WACHENDORFF
Prozesstechnik GmbH & Co. KG

Whitepaper
ISECOM STAR
Sicherheitszertifizierung für sichere Konnektivität

Ewon®
BY HMS NETWORKS

STAR
CERTIFIED OSSTMM 3.0
SECURITY TEST AUDIT REPORT

IndustrieROBUST

Zusammenfassung

Heutzutage gibt es im dynamischen Geschäftsumfeld zahlreiche Geschäftsrisiken, die, wenn sie nicht angegangen werden, zum Ausfall der Systemen, auf die sich Ihre Kunden verlassen, führen können. Sicherheitstests und -analysen machen einen großen Teil bei der Identifizierung solcher Risiken aus. Wie die Informationen gespeichert, verwaltet, abgerufen und geteilt werden, hat sich durch das Internet und die cloudbasierte Infrastruktur sowie Dienstleistungen stark verändert, da die Sicherheit von Daten vor Ort recht gering ist. Malware, Spyware und andere Datendiebstahlrisiken sowie Datenmissbrauch sind weit verbreitet.

Systeme mit Remote-Konnektivitätslösungen müssen daher sicher und standardbasiert sein. VPN-Technologien mit Remote Access erfordern, dass die Netzwerke und Geräte miteinander kommunizieren. Dies sollte jedoch auf Basis einer sicheren Kommunikation erfolgen.

Einführung

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 fremden 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.

STAR-Zertifizierung OSSTMM 3.0

Der Security Test Audit Report (STAR) ist eine Zertifizierung, die durch die Produktbewertung durch autorisierte externe Auditoren ausgestellt wird. Durch einen OSSTMM 3.0-Auditprozess stellt ein Unternehmen sicher, dass Sicherheitsparameter getestet und effektiv implementiert werden. Durch die STAR-Zertifizierung können Dienstleister jeder Größe potenziellen Kunden ein besseres Verständnis für ihren Grad an Sicherheitskontrollen vermitteln.

ISECOM und OSSTMM

ISECOM ist eine unabhängige Sicherheitsforschungseinrichtung, die das „Open Source Security Testing Methodology Manual“ (OSSTMM) erstellt und pflegt. Im Januar 2001 begann das "Institute for Security and Open Methodologies" (ISECOM) – eine offene Community und gemeinnützige Organisation – mit der Veröffentlichung des OSSTMM. Das war ein Schritt zur Optimierung des Testen und Implementierens von Sicherheit.

OSSTMM soll die Betriebssicherheit von physischen Standorten, Personen und Kommunikationsformen testen. Die Vernetzung von Menschen, Prozessen, Systemen und Software schafft ein komplexes, schwer zu kontrollierendes Netz. Durch geeignete Sicherheitsmaßnahmen können jedoch viele Risiken gemindert werden.

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.

Problemstellung

Die heutige Technologieumgebung ist durch Sicherheit auf jeder Ebene, jeder Schicht und an jedem gefährdeten Standort hochkomplex. Ein technisches Risiko kann leicht zum Geschäftsrisiko werden, sodass eine rechtzeitige Identifizierung für dessen Minimierung erforderlich ist. Unbefugter Zugriff und unverhohlene Sicherheitsangriffe bedrohen Unternehmen, da Kunden bei Kompromittierung ihrer Daten immer zu den ultimativen Opfern des Angriffs werden.

Lösungsdetails

Wie erfolgt die Zertifizierung?

Die OSSTMM-Zertifizierung ist die Gewährleistung der Unternehmenssicherheit nach den gründlichen Tests im Rahmen der OSSTMM-Standards und ist pro Überträger und Kanal für Unternehmen oder Teile von Unternehmen verfügbar, bei denen mindestens 90 % jährlich von einem unabhängigen externen Auditor validiert wurden.

Die Validierung von Sicherheitstests oder vierteljährlichen Metriken unterliegt den ISECOM-Validierungsanforderungen, um Konsistenz und Integrität zu gewährleisten.

Was deckt das Audit ab?

Zu den aufwendigen Schritten gehören Haltungsüberprüfung, Logistik, Überprüfung der aktiven Erkennung, Sichtbarkeitsprüfung, Zugangskontrolle, Vertrauensverifizierung, Kontrollverifizierung, Prozessverifizierung, Konfiguration und Schulungsverifizierung, Objektvalidierung, Segregationsprüfung, Competitive Intelligence Scouting, Quarantäneverifizierung, Privilegienprüfung, Überlebensvalidierung und Servicekontinuität sowie Enderhebung, Alarm- und Protokollprüfung.

Zweck des ISECOM OSSTMM-Auditberichts

Der Bericht bietet ein Standardberichtsschema auf Grundlage einer wissenschaftlichen Methodik für die genaue Charakterisierung der Sicherheit durch konsistente und zuverlässige Untersuchung. Er enthält auch Richtlinien, die es dem Auditor bei Einhaltung ermöglichen, ein zertifiziertes OSSTMM-Audit durchzuführen.

Geschäftsvorteile

- Als Basis brauchen cloudbasierte Infrastrukturen Sicherheit. Ist dies sichergestellt, ist das Unternehmen bereit für den Fall eines Sicherheitsangriffs. Die Zertifizierung hilft bei dieser Vorbereitung.
- Zum Erreichen der Unternehmensziele ist der Datenschutz einer der wichtigsten Aspekte, den man berücksichtigen muss. Die Anfälligkeit von Geräten, Netzwerken und Infrastrukturen für Angriffe und Verstöße kann dazu führen, dass Kunden von Ihren Produkten und Dienstleistungen Abstand nehmen.
- Das Befolgen branchenüblicher Best Practices, wie die Einhaltung von Sicherheitsprotokollen, schafft Vertrauen bei den Kunden.
- Die Zertifizierung verleiht dem Unternehmen ein hohes Maß an Vertrauenswürdigkeit. Durch spezifische Testinformationen, den Umfang und eine klare Erklärung zu den Sicherheitsmetriken sowie Details für Vergleiche mit früheren Sicherheitstests oder Branchendurchschnitten bietet sie potenziellen Kunden ein besseres Verständnis für das Maß, in dem Sicherheitskontrollen durchgeführt werden.
- Sie ermöglicht auch einen effektiven Vergleich mit anderen Unternehmen der entsprechenden Branchen und konzentriert sich auf die strategischen und operativen Geschäftsvorteile sowie eine effektive Partnerschaft.
- Die Zertifizierung dient als Nachweis einer Sachprüfung.
- Durch verständliche Kennzahlen weiß man, ob die erforderlichen Parameter eingehalten wurden oder nicht.
- Da Analysten für den Test verantwortlich sind, sind Fehler oder Fahrlässigkeit bei dem Audit höchst unwahrscheinlich.

eWON Talk2M und Argos haben die STAR-Sicherheitszertifizierung erhalten

Remote-Konnektivitätslösungen erfordern die Einhaltung von einem hohen Maß an Qualitäts- und Sicherheitsparametern – insbesondere für Industrieanlagen. Der Datenaustausch und die Nutzung von Services über die Cloud machen alles möglich. Die Kunden haben mehr Vertrauen in den Anbieter der Lösung, wenn der Datenaustausch über die Cloud sicher ist. Die Überprüfung und das detaillierte Audit der Systeme und Prozesse durch einen Zertifizierungsprozess gewährleisten diese Sicherheit.

HMS ist ein Anbieter von Qualitäts-Gateways/Routern, der aus der Ferne die Belastung durch Überwachung und Kontrolle vor Ort abnimmt, was Kosten und Zeit spart. Die Remote-Konnektivitätslösungen eWON Talk2M und Argos von HMS Industrial Networks besitzen beide die ISECOM STAR-Sicherheitszertifizierung. Die Talk2M-Infrastruktur ist als integriertes Element in die Fernzugriffslösung integriert, wobei Argos Teil einer Remote-Verwaltungs-/Dashboard-Lösung ist. Beide sind ein vollständig redundantes Netzwerk verteilter Server (VPN und IIoT) und anderer Dienste, die als sicherer Knotenpunkt für eWON-Geräte und -Benutzer dienen.

Kontaktieren Sie uns, um mehr über unsere Dienstleistungen zu erfahren sowie darüber, wie wir globale Sicherheitsstandards einhalten.

[ii]http://www.isecom.org/about-us.html
[iii]http://isecom.org/mirror/STAR.3.pdf

Talk2m: *ISECOM STAR certified*

Argos: *ISECOM STAR certified*

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.

www.wachendorff-prozesstechnik.de

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: