Sustainable Cyber Resilience im Transportsektor:

Transport, Verkehr und Logistik

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

09/2018

Management Summary

Der Schienen-, Straßen- und Schiffsverkehr sowie die Logistik zählen zu den kritischen Infrastrukturen und sind ein attraktives Ziel für Hacker. Um für angemessenen Schutz zu sorgen, reicht es nicht mehr aus, reaktive Maßnahmen zu ergreifen. Stattdessen müssen Unternehmen einen Zustand der Sustainable Cyber Resilience anstreben: der nachhaltigen Widerstandsfähigkeit. Dabei handelt es sich um ein umfassendes Konzept, das eher strategisch als technologisch ausgerichtet ist und einen Schritt weiter geht als IT Security. Sustainable Cyber Resilience sorgt zum einen dafür, Angriffsflächen zu verringern. Zum anderen stellt sie sicher, dass Unternehmen ihren Betrieb auch im Falle eines Angriffs aufrechterhalten und ihre angestrebten Geschäftsziele erreichen können – unter Berücksichtigung der Wirtschaftlichkeit. Dieses Whitepaper zeigt, warum Sustainable Cyber Resilience für den Transportsektor so wichtig ist, was sie bedeutet und wie sie sich mithilfe von Vulnerability Management umsetzen lässt.

Inhalte

Einleitung

Sustainable Cyber Resilience ist für Unternehmen aller Branchen wichtig. Unverzichtbar ist sie aber im Bereich der kritischen Infrastrukturen (KRITIS). Darunter fallen laut Definition der Bundesregierung „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." KRITIS-Organisationen müssen sich daher besonders gut gegen Cyber-Angriffe schützen – das schreibt der Gesetzgeber vor. Die EU begann bereits 2006 mit dem European Programme for Critical Infrastructure Protection (EPCIP) und erweiterte und ergänzte dieses in den folgenden Jahren. Mitgliedsstaaten setzen die EU-NIS Direktive in nationales Recht um, Deutschland beispielsweise mit dem IT-Sicherheitsgesetz (IT-SIG). Große Wirtschaftsnationen haben bereits Regulierungsinstanzen entwickelt. In den USA ist dies zum Beispiel das US National Institute of Standards and Technology und in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI).

In Deutschland sind die kritischen Infrastrukturen in 9 Sektoren eingeteilt. Einer davon ist Transport mit den Branchen Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr und Logistik. Funktionieren sie nicht mehr richtig, hat dies weitreichende Auswirkungen. Denn Mobilität bildet eine wichtige Voraussetzung für unsere moderne, arbeitsteilige Volkswirtschaft. Ist der Transport von Waren, Bauteilen oder Rohstoffen gestört, beeinträchtigt das zum Beispiel die Produktion und schadet damit der Wirtschaft. Dasselbe ist der Fall, wenn der öffentliche Nahverkehr ausfällt und Mitarbeiter nicht an ihren Arbeitsplatz kommen. Werden Lebensmittel nicht geliefert, haben wir zu wenig zu essen. Krankenhäuser sind auf den Transport von Medikamenten angewiesen. Mit einem Angriff auf Systeme im Transport- und Verkehrswesen können Cyberkriminelle also erheblichen Schaden anrichten.

Beispiele für Cyber-Attacken auf Transport-Infrastrukturen

In den vergangenen Jahren gab es bereits zahlreiche Vorfälle, bei denen Unternehmen aus dem Transportsektor Opfer von Cyber-Angriffen wurden. Meist handelte es sich dabei um Ransomware-Attacken, also Schadsoftware, die Systeme verschlüsselt und dadurch funktionsunfähig macht. Opfer werden zur Lösegeldzahlung aufgefordert, um die verschlüsselten Daten wieder freizukaufen. So befiel der Verschlüsselungstrojaner WannaCry im Mai 2017 unter anderem Rechner der Deutschen Bahn. Die Schadsoftware setzte die Anzeigetafeln auf zahlreichen Bahnhöfen außer Gefecht. Auch die Kameras für die Videoüberwachung und einige Fahrkartenautomaten fielen aus. Der Zugverkehr konnte glücklicherweise ungestört weiterlaufen. Es dauerte jedoch einige Tage, bis die Deutsche Bahn ihre Systeme wiederhergestellt hatte.

