Next-Generation Firewall im Härtetest: SBB setzt auf exklusives Sicherheitstesting durch Emitec

Ausgangslage des Projektes

Mit der Evaluation einer Next-Generation Firewall (NGFW) will die SBB sicherstellen, dass höchste Anforderungen an Sicherheit und Verfügbarkeit erfüllt werden. Die Next-Generation Firewall ist in der Lage, ausgeklügelte Angriffe zu erkennen und zu blockieren, indem sie Sicherheitsrichtlinien auf Anwendungs-, Port- und Protokollebene durchsetzt. Die Fälle von Cyber-Angriffen häufen sich und werden immer ausgeklügelter. In punkto Sicherheit dürften keine Kompromisse gemacht werden, wurde uns seitens der SBB mitgeteilt. Denn IT bewegt die Bahn: Sie spielt eine zentrale Rolle im Bahnbetrieb. Das breite Leistungsspektrum der SBB verdeutlicht dies. Es reicht von der Entwicklung und Bereitstellung des SBB-Internetportals über ein europaweit führendes Vertriebssystem bis zur Steuerung der Ticketautomaten in den Bahnhöfen.

Security Assessments für Firewalls

Im Rahmen einer Evaluation und Beschaffung hat die SBB verschiedene Angebote für eine NGFW-Lösung bewertet. Für die SBB ist es wichtig, dass die am besten passende Lösung für sie eruiert wird. Das bedeutet optimalen Schutz zum besten Preis. Firewalls dürfen nicht auf Basis eines Daten-blatts selektioniert werden. Deshalb definierte die SBB gemeinsam mit Emitec ein Test-Setup, das ein vergleichbares Testverfahren sicherstellt. Dabei werden folgende Ziele bestimmt:

- Optimale NGFW evaluieren (Sicherheit/Pricing)
- Passende Konfiguration (CPU/Memory) pro Standort finden
- Optimale Konfiguration für den Betrieb bestimmen
- Limite finden, bis welcher der Schutz optimal funktioniert

Das Test-Setup wurde zusammen mit den Praxistests von der Emitec AG begleitet und im Netzwerk-Labor der SBB durchgeführt. «Solche Art von Tests können nur mit einem BreakingPoint Traffic-Simu-lator unter realistischen Bedingungen im Labor angewendet werden», erklärt Armin Diethelm, CEO von Emitec.

Funktionsweise und Architektur

Zur Vorbereitung wurde ein typisches Traffic-Profil vom SBB-Netz übernommen. Damit konnte die NGFW mit dem möglichst gleichen Traffic wie später im Betrieb getestet werden. Die potenziellen Firewalls wurden im Zwei-Arm-Verfahren getestet, wobei der BreakingPoint-Simulator auf der einen Seite die Clients und auf der anderen die Server/Cloud's emuliert - eine sogenannte Zangen-Messung.

«Die BreakingPoint bietet als einziger Simulator im Markt die Möglichkeit, echten, realistischen Traffic zu simulieren», erklärt Armin Diethelm. Bei anderen oder ähnlichen Simulatoren erkennen die FW's (Security Devices), dass es sich um synthetisch generierten Traffic handelt. Sie analysieren nicht mehr jedes Paket, sondern nur noch jedes 100ste oder 1000ste, was zu falschen Resultaten und somit zu falscher Sicherheit führt.

BreakingPoint verfügt über ein patentiertes Verfahren zur Erzeugung von «realistischem» Traffic. Parallel dazu können Attacken und Exploits eingefügt werden.

Klare Messergebnisse bei der Evaluation

Durch den Einsatz der BreakingPoint-Plattform konnte die Telecomabteilung der SBB sicherstellen, dass die Ergebnisse der Firewall-Tests untereinander vergleichbar sind. Noch vor Beginn der Tests wurde anhand der verschiedenen Applikationsprofile der BreakingPoint-Plattform ein individueller Traffic-Mix zusammengestellt. Damit konnte gewährleistet werden, dass der im Labor simulierte Traffic ein möglichst genaues Bild des SBB-Netzwerks wiedergibt. Anhand der umfangreichen Tests schon während der Evaluationsphase erhielt die SBB eine klare Vorstellung der künftigen Next-Generation Firewall-Lösung. Zudem konnte durch die Verwendung eines SBB-Traffic-Mix aufgezeigt werden, dass auch Spezialfälle innerhalb des SBB-Netzwerks durch die neue Lösung optimal abgedeckt werden können. Das Risiko von teuren Workarounds während der Implementierung konnte dadurch verhindert werden.

Emitec Datacom | Birkenstrasse 47 | 6343 Rotkreuz | Tel: +41 41 748 60 10 | Mail: info@emitec.ch

emitec
datacom

Sicherheit durch Testen – auch im Alltag

Im täglichen Betrieb leistet die BreakingPoint-Plattform ebenfalls wertvolle Dienste für die SBB. «So können beispielsweise Updates in der Netzwerkinfrastruktur oder Konfigurationsänderungen vor-gängig im Labor getestet werden – auch dies unter realen Bedingungen», erläutert Armin Diethelm.

Auf der BreakingPoint-Plattform stehen über 65'000 Angriffsmuster zur Verfügung, unter anderem Virensignaturen und Exploits. Keysight stellt zudem laufend neue Angriffsmuster und «Evasion-Profi-les» bereit. Anhand von regelmässigen Tests kann die SBB somit mögliche Sicherheitslücken in der Infrastruktur frühzeitig erkennen – bevor dies andere tun.

Fazit des SBB Projektes

Dank exklusiven Tests konnte die SBB die optimale Next-Generation Firewall evaluieren, welche alle ihre Bedürfnisse vollumfänglich abdeckt. Dies zu einem Minimum an Kosten und ohne die Sicher-heit zu gefährden. Die Telecom der SBB bestätigt, dass sie dank dem Testverfahren bereits in der Evaluationsphase feststellen konnte, wo das jeweilige Limit liegt.

Nutzen auch Sie das volle Potenzial Ihrer IT-Sicherheit

Die erfolgreiche Zusammenarbeit zwischen der SBB und Emitec zeigt, wie entscheidend maßgeschneiderte Testverfahren in der Evaluationsphase einer Sicherheitslösung sind. Sie profitieren von einem exklusiven Test-Setup, das Ihnen ermöglicht, potenzielle Risiken frühzeitig zu erkennen und die ideale Next-Generation Firewall für Ihre spezifischen Anforderungen auszuwählen. Unsere Expertise hilft Ihnen, die beste Lösung zu finden – effizient, sicher und kostengünstig. Warten Sie nicht, bis Schwachstellen im laufenden Betrieb zu teuren Problemen werden. Kontaktieren Sie uns noch heute, um Ihre IT-Sicherheit auf das nächste Level zu heben!

Weiteren News und Case Studies

Bleiben Sie immer auf dem neuesten Stand der IT-Security! Besuchen Sie unseren Wissensblog auf unserer Webseite für tiefgehende Einblicke in aktuelle Projekte, innovative Lösungen und Best Practices. Oder folgen Sie uns auf LinkedIn, um regelmässig Updates zu erhalten und keine wertvollen Informationen zu verpassen.

LinkedIn

Haben Sie Fragen zu IT-Security Limit Tests?

Armin Diethelm steht Ihnen gerne zur Verfügung. Wenn Sie ein eigenes Projekt zur Evaluierung oder zum Testing einer Next-Generation Firewall planen, sprechen Sie uns an – wir unterstützen Sie gerne bei jedem Schritt!

Tel: +41 41 748 60 10

Mail: a.diethelm@emitec.ch