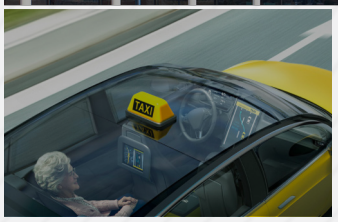

CrowdStrike bei TDK Electronics: Hersteller für elektronische Bauelemente macht Cloud zum Security-Hotspot

“Vorbildliche IT-Security und bester Support”

TDK Electronics hat das Thema IT-Sicherheit zur Chefsache erklärt. Kein Wunder: Für das Unternehmen mit hochkarätigen Kunden vor allem aus der Automobil- und Industrieelektronik ist für Cyber-Angriffe verschiedenster Art kein Platz. Dafür sorgt die cloudbasierte Lösung von CrowdStrike.

Die Herausforderung

„Die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität haben für unseren Vorstand absolute Priorität. Schließlich müssen wir als zuverlässiger Lieferant von elektronischen Bauelementen und Systemen für Branchen wie die Automobilindustrie eine sehr hohe IT-Sicherheit garantieren können“, kommt Thomas Zeulner, Information Security Officer bei TDK Electronics, München, rasch zum Punkt. Hinzu kämen neue gesetzliche Regularien wie die EUDSGVO, weshalb das Thema IT-Security beim ISO 9001-zertifizierten Unternehmen mit rund 20 Entwicklungs- und Fertigungsstandorten weltweit von sehr hoher Priorität ist.

Zeulner blickt zurück: „Der letzte Herstellerwechsel bei der Antivirensoftware liegt sieben Jahre zurück. Diese Lösung erfüllt die gestiegenen Anforderungen heute nicht.“ So seien in den letzten Jahren immer häufiger auch Anwender mobiler Endgeräte wie Tablets oder Smartphones ins Visier von Cyberkriminellen geraten. Gleichzeitig wurden die Schadsoftware und Angriffsmethoden auf die Clients und Server des Konzerns immer ausgefeilter. „Die Gefahr für unsere IT-Infrastruktur hat merklich zugenommen“, so der IT-Sicherheitsverantwortliche von TDK Electronics. Deshalb hatte man sich bei dem Elektronikhersteller dazu entschieden, in Sachen Endgerätesicherheit einen Produktwechsel einzuleiten. „Wir hatten im Lauf der Zeit unterschiedliche Produkte im Einsatz, mussten aber feststellen, dass diese Lösungsansätze uns nicht mehr weiterbrachten.“ Gefragt war eine Lösung, deren technisches Kernstück auf Künstlicher Intelligenz (KI) basiert, denn: „Eine KI

BRANCHE
Elektronik

STANDORT/ KONZERNZENTRALE
München, Deutschland

CHALLENGES
- Erkennung und Prävention von Angriffen
- Minderung der Komplexität im Security Stack
- Verringerung der False Positives

LÖSUNG
TDK Electronics verwendet die CrowdStrike Falcon®-Plattform, um die weltweite Umgebung vor ausgeklügelten Angriffen zu schützen und die Sicherheitsverwaltung zu vereinfachen

„Eine KI muss nicht auf Sicherheits-Updates warten.“

„Ich kann nun einfach einen Client vom Netzwerk isolieren, wenn er auffällig ist, und analysieren, was da vor sich geht.“

Thomas Zeulner
Information Security Officer
bei TDK Electronics

muss nicht auf Sicherheits-Updates warten."

Fündig wurde das Unternehmen relativ schnell. Der Haken: „Mit der bislang eingesetzten Lösung waren wir gezwungen, zwei Produkte – also den Antivirenschutz und die KI-Lösung – mit unterschiedlichen Konsolen zu betreiben. Das bedeutete, dass unsere Administratoren auch zwei Lösungen verstehen, unterschiedliche Dashboards bedienen und auch noch etwaige Angriffe identifizieren mussten." Problematisch waren laut Zeulner nicht zuletzt die „hohen False-Positive-Raten, speziell im Zusammenhang mit der Entwicklung elektronischer Bauelemente."

Die Implementierung

Vor diesem Hintergrund startete TDK Electronics einen neuen Evaluierungsprozess. Das Rennen machte CrowdStrike: Die Endpoint-Sicherheitslösung deckt alle Aspekte der IT-Sicherheit auf Clients und Servern ab und kombiniert KI-Ansätze, Verhaltensanalytik, Schwachstellen-Prävention und IT-Hygiene mit einer cloudgestützten EDR-Lösung. „Wir haben im Dezember 2019 ein Proof of Value mit CrowdStrike auf den ersten 700 Rechnern durchgeführt. Besonders wichtig war uns dabei die Integration in unsere Zwei-Faktor-Authentifizierung, um unsere mehrstufige Sicherheitsstrategie flächendeckend erreichen zu können." Geprüft wurde auch das granulare Rechtemanagement für die weltweiten Administratoren, mit dem Zugriffe rollenbasiert gewährt werden. „Auch das hat CrowdStrike mit Bravour bestanden", so Zeulner. Gleiches galt für die False Positives, die während des Proof of Value wesentlich niedriger ausgefallen waren als mit dem Konkurrenzprodukt aus der Vergangenheit.

Überzeugt war der Information Security Officer schließlich auch vom SensorSoftware Agent der CrowdStrike-Falcon-Plattform, als es im Februar 2020 um das weltweite Deployment auf insgesamt 12.000 Endgeräten bei TDK Electronicss ging – und das innerhalb einer Woche. „Die Client-Komponente ist extrem schlank und beeinträchtigt die Performance der Systeme nicht. Außerdem wird sehr wenig Bandbreite benötigt, um die Software großflächig zu verteilen." Die cloudnative Lösung erreicht nicht nur die verschiedenen Standorte von TDK Electronics, sondern auch alle Mitarbeiter im Home-Office wesentlich schneller und problemloser, als das innerhalb einer On-Premises-Infrastruktur möglich gewesen wäre. „Ich kann nun einfach einen Client vom Netzwerk isolieren, wenn er auffällig ist, und analysieren, was da vor sich geht."

Die Vorteile

Heute verfügt TDK Electronics über eine umfassende IT-Sicherheitslösung, die wesentlich weniger Administrationsaufwand benötigt als die in der Vergangenheit verwendeten Lösungen. Konkret schätzt der IT-Security-Verantwortliche, mit CrowdStrike rund 25 Prozent der Zeit einsparen zu können, die für die Verwaltung von Rechnern sonst aufgewendet worden wäre. Zeulners Resümee: „Die neue Lösung bietet uns viele Vorteile und höchstmögliche IT-Security Auch mit dem Support sind wir überaus zufrieden."

ERGEBNISSE

Geschätzte 25% Zeitersparnis bei der Verwaltung der IT-Sicherheit

ENDPUNKTE

CROWDSTRIKE-PRODUKTE

- Falcon Insight™ Endgeräteerkennung und Abwehr
- Falcon Prevent™ Antivirus der nächsten Generation
- Falcon OverWatch™ managed threat hunting
- Falcon Intelligence ™

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.**

Testen Sie jetzt kostenlos
den Virenschutz der nächsten Generation

Erfahren Sie mehr unter www.crowdstrike.de

CROWDSTRIKE