LÖSUNGSBESCHREIBUNG

Tripwire schützt industrielle Steuersysteme

So stärken Sie in drei einfachen Schritten die Cybersicherheit Ihrer OT-Umgebung

Highlights

Immer mehr für die Automatisierung konzipierte Geräte werden mit industriellen Netzwerken verbunden. Gleichzeitig steigt die Anzahl der Cyberrisiken, die ihre Sicherheit, Produktivität und Qualität bedrohen. Zu diesen Risiken zählen unter anderem Bedienfehler, Aktivitäten böswilliger Insider und externe Hacker, die versuchen, in das Netzwerk einzudringen. Alle haben eines gemeinsam: Sie haben das Potenzial, die Produktivität, Produktqualität und Sicherheitsstandards zu beeinträchtigen und somit erhebliche finanzielle Schäden zu verursachen und Ihre Mitarbeiter in Gefahr zu bringen. Aus diesem Grund ist es heute wichtiger denn je, industrielle Steuersysteme mit speziell darauf ausgerichteten Sicherheitslösungen zu schützen.

Branchen wie Fertigung, Energieversorgung, Erdöl- und Erdgas, Chemie und Transport bilden das Fundament unserer modernen Infrastruktur. Um einwandfrei zu funktionieren, verlassen sie sich auf hochverfügbare, zuverlässige und sichere industrielle Netzwerke. Industrielle Steuersysteme (Industrial Control Systems, ICS) – darunter SCADA-, PCS- und BACS-Systeme – sind für die Überwachung und Kontrolle industrieller und physischer Infrastrukturen verantwortlich. Organisationen in den obengenannten kritischen Industriebranchen sowie alle anderen Unternehmen, die mit ICS arbeiten, stehen unter enormem Druck, ihre Ressourcen zu modernisieren, sie vor zunehmend ausgefeilten Angriffen zu schützen, immer strengere gesetzliche Vorschriften einzuhalten und den Fachkräftemangel in ihren Cybersicherheitsteams zu überwinden.

Die größten Herausforderungen der Cybersicherheit

„Wenn es noch funktioniert, dann bloß nichts ändern!" ist oft die erste Reaktion auf Modernisierungsvorschläge – selbst, wenn es um die Cybersicherheit geht, die in jeder Organisation eigentlich auf dem neuesten Stand sein sollte. Gleichzeitig werden Hacker immer raffinierter und es spielen ihnen diverse andere Faktoren in die Hände:

- **Industrielle Geräte und Systeme wurden nicht konzipiert, um Cybersicherheitsanforderungen zu erfüllen.** Häufig nutzen sie veraltete, unsichere Kommunikationstools und -protokolle und viele Industrieanlagen arbeiten noch mit Geräten, die weder technische noch Sicherheits-Upgrades unterstützen.
- **Organisationen haben nur einen begrenzten Überblick** über die Geräte, die mit ihrem Netzwerk verknüpft sind, über

ihre Konfigurationen, potenzielle Konfigurationsänderungen, Muster in der Netzwerkkommunikation, Schwachstellen und darüber, welchen Risiken sie ausgesetzt sein könnten.

