet werden. Gleichzeitig ist eine Überwachung und Steuerung der Anlagen von außerhalb des Marktes möglich. Ist ein System zur Datenfernüberwachung allerdings nur mit Basismaßnahmen wie einer vom Benutzer selbst gewählten Username-Passwort-Kombination gegen Angriffe von außen gesichert, kann das verheerende Auswirkungen haben. Wenn Unbefugte zum Beispiel über die Systeme der Datenfernüberwachung die Parameter an den Kälteanlagen verstellen oder diese komplett außer Betrieb setzen und dadurch die gesamte gekühlte Ware verdirbt, hat das einen enormen finanziellen Schaden zur Folge. Da die Medien in der Vergangenheit großes Interesse an gehackten Sicherheitssystemen namhafter Handelsketten gezeigt haben, muss der Betreiber im Ernstfall zusätzlich einen erheblichen Imageverlust befürchten.



Das Multigate erlaubt durch eine Unterteilung in drei Gewerke mit je drei Zugangsleveln eine vielstufige Vergabe von Zugriffsrechten.

Gianluca di Lieto,
Leiter
Vertrieb und Marketing

Karsten Vossberg,
Leiter
IT-Softwareentwicklung,
Wurm GmbH & Co. KG
Elektronische Systeme,
Remscheid

Sensible Komponenten der Datenfernüberwachung

Handelsunternehmen, die mit einer Datenfernüberwachung arbeiten, müssen sich intensiv mit der Sicherheit von Daten und der eingesetzten Technik auseinandersetzen und ihre Systeme auf den neuesten Sicherheitsstandard bringen. Von den Komponenten, die für eine Fernüberwachung der Anlagen notwendig sind, müssen besonders das Gateway und die Software zur Auswertung und Steuerung der Anlagen vor unbefugten Zugriffen geschützt sein. Das Gateway dient als Schnittstelle zwischen den Regelgeräten der automatisierten Anlage und der Außenwelt: Via Telefonleitung, Internet oder Mobilfunk gibt es die gesammelten Daten

geordnet und in einem einheitlichen Protokollformat an einen Server weiter. Auf diesen können Betreiber sowie deren Service-Partner zugreifen. Ebenso werden Störungen im Ereignisfall sofort an die Serviceorganisation gesendet. Über Software-Lösungen wie FrigodataXP von Wurm ist es außerdem möglich, die Anlagen aus der Ferne zu parametrieren und Störungen direkt zu beheben.

Überblick über verschiedene Sicherheitsmechanismen

Grundsätzlich gilt: Je mehr Zugriffsmöglichkeiten es aus anderen Systemen gibt, desto verletzbarer ist das zu schützende System. Folglich muss jede Schnittstelle gesondert gesichert werden und die kommunizierenden Systeme müssen auf einem gleich hohen Sicherheitsstandard sein. Denn das schwächste Glied in der Kette bestimmt die Gesamtsicherheit. Es gibt verschiedene effektive Lösungen, um das Gateway und die Software vor Angriffen zu schützen und die Datenfernüberwachung zu einem sicheren System zu machen:

Für PC-Anwendungen allgemein:

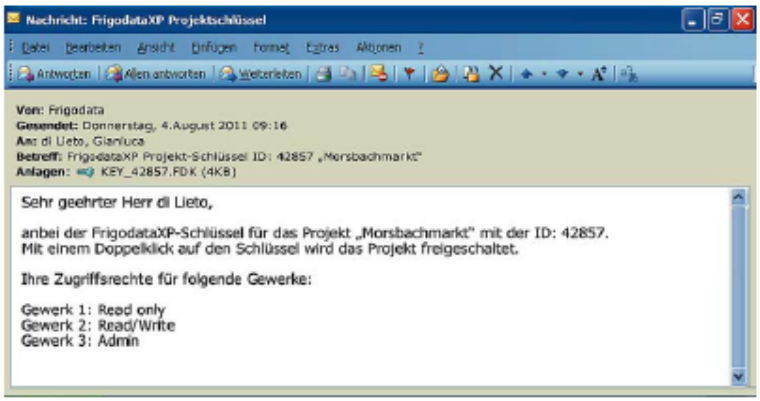
- Mehrstufige Passwortsysteme und Zugriffsrechte
- Vergabe sicherer Passwörter durch den Hersteller der Systeme
- Übermittlung und Ablage verschlüsselter Passwörter
- Sicherungen des Service-Computers mithilfe eines Dongles und einer Lizenz
- Dokumentation aller anlagenrelevanten Änderungen bei Fernzugriff
- Reduzierte Anzahl von Zugriffsmöglichkeiten

Zusätzlich für Browser- und Serveranwendungen:

- Anmeldung des Benutzers über eine zusätzliche Authentifizierung
- Verschlüsselte Datenübertragung via https
- Geschützte Verbindungen über VPN sowie eine leistungsfähige Firewall
- Absicherung der Serverräume

