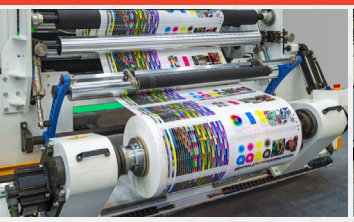
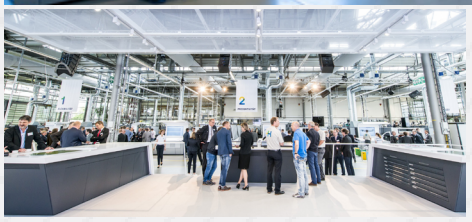
voices

CrowdStrike Kundenreferenz





HEIDELBERG

Heidelberger Druckmaschinen: Mit CrowdStrike auf Nummer sicher

Traditionskonzern schiebt IT-Security in die Cloud

Mehr als 11.500 Mitarbeiter, rund 2,4 Milliarden Euro Umsatz, 250 Standorte – was anno 1850 als kleine Glockengießerei begann, zählt heute weltweit zu den Aushängeschildern deutscher Ingenieurskunst: die Heidelberger Druckmaschinen AG. Verantwortlich für den Unternehmenserfolg ist neben den Präzisionsmaschinen seit vielen Jahren auch die Konzern-IT. Hier laufen die Fäden aus den vielen Geschäftsbereichen wie Forschung und Entwicklung, Produktion und Vertrieb zusammen. Mit "Heidelberg goes digital" begann kürzlich ein neues Hauptkapitel für den Traditionskonzern aus Baden-Württemberg: Das Fundament der Digitalisierungsstrategie – die Cyber-Sicherheit.

Die Herausforderung

„Die größte Herausforderung für die Security ist eine historisch gewachsene und entsprechend hoch komplexe IT-Landschaft und die damit verbundene fehlende Sichtbarkeit über Abläufe", erinnert sich Dr. André Loske an das ambitionierte IT-Sicherheits-Projekt, das Ende 2019 startete. Ziel war es in erster Linie, mit Hilfe eines ganzheitlichen Security-Systems eine bessere Transparenz zu schaffen, um schnell handeln zu können. Dabei ging es nach den Worten des Chief Information Security Officer (CISO) bei der Heidelberger Druckmaschinen AG neben der Reaktionsfähigkeit unter anderem auch darum, „in Richtung Digitalisierung mit Collaboration, Mobile Workstyles und Cloud-Computing aufzubrechen".

Dr. Loske konkretisiert: „Es war alles andere als trivial, ein neues Sicherheitskonzept für unsere insgesamt rund 12.000 Clients und etwa 2.000 Server ins Leben zu rufen." Dies galt nicht zuletzt auch deshalb, weil die Systeme des Konzerns zu jener Zeit nicht zentral verwaltet werden konnten. Hinzu kamen rechtliche Rahmenbedingungen, die bei der Implementierung einer neuen umfassenden Sicherheitsstrategie berücksichtigt werden mussten, um beispielsweise die EU-Datenschutzgrundverordnung (EU-DSGVO) und Gesetze zum Schutz von Geschäftsgeheimnissen erfüllen zu können.

BRANCHE

Produzierendes Gewerbe

STANDORT/ KONZERNZENTRALE

Heidelberg, Deutschland

HERAUSFORDERUNGEN

- Proaktives Erkennen und Reagieren auf Bedrohungen
- Entwicklung einer ganzheitlichen, zentral verwalteten Sicherheitsstrategie
- Maximierung der Wirkung des IT-Security Teams

LÖSUNG

Heidelberger Druckmaschinen setzt CrowdStrike Falcon® ein, um den Einblick in komplexe, heterogene IT-Landschaften zu verbessern und effiziente Prozesse zur Sicherung der weltweiten Infrastruktur einzurichten

„Es war alles andere als trivial, ein neues Sicherheitskonzept für unsere insgesamt rund 12.000 Clients und etwa 2.000 Server ins Leben zu rufen."

„Vor der Implementierung hatten wir den Fokus auf Prävention, heute erkennen wir Dinge und können reagieren. Das ist im Zeitalter mit Cloud-Computing und mobilen Endgeräten essenziell geworden. Ich kann CrowdStrike deshalb vorbehaltlos empfehlen."

Dr. André Loske
Heidelberger Druckmaschinen, CISO

voices

CrowdStrike Kundenreferenz

Die Implementierung

Dr. Loske geht ins Detail: „Wir hatten vorher eine klassische Antivirenlösung. Doch ein großes Problem hing mit unserer heterogenen IT-Topologie zusammen: die fehlende Sichtbarkeit." So mangelte es dem IT-Sicherheits-Verantwortlichen zufolge beispielsweise an technischen Möglichkeiten, um Sicherheitsbedrohungen rechtzeitig erkennen und schnell genug auf unterschiedliche Bedrohungen reagieren zu können: „Was man nicht sieht, kann man schließlich auch nicht bekämpfen."

