KVC Health Systems
people matter

KVC HEALTH SYSTEMS BESEITIGT E-MAIL-SICHERHEITSVORFÄLLE MIT VADE SECURE FOR MICROSOFT 365

Die Einführung von Vade Secure for Microsoft 365 führte zu einer 15% Verbesserung gegenüber früheren Lösungen.

ÜBER KVC HEALTH SYSTEMS

KVC Health Systems ist eine private, gemeinnützige Organisation mit 35 Standorten, verteilt über Kansas City, Kentucky, Missouri, Nebraska und West Virginia. KVC Health Systems wurde 1970 gegründet und bietet verhaltensbasierte Gesundheitsfürsorge, Kinderfürsorge, Gesundheits- und Wellnessdienste für Gemeinden sowie Gesundheitsberatung für private und staatliche Organisationen.

DIE HERAUSFORDERUNG

Mit 1.600 Mitarbeitern und der Unterstützung von 63.000 Kindern und Familien, die über fünf Staaten verteilt sind, erkannte KVC Health Systems (KVC), ein attraktives Ziel für Cyberkriminelle zu sein. „Gesundheitsdaten bringen die höchsten Einnahmen auf dem offenen Markt“, so Erik Nyberg, Vice President der IT bei KVC. „Es wäre schädlich für unseren Ruf - wenn nicht für unsere Organisation -, wenn eine Leckage dieser Informationen stattfinden würde.“

Vor Ende 2018 hatte KVC eine Fülle von Phishing- und Spear-Phishing-E-Mails erhalten. Nach der Migration auf Microsoft 365 nahmen die E-Mail-Angriffe exponentiell zu. „Unsere Führungskräfte schickten mir einmal pro Woche eine E-Mail über etwas, das durchgekommen war“, so Nyberg. „Es war schon immer ein Problem, stieg aber nach dem Wechsel auf Microsoft 365 stets weiter an“.

In den Vorjahren konzentrierten sich die E-Mail-Angriffe auf die C-Suite von KVC, aber wie bei vielen Unternehmen änderte sich dieser Trend. „Unsere Führungskräfte haben jetzt alles gesehen“, so Nyberg „Auf viel fallen sie nicht mehr rein.“ Heute, so Nyberg, kundschaften Hacker KVC über Social Media und andere Online-Daten aus, um Mitarbeiter zu finden, die Zugang zu den Systemen des Unternehmens haben, wie Finanzen, Personal und Sicherheit.

Zusätzlich zu den unspektakulären Phishing-E-Mails erhielt KVC äußerst anspruchsvolle, zielgerichtete Phishing- und Speer-Phishing-E-Mails, die konzipiert waren, um die Mitarbeiter in dem Unternehmen direkt anzusprechen. „Das Leitbild unseres gesamten Unternehmens ist es, Menschen zu helfen“, so Nyberg. „Mit einer E-Mail, die mit einer Bitte um Hilfe kommt, könnten die bösen Jungs eine viel höhere Erfolgsrate haben.“

Trotz der Verwendung einer Vielzahl von E-Mail-Sicherheitsprodukten im Laufe der Jahre hatte keine dieser Lösungen eine ausreichende Fangquote, um Microsoft 365 zu schützen. „Ich war noch nie zufrieden mit einer E-Mail-Sicherheitslösung“, so Nyberg. „Etwas, das 80% der Angriffe aufhält, ist einfach nicht gut genug“.

WARUM SICH KVC FÜR VADE SECURE ENTSCHIEDEN HAT

- ✓ Verbesserte Fangrate
- ✓ Einfache Inbetriebnahme:
- ✓ Native Integration:
- ✓ Vereinfachtes E-Mail-Management

DER MEHRWERT VON VADE SECURE FOR MICROSOFT 365

In den letzten drei Monaten blockierte Vade Secure fast 18.000 an KVC-Mitarbeiter gerichtete E-Mail-Bedrohungen.

Bedrohungsart	Gesamte Bedrohungen, die von Vade Secure erkannt wurden.
Phishing	2,751
Spear-Phishing	593
Malware	145
Spam	13,138
Scam	1,266
Gesamt	17,893

Von diesen 18.000 Bedrohungen blockierte Vade Secure fast 5.600, die EOP durchgehen ließ.

