

FALLSTUDIE

Stadt Stockton optimiert die Netzwerkinfrastruktur, verbessert die Sicherheit und reduziert den Verwaltungsaufwand mit Infoblox



ÜBERSICHT

Die **Stadt Stockton** ist der Verwaltungssitz des San Joaquin County im kalifornischen Central Valley.

Mit über 320.000 Einwohnern ist sie die bevölkerungsreichste Stadt des Landkreises und die elftgrößte Stadt Kaliforniens. Sie wurde 1999, 2004, 2015 sowie erneut 2017 und 2018 zur All-America City ernannt.

Mit fast sechzig Mitarbeitern ist das IT-Team von Stockton für die Verwaltung eines sicheren Netzwerks verantwortlich, das fast 2.000 Mitarbeiter in verschiedenen städtischen Abteilungen unterstützt, darunter Feuerwehr, Polizei, öffentliche Bauvorhaben, Tierschutz, Stadtwerke, Müllentsorgung und Recycling.

DIE SITUATION

Zukunftsorientierte IT-Abteilung gebremst durch Legacy-Netzwerktechnologie

Im Herbst 2023 trat Jamil Niazi der Stadt Stockton als Chief Technology Officer und IT-Direktor bei. Als gefragter Technologie-Veteran mit einer nachgewiesenen Erfolgsbilanz in der Leitung von IT-Organisationen im öffentlichen und privaten Sektor nahm er schließlich das Angebot an, das am besten mit seinen eigenen Ansichten darüber übereinstimmte, was moderne IT leisten kann. „Ich habe mich für die Stadt Stockton entschieden, weil ihre Führungsebene eine Leidenschaft und Vision für Technologie hat“, sagt er

Jamil war von Anfang an beeindruckt. Das Engagement des Stadtmanagers, die besten Lösungen für Cybersicherheit, KI, Cloud, Resilienz und andere Anforderungen einzusetzen, fand bei ihm Anklang. Die Stadt nutzte zahlreiche Sicherheitstools und setzte auch VMware sowie mehrere Cloud-Datensicherungslösungen wie Rubrik und Cohesity ein. Um das Disaster Recovery zu stärken, hatte Stockton Fördermittel erhalten, um ein Backup-Rechenzentrum im Hafen von Stockton einzurichten, das von PG&E auf einem separaten Stromnetz betrieben wird.

“ Infoblox bietet einen unglaublichen Mehrwert für Cybersicherheit, Produktivität und Ausfallsicherheit. Wir erhalten Spitzentechnologie und müssen uns nicht mehr darum sorgen, dass wir uns in die Details vertiefen müssen, um das zu bauen, was wir benötigen.

Jamil Niazi,
Chief Information Officer, Stadt Stockton

Jamil schätzte, dass er als neuer CIO der Stadt vollständige Autonomie bei der Bewertung und Beschaffung von Technologie haben würde. Er war jedoch besorgt über den aktuellen Ansatz zur Verwaltung von DNS, DHCP und IP-Adressmanagement (DDI). Die selbstentwickelte Lösung erfüllte ihren Zweck, verursachte jedoch auch einige Probleme, die mit der Mission der IT-Organisation, die „besten verfügbaren Technologien“ zu verwenden, in Konflikt standen.

DIE HERAUSFORDERUNG

Manuelle Verwaltung, mangelnde Sichtbarkeit und Kontrolle

Ein zentrales Problem mit Stocktons DDI-System war die Verwaltung von IP-Adressen. Jedes Gerät in einem Netzwerk benötigt eine dedizierte IP-Adresse, und eine kompetente Verwaltung dieser Adressen ist entscheidend für eine zuverlässige Netzwerkkonnektivität. In einer Stadt wie Stockton könnten IP-Adressprobleme möglicherweise Feuerwehrfahrzeuge, Streifenwagen und Mitarbeiter der öffentlichen Sicherheit beeinträchtigen und damit Leben und Eigentum gefährden. Als Jamil ankam, wies das bestehende System zur Verwaltung von IP-Adressen mehrere Einschränkungen auf. Zum Beispiel wurde es intern mit sogenannter „freier“ Software zusammengestellt, die für dynamische Netzwerkkumgebungen nicht geeignet war. Es war auch nur einer Person gleichzeitig möglich, auf das System zuzugreifen, was einen Single Point of Failure darstellte, wenn es darum ging, Updates und Fehlerbehebungen rechtzeitig durchzuführen.