Gründe genug für Dr. Loske und sein IT-Team, eine Evaluierung für den Austausch der bis dato verwendeten Antivirenlösung anzustoßen. „Wir haben viele Lösungen angesehen und uns schließlich für CrowdStrike Falcon entschieden, obwohl es im oberen Preissegment angesiedelt ist." Grund dafür war in erster Linie der Cloud-basierte Endgeräteschutz des marktführenden Cybersecurity-Anbieters, berichtet Dr. Loske. Hier überzeugte vor allem die so genannte Shared Threat-Intelligence. „Es bringt einen echten Mehrwert für die Sicherheit, dass man sich zusammen mit anderen Unternehmen in einem Threat-Intelligence-Netzwerk befindet. Kaum gibt es irgendwo einen Angriff auf ein System eines Unternehmens innerhalb des Netzwerks, sind unsere System auch schon immun dagegen. Das ist ein echter Game Changer in der Security und hat uns zu CrowdStrike gebracht."

Um auch bei der Auswahl auf Nummer sicher zu gehen, hatten die IT-Verantwortlichen im Rahmen eines Proof of Concept eine Pilotphase mit 200 Usern gemacht und CrowdStrike Falcon auf Herz und Nieren geprüft: „Wir hatten gewisse Vorbehalte, weil mit anderen Sicherheitslösungen in der Vergangenheit die eine oder andere Falschmeldung aufgetreten war", räumt Dr. Loske ein. „Hier gab es aber keinerlei Probleme." Aufgrund der durchweg positiven Erfahrungen begannen die IT-Profis kurz darauf, den Falcon Sensor auf 9700 weiteren Geräten in Betrieb zu nehmen. „Auch in komplizierten Umgebungen wie in unserer Forschungs- und Entwicklungsumgebung mit viel Spezialsoftware und selbst gestrickten Lösungen hat die Integration von CrowdStrike Falcon überraschend gut funktioniert. Hätten wir gewusst, dass alles so reibungslos läuft, hätten wir uns den großen Test gespart."

Die Vorteile

„Wichtig ist vor allem, dass wir jetzt über eine echte Transparenz über alle Geräte hinweg verfügen, um Cyberkriminalität aktiv bekämpfen zu können", so der Security-Verantwortliche weiter. Das sei vor allem deshalb wichtig, weil in den weltweit 250 Standorten nicht überall und jederzeit das benötigte IT-Personal vorhanden ist. Konkret ist das Unternehmen nun in der Lage, einzelne Rechner am jeweiligen Standort zu isolieren und forensisch zu untersuchen, bevor Spezialisten überhaupt an den Ort des Geschehens geschickt werden mussten. Dr. Loske: „Das Werkzeug von CrowdStrike ist sehr mächtig. Man kann sehr viel sehen, was da in den Systemen der Mitarbeiter vor sich geht. Daher wurde der Einsatz im Vorfeld mit dem Betriebsrat abgestimmt." Auch der hohe Grad an Automatisierung war ein wichtiger Entscheidungsgrund für die Lösung von CrowdStrike. Weil das Unternehmen Dr. Loske zufolge nicht über sehr viele dedizierte Security-Mitarbeiter verfüge, sei man darauf angewiesen, dass Prozesse automatisiert ablaufen. Die CrowdStrike Falcon Lösung ließ sich nahtlos in das neue Security-Information-and-Event-Management-(SIEM)-System der HDM integrieren. Somit haben die IT-Wächter einen ganzheitlichen Blick auf die IT-Sicherheit, indem Meldungen und Logfiles sämtlicher Systeme zur Analyse konsolidiert werden.

Dr. Loskes Fazit: „Wir sind nunmehr in der Lage, rasch zu handeln, wenn es einen Sicherheitsvorfall gibt." Mit CrowdStrike habe die Heidelberger Druckmaschinen AG im Bereich der IT-Sicherheit regelrecht einen Paradigmenwechsel vollzogen: „Vor der Implementierung hatten wir den Fokus

ENDPUNKTE

CROWDSTRIKE-PRODUKTE

- Falcon Prevent™ Antivirus der nächsten Generation
- Falcon Insight™ Endgeräteerkennung und Abwehr
- Falcon Discover™ IT-Hygiene
- Falcon Device Control™
- Falcon Firewall Management™
- Falcon Spotlight™ Vulnerability Management

voices

CrowdStrike Kundenreferenz

auf Prävention, heute erkennen wir Dinge und können reagieren. Das ist im Zeitalter mit Cloud-Computing und mobilen Endgeräten essenziell geworden. Ich kann CrowdStrike deshalb vorbehaltlos empfehlen."

ÜBER CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon® verfügt über eine einzigartige, Cloud-basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 3 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweitfortschrittlichsten Datenplattformen für Cyber-Sicherheit.

Mit CrowdStrike profitieren Kunden von besserem Schutz, besserer Leistung und sofortiger Time-to-Value – und das alles auf der cloud-nativen Falcon-Plattform.

Über CrowdStrike sollten Sie vor allem eines wissen: Wir stoppen Datendiebstahl.

Testen Sie jetzt kostenlos
den Virenschutz der nächsten Generation

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

CROWDSTRIKE

we stop breaches