tenable.ot

Absicherung von Verkehrsinfrastruktur

WICHTIGSTE TRENDS

- Vermehrter Einsatz von Automatisierung zur nahtlosen Verbindung von Logistik-, Termin-, Strecken- und Volumenplanung
- Verstärkte Einführung von IoT-Technologie, um die GPS-Verfolgung von Schiffen, Containern, Fahrzeugen und Gütern zu unterstützen
- Umstellung auf „elastische" Logistik und Just-in-Time-Fertigung
- Reibungsloseres Reisen ohne Kompromisse bei der Sicherheit für erhöhte Kundenzufriedenheit

WICHTIGSTE TRENDS

- Die Verflechtung von IT/OT erfordert die Orchestrierung komplexer Systeme, in denen sich unter Umständen Cyber-Schwachstellen befinden, die zu Patching-Zwecken nicht einfach außer Betrieb genommen werden können.
- Verkehrssysteme sind hochgradig vernetzt und voneinander abhängig; über vertrauenswürdige Stellen können Sicherheitsbedrohungen in Systeme gelangen
- Da Assets in Bewegung und in hohem Maße verteilt sind, sind sie eher anfällig für Cyber Exposure und Angriffe.

HINTERGRUND

Das Transportwesen umfasst eine Vielzahl verschiedener Teilbereiche, wie etwa die Personenbeförderung in Kraftfahrzeugen, im Schienen- und Luftverkehr und in der Schifffahrt, die Güterbeförderung auf dem Land-, See- und Luftweg sowie weitere Transportmethoden wie etwa über Straßen, Pipelines und andere Verkehrsträger. Operative Technologie spielt eine entscheidende Rolle dabei, die Zuverlässigkeit dieser komplexen Systeme zu gewährleisten. Wirtschaftsräume sind in hohem Maße von ihnen abhängig, um die Gesellschaft in der uns bekannten Form zu unterstützen. Selbst vorübergehende Unterbrechungen oder Ausfälle, die durch einen Sicherheitsvorfall verursacht werden, können verheerende und kaskadierende Konsequenzen haben.

Moderne Verkehrsinfrastrukturen sind zunehmend komplex, da unterschiedliche Systeme miteinander interagieren müssen, um Aktivitäten und Abläufe zu koordinieren. Intelligente Infrastruktur ist notwendig, um die Verfolgung und Koordination zahlreicher verschiedener Assets in Echtzeit zu unterstützen. Um neben Echtzeit-Betriebsabläufen auch die Vielzahl von Veränderungen zu unterstützen, die von einem Augenblick zum nächsten auftreten können, müssen Ihre Systeme sowohl untereinander als auch mit dem Internet vernetzt sein. Aus diesem Grund sind Sichtbarkeit, Sicherheit und Kontrolle in Ihrer OT-Infrastruktur unerlässlich, um einen zuverlässigen und effizienten Betrieb zu gewährleisten.

Beispiele für OT im Transportwesen:

- An Flughäfen kommt Betriebstechnologie zum Einsatz, um Gepäckkontrollen durchzuführen, Betankungsanforderungen zu koordinieren, Instandhaltungsarbeiten und Flugzeugwartung zu organisieren, die Vorräte in Flugzeugen aufzufüllen usw.
- In der Schifffahrt sind OT-Betriebsabläufe an der Planung von Versandplänen, dem Beladen von Schiffen und dem Echtzeit-Tracking von Schiffen und einzelnen Containern beteiligt.
- Im Straßen- und Schienenverkehr können OT-Systeme Ampelschaltungen, Bedingungen, die Streckenführung, Wartung und viele weitere Aspekte regeln.

Ihr verflochtenes Netzwerk bietet zwar große Effizienzsteigerungen, weist aber auch eine deutlich breitere Angriffsoberfläche auf, sodass sich Bedrohungen leicht von einem Bereich Ihrer OT-Infrastruktur auf den nächsten ausbreiten können. Deshalb zählen industrielle Cyberbedrohungen heutzutage zu den bedeutendsten Risiken für die Verfügbarkeit, Sicherheit und Zuverlässigkeit von OT-Infrastrukturen im Transportwesen.