Darüber hinaus erforderte das bestehende System, dass die IT-Mitarbeiter die Zehntausenden von IP-Adressen der Stadt mithilfe von Tabellenkalkulationen und ohne konsistente, leicht aktualisierbare Dokumentation verwalteten. IP-Adressenkonflikte waren unvermeidlich und beeinträchtigten die Zuverlässigkeit des Dienstes. Ein grundlegendes Hindernis war, dass Jamil und seine Kollegen keine wesentliche Kontrolle über die IP-Adressen hatten, was ein erhebliches Hindernis für ein so komplexes Netzwerk wie das von Stockton darstellt. „In unserem Netzwerk gibt es eine Menge komplizierter IP-Adressen“, sagt Jamil. Zu diesen Komplexitäten gehören die privaten VPNs und die computergestützten Einsatzleitsysteme (CAD), die von den Feuerwehr- und Polizeidienststellen genutzt werden, sowie die fortlaufende Notwendigkeit, nahtlos mit VLANs zu interagieren, die in anderen lokalen und regionalen öffentlichen Sicherheitsnetzwerken verwendet werden.

Das Problem für die Netzwerkadministratoren von Stockton bestand darin, dass ihre vorhandene IPAM-Implementierung keinen Einblick in die IP- und MAC-Adressen der Geräte bot, wann sie erschienen, in welches Subnetz/VLAN sie sich befanden, in die Geräteattribute oder in die DNS- und DHCP-Einträge. Ein weiteres Problem war, dass alle Änderungen, wie das Hinzufügen und Entfernen von IP-Bereichen und DNS-Einträgen sowie das Aktualisieren von Switch-Ports, manuell vorgenommen werden mussten, was für jedes Netzwerkteam eine mühsame und fehleranfällige Aufgabe darstellte.

Darüber hinaus müssen die Subnetze für die Feuerwehr und die Polizei von Stockton von anderen Netzwerksegmenten getrennt werden, um die Konformität mit den Criminal Justice Information Services (CJIS) aufrechtzuerhalten. Ohne klare Einsicht in die IP-Adresszuweisungen und ohne klare Dokumentation hatten die IT-Mitarbeiter von Stockton keine Möglichkeit, sofort zu erkennen, wann ein Gerät nicht konform war. Diese Unsicherheit führte zu Verbindungsstörungen. In einem Fall konnte sich ein Stadtverantwortlicher nicht in das Netzwerk einloggen. Nach einer Untersuchung stellte die IT-Abteilung schließlich fest, dass der Benutzer einen Laptop verwendete, der nicht für den IP-Adressbereich autorisiert war, der mit diesem Subnetz verbunden ist.

Kunde: Die Stadt Stockton
Branche: Regierung
Standort: Stockton, Kalifornien

ZIELE:

- Ersetzen Sie die störungsanfällige Implementierung der IP-Adressverwaltung, um einem „Best Technology“-Mandat gerecht zu werden und gleichzeitig die Migrationszeit zu minimieren.
- Reduzieren Sie Netzwerkunterbrechungen, die durch die manuelle Verwaltung von IP-Adressen in Tabellenkalkulationen verursacht werden.
- Verbesserung der Sicherheit für IP-Adressen

ERGEBNISSE:

- Robustere, automatisierte DDI-Lösung in weniger als zwei Monaten
- Reduzierung der DDI-Fehlerbehebungsaufgaben von 40 Stunden im Monat auf praktisch null
- Eine gestärkte Sicherheitslage mit verbesserter IP-Adressen-Automatisierung und Effizienz.

PRODUKTE:

- NIOS DDI

Die IT-Abteilung musste routinemäßig solche Probleme lösen. Dieser Aufwand beanspruchte Zeit und Aufmerksamkeit. Es war erforderlich, unzählige Tabellenkalkulationen zu durchforsten, um den Status der IP-Adressen einzelner Geräte nachzuverfolgen, was häufig zu Missverständnissen darüber führte, welche Adressen und Subnetze aktualisiert worden waren.

