Ontinue

CUSTOMER STORY

Infors schüttelt Cyberkriminelle mit Ontinue mühelos ab

Seit fast 60 Jahren entwickelt und produziert Infors HT High-Tech-Lösungen für die Biotechnologie. Das Portfolio umfasst Bioreaktoren, Schüttelinkubatoren sowie die passende Software für die Steuerung von Bioprozessen. Das familiengeführte Unternehmen, mittlerweile zur Aktiengesellschaft avanciert, unterhält Standorte in zahlreichen Ländern in Nordamerika, Asien und Europa, Hauptsitz ist das Schweizerische Bottmingen. Ein besonderes Merkmal des Unternehmens ist dessen mitarbeiter- und kundenorientiertes Handeln. Flache Hierarchien sorgen für ein angenehmes Klima, in dem Innovations- und Optimierungsvorschläge wohlwollend aufgenommen werden. Zudem arbeiten bei Infors HT viele Wissenschaftler, die aus dem operativen Forschungsbereich kommen: Das Traditionsunternehmen beschäftigt also nicht nur Ingenieure, die wissen, wie man Ventile baut, sondern auch Leute, die genau wissen, was die Kunden brauchen und welche Probleme sie lösen müssen.

Was sich bei Infors HT seit der Gründung 1965 drastisch verändert hat, ist die digitale Infrastruktur. Über die Jahre ist der Reifegrad der IT stetig gestiegen – und damit auch deren Komplexität. Heute befinden sich rund 90 Prozent der IT-Infrastruktur in der Cloud, während man in Sachen Anwendungssoftware vollständig auf Microsoft-Technologien setzt. Als global aufgestelltes Unternehmen

INFORS HT

Motivation

- Aufbau eines echten Security Operations Center (SOC)
- 24/7/365-Überwachung der IT-Infrastruktur
- Freischaufeln von Zeit für interne Audits und IT-Administration

Lösung

- Implementierung einer holistischen, Microsoft-basierten Security-Infrastruktur
- Auslagerung des Monitorings der Sicherheits-Tools an die Cyber Advisors und Cyber Defenders des MXDR-Services Ontinue ION

Ergebnis

- Konsistentes Monitoring und First Response durch Ontinue – rund um die Uhr
- Bessere Einbindung des hauseigenen First-Level-Supports in die Sicherheitsprozes-se
- Enge Kooperation zwischen Ontinue und Infors HT über Microsoft Teams
- Ein ganzheitlicher Schutz der IT-Infrastruktur
- Deutlich vergrößertes Zeitkontingent der Mitarbeitenden und somit mehr Möglichkeiten, interne Audits abzuhalten und die Sicherheitsmaßnahmen zu verbessern

About Infors HT

Infors HT entwickelt und produziert seit über 55 Jahren High-Tech-Lösungen für die Bio-technologie. Das Unternehmen ist stolz darauf, zu den Besten unter den Spezialisten für Bio-reaktoren, Schüttelinkubatoren sowie Software zur Steuerung von Bioprozessen zu gehören. Infors HT setzt sich tagtäglich dafür ein, die Arbeitsprozesse seiner Kunden durch den Einsatz von modernsten Technologien zu vereinfachen. Dazu bezieht das Unternehmen seine Kunden direkt in die Produkteentwicklung mit ein und entwirft so praxisorientierte Produkte, Softwarelösungen und Dienstleistungen, die nicht nur auf dem Papier sondern auch im herausfordernden Alltag das halten, was sie versprechen.

versteht es sich von selbst, dass Infors HT seine Standorte in aller Welt mit einer sehr weitläufigen WAN (Wide Area Network)-Infrastruktur vernetzt hat. „Wir sind ein Familienunternehmen und das merkt man am Umgang miteinander“, betont René Schröder, Hauptverantwortlicher für die IT-Sicherheit. „Und natürlich möchte ich meine Firma wie meine Familie schützen – in diesem Fall vor Cyberattacken wie Hacking- oder Phishing-Angriffen.“

Um diesem Willen Taten folgen zu lassen, richtete das IT-Team von Infors HT ein kleines „Micro Security Operations Center“ ein, das sich um die Alerts und Incidents der Microsoft-Tools Defender und Sentinel kümmerte. „Wir haben leider schnell gemerkt, dass wir nicht alle eingehenden Warnungen bearbeiten können. Irgendwann haben wir uns dann nur noch auf die High Alerts konzentriert und versucht, die kleineren Warnungen zu automatisieren“, so Schröder weiter. „Ehrlicherweise hat uns aber das Know-how gefehlt, die uns zur Verfügung stehenden Tools auch wirklich vollständig auszunutzen.“ Was Infors HT definitiv brauchte, waren echte Cybersecurity-Spezialisten, die sich gezielt in diesem Bereich weitergebildet haben. Das selbst zu stemmen und entsprechendes Fachwissen in vollem Umfang aufzubauen, kam durch den Workload der IT-Abteilung nicht in Frage. Die Beauftragung eines Anbieters für Managed Extended Detection and Response (MXDR) schien daher der einzig sinnvolle Weg zu sein.