- **Vielen ICS-Betriebsteams fehlen die nötigen Ressourcen** wie Personal, Zeit, Technologie oder Fachkenntnisse, um das Netzwerk gegen Cyberbedrohungen zu wappnen.
- **Kontinuierliche Schwachstellenscans und regelmäßiges Patching sind nicht tragfähig**, weil dies die Verfügbarkeit kritischer Systeme beeinträchtigen könnte.
- **Die Cybersicherheit ist in vielen Organisationen keine Priorität**. Führungskräfte sind mitunter geneigt, zu denken, dass ihr Unternehmen nie Opfer eines Cyberangriffs werden könnte, weil es ihrer Meinung nach kein lohnendes Ziel für Hacker ist oder weil die vorhandenen Sicherheitsmaßnahmen bisher vollkommen ausreichend waren.
- **Es ist nicht immer einfach, das Risikopotenzial industrieller Steuersysteme zu erfassen und zu messen**. Das erschwert auch die zeitliche und finanzielle Planung für die Implementierung eines einschlägigen Cybersicherheitsprogramms – es sei denn, das Programm wird an die Betriebsabläufe angepasst, was ein recht zeitaufwendiges Unterfangen sein kann.
- **Mitarbeiterfehler und unerwartete Ereignisse lassen sich meist nicht prognostizieren**. Ohne den Normalzustand der Systeme, Geräte und des Netzwerks zu kennen, ist es fast unmöglich, zeitnah und richtig auf ungeplante Änderungen zu reagieren.
- **Organisationen werden an eine wachsende Zahl von gesetzlichen Vorgaben gebunden** und müssen bei Nichteinhaltung mit immer höheren Geldstrafen rechnen.
- **Industrielle Steuersysteme sind zunehmend von der IT-Infrastruktur abhängig,** um Befehle an Geräte und Komponenten weiterzuleiten. Diese Digitalisierung verbessert die Datenerfassung, steigert die Systemeffizienz und ermöglicht eine schnellere Markteinführungszeit, ist aber auch mit Cyberrisiken verbunden.
- **Die Führungsriege, Abteilungen und Zweigstellen setzen unterschiedliche Prioritäten**. Die Geschäfts- und Cybersicherheitsziele all dieser Gruppen aufeinander abzustimmen, geschieht nicht von heute auf morgen.
- **Je länger sich Angreifer unerkannt im Netzwerk aufhalten,** desto mehr Zeit haben sie für die Ausspähung der Umgebung und Vorbereitung ihres Angriffs.
- **Unterschiedliche Verantwortlichkeiten bei der Implementierung von Cybersicherheitsmaßnahmen** zwischen den Bereichen IT und OT erschweren eine einheitliche Entscheidungsfindung.

Der Tripwire-Ansatz für ICS-Sicherheit

Wenn Sie mit diesen Herausforderungen zu kämpfen haben, ist es höchste Zeit, zu einem proaktiveren Sicherheitsansatz zu wechseln und Ihren Teams praxistaugliche Strategietipps zur Verfügung zu stellen. Zu allererst benötigen Ihre Mitarbeiter Tools, die ihnen einen besseren Überblick über sämtliche Ressourcen bieten, die Überwachung des Netzwerks vereinfachen und eine effektivere Abwehr und Fehlerbehebung ermöglichen. Mit den leistungsstarken Lösungen von Tripwire können Sie diese Ziele erreichen und eine umfassende Cybersicherheitsstrategie für Ihre ICS-Umgebung entwickeln.

Abb. 1: Drei Schritte für proaktivere Cybersicherheit in Industrieanlagen

Wichtige Fragen für die ICS-Sicherheit

- Wurden an meinen Geräten/Ressourcen Konfigurationsänderungen vorgenommen?
- Hat sich der Normalzustand im Betrieb geändert?
- Droht ein Ausfall meiner Geräte?
- Befinden sich nicht autorisierte Geräte in meinem Netzwerk?
- Hat sich mein Schwachstellenprofil geändert?

Bessere Transparenz

Für eine effektive Risikoeinschätzung sollten Sie sich ein detailliertes Inventar Ihrer Hard- und Software und ein Diagramm der Netzwerktopologie zulegen. Außerdem müssen Sie sich einen Überblick über die Kommunikation zwischen dem ICS- und dem IT-Netzwerk der restlichen Organisation, Konfigurationsänderungen, risikoreiche Schwachstellen, Logdateien aus Scans, den Fernzugriff per VPN und mobile Zugangspunkte verschaffen. Mit diesen Informationen können Sie Ihre Netzwerksicherheit stärken, Ereignisdaten erfassen und miteinander in Beziehung setzen und Fehler beheben, bevor sie die Zuverlässigkeit Ihrer ICS oder den Betrieb beeinträchtigen.

