infoblox

FALLSTUDIE

Stupp Bros. erhöht die Sicherheit mit Infoblox Threat Defense

ÜBERSICHT

Mit Hauptsitz in St. Louis, Missouri, ist Stupp Bros. ein führender Anbieter von Materialien und Dienstleistungen, die für den Aufbau kritischer Infrastrukturen in den gesamten Vereinigten Staaten unerlässlich sind.

Das Unternehmen stellt Stahlkonstruktionen her, die in Brücken, Hochhäusern, Krankenhäusern, Kongresszentren, Sportstadien und Unterhaltungsstätten im ganzen Land verwendet werden. Neben seinem Kerngeschäft bietet Stupp Bros. eine Reihe von Dienstleistungen an, darunter Regionalbanking, Datenerfassung, die es prozessintensiven Branchen ermöglicht, Vorschriften einzuhalten, sowie Breitbanddienste für Privathaushalte und Unternehmen.

> *„Threat Defense ist der Schutzwall um unsere Burg. Den müssen Angreifer zuerst überwinden, bevor sie die Außenwände beschädigen können.“*
>
> **John Roosa,**
> **Chief Information Officer,**
> **Stupp Bros.**

DIE SITUATION

Etablierung einer Defense-in-Depth-Mentalität

Vor über 165 Jahren gegründet, hat sich Stupp Bros. in erster Linie auf die Weiterentwicklung von Fertigungsmethoden und die Erschließung neuer Märkte für seine hochwertigen Baumaterialien konzentriert. Da die Geschäftstätigkeit des Unternehmens in den letzten Jahrzehnten jedoch zunehmend digital vernetzt wurde, gehört Cybersicherheit nun zu den obersten Prioritäten.

Mitte der 1990er Jahre war John Roosa als Berater tätig und unterstützte das Unternehmen bei der Optimierung der Netzwerkinfrastruktur in den frühen Tagen des Internets, als der Melissa-Virus zuschlug. „Das war mein Weckruf“, sagt er Dieser Vorfall von 1997 zeigte ihm, wie drastisch sich die Sicherheitslandschaft verändert hatte und wie unvorbereitet die Computernetzwerke auf diese neue Realität waren.

Seitdem ist Roosa ein überzeugter Verfechter der ganzheitlichen Cybersicherheit. Als CIO von Stupp Bros. in den letzten 18 Jahren hat er den Aufbau eines mehrschichtigen Verteidigungsansatzes überwacht, der darauf abzielt, das Unternehmen und seine über 350 Mitarbeiter vor modernen Bedrohungen zu schützen.

STUPP BROS., INC.
ESTABLISHED 1856 | ST. LOUIS, MISSOURI

Um diese Ziele zu erreichen, haben Roosa und seine Kollegen einen Sicherheits-Stack implementiert, der aus Firewalls der nächsten Generation (NGFWs) und anderen Endpunktschutzmaßnahmen besteht, verankert durch Microsoft Sentinel, Microsofts cloudbasierte Plattform für Security Information und Event Management (SIEM) sowie zugehörige Tools.

Obwohl diese Einsätze weitgehend effektiv waren, konnten sie ein ernsthaftes Sicherheitsproblem nicht angemessen lösen: Mitarbeiter, die sich versehentlich an riskantem Online-Verhalten beteiligen.

DIE HERAUSFORDERUNG

Wo Online-Nutzer hingehen, folgen Bedrohungen.

Aus Roosas Perspektive haben sich die Herausforderungen durch das Nutzerverhalten seit seinem Amtsantritt als CIO im Jahr 2007 dramatisch entwickelt. „Damals war es viel einfacher." „Die Risiken waren bei weitem nicht so komplex." Damals hatten die Nutzer weniger Geräte, Geschäftsanwendungen liefen hauptsächlich auf Desktop-Computern, und die Cloudtechnologie hatte gerade erst begonnen, sich zu entwickeln. Obwohl Risiken durch Mitarbeiter bestanden, „waren sie aus IT-Sicht im Vergleich zu heute leichter zu mindern", bemerkt Roosa.

