CUSTOMER STORY

Protecting Email on the High Seas

Proofpoint Helps a Global Shipping Company Secure Its Email

The Challenge

- Protect the company against email attacks, in an industry at great risk of exposure
- Find a solution that addresses the company's international complexity and the associated risks
- Update an existing, outdated email security solution

The Solution

- Proofpoint Security Awareness Training
- Proofpoint Protection Server
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull

The Company

Many companies are global, but only on land. Eidesvik Offshore ASA also has offices at sea. Based in Bømlo, Norway, the company owns and operates a worldwide fleet of purpose-built vessels that provide multiple services to a number of types of ships at sea. They include cargo supply and transportation of pipes between onshore bases and offshore oilfields. It also operates a fleet of subsea construction vessels that deliver construction and module handling services, inspections, maintenance and repair of subsea installations. What's more, Eidesvik serves both the commissioning and service phases of offshore wind farms. And finally, it operates several vessels which are specially equipped for seismic surveys.

Given its unique and complex industry, the company was especially vulnerable to cyber attacks. The IT team began a search for a better email security solution.

The Challenge

Managing email security is complicated enough when your company has offices, factories and warehouses to protect all over the world. Now, add to that having "floating branch offices" that you have to protect.

Such was the challenge facing Eidesvik Offshore ASA, a shipping company that has been provided with a new comprehensive IT security platform developed jointly by Data Equipment and Proofpoint. In particular, Eidesvik needed to markedly improve its email security.

"The shipping industry is unbelievably complex and vulnerable," said Thorbjørn Kirkeleit, an IT consultant for Eidesvik. "We constantly exchange data through email with customers, business partners and suppliers around the world. And this international complexity means that we are completely dependent on a platform that takes this risk picture into account."

The Results

- Improved visibility of the overall threat picture, which was the most important element in their search
- Automated security procedures to avoid having to respond to certain threats in day-to-day operations
- Gained customized solutions and opportunities for adapting the rest of the security platform
- Ensured the secure handling of email for vessel fleet continuously exchanging information with many unknown and international operators

Email phishing is one of the most popular ways cyber criminals attack. With phishing, users can be tricked into providing sensitive information about the business. It's a big risk, and it can often be the entry point for a number of other forms of cyber crime.

Eidesvik had hired the contractor Data Equipment several times in the past for IT projects. But this time, the Eidesvik IT team knew they needed additional help. Their current email system was outdated. And they were dealing with the international complexities of business and email. Kirkeleit said the company decided to bring in Proofpoint to handle the email part of the project.

"Eidesvik Offshore takes email security seriously," said Thomas Brodersen, sales manager for large enterprises at Data Equipment. While most companies understand the need to protect email systems, "It's clear that Eidesvik Offshore, with its 'floating branch offices' around the world, has a greater risk of fraud and international cyber attacks. It's in a special class."

> "The shipping industry is unbelievably complex and vulnerable. That means our IT security is absolutely essential. With Proofpoint, we now have an extremely effective solution that safely contributes to our complete security platform."
>
> **Thorbjørn Kirkeleit,** IT consultant at Eidesvik Offshore

The Solution

Data Equipment led the process to enhance IT security at Eidesvik. A year later, the Eidesvik team chose to implement several Proofpoint solutions. These included Proofpoint Protection Server, Targeted Attack Protection (TAP) and Threat Response Auto-Pull (TRAP). And next on their list is Proofpoint Security Awareness Training. This final step will engage and educate employees to make sure that phishing emails don't get through.

There were some industry-standard solutions also deployed. These include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC), which is based on a recipient looking up information associated with a domain name in DNS. When a domain is protected with Domain Name System Security Extensions (DNSSEC), it's possible to verify that the response comes from the right source. And it verifies that it hasn't been changed along the way.

"Proofpoint helped us automate a number of security procedures, so we can avoid having to respond to these in our day-to-day operations. That has absolutely provided us with a gain in efficiency. The customized solution and the ability to adapt the rest of the security platform have also been notable. Overall, the processes have been very positive," Kirkeleit concluded.

The Results

Visibility of threats has improved

Part of what was most important for Eidesvik Offshore has been to upgrade security and reliability in the email systems to enhance visibility of its entire IT system.

“Seen from a helicopter perspective, our visibility with respect to the threat picture is definitely the most important element in the Proofpoint solution,” said Kirkeleit. “We have now achieved that visibility with respect to what’s happening. And we are able to react to a potential threat.”

By using Proofpoint to automate some security procedures, the Eidesvik team can now avoid having to respond to certain threats in their day-to-day operations. This saves them time and money.

Secure configuration

Having a secure configuration is important. Some functions and applications can be particularly vulnerable because of extensive use both internally and externally. Infected email with malware (viruses, trojans and more) are common entry points for attacks in which content is customized in order to fool users. But now Eidesvik can better prevent attackers from being able to exploit the assets and resources of the company.

Adaptability

Email security is not a one-size-fits-all solution. The ability to customize their Proofpoint solutions and adapt the rest of the security platform going forward is a big help to Eidesvik.

“With Proofpoint, we have obtained an extremely effective solution. And it safely works in harmony with our existing Data Equipment security solution. This gives us a complete security platform,” said Kirkeleit.

Smooth sailing

With the support of Proofpoint and Data Equipment, the Eidesvik team knows that their email is secure. The vessels in their fleet continuously exchange information with many unknown and international operators. And now it is better protected from any associated risks.

“The collaboration between Proofpoint and Data Equipment has been invaluable. It’s given us the security we need for smooth sailing on the stormy seas of global shipping in these treacherous times,” said Stine-Elisabeth Engseth, IT manager at Eidesvik Offshore.

“We have now ensured the handling of email in a secure manner,” said Engseth. “It is absolutely crucial for the operation of our company that we can now be confident that this is being handled as risk-free as possible.”

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations’ greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.