Software-Testing-Pionier versperrt den auf C-Level spezialisierten Angreifern den Zugang.

Sentinel wehrt Spear-Phishing- und Fraud-Angriffe auf Führungskräfte mittels KI ab und lässt IT-Team nachts ruhig schlafen.

TRICENTIS

Ein buchstäblicher Weckruf

Andreas Gross wird kurz nach Mitternacht von seinem Handy aus dem Schlaf geklingelt. Er war nicht überrrascht, als er sich im Gespräch mit einer Führungskraft seines Unternehmens befand. Die Führungskraft machte sich Sorgen, mit dem Öffnen einer verdächtigen E-Mail einen Fehler begangen zu haben.

Es war nicht der erste Anruf dieser Art, und Andreas Gross bezweifelte, dass es der letzte war. Als VP der IT-Abteilung von Tricentis hat er eine Welle ausgefeilter, stark zielgerichteter, Spear-Phishing-Angriffe – vorwiegend auf C-Level-Führungskräfte – erlebt. Bislang konnten diese abgewehrt werden. Doch Andreas Gross weiß, dass es nur eine Frage der Zeit ist.

Tricentis ist ein global führender Anbieter von Continuous-Testing-Tools für Agile- und DevOps-Teams. Zu seinen Kunden zählen einige der größten, technisch hochentwickeltsten Unternehmen der Welt. Die potenziellen Kosten eines erfolgreichen Hacker-Angriffs auf kritische, hochvertrauliche Kundendaten sind nicht abschätzbar. Andreas Gross weiß, dass die E-Mail-Security von Tricentis verbessert werden muss.

Profil

- Sitz in Wien, Österreich
- Niederlassungen in EMEA, APAC und Nordamerika
- Weltmarktführer für automatisiertes Continous Testing für Software- und DevOps

Herausforderungen

- Vermehrt Spear-Phishing-Angriffe auf Führungskräfte
- Erweiterung des Security- Umfangs des neu eingeführten Office 365

Lösung

- Barracuda Sentinel
- Barracuda Essentials for Office 365
- Barracuda Message Archiver

Ergebnisse

- Reduziertes Risiko für C-Suite- und andere Mitarbeiter vor Account Takeover- und Spear-Phishing-/Whaling-Angriffen
- Schutz vor Domain-Spoofing
- 200%ige Steigerung der Spam-Erkennung
- Verbesserte Compliance durch revisionssichere E-Mail-Archivierung

Erhöhung der Office 365 Security

Tricentis ist im Rahmen umfangreicher Cloud-Investitionen früh auf Microsoft Office 365 umgestiegen. „Die Security-Funktionen von Microsoft Office 365 sind in Ordnung, aber wir benötigten ein höheres Maß an Schutz“, erklärt Andreas Gross. „Wir waren gerade dabei, unsere Security-Systeme zu verbessern, um das Risiko zu senken.“

Als der Ansturm von Spear-Phising-Angriffen sich weiter erhöhten, wendete sich Andreas Gross an einen vertrauenswürdigen Security-Berater, der ihm empfahl sich die Barracuda Lösungen anzusehen.

> „Wir prüften auch Produkte von Mimecast und Proofpoint, hatten aber von Beginn an den Eindruck, dass Barracuda Essentials die robusteren Security-Funktionen bietet.“
>
> **Andreas Gross**
> VP IT
> Tricentis

Die persönliche Note

Als Andreas Gross und ein paar seiner Teammitglieder geschäftlich in San Francisco zu tun haben, arrangiert Barracuda ein Treffen in seinem Hauptsitz in Campbell, CA. „Allein die Tatsache, dass Barracuda so schnell reagierte, war beeindruckend“, erklärt Gross. „Wir trafen uns mit leitenden Technikern und Produktmanagern, und es war sofort klar, dass sie sich stark auf unsere speziellen Bedürfnisse konzentrierten. Diese Aufmerksamkeit hat uns sehr viel bedeutet.“

Barracuda veranlasst umgehend eine Proof-of-Concept Demoinstallation mit Essentials for Office 365 und unterstützt das Tricentis Team bei der Optimierung der Einstellungen. Aufgrund des speziellen Spear-Phishing-Problems von Tricentis schlugen die Berater zusätzlich Barracuda Sentinel vor, eine Lösung, welche mit künstlicher Intelligenz Anomalien des Kommunikationsflusses erkennt und darauf reagieren kann.

Barracuda führt zunächst einen Email Threat Scan durch. Der kostenlose öffentliche Service überprüft Office 365-Postfächer mit Sentinel-Technologie auf schädliche E-Mails. „Das war ernüchternd“, erklärt Andreas Gross. „Uns war gar nicht bewusst, wie viele potenzielle Bedrohungen völlig unerkannt in unseren Posteingängen schlummerten. Sentinel hat uns schnell als Anti-Phishing-Lösung überzeugt.“

Ergebnisse und Erkenntnisse

„Wir testeten Barracuda Essentials und Sentinel zusammen, was extrem gut funktionierte. Die vollständige Einführung in die Produktion ging sehr schnell. Speziell Sentinel ließ sich in nur zwei Stunden einrichten. Die Produktexperten von Barracuda waren dabei eine große Hilfe. Zusätzlich haben wir Barracuda Message Archiver implementiert. Mit dem ausfallsicheren Audit- und Discovery-Prozess für E-Mails können wir unsere behördlichen Auflagen erfüllen.“

Der Einsatz von Barracuda zeigt sofort Wirkung. Phishing-, Fraud- und Account Takeover-Angriffe gingen schlagartig zurück, während sich die allgemeine E-Mail-Security deutlich verbesserte. Das IT-Team verzeichnet zudem eine 200% verbesserte Erkennung bösartiger E-Mails.

> „Essentials und Sentinel sind zusammen eine echt starke Kombination.“
>
> **Andreas Gross**
> VP IT
> Tricentis

„Meine C-Level-Kollegen klingeln mich jetzt nachts nicht mehr wegen echter oder vermeintlicher Angriffe aus dem Schlaf. Sentinel liefert uns außerdem einen erheblich transparenteren Einblick in die Domain-Einstellungen der Organisation. Wir können dadurch die Integrität unserer E-Mail-Kommunikation besser sicherstellen.“ Andreas Gross und sein Team waren auch von der persönlichen Betreuung während des gesamten Prozesses stark beeindruckt. Es war laut Andreas Gross „ein rundum perfekter Deal“.

Learn more about Barracuda Sentinel, Barracuda Essentials and Barracuda Message Archiver

barracuda.com/products/sentinel
barracuda.com/products/essentials
barracuda.com/products/messagearchiver

Barracuda
Your journey, secured.