KUNDENPROFIL
JUNGFRAUBAHNEN

Jungfraubahn-Gruppe verbessert die Cyberabwehr auf Endgeräten

Branche
Tourismus

Herausforderung
Erhöhung der Sicherheit bei allen Endgeräten, um Malware und Exploits abzuwehren sowie die Verfügbarkeit von Anwendungen zu verbessern

Lösung
Palo Alto Networks Traps™ für die Endpoint-Sicherheit

Ergebnisse

- Geringere Angriffsfläche durch sicherere Endpunkte
- Transparenz der Bedrohungslage
- Schutz der PCs, Notebooks und Smartphones von knapp 600 Mitarbeitenden
- Installation innerhalb von drei Tagen durch Omicron
- Keine Neuaufsetzen von Systemen mehr notwendig

Zum Höhepunkt jeder Reise in die Schweiz zählt das Jungfraujoch. Im Jahr 2017 reisten sagenhafte 1.041.500 Gäste zum „Top of Europe“. Auf 3454 Meter über dem Meer liegt hier der höchste Bahnhof Europas und wird durch die Bahn von der Jungfraubahn-Gruppe bedient. Ausserdem bietet sie Ausflüge zu den bekannten Erlebnisbergen der Jungfrau Region und ein grosses Wintersportangebot. Ferner betreibt sie ein eigenes Wasserkraftwerk, vermietet Räumlichkeiten für Lokalitäten und Shops. „Jungfrau – Top of Europe“ ist eine Allianz zwischen der Jungfraubahn Holding AG und der Berner Oberland-Bahnen AG. Für die Gesellschaften der beiden Unternehmen stellt die Jungfraubahnen Management AG Dienstleistungen in den Bereichen Marketing, Finanzen, HR, Infrastruktur und Corporates Services mit 78 Mitarbeitenden bereit. Das fünfköpfige IT-Team koordiniert und erbringt Leistungen von Verkabelung, Netzwerk, Client und Server für die ganze Bahngruppe.

Zur Abdeckung der Kommunikationsbedürfnisse ist das physische Netzwerk in verschiedene virtuelle, private Netze aufgeteilt. Die IT stellt die Anwendungen auf rund 400 PC- und Notebook-Arbeitsplätze sowie 225 Smartphones – Tendenz steigend – zur Verfügung.

„Die Bedrohungslage durch Malware hat sich für unsere Clients in den vergangenen Jahren deutlich erhöht. Durch unsere vielschichtigen Arbeitsfelder gehört bei unseren Mitarbeitenden auch der Einsatz von USB-Sticks, CDs und externen Festplatten zur Tagesordnung. Deshalb wurde eine passende Endpoint-Protection auf Dauer unabdingbar“, sagt Urs Siegenthaler, Chief Information Officer (CIO) der Jungfraubahn-Gruppe. „Das Risiko längerer Ausfälle unserer zentralen Infrastrukturen oder unserer Webplattformen, über die wir einen stetig wachsenden Teil unseres Kundengeschäfts abwickeln, können und wollen wir uns nicht erlauben.“

„Traps™ erkennt Schadsoftware zuverlässig. Wir mussten seit dem Start von Traps™ wegen Schadsoftware keine Systeme mehr neu aufsetzen“, so der CIO. „Ich bin überzeugt, dass wir ohne Traps™ in der Zwischenzeit bereits weitere Ausfälle gehabt hätten.“

Urs Siegenthaler | Chief Information Officer (CIO) | Jungfraubahn-Gruppe

Als dann die Ransomware WannaCry auch bei der Jungfraubahn-Gruppe für eine Infizierung sorgte, war dies für Siegenthaler der Anlass, schnell zu handeln. „Wir hatten schon länger Traps™ von Palo Alto Networks als hochentwickelten Schutz für die Endgeräte-Sicherheit in der engeren Auswahl. Palo Alto Networks hat in der Branche einen guten Ruf, ist innovativ und setzt die Messlatte für Mitbewerber auf ein hohes Niveau. Bei der Traps™ Roadshow des Schweizer IT-Security-Spezialisten Omicron hatte ich mich gründlich darüber informiert, sodass wir beim WannaCry-Angriff schnell handeln konnten“, erinnert sich der CIO. Omicron erhielt den Auftrag und agierte schnell und flexibel. „Wir konnten innerhalb von nur drei Tagen die Installation des zentralen Traps-Servers sowie die Installation auf rund 450 Windows-Clients und 100 Windows-Server durchführen“, freut sich Siegenthaler.

Omicron nutzte dabei die vom Traps™ Endpoint Security Manager zur Verfügung gestellte Wildfire Inspection Cloud-Technologie, um unbekannte Bedrohungen auf den Servern und Endgeräten zu identifizieren.

Traps™ ersetzt herkömmliche Antivirensoftware durch einen multimethodischen Schutzansatz: Um vor bekannter und unbekannter Malware zu schützen, werden statische Analysen durch maschinelles Lernen und mit Hilfe von WildFire Inspektionen und Analysen, Beschränkungen für vertrauenswürdige Anbieter sowie richtlinienbasierte Ausführungsbeschränkungen und Verwaltungsregeln vereint. Zum Schutz vor Exploits konzentriert sich Traps™ auf die Kerntechniken solcher Exploit-basierten Angriffe und nicht auf die Millionen individueller Attacken oder deren eigentlichen Sicherheitslücken. Traps™ stoppt solche Exploit Angriffe und blockiert diese Techniken von Beginn an.

Transparenter Überblick über alle Sicherheitsvorfälle

„Ich bin von Traps™ und vom Integrationspartner Omicron stark beeindruckt“, betont Siegenthaler. Seit der Installation läuft Traps™ bei der Jungfraubahn-Gruppe sehr stabil und hat negative Auswirkungen von Exploits sowie Malware auf allen Endgeräten wirksam verhindert. „Traps™ erkennt Schadsoftware zuverlässig. Wir mussten seit der Einführung von Traps™ keine Systeme mehr neu aufsetzen“, so der CIO. „Ich bin überzeugt, dass wir ohne Traps™ in der Zwischenzeit bereits weitere Ausfälle gehabt hätten.“

Urs Siegenthaler schätzt, dass sein Team durch Traps™ im Jahr zwischen 10 und 20 Arbeitstage an Installations- und Wiederherstellungsaufwand einspart. Hinzu kommen indirekte Kosten für Datenverlust und zusätzlichen Arbeitsaufwand. „Durch die zentrale Konsole des Traps™ Endpoint Security Managers haben wir einen transparenten Überblick über den Stand der Software und die Sicherheitsvorfälle“, erzählt er weiter.

Derzeit hat die Jungfraubahn-Gruppe noch eine weitere Lösung für die Endpoint-Sicherheit im Einsatz, die dank Traps™ aber schon bald abgeschaltet werden soll. Siegenthaler ergänzt: „Wir benötigen jetzt keinen zusätzlichen Viren-Schutz mehr, da Traps™ durch die Quarantäne-Funktion diese Eigenschaft miterfüllt und zudem deutlich besser schützt.“