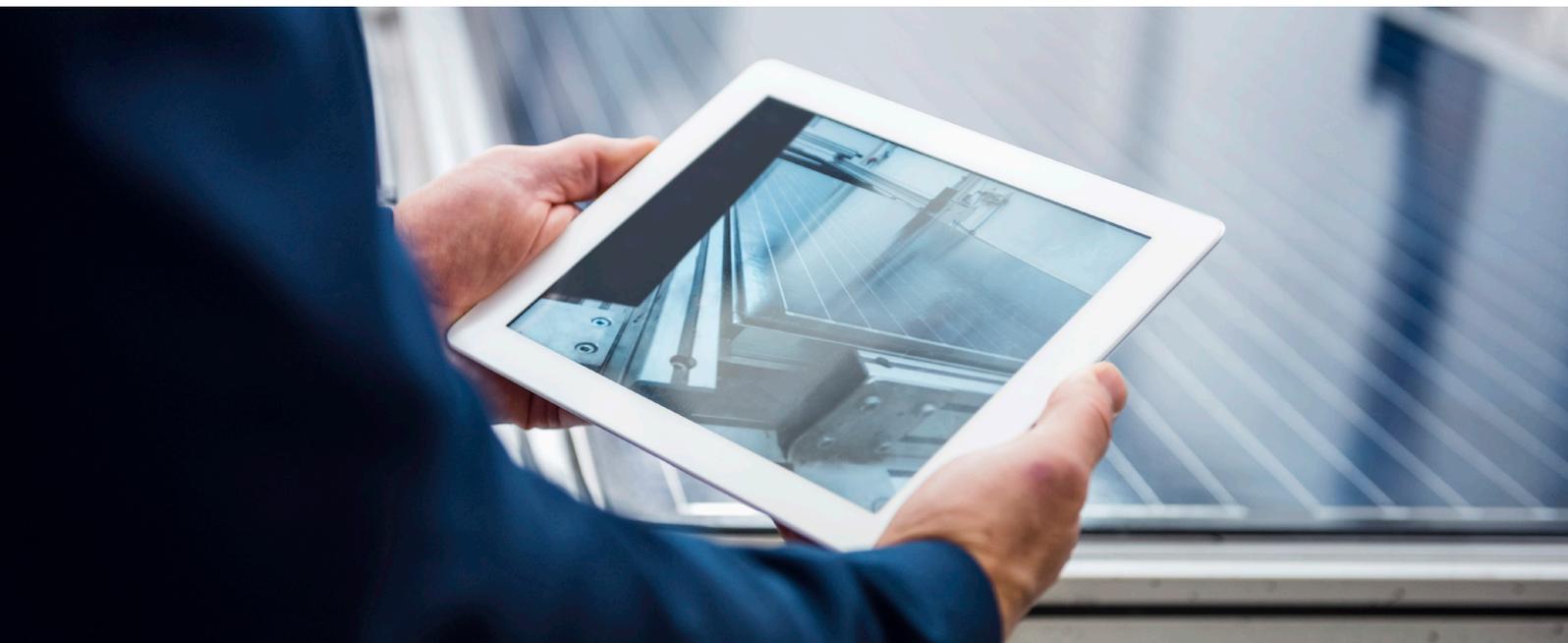


Kundenreferenz

Durchblick im Netzwerk für die Grazer Wechselseitige

Schnelle Implementierung und erhöhte Transparenz im Netzwerk



Auf einen Blick

Kunde:

Grazer Wechselseitige
Versicherung AG

Branche:

Versicherungswesen

Firmensitz: Graz, Österreich

Leistungen:

- Network Detection & Response

Das Unternehmen

Die Grazer Wechselseitige Versicherung AG (kurz: GRAWE) hat sich seit ihrer Gründung im Jahr 1828 von der ursprünglichen Feuerversicherung zu einem internationalen Konzern entwickelt und Versicherungen, Immobilien und Finanzdienstleistungen unter einem Dach vereint.

Der österreichische Versicherungskonzern mit Sitz in Graz und Niederlassungen in 13 zentral-, ost- und südosteuropäischen Staaten zählt mit über 500.000 Kunden allein in Österreich zu den Top Versicherungsunternehmen auf der Welt. Die GRAWE steht mit einer über 190-jährigen Tradition für Verlässlichkeit und Stabilität, für Sicherheit und Unabhängigkeit.

Ausgangssituation

Dieses Credo will das Unternehmen auch hinsichtlich der IT-Security weiterführen. Trotz zahlreicher implementierter Security-Lösungen, wurden im Rahmen mehrerer Penetrationstests, sogenannte „Blind Spots“ im Netzwerk entdeckt.