Nur wenig später trieb der Kryptotrojaner NotPetya weltweit sein Unwesen und infizierte unter anderem Systeme des dänischen Großkonzerns Maersk. Vor allem die Reederei Maersk Line, der Logistikdienstleister Damco und APM Terminals waren betroffen. In Folge des Angriffs standen Containerterminals still und Schiffe konnten weder beladen noch gelöscht werden. Nach eigenen Angaben erlitt der Maersk-Konzern dadurch einen Verlust von 200 bis 300 Millionen US-Dollar. Auch das Logistikunternehmen TNT-Express, eine niederländische Tochter von Fedex, wurde Opfer von NotPetya. Die Cyberattacke beeinträchtigte deren weltweites Geschäft, sodass dem Unternehmen laut Fedex ein Schaden von rund 300 Millionen US-Dollar entstand. Nach einer genauen Untersuchung der Malware gehen Sicherheitsexperten davon aus, dass NotPetya es weniger auf Erpressungsgeld abgesehen hatte, sondern vielmehr möglichst großen Datenverlust bei den Opfern verursachen wollte.

Bereits 2016 wurde die San Francisco Municipal Railway gehackt. Ticketautomaten zeigten die Meldung „Out of Service" oder „Metro Free". Auf den Bildschirmen an den Bahnhöfen erschien eine Meldung des Angreifers, in der er das Unternehmen aufforderte, Kontakt mit ihm aufzunehmen, um einen Deal auszuhandeln.

Für Furore sorgte auch ein Schülerstreich im polnischen Lodz, der schon zehn Jahre zurückliegt. Hier gelang es einem Teenager, eine herkömmliche TV-Fernbedienung so umzuprogrammieren, dass er damit Weichen im Trambahnnetz schalten konnte. Dadurch war der Schüler in der Lage, mit der Straßenbahn wie mit einer Modelleisenbahn zu spielen. Der Spaß hatte jedoch verheerende Folgen. Zwölf Menschen wurden bei einer Entgleisung verletzt.

IT-Systeme und Prozesse im Transportsektor

Unabhängig davon, was befördert wird (Menschen oder Güter), skizziert die Grafik unten den Verlauf eines Transports. Ohne die Erfassung (1) der notwendigen Daten (was soll zu welchem Zeitpunkt von wo nach wo transportiert werden) funktioniert keine Lieferkette. Fehlerhafte oder unvollständige Daten können auch beim Handling (2) schon zu einer falschen Zusammenstellung eines Pakets (Konfektionierung) führen. Auch vollautomatisierte Lager sind eine hochkritische Angriffsfläche. Die Beförderung (3) des Pakets, die Auswahl beziehungsweise die Kombination der Transportmittel, und der Übergang zwischen diesen ist ohne den Austausch von digitalen Informationen (EDI) nicht mehr denkbar. Ebenso ist die Abrechnung (4) und Dokumentation eines Transports gestützt auf IT-Systeme.

Im Transportsektor kommen heute eine Vielzahl von vernetzten Systemen, Geräten und Applikationen zum Einsatz. Um einen Zustand der Sustainable Cyber Resilience zu erreichen, müssen sie alle berücksichtigt werden, und zwar sowohl die Unternehmens-IT als auch die Operational Technology (OT). Zur Infrastruktur zählen zum Beispiel IT-Systeme zur Unternehmensadministration und zur Kundendatenverwaltung. Sie enthalten oft sensible Geschäftsgeheimnisse oder personenbezogene Daten, die unter die EU-DSGVO fallen. Dazu kommen Fahrkartenautomaten und IT-Systeme zur Mautabwicklung, ebenso wie Systeme zum Verkehrsmanagement, etwa der Zug- oder Bus-Kontrolle. Eine wichtige Rolle spielen auch Systeme zur Steuerung der Signalinfrastruktur wie Ampeln im Straßenverkehr oder Lichtzeichen an Gleisen. Würde ein Hacker sie manipulieren, könnte er für ein gravierendes Verkehrschaos sorgen und schlimme Unfälle verursachen. Züge und Busse sind zudem häufig mit Bildschirmen ausgestattet, auf denen Fahrgastinformationssysteme laufen. Nicht vergessen sollte man auch vernetzte Systeme der Gebäude-Technik wie Klimaanlagen oder Heizungen. Auch sie bieten einen Angriffspunkt.

Besondere Herausforderungen für Resilience im Transportsektor

Die Digitalisierung im Transportsektor schreitet zunehmend voran. Das führt dazu, dass immer mehr Systeme miteinander vernetzt sind und IT und OT zusammenwachsen. Doch mit jedem vernetzten Gerät vergrößert sich auch die Angriffsfläche. Schwachstellen in der Unternehmens-IT können sich jetzt auch auf die Funktionsfähigkeit von Zügen, Bussen, Trambahnen, Ampeln oder Stellwerken auswirken und umgekehrt. Gerade in Smart City-Konzepten mit einem hohen Vernetzungsgrad ist das Risiko groß, dass Hacker schon durch eine kleine Manipulation eine große Kettenreaktion auslösen können.

Abläufe im Transportwesen, IT-gestützt

Viele ICS-Systeme im Transportsektor haben heute Protokolle wie TCP/IP für die Internetkommunikation integriert und verfügen über Embedded-Versionen von MS Windows oder Linux. Das macht sie genauso angreifbar wie einen Bürocomputer. Außerdem ist es heute selbstverständlich, dass Geräte und Systeme aus IT und OT kontinuierlich Informationen austauschen. In manchen Fällen wird eine einzige Kommunikationsinfrastruktur sowohl für die Telefonie als auch für die Übertragung von Unternehmensdaten und von Kontrollsystem-Signalen verwendet. Dadurch würde ein Angriff auf diese Infrastruktur gleich alle drei Bereiche gefährden. Cyber-Attacken im Transportsektor könnten zum Beispiel ICS-Signale blockieren oder manipulieren. Sie könnten dadurch Alarmsignale ändern, die Funktionsfähigkeit von Equipment beeinträchtigen und im schlimmsten Fall Menschenleben gefährden.

Zudem muss Resilience im Transportsektor neben Security, also der technischen Absicherung der Systeme gegen Angreifer, auch Safety umfassen. Letztere bezeichnet die Sicherheit der physischen Assets, sodass Mitarbeiter oder Fahrgäste sich bei ihrem Betrieb nicht verletzen.

Vulnerability Management als wichtiger Baustein für Sustainable Cyber Resilience

Resilienz ist ein kontinuierlicher Prozess. Er verstärkt die Fähigkeiten eines Unternehmens, einer Attacke zu widerstehen, und versetzt es in die Lage, auch während eines Angriffes zu funktionieren. Um dies zu erreichen, ist es wichtig, die Angriffsfläche zu reduzieren und so die Basis zu stabilisieren. Das bedeutet, Schwachstellen zu identifizieren, die von einem Angreifer ausgenutzt werden könnten. Letztlich heißt es, dem Angreifer einen Schritt voraus zu sein.

Greenbones Schwachstellenmanagement funktioniert mit dem Greenbone Security Manager (GSM) und ist dafür gedacht, Resilience durch einen kontinuierlichen Prozess nachhaltig zu etablieren. Dieser besteht aus den folgenden, größtenteils automatisierten Schritten:

Prepare

Im ersten Schritt geht es darum, den Kontext zu IT-Sicherheits-Policies, Risikobewertungen, Unternehmensprozessen und unternehmenskritischen Systemen herzustellen. Was will ich wie und wie intensiv schützen? Wie viel Risiko bin ich bereit zuzulassen? In Konfigurationsrichtlinien legen die IT-Verantwortlichen fest, was im Rahmen der Sicherheitsvorgaben erlaubt ist. Diese Richtlinien können dann mit einer technischen Kontrolle im GSM verknüpft werden. Hinzu kommen Informationen rund um den Security Workflow und die Verantwortlichkeiten. Wer muss informiert sein? Wer entscheidet, ob eine Schwachstelle behoben werden soll oder darf? Wer behebt sie?

Identify

Jetzt folgt die Analyse der Ist-Situation. Ein Vulnerability Scan stellt fest, welche Schwachstellen die Infrastruktur aktuell aufweist und wo sie von Konfigurationsvorgaben abweicht. Dabei muss sichergestellt werden, dass die Datenbank mit den Schwachstelleninformationen auf dem neuesten Stand ist. Außerdem wird identifiziert, wo genau sich die Schwachstelle oder Abweichung von der Norm befindet, und hinterfragt, wie belastbar die gefundenen Ergebnisse sind. Das dient dazu, False Positives und False Negatives zu vermeiden. Greenbone hat dafür das Feature QoD „Quality of Detection“ eingebaut. Es nennt einen Prozentwert, mit welcher Wahrscheinlichkeit die Schwachstelle tatsächlich existiert.

Classify

Die gesammelten Informationen werden jetzt nach unterschiedlichen Kriterien eingeteilt, die das Unternehmen individuell festlegen kann – zum Beispiel wo ein System physikalisch steht, zu welcher Abteilung es gehört, in welchem Netzsegment es sich befindet und welche Funktion es im Unternehmen erfüllt. Diese Einteilung ist unabhängig von der Kritikalität der Schwachstelle. Classify macht nichts anderes, als die Funde anhand der vorhandenen Merkmale zu gruppieren. Wichtig hierbei ist, dass eine solche Gruppierung im Sinne der Automatisierung in Regeln abgebildet werden kann.

Prioritize

Jetzt wird priorisiert, was auf Basis der Ziele aus dem ersten Schritt „Prepare“ mit den gefundenen Schwachstellen aus dem Schritt „Identify“ anhand der Einteilungen von „Classify“ am wichtigsten und damit als Erstes zu tun ist. Welcher Fund hat die größte Auswirkung und muss zuerst bearbeitet werden?

