WACHENDORFF
Prozesstechnik GmbH & Co. KG

Whitepaper
ISO 27001 Zertifizierung
Ein Muss für Branchen, die mit IoT zu tun haben

Ewon®
BY HMS NETWORKS

ISO 27001
CERTIFIED
VINÇOTTE

IndustrieROBUST

Zusammenfassung

Sicherheitslücken sind heutzutage weit verbreitet – insbesondere in Branchen mit kritischen Infrastrukturen und Maschinen, wie z. B. öffentliche Versorgungseinrichtungen, Notfallsysteme, Steuerungen für Gebäudeumgebungen und Industrieanlagen. Daten oder Informationsbestände sind anfällig für ständige Angriffe von außen sowie Diebstahl und interne Verstöße auf Anbieterseite. Heutzutage ist das Realität.

Den richtigen Anbieter für die Bereitstellung von Cloud-Diensten und -Geräten im Umfeld der Stadtwerke und bei kritischen Geräten auszuwählen ist wichtig. Die wichtigsten Parameter dafür sind Sicherheitskontrollen und -maßnahmen. Jede Nachlässigkeit kann bei Beteiligung von Notfallsystemen und öffentlichen Einrichtungen zu finanziellen Verlusten, dem Verlust sensibler und kritischer Informationen, dem Verlust des guten Rufs und sogar zu einer möglichen Lebensgefahr führen. ISO/IEC 27001 ist ein Standard für Informationssicherheit, der gewährleistet, dass das Unternehmen wichtige Schritte zur Sicherung seiner Vermögenswerte unternommen hat, zu denen Kundendaten, Mitarbeiterdaten, Finanzinformationen oder geistiges Eigentum gehören können.

ISO27001: Qualitätsstandard für die Datensicherheit

VPN (Virtual Private Network) und Tunneling sind Techniken, die es unter anderem ermöglichen, Datenverbindungen zwischen Ihnen und einem anderen Computer zu verschlüsseln. Dieser Computer kann zu Ihrer Organisation, einer vertrauenswürdigen Person, einer anderen Organisation oder einem kommerziellen VPN-Dienst gehören.
Das Tunneling verkapselt einen bestimmten Datenstrom durch ein verschlüsseltes Protokoll, wodurch alles, was den Tunnel „passiert“, für jeden auf dem Übertragungsweg unlesbar wird. Die Nutzung von VPN oder eine andere Form des Tunnelings für die Verschlüsselung von Daten ist einer der besten Wege, um sicherzustellen, dass die Daten nur von Ihnen und den Menschen gesehen werden, denen Sie vertrauen.
Ein weiterer großer Vorteil dieser Technik ist die Authentifizierung von Remote-Parteien.

Aufgabenstellung

Sicherheitslücken reichen von gestohlenen Passwörtern bis hin zu komplizierten gezielten Angriffen, auf die man sich unmöglich hätte vorbereiten können. Das kein Unternehmen vor Daten- und Sicherheitsverstößen geschützt sei, ist eine eindeutige Aussage, denn selbst Regierungsabteilungen wie das Internal Revenue System in den USA sind schon Opfer solcher Angriffe geworden: 2016 wurden Informationen von mehr als 700.000 Personen preisgegeben. Ausländische Regierungen oder Organisationen, die böswillige Absichten haben, können von solchen Informationen profitieren, die für kriminellen Betrug verwendet werden können. Social-Media-Plattformen wie LinkedIn und Facebook sowie Einzelhändler wie Whole Foods wurden Opfer von Datenschutzverletzungen und Angriffen.
Was passiert nach einem Verstoß mit den Daten? Sie können für verschiedene illegale Zwecke missbraucht werden. Sie können an Underground-Cyberforen gelangen, in denen Einzelpersonen und Gruppen große Gewinne aus dem Weiterverkauf von Kontaktinformationen wie Namen, Adressen, Titeln, E-Mail-Adressen, Geburtsdaten und Kreditkarteninformationen machen wollen. Einer der größten Cyberangriffe im Jahr 2014 war ein Datenverstoß bei JP Morgan Chase, bei dem Informationen von über 76 Millionen Haushalten in Gefahr waren. Verizon Enterprise Solutions, einer der weltweit führenden Anbieter von Cloud-Sicherheitslösungen, ist Opfer eines Datenverstoßes mit mehr als einer Million betroffenen Unternehmenskunden geworden. Dies hätte weitreichende Folgen für Telekommunikations- und Cloud-Sicherheitslösungen haben können.
Sicherheit geht vor. Und wenn es um Ihre Sicherheit und die Ihrer Kundendaten geht: Auf wen würden Sie sich verlassen? Heutzutage sind Hacker- und unverhohlene Angriffe nämlich weit verbreitet.

