



EMEA-basierter Internet- und Kommunikationsanbieter sichert Schulnetzwerke mit Infoblox

DER KUNDE: TELEKOMMUNIKATIONSDIENSTLEISTER AUS DER EMEA-REGION

Ein in der EMEA-Region ansässiger Internet- und Kommunikationsanbieter, der für die Gewährleistung der Internetsicherheit und die Bereitstellung von Telekommunikationsdiensten für akademische Einrichtungen zuständig ist, wurde für den Aufbau eines groß angelegten nationalen Bildungsnetzwerks ausgewählt. Das Projekt basiert auf der Prämisse, 4,5 Millionen Kindern mit 700.000 Schulcomputern in 25.000 Grund- und Sekundarschulen eine sichere Internetverbindung zu bieten.

DIE HERAUSFORDERUNG

Sicherstellung eines sicheren Internetzugangs über große Netzwerke hinweg

Der Telekommunikationsdienstleister wollte sicherstellen, dass die Netzwerkverbindungen und das Nutzererlebnis nicht nur stabil, sondern auch sicher sind, vor allem, weil es sich bei den Nutzern um Schulkinder handelt. Außerdem sollte sichergestellt werden, dass die Kinder nicht auf ungeeignete Websites gehen oder versehentlich Malware herunterladen. Bei einem so umfangreichen Projekt war die Implementierung sicherer Web-Gateways (Secure Web Gateways, SWGs) allein zur Inhaltsfilterung ein hohes Risiko. Niemand hatte zuvor eine so umfangreiche Implementierung von SWGs durchgeführt. (Der geschätzte Download-Traffic liegt bei über 1 TBit/s, wofür etwa 200 Geräte der wichtigsten SWG-Anbieter benötigt werden). Für den Fall, dass etwas schief geht, wollte der Internetanbieter eine Möglichkeit zur Ergänzung der SWGs. Der Anbieter wollte sich jedoch nicht auf SaaS-basierte Sicherheitslösungen verlassen. Stattdessen musste die Sicherheitsimplementierung vor Ort, also On Premises, erfolgen, da er seine eigenen Netzwerke, Clouds und Rechenzentren aufbaute.

Das große private Netzwerk, das der Anbieter aufbaute, erforderte 100-Megabit-Verbindungen mit Routern für jede der 25.000 Schulen. Das Projekt wurde in drei Phasen unterteilt: Bereitstellung der Verbindungen, Bereitstellung der Netzwerkausrüstung und Sicherheit. Das Thema Sicherheit wurde in zwei Phasen umgesetzt. Die erste umfasste die grundlegende Sicherheit mit DNS Application Delivery Controllern (ADCs) und Firewalls. Die zweite umfasste den Einsatz von Web-Gateways.

Kunde: Internet- und Kommunikationsanbieter
Branche: Telekommunikation
Standort: EMEA

ZIELE

- Ein stabiles Netzwerk für ein groß angelegtes Bildungssystem aufbauen
- Bereitstellung einer sicheren Internetverbindung
- Implementierung einer lokalen Lösung

ERGEBNISSE:

- Ein sicheres und sauberes Surf-Erlebnis
- Malware-Abwehr
- DNS-basierte Inhaltsfilterung
- Grundlegende Sicherheitsdienste
- Eine kosteneffiziente, skalierbare Lösung

PRODUKTE

- NIOS DDI
- Einblick in die Bedrohung

DIE LÖSUNG

DNS-basierte grundlegende Sicherheit in einem internen privaten Netzwerk

Infoblox bewertete das Projekt der Schule und schlug vor, als ersten Schritt zum Schutz der Schulnetzwerke eine DNS-basierte Basissicherheit in Betracht zu ziehen. Obwohl auch SaaS-Anbieter an das Unternehmen herangetreten sind, hat es diese nie wirklich in Betracht gezogen. Grund dafür war, dass es etwas wollte, das in dem internen privaten Netzwerk eingesetzt werden konnte, das es für die Schulen aufbaute. Die meisten Dienstleister bauen ihre eigene Infrastruktur auf und werden deshalb keinen SaaS-basierten Dienst nutzen.

Mehrere zusätzliche Faktoren führten dazu, dass sich der Anbieter für Infoblox gegenüber anderen Wettbewerbern entschied:

- Infoblox bot **differenzierte Funktionen** an, wie z. B. Threat Insight, das in DNS-Anfragen versteckten Malware-Befehls- und Kontrolltraffic erkennen kann. Es kann auch das Vorhandensein von DNS-Tunneling erkennen, eine gängige Methode, die einige Schüler unter Umständen zur Umgehung der Beschränkungen der SWG-Sicherheitsrichtlinien nutzen können.
- Der Anbieter war der Meinung, dass Infoblox aufgrund seines technischen Fachwissens vor Ort ein **besserer technischer Partner** sei, was andere Wettbewerber aufgrund fehlender technischer Experten in der Region nicht erreichen konnten.
- Infoblox hat Referenzen von vielen anderen Dienstleistern und ähnlichen Einsätzen vorgelegt, die die Infoblox-Technologie nutzen.

