© Eisbär Eis GmbH

Risiken erkennen und einfrieren

Wie Produktions- und IT-Umgebungen bestmöglich gegen Hackerangriffe geschützt werden

Cyberkriminelle suchen nach Sicherheitsschwachstellen, durch die sie leicht in fremde Systeme eindringen können. Fündig werden sie nicht nur in IT-Umgebungen. Zunehmend ist zu beobachten, dass vernetzte und schlecht abgesicherte Umgebungen in produzierenden Unternehmen, die sogenannte Operational Technology (OT*), neue Einfallstore, insbesondere für Ransomware, bieten. Um alle Angriffe abwehren zu können, werden Gesamtlösungen benötigt, die IT- und OT-Netzwerke gleichermaßen schützen. Eine solche hat ACP IT Solutions jetzt für Eisbär Eis realisiert, einen der größten Speiseeisherstellers Europas.

* OT steht für Operational Technology und bezeichnet die Hard- und Software für die Fertigungssteuerung.

IT for innovators.

Resilient mit KI und Managed Security

Eisbär Eis im niedersächsischen Apensen produziert für europäische Handelsmarken täglich rund fünf Millionen Portionen Speiseeis. Neben dem Hauptsitz in Apensen betreibt das Unternehmen einen weiteren Produktionsstandort bei Ribnitz-Damgarten. Würde ein Cyberangriff die digital stark vernetzte Eisproduktion stoppen, wären die Folgen für das Unternehmen potenziell existenzbedrohend – wie für jedes Unternehmen. Deshalb hat Eisbär Eis zusammen mit ACP IT Solutions (ACP) eine umfassende IT-Sicherheitslösung zum Schutz seiner IT- und OT-Umgebung aufgebaut.

Mehr als jedes dritte Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von Cyberkriminellen geworden. Die Anzahl der Angriffsversuche ist dabei um ein Vielfaches höher. Infrastrukturen betroffener Unternehmen werden durch eingeschleuste Ransomware, Viren und Trojaner lahmgelegt und geschäftsrelevante Daten entwendet und verschlüsselt. Dies sind die klassischen Schadenszenarien.

Steigende Cyberrisiken durch stärker vernetzte OT-Netzwerke

Bei produzierenden Unternehmen kommt eine weitere Gefährdungsdimension hinzu, denn neben klassischen IT-Netzwerken betreiben diese Unternehmen auch noch Netzwerke für die Steuerung ihrer Produktionssysteme. Letztere werden als Operational Technology bezeichnet, kurz OT. Durch die fortschreitende Automatisierung sind viele OT-Umgebungen in den vergangenen Jahren stark gewachsen. „So war es auch bei uns", bestätigt Christoph Lück, der 2011 ins Unternehmen kam und seit zwölf Jahren IT-Leiter bei Eisbär Eis ist. „Früher hatten wir in der Produktion ein paar vernetzte Rechner im Einsatz. Heute ist jede einzelne Produktionslinie so umfassend vernetzt, dass sie mehrere Dutzend IP-Adressen benötigt und fortlaufend Daten sendet und empfängt."

Für Cyberkriminelle haben sich Unternehmen mit OT-Netzwerken längst zu attraktiven Zielen entwickelt. Hauptgrund dafür sind oftmals veraltete oder unzureichende Schutzmaßnahmen oder fehlendes Patchmanagement. Den Kriminellen geht es um Erpressung. Während das Druckmittel bei Angriffen auf herkömmliche IT-Netzwerke geklaute und verschlüsselte Daten sind, sind es bei Angriffen auf OT-Netzwerke sabotierte oder lahmgelegte Produktionsprozesse. „Beide Angriffsszenarien können und wollen wir uns nicht leisten", sagt Lück und ergänzt: „Als unser IT-Partner ACP IT Solutions uns dann auch noch proaktiv auf das stark gestiegene Cyberrisiko hinwies und vorschlug, einen Security-Check durchzuführen, um mögliche Schwachstellen aufzuzeigen, habe ich direkt gesagt: Das können wir uns sparen. Wir wissen, dass wir unseren Schutz verbessern müssen und fangen am besten gleich damit an."

Effektive Gesamtlösung für die IT- und OT-Security

Gesagt, getan: Christoph Lück beauftragte ACP damit, ein Gesamtkonzept für die Absicherung der IT- und Produktionsumgebung zu entwickeln. Das ist schnell und bedarfsgerecht erfolgt – auch, weil ACP als langjähriger IT-Partner die Prozesse

Eisbär Eis GmbH
www.eisbaer-eis.de

Facts

Standorte: Apensen, Ribnitz-Damgarten

Mitarbeiter*innen: rund 650

Jahresumsatz: ca. 200 Millionen

Branche: Lebensmittelindustrie

Partner

Darktrace
Sophos

Unsere Lösung

KI-gestützte Network Detection & Response für OT-Umgebung

Managed Detection & Response für IT-Umgebung

und Strukturen von Eisbär Eis kennt und dadurch die Anforderungen des Kunden zielsicher umsetzen konnte. „Besonders wichtig“, betont Lück, „war für uns neben der maximalen Schutzwirkung, dass die neue Lösung keinen Mehraufwand erzeugt.“

Um diese Anforderung zu erfüllen und ein effektives Schutzsystem für die gesamte Infrastruktur von Eisbär Eis zu realisieren, hat ACP verschiedene Lösungsansätze entwickelt, analysiert und priorisiert. Favorit für die IT-Security war das Managed Detection and Response-Angebot von Sophos in Kombination mit einer KI-gestützten Network Detection & Response-Lösung von Darktrace für den OT-Bereich. Wie gut diese Lösung zu den Anforderungen von Eisbär Eis passt, haben Darktrace und ACP in einem gemeinsam erarbeiteten Proof of Concept bewiesen.