High-Level-Lösung

Die Lösung ist, dass Unternehmen beim Schutz ihrer Infrastruktur und Daten proaktiver sein müssen. Das können Sie nur mit Maßnahmen wie dem Einsatz von Sicherheitstools und Praktiken zum Schutz von Daten sowie kontinuierlichen Anstrengungen zum Risikomanagement erreichen.
Eine internationale Zertifizierung wie die nach ISO27001 gewährleistet die Verpflichtung zu Qualität und Sicherheit. Der Dienstleister ist verantwortlich für die Minimierung und Verwaltung von Sicherheitsrisiken. Eine Sicherheitszertifizierung setzt einen Zuverlässigkeitsstempel unter die erforderlichen Sicherheitsmaßnahmen eines Unternehmens.

Was haben die Unternehmen davon?

- Kundenfreundliche Sicherheitsstandards werden eingehalten.
- Wenn Unternehmen ihre eigenen Informationssicherheitsrisiken in ihrer eigenen Umgebung bewerten, neben denen, die Cloud Services und Infrastruktur bereitstellen, investieren sie mehr in das Wachstum ihres Unternehmens und das ihrer Kunden.
- Die Zertifizierung gewährleistet eine vollständige Bewertung und Validierung von End-to-End-Sicherheitssystemen.
- Die Reaktionsfähigkeit bei Sicherheitsvorfällen steigt mit zunehmendem Bewusstsein und robusten Sicherheitsmaßnahmen.
- Die Einhaltung anerkannter Best Practices für Informationssicherheit beruhigt Kunden und Unternehmen.
- Die Einhaltung von Normen ermöglicht auch das Zusammenwirken von Systemen.
- Sie garantiert eine effiziente Verwaltung und Schutz vor potenziellen Bedrohungen.
- Hilft bei der Erreichung von Business Continuity und Zielen der betrieblichen Exzellenz.

Was haben die Kunden davon?

- Sie stellt die Verantwortlichkeit auf Seiten des Dienstleisters sicher.
- Hilft Kunden, eine fundierte Entscheidung bei der Anbieterauswahl zu treffen, der hinsichtlich der Sicherheit die höchstmöglichen Industriestandards erfüllt.
- Garantiert durch Berücksichtigung der Sicherheits- und Qualitätsaspekte den Standard und die Qualität der unternehmenseigenen Produkte.
- Sorgt für Glaubwürdigkeit bei den Kunden, da die Erwartungen an die Dienstleistung und die spezifischen Anforderungen erfüllt werden.

Was ist die ISO 27001-Zertifizierung?

ISO/IEC 27001 wurde von der International Organization for Standardization (ISO) entwickelt und ist ein Informationssicherheitsstandard, der Teil der Normenfamilie ISO/IEC 27000 ist, jedoch speziell für das Informationssicherheitsmanagementsystem (ISMS) entwickelt wurde. ISMS ist ein systematischer Ansatz zur Verwaltung sensibler Unternehmensinformationen. Es umfasst Personen, Prozesse und IT-Systeme unter Anwendung eines Risikomanagementprozesses.

Der Sicherheitsstandard bezieht sich auf die Speicherung, Überwachung und Pflege von Daten. Unternehmen sind nicht zur Zertifizierung verpflichtet, da es für sie ausreicht, nur die empfohlenen Best Practices für die Sicherheit zu befolgen. Ein Unternehmen gilt jedoch als sicher, wenn es das Zertifikat erhält und die Standards kontinuierlich und mit systematischem Ansatz befolgt. Die Zertifizierung ist seitens einer akkreditierten Zertifizierungsstelle erhältlich, was Glaubwürdigkeit und Vertrauen schafft.

Wie erfolgt die Zertifizierung?

Nach einem ersten Meeting mit der akkreditierten Stelle wird der ISMS-Umfang definiert. Dann müssen weitere Schritte unternommen werden, die folgendes umfassen: Sensibilisierungstraining, GAP-Bewertung, Identifizierung und Bestimmung von Vermögenswerten im Rahmen des Umfangs, Durchführung der Risikobewertung, Erstellung der Anwendbarkeitserklärung, Entwicklung des Risikomaßnahmenplans, Implementierung der ausgewählten Kontrollen, Bestimmung eines Verbesserungsplans in Bereichen mit unzureichender Kontrolle, Bereitstellung der operativen ISMS-Schulung, Durchführung der internen Bewertung, gefolgt von einem Beurteilungsbesuch und der eigentlichen formalen Zertifizierungsprüfung. Die Neubewertung gemäß ISMS erfolgt alle 12 Monate.