Assign, Mitigate & Remediate

Die technischen Erkenntnisse müssen in einem Arbeitsprozess münden, der zur Schließung der Schwachstelle führt. Ein Vulnerability-Management-Prozess sollte regeln, wer wann welche Informationen zu entdeckten Schwachstellen bekommt, wer für welche Schritte verantwortlich ist und welche Mittel und Wege zur Verfügung stehen. Das Vulnerability-Management-System sollte hier so viele Informationen wie nur möglich mitliefern. Die Handlung kann auch über den Austausch mit anderen Workflow Tools initiiert werden, zum Beispiel einem ISMS, einem Ticket-System für Helpdesks oder einem SIEM-System zur weiteren Korrelation von Security Events beziehungsweise Incidents.

Store & Repeat, Improve

Die letzten Schritte dienen der Auditierbarkeit des Systems nach ISO 27000 sowie der Verbesserung, Veränderung und Anpassung. Store & Repeat protokolliert wichtige Informationen, zum Beispiel, wann eine Schwachstelle zum ersten Mal gefunden wurde, wann sie gemeldet wurde und wie lange es gedauert hat, sie zu beheben. Dies hilft bei der Analyse von Sicherheitsvorfällen. „Improve“ ist der Übergang zu einem erneuten Durchlauf des Vulnerability-Management-Prozesses, der wieder mit „Prepare“ beginnt. Jetzt können Sicherheitsverantwortliche die Zielsetzung verfeinern, verschärften oder an veränderte Policies anpassen. Schwachstellenmanagement ist kein statisches System, sondern ein dynamischer Prozess, bleibt aber immer automatisierbar.

Widerstandsfähigkeit durch den Schwachstellen-Management-Prozess

Grenzen von Vulnerability Management

Vulnerability Management ist ein wichtiger Baustein, um Sustainable Cyber Resilience zu erreichen. Es ist jedoch nur ein Element in einer umfassenden Gesamtarchitektur. Für nachhaltige Cyber Security und Widerstandsfähigkeit sind noch viele weitere Faktoren zu berücksichtigen, die ineinandergreifen müssen. Neben der Absicherung der Systeme gegen Hackerangriffe dürfen Unternehmen auch die physische Sicherheit nicht vernachlässigen. Zudem spielen organisatorische Maßnahmen eine wichtige Rolle. Unternehmen müssen genau festlegen und dokumentieren, wie Security-Prozesse aussehen und wer welche Aufgaben und Verantwortung übernimmt. Außerdem dürfen Unternehmen den Faktor Mensch nicht vergessen. Eine wichtige Präventionsmaßnahme sind nach wie vor Schulungen zur Sensibilisierung für IT-Risiken. Denn viele Mitarbeiter sind sich nicht bewusst, wie gefährlich Fehlverhalten oder Unachtsamkeit sein kann.

Nicht umsonst schreiben zahlreiche Richtlinien und Gesetze Schwachstellen-Scans und Risikobewertung vor. So erwartet zum Beispiel die EU-DSGVO ein implementiertes Schwachstellenmanagement. Auch für eine ISO 27001-Zertifzierung ist dies Voraussetzung. Die Fähigkeit, Schwachstellen zeitnah aufzufinden, zu priorisieren und zu beseitigen, ermöglicht es Unternehmen, ihre IT-Systeme kontinuierlich sicherer zu machen und die Angriffsfläche zu reduzieren. Das ist ein laufender Prozess, der nie abgeschlossen sein darf. Für Organisationen, die unter die KRITIS fallen, ist Vulnerability Management Pflicht.

Über Greenbone

Greenbone Networks wurde 2008 von Netzwerksicherheits- und Open-Source-Experten gegründet. Hauptsitz des international agierenden Privatunternehmens ist Osnabrück. Die Greenbone Security Manager (GSM) basieren auf Open Source Software. Sie analysieren IT-Netzwerke auf Schwachstellen und liefern Sicherheitsberichte sowie Hinweise zur Behebung, bevor Angreifer die Sicherheitslücken ausnutzen können. Bestandteil der Lösungen ist ein tägliches, automatisches Security Update. Es bündelt Prozeduren zur Erkennung von aktuellen Sicherheitsproblemen und überwacht Desktop-PCs, Server, Anwendungen und intelligente Komponenten wie etwa Router oder VoIP-Geräte. Die Greenbone-Lösung ist inzwischen eine wichtige Sicherheitskomponente in über 30.000 professionellen Installationen und Integrationen quer durch alle Branchen und Unternehmensgrößen. Die Greenbone Vulnerability Management Software wurde bereits mehr als 2,5 Millionen Mal heruntergeladen.

Weitere Informationen unter **greenbone.net**
Folgen Sie uns auf Twitter: **twitter.com/GreenboneNet**