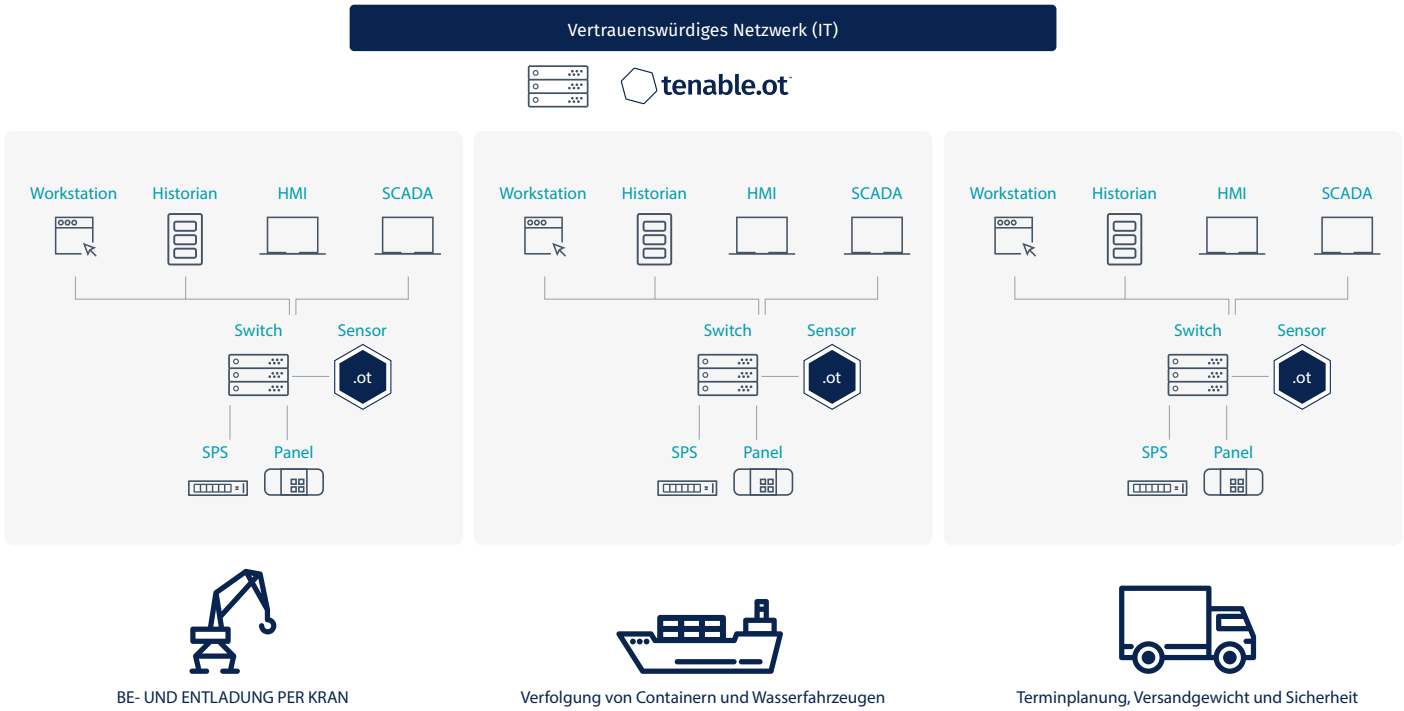
ANATOMIE EINES CYBERANGRIFFS IM TRANSPORTWESEN

1. Anfängliche Infiltration eines Verkehrsnetzes
2. Errichtung eines Brückenkopfes in einem der Assets des Netzwerks
3. Beginn der Auskundschaftung zwecks Bestimmung von Zielen, anfälligen Geräten und Schwachpunkten
4. Ausbreitung auf weitere Assets, um in die gewünschten Bereiche zu gelangen
5. Durchführung des Angriffs, wodurch der gewöhnliche Transportfluss von Personen, Produkten und Waren lahmgelegt wird und Rückwirkungen auf andere Branchen entstehen, die von Verkehrsinfrastruktur abhängig sind

Kürzliche Vorfälle

- **2020 –** Angreifer nahmen das Hafenterminal Shahid Rajaee im Iran ins Visier, was den gesamten Hafenbetrieb zum Erliegen brachte und mit erheblichen Auswirkungen auf das Be- und Entladen von Schiffen verbunden war. Dieser Angriff machte sich bis in weite Teile der Supply Chain bemerkbar.
- **2018 –** Subaru kündigte bei seinem neuen Ascent-Modell einen Fahrzeugaustausch an. Statt die Fahrzeuge zurückzurufen, musste das Unternehmen wegen eines fehlenden kritischen Schweißpunkts einen Austausch vornehmen. Eine spätere Analyse ergab, dass „fehlerhafte Softwareprogrammierung für Schweißroboter" die Ursache war.
- **2017 –** Die Malware NotPetya verursachte einen geschätzten Schaden von 10 Mrd. USD und verursachte schwere Störungen bei Transportunternehmen wie Maersk und TNT. Wegen nicht funktionsfähiger Computer stellten Terminals und Verteilerzentren in einigen Fällen den Betrieb ein.

