

Führender Anbieter für Callcenter-Automatisierung [24]7.ai setzt auf Proofpoint als Sicherheitspartner

Anbieter KI-gestützter Chatbots schützt seine verteilte Belegschaft mit personenzentrierter Cybersicherheit

HERAUSFORDERUNG

- Schutz von Kundendaten und geistigem Eigentum aus verschiedensten Branchen
- Schutz der jetzt auch verteilten Belegschaft, einschließlich der Mitarbeiter im Home Office
- Skalierung der Sicherheitsfunktionen ohne große Kostensteigerung

LÖSUNG

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull

ERGEBNISSE

- Abwehr eines breiten Spektrums von E-Mail-Bedrohungen
- Identifizierung gezielt angegriffener Anwender und Abteilungen, die zusätzlichen Schutz benötigen
- Schutz für Mitarbeiter im Home Office und Gewährleistung ihrer Compliance
- Gestärktes internes Sicherheitsteam durch externe Bedrohungsdaten und Forschungsergebnisse

Das Unternehmen

Haben Sie sich auch schon in einem Sprachmenü verirrt, ein unsinniges Gespräch mit einem Chatbot geführt oder mit einem Callcenter-Mitarbeiter gesprochen, der einfach nicht von Skript abweichen wollte? [24]7.ai kann nachvollziehen, wie sich das anfühlt.

Das 20-jährige Unternehmen aus dem Silicon Valley hat es sich zum Ziel gesetzt, den Dienst am Kunden einfacher und angenehmer zu gestalten – etwas, das immer dringender wird in einer Zeit des verstärkten Wechsels zum digitalen Handel und zur Arbeit im Home Office. „Wenn Kunden Ihre Website aufrufen und das Gesuchte nicht schnell und einfach finden können, dann kommen sie so schnell nicht wieder“, sagt Rebecca Wynn, Global CISO und Chief Privacy Officer bei [24]7.ai. „Die Menschen haben einfach nicht mehr die Geduld dafür.“

Meistens nehmen Unternehmen zu [24]7.ai Kontakt auf, wenn sie merken, dass ihre Kunden ein schlechtes Online-Erlebnis haben und ihre Käufe nicht abschließen – quasi als ob Käufer im Supermarkt ihren halb gefüllten Wagen im Gang stehen lassen.

Kunden wollen auch online ein persönliches Erlebnis. Das können Unternehmen naturgemäß nur schwer im großen Maßstab anbieten. Für [24]7.ai besteht die Lösung in einer Mischung aus künstlicher Intelligenz und menschlichem Verständnis, um Kundenerlebnisse vorhersagen, individuell gestalten und digitalen Interaktionen so eine menschlichere Note verleihen zu können. Künstliche Intelligenz soll dabei helfen, die von Kunden gewünschte Unterstützung zu ermitteln und schnell zu liefern. Der KI-gestützte Dialog kann sich an das vom Kunden verwendete Gerät anpassen – ganz gleich, ob es sich um ein Laptop, Smartphone, einen Nachrichtendienst oder ein Gespräch mit einem Live-Agenten handelt.

Das ursprünglich unter dem Namen [24]7 Customer gegründete Unternehmen begann als Business Process Outsourcing-Unternehmen (BPO) bzw. Callcenter. Laut Lisa Matherly, Vice President of Marketing bei [24]7.ai, konzentrierten sie sich zunächst auf die Auslagerung von Kundendienst-Funktionen.

Der große Wechsel des Unternehmens zu KI ergab sich ganz natürlich aus der Arbeit mit seinen Kunden. Diese waren immer darum bemüht, ihren Kunden-Support effizienter, die Voice-Bots produktiver und das Kundenerlebnis insgesamt angenehmer zu gestalten. [24]7.ai hat basierend auf seinen Erfahrungen ein Portfolio an Produkten zusammengestellt, mit denen Support-Aufgaben automatisiert werden können. Außerdem wissen sie, zu welchem Zeitpunkt Mitarbeiter involviert werden sollten, um Interaktionen menschlicher zu gestalten.

