infoblox

CASE STUDY

infra fürth augments security toolbox with Infoblox solutions

OVERVIEW

As one of almost 2,500 municipal utilities in Germany, the infra fürth group serves the citizens of the city of Fürth in Germany's Barvaria region with critical infrastructure and services.

Infra's municipal responsibilities are diverse and include supplying the population with electricity, gas, water and district heating, public transport and managing swimming pools and car parks. infra fürth also maintains its own energy generation plants for green electricity. Almost 700 employees support 70,000 local customers, helping them achieve and sustain a better quality of life. With such varied and supply-critical services, infra fürth's IT infrastructure has a significant role to play.

> *"With Infoblox, an affected device can now be located in seconds. This used to take hours."*
>
> **Martin Hofmann,**
> **Technical CIO, infra fürth**

THE CHALLENGE

Critical infrastructure requires the best protection

As a default service provider, infra fürth is one of the critical infrastructures (KRITIS) federally specified in Germany. A service outage – whether caused by network problems or a cyber attack – could lead to "long-lasting supply shortages and significant disruptions to public safety." Consequently, infra fürth has prioritized cybersecurity for more than 20 years and has been fully ISO 27001 certified for the past 16. Even so, it is crucial for infra fürth to have access to the right IT solutions to safeguard customer data and public services in Fürth, particularly in today's climate where hacker attacks cause increasing downtime, even for critical infrastructures.

infra fürth

infra fürth isn't alone in this experience; numerous municipal utilities in Germany have also experienced service outages due to cyber attacks over recent months and years. Their experiences form part of a global trend. Ransomware attacks, in particular, make things difficult for government agencies, hospitals, universities and a wide range of public institutions, as confirmed by Infoblox's Global State of Security Report 2023. Phishing and ransomware attacks were the most common methods of attack, both in Germany and around the world.

"Attackers are clearly focusing on us," says Martin Hofmann, Technical CIO at infra fürth, when assessing the situation. "Our challenge is to safeguard our IT services for our 700 employees in various locations and across a wide range of tasks. To guarantee this, we have deliberately increased our protection by working with Infoblox."

THE SOLUTION

Network management and security go hand in hand

At infra fürth, network management and security are closely connected and organizationally united, creating the ideal conditions for using Infoblox's BloxOne ThreatDefense and NIOS DDI. These solutions are closely intertwined and overcome the classic silos of network management and security. NIOS provides uniform and central administration of all DNS, DHCP and IPAM services for hybrid and multi-cloud networks. It can therefore be centrally controlled and automated. Hofmann confirms: "For us, NIOS DDI is a flexible system that is scalable and which provides granular transparency." BloxOne Threat Defense operates at the DNS level to stop attacks early on thanks to its deep visibility. In particular, the integration into a broad ecosystem also increases the effectiveness of the existing security stack. Hofmann explains: "Infoblox is an important component in our security toolbox, helping us implement early detection and prevention measures." Complete transparency helps Hofmann and his team identify which specific device is communicating and where these communications are received – even for defective connections. "With Infoblox, an affected device can now be located in seconds. This used to take hours," reports Hofmann.

Customer: infra fürth
Industry: Government
Location: Fürth, Germany

PROJECT:

- Safeguarding critical infrastructure
- Central management of all DDI services
- DNS traffic transparency

RESULTS:

- Rapid and smooth integration even without proof-of-concept
- Quick identification of infected devices
- DDI solution scalability

SOLUTIONS:

- Infoblox NIOS DDI
- BloxOne® Threat Defense

Implementing BloxOne Threat Defense and NIOS DDI did not take long at infra fürth – even without proof-of-concept beforehand. “We were fully operational across all segments at the beginning of December, barely three months after purchase,” recalls Hofmann. After a short adjustment period, when minor infrastructure-related adjustments were made, Infoblox now works perfectly.

infra fürth demonstrates that it is well worthwhile combining network management and security as a municipal utility. infra fürth's critical infrastructure protection has improved significantly by using Infoblox. “Infoblox is an effective tool that we have already utilized to defend ourselves,” says Hofmann. “The network transparency and ability to respond quickly when needed was what won us over.”

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com