axians

USE CASE

Tenable SecurityCenter

Zuverlässiger Nahverkehr braucht sichere IT-Infrastruktur.

Projektumfeld

Damit Bus, Bahn und Tram zuverlässig von A nach B kommen und die Kassensysteme funktionieren, ist im Hintergrund eine aufwändige IT-Infrastruktur erforderlich. Eine solche kritische Infrastruktur ist ein attraktives Ziel für Hacker, was eine effektive Absicherung zwingend voraussetzt. Viele Transportunternehmen wissen jedoch nicht, welche Schwachstellen ihre komplexe IT-Landschaft aufweist. Das dafür notwendige Wissen, welche Systeme und Dienste mit welcher Software und in welcher Konfiguration betrieben werden, kann von kleinen Sicherheitsteams meist nicht präzise und dauerhaft aktuell erfasst werden. So auch im Falle eines führenden deutschen Nahverkehrsanbieters. Das Unternehmen verfügt über mehrere Tausend Mitarbeiter, betreibt Lokomotiven, Triebwagen, Reisezugwagen, Straßenbahnen und Busse und hat bundesweit zahlreiche Tochterunternehmen. Mit der Einführung eines Schwachstellen-Managements wollte man die vielseitige IT-Infrastruktur nun transparenter und sicherer machen.

Projektanforderungen & Projektziele

Ausgangssituation war eine heterogene IT-Umgebung mit verschiedenen Servern, Clients und Kassensystemen, auf denen eine Vielzahl an Betriebssystemen und Software-Lösungen im Einsatz waren. Auch unterschiedliche Patch-Stände boten viel Angriffsfläche. Für das kleine Security-Team des Nahverkehrsanbieters stellte die manuelle Überwachung des komplexen Systems einen großen Aufwand dar, daher fehlte ein detaillierter Überblick über die IT-Infrastruktur und den Sicherheitsstand der einzelnen Assets. Zudem erschwerte die mangelnde Transparenz die Integration neuer IT-Systeme, beispielsweise bei der Eingliederung von Tochterunternehmen. Im ersten Schritt sollte deshalb eine automatisierte Inventurliste angelegt werden. Darauf aufbauend wollte man den Sicherheitsstatus der Systeme überprüfen, um Informationen über mögliche Schwachstellen zu gewinnen und sie zielgerichtet zu beheben. Bisher fehlte eine Lösung, die effiziente Prozesse sowohl für die Inventarisierung als auch für ein durchgängiges Patch-Management ermöglicht.

Umsetzung

Der Nahverkehrsanbieter wurde bereits seit vielen Jahren von seinem Trusted Partner für IT-Sicherheit, der Axians IT Security, beraten und wandte sich deshalb an deren Experten. Nach einer kurzen Evaluierungsphase entschied man sich für die Lösung „SecurityCenter“ des Herstellers Tenable. Der Schwachstellen-Scanner bietet sowohl eine Inventarisierungsmöglichkeit als auch ein umfangreiches Vulnerability Management. Außerdem konnte er durch Funktionsvielfalt sowie flexibel an Kundenbedürfnisse anpassbares Reporting punkten. Da Axians be-

NUTZEN

- Mehr Transparenz – Detaillierter Überblick über die IT-Landschaft und potenzielle Schwachstellen
- 99 % der Sicherheitsvorfälle können vermieden werden
- Schnellere Reaktionszeiten, da nur noch vereinzelte Sicherheitsvorfälle auftreten, können Security-Verantwortliche schneller handeln

Tenable Security Center

reits über fundierte Erfahrung mit dieser Plattform in vielen anderen Projekten verfügte und sich durch tiefes Expertenwissen auszeichnete, war ein gemeinsamer Proof of Concept schnell beschlossene Sache.

Zunächst ging es darum, den Aufbau der IT-Infrastruktur zu analysieren und die Scan-Zonen zu identifizieren. Darauf basierend hat Axians die Architektur ausgearbeitet und das Security Center bereitgestellt. Auf technischer Seite benötigte der Nahverkehrsanbieter für die Analyse-Plattform lediglich eine mittelgroße virtuelle Maschine in einer sicheren Zone. Neben den üblichen stationären Scannern in den wichtigsten Netzen führten die Security-Experten Axians IT Security einen zusätzlichen mobilen Scanner auf einem Laptop ein, welcher die verbleibenden Netze analysieren kann. Während der gesamten Umsetzungsphase wurde der Kunde fachkundig in die neue Lösung eingeführt und profitierte vom umfassenden Know-how der Berater. Nach sechs Arbeitstagen vor Ort war das Projekt abgeschlossen.

Projektergebnis

Seit Mitte 2016 hat der Nahverkehrsanbieter Tenable SecurityCenter erfolgreich im Einsatz. Der Schwachstellen-Scanner zeigt genau, welche Software wo im Unternehmen im Einsatz ist und auf welchem Stand sie ist. Er vergleicht dies mit dem maximal Möglichen und identifiziert eventuelle Sicherheitslücken. Dadurch wird für die Security-Verantwortlichen klar, welches die kritischsten Punkte sind und worauf sie ihre Aufmerksamkeit konzentrieren müssen. So sparen sie sich viel Aufwand. Das proaktive Vulnerability Management schützt effektiv gegen Angriffe, die mit automatisierten Tools ausgeführt werden, um bekannte Schwachstellen auszunutzen. Diese machen einen Großteil der üblichen Attacken aus. Da dadurch so gut wie keine Sicherheitsvorfälle mehr auftreten, kann das Security-Team schnell auf die wenigen Einzelfälle eingehen. „Entscheidend ist immer, dass der Angreifer im Vergleich zu seinen Erfolgsaussichten einen viel zu hohen Aufwand hat. Mit unserer Lösung haben wir ihm die einfachen Wege abgeschnitten“, sagt Sebastian Haas, IT-Consultant bei Axians IT Security.

Derzeit nutzt der Nahverkehrsanbieter nur einen Teil der Möglichkeiten, die das Tenable Security-Center bietet. Axians kann die Lösung jederzeit individuell an die künftigen Kundenbedürfnisse anpassen. So ist im nächsten Schritt auch eine passive Netzwerküberwachung möglich oder die Einbeziehung mobiler Geräte, die das Unternehmen verlassen. Neben Schwachstellen kann das Security Center auch Compliance-Verstöße erfassen. Vordefinierte Regelwerke für beispielsweise BSI Grundschutz oder ISO27000 liefert das Security Center dabei von Haus aus mit. Darüber hinaus können aber auch eigene Unternehmensrichtlinien abgebildet und anschließend kontinuierlich überwacht werden.

ÜBER AXIANS IT SECURITY

Die Axians IT Security ist ein dynamisch wachsendes Unternehmen mit Hauptsitz in Hamburg und einer der Marktführer im deutschen IT-Security-Markt. Das Portfolio der Axians IT Security beinhaltet alle Bausteine für die sichere elektronische Datenkommunikation und zum Schutz vor Datendiebstahl, Datenverlust und Datenmanipulation. Als Trusted Advisor unterstützt das Unternehmen Kunden aus allen Branchen und jeglicher Größe bei Integration, Betrieb und Support von Sicherheitslösungen. Dafür kooperiert Axians IT Security eng mit allen führenden Herstellern wie Check Point, Blue Coat, F5, Cisco, Fortinet und Tenable.

ANSPRECHPARTNER

Intern: Till Kahnwald (Vertrieb Security, Axians) · E-Mail: info-itsecurity@axians.de · Tel.: +49 40 271661-0

axians.de

Stand 02/17