Security Cyber Security Features Shipping Maritime & Shipping

Shipping gaining a reputation for cyber vulnerability

Sea News File Photo

By Lars Fischer, Managing Director, Softship Data Processing Ltd, Singapore

Lars Fischer

In the past five years, all four of the largest container lines have experienced significant cyber-attacks – each slightly different, but all ransomware attacks causing serious disruption to operations and damage to reputations. What is most concerning is that these companies were – relatively speaking – well-equipped to handle such challenges but fell prey due to easily avoided mistakes. This speaks volumes of the risks to smaller shipping companies.

The exact number of smaller shipping companies experiencing cyber-attacks is largely unknown, but there are reports of attacks increasing between 400% and 900% over the same five-year period. What this suggests is that cyber criminals have pinpointed the shipping industry as an easy target, with large-scale attacks very publicly exposing the weaknesses and vulnerabilities of all global shipping companies, many of which are also ill-equipped to recover, to cyber criminals lying in wait the world over.

Why are hackers going after shipping companies?

Shipping companies are low-hanging fruit for cyber criminals for several reasons. Not only do most shipping companies operate worldwide, but they also depend upon the exchange of huge amounts of data and information from countless parties. This makes it harder for shipping companies to exercise control and discipline over people and IT systems.

This is particularly the case for container lines, which transact with a large pool of agents, authorities, service providers and freight forwarders (to name a few), many of which must share documents, links, and financial data. These are tools that cyber criminals use as vectors to access the shipping company's network. These fake emails, links, websites and documents are also increasingly difficult to spot, as attackers have become more adept at imitating legitimate organisations.

Making the situation even more difficult to control now is the fact that many shipping companies have had to switch to remote working and are having to rapidly adapt systems and processes during the COVID-19 pandemic, with its ever-fluctuating demands on business processes. For IT departments, home networks provide new and difficult to manage weak points in defending against cyber risk.

How are cyber criminals targeting shipping companies?

The most pervasive threat to shipping companies is that of a malware attack. A malware attack is when cybercriminals create malicious software that's installed on someone else's device without their knowledge to gain access to personal information or to damage the device, usually for financial gain. Different types of malware include viruses, spyware, ransomware, and Trojan horses. Malware attacks can occur on all sorts of devices and operating systems, including Microsoft Windows, macOS, Android, and iOS. They are particularly vicious because they are very difficult for individuals to detect until it is too late.

It's usually a staff member that inadvertently allows a hacker entry to a corporate IT system and many infiltrations can be avoided simply through raised awareness and training. To give an example, a recent high profile and far-reaching attack on a global logistics provider began in a relatively remote location when an administrator downloaded and opened what they thought was a legitimate file from their central government tax authority. The link was fake and the file contained malware which quickly infected the entire global operation.

What can be done to reduce exposure to attack?

Carefully selecting software/storage options: work with your IT departments and software service providers to develop robust cyber-security mechanisms. They must ensure that automated back-up and archiving of all documents occurs on a continuous basis, and that they utilise web-based storage systems and modular software solutions as best possible.

Implement awareness training: ensure that every single staff member receives comprehensive training and updates about cybersecurity and best practice on an ongoing basis. Effort should be invested in implementing global compliance rules and ensuring they are robust and followed to the letter. Similarly, your corporate compliance rules should be updated and steps taken to ensure they are followed throughout the organisation.

Follow recognised guidelines: ensure all your installed software applications have been developed to comply with OWASP guidelines and recommendations. The Open Web Application Security Project (OWASP) details a globally accepted basis for testing web application technical security controls as well as providing a list of requirements to ensure safe development. Compliance with OWASP means your software has been developed and tested to a globally accepted standard for web security – and that's vital.

Stress-test your defences: use your technical partners to perform regular penetration tests based on OWASP guidelines to verify your level of protection. And for added protection employ an external, independent company to carry out a full security audit and perform a series of penetration tests for you. As routine, you should check that adequate firewalls are in place and vulnerability test are undertaken regularly.

Utilise cloud-based software: the cloud is significantly safer than hosting your systems and data in house. A cyber-hacker is looking for a payday and that often comes through holding a high-profile company to ransom. Attempting to extort cash from a data centre has less impact.

What protection does the cloud provide?

Within the cloud, your data will be ring-fenced and protected, access will be limited and tightly controlled. This means there is a much-reduced opportunity for staff members to allow malicious entry to your systems by doing something inadvertently. Added to this, your cloud provider will be able to offer you a fail-over alternative. In the event your systems are hacked, this should allow you to get back up and running with the minimum delay. It is unlikely that any small or medium sized companies would have this back-up facility in place.

As a software solutions provider, at Softship, we have a responsibility to ensure that our customers are aware of the threats that they face and encourage them to be proactive and seek assistance. They must be mindful that these extremely sophisticated cyber-attacks can be unleashed with ransomware that can creep into the smallest crevice, infiltrate an organisation through even the most miniscule vulnerability and launch a destructive chain reaction in a matter of moments. Taking the opportunity to prepare, with a cool head and a careful plan, will pay dividends.

Sea News Feature, July 30

Author: Baibhav Mishra

Associate Editor, Sea News