Ontinue

CUSTOMER STORY

Dekorativ, aber sicher – dank lückenloser Überwachung

Schwan Cosmetics bringt Farbe in den Alltag vieler Menschen. Für kleine wie große Labels fertigt das Unternehmen weltweit dekorative Stiftkosmetik. Schwan Cosmetics ist Teil des Konzerns STABILO, der vor allem durch seine Schreibgeräte in der Öffentlichkeit bekannt ist. Zur Holding gehört zudem eine Outdoorsparte, die bekannte Marken wie Deuter, Ortovox, Maier Sports oder Gonso beinhaltet. Auch wenn die IT-Abteilungen der Tochtergesellschaften von STABILO durch ein sogenanntes IT-Council im regelmäßigen Austausch stehen, so verwaltet jedes Unternehmen seine Hard- und Software autark, denn schon die unterschiedlichen Produktionsabläufe erfordern eigenständige ERP (Enterprise Resource Planning)-Systeme mit diversen Schnittstellen zu weiteren Applikationen. Um seinen Nutzern die nötige Rechenleistung zur Verfügung zu stellen, betreibt Schwan Cosmetics eigene Rechenzentren.

Für das Security Incident Management setzt das Unternehmen seit Oktober 2023 auf die Zusammenarbeit mit dem MXDR (Managed Extended Detection and Respons)-Anbieter Ontinue. Die initiale Idee dazu, das Security Operations Center (SOC) an einen externen Partner auszulagern, kam von Robert Hans, Director Security bei Schwan Cosmetics, auf einem Security-

schwan cosmetics

Motivation

- Aufbau eines professionellen Security Operations Center mit 24/7-Überwachung
- Einführung weiterer Sicherheitssysteme Lösung

Lösung

- Anpassung und Erweiterung des bestehenden Security-Portfolios von Microsoft
- Implementierung von Microsoft Identity Protection
- Alert-Management über das SOC von Ontinue

Ergebnis

- 24/7-Alert-Überwachung in Echtzeit
- Einfache Incident-Kommunikation per Teams Channel
- Abgestimmte Eskalationsmatrix
- Schnellere Reaktionsgeschwindigkeit und erhöhtes Sicherheitsniveau
- Entlastung der IT

Über Schwan Cosmetics

Schwan Cosmetics ist ein weltweit tätiger Private-Label-Hersteller von dekorativen Kosmetika. Das Unternehmen mit Hauptsitz im mittelfränkischen Heroldsberg beschäftigt weltweit mehr als 3.000 Mitarbeiter in sieben Ländern und verfügt über modernste Produktionsanlagen.

Kongress. Im Rahmen der internen Evaluation wurde schnell deutlich, dass ein MXDR-Provider zu mehr Effizienz und einer besseren Ressourcennutzung im Bereich der Cybersicherheit beitragen könnte. Vor der Implementierung musste sich das Team zwar nur etwa einem kritischen Incident pro Monat stellen, doch die hohe Zahl der „False Positives“ erwies sich als zeitaufwendiger und repetitiver Block im Arbeitsalltag von Alexander Wurm, Administrator Netzwerk und Security bei Schwan Cosmetics Germany, und seinen Teamkollegen. „Die Prüfung der Vorfälle war für uns rein zeitlich gerade noch abzubilden, allerdings war es uns so kaum möglich, wertschöpfende oder innovative Projekte voranzutreiben“, betont Wurm. „Glücklicherweise hatte kein Angriff schwerwiegendere Konsequenzen, als uns Zeit für andere Aufgaben zu rauben.“

> „Durch die Zusammenarbeit mit Ontinue hat sich das Sicherheitsniveau stark verbessert. Zudem sind interne Kapazitäten frei geworden, die wir für strategische Security-Projekte einsetzen können.“
>
> Robert Hans
> **Director Security**
> **Schwan Cosmetics**

Lückenlose Überwachung dank 24/7-Betrieb

Da eine interne Risikobetrachtung das enorme Schadenspotential eines erfolgreichen Cyberangriffs verdeutlichte, entschloss sich Schwan Cosmetics, in ein SOC zu investieren. Die Wahl fiel schließlich auf ein 24/7 gemanagtes SOC eines externen MXDR- Anbieters, da eine Umsetzung durch die hauseigenen IT-Experten ressourcenbedingt nicht möglich war. Als international agierendes Unternehmen mit knapp 1500 Usern hatte sich gerade die lückenlose Überwachung, das Ontinue im Zuge des Services Ontinue ION anbietet, schnell als wichtiger Aspekt herauskristallisiert.

