infoblox

CASE STUDY

infra fürth schärft Security-Werkzeugkasten mit den Lösungen von Infoblox

Die infra fürth Unternehmensgruppe stellt als eines von knapp 2.500 Stadtwerken in Deutschland die Grundversorgung der Bevölkerung sicher. Zu ihren vielfältigen kommunalen Aufgaben zählen unter anderem die Versorgung der Bevölkerung mit Strom, Gas, Wasser und Fernwärme, die Betreuung des ÖPNV sowie der Bäder- und Parkhausbetrieb. Die infra fürth unterhält auch eigene Energieerzeugungsanlagen für Ökostrom. Fast 700 Beschäftigte betreuen rund 70.000 infra fürth-Kunden vor Ort und verhelfen ihnen zu einer besseren Lebensqualität. Bei so vielen verschiedenen und vor allem versorgungskritischen Leistungen spielt die eigene IT-Infrastruktur für infra fürth eine wichtige Rolle.

> *Dank Infoblox wird das betroffene Gerät jetzt im Bereich von Sekunden ausfindig gemacht. Vorher lag das im Bereich von Stunden."*

infra fürth

DIE HERAUSFORDERUNG

Kritische Infrastruktur braucht den bestmöglichen Schutz

Als Grundversorger zählt infra fürth zu den vom Bund definierten Kritischen Infrastrukturen (KRITIS) in Deutschland. Ein Ausfall ihrer Dienstleistungen – egal, ob durch Netzwerkprobleme oder Cyberangriffe verursacht – könnte zu „nachhaltig wirkenden Versorgungsengpässen und erheblichen Störungen der öffentlichen Sicherheit" führen. Deshalb beschäftigt sich infra fürth schon seit über 20 Jahren mit dem Thema Cybersecurity und ist bereits seit 16 Jahren voll ISO 27001 zertifiziert. Doch gerade in Zeiten, in denen Hackerangriffe auch bei Kritischen Infrastrukturen immer häufiger zu Ausfällen führen, ist es für infra fürth von entscheidender Bedeutung, die richtigen IT-Werkzeuge zu haben, um Kundendaten und die Daseinsvorsorge in Fürth schützen zu können.

Eine Situation, in der nicht nur infra fürth steckt: Zahlreiche Stadtwerke in Deutschland haben in den letzten Monaten und Jahren bereits Ausfälle ihrer Leistungen durch Cyberangriffe zu verzeichnen gehabt. Damit reihen sie sich in einen globalen Trend ein. Insbesondere Ransomware-Attacken machen Behörden, Krankenhäusern, Hochschulen und zahlreichen anderen öffentlichen Einrichtungen das Leben schwer. Das bestätigt auch der Global State of Security Report 2023 von Infoblox. Phishing- und Ransomware-Attacken waren demnach die häufigsten Angriffsmethoden in Deutschland und auf der ganzen Welt.

„Wir stehen klar im Fokus der Angreifer", schätzt Martin Hofmann, technischer CIO von infra fürth, die Lage ein. „Unsere Herausforderung ist es, den IT-Service für unsere knapp 700 Mitarbeiter an verschiedenen Standorten mit unterschiedlichsten Aufgaben sicherzustellen. Um dies zu gewährleisten haben wir unseren Schutz mit Infoblox bewusst auf ein neues Level gehoben."

Kunde: ***infra fürth***
Branche: ***Stadtwerke und Versorger***
Standort: ***Fürth, Deutschland***

VORHABEN:

- Absicherung der Kritischen Infrastruktur
- Zentrale Verwaltung aller DDI-Services
- Transparenz des DNS-Traffics

ERGEBNISSE:

- Schnelle und reibungslose Integration auch ohne Proof-of-Concept
- Schnelle Sichtbarkeit infizierter Geräte
- Skalierbarkeit der DDI-Lösung

LÖSUNGEN:

- Infoblox NIOS DDI
- BloxOne® Threat Defense

DIE LÖSUNG

Netzwerkmanagement und Security gehen Hand-in-Hand

Bei infra fürth gehen Netzwerkmanagement und Netzwerksicherheit Hand-in-Hand und sind auch organisatorisch vereint. Ideale Voraussetzungen für den Einsatz der Lösungen BloxOne ThreatDefense und NIOS DDI von Infoblox. Denn die Lösungen spielen sich quasi die Bälle zu und überwinden die klassischen Silos von Netzwerkmanagement und Security: NIOS liefert eine einheitliche und zentrale Verwaltung aller DNS-, DHCP- und IPAM-Services für hybride und Multi-Cloud-Netzwerke, die sich damit zentral steuern und automatisieren lassen. Das bestätigt auch Hofmann: „NIOS DDI ist für uns ein flexibles System, das skalieren kann und sehr granulare Transparenz bringt." BloxOne Threat Defense arbeitet auf DNS-Ebene, um mit seiner tiefgreifenden Visibilität Angriffe frühzeitig zu stoppen. Gerade auch die Integration in ein breites Ökosystem erhöht die Effektivität des bestehenden Security-Stacks. Hofmann berichtet: „Infoblox ist ein wichtiger Baustein in unserem Security-Baukasten, der uns hilft, Früherkennung und Frühabwehrmaßnahmen zu fahren. Die umfassende Transparenz hilft Hofmann und seinem Team ganz konkret zu erkennen, welches Gerät mit wem kommuniziert – auch wenn es schadhafte Kommunikation ist. „Dank Infoblox wird das betroffene Gerät jetzt im Bereich von Sekunden ausfindig gemacht. Vorher lag das im Bereich von Stunden", berichtet Hofmann.

Die Implementierung von BloxOne Threat Defense und NIOS DDI bei infra fürth lief schnell – selbst ohne Proof-of-Concept vorweg. „Bereits Anfang Dezember, also knapp 3 Monate nach Kauf, waren wir mit allen Segmenten voll produktiv", berichtet Hofmann. Nach einer kurzen Warmlaufphase, in der noch kleinere, Infrastruktur-bedingte Anpassungen gemacht wurden, läuft Infoblox nun absolut reibungslos.

infra fürth zeigt, dass es sich als Stadtwerk lohnt, Netzwerkmanagement und Security zu verbinden. Denn die Absicherung der Kritischen Infrastruktur der infra fürth hat durch den Einsatz von Infoblox deutlich dazu gewonnen. „Infoblox ist für uns ein wirkungsvolles Tool, das wir auch schon für unsere Abwehr verwendet haben", so Hofmann. „Die Netzwerk-Transparenz und die Möglichkeit, schnell reagieren zu können, wenn es nötig ist, haben uns überzeugt."