



**ANTARES  
NETLOGIX**



**SUCCESS STORY**

Frauenthal Handel Gruppe AG und ANLX bauen Partnerschaft aus!

## MANAGED SOC FÜR DAS EXTRA AN SICHERHEIT

Wenn das eigene Team zwar leistungsstark, aber klein ist, stößt es in Sachen „allumfassende IT-Security“ schnell an seine Grenzen. Um dennoch auf die gestiegene Gefahr eines Cyberangriffs vorbereitet zu sein, hat sich die Frauenthal Handel Gruppe AG für das Managed SOC (Security Operations Center) von Antares-Netlogix entschieden.



### AUSANGSSITUATION

Noch mehr Sicherheit

FHG und Antares Netlogix verbindet eine langjährige Partnerschaft, denn das Handelsunternehmen hat sich bereits in diversen Bereichen die Unterstützung der ANLX Experten gesichert. Nun galt es, neben der Managed Infrastructure weitere Maßnahmen für die IT-Security zu ergreifen, um der steigenden Bedrohungslage durch Cyberangriffe Herr zu werden. Bei der Entscheidung für einen Dienstleister lag die Wahl aufgrund der positiven Erfahrungen mit ANLX nahe.



### HERAUSFORDERUNG

Dieselbe Manpower bei mehr Risiken

Die Frauenthal Handel Gruppe AG setzt eine Vielzahl an Systemen ein, die aufgrund zunehmender Gefahren aus dem Internet jederzeit vor Angriffen abgesichert und geschützt sein sollen. Da das Unternehmen inhouse aber weder über die personellen Ressourcen noch über das entsprechende Know-how verfügt, sollten die Profis von Antares-Netlogix mit dem Managed SOC eingreifen. Dabei war es der Wunsch des Auftraggebers, die bereits genutzten Security-Lösungen einschließlich Log Management zu konsolidieren und proaktiv zu überwachen, um den Schutz zu steigern.



### AUFTRAGGEBER

**Frauenthal Handel Gruppe AG**



In Österreich ist die Frauenthal Handel Gruppe die klare Nummer 1 im Großhandel für Installateure, Bauherren, Bauträger, Architekten und Kommunen. Die Division besteht aus den Sanitär, Heizung und Installationstechnik Großhändlern SHT und ÖAG, dem Rohrleitungs- und Tiefbauspezialisten Kontinentale, dem österreichischen Online-Elektrogroßhandel Elektromaterial.at, sowie dem Logistik- und Dienstleistungspartner Frauenthal Handel Gruppe mit 25 Bad & Energie Schauräumen und über 75 ISZ Abholmärkten. Am Markt agieren alle Unternehmen als eigenständige Marken.



### LÖSUNG

Managed SOC und Endpoint Security

Gemeinsam entschied man sich für die Einführung eines Managed SOC sowie des Managed EDR. Indem mit Endpoint Detection & Response (EDR) neben den Systemen auch das gesamte Netzwerk und darin befindliche Endgeräte überwacht werden, wird ein noch höheres Schutzniveau erzielt. Außerdem galt es, neben der Einführung technischer Hilfsmittel auch die Awareness der Mitarbeiter zu schulen, um die Kompetenzen rund um IT-Security langfristig auf- und auszubauen.



## UMSETZUNG UND ERGEBNIS

In 14 Monaten zum Ziel

Aufgrund der Vielfalt der Systeme wurde ein Projektplan aufgestellt, der die Einführung des Managed SOC und des Managed EDR in vier Projektphasen unterteilte. Nach insgesamt 14 Monaten war die Technologie ebenso wie das Team bei ANLX und bei FHG dann bereit, gemeinsam gegen die aktuellsten Gefahren aus dem Internet binnen kürzester Zeit vorzugehen und das Handelsunternehmen vor Schäden durch böswillige Angriffe abzuschotten.

Nach Abschluss des initialen Projekts laufen die aufgesetzten Prozesse heute reibungslos. ANLX kümmert sich proaktiv um alle außergewöhnlichen Vorkommnisse, behält die Logs im Auge und ist auch dann schnell zur Seite, wenn es zu Fragen auf Seiten der Frauenthal Handel Gruppe AG kommt.

„Die Managed Security im SOC-Umfeld hat für uns einen noch besseren Schutz unserer Systeme geboten. Dabei sind auch Themen aufgetaucht, die wir anfänglich noch gar nicht im Blick hatten. Wir sind sehr zufrieden und würden die Zusammenarbeit mit ANLX jederzeit weiterempfehlen. Wir selbst planen, noch intensiver zu kooperieren.“

**Günther Novak,**

Leitung IT Service Delivery Managment/Information Security Officer, FHG

### Das ANLX SOC

Mit dem ANLX.Cloud SOC as a Service erhalten Sie eine ganzheitliche Verteidigungsstrategie und proaktive 360°-Security-Plattform.

Mit unserem Service können Sie sicher sein, dass Ihre gesamte Netzwerkumgebung von unseren Cybersecurity-Analysten in Hinblick auf neue Bedrohungen kontinuierlich überwacht wird.

Unser SOC Agent überwacht den Normalbetrieb Ihres Unternehmens und sammelt Log-Daten. Bei ungewöhnlichen Aktionen wird nicht sofort ein Alarm ausgelöst, sondern eine Analyse des Problems von unseren Experten durchgeführt. Wird tatsächlich eine Bedrohung festgestellt, erreichen Sie ein Alarm in Form eines Tickets per Mail oder als Anruf. Somit werden Fehlalarme vermieden und die Problemlösung kann sofort eingeleitet werden.

[www.netlogix.at](http://www.netlogix.at)



**ANTARES-NETLOGIX**

**Wir sind für Sie da!**

Antares Netlogix ist als IT-Consulting-Unternehmen in der DACH-Region tätig und bietet umfassende IT-Security Services in der ANLX Cloud an.

Vertraulichkeit und die Kontinuität der Geschäftsprozesse stehen an höchster Stelle. Höchste Zertifizierungen und die hohe Loyalität der 60 Mitarbeiter sind die Basis für den Erfolg des eigentümergeführten Unternehmens aus dem Mostviertel.

### Sie haben Fragen?

Das ANLX-Team steht Ihnen gerne zur Verfügung!



**Antares-Netlogix Netzwerkberatung GmbH**

Feldstraße 13, A-3300 Amstetten

T: +43 74 72 / 65 480-0 E: [office@netlogix.at](mailto:office@netlogix.at)

[www.netlogix.at](http://www.netlogix.at)