EVIDEN

Zero Touch Onboarding

Sichere, automatisierte digitale Identitäten für OT-Systeme

Operational Technology (OT): Von Cyberangriffen bedroht

Operational Technology (OT) steuert zahlreiche Prozesse in kritischen Sektoren wie Energie, Fertigung, Verkehr, Logistik und Handel. Von Stromnetzen bis hin zur Wasserversorgung sind solche Systeme ein wichtiger Bestandteil der nationalen Sicherheit.

Viele OT-Systeme sind jedoch nicht für die aktuelle Bedrohungslage geschaffen. Oft wurden diese Umgebungen zunächst mit nur rudimentären Sicherheitsfunktionen versehen, da Funktionalität und Effizienz Vorrang hatten. Der dadurch entstandene Mangel an Cybersicherheit in vielen Altsystemen macht diese zu leichten Zielen für Cyberangriffe. Der Trend zur Vernetzung und zur Verschmelzung mit der IT vergrößert die Angriffsfläche derzeit noch weiter.

Abbildung 1: OT-Angriffe sind eine Herausforderung für die kommenden Jahre. Quelle: Gartner[1], SecurityIntelligence[2]

In den letzten Jahren haben Cyberangriffe zahlreiche Ausfälle verursacht – unter anderem bei Automobilherstellern, Reifenfabriken, Lebensmittelunternehmen und Verlagen. Weitere OT-Sicherheitsvorfälle haben zu Flugverspätungen für Zehntausende von Passagieren, zu Produktionsstopps in der Metallindustrie und im Bergbau, zu Bränden und Schäden an Anlagen sowie zu Fehlfunktionen in Frachtcontainern und in der Kraftstoffversorgung geführt.

Eviden geht von einer weiteren Zunahme direkter und indirekter OT-Angriffe in den kommenden Jahren aus – ein Problem, das durch den Mangel an OT-Sicherheitsspezialisten noch verschärft wird.

[1] https://www.forescout.com/gartner-market-guide-for-operational-technology-ot-cybersecurity
[2] https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140

Die Lösung: Digitale Identitäten

Die Sicherheit von OT-Systemen ist nicht nur eine interne Angelegenheit, sondern längst auch Gegenstand von Gesetzen. Sicherheitsstandards wie IEC 62443 unterstützen deren Einhaltung, wobei der Schwerpunkt dieser Spezifikation auf dem Risikomanagement und der Sicherheit über den gesamten Lebenszyklus liegt. Beispielsweise schreibt die NIS2-Richtlinie den Betreibern kritischer Dienste Sicherheitsmaßnahmen vor und fordert ein Risikomanagement sowie die Meldung von getroffenen Sicherheitsmaßnahmen und Vorfällen. NIS2 wird voraussichtlich dazu führen, dass zusätzliche Bereiche in die OT-Sicherheit einbezogen werden und dass Rechtsvorschriften wie KRITIS (Deutschland) oder OIV/SIIV (Frankreich) erweitert werden. Der Cyber Resilience Act (CRA) der Europäischen Union zielt darauf ab, die Cybersicherheit für vernetzte Geräte – OT-Systeme gehören dazu – durch strengere Sicherheitsstandards zu verbessern.

Digitale Identitäten sind der Schlüssel zur OT-Sicherheit.

Wenn jede Einheit in einem OT-System als eigenständige Identität arbeitet, können Geräte sicher miteinander interagieren – beispielsweise durch verschlüsselte Kommunikation, gegenseitige Authentifizierung und Gewährleistung der Datenintegrität. Jede Identität ist mit einem digitalen Zertifikat verknüpft, durch ein öffentliches/privates Schlüsselpaar verankert und folgt einem Lebenszyklus, der mit dem Onboarding beginnt und mit der Außerbetriebnahme endet. Die Einrichtung sicherer digitaler Identitäten bildet die Grundlage für eine sichere und effiziente Geräteverwaltung in OT-Umgebungen.

Aktuelle Herausforderungen im OT-Identity-Management

In vielen Unternehmen und Behörden haben die Entscheider den Wert sicherer digitaler Identitäten längst erkannt und fordern deren Einführung in allen OT-Umgebungen. Für viele Fachverantwortliche stellt dies eine Herausforderung dar. Denn bisher werden Versandkontrolle, Aufzeichnungen in Inbetriebnahme-Tools sowie Domain-Registrierung und -Profilierung meist noch von Hand erledigt. Hinzu kommt, dass oft keine sicheren Bereitstellungs- und Erneuerungsprozesse implementiert sind. Wenn ein digitales Zertifikat abläuft (die Gültigkeitsdauer ist in der Regel auf 2 Jahre festgelegt), kann dies aufgrund von Authentifizierungsfehlern zu Serviceausfällen führen. Da in vielen OT-Systemen kein Fernzugriff vorhanden ist, verkomplizieren sich diese Prozesse zusätzlich, denn der Bediener muss sich persönlich zum System begeben.

