infoblox.

FALLSTUDIE

Der Oxnard Union High School District nutzt Netzwerkinformationen, um proaktive Sicherheitsmaßnahmen zu ermöglichen

ÜBERSICHT

Der Oxnard Union High School District (OUHSD), gelegen im Ventura County, Kalifornien, umfasst 13 Schulen, die Schüler und Schülerinnen der Klassen 9 bis 12 betreuen.

Der Bezirk umfasst die Oxnard-Ebene, einschließlich der Städte Oxnard, Port Hueneme und Camarillo, sowie die nahegelegenen nicht eingetragenen Gemeinden El Rio, Somis und Channel Islands Beach.

> *"Mit BloxOne Threat Defense haben wir viel mehr Vertrauen in unsere Fähigkeit, alle Benutzer und Geräte im gesamten Bezirk vor Cyberangriffen zu schützen und Vorfälle zu verhindern, bevor sie passieren."*
>
> **Juan Castano**
> **Senior Network Administrator, Oxnard Union High School District**

DIE SITUATION

Ein uneinheitlicher Netzwerkbetrieb

Der Bezirk stellt jedem seiner fast 17.000 Lernenden und 1.900 Lehrkräfte und Bediensteten die Technologie und Unterstützung zur Verfügung, die sie zur Maximierung des Lernerfolgs benötigen. Für Juan Castano, den leitenden Netzwerkadministrator des OUHSD, ist dies ein gemeinschaftliches Unterfangen. „Alle arbeiten zusammen, um Ergebnisse zu erzielen."

Die Schulen des Bezirks stellen den Schülern und Schülerinnen entweder Chromebooks oder Windows-Laptops zur Verfügung, dazu eine Internetverbindung, Online-Portale und andere digitale Dienste. Unter dem Gesichtspunkt der Vernetzung und Sicherheit muss der OUHSD auch die verschiedenen zusätzlichen Laptops, Tablets und anderen persönlichen elektronischen Geräte, die von Lernenden und Lehrkräften im Laufe des Tages genutzt werden, unterbringen.

Vor diesem Hintergrund hatte sich die Landschaft des Bezirks für die Verwaltung kritischer Netzwerkdienste im Laufe der Zeit weiterentwickelt und umfasste unterschiedliche Lösungen, darunter Microsoft DNS und Active Directory sowie benutzerdefinierte Domain-Controller. Der Bezirk verwendete außerdem Infoblox NIOS für bestimmte Netzwerkzonen. Was die Sicherheit anbelangt, so hatten Castano und seine 15 Außendiensttechniker keine zuverlässige Möglichkeit zur Erkennung und Unterbindung von Sicherheitsvorfällen, bevor diese eintraten.

OXNARD UNION HIGH SCHOOL DISTRICT
Creating Prosperity through Equity, Inquiry, and Wellness

DIE HERAUSFORDERUNG

DNS-Konflikte und zeitaufwendige Sicherheitsmaßnahmen

Als Castano vor zwei Jahren seine jetzige Position antrat, war klar, dass die Netzwerkinfrastruktur des OUHSD die Effizienz beeinträchtigte. Um den Betrieb zu rationalisieren, begannen er und seine Mitarbeitenden damit, veraltete Server und Dienste auszumustern. Als diese Arbeit jedoch begann, kam es zu Ausfällen, sodass bestimmte Dienste nicht mehr erreicht werden konnten. „Die Dinge funktionierten einfach nicht“, erinnert er sich.

Die Ursache wurde bald auf unzusammenhängende Lösungen für die Verwaltung von DNS, DHCP und IP-Adressen (zusammenfassend als DDI bekannt) zurückgeführt, die alle modernen Netzwerkinteraktionen möglich machen. Da sich die IT-Infrastruktur des Bezirks im Laufe der Zeit entwickelt hatte, war der DNS-Traffic so konfiguriert worden, dass er zu Microsoft DNS-Servern und Infoblox NIOS-Servern geleitet wurde. Die daraus resultierenden DNS-Konflikte beeinträchtigten die Netzwerkleistung. Außerdem liefen grundlegende Funktionen wie das Network Time Protocol (NTP), das die Computeruhren der Netzwerkgeräte synchronisiert, auf mehreren Systemen. „Die Dinge zeigten auf einander. Es war ein riesiges Durcheinander“, sagt Castano.