Mehrstufige Passwort-Konzepte und Zugriffsrechte

Das Sicherheitsdesign des Multigates von Wurm sieht beispielsweise ein mehrstufiges Passwort-Konzept vor. Da das Mul-



Die Benutzer erhalten die Passwörter von Wurm per E-Mail in einem verschlüsselten Projektkey.

tigate als Schnittstelle wichtige Funktionen übernimmt, ist ein hoher Sicherheitsstandard und eine exakte Verteilung der Zugriffsrechte notwendig: Zum einen leitet das Multigate Daten von Anlagen an einen eigenen Web-Server, an Frigodata oder aber sogar an eine externe Managementsoftware weiter. Zum anderen werden Sollwertänderungen von Frigodata an die entsprechenden Regelgeräte verteilt. Deshalb ist das Gateway individuell in drei unterschiedliche Gewerke unterteilbar, zum Beispiel Kältetechnik, Haustechnik und steckerfertige Geräte. Jedes Gewerk hat wiederum drei verschiedene Zugangslevel mit einem entsprechenden Passwort. So kann gewerkeübergreifend in freier Kombination die Zugangsebene den Nutzeranforderungen angepasst werden.

Zusätzlich bietet die PC-Software FrigodataXP ein mehrstufiges Rechtesystem – das heißt, es gibt mehrere Benutzergruppen, die jeweils ein separates Passwort haben und mit diesem nur auf bestimmte Daten und Funktionen Zugriff erhalten. Somit kann der administrierende Nutzer individuell festlegen, welcher Mitarbeiter welche Rechte hat. Das verhindert unter anderem auch versehentliche Sollwertänderungen, durch die Anlagen verstellt werden können.

Sichere Vergabe von Passwörtern

Die Passwörter für alle Systeme werden direkt von Wurm vergeben. Diese können vom Kunden nicht verändert werden. Wechselt ein Marktbetreiber seine Servicefirma, wird deren Passwort von Wurm bei schriftlicher Aufforderung der Handelskette deaktiviert, damit die Vorgängerfirma keinen Zugriff mehr auf die Daten und Anlagen hat.

Da eine Vergabe der Passwörter nur über Telefon oder E-Mail ein zu großes Sicherheitsrisiko darstellt, hat Wurm eine neue Methode entwickelt: Der Benutzer erhält per E-Mail einen verschlüsselten Projektkey. Der Empfänger kann diesen nur entschlüsseln, wenn eine lizenzierte Softwareversion

WURM IN KÜRZE

Als Pionier im Bereich der Datenfernübertragung hat das Unternehmen Wurm bereits Ende der 1980er-Jahre die ersten Gewerbekälteanlagen mit Fernwartung ausgestattet. Damals war es das Ziel, mit einfachen DOS-Programmen wie zum Beispiel Frigodata 4 die Inbetriebnahme und Anlagenanpassung zu erleichtern. Im Laufe der Zeit änderten sich die Ansprüche und machten leistungsstärkere und umfangreichere Programme notwendig. Mit der aktuellen Software FrigodataXP stehen dem Nutzer Anwendungen zur Verfügung, die unterschiedlichste Anforderungen erfüllen, beispielsweise Anlageninbetriebnahme und -service, Parametrierung, Visualisierung, Dokumentation und Alarmmanagement.

von FrigodataXP auf seinem Computer installiert ist. Der Projektkey enthält nicht nur die Passwörter, sondern auch die Projekteigenschaften. Ein einfacher Klick auf den Schlüssel in der E-Mail installiert automatisch das Projekt in FrigodataXP. Ein Klartext-Passwort muss nicht eingetragen werden – somit ist ein Missbrauch des übermittelten Projektkeys unmöglich.

Verifizierung mit Dongle und Seriennummer

Zusätzlich zu einem Benutzername-Passwort-System arbeitet Wurm auch mit sogenannten Dongles – die gleichzeitig als Kopierschutzstecker und Lizenz dienen. Bei Einzelplatzanwendungen ist hierzu ein zertifizierter USB-Stick zur Verifizierung notwendig. Bei Mehrfachanwendungen kann ein im Netzwerk installierter Lizenzmanager diese Aufgabe übernehmen. Der Dongle enthält eine Seriennummer, die den Zugriff auf die installierte Software verifiziert und zur Dokumentation bei Verstellungen der Anlage in die Geräte geschrieben wird.

Zur Dokumentation von Verstellungen ermöglichen Systeme wie das Multigate eine genaue Nachverfolgung, von welchem Computer oder Benutzerkonto aus Sollwertänderungen vorgenommen wurden. Die Änderung wird zusammen mit einer eindeutigen Benutzer-ID wie zum Beispiel der Dongle-Seriennummer sowie Datum und Uhrzeit gespeichert. Sollten die kältetechnischen Anlagen mutwillig beschädigt werden, kann Wurm anhand der Benutzer-ID feststellen, von wo aus auf die Anlage zugegriffen wurde.

