ANDECHSER MOLKEREI SCHEITZ FÜHRT CORTEX XDR MIT INDEVIS EIN

Ist unsere Cybersicherheit noch zeitgemäß? Diese Frage stellte sich die Andechser Molkerei Scheitz und beschloss, den bestehenden Virenschutz durch eine Cloud-basierte XDR-Plattform abzulösen. Mit der Endpoint Protection Cortex XDR von Palo Alto Networks und der Unterstützung von indevis ist das Unternehmen jetzt zukunftssicher aufgestellt, um moderne Cyber-Bedrohungen schneller zu erkennen und abzuwehren.

Schmackhafte Bio-Milchprodukte aus dem Voralpenland: Dafür ist die Andechser Molkerei Scheitz bekannt. Das 1908 gegründete Familienunternehmen aus dem oberbayerischen Andechs wird seit 2003 in dritter Generation von Barbara Scheitz geführt und verarbeitet seit 2009 ausschließlich Milch aus zertifizierter ökologischer Landwirtschaft. Bereits zum wiederholten Mal wurde das Unternehmen mit dem deutschen Nachhaltigkeitspreis ausgezeichnet. Rund 150 Bio-Molkereiprodukte umfasst das Sortiment der Marke Andechser Natur. Dafür wird täglich Milch von 660 Bio-Bauern aus der Region abgeholt und 24/7 rund um die Uhr verarbeitet. Damit die Produktion kontinuierlich läuft, braucht die Molkerei eine hochverfügbare IT. Störungen oder Ausfälle durch Cyberangriffe kann sie sich nicht erlauben. Die IT-Sicherheit spielt daher eine wichtige Rolle für das Unternehmen.

DIE CYBERSICHERHEIT AN WACHSENDE BEDROHUNGEN ANPASSEN

Um sich vor Malware zu schützen, hatte die Andechser Molkerei bisher eine On-Premises Anti-Virus-Lösung im Einsatz. „Das war viele Jahre angemessen und hat sehr gut funktioniert", sagt Peter Hehl, IT-Leiter bei der Andechser Molkerei. „Mittlerweile haben sich die Bedrohungslage und unsere Anforderungen geändert. In der IT und IT Security ist ja immer alles im Fluss. Daher prüfen wir regelmäßig, welche neuen Entwicklungen es gibt und ob wir noch gut aufgestellt sind." Klar ist: Cyberangriffe werden immer ausgeklügelter und komplexer. Klassische signaturbasierte AV-Lösungen sind häufig nicht mehr in der Lage, moderne Ransomware-Attacken zu erkennen. Während Schadprogramme früher meist über einen direkten Download auf einem Endgerät landeten, gehen Cyberkriminelle heute in der Regel in mehreren Phasen vor. Sie dringen immer noch über die E-Mail als Einfallstor Nummer eins ins Netzwerk ein, verhalten sich zunächst unauffällig und laden erst später Schadcode nach.

DIE AUSGANGSLAGE: FEHLENDE TRANSPARENZ UND HOHER AUFWAND

Die bestehende On-Premises Security-Lösung bei Andechser war der veränderten Bedrohungslage nicht mehr gewachsen. Angriffsmuster konnten aufgrund der fehlenden zentralen Managementansicht nur schwer erkannt werden. „Außerdem hat die manuelle Administration unser IT-Team stark belastet", erklärt Michael Oesterhelt, IT-Administrator bei der Andechser Molkerei. „Aktualisierung der Signaturen und Einspielen der Softwareupdates war zeitintensiv und leider nicht vollautomatisiert."

DIE ANFORDERUNGEN AN DIE NEUE ENDPUNKT-SICHERHEITSLÖSUNG

Um diese Herausforderungen zu meistern, wollte die Andechser Molkerei eine Cloud-basierte XDR-Plattform (Extended Detection and Response) für den Endpoint-Schutz einführen und suchte einen Partner, der sie kompetent unterstützt. Die Anforderungen an die neue XDR-Security-Lösung waren klar: Sie sollte in der Lage sein, alle sicherheitsrelevanten Daten in einem zentralen Data Lake zu konsolidieren und Anomalien sowie unbekannte Bedrohungen atomatisiert zu erkennen. Außerdem sollte sie leicht zu managen und skalierbar sein. „Wichtig war uns auch, dass die neue Lösung kontinuierlich weiterentwickelt wird und künftige Compliance-Anforderungen erfüllen kann", ergänzt Michael Oesterhelt. „Daher wollten wir auf einen zukunftssicheren Hersteller setzen, der am Markt etabliert ist."

ANDECHSER NATUR

ECKDATEN

Kunde: Andechser Molkerei Scheitz GmbH
Branche: Lebensmittelindustrie
Standort: Andechs, Deutschland
Mitarbeiterzahl: 241 (Stand: 2025)
Umsatz: Rund 250 Millionen Euro

PROJEKT UND VORTEILE

+ Implementierung von Cortex XDR in die IT-Infrastruktur
+ Proof of Concept und Grund-konfiguration des Systems
+ Rollback der bestehenden AV-Lösung und Rollout der Cortex XDR-Agenten
+ KI-gestützte, verhaltensbasierte Anomalie- und Bedrohungs-erkennung über alle Endpunkte hinweg und im Netzwerk
+ Bessere Übersicht über den IT-Sicherheitsstatus
+ Leistungsfähiges, zukunftssicheres Security-System zur wirksamen Bekämpfung moderner Cyber-bedrohungen
+ Produktivitätssteigerung in der internen IT dank effizienterer Administrations-Prozesse und Automatisierung
+ Unterstützung durch einen kompetenten Partner bei allen Fragen rund um das Thema IT-Sicherheit

indevis GmbH
Koppstraße 14
81379 München
Tel. +49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

„indevis ist für uns seit vielen Jahren ein strategischer Partner, mit dem wir sehr vertrauensvoll zusammenarbeiten. Ausschlaggebend für unsere Entscheidung war nicht nur das überzeugende Feature-Set von Cortex XDR, die Synergien zur Palo Alto Networks Firewall, sondern auch die Expertise von indevis auf diesem Gebiet. So wussten wir, dass wir immer kompetente Unterstützung an der Seite haben."

Peter Hehl, IT-Leiter Andechser Molkerei

ÜBER DIE INDEVIS GMBH

Die ISO 27001 zertifizierte indevis GmbH mit Sitz in München bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienstleistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT Security und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT-Sicherheit muss strategisch geplant werden.

Dabei ist indevis nicht nur in München und Umgebung vertreten: Unsere Mitarbeiterinnen und Mitarbeiter sind an Standorten in ganz Deutschland aktiv.

indevis
Sicherheit in einer vernetzten Welt

SIE WOLLEN MEHR ERFAHREN?

Unsere Experten beraten Sie gerne und unterstützen auch Sie dabei, Ihre Cybersicherheitsstrategie zu optimieren. Kontaktieren Sie uns:

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

TÜV SÜD ISO 27001

Bei der Entscheidungsfindung ließ sich die Andechser Molkerei von mehreren Dienstleistern beraten und evaluierte verschiedene XDR-Lösungen. Am Ende fiel die Wahl auf indevis und Cortex XDR von Palo Alto Networks. „indevis ist für uns seit vielen Jahren ein strategischer Partner, mit dem wir sehr vertrauensvoll zusammenarbeiten", sagt Peter Hehl, Leiter IT. „Ausschlaggebend für unsere Entscheidung war nicht nur das überzeugende Feature-Set von Cortex XDR, die Synergien zur Palo Alto Networks Firewall, sondern auch die Expertise von indevis auf diesem Gebiet. So wussten wir, dass wir immer kompetente Unterstützung an der Seite haben."

SCHNELLE UND EINFACHE EINFÜHRUNG

Da Cortex XDR als SaaS bereitgestellt wird, verlief die Einführung schnell und unkompliziert. In einem zweiwöchigen Proof of Concept (POC) testeten indevis und die Molkerei zunächst, wie sich die Lösung im Praxiseinsatz verhält. Gibt es zum Beispiel Anwendungen oder Prozesse, die die automatische Bedrohungserkennung fälschlicherweise als gefährlich einstuft und blockiert? Um solche False Positives im Produktivbetrieb zu vermeiden, wurde der Rollout der Endpunkte größtenteils schon in der POC-Phase geplant. Anschließend nahm indevis innerhalb von wenigen Stunden die Grundkonfiguration des Cortex XDR-Systems vor. Um den Rollout der Cortex-Agenten auf den Endpunkten kümmerte sich die Molkerei selbst. Da das IT-Team sehr vorsichtig vorgehen musste, dauerte diese Projektphase drei bis vier Monate. Christian Linke, IT-Administrator bei der Andechser Molkerei, erklärt: „Wir produzieren ja 24/7. Wenn man eine Software installiert, muss man die Systeme teilweise neu starten. An manche Server kommen wir nicht immer problemlos ran."

DAS ERGEBNIS: ZUKUNFTSFÄHIGE BEDROHUNGSERKENNUNG MIT ZENTRALER ÜBERSICHT

Mit Cortex XDR verfügt die Andechser Molkerei jetzt über eine umfassende Plattform für Endpunktsicherheit, die anhand von KI-gestützten Verhaltensanalysen komplexe Bedrohungen erkennen und blockieren kann. Neben den Endpunkten hat indevis auch die bestehende Palo Alto Networks Firewall und die Segmentierungs-Firewall von Fortinet integriert. Die Log-Daten aller angeschlossenen Systeme laufen im Strata Logging Service (früher Cortex Data Lake) zusammen, werden zentral korreliert und analysiert. So gewinnt die Andechser Molkerei eine bessere Übersicht über ihren IT-Sicherheitsstatus und kann schneller auf Bedrohungen reagieren. Die effizienteren Prozesse und die Automatisierung entlasten das interne IT-Team, das jetzt produktiver arbeiten kann. Und wenn Fragen rund um das Thema IT-Sicherheit auftauchen, unterstützt indevis jederzeit kompetent. IT-Leiter Peter Hehl freut sich: „Mit Cortex XDR und indevis können wir auch neue regulatorische Anforderungen erfüllen. Als Lebensmittelhersteller fallen wir unter die NIS-2-Direktive. Zum Projektstart war das noch kein Thema. Heute sind wir froh, dass wir auf die richtige Lösung gesetzt haben."

Produktion - Andechser Molkerei Scheitz