Neben den Problemen bei der Netzwerkverwaltung hatte der OUHSD auch drängende Sicherheitsprobleme aufgrund der zeitaufwendigen Untersuchung von Bedrohungen und der Reaktionsprozesse. Wenn Castano und seine Kollegen einen Sicherheitshinweis erhielten, mussten sie eine langwierige, mehrstufige Untersuchung einleiten, bei der sie zwischen mehreren Tools hin- und herspringen mussten, um die betroffenen Geräte zu identifizieren, Details über die Bedrohung herauszufinden und Eindämmungs- oder andere Reaktionsmaßnahmen einzuleiten. Dieser Prozess war nicht nur zeitaufwändig, sondern auch sehr reaktiv. „Zu dem Zeitpunkt, als wir alle Untersuchungen abgeschlossen hatten, war es bereits zu spät, sodass wir das Problem irgendwie beheben mussten“, bemerkt Castano. „Es gibt eine ganze Phase, in der es nur um die Untersuchung und Entdeckung dieser einen Malware geht. Und dann kann man nur noch hoffen, dass es sich tatsächlich um diese eine Malware handelt. Die durchschnittliche Untersuchungszeit betrug vier Stunden.“

Die reaktive Sicherheitslage des Bezirks, die bereits ein Problem darstellte, wurde noch deutlicher, als das Department of Homeland Security (DHS) auf den Plan trat. Die Behörde machte den Bezirk darauf aufmerksam, dass auf einem der Rechner in seinem Netzwerk bestimmte Aktivitäten festgestellt worden waren, die auf einen möglichen Ransomware-Angriff hindeuteten. Ein Schüler hatte eine Unternehmenswebsite aufgerufen, um eine Vorlage für eine Hausarbeit herunterzuladen, die eine bösartige ausführbare Datei enthielt.

Die Sicherheitsmaßnahmen des OUHSD haben die Aktivität nicht aufgedeckt, aber die des FBI schon. Der fragliche Rechner wurde zwar schnell und ohne Schaden repariert, doch der Vorfall erregte die Aufmerksamkeit des Bezirks. „Das war ein wirklich böses Erwachen“, sagt Castano.

Kunde: ***Oxnard Union High School District***
Branche: ***Bildung***
Standort: ***Oxnard, Kalifornien***

ZIELE:

- Behebung der Netzwerkkonflikte, die durch mehrere Systeme für DNS, DHCP und IPAM verursacht werden
- Reduzierung des Server-Wildwuchses und Steigerung der betrieblichen Effizienz
- Verringerung des manuellen Aufwands für die Netzwerkverwaltung und die Untersuchung von Bedrohungen

ERGEBNISSE:

- Konsolidierte DNS-Verwaltung in eine einzige, einfach zu bedienende Lösung
- Vereinfachte Verwaltung kritischer Netzwerkdienste mit einer webbasierten Benutzeroberfläche, die keine Schulung erfordert
- Reduzierte durchschnittliche Untersuchungszeit von Bedrohungen von 4 Stunden auf 20 Minuten

PRODUKTE:

- NIOS DDI
- BloxOne Threat Defense

DIE LÖSUNG

DNS-Konsolidierung, proaktive Bedrohungserkennung und umfassende Sichtbarkeit

Für Castano bestand die Antwort auf die chronischen Netzwerkprobleme des Bezirks darin, alle DNS- und NTP-Zuständigkeiten in der bereits vorhandenen Lösung zu konsolidieren, die alle DDI-Anforderungen erfüllen konnte: Infoblox NIOS. „Anstelle dieser überkomplizierten Einrichtung, bei der wir Datensätze auf bestimmten Windows-Rechnern und Datensätze auf Infoblox haben und diese miteinander zu synchronisieren versuchen, beschlossen wir, alles auf das NIOS-Grid zu übertragen“, erinnert er sich.