Bedrohungsart	Einzigartige Bedrohungen, die von Vade Secure erkannt wurden.
Phishing	714
Spear-Phishing	243
Malware	31
Spam	4,435
Scam	175
Gesamt	5,598

DIE LÖSUNG

KVC war bewusst, dass sie eine neue Lösung benötigten, aber sie waren nicht der Ansicht, dass es ein E-Mail-Sicherheitsprodukt auf dem Markt geben würde, das den Schutz von Microsoft 365 deutlich verbessern könnte. „Ich war mit allen Produkten da draußen vertraut, und ich wusste, dass keines die 80-90-prozentige Fangrate überschritt." Nach einem Gespräch mit Vade Secure vereinbarte Nyberg, ein Proof of Concept (POC) mit Vade Secure for Microsoft 365 zu starten. „Sie sagten, sie lägen über 90 Prozent", so Nyberg. „OK", sagte ich. „Zeigen Sie es mir".

Vade Secure for Microsoft 365 ist eine KI-basierte E-Mail-Sicherheitslösung, die nativ in Microsoft 365 integriert ist. Im Gegensatz zu sicheren E-Mail-Gateways befindet sie sich innerhalb des Microsoft 365-Gefüges und ergänzt Microsoft Exchange Online Protection (EOP), ist aber für Benutzer transparent und für Cyberkriminelle unsichtbar.

Die Anti-Phishing-Technologie von Vade Secure for Microsoft 365 nutzt künstliche Intelligenz, einschließlich maschinellen Lernens (beaufsichtigt und unbeaufsichtigt) und tiefen Lernens (Computer Vision), um URLs und Webseiten in Echtzeit zu durchforsten. Durch die Analyse von Herkunft, Inhalt und Kontext von E-Mails und Webseiten erkennen maschinelle Lernmodelle ausgefeilte Verschleierungstechniken, mit denen Cyberkriminelle E-Mail-Filter umgehen, einschließlich der Erstellung von URL-Aliasen mit Verkürzern, der Umleitung legitimer Webseiten auf Phishing-Seiten, der Änderung von Markenlogos und der Fälschung von E-Mail-Adressen.

Um Spear-Phishing-Angriffe zu blockieren, identifizieren unbeaufsichtigte Anomalieerkennung und natürliche Sprachverarbeitung Muster und Anomalien, die in Spear-Phishing-E-Mails vorkommen, und warnen den Benutzer mit einem anpassbaren Banner.

Um die Bedrohungserkennung zu verbessern und die Belastung durch Ermittlungen und Vorfallsreaktionen zu verringern, ist Vade Secure for Microsoft 365 mit Auto-Remediate ausgestattet. E-Mail-Bedrohungen, die den Filter ursprünglich umgangen haben, werden automatisch aus den Posteingangsfächern entfernt und in einen vom Administrator festgelegten Ordner verschoben. Während die KI-Engine weiter lernt, verbessert sie sich auf der Grundlage von Benutzerfeedback und Bedrohungsinformationen.

DIE ERGEBNISSE

Das Fangvolumen in Vade Secure for Microsoft 365 überraschte Nyberg. „Vade Secure erreicht derzeit eine Fangrate von 90 bis 95 Prozent. Ich hätte nicht gedacht, dass es da draußen ein Produkt gibt, das hierzu fähig ist". Außerdem erfasst Vade Secure for Microsoft 365 eine große Anzahl von E-Mails, die die native Microsoft 365-E-Mail-Sicherheit umgehen. Im Jahr 2019 entdeckte Vade über einen Zeitraum von drei Monaten fast 5.600 E-Mail-Bedrohungen, welche EOP umgangen hatten.

Ein weiterer Motivationsfaktor für die Einführung des Produkts war die native Integration mit Microsoft 365 und die einfache Inbetriebnahme sowie die schnelle Einrichtung und einfache Benutzeroberfläche. „Wir mögen die Einfachheit von Vade auf der IT-Seite definitiv", so Nyberg. In Microsoft 365 zur Whitelist- oder Blacklist-Administration zu gehen, ist ein extrem mühsamer, 10-15-minütiger Prozess. Mit Vade dauert es fünf Sekunden. Vade ist 90 Prozent einfacher als Microsoft 365 zu benutzen."

In den neun Monaten seit der Inbetriebnahme von Vade Secure for Microsoft 365 hat KVC schließlich keinen ernsthaften E-Mail-Angriff mehr erlebt, der das Unternehmen betraf. „Die meisten Jahre", so Nyberg, „kamen mindestens ein bis zwei Phishing-Angriffe oder Versuche durch. Seit ich mit Vade online gehe, habe ich keine kritischen E-Mail-Situationen."

> *Die Fangrate von Vade Secure for Microsoft 365 stellt eine 15%ige wenn nicht sogar höhere Verbesserung gegenüber jedem anderen E-Mail-Filter dar, den ich jemals gesehen habe. Vade fängt ein, was Microsoft entwischt.*
>
> **Erik Nyberg, Vice President, IT**