So hilft Tripwire:

- **Cybersicherheitsbewertungen:** Eine interne oder von einer zuverlässigen Drittpartei durchgeführte Bewertung Ihrer industriellen Netzwerkinfrastruktur gibt Ihnen Einblick in die verschiedenen Komponenten und unterstützt Sie dabei, Risiken zu identifizieren, zu reduzieren und letztendlich Ihre Geschäftsziele zu erreichen.
- **Ressourcenerfassung:** Mit der anbieterunabhängigen Cybersicherheitsplattform für Industrieanlagen von Tripwire steht Ihnen ein funktionsreiches Tool für die Datenerfassung zur Verfügung, das aktive, passive, integrierte oder eine Kombination dieser Ansätze unterstützt. Erfahrungsgemäß erhalten Kunden mit Sicherheitsmodellen, die sich all diese

Ansätze zunutze machen, die umfassendsten, präzisesten Erkenntnisse aus ihren ICS-Umgebungen und profitieren von störungsfreien Datenerfassungsverfahren.

Tripwire-Lösungen nutzen native industrielle Protokolle für die aktive Ressourcenerkennung; importieren und parsen automatisierte Konfigurationsdateien von Anbietern, um bei der Systemüberwachung einen Hybrid-Ansatz zu verfolgen; lassen sich mit Produkten von Drittanbietern wie Rockwell Software FactoryTalk AssetCentre und MDT Autosave integrieren; und unterstützen die passive Datenerfassung, indem sie eine Kopie der Datenpakete im Netzwerkverkehr erstellen und diese gründlich analysieren. Durch diesen variierten Sicherheitsansatz können Sie kritische Statusinformationen viel einfacher zusammentragen, ohne dabei den Geschäftsbetrieb zu stören. Außerdem können Sie Tripwire mit Hardware-Plattformen integrieren und diese zur Datenerfassung einsetzen.

Schutz- und Abwehrmaßnahmen

Nachdem Sie sich einen besseren Überblick über Ihre Ressourcen, Daten und Systeme verschafft haben, können Sie mit der Implementierung passender Sicherheitsmaßnahmen beginnen, um Cyberbedrohungen abzuwehren und das Geschäftsrisiko zu minimieren. Dabei spielen die Netzwerksegmentierung und Stärkung der Gerätesicherheit eine besonders wichtige Rolle.

- **Netzwerksegmentierung:** Hier geht es darum, das Netzwerk in verschiedene kleinere Segmente oder Zonen aufzuteilen, in denen nur die Kommunikation zwischen bestimmten industriellen Ressourcen erlaubt wird.
- **Stärkere Sicherheit für Geräte:** Indem Sie sämtliche mit Ihrem Netzwerk verbundenen Geräte (Nutzerschnittstellen, Engineering-Workstations, Switches, Router und Firewalls) auf die Cybersicherheitsstandards Ihrer Branche (wie IEC 62443) abstimmen, können Sie Ihren Sicherheitsstatus verbessern.

So hilft Tripwire:

Für eine robuste, zuverlässige Netzwerksegmentierung bedarf es guter Teamarbeit: Tofino Security unterstützt Kunden mit robusten Sicherheitsappliances und Tripwire ergänzt diese mit einem Bewertungs-Modul, das prüft, ob die Konfiguration der Geräte im Netzwerk mit den einschlägigen Best Practices und Cybersicherheitsstandards übereinstimmt. Wir sorgen dafür, dass Sie immer auf dem neuesten Stand sind und überprüfen dazu kontinuierlich einer Vielzahl gesetzlicher Vorgaben, darunter:

- IEC 62443
- NERC CIP
- NEI 08-09
- NIST SP 800-82
- NIST Cybersecurity Framework
- Vorschriften für Prozesskontrollnetzwerke der American Water Works Association
- ISO 27001
- Empfehlungen des Center for Internet Security (Center for Internet Security's Critical Security Controls, CIS CSC)
- u. v. a. m.

IT und OT: ein starkes Team

Die IT-Perspektive: IT-Mitarbeiter sind für den Schutz des Netzwerkperimeters und für sicheres Zugriffsmanagement verantwortlich. Dazu setzen sie Firewalls ein, legen demilitarisierte Zonen fest, segmentieren das Netzwerk und implementieren Single-Sign-On-Lösungen. IT-Umgebungen werden typischerweise von internen Mitarbeitern oder externen Partnerunternehmen zentral verwaltet und werden regelmäßig verändert und ergänzt, zum Beispiel mit neuer Hardware, Anwendungs- und Software-Updates, zusätzlichen virtuellen Systemen und wöchentlichen oder monatlichen Patching-Zyklen. Für IT-Beauftragte stehen der Schutz vertraulicher Daten und die Gewährleistung ihrer Integrität an erster Stelle, weswegen es manchmal zu Verfügbarkeitsengpässen dieser Informationen kommen kann.

Die OT-Perspektive: OT-Teams hingegen haben andere Prioritäten. Sie müssen die Verfügbarkeit, Zuverlässigkeit und Sicherheit des physischen industriellen Netzwerks gewährleisten. Die Cybersicherheit ist ein relativ neuer Verantwortungsbereich. Möglicherweise können neue Cybersicherheitsmaßnahmen nur während eines der seltenen Zeitfenster für Wartungsarbeiten implementiert werden, die beim Upgrade einer Produktionslinie oder der Einrichtung einer neuen Anlage stattfinden. OT-Teams haben sich bislang relativ eigenständig um ihre Netzwerke gekümmert und die enge Zusammenarbeit mit den IT-Verantwortlichen bringt neue Herausforderungen mit sich. Daher sollten sämtliche Eingriffe gut durchdacht sein, Sicherheitsmaßnahmen zum Schutz der Kommunikation zwischen OT- und IT-Umgebungen implementiert und demilitarisierte Zonen festgelegt und klar markiert werden.

IT/OT im Einklang: Netzwerke werden zunehmend auf Konnektivität zwischen Ressourcen, Umgebungen, Geräten und Systemen ausgerichtet und die Grenze zwischen IT und OT verschwimmt immer mehr. Daher ist es umso wichtiger, die Zusammenarbeit zwischen diesen beiden Bereichen zu fördern. OT-Teams sollten über die Cybersicherheitsanforderungen der IT in puncto Systeme, Prozesse und Zugriff nachdenken. Und IT-Beauftragte sollten sich überlegen, wie sie die nötigen Sicherheitsmaßnahmen implementieren können, ohne die Zuverlässigkeit oder Verfügbarkeit des industriellen Netzwerks zu beeinträchtigen. Es gilt also, die jeweiligen Geschäftsziele zu verstehen und sich gegenseitig beim Erreichen dieser Ziele zu unterstützen.

Dieses Verständnis ließe sich zum Beispiel fördern, indem ein Vertreter der IT- oder OT-Teams eine Zeit lang in der anderen Abteilung oder in der Partnerorganisation arbeiten und sich vor Ort ein Bild des täglichen Betriebs machen würde. Sicherheitsvorfälle sind heute leider unvermeidlich geworden, ob durch einen externen Cyberangriff, Aktivitäten eines böswilligen Insiders oder durch Bedienfehler. Daher ist es unentbehrlich, dass IT- und OT-Teams zusammenarbeiten, um die industriellen Steuersysteme der Organisation mit leistungsfähigen Technologien, Erkennungs- und Abwehrmaßnahmen und einer starken Cybersicherheitsstrategie vor ruf- und betriebsschädlichen Bedrohungen zu bewahren.