LOGIK EINES BEREITSTELLUNGSBEISPIELS: SEESCHIFFFAHRT



SYSTEMWEITE TRANSPARENZ

In Umgebungen des Transportwesens gibt es zahlreiche Systeme, die perfekt synchronisiert zusammenarbeiten müssen, um einen reibungslosen Betrieb zu gewährleisten. An Flughäfen beispielsweise verweilen Flugzeuge nach der Landung oftmals weniger als 90 Minuten. Damit der Abflug sicher und pünktlich erfolgt, ist ein Zusammenwirken von Teams und Systemen notwendig, um ein Gate zuzuweisen, Protokolle bei der Entladung, Bevorratung, Wartung sowie im Hinblick auf Treibstoff, Flugrouten, Wetter, Flugzeuggewicht und physische Sicherheit einzuhalten und andere kritische Abläufe auszuführen.

Die Systeme, die all das erst möglich machen, sind auf eine konvergente IT/OT-Infrastruktur angewiesen. Vollständige 360-Grad-Sichtbarkeit in der gesamten Infrastruktur stellt dabei sicher, dass keine sicherheitsrelevanten blinden Flecken vorliegen, die den Betrieb möglicherweise stören oder gänzlich zum Stillstand bringen können. Sichtbarkeit muss auf Netzwerkebene vorhanden sein, um fragwürdigen oder ungewöhnlichen Datenverkehr zu identifizieren, sowie auf Geräteebene, um sämtliche infizierten Geräte ausfindig zu machen – ob diese über das Netzwerk kommunizieren oder nicht. Da Angriffe sich zunächst in einem Bereich ereignen und dann schnell auf einen anderen Bereich ausbreiten können, sollte diese Sichtbarkeit sowohl für IT- als auch OT-Geräte bestehen.

SCHNELLERES SCHLIESSEN VON SCHWACHSTELLEN

Im Gegensatz zu herkömmlichen IT-Netzwerken oder Fertigungsstätten, die sich in der Regel in einem großen Komplex befinden, sind Verkehrs- und Transportnetze naturgemäß über ein großes Gebiet verteilt und quasi ständig in Bewegung. Reedereien betreiben beispielsweise Megaschiffe, die Tausende von Containern fassen können. Eine große Reederei muss in Echtzeit Rechenschaft über seine Flotte ablegen können, die möglicherweise auf dem gesamten Globus operiert. Dies gilt auch für die vielen Tausend Container und die Fracht jedes einzelnen Schiffs. Hierzu ist ein robustes OT-Netzwerk erforderlich.

Durch Asset-Verfolgung wird das OT-Bestandsverzeichnis stets auf aktuellem Stand gehalten und Warnmeldungen können auf unbefugte Aktivitäten und nicht erfasste Änderungen hinweisen. Die Echtzeit-Benachrichtigung bei sämtlichen Aktivitäten ist besonders wichtig – sowohl auf dem Seeweg als auch im Hafen. Aus diesem Grund muss Ihre OT-Sicherheitslösung regelmäßig einzelne Geräte abfragen, die den OT-Betrieb an sämtlichen Standorten aufrechterhalten, um eine genaue Lageerkennung zu gewährleisten und Änderungen zu ermitteln. Ihre OT-Lösung sollte alle SPS, HMIs, Server, Workstations, Netzwerkgeräte, Gateways und anderen operativen Geräte abfragen, die in der Schifffahrt zum Einsatz kommen.

Tenable.ot nutzt patentierte Technologien für aktive Abfragen und ist zudem die erste Lösung mit spezifischen Active Querying-Engines für Umgebungen im Transportwesen. Die Technologie setzt aktive Abfragen sowohl für dokumentierte als auch undokumentierte Protokolle ein, um eine möglichst genaue Lageerkennung zu ermöglichen und eine maximale Abdeckung aller Geräte in einer verteilten OT-Umgebung zu erzielen.

ABSICHERUNG DES VERTEILTEN ÖKOSYSTEMS

Multi-Detection Engines sind erforderlich, um Ereignisse in jeder Phase eines Angriffs identifizieren zu können. Diese sollten Folgendes beinhalten:

a) Angriffsvektoren, anhand derer Schwachpunkte proaktiv identifiziert werden können, bevor Bedrohungsakteure einen Angriff durchführen; Allgemeine Traffic-Zuordnung und Traffic-Visualisierung sowie Identifizierung von riskanten Protokollen, offenen Ports und Schwachstellen, um Risikofaktoren in Ihrer gesamten Infrastruktur zu beseitigen.

b) DPI-Engines für dokumentierte und proprietäre Protokolle, um Aktivitäten, die gegen festgelegte Regeln verstoßen, sowie Ereignisse der Auskundschaftung zu identifizieren. In der Regel stützt sich dies auf Richtlinien, die Schutz vor bekannten Angriffen bieten können.

c) Anomalie-Erkennung, um Zero-Day- oder gezielte Angriffe zu identifizieren, für die noch keine Signatur vorliegt. Dies sollte zur Ermittlung von Traffic-Mustern und Verhaltensweisen genutzt werden, die vom regulären, täglichen Betrieb abweichen.

d) Bei signaturbasierter Erkennung kommt eine Datenbank wie Suricata zum Einsatz. Als Open-Source-Datenbank ist sie deshalb wertvoll, weil die breitere Security-Community neue Signaturen hinzufügen kann, wovon auch die größere OT-Security-Community profitiert. Sie kann eingesetzt werden, um bekannte Bedrohungen zu identifizieren, die Angreifer zur Errichtung von Brückenköpfen oder zur Ausbreitung innerhalb der Transportinfrastruktur nutzen.