Ein Sicherheitspaket aus einem Guss

Bei der Suche nach dem richtigen Anbieter war ein Punkt absolute Voraussetzung: Er musste sich exzellent mit Microsoft-Technologie auskennen, denn sowohl Client- als auch Cloud-seitig und natürlich in Sachen Sicherheitstechnologie setzt Infors HT seit Jahren komplett auf Microsoft. „Uns war insbesondere wichtig, dass unser Security-Partner nicht gegen den Hersteller unserer Sicherheitssoftware arbeitet. Viele MXDR-Dienstleister setzen eigene Tools ein, die die nativ verwendeten overrulen oder in ihrer Arbeit behindern. Außerdem wollten wir nicht noch mehr Komplexität, sondern ein Gesamtpaket aus einem Guss“, erklärt Schröder die wichtigsten Kernelemente für den Evaluierungsprozess.

„Wir haben uns dann einige Unternehmen angeschaut und Präsentationen angehört, doch die meisten haben Sentinel und die Defender-Suite nicht oder nur rudimentär verstanden und eingesetzt. Ontinue hingegen hat uns mit seiner Microsoft-Expertise überzeugt“, so Schröder weiter. Hinzu kam, so der Hauptverantwortliche für die IT-Sicherheit, dass Infors HT in Sachen Netzwerkverwaltung und -absicherung sich seit Jahren auf Open Systems verlässt, also den Anbieter, aus dem Ontinue

> **„Wir hatten bei Ontinue jederzeit Ansprechpartner und Cyber Advisor, die sofort wussten, was wir brauchen, was wir meinen und wie wir die Hürden überwinden können, die bei der Zusammenarbeit mit externen Dienstleistern zwangsläufig auftauchen.“**
>
> 
>
> René Schröder
> **Hauptverantwortlicher für die IT-Sicherheit**
> Infors HT

hervorgegangen ist. Lob hat auch die gute Kommunikation trotz hochtechnologischer Themen verdient, die mit Ontinue weitergeführt wird, sagt er: „Wir hatten bei Ontinue jederzeit Ansprechpartner und Cyber Advisor, die sofort wussten, was wir brauchen, was wir meinen und wie wir die Hürden überwinden können, die bei der Zusammenarbeit mit externen Dienstleistern zwangsläufig auftauchen.“

Nicht zu teuer und absolut sinnvoll

Mit Ontinues MXDR-Service ION hat sich Infors HT einerseits davon emanzipiert, selbst allen Security-Events und -Incidents auf den Grund gehen zu müssen – viele werden direkt vom Security Operations Center (SOC) von Ontinue abgefangen, sodass nur eines von Hunderttausend Events an Infors HT eskaliert wird. Das schaufelt Ressourcen für René Schröder und seine Kollegen frei, die sie dafür nutzen, die Infrastruktur zu verwalten, Organisatorisches zu klären und interne Audits durchzuführen. Natürlich ist es auch ein beruhi-

gender Fakt für René Schröder und sein Team, dass die IT-Infrastuktur auch nach Feierabend und an allen Tagen der Woche ausreichend überwacht wird. So fallen Anomalien und Cyberattacken sofort auf und den Angreifern bleibt viel weniger Zeit, bevor die nötigen Gegenmaßnahmen ergriffen werden.

Kommuniziert wird zwischen René Schröder, seinem Team und Ontinue über den gemein-samen Channel in Microsoft Teams, was die Absprachen zwischen Cyber-Defendern, Cyber-Advisorn und internen Sicherheitsexperten reibungslos gestaltet. Die Security-Professionals vom MXDR-Partner Ontinue integrieren sich so sehr in das hauseigene IT-Team, dass es sich anfühlt, als wären sie Teil des Unternehmens. „Auch unsere eigenen First-Level-Supporter können wir so besser in die Sicherheitsprozesse einbinden", erklärt Schröder. „Sie können via Teams direkt die Cyber Defender und Cyber Advisor von Ontinue fragen, welche Empfehlungen sie für bestimmte Vorfälle haben. Die antworten in der Regel sofort und haben bereits Vorschläge parat, wie wir reagieren sollten. Das ist insbesondere deswegen wichtig, weil wir in den USA, also einer komplett anderen Zeitzone, beispielsweise keine IT-Administratoren, sondern nur First-Level-Support haben." Für die entsprechenden Prozesse wurden zu Beginn der Zusammenarbeit Eskalationsmatrixen erstellt, die Zugriffs-berechtigungen, Zuständigkeiten und Ansprechpartner an allen neuralgischen Punkten festlegen.

> **„MXDR-Services sind weder zu teuer, noch sind sie sinnfrei für kleine und mittelständische Unternehmen – im Gegenteil: Sie sind genau das, was sie brauchen, um ihre IT-Infrastruktur angemessen abzusichern, ohne über gigantische Budgets zu verfügen."**

René Schröder
Hauptverantwortlicher für die IT-Sicherheit
Infors HT

Die Experten von Ontinue und Infors HT sind mittlerweile zu einem Security Operations Center (SOC) zusammengewachsen. René Schröder quantifiziert das Plus an Sicherheitsleistung anhand der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik und dem Schweizer IKT-Standard wie folgt: „Wir sind einer sicheren IT-Infrastruktur um etwa 50 Prozent nähergekommen. Das zeigt einmal mehr, dass MXDR-Services weder zu teuer, noch sinnfrei für kleine und mittelständische Unternehmen sind – im Gegenteil: Sie sind eine wirklich gute Sache und gerade KMU sollten nicht am falschen Ende sparen, wenn es um ihre Sicherheit geht."

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