Zudem besteht die Möglichkeit, Vorgaben zu modifizieren oder sogar Ihre eigenen zu erstellen, um das Modul an Ihre geschäftlichen Sicherheitsanforderungen anzupassen. Diese Option ist besonders für Organisationen mit hochspezialisierten oder älteren Geräten von Nutzen.

Kontinuierliche Überwachung

Mit einer soliden Basis für Transparenz und Sicherheit im Netzwerk können Sie sich der Überwachung Ihrer IT-Umgebung widmen. Indem Sie sich Einblick in Ihre Systeme und Ressourcen verschaffen, ist es einfacher, unerwartetes oder schädliches Verhalten frühzeitig aufzudecken, den Betrieb vor Angriffen zu schützen und ungeplante Ausfälle zu vermeiden.

So hilft Tripwire:

» In Kombination mit den Tools für bessere Transparenz und stärkere Sicherheitsmaßnahmen profitieren Tripwire-Kunden von einem dritten Vorteil: die Verarbeitung der erfassten Daten zu praxistauglichen Erkenntnissen und Warnmeldungen bei unerwarteten Ereignissen im Netzwerk. Mit solch aussagekräftigen Informationen sind Sie in der Position, Bedrohungen rasch zu erkennen, abzuwehren und Ihre Systeme nach Ausfällen schnell wieder in Gang zu bringen. Tripwire-Lösungen stärken Ihre ICS-Sicherheit und reduzieren Ausfallzeiten, indem sie

- unerwartete Änderungen an Controllern oder Konfigurationen identifizieren,
- erkennen, ob nicht autorisierte Ressourcen das Netzwerk nutzen und Malware oder sonstige schädliche Inhalte verbreiten oder Verbindungen mit weiteren Netzwerken herstellen, und
- Engineering-Workstations überwachen, um sicherzustellen, dass sämtliche (neue) Konfigurationen interne Spezifikationen oder gesetzliche Sicherheitsvorgaben erfüllen.

Tripwire-Lösungen

Wir stellen Organisationen in industriellen Branchen ein breites, bewährtes, speziell auf Automatisierungsumgebungen abgestimmtes Produktportfolio an, um genau wie ein SCADA-System zur Optimierung und Steuerung grundlegender Cybersicherheitskontrollen in industriellen Umgebungen beizutragen. Mit branchenführenden Datenerfassungsfunktionen unterstützt Tripwire seine Kunden dabei, sich einen umfassenden, detaillierten Überblick über ihre industriellen Steuersysteme, die Kommunikation zwischen verteilten Netzwerken, Geräten und Ressourcen, und über die gesamte Enterprise-IT zu verschaffen – alles, ohne den Betrieb zu unterbrechen.

Tripwire Industrial Visibility (TIV)

Tripwire Industrial Visibility stellt Ihnen Funktionen für die Erfassung des Ressourcenbestands, Erkennung von verdächtigem oder unwartetem Verhalten und für das Schwachstellenmanagement zur Verfügung. Somit wissen Sie stets genau, was sich in Ihrem ICS-Netzwerk befindet und wie Ressourcen miteinander kommunizieren, und sind in der Lage, Risiken frühzeitig zu identifizieren. Passive, aktive, integrierte oder kombinierte Überwachungsansätze ermöglichen dabei umfassende Transparenz.

Außerdem bieten wir TIV in einem Lösungspaket mit Tripwire Log Center an, unserem Tool zur Erfassung und Zusammenführung von Logdateien aus Geräten in verschiedenen Umgebungen und von unterschiedlichen Anbietern. Log Center verarbeitet und normalisiert auch von TIV erfasste Ereignisdaten über kritische Warnmeldungen zu unerwarteten Änderungen an Controllern oder deren Konfiguration, zu hochgeladener Firmware und Abweichungen vom Normalsystemzustand und fasst diese in vordefinierten Berichten zusammen. Dadurch profitieren Kunden von kontextreichen Einblicken und bewahren die Integrität ihres ICS-Netzwerks. Während Tripwire Industrial Visibility Ihre OT-Umgebung schützt, können Sie sich also wieder der Produktivitäts- und Verfügbarkeitssteigerung sowie der Sicherheit im Betrieb widmen.