Heute haben alle Mitarbeiter von Stupp Bros. Smartphones oder andere Geräte, die ihnen überall sofortigen Internetzugang ermöglichen. Zunehmend stützt sich ein Großteil der Arbeit in der modernen Stahlverarbeitung, im Bauwesen und im Bereich des Glasfaser-Breitbands auf E-Mail, Textnachrichten und den Zugriff auf Cloud-Anwendungen und -Ressourcen.

Jedoch ist es mit so vielen Verbindungsmöglichkeiten für Roosa und sein Team zunehmend schwieriger geworden, zu kontrollieren, wohin die Mitarbeiter gehen und was sie online tun. Im Gegensatz zu größeren Unternehmen verfügt Stupp Bros. nicht über die Ressourcen, um gesperrte Geräte auszugeben oder verwaltete Desktops für jeden einzelnen Mitarbeiter bereitzustellen. Infolgedessen klickten die Mitarbeiter gelegentlich auf Phishing-Links oder besuchten Websites mit fragwürdigen Banneranzeigen, die sie zu bösartigen Webzielen weiterleiteten oder, schlimmer noch, einen Virusdownload einleiteten.

Für Roosa war die Schulung der Mitarbeiter entscheidend, um diese Risiken zu mindern. Insgesamt haben sich diese Bemühungen als sehr effektiv erwiesen; aber sie waren nicht immer rechtzeitig genug. Zum Beispiel stiegen die Sicherheitswarnungen an, als Stupp Bros. eine neue Geschäftseinheit übernahm, bevor die Mitarbeiter die erforderliche Sicherheitsschulung erhalten hatten.

Roosa war entschlossen, solche Situationen künftig zu verhindern. Doch selbst die erfahrensten Nutzer können Opfer von bösartigen Online-Inhalten werden, die geschickt als legitim getarnt sind. Unvermeidlich erreichten Virenbenachrichtigungen die NGFWs und andere Endpunkt-Sicherheitstools bei Stupp Bros., was die Sicherheitsteams dazu veranlasste, Stunden mit der Untersuchung und Behebung zu verbringen.

Um diese Herausforderung zu bewältigen, benötigte Stupp Bros. eine umfassende Lösung, die die mit unsicheren Online-Aktivitäten verbundenen Risiken reduziert und gleichzeitig die Sicherheitslage mit minimalen Auswirkungen auf die Mitarbeiter und das Sicherheitspersonal verbessert.

DIE LÖSUNG

Nutzung der proaktiven Sicherheitskraft von DNS

Roosa erkannte, dass der beste Weg, um Mitarbeiter davon abzuhalten, auf riskante Links zu klicken, darin besteht, sie von vornherein daran zu hindern. Dementsprechend setzte Stupp Bros. eine Reihe von Webfilterprodukten ein, die jedoch alle letztlich unbefriedigende Ergebnisse lieferten. „Es waren die typischen klobigen Regeln: ‚Dieses Thema erlauben, jenes nicht'", sagt Roosa

Kunde: ***Stupp Bros.***
Branche: ***Bauwesen***
Standort: ***St. Louis, MO***

ZIELE:

- Risiken im Zusammenhang mit unsicherem Online-Verhalten mindern
- Optimieren Sie die Verwaltung der Webfilterung, um den manuellen Aufwand zu verringern.
- Reduzieren Sie das Volumen der Virenwarnungen und die Zeit, die für deren Behebung erforderlich ist

ERGEBNISSE:

- 15-minütige Bereitstellung der cloudbasierten DNS-Sicherheitslösung
- Proaktives Blockieren von bösartigen digitalen Interaktionen im gesamten Netzwerk
- Nahezu vollständige Eliminierung von Virenwarnungen, wodurch das Alarmrauschen drastisch reduziert wird.
- 50 % Reduzierung der durchschnittlichen Zeit zur Untersuchung von Bedrohungen

