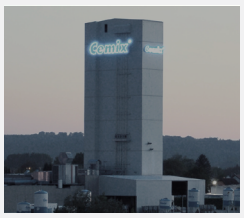
voices

CrowdStrike Kundenreferenz



lasselsbergergroup

Führender eurasischer Rohstoff-, Baustoff- und Fliesenproduzent setzt zum Schutz vor Ransomware auf moderne Cloud-basierte IT-Security

Das Familienunternehmen Lasselsberger Group ist ein eurasischer Hersteller von Rohstoffen, Baustoffen und Keramikfliesen. Klar strukturiert in die drei Divisionen Ceramics, Minerals und Building Materials, werden von den Produktionsstandorten in Zentral- und Osteuropa nicht nur die lokalen Heimmärkte, sondern auch viele internationale Märkte – vor allem in Westeuropa – beliefert.

Durch den kontinuierlichen Ausbau der Produktlieferungen an Unternehmen aus den verschiedensten Branchen (wie Glasfaser-, Papier- oder Feuerfestindustrie) entwickelt sich die Lasselsberger Group zunehmend unabhängig von der Entwicklung der Bau- bzw. Baustoffindustrie.

Marktführerschaften in vielen Bereichen, kombiniert mit jahrzehntelangen Produktionstraditionen und langfristig abgesicherten Rohstoffreserven, sichern das erfolgreiche Wachstum der gesamten Firmengruppe.

Laut Mario Hinterndorfer, Head of Group IT Infrastructure, sah sich Lasselsberger im Bereich IT-Security verschiedenen Herausforderungen gegenüber, die dringenden Handlungsbedarf nach sich zogen: „Vor CrowdStrike hatten wir nicht das Gefühl, dass wir ausreichend vor Ransomware und modernen Attacken geschützt waren. Und natürlich ist für uns nach dem Shift von einer No-Cloud-Strategie hin zu einem fast vollständigen Cloud-First-Ansatz die Cloud-Security ein sehr wichtiges Thema."

Um diese Herausforderungen zu meistern, machte sich Lasselsberger auf die Suche nach einer neuen Security-Lösung, die einen modernen Ansatz verfolgt und auf die Abwehr fortschrittlicher Angriffe hin optimiert ist. „Wir waren mit unserer alten Lösung nicht mehr glücklich. Der signaturbasierte Schutz war einfach nicht mehr zeitgemäß und wir haben sehr viel Zeit auf den Versuch verwendet, Lücken mit neuen Konfigurationen zu schließen, was jetzt dank CrowdStrike einfach per Knopfdruck geht. Zudem hatten wir zuvor keine Endoint Detection and Response (EDR), weshalb wir vieles gar nicht gesehen haben, was wir inzwischen aber beheben konnten", so Hinterndorfer weiter.

Schon früh haben Hinterndorfer und sein Kollege René Hochberger, Group IT & Process Solutions IT Support, festgestellt, dass sich auch der administrative Aufwand deutlich verringert hat. Wo zuvor mindestens ein Tag pro Woche für die Verwaltung des alten Produkts aufgewendet werden musste, beschränkt sich der zeitliche Aufwand nun auf eine Stunde pro Woche. Zudem entdeckt Lasselsberger nun auch deutlich mehr verhaltensbasierte Bedrohungen, die zuvor verborgen geblieben sind.

BRANCHE

Rohstoff-, Baustoff-, Fliesenproduktion

KONZERNZENTRALE

Pöchlarn, Österreich

HERAUSFORDERUNGEN

- Unternehmensweite Absicherung vor moderner Ransomware
- Keine Möglichkeit, blinde Flecken des veralteten, signaturbasierten AV-Produkts auszuschließen
- Hohe Anzahl von False-Positives
- Transformation von einer No-Cloud Strategie zu einem fast vollständigen Cloud-First Ansatz

LÖSUNG

Die CrowdStrike Falcon® Plattform und das CrowdStrike Falcon OverWatch™-Team bieten Lasselsberger eine umfassende IT-Sicherheitslösung, die nicht nur weniger administrativen Aufwand bedeutet, sondern auch zuverlässigen Schutz vor modernen Bedrohungen wie Ransomware bedeutet.

„CrowdStrike gibt uns das Gefühl, wichtig zu sein, sie geben uns das Gefühl, dass alles richtig eingestellt ist und sie geben uns das Gefühl, gut schlafen zu können."

