Case Study: The Hamburg Port Authority and XM Cyber

When one of Europe’s largest seaports needed help securing its vast IT infrastructure, XM Cyber delivered its Attack-Centric Exposure Prioritization Platform

The Challenges of Finding and Fixing

The port of Hamburg, Germany is much like a small city, teeming with commercial activity. The task of managing this bustling operation falls to the Hamburg Port Authority (HPA), a local governmental agency that manages all harbor-related infrastructure for the city of Hamburg. This includes streets and bridges, railways and water infrastructure.

Given this large mandate, the IT infrastructure the HPA relies upon to manage port operations safely and securely is substantial. This infrastructure includes 350 kilometers of fiber cable, 850 routers and switches, 500 servers in two data centers (95% virtualized) and thousands of computers and smartphones running more than 600 applications. All this activity occurs over 63 separate locations with hundreds of operated IT devices.

The Challenge of Managing Port Infrastructure

When HPA IT managers reviewed the full scope of their environment, they realized that conditions on the ground had created some demanding security challenges to overcome. More than 100 local administrators were in the field and service providers were managing applications without support, or follow-up, from administrators. Additionally, not every application had an owner responsible for its security or lifecycle management.

Complicating matters further, the flat network structure being used was focused on performance and flexibility, rather than security. HPA workers, for their part, were not optimally aware of best security practices. They had concerns about exposures from across their network that were not identified by existing security controls.

In addition to these challenges, HPA IT leaders were supporting a large technology stack and working with international communities with no standards for collaboration. Standards that did exist were quickly outdated, thanks to fast-changing requirements.

Given the breadth of these challenges, HPA IT leaders decided to engage XM Cyber to identify where port IT infrastructure was vulnerable, then remediate any security gaps that were uncovered.
The Results

After running XM Cyber’s industry-leading Attack-Centric Exposure Prioritization Platform (ACEPP), HPA leaders identified several issues. Developer machines had unsecured databases; write access was discovered on shared folders containing PS-scripts; patches that had been previously reported as installed were, in fact, missing. Test machines were left unsecured. The results of the initial work with XM Cyber showed administrators a more complete view of their overall security posture. Work to make port infrastructure more secure began immediately.

HPA leaders decided to formalize their relationship with XM Cyber, using its attack-centric exposure prioritization platform to help address security issues on a day-by-day basis.

After fully implementing XM Cyber in October 2019, HPA leaders began an ongoing process of continuously resolving vulnerabilities. Upon completion of each remedial task, HPA’s IT team validated the success of the remediation again using XM Cyber. In cases HPA was not sure about the best way to solve the issues, XM Cyber’s professional services team would help analyze and find the best possible solution.

Domain credential issues proved to be one of the most significant security challenges to overcome. Credential re-use and missing admin tier levels made it easy for the attacker to pivot quietly across the environment, making it the most significant security issue within the port’s IT infrastructure. XM Cyber identified this issue multiple times due to the platform’s attack-centric risk analysis. To address this, HPA IT leaders reduced the number of domain admins and streamlined the use of different accounts for separate needs.

The Hamburg Port Authority

- The third-largest seaport in Europe
- Second busiest container port in Europe
- A key trade lane connecting Eastern Europe to the rest of the world
- Provides more than 150,000 jobs
- Processes more than 135 million tons of cargo
- Annual 9 million TEU capacity to double by 2025
XM Cyber is the global leader in Attack-Centric Exposure Prioritization, which is also known as Risk-Based Vulnerability Management (RBVM). The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options. XM Cyber helps to eliminate 99% of the risk by allowing IT and Security Operations to focus on the 1% of the exposures before they get exploited to breach the organization’s “crown jewels” – its critical assets.

XM Cyber was founded by top executives from the Israeli cyber intelligence community and has offices in North America, Europe, and Israel. For more information, go to xmcyber.com and follow us on Twitter @XMCyber_ and LinkedIn.com/company/xm.

“Because it offers continuous, automated protection, security issues that would normally take dozens of manual steps to discover are surfaced almost instantaneously.

We have historically been compelled to focus pen tests on non-critical areas of infrastructure, as the risk of collateral damage-related downtime was too great.

Thanks to XM Cyber’s automated testing, this problem was solved, and protection was extended across the entire infrastructure.”

Jens Meier
(CEO, Hamburg Port Authority)