NORTHSHORE UTILITY DISTRICT: WHEN FEDERAL REQUIREMENTS RAISE SECURITY STAKES

Northshore Utility District (NUD) is a local water and sewer municipality just north of Seattle, Washington. Serving 65,000 people over a 17 square mile area, spread across six cities. The utility has five major water reservoir sites, ten sewer pumping stations, and multiple connections to the regional water supply network in Seattle; as well as many links with adjacent cities and serves a major regional hospital.

> "In all 60 cases of multi-stage malware seen in the wild, the FireEye platform correctly identified and managed the attacks – a 100% success rate!"
>
> — **Stephen Schommer,** IT director, Northshore Utility District

A 1998 American Presidential directive set up a national program to identify critical infrastructure components that needed elevated protection from possible terrorist attacks. Critical infrastructures can include any element that supports emergency services, telecommunications, energy, financial, water, food, transportation sectors, and anything involved in ensuring continuity of government.

Given the year of its launch, the executive order was naturally biased towards the protection of physical components but the exponential surge in cyber-based threats has widened thinking to include items such as digital assets and Internet-connected infrastructures.

Stephen Schommer, IT director for the Northshore Utility District, observed, "Our security model was no longer comprehensive enough." The utility had conventional firewalls and endpoint virus protection, which could not be relied on to be effective against sophisticated attacks, such as advanced persistent threats (APTs), custom malware, and the phishing attempts that were increasingly targeting NUD.

The utility also needed greater protection for its internal network, which included supervisory control and data acquisition (SCADA) systems, remote sites such as water reservoirs, and mobile sites, including trucks and handheld devices, like tablets and phones.

FireEye®

"I was fascinated by the FireEye approach to analyzing new threats. The FireEye MVX technology analyzes what the threat does in an isolated environment and reports on it — sending what it finds to the cloud."

— **Stephen Schommer,** IT director, Northshore Utility District

NOT ANOTHER NEWSPAPER HEADLINE

At first, Schommer deployed conventional layers of defense, consisting of hardware-based virtual private networks (VPNs) and intrusion protection systems (IPS) from the incumbent firewall vendor. He instituted endpoint signature-based malware scanning and installed a spam-filtering appliance. He also segmented the utility's web presence with a 'demilitarized' zone (DMZ), intranet, and SCADA for remote telemetry of water and sewer sites.

Still Schommer was uneasy and knew it wasn't enough. For example his endpoint antivirus defenses only reacted to malicious communication and code after a payload had been executed. Additionally, the reporting, logging and monitoring capabilities were not nearly comprehensive enough to battle increasingly sophisticated threats.

"I didn't feel we were ahead of the curve with security," said Schommer. "We were just 'holding our own' and hoping we wouldn't be next." He already had insights into the experiences of a small nearby city that had been overrun by malware to the point that a botnet controlled all the PCs in the city administration, public works and police department. The city's IT department spent more than three months eradicating

the intrusion. In addition, another city lost $400,000 in a cyber attack, and a nearby hospital was defrauded out of more than $1 million by hackers.

"I didn't want to be another headline in the newspaper," Schommer reflected. "We needed a modern, multilayered and proactive defense."

INDUSTRY REPORTS LED TO FIREEYE

"Schommer wanted to start by hardening the communication tunnels that NUD deployed to its vehicles and tank sites. He also wanted to implement detailed reporting capabilities down to the endpoint level.

His own research and industry reports led Schommer straight to FireEye and its market-leading incident response services from Mandiant Consulting.

Schommer liked that the FireEye Network Security (NX series) platform offered behavioral analysis and real-time protection again custom malware, APTs and zero-day exploits.

To be certain he was making the right decision, he reviewed a comparison analysis produced by Delta Testing. The results were

stunningly clear: FireEye detected 99.14% of zero-day cyber threats. The closest competitor only discovered 33.62%.

A SMOOTH IMPLEMENTATION

Schommer configured his FireEye NX series for inline operation at the ingress and egress points of each subnet. "The platform was very easy to deploy," he recalled. The dual-port capability enables the utility to monitor its DMZ perimeter and intranet separately. In this configuration the unit blocks web exploits, multi-protocol callbacks and multi-stage malware in real-time, as they occur.

"I was fascinated by the FireEye approach to analyzing new threats," says Schommer. "The FireEye Multi-vector Virtual Execution engine (MVX) technology analyzes what the threat does in an isolated environment and reports on it, sharing the results to the cloud to warn other installations."

NUD also installed hardware firewalls at both ends of the network for its VPNs. FireEye Network Security was installed between the firewalls and the intranet switch, as the last line of defense. To fully leverage the utility's investments, all local and remote traffic is routed through the FireEye platforms deployed at the

FireEye

headquarters location: "We've architected the environment to make sure that there are no weak links and that everything has to go through the industrial-strength scrutiny of the FireEye solutions," commented Schommer.

A SHARED INTELLIGENCE COMMUNITY

The NX series communicates information on real-time threats and attacks back to FireEye, and uploads it into its global database to alert all customers of the latest security challenges. NUD, in turn, gets the benefits of this near-real-time sharing of threat intelligence from FireEye deployments around the world. "Because of the immediacy, an exploit doesn't have much time to gain a foothold," described Schommer.

Deployed in inline mode, the NX platform immediately identifies and proactively blocks anything malicious that has passed through the firewall and reports it to Schommer's team. "The very few false positives we initially received were minimized by minor adjustments of a few parameters," he recalled. NUD also subscribes to FireEye as a Service (FaaS) to provide

an additional layer of protection for the utility. "FaaS gives us access to broader set of capabilities without having to recruit additional headcount in an already overly competitive job market. Having this caliber of expertise and technology on call when we need it most really gives us the best of both worlds."

Schommer uses reports of blocked servers to contact his colleagues in other cities, districts and organizations to let them know they have an infected host. He also has implemented two-factor authorization and remote hardware-level encryption to minimize exposure.

NUD relies on FireEye Email Security (EX) to protect its email. "My decision to deploy EX was heavily influenced by the positive results we had with Network Security," explained Schommer.

In the 12 months since deploying Network Security, NUD successfully resolved 12 signature-based alerts and 220 IPS events without incident. Schommer finds great value in Network Security because it shows him the exact types of attack attempts and probes that are occurring. He stated, "NX tells us where we need to enhance our defenses. FireEye keeps

us informed: Everything starts with the data!" Adding that FireEye gives insight into security issues that previously weren't known, helping to harden the NUD security stance and make the utility better prepared for when a genuine alert sounds.

He concluded, "We recently blocked several serious targeted attempts sourced from both email and websites – including ransomware and credential stealing – where FireEye more than proved its worth.

"It's critical to ensure there's a process to deal with the malware that's caught: No one wants to become the company that ignored a threat. With FireEye we are much more confident that we're prepared for whatever happens."

To learn more about FireEye, visit: **www.FireEye.com**

"FireEye Network Security was very easy to use and deploy. Network Security proved itself very quickly."

— **Stephen Schommer,** IT director, Northshore Utility District

◆ FireEye®