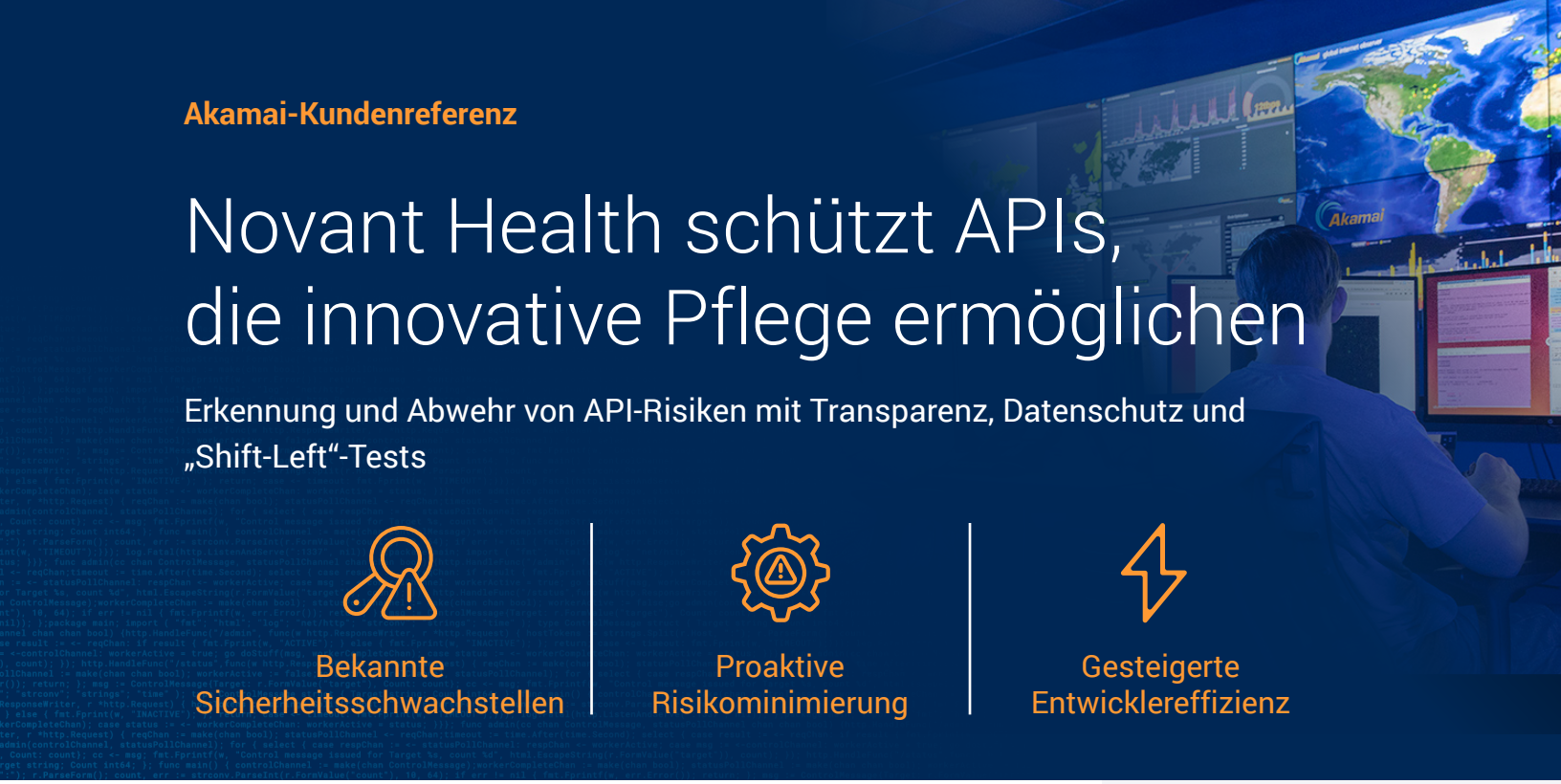
Akamai-Kundenreferenz

Novant Health schützt APIs, die innovative Pflege ermöglichen

Erkennung und Abwehr von API-Risiken mit Transparenz, Datenschutz und „Shift-Left“-Tests



Bekannte Sicherheitsschwachstellen

Proaktive Risikominimierung

Gesteigerte Entwicklereffizienz

Wie viele Leben kann ein Gesundheitsanbieter durch eine umfassende Versorgung, bei der die Gemeinde im Vordergrund steht, verbessern? Im Fall von Novant Health ist die Antwort erstaunlich und umfasst:

- 6,8 Millionen Besuche in Arztpraxen
- 155.964 stationär versorgte Patienten
- 602.590 Besuche in der Notaufnahme
- 22.082 Geburten

Diese Zahlen vermitteln auch einen klaren Eindruck davon, wen und was eine Gesundheitseinrichtung vor Cyberkriminellen schützen muss, die durch API-Verletzungen versuchen, sensible Daten zu kompromittieren.