FORTWÄHRENDE DOKUMENTIERUNG

OT-Umgebungen enthalten häufig einen Mix aus älteren Geräten, die in IT-Umgebungen in der Regel nicht vorhanden sind. Da jeder Gerätetyp unterschiedliche Revisionsnummern aufweist, ist die Aufrechterhaltung eines stets aktuellen Patch-Management-Programms mit Schwierigkeiten verbunden. Umgebungen im Transportwesen können nicht einfach im Zuge regelmäßiger Wartungsfenster außer Betrieb genommen werden. Daher kann es sein, dass der Betrieb über einen längeren Zeitraum mit vorhandenen, bekannten Schwachstellen erfolgt. Wenn ein Wartungsfenster eingeplant ist und das Patching manuell erfolgt, kann es dennoch zu Versäumnissen und Fehlern kommen – vom damit verbundenen enormen Zeit- und Arbeitsaufwand ganz zu schweigen. Und möglicherweise richten Sie den Fokus dabei nicht einmal auf die Behebung der kritischsten Schwachstellen.

Es ist von entscheidender Bedeutung, dass der Zustand und sämtliche Merkmale all Ihrer Geräte genauestens bekannt sind. Dazu gehört auch, den spezifischen Zustand von Geräten exakt mit der verfügbaren Wissensdatenbank zu Schwachstellen abzugleichen, in der damit zusammenhängende Exploits aufgeführt sind. Aufgrund der dynamischen Beschaffenheit von Umgebungen im Transportwesen sollte Ihre OT-Lösung diese Informationen regelmäßig aktualisieren und mit neu aufgedeckten Schwachstellen abgleichen. Ein Vulnerability Priority Rating (VPR) kann Ihnen beispielsweise eine geordnete Liste von Schwachstellen liefern, mit denen sie sich – ausgehend vom höchsten bis zum niedrigsten Schweregrad – befassen sollten. Die Einordnung erfolgt basierend auf zahlreichen Kriterien, wie etwa der CVSS-Bewertung, der Asset-Kritikalität, der Position in Ihrer Umgebung und vielen weiteren Aspekten. Dadurch steht Ihnen eine automatisierte, vollständig geprüfte und nach Priorität geordnete Liste der Schwachstellen zur Verfügung, die Sie beheben sollten, um die für Ihre Umgebung spezifische und relevante Cyber Exposure zu senken.

ZUSAMMENFASSUNG

Inzwischen ist weithin bekannt, dass OT-Cybersecurity ein elementarer Bestandteil einer stets zuverlässigen, effizienten und sicheren Umgebung im Transportwesen ist. Lückenlose Transparenz, Sicherheit und Kontrolle über all Ihre operativen Assets sind zur Eindämmung von Risiken unverzichtbar.

Tenable.ot bietet vollständige Sichtbarkeit von IT- und OT-Assets. Durch die Asset-Bestandsaufnahme wird jedes einzelne Asset in Ihrer Umgebung identifiziert – in Kombination mit einer umfassenden Situationsanalyse bis hin zur Firmware- und Backplane-Ebene. Bei der aktiven Suche nach Bedrohungen kommen proaktive Angriffsvektoren zum Einsatz, mit deren Hilfe Schwachpunkte bereits identifiziert werden, bevor Bedrohungsakteure einen Angriff durchführen. Eine hybride Erkennungs-Engine identifiziert bekannte wie auch unbekannte Bedrohungen, sobald diese auftreten. Durch Schwachstellen-Management werden Schwachstellen mit bekannten Exploits priorisiert, die für Ihre spezifische Umgebung relevant sind. Bei Bedarf identifiziert die Konfigurationskontrolle zu Audit- und Rollback-Zwecken sämtliche Änderungen an Ihrer OT-Infrastruktur und erstellt entsprechende Snapshots. Die flexiblen Bereitstellungsoptionen von Tenable.ot und die Integration mit führenden IT-Sicherheitsanbietern sorgen dafür, dass Verkehrsinfrastrukturen sicher und mit geringerem Risiko betrieben werden.

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf **de.tenable.com**.