SUCCESS STORY

ERFOLGE DER TECHNOLOGIE-PARTNERSCHAFT
MIT DER MARC O‘POLO AG

sure[secure]

Marc O'Polo®

WEBSITE

https://www.marc-o-polo.com/

REGION

Gegründet in Stockholm, Schweden; Headquarter in Stephanskirchen, Bayern

BRANCHE

Bekleidung, Accessories

MITARBEITER

Rund 2.000 Angestellte

01 DAS UNTERNEHMEN

Die Casual-Lifestyle Brand Marc O'Polo blickt auf eine lange Geschichte zurück: es wurde im Jahr 1967 in Stockholm als kleines Unternehmen von Rolf Lind, Göte Huss und Jerry O'Sheets gegründet, ist heutzutage in Deutschland beheimatet, in über 60 Ländern vertreten und beschäftigt weltweit rund 2.000 Mitarbeiter:innen aus über 60 Nationen.

Marc O'Polo steht für gehobene, zeitgemäße Premium Modern Casual Wear. Die Vorliebe für natürliche Materialien, hochwertige Qualitäten und besondere Details zeichnen den individuellen Stil der Premiummarke mit skandinavischen Wurzeln aus – ganz im Sinne der Philosophie ihrer Gründer: „Die Freiheit, sich selbst treu zu bleiben."

Die Marke beliefert mehr als 2.300 Filialen und Handelspartner in mehr als 60 Ländern. Das Jahr 2019 konnte zudem als ein sehr erfolgreiches Geschäftsjahr abgeschlossen werden. Entgegen dem Markttrend wächst Marc O'Polo

Und dann kam der Schock…

02 DER VORFALL

Im September 2019 wird Marc O'Polo mit Sitz in Stephanskirchen Opfer eines Cyberangriffs – ironischerweise am Freitag den 13., an einem Tag nach einer großen Firmenfeier.

Sämtliche IT- und Kassen-Systeme fielen aus, Ware konnte nicht ausgeliefert werden und Sicherheits-Backups nicht gestartet.
„Alle IT-Bereiche des Unternehmens waren komplett verschlüsselt", erinnert sich Daniel Zimmer, Information Technology Security Manager bei der Marc O'Polo AG.

Die Unternehmensleitung vermutet, dass hier Profis am Werk waren, die diesen Erpressungsversuch gegen Marc O'Polo von langer Hand planten. Über mehrere Monate drangen die Cyber-Kriminellen immer tiefer in das Unternehmenssystem vor, mit Bedacht geplant und durchgeführt – ganz ohne aufzufallen.

Der Angriff wurde höchstwahrscheinlich durch ein simples Update ermöglicht, welches von einem Mitarbeitenden an seinem Laptop über ein offenes WLAN durchführte – und die schadende Malware empfing. Der zu diesem Zeitpunkt noch neue Chief Operating Officer von Marc O'Polo, Dr. Patric Spethmann, reagierte nach Bekanntwerden des Angriffs schnell und zog sofort ein Team externer Fachleute hinzu, bestehend aus Forensiker:innen und IT-Expert:innen. Das Ziel war es unter anderem, die IT-Systeme umgehend wieder zum Laufen zu bekommen und dann eine neue Systemarchitektur aufzusetzen. Ersteres, um das Geschäft so schnell wie möglich wieder zu starten. Letzteres, um die Unternehmens-IT im übertragenen Sinne nicht mehr nur in einem „Haus" unterzubringen, sondern in verschiedenen Häusern.

„Cyberangriffe nehmen stetig zu, es hat gerade erst begonnen! Von daher müssen wir uns alle, auch wir bei Marc O'Polo, darauf einstellen, dass es wieder passieren wird. Technologisch, organisatorisch und prozessual muss man vorbereitet sein, damit solch ein Threat kontrollierbar, beherrschbar und lösbar bleibt.

