

e x e o n

Smart Cyber Security.

Planzer – eine ExeonTrace NDR Case Study

ExeonTrace sichert

Planzers dezentrales Netzwerk





Planzer Management: Nils Planzer, Nicolas Baer und Severin Baer, v.l.n.r.



Auf einen Blick

Branche: Logistik und Transporte

Ergebnisse:

- Sichtbarkeit der weit verteilten IT-Infrastruktur
- Rein softwarebasiert – Einsatz innerhalb weniger Tage und ohne zusätzliche Hardware
- Laufende Überwachung von Vorfällen – innerhalb weniger Tage einsatzbereit
- Hochgradig geschützte Altsysteme

Herausforderungen:

- Dezentrales Netzwerk mit über 70 verschiedenen Standorten weltweit
- Ausfälle würden weitreichende betriebliche und finanzielle Schäden haben
- Historische Protokolldaten werden benötigt, um mögliche Vorfälle zu lokalisieren
- Altsysteme, die gesichert werden müssen

— Business Hintergrund

Mit mehr als 5'000 Mitarbeitern weltweit und einem Umsatz von fast 1 Mia. CHF ist Planzer ein führendes Schweizer Logistikunternehmen.

Planzer betreibt 1'900 Fahrzeuge an 70 Standorten unter anderem in der Schweiz, Italien, Frankreich, Deutschland und Hongkong.

Die familiengeführte Planzer-Gruppe transportiert Waren und Pakete auf Strassen und Schienen im In- und Ausland. Darüber hinaus bietet Planzer auch lagerlogistische Dienstleistungen für nationale und globale Kunden an.



PLANZER

An abstract graphic in the bottom-left corner consisting of a dense, tangled mass of thin, wavy lines in various colors including red, orange, yellow, and green. The lines appear to flow and curve, creating a sense of movement and complexity.

“Als CEO & Inhaber einer eng getakteten Logistikfirma kann ich mir Systemausfälle wegen Cybervorfällen nicht leisten. Mit ExeonTrace haben wir bei Planzer eine Schweizer Lösung gefunden, um unser Netzwerk zu überwachen und Cyberbedrohungen frühzeitig zu erkennen.”

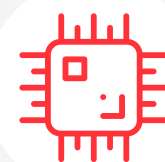
Nils Planzer

CEO & Inhaber Planzer

— Herausforderungen



Das Tagesgeschäft von Planzer hängt in hohem Masse von digitalen Systemen ab, Ausfallzeiten haben schwerwiegende Konsequenzen. Ausserdem hat der Maersk-Cyberangriff im Jahr 2017 gezeigt, dass die Branche eine Cyberabwehr braucht, die Alarm schlägt, bevor der Schaden entsteht.



Da Planzer an 70 Standorten tätig ist, war der geringe Einrichtungsaufwand ohne zusätzliche Hardware an jedem Standort eine Voraussetzung.



Das Sicherheitsteam von Planzer suchte nach einer Lösung, mit der es einfach durch die Log-Daten navigieren kann, um im Falle eines Sicherheitsvorfalls oder -problems die historischen Daten in die Analyse einbeziehen können.



Ausserdem wollte Planzer kritische Altsysteme absichern, die für den täglichen Geschäftsbetrieb unerlässlich sind, aber besonders anfällig für Angriffe sind, da sie nicht mehr aktualisiert werden können.

— Lösungen



Komplette Visibilität:

Durch die Integration von ExonTrace können alle Standorte und Netzwerke von Planzer überwacht werden. Mit dem Algorithmus-gesteuerten Threat Scoring wird das Netzwerk ständig überwacht und fortgeschrittene Angriffe werden sofort durch einen Alarm gemeldet.



Software-basiert:

ExeonTrace-Software wird als VM in der Azure-Cloud des Kunden bereitgestellt.



Intelligentes Datenhandling:

Sammlung von Flow-Daten (NetFlow) von 70 Standorten, die über die ganze Welt verteilt sind. Daten werden von den bestehenden Firewalls des Kunden exportiert. Durch die Verwendung von NetFlow-Daten, ist die zur Analyse benötigte Bandbreite sehr leichtgewichtig und reduziert.



Schnelles Aufsetzen:

Das Einrichten der Lösung und die Herstellung der Sichtbarkeit über 70 Standorte dauerte nur einen einzigen Tag. Die anschliessende Konfiguration und Feinabstimmung der Lösung mit dem Kunden dauerte insgesamt etwa eine Woche.

Vorteile



Einzigartig: ExeonTrace ermöglicht es dem Kunden, die Netzwerkaktivitäten aller 70 Standorte zentral zu überwachen und zu navigieren – ganz ohne Hardware. Diese hardwarefreie Lösung ist sowohl im Aufbau als auch im Betrieb kosten- und zeiteffizient.



ExeonTrace bietet Einblick in die hochgradig distribuierte IT-Infrastruktur von Planzer.



Das Sicherheitsteam von Planzer überprüft regelmässig das UI von ExeonTrace und untersucht die von ExeonTrace ausgelösten Anomalien. Die Anomalien berücksichtigen historische Daten und machen diese sichtbar, um die Ursachen effizient zu finden.



ExeonTrace wird nicht nur vom Security-Team, sondern auch von Operations genutzt, um die Auslastung der Systeme standortübergreifend zu überwachen, Netzwerkänderungen zu planen sowie zu verifizieren (z.B. Migration von Services in die Cloud).



ExeonTrace bietet zusätzliche Sicherheit für das gesamte Firmennetzwerk und insbesondere für die geschäftskritischen Legacy-Systeme, da die Überwachungsregeln noch stärker eingeschränkt wurden.



ExeonTrace ermöglicht die Aufzeichnung und Langzeitpeicherung von relevanten Security-Log-Daten. Eine Graphdatenbank erreicht eine Datenreduktion und ermöglicht eine einfache Navigation durch die Logdaten in der Oberfläche.

“Ich bin von der technischen Umsetzung dieser
Network Detection & Response Lösung begeistert.
Mit Exeon Trace in unserem Netzwerk kann
ich definitiv ruhiger schlafen.”

Peter Hagen

CIO Planzer



Kontakt

e x e o n

Smart Cyber Security.



Gregor Erismann
CCO
+41 78 797 05 09
gregor.erismann@exeon.com

Exeon Analytics AG
Grubenstrasse 12
8045 Zurich
Switzerland
contact@exeon.com

exeon.com