Die Stadtverantwortlichen waren kaum die einzigen, die betroffen waren. Das Team von Jamil verbrachte bis zu 40 Stunden im Monat mit der Behebung von Verbindungsproblemen, die Mitarbeiter in der ganzen Stadt betrafen. Die Folgen gingen über die IT hinaus. Sie haben einen Feuerwehrmann oder einen Polizisten, der um 3 oder 4 Uhr morgens nicht online gehen kann. Sie verlieren Zeit wegen Verbindungsproblemen. „Sie rufen mich an, ich wende mich an den zuständigen Mitarbeiter, und wenn er das Problem nicht lösen kann, muss er es an einen ranghöheren Mitarbeiter weiterleiten“, sagt Jamil „Das ist viel verlorene Zeit.“

Die Risiken der bestehenden IP-Adressverwaltung der Stadt umfassten mehr als nur die Zuverlässigkeit und Leistung des Netzwerks. Der manuelle Aspekt der IP-Adressverwaltung erhöhte ebenfalls die Sicherheitsrisiken. Jamil und seine Kollegen waren gezwungen, die IP-Adress-Tabellen der Stadt per E-Mail oder über Online-Plattformen auszutauschen und zu aktualisieren, wodurch sie potenziell Bedrohungsakteuren ausgesetzt wurden. Aus Jamils Sicht musste die IP-Adressverwaltung der Stadt vollständig automatisiert und die Adressdatenbank gesichert werden.

DIE LÖSUNG

Schnelle Migration zu einer robusten IP-Adressverwaltung

Als Jamil beschloss, dass es an der Zeit war, die problembehaftete DDI-Lösung der Stadt zu ersetzen, stand Infoblox bereits auf dem Radar der IT-Abteilung. Die Stadt hatte die Lösungen von Infoblox untersucht, bevor er an Bord kam. Jedoch führten diese Diskussionen immer zu demselben Schluss: Die bestehende Implementierung der Stadt war zu stark verankert, und ein Austausch wäre zu zeitaufwendig und riskant.

Trotz dieser Einwände wusste Jamil, dass aus technologischer Sicht die Beibehaltung des Status quo mit der bestehenden DDI-Lösung keine tragfähige Option war. Daher begannen er und sein Team, die wesentlichen Anforderungen für ein neues DDI-System zu identifizieren. Aus seinen Recherchen erfuhr er, dass die IP-Adressautomatisierung, die Sicherheits- und Berichtsfunktionen von [NIOS DDI](#) seinen Kriterien entsprachen. Zudem würden die Verteilungsfähigkeiten des Infoblox Grid die hohe Verfügbarkeit bieten, die das städtische Netzwerk erforderte.

Jamil war sehr daran interessiert, NIOS zu übernehmen, bestand jedoch darauf, dass die Migration in höchstens drei Monaten erfolgen müsse, ein Zeitrahmen, der von vielen seiner Gesprächspartner, darunter auch andere Anbieter, als zu optimistisch angesehen wurde. „Alle sagten, die Umstellung würde zwischen sechs Monaten und einem Jahr dauern, da unser Netzwerk so komplex sei.“ In Gesprächen mit [Infoblox Professional Services](#) und dem NIOS-Projektteam erhielt er eine ganz andere Antwort. „Sie bestanden darauf, dass wir das in einem Monat schaffen könnten, wenn wir uns einmal pro Woche treffen würden. Fast hätten wir es geschafft. Das einzige Hindernis war unsere Terminplanung.“

Jamil führt die reibungslose Einführung auf die gründliche Planung und klare Kommunikation der Infoblox-Teammitglieder zurück. „Sie sind wirklich engagiert.“ „Sie haben Dinge gesehen, die wir vielleicht nicht gesehen haben, und die Details wirklich ausgearbeitet.“

DAS ERGEBNIS

Beseitigung von Netzwerkunterbrechungen, Senkung der Kosten und Verbesserung der Sicherheit

Nach Abschluss der Migration erhielt das Netzwerk von Stockton die felsenfeste Konnektivität und Ausfallsicherheit, die ihm mit dem vorherigen DDI-System gefehlt hatte. Die NIOS-Lösung der Stadt umfasst virtuelle Infoblox-Server sowie zwei physische Server, die sich im Rechenzentrum von Stockton befinden, um die Disaster Recovery und Geschäftskontinuität weiter zu verbessern.

NIOS automatisiert die IP-Adressverwaltung von Stockton vollständig und ermöglicht die vollständige Erkennung aller Adressen und endpoints. Es wird sichergestellt, dass IP-Adressen stets aktuell sind, über die DDI-Infrastruktur von Stockton synchronisiert werden und korrekt den richtigen Subnetzen zugeordnet sind. Darüber hinaus werden die IP-Adressen der Stadt jetzt in einer hochsicheren, zugriffsgeschützten Datenbank verwaltet.

