Ontinue

CUSTOMER STORY

Internationales Gourmet-Catering-Unternehmen erreicht 90%ige Reduzierung von Cybersecurity-Vorfällen durch Partnerschaft mit Ontinue

DO & CO schien ein unwahrscheinliches Ziel für einen Cyber-Angriff zu sein. Als Gourmet-Catering-Unternehmen mit den drei Hauptgeschäftsfeldern Airline Catering, International Event Catering und Restaurants, Lounges & Hotels betreibt DO & CO 32 Gourmetküchen in zwölf Ländern und beschäftigt 12.000 Mitarbeiter:innen, die die Formel 1, die FIFA Fußball-Weltmeisterschaft und andere internationale Veranstaltungen beliefern.

Das Geschäft von DO & CO ist häufig kurzfristigen Änderungen unterworfen – in Bezug auf Anzahl, Veranstaltungsorte, Logistik, Flüge –, ist das Unternehmen im Wesentlichen dafür verantwortlich, jeden Tag „das Unmögliche möglich zu machen". Dennoch hatte DO & CO bis jetzt kein formelles Cyber-Sicherheitsprogramm.

„Analysierte man die Umgebung von DO & CO war ein Cybervorfall zu erwarten", sagt Johann van Duyn, Global CISO bei DO & CO, der bemerkt, dass dieser Tag am 23. November 2020 gekommen war.

DO & CO

Motivation

- Notwendigkeit einer modernen Sicherheitsstrategie aufgrund von Ransomware-Angriff 2020
- 24/7-Überwachung
- SOC intern aufzubauen, war keine Option

Lösung

- Ontinue ION managed extended Detection and Response (MXDR) Service
- Microsoft E5 Security
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365
- Microsoft Sentinel

Ergebnis

- 90%ige Reduzierung von Cybersicherheitsvorfällen
- 40 % Einsparung bei den SecOps-Datenkosten
- 75 % der Warnungen wurden bereits durch Automatisierung geschlossen
- Optimierte Kommunikation und Zusammenarbeit durch Microsoft Teams
- Mit einem 24/7-Service, den Angriffen immer einen Schritt voraus
- Gewonnene Zeit für neue innovative SecOps-Projekte

Über DO & CO

DO & CO, ein Gourmet-Catering-Unternehmen mit den drei Hauptgeschäftsfeldern Airline Catering, International Event Catering und Restaurants, Lounges & Hotels, betreibt 32 Gourmetküchen in zwölf Ländern und beschäftigt 12.000 Mitarbeiter:innen. Um die höchsten Standards im Produkt- sowie Service-Bereich umsetzen zu können, setzt DO & CO auf seine Mitarbeiter:innen – alle geprägt durch eine eigene, starke Persönlichkeit und Gastgeber aus Leidenschaft.

„Die Organisation wurde Opfer eines großen Ransomware-Angriffs durch die DoppelPaymer-Gruppe“, erzählt er. „Die Bildschirme wurden alle rot. Drei Monate an Backups wurden beschädigt. Der uns zur Verfügung gestellte Entschlüsseler funktionierte nicht. Kurz gesagt: Alles war zerstört. Die Folgen für DO & CO waren nicht unerheblich. Das Unternehmen konnte sich nicht einmal mehr auf das Active Directory verlassen, was, wie Sie sich vorstellen können, kein guter Ausgangspunkt ist“.

Für ein Unternehmen mit einem Jahresumsatz von 935 Millionen Euro bedeutete der Rückgriff auf manuelle Ad-hoc-Prozesse das Scheitern vieler vertraglicher Anforderungen, rechtliche Probleme, Reputationsverlust - und damit auch finanzielle Verluste.

Es war aber auch ein Weckruf. Als Reaktion darauf stellte das Unternehmen einen CIO ein und Van Duyn kam später als CISO hinzu.

Gemeinsam entwickelten sie eine Cyberstrategie, migrierten in die Cloud und trafen neben anderen strategischen Entscheidungen einen Microsoft-Ansatz für Cybersicherheit, indem sie sich für die Sicherheitsfunktionen von Microsoft E5 mit Microsoft 365 Defender als Kernstück entschieden.