Sicherheit bei Browser- und Serveranwendungen

Neben gesicherten Soft- und Hardwarelösungen für die Datenfernüberwachung muss die Übertragung der Daten selbst über sichere Verbindungskanäle erfolgen. Wurm stellt zum Beispiel zu allen Online-Anwendungen den „abhörsicheren" https-Modus zur Verfügung, der auch beim Online-Banking eingesetzt wird. Die Datenübertragung zu Anlagen filialisierender Unternehmen geschieht üblicherweise über einen VPN-Tunnel (Virtual Private Network).

Ein eigens von Wurm für den Onlinezugriff entwickeltes Zugangsverfahren ist die telefonische Authentifizierung in Kombination mit dem passenden Benutzernamen. Mit dieser Technik ist die auf einer Internet-Browsertechologie basierende Wurm-Software FrigodataOnline gesichert. Diese bietet dem Nutzer sowohl die Möglichkei-

Die Sicherheit der Serverfarm und Softwareentwicklung von Wurm wurde 2010 vom TÜV Rheinland zertifiziert.

ten der Einzelbetrachtung eines Projektes oder gar Regelgerätes als auch die filialübergreifende Auswertung von Anlagendaten. Da die Internettechnologie konzeptionelle Schwächen aufweist, sind hierbei besonders anspruchsvolle Sicherheitskonzepte notwendig: Die telefonische Authentifizierung beruht auf dem Mobiltelefon des Benutzers, das er in der Regel immer griffbereit hat. Für die Anmeldung gibt der registrierte Nutzer seinen Benutzernamen in den Browser ein und wählt dann mit seinem Mobiltelefon, dessen Nummer bei FrigodataOnline hinterlegt ist, die kostenfreie Wurm-Rufnummer. Die Mobilnummer wird dort automatisch mit dem Benutzernamen verglichen und erst wenn beides übereinstimmt, erhält der Nutzer Zugriff auf das Programm. Diese Methode bietet mehr Sicherheit als eine ausschließliche Benutzername-Passwort-Kombination.

Ein Nutzer mit entsprechenden Rechten hat auch mit FrigodataOnline die Möglichkeit, Anlageneinstellungen zu verändern. Hierzu muss er sich allerdings ähnlich wie bei dem von Banken genutzten mobileTAN-Verfahren authentifizieren. Die Dokumentation dieser Änderungen ermöglicht hierbei eine spätere Nachverfolgung.

Serverraum mit Fingerscanner gesichert

Viele Handelsketten nutzen die Managementtools von Wurm in FrigodataOnline, insgesamt sind dies derzeit 65 Mrd. Datensätze. Alle Daten werden über Server verwaltet, die in dem Remscheider Unternehmen stehen. Das große Volumen sensibler Daten verlangt leistungsfähige Sicherheitsvorkehrungen vor Ort. Bei Wurm sind beispielsweise die drei redundanten, videoüberwachten Serverräume nur für wenige Befugte zugänglich, die über einen Fingerabdruckscanner identifiziert werden müssen. Jeder Serverraum wird durch mehrere Klimaanlagen und Brandschutzvorkehrungen gesichert – fällt ein Gerät aus, übernehmen die anderen dessen Aufgabe. Durch tägliche Daten-Backups ist im Notfall eine lückenlose Wiederherstellung aller Daten möglich.

Um den Kunden die maximale Sicherheit zu bieten, hat Wurm 2010 seine gesamte Serverfarm und die Softwareentwicklung vom TÜV Rheinland prüfen lassen. Dieser hat untersucht, ob die Daten vertraulich behandelt werden, die Kundendaten gemäß des Bundesdatenschutzgesetzes geschützt sind und alle technischen Systeme gegen Angriffe von außen und innen gesichert sind. Wurm hat hierbei die Zertifizierung für ausgezeichnete Sicherheitsstandards erhalten.

Fazit

Mit einer Datenfernüberwachung erhalten Betreiber einen schnellen Überblick über alle Märkte, und deren Service-Firmen können die Anlagen zeit- und kosteneffizient überwachen, steuern und optimieren. Deshalb sollten Unternehmen, die Datenfernüberwachung einsetzen, das Gespräch mit den Herstellern suchen und sich mit deren Sicherheitsmaßnahmen gründlich auseinandersetzen. Eine Öffnung von Regelungssystemen und Protokollen kann die herstellereigenen homogenen Sicherheitskonzepte eines Systems gravierend schwächen oder gar zum Versagen der gesamten Sicherheitskette führen. Eine regelmäßige Überprüfung der Sicherheitsstandards ist daher zwingend notwendig, denn die Betreiber erwarten vom Hersteller der Regelungstechnik einen absolut verlässlichen Betrieb ihrer Anlagen, so wie sie auch von ihrer Bank maximal geschützte Konten erwarten. Nur so ist Datenfernüberwachung auch in Zukunft effizient und sicher möglich. ■