Wissen, was auf dem Spiel steht

Novant Health ist ein gemeinnütziges integriertes System aus 16 medizinischen Versorgungszentren und mehr als 1.900 Ärzten an mehr als 900 Standorten. Das Unternehmen aus Winston-Salem, das mehr als 36.000 Teammitglieder und Partnerschaften mit Ärzten umfasst, versorgt Patienten in North Carolina und South Carolina.

Durch eine Reihe digitaler Initiativen gestaltet Novant die Patientenversorgung effektiver, persönlicher und effizienter. APIs bilden den Kern dieser Innovation und ermöglichen einen nahtlosen Austausch von Patientendaten zwischen Anwendungen, Geräten und Systemen. APIs spielen sogar eine so große Rolle, dass Novant ein Kompetenzzentrum (Center of Excellence, COE) aufgebaut hat, zu dem Mitarbeiter, Wissen und Ressourcen gehören, die eine erstklassigen API-Produktentwicklung gewährleisten sollen.

NOVANT HEALTH

Standort

Winston-Salem, North Carolina
novanthealth.org

Branche

Gesundheitswesen und Life Sciences

Lösung

API Security

Akamai

Nachdem es sich informiert hatte, wie sich API-fokussierte Angriffe auf Gesundheitsdienstleister auswirken, hat das Team zurecht die API-Sicherheit als oberste Priorität betrachtet. Auch die Branchenstatistiken, die sie dabei offengelegt haben, sind erstaunlich – allerdings nicht im positiven Sinne. So belaufen sich die durchschnittlichen Kosten einer Datenschutzverletzung im Gesundheitswesen auf 9,7 Millionen USD. Und 79 % der Gesundheitseinrichtungen haben in den letzten 12 Monaten einen API-Sicherheitsvorfall erlebt.

Das Problem identifizieren

Zunächst stellte das API-COE fest, dass die API-Sicherheit im gesamten Betrieb von Novant verbessert werden musste. Die einzige Lösung, die bisher zum Einsatz gekommen war, war eine Web Application Firewall (WAF). Diese Tools bieten Schutz vor bereits bekannten Angriffen, doch heutzutage benötigen Gesundheitsorganisationen einen umfassenderen Ansatz zum Schutz von APIs. Dazu gehören:

- Transparenz über die Anzahl der APIs in der IT-Umgebung eines Unternehmens
- Einblicke in die Risikoattribute jeder API, z. B. die Arten der verarbeiteten Daten
- Detaillierte Analysen der API-spezifischen Sicherheitslage eines Unternehmens, einschließlich der Aufdeckung von Fehlkonfigurationen, die Angreifer ausnutzen
- Schutz vor Angriffen, die Fehler in der API-Geschäftslogik ausnutzen

Darüber hinaus identifizierte das COE-Team von Novant wichtige Lücken im „Shift-Left"-Ansatz des Unternehmens und den Bemühungen, Sicherheit schon in die frühen Entwicklungsphasen einzubetten. Sie verfügten über Tools zum Testen von Docker-Containern, benötigten aber eine Lösung für die Entwicklung von APIs. Da vertrauliche Daten wie Patientendatensätze gefährdet waren, einigte sich das COE-Team von Novant darauf, dass ein Anbieter gefunden werden müsse, dessen Mitarbeiter und Produkte zu 100 % auf die Sicherung von APIs ausgerichtet sind.

Entstehen von „Aha-Momenten"

Das COE von Novant traf die Noname Security (jetzt ein Unternehmen von Akamai), nachdem es von deren umfassendem Ansatz zur Sicherung von APIs erfahren hatte. Gemeinsam führten sie eine eingehende Analyse des Sicherheitsmanagements aller APIs in der IT-Umgebung von Novant durch. Mithilfe der API-Sicherheitsplattform von Noname (jetzt Teil von Akamai API Security) identifizierte das Team eine Azure-Schwachstelle, die erhebliche Auswirkungen auf die Sicherheit hatte.