Tripwire Enterprise für industrielle Geräte

Unsere Tripwire Enterprise-Lösung für industrielle Geräte schließt eine spezielle Engine zur Erkennung und Auswertung von Konfigurationsänderungen an Geräten und zur Generierung einschlägiger Warnmeldungen ein. Damit gewährleisten Sie, dass Ihre Geräte optimal geschützt und auf interne, oder auch auf externe Sicherheitsvorgaben wie IEC 62443, abgestimmt sind. Wenn Sie zum Beispiel festgelegt haben, dass sämtliche USB-Ports auf Engineering-Workstations deaktiviert werden sollen, können Sie mit Tripwire Enterprise feststellen, welche Workstations diese Vorgaben nichteinhalten. Gleichzeitig profitieren Organisationen, die gesetzlichen Branchenstandards unterliegen, von Funktionen für die Durchsetzung von Compliance-Maßnahmen und zur Stär-kung der Sicherheitsinfrastruktur. Somit sparen sie Kosten und vereinfachen die Vorbereitung auf Betriebsprüfungen. Außerdem unterstützt Sie Tripwire Enterprise mit leistungsfähigen Automatisierungsfunktionen und Empfehlungen bei der schnellen Wieder-herstellung von Fehlkonfigurationen und lässt sich unter anderem mit SIEMs, IT-GRC-Management, Workflow-Systemen und CMS-Lösungen (Change Management Systems) integrieren.

Enterprise punktet zudem mit speziell für industrielle Geräte konzipierten Überwachungsfunktionen und agentlosen Datenerfassungsmethoden, die industrielle Protokolle wie Modbus TCP und Ethernet/IP CIP sowie weitere in industriellen Netzwerken eingesetzte Protokolle wie SNMP und webbasierte Anwenderschnittstellen nutzen. Hinzu kommen die Integration mit Rockwell Automation FactoryTalk AssetCentre, MDT AutoSave und Kepware und die einzigartige Tofino-Engine zur Erkennung von Änderungen an Firewallkonfigurationen.

Tripwire Whitelist Profiler

Tripwire Whitelist Profiler erweitert Tripwire Enterprise um Funktionen, die es Kunden ermöglichen, autorisierte Systemeinstellungen in einer Whitelist festzulegen. Bei Systemscans werden dann alle Einstellungen, die mit der Whitelist übereinstimmen, in einem Bericht aufgeführt (einschließlich Name des Softwarepakets, Versionsnummer und zusätzlichen nutzerdefinierten Feldern). Konfigurationen, die nicht den Einstellungen in der Whitelist entsprechen, werden im Bericht entsprechend getaggt und es wird eine Warnmeldung generiert. Bei Bedarf können Sie auch weitere Erklärungen in den Bericht aufnehmen, um Betriebsprüfer mit den nötigen Kontextinformationen zu versorgen. Einstellungen können in Tripwire Whitelist Profiler in vier Kategorien eingeteilt werden: genehmigte Netzwerkports, aktive Betriebssystemdienste, installierte Software und aktive Nutzer-

konten. Jede dieser Kategorien hat ihre eigene Whitelist und eigene Workflows.