Der unmittelbarste Vorteil nach der Migration war die Möglichkeit für jede Person, selbst mit minimaler Schulung, DDI-Aufgaben über die intuitive Weboberfläche von Infoblox durchzuführen. Heute können mehrere Mitarbeiter des IT-Teams gleichzeitig arbeiten, wodurch der Single Point of Failure der vorherigen Implementierung entfällt und die Problemlösung erheblich beschleunigt wird.

Mit den umfangreichen Dashboards in NIOS hat Jamils Team einen granularen Einblick in alle IP-Adressen gewonnen. Sie müssen nicht mehr durch Tausende von Tabellenkalkulationszeilen blättern. „Alles ist in Ordnung. Wir können jedes einzelne Gerät sehen, das eine verwaltete IP-Adresse hat“, sagt er. Für das IT-Team der Stadt ist es jetzt ein Kinderspiel, IP-Adressen zuzuweisen oder Konflikte zu beheben. „Das ist das Schöne an Infoblox. Man muss keine Personen ausfindig machen, keine Tabellen einsehen und keine IP-Konfigurationen durchführen. Man geht einfach zum Dashboard, und bumm, schon ist es erledigt.“

Die Einhaltung der CJIS-Vorschriften ist jetzt ebenfalls viel einfacher, da die Teammitglieder schnell Details wie einzelne Domain-Controller und mobile Geräte in Polizeiautos und Feuerwehrautos einsehen können. Mit NIOS konnte Stockton die durch Nichteinhaltung verursachten Störungen sowie Konflikte mit anderen öffentlichen Sicherheitsnetzwerken im Virtual Local Area Network vermeiden. „Wir haben keines dieser Probleme gehabt. Kein einziges“, sagt Jamil.

Für Stockton hat die zuverlässige und effektive Verwaltung von IP-Adressen erhebliche Einsparungen generiert. Seit der Implementierung von NIOS gab es keine Anrufe mehr von Feuerwachen um 3 Uhr morgens. NIOS hat diese Vorfälle und die damit verbundenen kostspieligen Überstunden beseitigt. Darüber hinaus hat die Lösung das IT-Team der Stadt davon befreit, ständig Verbindungsstörungen beheben zu müssen, was bis zu 40 Stunden pro Monat in Anspruch nehmen konnte, sodass sie sich stattdessen auf wertvollere Aufgaben konzentrieren können. „Es ist schwer, es in Zahlen zu fassen, aber die Einsparungen waren grenzenlos. Früher fielen uns durch Reaktionen auf Ausfälle erhebliche Überstundenkosten an. Jetzt sparen wir nicht nur diese Stunden, sondern haben auch den Stress und die Auswirkungen auf unser Team beseitigt.“

Im Sicherheitsbereich leistet NIOS mehr, als nur die IP-Adressdatenbank von Stockton zu schützen. Durch die Beseitigung von Adressduplikaten, Konflikten und Instanzen der Nichteinhaltung wird auch die Sicherheitslage der IT-Abteilung verbessert. „Unsere Anfälligkeit für IP-Adressen hat sich durch diese Implementierung erheblich verringert“, sagt Jamil.

Mit Infoblox können Jamil und sein Team schneller auf Sicherheitsereignisse reagieren. Wenn die IT beispielsweise eine Warnung von einer Endpunktsicherheitslösung erhält, die mit bestimmten IP-Adressen verknüpft ist, müssen die Teammitglieder keine Zeit mit Untersuchungen oder dem Zugriff auf verschiedene Tools verbringen, um die betroffenen Geräte zu finden. „Sie gehen zu Infoblox und die IP-Quelle ist direkt dort. Sie identifizieren es, deaktivieren es und eliminieren die Bedrohung direkt über Infoblox“, sagt Jamil.

In den kommenden Monaten plant die Stadt Stockton, ihre Sicherheit weiter zu verbessern, indem sie [Infoblox Threat Defense™](#) einsetzt. Obwohl die Zusammenarbeit mit NIOS Jamils erste Erfahrung mit Infoblox ist, plant er, darauf aufzubauen. „Infoblox bietet einen unglaublichen Mehrwert für Cybersicherheit, Produktivität und Ausfallsicherheit. Wir erhalten Spitzentechnologie und müssen uns nicht mehr um die Details kümmern, um das zu entwickeln, was wir brauchen.“



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