Was deckt die Bewertung ab?

Die interne Checkliste umfasst alles folgende: Informationssicherheitsrichtlinien, Organisation der Informationssicherheit mit definierten Rollen und Verantwortlichkeiten, HR (vor, während und nach dem Arbeitsverhältnis), Richtlinien für mobile Geräte und Telearbeit, Vermögensverwaltung und -kontrolle, Informationsklassifizierung, Umgang mit Wechselmedien, Entsorgung und Übertragung, Kryptografie, physische und ökologische Sicherheit, Betrieb, Kommunikation (Netzwerksicherheitsmanagement und Informationsübertragung), Systembeschaffung, Entwicklung und Wartung, Informationssicherheit in Beziehungen mit Anbietern, Störfall-Management im Bereich Informationssicherheit sowie Einhaltung gesetzlicher und vertraglicher Anforderungen.

Das Business Continuity Management ist ein wichtiger Aspekt der Informationssicherheit. Damit wird bestimmt, ob das Unternehmen Prozesse geplant, dokumentiert, implementiert und gewartet hat, die die Dienstleistungskontinuität sicherstellen, wenn eine ungünstige Situation eintritt. Dies muss ebenfalls in regelmäßigen Abständen validiert und verifiziert werden.

Lösungsdetails

Welche Maßnahmen werden ergriffen, um die Einhaltung branchenspezifischer Sicherheitsstandards zu gewährleisten? Wie wählt man den richtigen Produktanbieter aus?
Bei der Arbeit mit Remote-Verbindungen zu industriellen Steuersystemen sind Netzwerksicherheit, Integrität und Zuverlässigkeit der Cloud-Infrastruktur und der Kundennetzwerke von größter Bedeutung. Branchenweit beste Fernzugriffslösungen zu schaffen, bedeutet auch, einen verwalteten, hybriden, mehrschichtigen Cybersicherheitsansatz zum Schutz der Geräte, des Netzwerks und vor allem der industriellen Systeme der Kunden zu entwickeln.
Mit starken Sicherheitsprozessen und Sicherheitskontrollen kann das Unternehmen die Bereiche identifizieren, die über starke Sicherheitskontrollen verfügen, sowie Bereiche, in denen Verbesserungen erforderlich sind.

All diese Maßnahmen gewährleisten, dass das System in der Lage ist, mit Änderungen Schritt zu halten, Schwachstellen zu identifizieren, Sicherheitsbedrohungen vorherzusagen und die Auswirkungen auf das Unternehmen im Falle eines Sicherheitsverstoßes zu begrenzen.

Geschäftsvorteile

Das Geschäfts- und Marktwachstum hängen davon ab, ob Unternehmen die Vorschriften und Compliance-Standards einhalten oder nicht. Im Managementsystem ISO27001 sind Sicherheitspraktiken integriert, die kontinuierlich verbessert werden müssen, so dass die Sicherheit überall gewährleistet ist. Die Zertifizierung beinhaltet auch interne Schulungsmaßnahmen, so dass die Mitarbeiter des Unternehmens und der Anbieter geschult und befugt sind, die Informationen zu schützen.

Durch die hohen Risiken einer Datenschwachstelle müssen der Schutz, die Speicherung und Verwaltung von Daten auf bewährten Praktiken und systematischen Ansätzen basieren. Durch eine verbesserte interne Kontrolle der Unternehmensvermögenswerte kann Kunden versichert werden, dass es einen streng verwalteten und dokumentierten Ansatz für den täglichen Betrieb gibt. Manchmal ist die ISO die Mindestanforderung, um geschäftlich tätig zu sein. Somit gibt es einen großen Wettbewerbsvorteil, da der Schutz der eigenen Unternehmensreputation und der des Kunden einen Vorsprung bietet.

Wie treffen Sie Ihre Wahl?

Auf welchen Anbieter würden Sie sich für Produkte in der Cloud verlassen, auf die „remote“ zugegriffen wird, die überwacht werden und einen direkten Einfluss auf die Marke und den Ruf Ihres Unternehmens haben? Auf den mit einer international anerkannten Zertifizierung.