KI erkennt Anomalien im Netzwerkverhalten autonom

„Der Lösungsansatz von Darktrace hat uns sofort überzeugt“, erinnert sich Lück. Der Grund liegt in der Herangehensweise. Darktrace analysiert nicht primär den Zustand der IT in der Produktion, sondern das Netzwerkverhalten – sprich: den Datenverkehr aller Maschinen und Anlagen. Die Künstliche Intelligenz der Softwarelösung von Darktrace weiß nach kurzer Trainingszeit, welches Verhalten typisch für die jeweilige Produktion ist. Die KI erkennt Abweichungen und Anomalien in Echtzeit und leitet sofort Maßnahmen zur Gefahreneindämmung ein. Beispiel: Wenn ein Sensor plötzlich ungewöhnlich viele Daten übermittelt, würde das System dies automatisch als Anomalie erkennen und den Datenstrang, von dem die potenzielle Bedrohung ausgeht, gezielt von der Kommunikation abschneiden.

„Das System arbeitet komplett autonom und bringt uns enorme Vorteile“, weiß Lück und erklärt: „Geht die Anomalie wirklich von einer Bedrohung aus, friert das System diese sofort ein, sodass es gar nicht erst zu einer Ausbreitung kommt. Steckt keine Bedrohung dahinter, sondern einfach nur ein technischer Fehler, bemerken wir diesen frühzeitig und informieren unser Wartungsteam, bevor Schäden in unserer Produktionsstrecke entstehen können.“ Die autonome Echtzeit-Reaktion auf jede Abweichung von der Norm und das Isolieren der Quelle schafft zudem Transparenz über etwaige Schwachstellen. Nach einem Ernstfall würde Eisbär Eis das Einfallstor genau kennen und kann es zielgerichtet schließen.

> „ACP hat eine Gesamtlösung für unsere IT-Sicherheit entwickelt, die bestmöglichen Schutz verspricht – sowohl für unsere klassische IT-Umgebung als auch für unsere Produktionsnetzwerke. Und das bei größtmöglicher Entlastung unseres IT-Teams. So können wir uns auf das Wesentliche konzentrieren und unsere Ressourcen effizient einsetzen.“
>
> **Christoph Lück**
> Head of IT, Eisbär Eis GmbH

Rund um die Uhr geschützt – mit Managed Cyber Security

Einmal implementiert, läuft das System autonom. Auch das KI-Modell reagiert selbstständig auf Veränderungen in der Netzwerkumgebung und lernt kontinuierlich dazu. Noch ein Pluspunkt: Die OT Security-Lösung von Darktrace ist bei Eisbär Eis vollständig in die Managed Detection and Response (MDR)-Umgebung von Sophos eingebunden. „Das erhöht den Return on Invest für uns spürbar", sagt Lück, „denn auch das Sophos-Team hat Zugriff auf die Informationen des Darktrace-Systems und hat so neben der IT-Security auch unseren OT-Bereich im Blick."

Sophos MDR ist ein vollständig gemanagter 24/7-Service für Threat Detection und Response. Expertinnen und Experten von Sophos überwachen sämtliche Rechner, Server, Netzwerke, Cloud-Workloads und E-Mail-Konten von Eisbär Eis, erkennen und werten etwaige Cyberangriffe zuverlässig mithilfe von KI und Machine Learning aus und ergreifen im Fall der Fälle sofort Abwehrmaßnahmen – auch manuell bei komplexen Vorfällen. Und das alles außergewöhnlich effizient: Die rechnerische Mean-Time-to-Respond (MTTR) liegt bei gerade mal 38 Minuten – das ist 96 Prozent schneller als der Branchenstandard!

„Dies und die Möglichkeit, unsere IT-Sicherheit extern von Sophos und rund um die Uhr überwachen zu lassen, sind für uns entscheidende Vorteile", sagt Lück. „So können wir uns auf die strategische Weiterentwicklung unserer IT und die Unterstützung, Information und Schulung unserer Mitarbeitenden konzentrieren." Auf permanente Wissensvermittlung legt der IT-Leiter speziell in Fragen der IT-Sicherheit größten Wert. „Trotz aller Vorsichtsmaßnahmen geht von der E-Mail-Kommunikation immer noch die größte Bedrohung aus. Wir informieren deshalb ständig über die neuesten Phishing-Mails und schärfen durch kontinuierliche Weiterbildung das Bewusstsein unserer Kolleginnen und Kollegen zu Cyberrisiken." Das ist der wirksamste Schutz gegen Cyberkriminalität. Verstärkt wird die Resilienz gegenüber Cyberangriffen bei Eisbär Eis nun zusätzlich durch die neue, gemeinsam mit ACP realisierte ganzheitliche IT-Sicherheitslösung.

„Unser Anspruch ist es, die Geschäftsprozesse des Kunden zu verstehen. Wir möchten mit dem Kunden ein gemeinsames Zielbild haben. Mit dem Einsatz unserer IT-Security-Lösungen stärken wir die IT-Teams unserer Kunden."

Jan Köhler
Head of Network & Security,
ACP IT Solutions AG

Einfach für Sie da.

ACP IT Solutions AG

+49 40 822168600
acp.nord@acp.de
www.acp-gruppe.com