PRODUKTE:

- Infoblox Threat Defense™

Diese Lösungen legten Roosa und seinem Team die zusätzliche Last auf, manuell zu bestimmen, welche Themen und Webziele zu den Sperrlisten hinzugefügt werden sollten, eine zeitaufwändige Aufgabe, die Recherche und fortlaufende Konfiguration erforderte. Der größte Nachteil war jedoch der grundlegende Designfehler, der im Kern dieser Screening-Tools lag. „Ich bin wirklich nicht gern im Net-Nanny-Geschäft, weil ich verstehe, wie das Internet funktioniert und wie einfach es ist, viele dieser [Filter] zu umgehen“, sagt Roosa

Roosa stieß zum ersten Mal auf Infoblox, als er nach DHCP-Verwaltungsoptionen für die Glasfaser-Internet-Abteilung des Unternehmens recherchierte. Während dieser Erkundung erfuhr er anschließend von Infoblox Threat Defense™ und seinem innovativen Ansatz für DNS-basierte Sicherheit. „Infoblox war für mich eine Art Offenbarung“, sagt er. „DNS ist der Ausgangspunkt.“

Mit Threat Defense erkannte Roosa, dass er „zwei Fliegen mit einer Klappe schlagen“ konnte. Zunächst wurde das Problem gelöst, festzustellen, welche Webziele bösartig sind. Zweitens, da es auf der DNS-Kontrollebene arbeitet, blockiert es den Zugriff der Benutzer auf diese Standorte vollständig und eliminiert damit die mit anderen Filteroptionen verbundenen Umgehungslösungen. „Es hat sich endlich in meinem Kopf gefestigt“, fährt Roosa fort „Wenn ich die DNS bei der Namensauflösung kontrollieren kann, kann ich viele Aktivitäten unterbinden, bevor sie überhaupt beginnen.“

Roosa und seine Teams haben die cloudbasierte Lösung problemlos in nur 15 Minuten bereitgestellt. Die Implementierung war nahtlos, für Endnutzer transparent und funktioniert über die gesamte Infrastruktur hinweg – lokal, hybrid und in Multi-Cloud-Umgebungen. Threat Defense schützt alle Mitarbeiter von Stupp Bros. im Netzwerk, unabhängig von ihrem Standort oder Gerät. Es blockiert proaktiv Benutzer daran, mit Webdomänen zu kommunizieren, die mit potenziellen Risiken verbunden sind, einschließlich des automatischen Herunterladens von Malware und Viren, des Diebstahls von Anmeldedaten und der Datenexfiltration, unter vielen anderen.

Die erweiterten Webfilterfunktionen von Threat Defense sind in hohem Maße anpassbar. Darüber hinaus werden sie kontinuierlich mit den neuesten betroffenen Domänen aktualisiert, die von Infoblox Threat Intel, der führenden Forschungsgruppe der Branche mit Schwerpunkt auf neu auftretenden DNS-basierten Bedrohungen, aufgedeckt wurden. Diese Informationen werden durch KI-basierte Algorithmen ergänzt, um Bedrohungsindikatoren in Bereichen aufzudecken, die mit anderen Sicherheitsmethoden nicht erkannt werden können.

Bei Stupp Bros. arbeitet Threat Defense zusammen mit anderen Sicherheitslösungen, einschließlich Microsoft Sentinel und verwandten Tools, die kompromittierte Geräte verwalten und deren Remediation durchführen. Während diese Bereitstellungen in erster Linie reaktiv sind und erst dann reagieren, wenn Endpunkt-Sicherheitstools eine Bedrohung erkennen, verhindert Threat Defense proaktiv, dass Bedrohungen überhaupt die Netzwerkgrenze erreichen. Dies ist eine wesentliche Fähigkeit, die der CIO sehr zu schätzen weiß. „Threat Defense ist unsere erste Verteidigungslinie für alles“, bemerkt Roosa