[24]7.ai hilft seinen Auftraggebern dabei, deren Kunden ein persönlicheres und reibungsloseres Erlebnis zu bereiten. Die KI-gestützten Computer- und Sprachassistenten erkennen die Bedürfnisse von Kunden im Voraus und sorgen für einen schnelleren und besseren Service. Das Unternehmen bietet auch Self-Service-Tools an, mit denen Auftraggeber ihre Verkaufs- und Kundendienst-Erlebnisse ganz einfach selbst zusammenstellen, automatisieren und optimieren können.

Herausforderung

Zwei der wichtigsten Aspekte sind für [24]7.ai der Schutz des eigenen geistigen Eigentums und die Geheimhaltung der Daten von Auftraggebern.

Das Unternehmen besitzt mehr als 200 anerkannte oder angemeldete Patente sowie streng geschütztes geistiges Eigentum. Auch der Schutz seiner Kundendaten ist wichtig. Bei einigen Chat-Sessions kann es zum Beispiel um Kreditkartennummern oder personenbezogene Informationen gehen.

Die Kunden von [24]7.ai kommen aus allen Branchen, darunter auch viele stark regulierte Sektoren wie Gesundheitswesen, Finanzinstitute und Behörden. [24]7.ai muss dafür sorgen, dass Kundendaten nicht in die Hände von Cyberkriminellen geraten und entsprechend einer wachsenden Anzahl von Vorschriften gehandhabt werden.

„Ich suche nach jemandem, mit dem ich gut zusammenarbeiten kann und der mein Personal gut ergänzt. Wir befinden uns im Cyberkrieg und ich brauche Leute, die diesen Krieg mit mir gemeinsam kämpfen.“

Rebecca Wynn, Global CISO und Chief Privacy Officer, [24]7.ai

„Cybersicherheit spielt in unserem Geschäft eine sehr große Rolle“, meint Rebecca Wynn. „Wir führen einen Krieg gegen Menschen, die irgendwo hinter einer Tastatur sitzen und uns allen schaden wollen.“

Mit COVID-19 ist dieser Kampf noch schwieriger geworden. Die globale Pandemie zerstreut die Belegschaft, drängt den Handel ins Internet und schafft neue Sicherheits- und Compliance-Risiken.

Zum Glück war [24]7.ai darauf vorbereitet. Als die Pandemie begann, war das Unternehmen bereits dabei, die Arbeit ins Home Office zu verlagern, und war so besser als die meisten anderen auf den plötzlichen Wechsel vorbereitet. (Die Mehrheit seiner 10.000 Mitarbeiter arbeitet jetzt im Home Office, andere arbeiten in kleinen Büros zusammen, die auf die Einhaltung der örtlichen Abstandsregeln ausgelegt sind.)

[24]7.ai traf sich mit den wichtigsten Anbietern, Betreibern von Rechenzentren und den größten Kunden, um über den potenziellen Einfluss der Pandemie auf den Betrieb und Reaktionsmöglichkeiten zu sprechen. Während das Unternehmen ein Team für Geschäftskontinuität zusammenstellte und zügig die Kunden beruhigte, rückten neue Sicherheitsprobleme in den Mittelpunkt.

Datenschutz ist dabei nur ein Beispiel von vielen.

Dabei geht es um Fragen wie „Welche Person im Haus ist vertrauenswürdig?“, „Wie sieht eine sichere Umgebung aus?“ und „Wenn jemand aus Ihrer Familie kurz vorbeikommt und Hallo sagt, könnte er oder sie etwas auf Ihrem Bildschirm sehen?“

Lösung

Für [24]7.ai und andere Unternehmen besteht die neue Arbeitsumgebung eigentlich eher aus tausenden von neuen Arbeitsumgebungen. Anders als bei einem Büro mit einheitlichen Arbeitsplätzen unter leicht kontrollierbaren Bedingungen ist jede häusliche Umgebung individuell. Unternehmen müssen daher unzählige Kombinationen von Geräten und Netzwerken berücksichtigen, die für die IT-, Sicherheits- und Compliance-Abteilungen alle unerreichbar sind.

Um das Chaos besser in den Griff zu bekommen, erarbeitete [24]7.ai neue Vereinbarungen für die akzeptable Nutzung von Unternehmensressourcen. In einigen Fällen sollten Mitarbeiter ein Foto ihrer Arbeitsumgebung schicken, damit das Unternehmen den Kunden zusichern konnte, dass ihre Daten ordnungsgemäß verwaltet und geschützt werden.

Arbeiten im Home Office bedeutet auch, sich noch mehr auf den personenzentrierten Ansatz für Cybersicherheit zu konzentrieren. „Cyberangreifer nehmen schon seit längerer Zeit den Menschen statt die herkömmliche IT-Infrastruktur ins Visier. Der Schutz der Mitarbeiter aus der Ferne ist jedoch noch schwieriger“, erklärt Rebecca Wynn.

„Ich kann nicht überall Hausgeist spielen“, sagt sie. „Wie schaffe ich es also, dass ich über die gleichen Sicherheits- und Datenschutz-Kontrollen verfüge, wenn sie an ihren Computern sitzen?“

Zur Lösung des Problems nahm Rebecca Wynn die Hilfe des Cybersicherheitsanbieters Proofpoint in Anspruch, der für sie bereits ein starker Verbündeter im Kampf gegen Cyberbedrohungen und Compliance-Risiken ist.

„Ich suche nach jemandem, mit dem ich gut zusammenarbeiten kann und der mein Personal gut ergänzt“, sagt sie. „Wir befinden uns im Cyberkrieg und ich brauche Leute, die diesen Krieg mit mir gemeinsam kämpfen.“

Das Unternehmen setzt Proofpoint Email Protection ein, um verschiedenste Cyberbedrohungen abzuwehren, noch bevor sie den Posteingang der Anwender erreichen. Die preisgekrönte Lösung stoppt Spam, Malware und Angriffe, die statt technischer Schwachstellen mit Social-Engineering-Taktiken menschliche Schwächen ausnutzen.

Zu diesen Malware-losen Bedrohungen gehören auch E-Mail-Scams wie Business Email Compromise (BEC, auch Chefmasche genannt). Dabei geben sich Angreifer als vertraute Kollegen, Geschäftspartner und Marken aus – und zwar auf eine Weise, die von konventionellen E-Mail-Schutzmaßnahmen nicht immer so einfach zu erkennen ist.

Wenn etwas durchkommt oder sich nach der Zustellung als verdächtig herausstellt, entfernt Proofpoint Threat Response Auto-Pull automatisch die Nachricht, zusammen mit allen Kopien, die an andere Anwender weitergeleitet wurden.



Ergebnisse

Mit den Proofpoint-Lösungen kann [24]7.ai einen personenzentrierten Sicherheitsansatz verfolgen und bekommt so einen Überblick über die am stärksten angegriffenen Anwender im Unternehmen, die Proofpoint als Very Attacked People™ bezeichnet.

„Ich kann sehen, welche Personen in welchen Abteilungen auf welche Art angegriffen werden“, meint Rebecca Wynn. „Dadurch weiß ich, ob ich zusätzliche Schulungen zuweisen oder diese Mitarbeiter persönlich ansprechen muss. Und ich kann dadurch das ganze Unternehmen besser schützen.“

Nach Rebecca Wynns Ansicht machen unter anderem die umfangreichen Bedrohungsdaten Proofpoint zu einem so wertvollen Partner. Genauso wie [24]7.ai ist Proofpoint in vielen Branchen tätig. Daher ist Proofpoint in der Lage, die potentiellen Cyberbedrohungen gegen die Branchen zu erkennen, die von [24]7.ai bedient werden.

Proofpoint hilft Rebecca Wynn dabei, effizienter zu sein, da es zu einer Erweiterung des internen Sicherheitsteams geworden ist. Dank Proofpoints Investitionen in Forschung und Entwicklung sowie der äußerst umfangreichen Bedrohungsdaten, kann Rebecca Wynn ihr Team nun bei Sicherheitsproblemen einsetzen, die am besten intern gehandhabt werden sollten.

„Proofpoint ist Teil meines Teams“, sagt Rebecca Wynn.

Durch den Zugang zu Proofpoints Daten und Erkenntnissen zu Cybersicherheit erhält [24]7.ai beinahe in Echtzeit wichtige Informationen und kann fundiertere Entscheidungen treffen. Auf diese Weise kann sie ihr Team effizienter und ihr Unternehmen sicherer machen.

„Dank Proofpoint kann ich nachts ruhig schlafen, denn sie erleichtern mir die Arbeit“, sagt sie.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.