GRAZER WECHSELSEITIGE
Versicherung Aktiengesellschaft

Bisher war es der GRAWE nicht möglich, Anomalien und unübliche Datenströme im Netzwerk zu erkennen, und adäquat auf auffällige Verhaltensmuster zu reagieren.

Anforderungen

Die GRAWE suchte nach einer Lösung, die Transparenz und Visibilität im Netzwerk signifikant erhöht und gleichzeitig die komplexe Infrastruktur möglichst einfach und übersichtlich darstellen kann. Durch diese Faktoren sollten auffällige Netzwerk-Anomalien erkannt, sowie unentdeckte Angriffe aufgedeckt werden.

Neben der Einhaltung rechtlicher Rahmenbedingungen war eine grundsätzliche Anforderung der GRAWE, dass neue Security-Tools einen möglichst geringen operativen Aufwand erzeugen, der vom bestehenden Security-Team abgedeckt werden kann. Unterstützung statt Überlastung war hier gefragt.



Entscheidungsmatrix

Um eine maßgeschneiderte Lösung für dieses Problem ausarbeiten zu können, wurde zunächst mit Hilfe einer Entscheidungsmatrix festgestellt, welche Lösung die Anforderungen erfüllen und die vorhandenen Probleme lösen kann. Unter anderem wurden hierbei die Möglichkeiten zur Integration in das Netzwerk und die virtuellen Umgebungen miteinbezogen, ebenso wie die Optionen zur Einbindung in Syslog und AD-Authentifizierung. Weitere Kriterien waren außerdem Berechtigungskonzepte, Transparenz & Komplexitätsgrad der Alarme, sowie eine möglichst einfache Anbindung in die bestehende Infrastruktur. Die Cognito® Plattform von Vectra Networks® erschien nach eingehender Analyse der Entscheidungsmatrix als effizientestes Produkt und stellte aufgrund der langjährigen Partnerschaft mit Orange Cyberdefense die beste Lösung dar, um die Anforderungen der GRAWE abzudecken.

Durchführung

In einem begleiteten Proof-of-Concept (PoC) trat der Mehrwert deutlich zu Tage und man erkannte bereits während der Anlernphase erste kritische Punkte in der bestehenden Infrastruktur.



Orange Cyberdefense konnte mit Vectra Networks® die Anforderungen der GRAWE bestens erfüllen und die „Blind Spots“ im Netzwerk aufdecken. Die Lösung punktet mit einem klar und intuitiv strukturierten Dashboard, das Anomalien und auffällige Verhaltensmuster im Netzwerk erfasst und eine schnelle Identifizierung betroffener Systeme sicherstellt.

Der Netzwerkverkehr wird strukturiert und vollständig analysiert und somit können die Alarme organisiert aufbereitet werden. Dieses zielgerichtete Monitoring gibt viele Einblicke in das Verhalten von Netzwerkkomponenten. Des Weiteren ist die Lösung eine effiziente Ergänzung zur bestehenden Security-Umgebung und konnte vom GRAWE Security-Team ohne zusätzlichen Personal- und Schulungsaufwand betreut werden.

Fazit

Durch eine reibungslose Durchführung wurde die Lösung nach erfolgreichem PoC in die Produktion überführt. Die Anforderungen der GRAWE an schnelle und nahtlose Implementierung wurden vollständig erfüllt. Durch komplette Visibilität und automatisierte Auswertung durch Vectra konnten Blind Spots im Netzwerk komplett eliminiert werden.

Vorteile

- Visibilität
- Schnellere Erkennung versteckter Angriffe
- Effiziente Unterstützung bestehender Prozessabläufe
- Geringer Schulungsaufwand
- Schnelle und einfache Implementierung
- Kein zusätzliches Know-How im Security-Team erforderlich

Über Orange Cyberdefense

Orange Cyberdefense ist eine Geschäftseinheit der Orange Group, welche sich der Cybersecurity widmet. Als Europas führender Anbieter für Cybersecurity ist unser Bestreben eine sichere digitale Gesellschaft aufzubauen. Wir bieten unseren Kunden Consulting, Solutions und Managed Security Services. Speziell mit unseren Managed Detection & Response und Threat Intelligence Services helfen wir unseren Kunden Bedrohungen zu erkennen, Risiken zu identifizieren und auf Vorfälle angemessen zu reagieren. Mit über 2.100 Mitarbeitern in weltweit 19 Ländern sind wir stets dort, wo unsere Kunden uns brauchen. Erfahren Sie mehr auf unserer Website.

