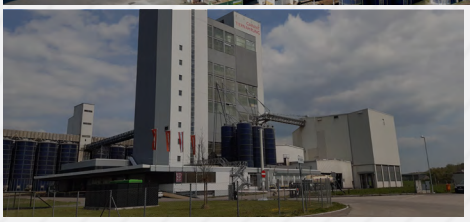
voices

CrowdStrike Customer Case Study



GARANT TIERNAHRUNG

Führender österreichischer Futtermittelproduzent setzt auf Cloud-basierte IT-Security, um Geschäftsbetrieb rund um die Uhr sicherzustellen

Garant Tiernahrung ist der führende österreichische Produzent von Tierfuttermitteln, mit drei Standorten in Pöchlarn, Graz und Aschach an der Donau. Die hundertprozentige Tochter der Raiffeisen Ware Austria AG ist verantwortlich für die großflächige Versorgung von Nutztieren mit Futtermittel in Österreich.

Die größte Herausforderung an die IT-Security, die sich bei einer derartigen Verantwortung stellt, ist die Sicherstellung der Produktion rund um die Uhr, an sieben Tagen die Woche. „Wir sind ein mittelständischer Betrieb mit knapp 200 Mitarbeitern. An unseren drei Standorten produzieren wir pro Jahr etwa 380.000 Tonnen Tierfutter im 24/7-Betrieb. Bei uns hängt alles davon ab, dass die Produktion ununterbrochen durchläuft“, erklärt Markus Hinterndorfer, Head of IT bei Garant. „Selbst Routinewartungen werden bei uns mit großem Vorlauf geplant und müssen innerhalb eines bestimmten Zeitfensters abgeschlossen sein. Wir sind eine Vorstufe der Lebensmittelindustrie und müssen daher sehr hohe Auflagen erfüllen.“

Unter diesen besonderen Voraussetzungen und um sich gleichzeitig gegen moderne Angreifer und deren Methoden (TTPs) zu schützen, beschloss Garant, sich eine neue Security-Lösung zuzulegen, die die vielfältigen Anforderungen erfolgreich vereinen soll. Ein weiteres Ziel war die Verringerung des administrativen Aufwands. Da das bisher eingesetzte Produkt nicht nur auf quartalsweise Updates angewiesen war, die einen Neustart aller Server erforderten, sondern zudem noch signaturbasiert und damit anfällig für moderne Angriffe war, entschied sich Garant für die Cloud-native Lösung der nächsten Generation von CrowdStrike. Ein sofort sichtbarer Vorteil der CrowdStrike-Lösung war, dass sich die Zahl der benötigten Ausnahmen innerhalb der Endpoint-Lösung auf drei reduziert hat.

Ein weiterer Pluspunkt für die CrowdStrike-Lösung war für Hinterndorfer und sein Team die von der Plattform eingesetzte Künstliche Intelligenz (KI). „Wir haben bereits seit vier Jahren sehr gute Erfahrungen mit KI im Bereich Netzwerk-Security gemacht. Für uns war es ein logischer Schritt, dass wir mit CrowdStrike die KI auch auf unsere Endpoints gebracht haben.“

Garant setzt zum Schutz der Produktion auf die Cloud

Der Rollout der CrowdStrike-Lösung verlief dabei denkbar unkompliziert. Dank Deployment über MS System Center konnte Garant den schlanken CrowdStrike Agenten innerhalb einer Woche automatisiert auf 300 Endgeräten ausrollen, ohne Neustart. Auch der Parallelbetrieb mit dem alten

BRANCHE

Futtermittel

STANDORT/KONZERNZENTRALE

Pöchlarn, Österreich

HERAUSFORDERUNG

- Absicherung der Unternehmens-IT, Sicherstellung der 24/7-Produktion

LÖSUNG

Die Cloud-basierte CrowdStrike Falcon® Plattform bietet Garant eine umfassende IT-Sicherheitslösung, die nicht nur einen 24/7 Produktionsbetrieb sicherstellt, sondern dank mehr Sichtbarkeit und Transparenz auch die Inventarisierung vereinfacht.

„Ich kann jetzt definitiv wieder ruhiger schlafen.”

Markus Hinterndorfer
Head of IT
Garant Tiernahrung

voices

CrowdStrike Customer Case Study

Sicherheitsprodukt während der Übergangsphase verursachte keinerlei Probleme, zur großen Überraschung von Hinterndorfer und seinem Team, die hier zunächst mit Komplikationen gerechnet hatten: „Eine goldene Regel in der IT sagt immer, man weiß nicht, wie sich mehr als ein Endpoint-Produkt auf demselben Gerät auswirkt. Doch mit CrowdStrike parallel zu unserem alten Produkt gab es hier keine Probleme". Zudem wird der CrowdStrike-Agent zukünftig automatisch auf jedem neuen Rechner oder Server installiert, wenn dieser einer Domain beitritt.

Auch das Ausrollen der CrowdStrike-Lösung auf Maschinen zur Anlagensteuerung, die per Policy keinen Zugang zum Internet haben dürfen, gestaltete sich deutlich unkomplizierter, als angenommen. Die Konfiguration der Firewall, die eine Kommunikation ausschließlich mit CrowdStrike-Hosts erlaubt, sorgte hier dafür, dass die Maschinen trotzdem an die Cloudverwaltung angeschlossen werden konnten.

Unerwarteter Einsatz der Technologie

Die CrowdStrike-Lösung erfüllt, wie Hinterndorfer und sein Team festgestellt haben, neben den Security-Funktionen noch einen weiteren Zweck: „Wir haben sehr schnell gemerkt, dass die Lösung dadurch, dass sie extrem viele Daten analysiert und bereitstellt, auch hervorragend für administrative Zwecke geeignet ist. Wir können jetzt zum Beispiel sehen, wer eine Datei oder ein Verzeichnis wohin verschoben hat. Oder welche Softwareversionen wo installiert sind. Das hat uns die Inventarisierung deutlich erleichtert."

Mit der neuen Lösung ist Garant sehr zufrieden: „Klar, 100 Prozent Sicherheit gibt es nie. Aber mit unserer Kombination von KI im Netzwerk und am Endpoint haben wir schon ein wesentlich besseres Gefühl als zuvor mit dem rein signaturbasierten Produkt."

„Wir brauchen uns keine Gedanken mehr machen, wenn ein Mitarbeiter mit seinem Gerät das Firmengelände verlässt und vom Hotel oder von zuhause aus arbeitet. Ich kann jetzt definitiv wieder ruhiger schlafen."

ERGEBNISSE

- Keine Downtime während Security-Updates
- Sicherstellung des 24/7-Produktionsbetriebs
- Einsatz von CrowdStrikes Datenanalysefähigkeiten für Administrationszwecke

ENDPOINTS

300

EINGESETZTE CROWDSTRIKE-PRODUKTE

- Falcon Discover™ IT Hygiene
- Falcon Insight™ Endpoint Detection und Response (EDR)
- Falcon Prevent™ Antivirus der nächsten Generation
- Falcon Spotlight™ Vulnerability Management

ÜBER CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Plattform zum Schutz von Workloads, Endgeräten, Identitäten und Daten die Sicherheit im Cloud-Zeitalter neu. Dank der CrowdStrike Security Cloud und erstklassiger künstlicher Intelligenz kann die CrowdStrike Falcon®-Plattform Echtzeit-Angriffsindikatoren, Bedrohungsdaten, sich ständig weiterentwickelnde Methoden der Gegner sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen nutzen, um hochpräzise Detektionen, eine automatisierte Schutz- und Abhilfemaßnahme, erstklassiges Threat Hunting und eine nach Prioritäten geordnete Beobachtung von Schwachstellen zu ermöglichen.

CrowdStrike: **We stop breaches.**