Tripwire Log Center

Tripwire Log Center agiert wie ein Datenwissenschaftler, der Ereignisdaten aus industriellen Betriebsprozessen sowie Messdaten aus Sensoren erfasst und bereitstellt und es Ihnen dadurch ermöglicht, den Betrieb zu straffen. Log- und Ereignisdateien, die aus Geräten in Ihrem industriellen Netzwerk zusammengetragen werden, gewähren Ihnen zudem Einblick in den Cybersicherheitsstand und den Betrieb. Einfach ausgedrückt sind diese Ereignisdaten Informationen über den Betriebszustand und über Betriebsfehler, die von Netzwerkgeräten (wie Router, Switches oder Firewalls), SPS-Geräten, SCADA-Systemen, Prozessleitsystemen, Nutzerschnittstellen, Engineering-Workstations und Authentifizierungs-systemen generiert werden. Diese Logdateien können über Syslog im Netzwerk versendet und entweder als lokale Flatfile oder in einer Datenbank gespeichert werden. Tripwire Log Center sammelt diese Logs aus verschiedenen Geräten und Repositorys und nutzt seine intuitive Schnittstelle, um Korrelationsregeln für die Erkennung und Analyse von Cybersicherheitsereignissen zu erstellen und Ihnen praxistaugliche Daten zur Reaktion auf Risiken oder potenzielle Bedrohungen bereitzustellen.

Dadurch profitieren Sie von einem umfassenden Überblick über Ihre Netzwerksicherheit, können selbst Geräte von Drittanbietern im Auge behalten und vermeiden Betriebsausfälle.

Professionelle Beratung

Eine Investition in Tripwire-Lösungen bedeutet eine Investition in nachhaltige Netzwerksicherheit und Compliance. Aus diesem Grund stellen wir Kunden speziell auf industrielle Umgebungen ausgerichtete professionelle Beratungsdienste zur Verfügung, darunter Cybersicherheitsbewertungen zur Identifizierung von Schwachstellen und Priorisierung von Patching-Maßnahmen, Penetrationstests zur Beleuchtung von Risikobereichen und die Bereitstellung fachkundiger Techniker vor Ort für die Verwaltung des Tripwire-Portfolios.

Tofino Xenon für industrielle Steuersysteme

Tofino Xenon für industrielle Steuersysteme ist eine vielseitige, robuste Sicherheitsappliance, die sich nahtlos in Ihr Netzwerk integrieren lässt und im Hintergrund arbeitet, um die Integrität und den Betrieb Ihrer industriellen Steuersysteme zu gewährleisten und zu schützen. Xenon dient der Inline-Überwachung industrieller Protokolle und nutzt Deep Packet Inspection-Funktionen (DPI), um Protokollanomalien zu erkennen und Zero-Day-Angriffe zu stoppen, ohne Signaturen aktualisieren zu müssen. Von Vorteil ist, dass keine Änderungen an der Netzwerkarchitektur erforderlich sind, da Xenon auf der Datenebene eingesetzt wird (Layer 2 des OSI-Netzwerkmodells). Da die Appliance ohne IP-Adresse operiert, kann sie von nicht autorisierten Personen auch nicht erkannt werden. Durch die Integration mit Tripwire Enterprise ist sichergestellt, dass Tofino Xenon Audit-Vorgaben und einschlägige Branchenstandards für das Änderungsmanagement erfüllt. Außerdem können Sie von Tofino Xenon erfasste Log- und Ereignisdateien über Syslog zur Analyse an Tripwire Log Center schicken, wo die Daten in Form von Dashboards und Berichten bereitgestellt werden.

Erste Schritte

Durch unsere langjährige Zusammenarbeit mit Organisationen aus Industriebranchen sind wir betens über Sicherheit (und Sicherheitsherausforderungen) in OT- und IT-Umgebungen informiert und damit ideal aufgestellt, Sie beim Schutz dieser kritischen Geschäftsbereiche, industrieller Steuersysteme und der Netzwerkinfrastruktur vor Cyberrisiken und -angriffen zu unterstützen. Mit den Produkten und Services von Tripwire profitieren Sie von umfassender Transparenz, robusten Schutz- und Abwehrmaßnahmen und leistungsfähigen Funktionen zur granularen, störungsfreien Überwachung Ihrer ICS-Umgebung.