DAS ERGEBNIS

Eine stärkere Sicherheitslage schaffen

Im Bereich Threat Defense hat Stupp Bros. eine elegante Lösung für das Problem gefunden, wie Mitarbeiter vor Bedrohungen geschützt werden können, die moderne digitale Interaktionen ausnutzen. Indem der Zugriff auf bösartige Webziele im Netzwerk verhindert wird, wird riskantes Online-Verhalten eliminiert. „Wenn Infoblox sagt, dass es keine gute Seite ist, dann rufen sie sie nicht auf“, sagt Roosa

Die Filterfunktionen der Lösung erfordern keinerlei Eingriff seitens der Mitarbeiter. Sie erleichtert Roosa und seinem Team auch erheblich die Entscheidung, welche Ziele gesperrt werden sollen, was er als einen wesentlichen Vorteil ansieht. „Jetzt muss ich mir keine Gedanken mehr darüber machen, was wir blockieren sollten. Threat Defense kümmert sich darum.“

Da Threat Defense Bedrohungen auf der DNS-Kontrollebene stoppt, hat es die Belastung der Perimeterabwehr von Stupp Bros. erheblich reduziert. Wie Roosa erklärt: „Wir blockieren den Großteil des schädlichen Datenverkehrs, bevor er uns überhaupt erreicht. Das erzeugt viel weniger Lärm auf unserer Analyseplattform.“

Diese Reduzierung des Geräuschpegels, kombiniert mit einer extrem niedrigen Falsch-Positiv-Rate von nur 0,0002 Prozent, bedeutet, dass das Sicherheitspersonal deutlich weniger Alarme zu verwalten hat. Zum Beispiel sind seit der Einführung von Threat Defense die früher häufigen Virenmeldungen nahezu verschwunden. Laut Roosa haben seine Sicherheitsteams dank der von Infoblox ermöglichten Reduzierung des Alarmvolumens die Zeit für die Bedrohungsuntersuchung halbiert, wodurch sie sich auf strategische Initiativen konzentrieren können, die die allgemeine Sicherheitslage des Unternehmens stärken.

Threat Defense hat Roosa ebenfalls wertvolle Zeit zurückgegeben. Er vertraut darauf, dass die riskanten Interaktionen, die die Plattform rigoros stoppt, auf den aktuellsten Brancheninformationen zu schnell entwickelnden DNS-basierten Bedrohungen basieren. „Das ist der schöne Teil dieses Produkts“, sagt er „Ich kann Ihnen ehrlich sagen, dass ich keine Zeit damit verloren habe, es zu verwalten, mich damit zu befassen oder dergleichen.“

Zusätzlich zur Nutzung der fortschrittlichen Webfilterfunktionen von Threat Defense wird Stupp Bros. in Kürze weitere Funktionen aktivieren, beginnend mit der Integration von Infoblox-Daten in sein Microsoft-Sicherheitsökosystem. Roosa prognostiziert, dass die Echtzeit-Telemetrie der DNS-Bedrohungsaktivität der Lösung die Triage- und Remediation-Maßnahmen des Unternehmens erheblich verbessern wird. „Mit Threat Defense werden wir viel mehr sehen können“, sagt er

Allgemeiner ausgedrückt fasst Roosa den Wert der Infoblox-Implementierung ohne Umschweife zusammen: „Threat Defense ist der Schutzwall um unsere Burg. Den müssen Angreifer erst überwinden, bevor sie die Außenwände beschädigen können. Wir werden sie ausschalten, bevor Sie uns zu nahe kommen.“

infoblox.

Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1.408.986.4000
www.infoblox.com/de

© 2025 Infoblox, Inc. Alle Rechte vorbehalten. Das Infoblox-Logo und andere hier dargestellte Marken sind Eigentum von Infoblox, Inc. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer.

Version: 20250620v1