„Das war die beste Entscheidung, die wir je getroffen haben. E5 bietet viele Funktionen in einer einzigen Anschaffung“, so Van Duyn, der festgestellt hat, dass Microsoft Defender for Office 365 die Anzahl der Malware- und Phishing-E-Mails in den Posteingängen der Benutzer sofort reduziert hat. „Defender for Endpoint war eine wahre Goldgrube bei der Erkennung unerwünschter Aktivitäten in der Umgebung - selbst bei Administratoren, die versuchen, Software zu installieren, die sie nicht installieren sollten“.

Aber wie jedes SecOps-Team weiß, halten sich Bedrohungsakteure nicht an Geschäftszeiten.

„Sie wollen uns zu jeder Tages- und Nachtzeit attackieren“, sagt Van Duyn. „Wir mussten also mit einem Security-Provider sprechen, der uns einen 24/7-Schutz bieten konnte.“

Ontinue ION: Verbesserung von Erkennung, Reaktion und Prävention

Die kontrollierte Erkennung und Reaktion von Cyberangriffen wurden für DO & CO, Van Duyn und sein Team eindeutig zu einer operativen Notwendigkeit: Ontinue ION Managed Extended Detection and Response (MXDR) erfüllte alle Anforderungen.

„Ein SOC intern aufzubauen, ist für uns einfach keine Option“, sagt Van Duyn. „Wir haben ein sehr kleines Team. Die Kosten, die Qualifikationsanforderungen, die Abwanderung von Analysten und die Notwendigkeit, mit den ständigen technologischen Veränderungen Schritt zu halten, machten es für uns unmöglich. Ontinue kam zu uns als MXDR-Experte, ein auf Microsoft E5 und Sentinel spezialisiertes Unternehmen. Ontinue integriert sich in Microsoft Teams, bietet Automatisierung durch maschinelles Lernen und KI und stellt Microsoft Sentinel in unserer Azure-Umgebung bereit.“

Für Van Duyn begann die erfolgreiche Zusammenarbeit mit Ontinue bereits mit der Implementierung der Lösung. Seitdem hat sich die Zusammenarbeit intensiviert und verstärkt. „Das sind wahrscheinlich die professionellsten und kompetentesten Leute, mit denen ich je zusammengearbeitet habe”, kommentiert der Leiter der Infrastrukturabteilung während der Umsetzung.

Van Duyn berichtet, dass der Senior Analyst in seinem Team mit Ontinue ION über Microsoft Teams interagiert, wo alle Details klar kommuniziert werden, sodass er nicht suchen muss. „Wir können uns neuen innovativen Projekten widmen, da Ontinue die Sicherheitserkennung und -reaktion von möglichen Cyberangriffen übernimmt“, sagt er. „Das Anreichern von Warnmeldungen mit zusätzlichen Informationen durch Ontinue ist für uns sehr wertvoll. Es ermöglicht uns, Warnmeldungen viel schneller zu verstehen, als wir es vor dem Start von Ontinue konnten.

Automatisierung verbessert die Prävention

Die Automatisierung hat sich als Schlüssel zur Effizienz und in einigen Fällen auch zur Prävention erwiesen.

„Ich schätze es sehr, wenn Unregelmäßigkeiten bereits durch Automatisierung effizient eliminiert werden", sagt Van Duyn. „Das ist ein klarer Gewinn. Die Cyber Defenders von Ontinue gehen aber auch noch über die bloße Bearbeitung der Vorfälle hinaus. Sie informieren uns nicht nur darüber, was passiert ist, sondern geben uns auch wertvolle Empfehlungen, wie wir zukünftige Attacken verhindern können. Darüber hinaus zeigen sie uns, wie wir unsere IT-Umgebung und unsere gesamte Organisation widerstandfähiger gegenüber Cyberattacken machen können."

Die Angreifer entwickeln sich weiter, und Van Duyn ist froh, mit Ontinue einen Security-Experten zu haben, der sich ebenfalls kontinuierlich weiterentwickelt, um den aktuellen Angriffen immer einen Schritt voraus zu sein. „Wir haben auch gesehen, dass Ontinue bei der letzten Welle von Attacken QR-Code-Phishing-Angriffe verhindern konnte", fügt er hinzu.

Was würde Van Duyn anderen CISOs raten, die einen Anbieter für Managed Detection and Response suchen?

> „ Würde ich die Zusammenarbeit mit Ontinue weiterempfehlen? Auf jeden Fall. Wir sind außerordentlich froh, mit Ontinue einen wertvollen Partner auf unserem Weg zur Cybersicherheit gefunden zu haben".

Johann Van Duyn
Global CISO
DO & CO

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