CYBERSPRINT
BREAKTHROUGH SECURITY

ANWENDUNGSFALL

FUSSABDRUCK-MAPPING BEI IFM ELECTRONICS

INTERVIEW MIT KEVIN KAMPETER, IT-SICHERHEITSSPEZIALIST DER IFM ELECTRONIC GMBH

Kevin Kampeter

Q **Kevin, würden Sie sich zunächst vorstellen und uns von ifm erzählen?**

A “Ja, klar. Ich bin ein echter Techie. In früheren Jobs habe ich als Programmierer für Virtual-Reality-Funktionen bei Bauprojekten und als IT-Sicherheitsberater gearbeitet.

Ich hatte schon immer Interesse an den Möglichkeiten von Technologien, wie man sie richtig programmiert, und auch daran, welche Wege es zur Absicherung gibt.

Ich kam vor zwei Jahren als IT-Sicherheitsspezialist zur ifm — die Rolle, die ich auch heute noch ausübe. Die ifm electronic gmbh ist ein deutscher Hersteller von Industriesensoren. Vor 50 Jahren von zwei Freunden gegründet, sind die Eigentümer inzwischen die jeweiligen Söhne. Trotz der Organisationsgröße (7.300 Mitarbeiter in 95 Ländern) ist das Wesen eines Familienunternehmens nach wie vor in unserer Unternehmenskultur verankert.

Die Sensoren, die wir produzieren, findet man in den unterschiedlichsten Industrien, Branchen und Maschinen, z. B. in der Luft- bzw. Raumfahrt, der Automobilindustrie, in Haushaltsgeräten, der automatischen Autowäsche, in Rennwagen usw.”

Q **Wie spiegelt sich aus Ihrer Sicht die Geschäftstätigkeit der ifm in Ihren Aufgaben wider?**

A “Da ifm zahlreiche Märkte bedient, ist auch unsere Online-Reichweite und -Präsenz sehr stark. Dazu gehören die länderspezifischen Webseiten aller Geschäftsbereiche sowie deren lokale Lieferanten und andere Drittparteien. Ich bin für die IT-Sicherheit der gesamten Organisation und aller Tochtergesellschaften verantwortlich.

Ich versuche, die Kontrolle über so viele Aspekte unserer digitalen Umgebung wie möglich zu behalten. Das bedeutet, dass ich Herausforderungen selbst und mit den richtigen Kollegen angehe. Zu meinen Aufgaben gehören darüber hinaus die Erstellung von Sensibilisierungskampagnen unter den Mitarbeitern, SOC-bezogene Aufgaben wie die Verhinderung und Eindämmung von Datenlecks und anderen Vorfällen sowie die Überwachung und Steuerung unserer Online-Assets. Schließlich kümmere ich mich auch um die Berichterstattung über unsere Sicherheitsabteilung (inkl. Ereignismanagement) an die oberste Führungsebene.”

Q **Als Sie bei ifm anfingen, was waren Ihre ersten Erfahrungen und Prioritäten?**

A “Als ich anfing, gab es mein Team noch nicht. Wir wollten uns einen Überblick über unseren Online-Fußabdruck verschaffen und einen Zielkatalog für unsere Cyber-Sicherheit setzen, was jedoch leichter gesagt als getan war. Bei so vielen Mitarbeitern hatten Leute aus verschiedenen Teams die Online-Umgebung für ihre eigenen Zwecke erweitert. Da solche Aktivitäten nicht immer den IT-Teams gemeldet wurden, bestand unsere größte Herausforderung darin, eine Bestandsaufnahme der ifm-Online-Assets mit den entsprechenden Servern zu machen und festzustellen, wer für die Assets verantwortlich ist. Angesichts der Organisationsgröße und der umfangreichen Schatten-IT wäre es jedoch zu zeitaufwändig und ineffektiv, unseren Online-Fußabdruck von Hand zu analysieren.”

Q **Was haben Sie getan, um die Aufgabe zu erledigen?**

A “Wir selbst konnten diese Herausforderung mit unseren gegebenen Ressourcen nicht bewältigen. Daher brauchten wir ein Werkzeug, mit dem wir unsere Assets automatisch und schnell erkennen können. Die Ausgangspunkte waren die Ermittlung unseres Online-Fußabdrucks, wo die Sicherheit verbessert werden musste und wer die Kontrolle über die Assets hatte.