Die Entscheider haben den Wert sicherer digitaler Identitäten längst erkannt und fordern deren Einführung in allen OT-Umgebungen. Dies stellt für viele Fachverantwortliche eine Herausforderung dar.

Zero Touch Onboarding – Eine kurze Einführung

Zero Touch Onboarding (ZTO) automatisiert das Identitätsmanagement in OT-Umgebungen. Es handelt sich um einen standardisierten Ansatz. ZTO ermöglicht die einfache und sichere Integration neuer Geräte – repräsentiert durch ihre eindeutigen digitalen Identitäten – in ein OT-Netzwerk, ohne dass eine direkte menschliche Beteiligung erforderlich ist. Der ZTO-Prozess beginnt beim Gerätehersteller und gewährleistet durch standardisierte Protokolle einen reibungslosen Übergang in die Umgebung des Betreibers.

Es gibt mehrere wichtige Standards für das ZTO. Beispiele sind BRSKI (Bootstrapping Remote Secure Key Infrastructure) und FDO (FIDO Device Onboarding), die die anfängliche Authentifizierung und Schlüsselerstellung für Geräte automatisieren, sowie EST (Enrollment over Secure Transport) für die sichere Registrierung von Geräten bei einer Zertifizierungsstelle. Bisher unterstützen zwar viele IoT-Geräte diese Standards nicht und sind daher auch nicht ZTO-fähig. Mit dem Laden des Eviden ZTO-Clients auf ein Gerät gibt es jedoch einen einfachen Weg, um dies zu ändern.

ZTO reduziert den Arbeitsaufwand drastisch und verschafft Herstellern einen Wettbewerbsvorteil, indem es sichere Lösungen ermöglicht, die die Kundenbindung erhöhen.

ZTO bietet klare Vorteile für alle Beteiligten. Für den Betreiber reduziert sich der Arbeitsaufwand für sichere Geräte drastisch, während der Hersteller einen Wettbewerbsvorteil auf einem Markt erlangt, der zunehmend sichere, ZTO-basierte Lösungen fordert. Mit ZTO machen die Hersteller ihre Produkte nicht nur für Kunden attraktiver, sondern stärken auch die Kundenbindung.

ZTO im Vergleich zum manuellen Onboarding

ZTO automatisiert Schritte, die derzeit meist manuell durchgeführt werden (Abbildung 2). Der ZTO-Prozess beginnt beim Hersteller, wo einer Komponente eine temporäre Identität in Form eines digitalen Zertifikats aus der PKI des Herstellers zugewiesen wird. Diese temporäre Identität wird später beim Kunden verwendet, um das Gerät zu authentifizieren und um eine lokale Identität inklusive eines Zertifikats zu erzeugen. Sobald der Onboarding-Prozess abgeschlossen ist, kann das Gerät sicher mit anderen Identitäten kommunizieren und außerdem sein Zertifikat vor Ablauf selbständig erneuern, wodurch eine kontinuierliche Sicherheit gewährleistet wird.