René Hochberger
Group IT & Process Solutions: IT Support
Lasselsberger GmbH

voices

CrowdStrike Kundenreferenz

„Wir mussten erst lernen, dass CrowdStrike dank des signaturlosen NextGen AV anders funktioniert als unser bisheriges Produkt und wir uns dennoch darauf verlassen können, dass alles funktioniert. Wir sehen jetzt viele Dinge, wie über den Browser ausgeführte Codezeilen, die wir vorher nicht gesehen haben", erklärt Hochberger.

Lasselsberger setzt zur Abwehr moderner Bedrohungen auf Sicherheit aus der Cloud

„Der Rollout und der Wechsel von unserem alten Produkt hin zu CrowdStrike haben problemlos funktioniert", ergänzt Hinterndorfer. „Zunächst hatten wir beide Produkte parallel laufen, was auch reibungslos geklappt hat. Per Knopfdruck konnten wir dann CrowdStrike aktiv schalten und das alte Produkt deinstallieren, ganz ohne Reboot."

Der schlanke Agent von CrowdStrike war für Lasselsberger auch einer der ausschlaggebenden Gründe, warum sie sich für CrowdStrike entschieden haben. Der Agent läuft nun ausnahmslos auf allen Systemen von Lasselsberger, inklusive Produktionssystemen, auf denen zuvor aus Angst vor Produktionsstörungen durch einen Client kein Sicherheitsprodukt aufgespielt war.

Ein weiterer Punkt, der Lasselsberger im Live-Betrieb positiv überrascht hat, war die stark reduzierte Zahl an Antivirus-Ausnahmen. Wo Lasselsberger zuvor hunderte entsprechende Ausnahmen konfigurieren musste, hat sich diese Zahl mit CrowdStrike auf fünf bis zehn Stück reduziert.

Zur Unterstützung der eigenen IT baut Lasselsberger auf OverWatch

Um auch wirklich vor allen Gefahren einer modernen Bedrohungslandschaft geschützt zu sein, verlässt sich Lasselsberger nicht allein auf Technologie. Zur Ergänzung des Schutzes hat man sich für den Einsatz von CrowdStrike Falcon OverWatch™ Threat Hunting entschieden. Die Expertise der OverWatch-Experten, die Lasselsberger rund um die Uhr zur Verfügung stehen, ergänzt die Technologie und sorgt dafür, dass das Unternehmen unbesorgt in die Zukunft blicken kann.

Insgesamt hat sich die Lasselsberger Group für vier verschiedene CrowdStrike-Produkte entschieden, um gegen aktuelle und künftige Bedrohungen gerüstet zu sein. Neben Falcon OverWatch Managed Threat Hunting hat das Unternehmen noch Falcon Prevent™ NextGen AV und Falcon Insight™ EDR im Einsatz. Außerdem hat man sich für den Essential Support entschieden.

Letzterer wird auch von Mario Hinterndorfer und René Hochberger in höchsten Tönen gelobt:

„Unserer Meinung nach haben wir bei CrowdStrike den besten Support, den wir je bei einem Produkt hatten. Das Gefühl hatten wir von Anfang an. Bereits bei der Beratung und der Produktvorführung konnten alle unsere Fragen bis ins Detail hinein beantwortet werden. Und mit dem Technical Account Manager haben wir einen direkten Ansprechpartner für den Alltag, der uns hervorragend unterstützt."

ERGEBNISSE

Reduktion des administrativen Aufwands von vorher mindestens einem Tag pro Woche auf eine Stunde pro Woche

Entdeckung offener und bisher nicht bekannter Spectre/Meltdown-Lücken auf ca. 300 Geräten dank CrowdStrike

Deutlich höhere Rate entdeckter Bedrohungen, vor allem bei verhaltensbasierten Bedrohungen

ENDPUNKTE

2,500

EINGESETZTE CROWDSTRIKE-PRODUKTE

- Falcon Insight™ - Endpunktbasierte Detektion und Reaktion (EDR)
- Falcon OverWatch™ - Managed Threat Hunting
- Falcon Prevent™ - Virenschutz der nächsten Generation
- Essential Support

Start Free Trial
of Next-Gen AV

Erfahren Sie mehr unter **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches