CASE STUDY

LAUDA Optimizes Security by Increasing Visibility and Control

Threats and Challenges

It was the type of call no one wants to receive. In April 2020, BSI (the German Federal Office for Information Security or Bundesamt für Sicherheit in der Informationstechnik) called to inquire whether Martin Rothaler, Director of Information Technology at LAUDA DR. R. WOBSER GmbH & Co. KG, was aware his IT environment was under attack.

Rothaler was responsible for building and managing a holistic IT solution for LAUDA that enabled today's complex global landscape. The last thing he needed to deal with was an attack. Rothaler's resources were spent managing the complexity of multiple geographies, environments, and industrial control systems operations. Because LAUDA's offices and IT environment are distributed worldwide, the solution features a complex myriad of connections. Each one also represented an opportunity for attack or data leakage. Strong, sophisticated security is important.

Seeking a Solution

To help fully understand, stop and remediate the attack, and to mitigate damage, Rothaler turned to QGroup. He was grateful that the costs associated with this attack would be covered via their security insurance. The more concerning issue was that LAUDA wasn't alerted by its existing solutions to the intrusion in the first place. Specifically, he had assumed any unrecognized command and control traffic would be recognized or picked up.

QGroup brought in Fidelis Cybersecurity to eliminate blind spots, identify traffic anomalies, and quickly respond to advanced threats. The team had the Fidelis Network® solution up-and-running very quickly.

Benefits

- Accelerate triage, investigation and incident response across endpoints, network and cloud
- Detect sophisticated threats at any point along the kill chain
- Uncover attackers who had been silently lurking in the environment

The Company

LAUDA is the world leader in exact temperature control devices. The company plans and builds process cooling systems, heat transfer systems and secondary circuit units that guarantee the optimum temperature in research, production, and quality control. LAUDA is headquartered in Lauda, Germany, with more than 500 employees worldwide in locations such as US, UK, Spain, France, Russia, Italy, Shanghai, Singapore, and more.

LAUDA's IT environment is complex and contains sensitive data. The organization's IT environment revolves around a centralized datacenter, with consistent services delivered to its subsidiaries worldwide using Citrix. The organization's IT structure is comprised of centralized email systems, CRM, and ERP, and a global active directory so all locations with production facilities have access to the main location through VPN. With stack consolidation well underway, LAUDA's team next turned its attention to migrating two ERP systems and an IoT project to the cloud. Hybrid environments add substantially more complexity to IT environments.

Visibility and Control

Fidelis helps scale detection accuracy with contextual visibility and control across endpoints, networks and cloud traffic. Its deep data and asset visibility removes hiding places for even the most advanced adversaries. Using Fidelis, the team was able to quickly generate terrain maps and inventories of all infrastructure and assets. This helped identify traffic anomalies to quickly detect and disrupt intrusions.

Remarkably, they found they had caught the intrusion in the early stages. The attack only impacted one client and two servers. Therefore, it was easy to isolate and destroy the threat in the impacted systems.

When it was all over, the State Criminal Police Office (i.e., the Kriminalpolizei) interviewed LAUDA about their handling of the latest attack. The conversations focused on the value of enterprise-wide visibility in better managing the attack surface. Malware attacks had plagued many companies in their area. Knowing it wasn't the only organization that was attacked helped justified the organization's ongoing investment in sophisticated security solutions despite tight budgets.

Threat Detection

Through its investigations, Fidelis also discovered remains of previous (undiscovered) attacks on several machines. Luckily, those attacks had died from starvation because their command servers had vanished. The Fidelis team helped LAUDA remove all remaining traces of those attacks.

Trusted Advisor

LAUDA decided to outsource its entire security operations to QGroup. They continue to rely on Fidelis Cybersecurity to automatically discover, classify, and detect behavior anomalies. Now there are very few reported issues.

"I know it's unlikely to ever be 100% secure, but QGroup and Fidelis give me confidence that our security is at the highest possible level."

– Martin Rothaler, Director Information Technology

Each year, LAUDA increases its security investment, but Rothaler admits that investments are never enough. In December 2020, a neighbour company suffered an attack. Months later, the organization is still not fully recovered. LAUDA considers this further justification for investing in security solutions with QGroup and Fidelis.

LAUDA believes the holistic visibility and control and faster mean-time-to-detection that Fidelis provides across their environment is helping LAUDA mitigate risk and protect them from today's sophisticated attackers. While the Company is always considering alternative solutions, they doubt any other solutions will sufficiently meet their security needs.