Ontinue

CUSTOMER STORY

Ontinue hält die IT-Infrastruktur von CWS hygienisch rein

Die praktischen Stoffhandtuchspender, die in nahezu jedem öffentlichen Waschraum hängen, kennt jeder. Und auch die Marke dahinter, die CWS International GmbH, ist wohl den meisten Menschen in Europa bereits einmal untergekommen. Wer allerdings glaubt, dass das Unternehmen mit dem markanten Logo nur Hygieneartikel bereitstellt, irrt gewaltig. Die 1954 von Conrad Wolfgang Schnyder gegründete CWS ist heute auch einer der größten Vermieter von Arbeitskleidung in Europa und hat mittlerweile zudem die Bereiche Brandschutz, Reinraumreinigung und die Reinigung medizinischer Gerätschaften zum Serviceportfolio hinzugefügt. In diesen Geschäftsfeldern erwirtschaften die rund 11.000 Mitarbeitenden einen Gesamtumsatz von über 1 Milliarde Euro. Firmenhauptsitz ist seit jeher Duisburg, aktiv ist das Unternehmen allerdings in 15 europäischen Ländern.

Als international aufgestelltes Unternehmen ist die IT-Infrastruktur erwartungsgemäß diversifiziert und weitläufig. Das liegt unter anderem daran, dass die CWS über viele Jahre anorganisch gewachsen ist. Dementsprechend hat sich eine sehr große Menge an Legacy-Systemen angesammelt. An deren Aufarbeitung und Abbau arbeitet das IT-Team seit einiger Zeit

CWS

Motivation

- Aufbau eines Security Operations Center
- Rund-um-die-Uhr-Überwachung der IT-Security-Tools
- Schnellere Reaktion auf Cyberattacken
- Verbesserung der Visibilität über die IT-Infrastruktur
- Höheres Zeitkontingent für die Reduzierung des Risikoniveaus in anderen Geschäftsbereichen als der IT-Sicherheit

Lösung

- Erweiterung des unternehmensinternen Sicherheitsteams zu einem vollständigen Security Operations Center durch MXDR-Dienst Ontinue ION und Microsoft-Teams-Kanal
- Teilexternalisierung der Bearbeitung von Security Incidents
- Schaffung eines Single Pane of Glass via Microsoft Sentinel und Microsoft Defender

Ergebnis

- 24/7/365-Überwachung der IT-Infrastruktur
- Schnellere Reaktion auf kritische Sicherheitsrisiken
- Höhere Visibilität über die gesamte IT-Infrastruktur
- Freie Mitarbeiterressourcen für Verbesserung der Prozessreife und des Sicherheitsniveaus in anderen Geschäftsbereichen

Über die CWS International GmbH

Mit innovativen, nachhaltigen und digitalen Mietlösungen trägt CWS zu einer gesünderen und sicheren Zukunft bei. Das Angebot gliedert sich in Produkte und Services aus den Bereichen Hygiene, Matten, Berufskleidung, Brandschutz, Reinraum sowie Gesundheit und Pflege. Mit seinem Servicemodell verfolgt das Unternehmen die Grundidee der Kreislaufwirtschaft in allen Bereichen: Materialien werden reduziert, mehrfach eingesetzt und ressourcenschonend aufbereitet. CWS ist eine Marke der CWS International GmbH und ihrer Tochtergesellschaften.

und konnte die Vielzahl an unterschiedlichen Rechenzentren und Active Directories zu jeweils einem einzigen konsolidieren. Auch eine Cloud-Strategie befindet sich in der praktischen Umsetzung, allerdings ist erst rund ein Drittel der IT-Infrastruktur tatsächlich Cloud-basiert, der Großteil läuft nach wie vor on-premises. Doch gerade für alltägliche Anwendungen wie die Bürosoftware und andere Programme, die nicht essenzieller Bestandteil des Kerngeschäfts sind, setzt CWS seit einiger Zeit auf Software-as-a-Service-Angebote. Insbesondere Microsoft hat sich in dieser Hinsicht als vertrauenswürdiger Partner erwiesen und so stellte das Unternehmen auch die Sicherheitsinfrastruktur auf die E5-Suite mit dem Microsoft Defender als EDR (Endpoint Detection and Response)-Tool und Sentinel als SIEM (Security Information and Event Management)-Plattform um.

„Während unserer Konsolidierungsarbeiten passierte schließlich das, wovor sich jede IT-Abteilung fürchtet: Hackern gelang es, eine erfolgreiche Cyberattacke gegen uns zu lancieren", verrät Benjamin Boecker, Information Security Manager bei CWS. „Da haben wir am eigenen Leib erfahren, was wir ohnehin bereits wussten – nämlich, dass es nicht ausreicht, hin und wieder in den Security-Tools zu schauen, ob vielleicht gerade ein Angriff läuft." Was die CWS dringend benötigte, war eine Rund-um-die-Uhr-Überwachung der Sicherheitsanwendungen, die an jedem Tag im Jahr ein schnelles Eingreifen ermöglicht. „Uns war allerdings nicht nur klar, dass wir ein voll funktionsfähiges Security Operations Center, sondern auch professionelle externe Unterstützung benötigen", so Boecker.