Bei der Migration wurden wichtige DDI-Funktionen von Microsoft DNS und zusätzlichen Domain-Controllern auf Infoblox übertragen. Castano dankt Infoblox Professional Services für die Unterstützung seines Teams bei der reibungslosen und störungsfreien Durchführung der Migration. „Die Unterstützung war fantastisch, was die Umstellung zu einem echten Erfolg machte.“ Heute werden alle DDI- und NTP-Funktionen des Bezirks über das NIOS Grid verwaltet, das auf zwei virtuellen NIOS-Servern läuft. Nach dem Ransomware-Vorfall suchte der OUHSD nach einer Lösung zur Beseitigung der blinden Flecken, durch die Bedrohungen bisher unentdeckt blieben. Gleichzeitig sollten Castano und sein Team in die Lage versetzt werden, proaktiver zu handeln und Bedrohungen frühzeitig im Angriffszyklus vor ihrer Aktivierung zu erkennen und zu neutralisieren. Der Bezirk arbeitete mit Infoblox Professional Services zusammen, um BloxOne Threat Defense Advanced auf einer Proof-of-Value-Basis einzusetzen. Die Lösung bietet eine zentrale Sichtbarkeit und Kontrolle für jedes Gerät, das mit der Netzwerkinfrastruktur des Bezirks verbunden ist, KI und maschinelles Lernen zur Erkennung von Verhaltensbedrohungen sowie umfassende Funktionen zur Untersuchung von Ereignissen und zur Reaktion darauf. Von dem Moment an, als die Lösung in Betrieb genommen wurde, begann sie, Bedrohungen und Anomalien zu erkennen, die den vorhandenen Malware- und Bedrohungserkennungs-Tools des Bezirks entgangen waren. „Es war augenöffnend. Die Anzahl der eindeutigen Erkennungen war überraschend hoch“, sagt Castano. „Es gab viel mehr, was wir nicht gesehen hatten.“

DAS ERGEBNIS

Steigerung der Effizienz, Stärkung der Sicherheit

Durch die Eliminierung unnötiger Hardware und die Konsolidierung der DDI-Funktionen mit Infoblox ist die Netzwerkinfrastruktur des Bezirks viel schlanker und effizienter geworden. Castano und seine Netzwerktechniker verfügen nun über eine zentrale Plattform zur Netzwerkverwaltung in allen Schulen des Bezirks. Castano sagt: „Jetzt, wo alles auf NIOS zentralisiert ist, befinden sich alle meine Netzwerke an einem Ort. Ich kann einfach auf jedes Netzwerk zugreifen sowie reservierte IPs, feste IPs und Leases einsehen.“

Neben einer einfacheren Umgebung bietet NIOS Castano und seiner IT-Organisation eine noch nie dagewesene Einfachheit und Benutzerfreundlichkeit, angefangen bei der webbasierten Benutzeroberfläche. „Sie erfordert keinerlei Schulung und man weiß immer ganz genau, was vor sich geht. Wenn man eine neue Schule oder einen neuen Standort hinzufügt, lässt sich alles ganz einfach replizieren. Einfach alles funktioniert einwandfrei.“