Fordern Sie eine Demo an

Erleben Sie unsere Tools für ICS-Sicherheit und -Compliance in einer Demo in Aktion und stellen Sie uns Ihre Fragen. Näheres erfahren Sie unter **tripwire.com/contact/request-demo**

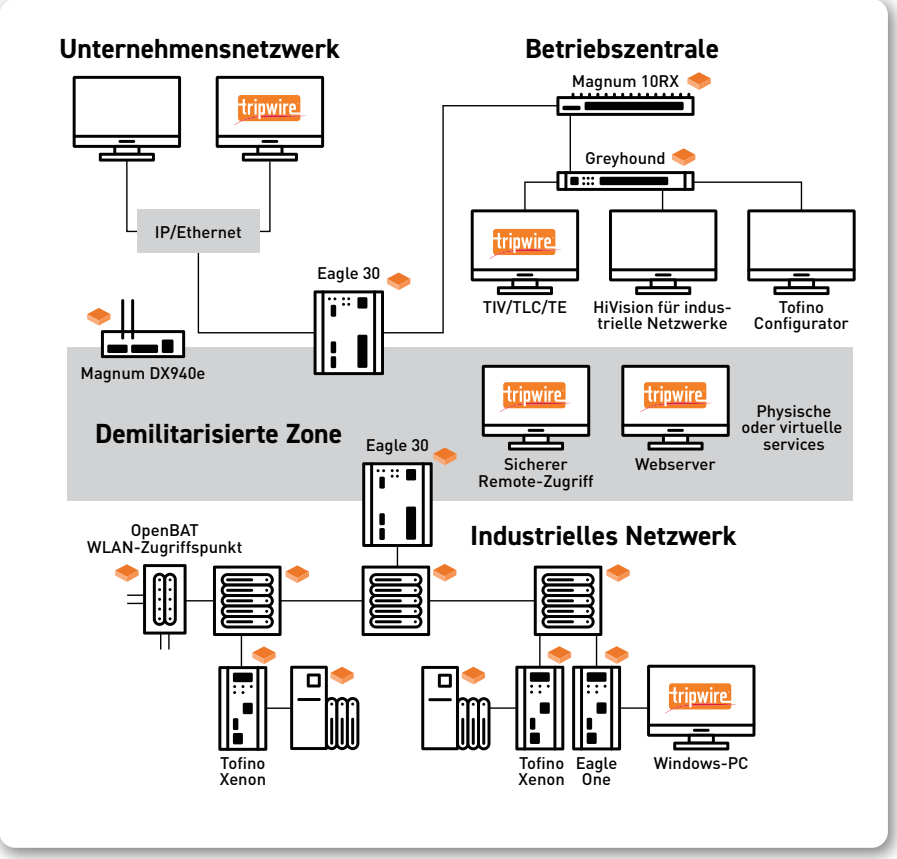

Abb. 2: Tripwire Industrial Visibility (TIV), Tripwire Log Center (TLC) und Tripwire Enterprise (TE): die perfekte Kombination zum Schutz von IT- und OT-Umgebungen

Tripwire stellt Kunden branchenführende Produkte zur Stärkung ihrer Cybersicherheit zur Verfügung. Wir schützen prominente Unternehmen auf der ganzen Welt vor Sicherheitsverletzungen und Cyberangriffen – und weil Hacker immer raffinierter werden, entwickeln auch wir unsere Technologien seit mehr als 20 Jahren ständig weiter. Unsere Lösungen sind sowohl On-Premises als auch in der Cloud verfügbar, wo sie Ihre digitale Infrastruktur schützen sowie Bedrohungen aufdecken und abwehren, ohne den Geschäftsbetrieb oder die Produktivität zu beeinträchtigen – sozusagen als unsichtbare Schutzbarriere für Ihre Systeme. **Weitere Informationen erhalten Sie unter tripwire.com.**

***The State of Security*: Aktuelles, Trends und interessante Einblicke finden Sie unter tripwire.com/blog**
Folgen Sie uns auf LinkedIn, Twitter und Facebook

SBSICS6b 1910