Zeitdruck und Reevaluierung

Da der Aufbau eines Security Operations Centers (SOC) in Eigenregie nicht in Frage kam, der Cyberangriff das Team von Benjamin Boecker und die IT-Abteilung von CWS aber unter Zeitdruck setzte, entschied man sich für einen MDR-Anbieter, der kurzfristig verfügbar war. Nach einem Jahr und dem Abschluss der Implementierung von Microsoft Sentinel und dem Microsoft Defender war jedoch eine Neubewertung der Sicherheitslage erforderlich. Der erste Schritt war die Lizenzierung der E5-Suite von Microsoft und die praktische Umsetzung des Plattformansatzes anstelle eines Best-of-Breed-

> **„ Ontinue schafft es, unsere Reaktionsgeschwindigkeit bei Bedrohungen massiv zu beschleunigen. So können wir uns ruhigen Gewissens darum kümmern, die Prozessreife und das Risikoniveau in anderen Geschäftsbereichen zu verbessern."**

Benjamin Boecker
Information Security Manager
CWS International GmbH

Ansatzes. Der Aufwand, die jeweils besten Security-Anwendungen unter einen Hut zu bekommen, stand in keinem Verhältnis zu den Vorteilen einer Sicherheitsinfrastruktur aus einem Guss. In diesem Zuge empfahl Microsoft selbst drei MXDR (Managed Extended Detection and Response)-Anbieter, unter anderem auch Ontinue, das Unternehmen, das die CWS am Ende überzeugte.

Die größten Pluspunkte von Ontinue waren die Geschwindigkeit, mit der alle Service- und Kommunikationsschnittstellen implementiert werden konnten, sowie das stimmige Gesamtpaket. Auch menschlich und unternehmerisch war die Zusammenarbeit von Anfang an positiv und passte einfach. „Im Gegensatz zu anderen Anbietern haben wir schnell gemerkt, dass Ontinue kein typischer Sales-getriebener MXDR-Provider ist. Auch ihr Beharren auf einem holistischen Ansatz hat uns am Ende überzeugt, auch wenn wir selbst andere Prioritäten gesetzt hätten", erklärt Boecker. „Die Implementierung verlief am Ende so problemlos, dass wir in Rekordzeit mit der Zusammenarbeit loslegen konnten."

Feste Prozesse und hervorragende Ergebnisse

An der Sicherheitsinfrastruktur bei CWS hat sich durch den Wechsel zum MXDR-Service Ontinue ION kaum etwas geändert. Was sich allerdings gewandelt hat, ist die Betreuung der verwendeten Sicherheitssoftware: Die Cyber Defender von

Ontinue überwachen die Microsoft-Tools rund um die Uhr und haben so eine holistische Visibilität hergestellt. Das Team von Benjamin Boecker weiß somit zu jeder Zeit, was in ihrer IT-Infrastruktur vor sich geht, inklusive welche Log-ins stattfinden und welche Events vom Domain Controller ausgeführt werden. „Wir sehen mittlerweile nicht nur, wenn eine verseuchte Datei geöffnet wird, sondern auch, wo sie herkam und in welchen E-Mails sie noch auftaucht. Unser MXDR-Partner gibt uns diese Informationen inklusive des relevanten Kontexts, die uns bei der Entscheidungsfindung helfen. Auf diese Weise schafft es Ontinue, unsere Reaktionsgeschwindigkeit bei Bedrohungen massiv zu beschleunigen“, so Boecker.

Ein gutes Gefühl entsteht bei der CWS auch dadurch, dass Prozesse für die Eskalation und die Alarmierung der unternehmensinternen IT-Abteilung klar definiert sind. Benjamin Boecker und sein Team erhalten umgehend Meldung im gemeinsamen Teams-Channel, wenn ein Security Incident stattfindet – außerhalb der Geschäftszeiten auch via Mail und per Anruf, sofern es sich um einen dringenden Notfall handelt. Für kleinere Events gibt es ebenfalls Handlungsprotokolle, sogenannte Playbooks, in denen definiert ist, welche Art der Incidents Ontinue selbst lösen darf und wie. Eine Meldung an die CWS machen die Cyber Defender aber in jedem Fall. Wenn die IT-Fachabteilung involviert werden muss, übernehmen das Benjamin Boecker und sein Team. „Insbesondere die Kommunikation über Teams ist Gold wert“, betont Boecker. „Diese Art der Zusammenarbeit ist deutlich intuitiver und zuverlässiger als Ticketsysteme oder Browser-basierte Plattformen. So fühlt sich der MXDR-Service nicht wie eine externe Entität an, sondern wir agieren gemeinsam als einheitliches SOC.“

Der Erfolg spricht ebenfalls für sich. Die jährlich bei der CWS anstehende Risikoanalyse durch einen externen Dienstleister hatte der IT-Abteilung Jahr für Jahr ihre Shortcomings und den Nachbesserungsbedarf in Sachen Incident-Management aufgezeigt. Seitdem das Unternehmen mit Ontinue zusammenarbeitet, ist dieser Bereich kein Problem mehr, sondern erhält die höchsten Bewertungen. „In Zukunft können wir uns ruhigen Gewissens darum kümmern, die Prozessreife und das Risikoniveau in anderen Geschäftsbereichen zu verbessern. Ontinue verschafft uns durch die unermüdliche Arbeit der Cyber Defender und Cyber Advisor diese Freiheit“, fasst Boecker zusammen. „An den Wochenenden können wir somit unsere Nerven ruhen lassen und müssen nicht ständig Twitter oder die einschlägigen Newsportale durchforsten, ob es aktuelle Bedrohungen gibt – ein gutes Gefühl.“

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