In der Folge sind wir auf Cybersprint aufmerksam geworden. Wir haben uns für diese Digital Risk Protection-Plattform entschieden, weil sie uns genau die Werkzeuge bereitstellt, die wir für unser Vorhaben benötigten. Und da wir diese so schnell wie möglich nutzen mussten, waren wir froh, dass die Plattform keine Installation erforderte. Da die Software über die Cloud läuft, war sie innerhalb von Minuten einsatzbereit. Ich habe noch nie zuvor erlebt, dass eine ähnliche Software so schnell genutzt werden kann.”

Q **Welche Erfahrungen haben Sie mit der Plattform und dem Service von Cybersprint gemacht?**

A “Da ich es vorziehe, die Kontrolle über die Assets selbst zu behalten, bin ich mit der 24/7-Verfügbarkeit der Plattform sehr zufrieden. Die Software zeigt mir deutlich, welche Assets Teil unseres Fußabdrucks sind, wie die individuelle Sicherheitseinstufung aussieht und eventuelle Schwachstellen abgestellt werden können — ohne den Prozess zu stören.

Zuerst waren die Ergebnisse ziemlich überwältigend. Als wir anfingen, mit der Plattform zu arbeiten, fand sie wesentlich mehr Assets als erwartet — über tausend Stück, die wir durchkämmen mussten. Anhand der Bewertung des

Sicherheitsrisikos pro Asset konnten wir jedoch feststellen, welche Teile des Fußabdrucks wir zuerst angehen mussten. Wir kombinierten diese Erkenntnisse mit unserer Sicht auf die wichtigsten Teile der ifm-Infrastruktur. Schließlich machten wir uns zuerst an die Sicherung unserer Hauptdomain ifm.com, dann an die Sicherung unserer Vertriebsplattform und arbeiteten uns von dort aus weiter."

Q **Haben Sie rückblickend auf diesem Weg versteckte Herausforderungen oder Lösungen entdeckt?**

A "In der Anfangsphase der Implementierung war die persönliche Unterstützung von Cybersprint besonders wertvoll. Während regelmäßiger Videoanrufe half mir mein Ansprechpartner bei der Datenanalyse und gab mir Tipps für den Umgang mit der Plattform. Er zeigte mir, wie mehrere Assets tatsächlich Teil einer einzigen URL waren, die auf vier verschiedene Arten geschrieben wurde: "http", "https", mit "www" und ohne "www". Dies half uns bei der Lösung eines Problems, von dem wir vorher nicht wussten, dass wir es hatten.

Außerdem planten wir bei der Formulierung unserer Hauptaufgaben die nächsten Schritte auf der Grundlage der Scan-Ergebnisse. Welche Assets würden wir selbst verwalten, oder welche zusätzlichen Informationen würden wir benötigen? Als neuer Mitarbeiter wusste ich jedoch nicht, zu welchen Teilen der Organisation die jeweiligen Assets gehörten oder in welchem Stadium des Verbesserungsprozesses sich bestimmte Schwachstellen befanden. Anstatt mit verschiedenen Teams und Geschäftsbereichen Kontakt aufnehmen zu müssen, konnte ich die Ergebnisse anhand der detaillierten Informationen pro Asset selbst strukturieren und jede einzelne mit einem individuellen Schlagwort versehen. Diese Funktion verwende ich auch heute noch. Ich habe etwa 25 Tags erstellt, z. B. "überprüft", "abzuschalten" usw. Da die Plattform unsere Assets rund um die Uhr und 7 Tage die Woche überwacht, kann ich das Schlagwort je nach letztem Suchlauf ändern.

Insgesamt haben mir die Plattform und der Service von Cybersprint sehr geholfen, den Online-Fußabdruck der ifm abzubilden und die Erkenntnisse zu gewinnen, die ich für meine tägliche Arbeit benötige. Ich kann auf die technischen Analysen der Plattform aufbauen, um unsere Cyber-Abwehr zu stärken und die erforderlichen Informationen bei der Erstellung eines Berichts zu isolieren."

BESUCHEN SIE CYBERSPRINT.COM/RESOURCES FÜR WEITERE ANWENDUNGSFÄLLE, WHITEPAPER, WEBINARE UND MEHR.