Die Zertifizierung selbst bekommt man nicht so einfach. Durch die Prüfung und Bewertung durch eine akkreditierte, international führende Zertifizierungsstelle, lange Überprüfungen und eingehende Compliance-Audits sowie Follow-up-Audits ist das Produkt nicht nur zuverlässig, sondern schafft auch Vertrauen bei den Kunden, da sie sehen, dass ihr Anbieter in Informationssicherheitsmaßnahmen investiert hat.

Zusammenfassung

HMS Industrial Networks hat die ISO 27001-Zertifizierung für seine preisgekrönte Cloud-Konnektivitätsplattform Ewon Talk2M erhalten, die sicherstellt, dass Sicherheitsmaßnahmen für Infrastruktur, Rechenzentren und Dienste ergriffen wurden. Mit der Zertifizierung reiht sich HMS in die Reihe der Unternehmen ein, die den höchsten internationalen Standards folgen und in Übereinstimmung mit branchenführenden Best Practices wie Cisco Services Organization (für ihre Netzwerk-, Rechenzentrums-, Kommunikations- und Kollaborationsprodukte und -lösungen) oder Amazon Web Services (AWS) arbeiten.

Die Zertifizierung ist für die Kunden von Vorteil, da sie aufgrund der angewandten Prozesse wissen, dass ihre Daten in der sichersten Umgebung solcher Unternehmen geschützt sind. Im Umgang mit dem Internet der Dinge (IoT) ist Datensicherheit unerlässlich. Nicht nur die Mitarbeiter müssen engagiert auf eine kontinuierliche Prävention hinarbeiten und Sicherheitsbedrohungen durch Systeme, Tools und Prozesse überwachen, sondern auch sicherstellen, dass Drittanbieter diese Praktiken ebenfalls einhalten.

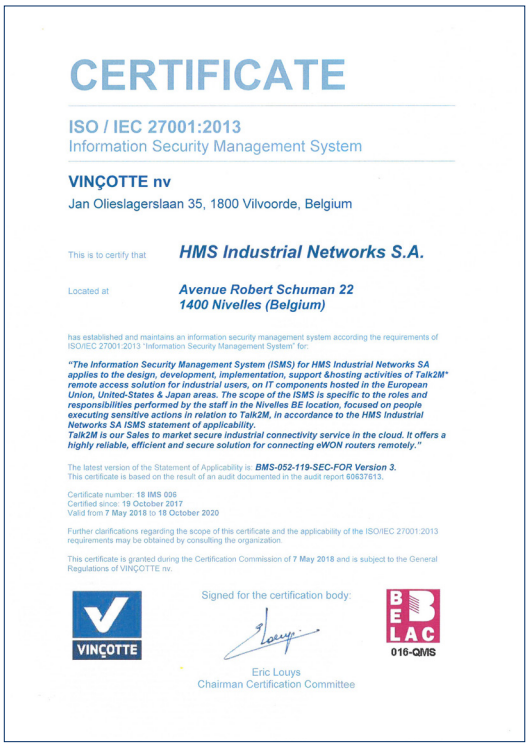
Sicherheit – Bestandteil des Entscheidungsfindungsprozesses

Ein Unternehmen zu wählen, das einem globalen Standard für das Informationssicherheitsmanagement folgt, ist das erste Kriterium, das ein Unternehmen oder eine Firma berücksichtigen muss, bevor es Aufträge vergibt. Vertrauliche Behandlung und ständige Datenverfügbarkeit sind die Gütesiegel guter Sicherheitspraktiken und -kontrollen. Der Umgang mit Informationssicherheitsrisiken kann sich nämlich auf die Integrität und den Ruf des Unternehmens und der Daten seiner Kunden auswirken. Dieses Whitepaper zeigt, warum die ISO 27001-Zertifizierung ein wesentlicher Schritt in diese Richtung ist.

HMS ist ein Anbieter von Qualitäts-Gateways/Routern, der – sofern dies aus der Ferne möglich ist – die Belastung durch Überwachung und Kontrolle vor Ort abnimmt, was Kosten und Zeit spart. Der Erfolg dieser Lösung hängt davon ab, ob der Datenfluss gut überwacht und abgesichert wird, was HMS aufgrund der Einhaltung der ISO 27001-Standards gewährleisten kann.

Besuchen Sie die Ewon-Website (www.ewon.biz/security) um mehr über unsere Dienstleistungen und darüber, wie wir globale Sicherheitsstandards einhalten, zu erfahren.

https://www.crn.com/news/security/300080151/telecom-partners-say-cloud-security-is-top-of-mind-in-wake-of-verizon-breach.htm?itc=refresh
https://www.iso.org/isoiec-27001-information-security.html



CERTIFICATE

ISO / IEC 27001:2013
Information Security Management System

VINÇOTTE nv
Jan Olieslagerslaan 35, 1800 Vilvoorde, Belgium

This is to certify that: HMS Industrial Networks S.A.

Located at: Avenue Robert Schuman 22
1400 Nivelles (Belgium)

has established and maintains an information security management system according the requirements of ISO/IEC 27001:2013 "Information Security Management System" for:

"The Information Security Management System (ISMS) for HMS Industrial Networks SA applies to the design, development, implementation, support &hosting activities of Talk2M remote access solution for industrial users, on IT components hosted in the European Union, United-States & Japan areas. The scope of the ISMS is specific to the roles and responsibilities performed by the staff in the Nivelles BE location, focused on people executing sensitive actions in relation to Talk2M, in accordance to the HMS Industrial Networks SA ISMS statement of applicability.*
Talk2M is our Sales to market secure industrial connectivity service in the cloud. It offers a highly reliable, efficient and secure solution for connecting eWON routers remotely."

The latest version of the Statement of Applicability is: **BMS-052-119-SEC-FOR Version 3.**
This certificate is based on the result of an audit documented in the audit report **60637613.**

Certificate number: **18 IMS 006**
Certified since: **19 October 2017**
Valid from **7 May 2018** to **18 October 2020**

Further clarifications regarding the scope of this certificate and the applicability of the ISO/IEC 27001:2013 requirements may be obtained by consulting the organization.

This certificate is granted during the Certification Commission of **7 May 2018** and is subject to the General Regulations of VINÇOTTE nv.

VINÇOTTE

Signed for the certification body:

Eric Louys
Chairman Certification Committee

BELAC 016-QMS

ISO 27001 certification

Der Inhalt dieses Dokuments wurde von Wachendorff Prozesstechnik aus dem Englischen ins Deutsche übersetzt. Das diesem Whitepaper zugrunde liegende Original-Dokument ist geistiges Eigentum von HMS Industrial Networks.
Alle Angaben ohne Gewähr, Irrtümer und Änderungen vorbehalten.

prozesstechnik.de

www.wachendorff-

Entscheidungssicherheit und Service

Das können Sie von uns erwarten:

- Kompetente und erreichbare Gesprächspartner für Ihre Entscheidungsträger im technischen und kaufmännischen Bereich – vor und nach dem Kauf!
- Technische Beratung und Unterstützung zu Produkten und Anwendungen per Telefon, E-Mail, Chat – und sehr gerne auch vor Ort.
- Spezifikation und Absicherung von Funktionen infrage kommender Komponenten
- Abstimmung von Anforderungen und Vorgehensweisen
- Teilnahme an Projektbesprechungen, einschließlich (End-)Kundenbesuchen, Präsentationen, Ausrichtung von Trainingsaktivitäten
- Überprüfung der Applikation unter definierten Bedingungen
- Vorbereitung, Durchführung der Integration, Unterstützung bei Inbetriebnahme und Dokumentation
- 3(!) Jahre Garantie

Seit 1978 sind wir zuverlässiger Lieferant industrierobuster und hochqualitativer Geräte für die Visualisierung, Kommunikation und Verarbeitung von Daten in den Bereichen Maschinen-, Anlagen- und Gebäudeautomation.

Mit absoluter Begeisterung und Verlässlichkeit arbeiten unsere motivierten Anwendungsberater und Vertriebsingenieure - sowie das gesamte Wachendorff-Team hinter den Kulissen - für Ihren Erfolg.

Wir tun alles dafür, dass Sie mit unseren Lösungen absolut zufrieden sind, heute und in der Zukunft.

Stellen Sie uns Ihre Automatisierungsaufgabe - jetzt!

Anwendungsberatung, Produktauswahl: Tel.: +49 (0) 67 22 / 99 65 - 966
Oder senden Sie uns eine E-Mail an: beratung@wachendorff.de

WACHENDORFF

Wachendorff Prozesstechnik GmbH & Co. KG
Industriestrasse 7 • D-65366 Geisenheim

Tel.: +49 (0) 67 22 / 99 65 - 20
Fax: +49 (0) 67 22 / 99 65 - 78
E-Mail: wp@wachendorff.de
www.wachendorff-prozesstechnik.de

2019

Ihr Partner: