OpenDNS

OpenDNS gehört jetzt zu Cisco.

Anwenderbericht:

GLOBALER PHARMAHERSTELLER SCHIEBT RANSOMWARE DEN RIEGEL VOR

„Das Risiko, uns über das Web mit Ransomware zu infizieren, ist erheblich gesunken. Und das bei deutlich stabileren Internetverbindungen für unsere Endnutzer.“

- **Jason Hancock**
  Leiter Netzwerktechnik, Octapharma

octapharma

Projektdetails:

Unternehmen:
Octapharma

Hauptsitz:
Lachen, Schweiz

Anzahl der geschützten Nutzer und Standorte:
Neben 5.000 Mitarbeitern in 31 Ländern schützt die Lösung auch das Gast-Wi-Fi in 60 Spendezentren von Octapharma in den USA, das pro Tag von rund 15.000 Spendern genutzt wird.

Herausforderung:
Schutz vor Ransomware und anderen Bedrohungen stärken, ohne dabei die Leistung des weltumspannenden Netzwerks zu beeinträchtigen

Lösung:
OpenDNS Umbrella

Auswirkung:

- Deutlicher Rückgang der Ransomware-Vorfälle
- Optimiertes Sicherheitsmanagement
- Verbesserte Internetleistung

HERAUSFORDERUNG:

Begrenzte Ressourcen stehen gegen schier grenzenlosen Herausforderungen gegenüber

Seit seiner Gründung im Jahr 1983 ist Octapharma stetig gewachsen und gehört heute zu den größten Herstellern von Präparaten aus menschlichem Protein. Und seit Octapharma jüngst eine Initiative angestoßen hat, die bis 2019 eine Verdopplung der Produktionskapazität und eine Steigerung der Effizienz insgesamt vorsieht, expandiert das Unternehmen wie nie zuvor.

Dieser Wachstumsschubs macht sich im gesamten Unternehmen bemerkbar – sogar auf Ebene des Netzwerks. „An vielen Standorten stellen wir neues Personal ein. Damit steigt natürlich auch die Zahl der Mobilgeräte und Cloud-Services, die in unserem Unternehmen genutzt werden, was in der Folge auch neue Schwachstellen in unserem Netzwerk bedeutet“, so Jason Hancock, Leiter Netzwerktechnik bei Octapharma. „In unserem Netzwerk sind die schädlichen Aktivitäten sprunghaft angestiegen, insbesondere von Ransomware.“

„Dieser Entwicklung durch Aufstockungen unserer Teams entgegenzuwirken, wäre angesichts des anhaltenden Mangels an Security-Fachkräften schwierig gewesen – und auch kaum mit den Effizienzzielen unseres Unternehmens vereinbar. Daher mussten wir uns nach neuen Lösungen umsehen“, fügt er hinzu.

„Mit Blick auf die Effizienz – sowohl unseres Teams als auch der Endnutzer –, mussten wir als erstes dafür sorgen, dass das Netzwerk nicht mehr alle 15 Minuten ausfällt. Als ich 2014 in die Firma kam, ging es im ersten Schritt darum, die Systeme stabiler zu machen und dann schrittweise unseren Malware-Schutz zu verbessern. Hierbei konzentrierte ich mich zunächst auf besonders aggressive Varianten, darunter auch die CryptoLocker-Ransomware, mit der es bei uns in der Vergangenheit bereits zu einem Sicherheitsvorfall kam.“

„Im ersten Schritt ging es darum, die Systeme stabiler zu machen und dann schrittweise unseren Malware-Schutz zu verbessern. Hierbei konzentrierte ich mich zunächst auf besonders aggressive Varianten, darunter auch die CryptoLocker-Ransomware, mit der es bei uns in der Vergangenheit bereits zu einem Sicherheitsvorfall kam.“

- **Jason Hancock**
Leiter Netzwerktechnik

LÖSUNG:

Funktionalität, die „einfach passt“

„Als ich bei Octapharma anfing, war bereits seit einiger Zeit ein Projekt im Gange, in dessen Rahmen die bei uns eingesetzten Web-Security-Appliances zum Cloud-Service desselben Anbieters migriert werden sollten, den einer meiner Vorgänger ausgewählt hatte. Dieses Projekt sollte ich dann zum Abschluss bringen“, erinnert sich Hancock. „Als ich aber sah, womit ich es zu tun hatte, war mir sofort klar, dass wir mit diesem Produkt nicht weit kommen würden.“

„Wir stießen auf erhebliche Probleme, die zunehmend Zweifel an der Eignung des Produkts für unsere Umgebung aufkommen ließen. Das fing schon an mit der Internetfunktionalität.“ Hancock berichtet weiter „Wir erhielten reichlich Beschwerden über Probleme mit dem Internetservice, sowohl im Zusammenhang mit dem Cloud-Service, als auch mit dem Client, der auf den Endnutzersystemen installiert war.“

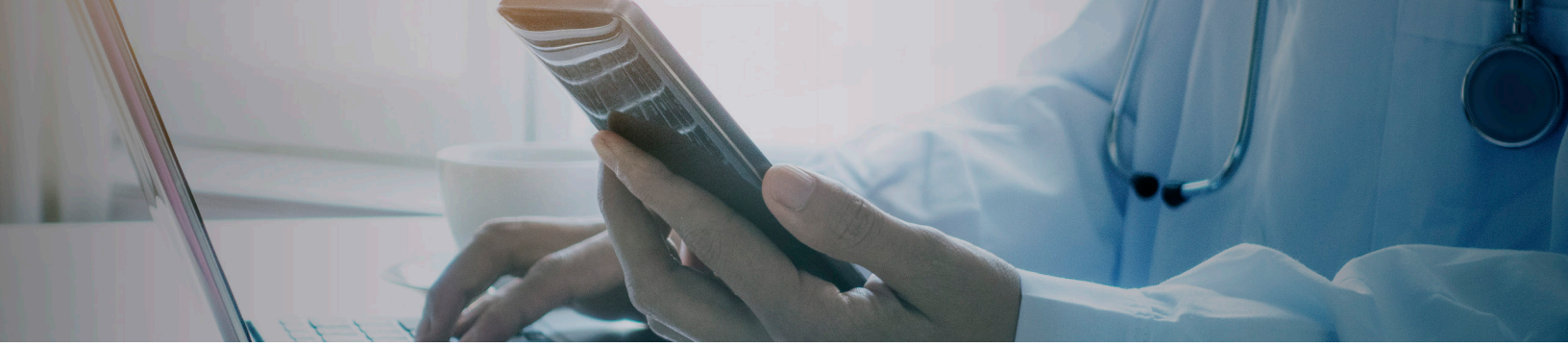
„Darüber hinaus war der Funktionsumfang für uns nicht ausreichend, und auch die Administration gestaltete sich schwierig – wir mussten unsere Teams umfangreich schulen, bevor sie mit der komplexen, nicht intuitiven Verwaltung von Richtlinien und diversen Komponenten zurechtkamen.“

„Als wir die Lösung nach einer äußerst holprigen Installationsphase dann endlich an unseren Standorten in Nordamerika ausgerollt hatten, fiel unser Netzwerk regelmäßig aus – teilweise für mehrere Stunden. Diese Probleme ließen unser Team natürlich denkbar schlecht aussehen, konnten aber auch nicht über den Support des Herstellers behoben werden.“ „Vonseiten des Herstellers riet man uns dann schließlich, die Migration in die Cloud abzubrechen und stattdessen virtuelle Appliances einzuführen. Doch dazu hätten wir den Traffic von weltweit mehr als 50 Standorten umleiten müssen, was nicht nur unerwünscht, sondern in einigen Fällen auch unmöglich war.“

„An diesem Punkt schritt ich ein. Ich machte deutlich, dass wir das Problem nur mit OpenDNS lösen würden, und dass ich diese Lösung binnen sechs Wochen ausrollen und damit unser gesamtes globales Netzwerk schützen könnte.“ Sicher, in die bestehende Lösung war bereits viel Geld geflossen, aber sie funktionierte eben nicht bei uns. Deshalb schlug ich eine Lösung vor, von der ich aus früherer Erfahrung wusste, dass sie Erfolg haben würde: OpenDNS Umbrella.“

„Sicher, in die bestehende Lösung war bereits viel Geld geflossen, aber sie funktionierte eben nicht bei uns. Deshalb schlug ich eine Lösung vor, von der ich aus früherer Erfahrung wusste, dass sie Erfolg haben würde: OpenDNS Umbrella.“

- **Jason Hancock**
  Leiter Netzwerktechnik



ERGEBNISSE:

Deutlicher Rückgang der Ransomware-Vorfälle
Der Rollout der Lösung gestaltete sich äußerst einfach – und zeigte sofort Ergebnisse. „Seit der Einführung von Umbrella haben wir keine Probleme mit der Web-Sicherheit mehr“, so Hancock.

„Wir sind jetzt deutlich weniger anfällig für Ransomware-Angriffe. Tatsächlich gab es seither keinen einzigen Fall mehr, bei dem sich ein Nutzer durch Klicken auf einen schädlichen Link eine Ransomware eingefangen hätte. Tatsächlich werden bei uns jetzt jede Woche mehrere Zehntausend solcher Web-Anfragen mithilfe unserer Sicherheitsrichtlinie blockiert. Und das schließt noch nicht einmal die Blockierungen auf Grundlage unserer Kategorie-Richtlinien mit ein“, fügt er hinzu. „Das Risiko, uns über das Web mit Ransomware zu infizieren, ist erheblich gesunken. Und das bei deutlich stabileren Internetverbindungen für unsere Endnutzer.“

„Wir haben uns sogar einige Phishing-E-Mails herausgesucht und auf die darin enthaltenen Links geklickt, um zu sehen was passiert: Der Zugriff auf diese Websites wurde von OpenDNS zuverlässig blockiert.“

Hancock berichtet zudem von einem weiteren Vorteil, mit dem er nicht gerechnet hatte: „Als wir die Daten aus dem Umbrella-Dashboard mit den Daten von unseren internen Systemen abglichen, fanden wir weitere infizierte Systeme, die zuvor durchs Raster gefallen waren.“

Nachdem Bedrohungen bei Octapharma jetzt auf DNS-Ebene blockiert werden, will Hancock den Schutz des Netzwerks jetzt durch ein proaktives Sicherheitsmanagement zusätzlich stärken. „OpenDNS kann Websites auf Grundlage von Kategorie-Richtlinien äußerst effektiv blockieren. Damit bildet die Lösung ein zentrales Element unserer Verteidigungsstrategie. Ich prüfe derzeit weitere Tools aus dem Cisco Security-Portfolio, um diese Strategie weiter voranzutreiben“, merkt Hancock an. „Dafür in Frage kommen z. B. Firewalls, Malwareschutz für Endpunkte und Möglichkeiten bei Cisco, die Produkte in unserem Security-Stack besser zu koordinieren.“

Für Jason Hancock war schon immer klar: Die Überzeugung für eine Sache kommt, wenn man ihre Vorteile sofort sehen kann. „Zu Hause nutze ich OpenDNS schon seit Jahren“, sagt er. „Und jetzt habe ich die Lösung bereits in zwei Unternehmen mit sehr großem Erfolg eingeführt. Meine Kollegen sind genauso begeistert von dem hochgradig effektiven Sicherheitsansatz von OpenDNS wie ich selbst.“

> *„Wir sind jetzt deutlich weniger anfällig für Ransomware-Angriffe. Tatsächlich gab es seither keinen einzigen Fall mehr, bei dem sich ein Nutzer durch Klicken auf einen schädlichen Link eine Ransomware eingefangen hätte.“*
>
> - **Jason Hancock**
> Leiter Netzwerktechnik

OpenDNS

OpenDNS gehört jetzt zu Cisco. CISCO

Wenden Sie sich für eine kostenlose Testversion oder nähere Informationen zum Kauf an unser Team:
1-877-811-2367 | sales@opendns.com | www.opendns.com