Für Castano ist die Absicherung der Benutzer und Daten des Bezirks dank Infoblox auch wesentlich effizienter geworden. Zum Beispiel blockieren die Filterfunktionen von BloxOne Threat Defense automatisch den Zugriff von Studierenden und Lehrkräften auf bösartige Domains. Dadurch kann der OUHSD alarmierende Ereignisse wie das, das die Aufmerksamkeit der Homeland Security auf sich zog, vermeiden. Die Funktion nutzt den riesigen DNS-Datenspeicher von Infoblox und aktuelle Bedrohungsdaten zur Erkennung von Sicherheitsproblemen, die andere Lösungen nicht erfassen können. So kann Castano Ziele, die mit Hackerangriffen, Malware, NX-Domains und dubiosen IP-Adressen in Verbindung gebracht werden, mit hoher Genauigkeit blockieren und sicherstellen, dass der legitime Traffic ungehindert fließt. Die proaktive Natur der Infoblox-Filterung gibt Castano Sicherheit. „Mit BloxOne Threat Defense haben wir viel mehr Vertrauen in unsere Fähigkeit, alle Benutzer und Geräte im gesamten Bezirk vor Cyberangriffen zu schützen und Vorfälle zu verhindern, bevor sie passieren.“

Wenn heute Sicherheitsereignisse eintreten, verkürzt der umfassende Einblick in die Bedrohungen, den Castano durch Infoblox erhält, die Reaktionszeit. „Was normalerweise vier Stunden dauern würde, dauert jetzt etwa 20 Minuten. Kritischer Gerätekontext wird automatisch von der IPAM-Lösung gesammelt und mit Sicherheitswarnungen versehen. Die Dossier-Funktion in BloxOne Threat Defense automatisiert viele der zuvor mühsamen Schritte zur Untersuchung von Bedrohungen, damit die Analysten mehr über die Bedrohung, die dahinter stehenden Akteure, die WHOIS-Daten hinter der Hosting-Site und mehr erfahren. „Es ist ungeheuer hilfreich, dass alles für mich gesammelt und an einem Ort präsentiert wird, statt dass ich all diese Informationen manuell suchen muss. Das ist eine enorme Zeitersparnis."

Wenn es um Cybersicherheit oder Netzwerkmanagement geht, ist Zeit alles. Dank Infoblox können Castano und seine Mitarbeitenden noch mehr Zeit sparen, denn sie haben eine einzige Umgebung, in der sie leicht zwischen Netzwerk- und Sicherheitsaufgaben wechseln können. Und das ist ein entscheidender Vorteil für kleine und mittelgroße Organisationen wie die ihre, in denen alle Mitarbeitenden verschiedene Funktionen übernehmen müssen. Wenn beispielsweise verdächtige DNS-Aktivitäten auf einem Rechner im Netzwerk auftreten, kann Castano den DNS-Verlauf des Geräts schnell auf unangemessenes Verhalten, verdächtige Web-Apps oder tatsächliche Cyberbedrohungen untersuchen. Die umfangreichen Gerätedaten von NIOS liefern automatisch den Kontext zu diesen Ereignissen, einschließlich umfangreicher Benutzer- und Gerätedetails. „Da ich in NIOS alles so sauber unterteilt habe, kann ich ein Ereignis nicht nur schnell auf den Standort, sondern auch auf das jeweilige Gebäude eingrenzen." Sobald eine Cyberbedrohung lokalisiert ist, kann sich das Team auf die schnellen Funktionen von BloxOne Threat Defense verlassen, um ein betroffenes Gerät automatisch zu isolieren und zu bereinigen.

Die Zusammenführung von Netzwerk und Sicherheit mit Infoblox hilft dem OUHSD nicht nur, die Netzwerkleistung und den Schutz zu verbessern, sondern gibt Castano und seinen Mitarbeitenden auch die Freiheit, innovativ zu sein. „Ich verbringe nicht mehr einen großen Teil meines Tages mit der Sicherstellung, dass alles gut läuft", bemerkt er. „Infoblox gibt mir die Freiheit, für die Zukunft zu planen, und diese Zeiteinsparungen sind wirklich wichtig, denn ohne sie würde ich mich nur im Kreis drehen und alltägliche Prozesse reparieren."

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

+1 408 986 4000
www.infoblox.com

Version: 20241004v1