> Für uns bei Novant Health hat Akamai eine beträchtliche Lücke geschlossen und uns einen besseren Einblick in eine der Ressourcen ermöglicht, die am häufigsten angegriffen werden. Die bisherigen Erkenntnisse und verwertbaren Informationen zu Sicherheitslücken in unserem API-Ökosystem haben sich bereits als sehr wertvoll erwiesen. Bei Novant Health hat der Schutz unserer Datenbestände oberste Priorität. Akamai arbeitet mit denselben Werten und hat sich als grundlegende Funktion in unserem gesamten Datensicherheitssystem etabliert.
>
> – Justin P. Byrd
> Vice President, Data Platform and Integration, Novant Health

Akamai

Die API-Sicherheitsmanagement-Lösung der Plattform zeigte an, dass einige Anfragen an APIs in der Cloudumgebung von Novant das WAF-Tool *umgingen*, anstatt die Firewall zu durchlaufen. Angreifer umgingen die WAF durch eine „offene Tür“, die die WAF nicht sichern konnte, und griffen wiederholt die APIs von Novant an, wobei das Unternehmen vollkommen exponiert und ahnungslos war.

Die von Akamai bereitgestellten Erkenntnisse waren zwar schockierend, aber auch hilfreich, um sofort Gegenmaßnahmen zu ergreifen. Um APIs sicher zu entwickeln und zu verwalten, benötigt Novant Health einen vollständig geschützten Cloud-Arbeitsbereich. Justin P. Byrd, Vice President von Novant, und sein Team waren beeindruckt von der Bereitschaft des Akamai Teams, die Ärmel hochzukrempeln und ihre API-Lösung für das Sicherheitsmanagement einzusetzen, um die aufgedeckten Schwachstellen zu finden und zu beseitigen.

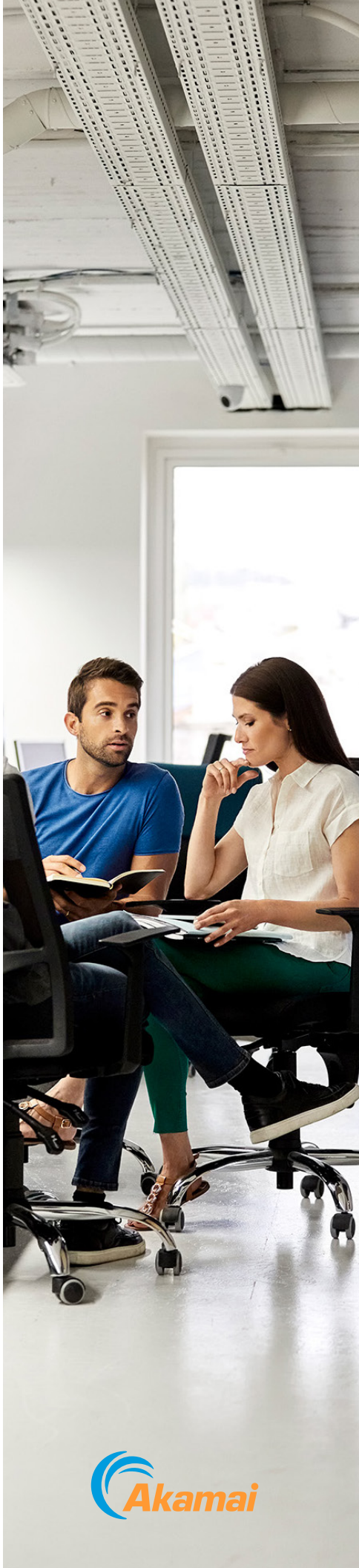
Ausgehend von seinen initialen Erkenntnissen kann das COE-Team nun die automatisierten Funktionen der API-Sicherheitsmanagement-Lösung von Akamai nutzen, die APIs kontinuierlich auf Fehlkonfigurationen und versteckte Risiken überprüfen, sodass das Unternehmen Maßnahmen ergreifen kann, um diese proaktiv zu mindern. Dazu gehört auch die Fähigkeit, zu ermitteln, welche APIs und internen Nutzer auf sensible Daten zugreifen können.

Für ein Unternehmen wie Novant, das Gesundheitsdaten verwaltet, die Millionen von Patienteninteraktionen umfassen, ist es entscheidend zu wissen, welche APIs mit sensiblen Informationen interagieren, um mit den Patienten, Anbietern und Aufsichtsbehörden ein Vertrauensverhältnis aufzubauen und zu wahren.

Schafft sowohl Sicherheit als auch Mehrwert

Für das COE von Novant – zu dem führende Entwickler mit praktischer Erfahrung gehören – stellte die Integration von Sicherheit in die API-Tests des Unternehmens eine weitere Priorität dar. Bei jeder API ist die Entwicklungsgeschwindigkeit ein entscheidender Faktor, und das gilt insbesondere für Unternehmen wie Novant, deren APIs eine maßgebliche Rolle bei der Patientenversorgung spielen. Der Druck, APIs schnell zu entwickeln, erhöht allerdings die Wahrscheinlichkeit, dass Schwachstellen oder Designfehler unentdeckt bleiben, während Entwickler die API schnell in die Produktion bringen wollen.

Das COE suchte nach zuverlässigen API-Testfunktionen, um die in jeder API implementierten Sicherheitsmaßnahmen zu bewerten. Dazu gehören umfassende Tests zur Identifizierung von Schwachstellen in Variablen wie den Authentifizierungsmechanismen, Autorisierungskontrollen, der Datenintegrität und den Verschlüsselungsprotokollen.



Bei der Implementierung eines neuen Sicherheitstools hängt der Erfolg natürlich nicht nur von der Funktionalität, sondern auch von der Interaktion mit wichtigen Partnern ab. Entwickler wissen, wie wichtig Sicherheit ist, aber angesichts der Notwendigkeit für Geschwindigkeit sind sie in der Regel skeptisch gegenüber unbekannten Tools, die zu Verlangsamungen führen können.

Das war zunächst auch bei Novant Health der Fall.

Im Zuge der weiteren Zusammenarbeit mit Akamai hat das Novant Team eine Reihe von Funktionen ausgemacht, mit denen Entwickler ihre Arbeit sicher und effizient erledigen können. So konnte beispielsweise das Active Testing von Akamai API Security proaktiv Fehler aufdecken, die später im Prozess zu erheblichen und zeitaufwändigen Problemen geführt hätten.

Darüber hinaus versetzte die Lösung das COE in die Lage, Entwicklern Schnellnotizen zur Effizienzsteigerung zu geben – eine angenehme Überraschung für die Mitglieder des COE-Teams, denen nicht bewusst war, dass die Lösung auch Qualitätsprüfungen ohne Sicherheitsbezug durchführt. Beispielsweise konnten sie jetzt bestimmen, ob die Spezifikationen einer API mit dem übereinstimmen, was die erstellte API tatsächlich bereitstellt. Es dauerte nicht lange, bis auch die Entwickler – die zunächst nur mäßig begeistert waren – die Vorteile für Sicherheit und Effizienz erkannten und von der Arbeit mit Akamai API Security begeistert waren.

„Akamai war vom ersten Tag an ein vertrauenswürdiger Berater bei der Erkennung, dem Schutz und dem Testen unserer APIs in allen Phasen – von der Programmierung bis zur Produktion. So kann unser Kompetenzzentrum dem gesamten Unternehmen zeigen, wie Sicherheit und Effizienz gleichzeitig gewährleistet werden können“, erklärt Byrd. „Bei dieser Partnerschaft geht es um mehr als nur um Produkte. Die Mitarbeiter des Noname-Teams (jetzt ein Unternehmen von Akamai) verstehen unsere Welt und die Geschäftsfaktoren hinter der API-Entwicklung.“

Die Geschäftsführung von Novant sieht es genauso und verweist dabei auf die Fähigkeit von Akamai API Security, Dinge zu erfassen, bevor sie zum Problem werden. Außerdem trug die Lösung dazu bei, die API-Sicherheit in den „Shift-Left“-Bemühungen des Unternehmens zu verankern.

Die Vorteile der API-Sicherheit nutzen

Heute nutzt Novant API Security von Akamai, um „automatischen Schutz“ für ihre APIs und jede digitale Initiative bereitzustellen. Aufbauend auf den Erfolgen von Novant bei der Entdeckung, Inventarisierung, Bewertung und Prüfung von APIs wendet das COE-Team nun den umfassenden Schutz der Plattform auch für neue APIs an, die Novant entwickelt. Das Team ist davon überzeugt, dass jede API automatisch geschützt ist, wenn die Entwickler von Novant APIs basierend auf abgestimmten Best Practices entwickeln.

Mit Blick auf die Zukunft plant das COE-Team, die Nutzung von Akamai API Security auf andere Teams innerhalb des Unternehmens auszuweiten. Mit dem Ziel, ein unternehmensübergreifendes Modell für den API-Schutz zu entwickeln, stellt das COE sich eine Partnerschaft zwischen sich, dem Sicherheitsteam von Novant Health und dem Foundation-Structure-Team des Unternehmens bei der Verwendung von Akamai API Security vor.

NOVANT HEALTH

Novant Health ist ein gemeinnütziges, integriertes System von 19 medizinischen Versorgungszentren und mehr als 2.000 Ärzten an über 900 Standorten sowie zahlreichen ambulanten chirurgischen Zentren, medizinischen Einrichtungen, Rehabilitationsprogrammen, Zentren zur diagnostischen Bildgebung und kommunalen Gesundheitsprogrammen. Die fast 40.000 Teammitglieder und Ärztepartner von Novant Health versorgen Patienten und Gemeinden in North Carolina und South Carolina.

©2025 Akamai Technologies | Support | | Veröffentlicht: Januar 2025

Akamai