Die Transparenz zu potenziellen Cyberangriffen ist einer der großen Benefits, der aus der Zusammenarbeit mit Ontinue gewachsen ist. „Es war immer eine gewisse Sorge da, ob wir wirklich schnell genug alles erkennen“, bestätigt Robert Hans. „Gerade bei einem kritischen Vorfall darf es keine Lücken und keine Zeitverzögerung geben. Auch wenn wir uns mit unseren klassischen Maßnahmen gut aufgestellt sahen, so war eine gewisse Blindheit schon vorhanden.“ Da der Microsoft Defender bereits teilweise vorher im Einsatz war, gestaltete sich das Onboarding als überraschend schnell und effektiv – immerhin stellen die Sicherheitstechnologien von Microsoft auch die Basis für den MXDR-Service Ontinue ION dar. Innerhalb von wenigen Wochen wurde dann die restliche erforderliche Infrastruktur aufgesetzt. „Uns hat vor allem gefallen, dass Ontinue sich in seinem Geschäftsmodell wirklich auf MXDR fokussiert“, bestätigt Robert Hans. „Außerdem werden wir durch die Cyber Defender und Cyber Advisor, aus denen sich das Security Operations Center zusammensetzt, als Spezialisten auf Augenhöhe betrachtet – das fördert eine vertrauensvolle und angenehme Zusammenarbeit.“ Der gemeinsame Microsoft-Teams-Kanal sorgt darüber hinaus für eine einfache und schnelle Kommunikation zwischen Ontinue und Schwan Cosmetics. Das ist bei den Incidents ein echter Vorteil im Gegensatz zur klassischen Absprache via E-Mail. So arbeiten die Cyber Defender und Cyber Advisor mit dem Team von Schwan Cosmetics in Echtzeit zusammen.

Gestiegene Reaktionsgeschwindigkeit

Innerhalb des ersten Jahres der Zusammenarbeit hat sich bereits gezeigt, dass die Reaktionszeit im Incident-Management deutlich gesunken ist. Dabei profitiert das unternehmensinterne IT-Team davon, dass durch die Vorselektion von

Ontinue viel weniger zu bearbeitende Fälle auf ihrem Schreibtisch landen. Durch die proaktiven Sicherheitshinweise der Cyber Advisor von Ontinue zu Sicherheitslücken oder Konfigurationen lassen sich gefährliche Lücken zudem bereits frühzeitig erkennen und entsprechende Gegenmaßnahmen einleiten, bevor Angreifer sie ausnutzen können. Die durch die Nutzung des Services gewonnene Zeit kann nun zielführend in weitere strategische Security-Projekte investiert werden.

Ontinue

Über Ontinue

Ontinue, der Experte für KI-gestützte Managed Extended Detection and Response (MXDR), ist ein rund um die Uhr verfügbarer Sicherheitspartner mit Hauptsitz in Zürich. Um die IT-Umgebungen seiner Kunden durchgehend zu schützen, ihren Sicherheitsstatus zu bewerten und kontinuierlich zu verbessern, kombiniert Ontinue KI-gesteuerte Automatisierung und menschliches Fachwissen mit dem Microsoft-Sicherheits-Produktportfolio. Durch die intelligente, Cloud-basierte Nonstop SecOps-Plattform reicht Ontinues Schutz vor Cyberattacken weit über die grundlegenden Detection- und Response-Services hinaus.

Weitere Informationen gibt es unter www.ontinue.com