Daher arbeiten wir an allen drei Säulen der IT-Security: Protection, Detection & Defense"

Dr. Patric Spethmann, Chief Operating Officer von Marc O'Polo

03 DIE SURESECURE

Um eine ständige, ganzheitliche Übersicht sowie Kontrolle über die eigene IT-Sicherheit zu erhalten, nimmt das Marc O'Polo seit April 2021 den MSS SOCaaS (Managed Security Service: Security Operation Center as a Service) der suresecure in Anspruch, denn das Fashion Label weiß sowohl den direkten, partnerschaftlichen Draht zu den suresecure Expert:innen zu schätzen, als auch die besonders schnelle Reaktionszeit des Teams.

Was bedeutet das konkret?

Unser SOC managt alle sicherheitsrelevanten Themenbereiche der IT-Infrastruktur an einer zentralen Stelle. Alle sicherheitsrelevanten Systeme wie das Unternehmensnetzwerk, Server, Rechner und Internetservices werden proaktiv integriert, überwacht und analysiert. Durch die frühzeitige Erkennung von Cyberangriffen und unsere schnelle Reaktionszeit sind die jeweiligen Systeme optimal geschützt.

Um den Mehrwert unseres SOCs zu erkennen und in der eigenen Infrastruktur zu prüfen, bieten wir einen Proof of Concept unseres SOCs von 6 Monaten mit 24/7 Servicezeit an.

In dieser Testphase verschaffen wir Visibilität der Unternehmens-IT. Der PoC umfasst dabei die regelmäßige Sichtung und Analyse eingehender Logs und Log-Daten über einen Zeitraum von 6 Monaten. Hier zeichnen sich die Trends ab, die wir im weiteren Ablauf beleuchten. Ebenso erfolgt die Einstufung der Kritikalität der Events.

So erhielt das Unternehmen Marc O'Polo produktübergreifende Security-Insights, gewann anhand der Auswertung dieser Phase einen Überblick über den Zustand der IT-Umgebung – und verlängerte am 30.11.21 den SOC-Vertrag mit uns um weitere 12 Monate.

04 ERREICHTE ERFOLGE

Mit dem MSS SOCaaS (Managed Security Service: Security Operation Center as a Service) ermöglicht die suresecure-Lösung bereits erhebliche Verbesserungen in der IT-Infrastruktur von Marc O'Polo.

Erhöhung der Schutzmechanismen durch:

- Risikomanagement
- SOC as a Service Vertrag
- PoC (Proof of Concept) Phase
- Phising Kampagne
- Umfassendes Firewall Konzept
- Sandboxing

05 DER AUSBLICK

Daniel Zimmer empfiehlt jedem Unternehmen, dass es sich lohnt, alle Mitarbeiter:innen bezüglich des IT- und Informationssicherheitsbewusstsein zu schulen (Security Awareness) und in guten Zeiten einen vertrauensvollen, zuverlässigen Partner für die interne IT- und Informationssicherheit zu wählen. Denn nur so können sich Unternehmen wirklich auf den Ernstfall vorbereiten und Cyberangriffen vorbeugen.

Timeline:

2019

Marc O´Polo schließt 2019 das erfolgreichste Geschäftsjahr seit fünf Jahren ab.

2019

Freitag der 13.09.2019
Hackerangriff: Alle IT-Bereiche des Unternehmens komplett verschlüsselt

2019

Externe Forensiker:innen und IT-Expert:innen werden sofort hinzugezogen

Bis 2021

Das Unternehmen erneuert die vollständige IT-Infrastruktur und Systemarchitektur

2021

Partnerschaft mit suresecure

2021

30. April: MSS SOCaaS
(Managed Security Service:
Security Operations Center as a Service)
mit 6-monatiger PoC (Proof of Concept) Phase

2021

Ende der 6-monatigen PoC (Proof of Concept) Phase

2021

30. November: SOC-Vertrag

„Wir sehen die suresecure nicht nur als starken und zuverlässigen Geschäftspartner gegen Cyberkriminalität und für Informationssicherheit, sondern vor allem als Sparring Partner mit einem gemeinsamen Ziel: ***IT-Security.***

Das passionierte Team der suresecure befasst sich professionell mit all unseren Belangen und vermittelt uns eindeutig, dass es nicht nur ums Geschäft und den finanziellen Profit geht. Das gibt uns auch für die Zukunft ein gutes Gefühl."

Daniel Zimmer, Information Technology Security Manager, Marc O'Polo AG

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de