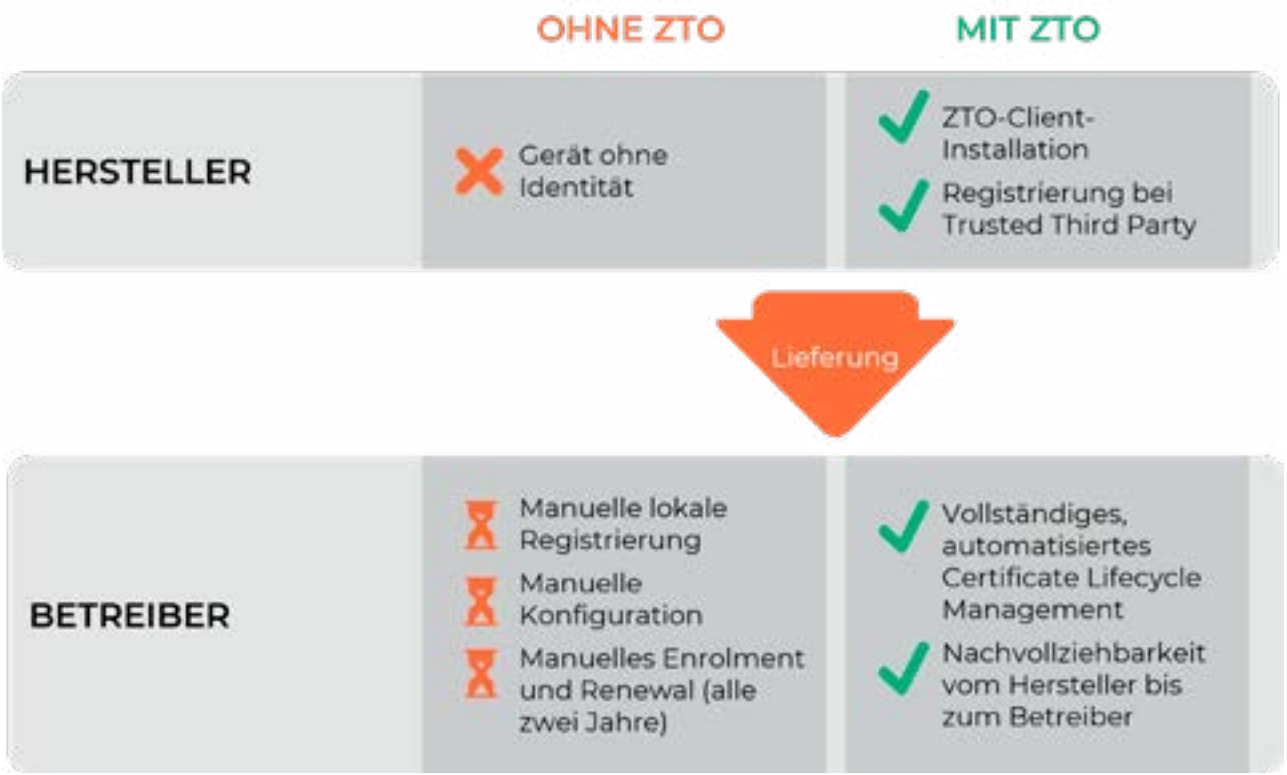

Abbildung 2: Weg des Geräts vom Hersteller zum Betreiber

Das Portfolio von Eviden Digital Identity

Eviden bietet ein umfassendes Portfolio von Produkten und Dienstleistungen für ZTO, darunter den Eviden ZTO Client, Eviden MASA (Manufacturer Authorized Signing Authority) und Eviden Domain Registrar. Diese Komponenten sind vollständig kompatibel mit jeder X.509-PKI.

Wer eine schlüsselfertige Lösung bevorzugt, kann zusätzlich die IDnomic PKI von Eviden nutzen.

Nach mehr als zwei Jahrzehnten am Markt und mit der Erfahrung aus zahlreichen Großprojekten ist IDnomic PKI eine ausgereifte, sichere und zuverlässige Lösung.

Die genannten ZTO-Lösungen werden durch die Beratungskompetenz von Eviden noch wertvoller. Wir unterstützen sowohl die Betreiber als auch Systemintegratoren bei der Implementierung unserer Lösungen.

Kontakt

Sie betreiben eine größeres OT-System? Dann informieren Sie sich über das volle Potenzial von Zero Touch Onboarding. Sie sind Gerätehersteller? Dann laden wir Sie ein, unsere ZTO-Technologie in ihre Produkte zu integrieren. Sie sind Systemintegrator? Dann machen Sie sich mit unserem Angebot vertraut.

Gerne erklären wir ihnen, wie Sie mit ZTO Prozesse rationalisieren, Kosten senken und die allgemeine Systemleistung verbessern können. Wir stellen Ihnen auch gerne eine Demo zur Verfügung. So können Sie uns kontaktieren:

cv-info@eviden.com

www.cryptovision.com

Unser Consulting-Team setzt sich gerne mit Ihnen in Verbindung.

EVIDEN

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

Eviden[1]

Eviden zählt zu den führenden Experten auf den Gebieten der Quantencomputer-Technik und der Kryptografie. Durch diese einzigartige Kombination ist Eviden Ihr idealer Partner für die Post-Quanten-Kryptografie. Wir unterstützen Sie dabei, Ihre Kryptografieprodukte, einschließlich HSMs, E-Mail-Verschlüsselungs-Software, VPN-Lösungen und PKI-Systemen, quantensicher zu machen. Darüber hinaus begleiten wir Ihre Organisation beim Migrationsprozess.

1 Eviden betreibt folgende Marken: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid, X-Perion. Eviden ist eine eingetragene Marke. © Eviden SAS, 2025.

Soziale Medien

eviden.com