Im Rahmen seiner Diskussionen veranstaltete Infoblox einen umfassenden Sicherheitsworkshop, der verschiedene Beispiele für Malware und deren Nutzung des DNS für Befehls- und Kontrollfunktionen behandelte. Darüber hinaus entwickelte sich eine grundlegende Diskussion mit Infoblox über die Eindämmung von Malware schnell zu einer umfassenderen Diskussion, die Folgendes umfasste:

- Wie die Kategorisierung von Inhalten mithilfe von DNS die Leistung von sicheren Web-Gateways kosteneffizient steigern kann
- Wie die Überprüfung des Datenverkehrs auf DNS-Ebene eine stabile, skalierbare Erweiterung für SWGs bieten kann. Mit Infoblox ist der Anbieter jetzt in der Lage, Schülern den Zugriff auf offensichtlich ungeeignete Inhalte wie Websites für Erwachsene zu verwehren, indem er den Datenverkehr auf DNS-Ebene blockiert. Nebulösere Websites wurden mithilfe von SWGs auf der Grundlage von URLs gefiltert (Abb. 1).
- Wie dieser kombinierte Ansatz die Menge an böartigem Datenverkehr, den die SWGs bewältigen müssen, begrenzt und die Gesamtkosten der Bedrohungsabwehr senkt

DAS ERGEBNIS

Eine einfache, stabile Implementierung, die sofortigen Mehrwert bietet

Während des ersten, begrenzten Einsatzes implementierte ein Infoblox-Partner die DNS-Lösung in nur sieben Tagen für zwei Standorte des Diensteanbieters. Dieser Einsatz hat gezeigt, dass die Infoblox-Lösung **einfach zu implementieren und stabil** ist, was den Anbieter zuversichtlich stimmte, dass die Lösung auch in großem Maßstab funktionieren würde. Die Implementierung für die restlichen 16 Standorte läuft seit Juni 2019. Der Anbieter hat bereits mehrere Vorteile festgestellt, darunter die zentrale Verwaltung von Sicherheitsrichtlinien auf DNS-Firewalls und die Abmilderung vorübergehender Probleme mit der Traffic-Kontrolle auf ADC und SWG dank der Inhaltsfilterung auf den DNS-Servern von Infoblox, die sich als wertvolle Erweiterungs- und Entlastungslösung erwiesen hat. Mit Hilfe von Infoblox war der Anbieter somit in der Lage, **ein sicheres und sauberes Surferlebnis für Lernende in der gesamten Region zu bieten**.

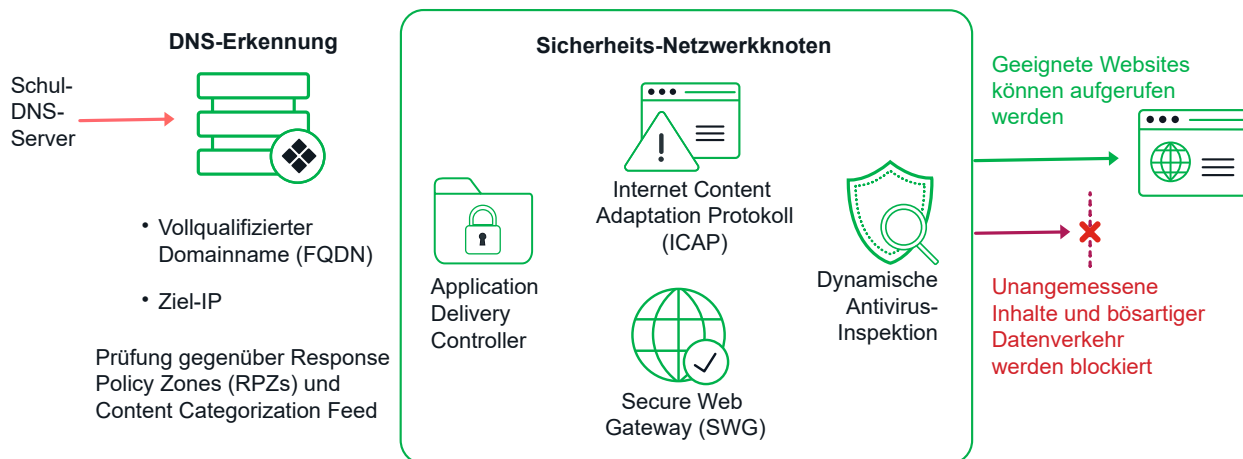


Abbildung 1: Die Infoblox-Lösung nutzt DNS-basierte Inhaltskategorisierung und -inspektion, um SWGs bei der Inhaltsfilterung zu unterstützen.



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