Comment: Following simple rules can keep your data safe from cyber crime

ID 97070175 © Alexandersikov | Dreamstime.com

By Lars Fischer, MD Softship Data Processing in Singapore 23/07/2021

Only last month a major shipping group reported lost business due to a cyber-attack on its email systems – recent high-profile attacks on other shipping and logistics companies are well documented.

Paying ransoms and costs to restore systems is only part of the consequence – arguably, business interruption, failing customers and tarnishing reputations carry a higher price.

Sadly, the frequency and ferocity of cyber-attacks continues to grow and, although some hackers are simply "showing off", most are demanding a payout.

Inevitably, the more companies are prepared to offer cash in return for having their systems restored, the more encouragement is given to the darker side of the IT fraternity.

Shipping and logistics companies are particularly vulnerable, as they tend to operate multiple sites in multiple geographies, which makes it harder to exercise control and discipline over their people and their systems. It's usually a staff member that inadvertently allows a hacker entry to a corporate IT system, which often can be avoided simply through raised awareness and training.

Following a suspect link on *Google* or clicking an unknown email attachment will crack open a door to the IT system to allow a hacker through.

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 the central government tax authority.

The link was fake and the file contained malware, which quickly infected the global operation. Business was compromised and large sums were paid out to restore normality. But protection is relatively easy – simply train your staff to be suspicious of all unknown links, files and attachments, and have a mechanism in place to deal with them.

Human error is the most likely way a company will be hacked and effort should be invested in implementing global compliance rules and ensuring they are robust and followed to the letter.

Next, ensure all your installed software applications have been developed to comply with Open Web Application Security Project (OWASP) guidelines and recommendations. The OWAP 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.

You need to work with your software developer or IT provider to ensure you remain safe. By combining your efforts, you will be in a much better position to assess and strengthen your infrastructure and reduce your vulnerability. 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 tests are undertaken regularly. Similarly, your corporate compliance rules should be updated and steps taken to ensure they are followed throughout the organisation.

There is an increasing trend for shipping and logistics providers to move their IT requirements into the cloud, and this is good news for security. The cloud is significantly safer than hosting your systems and data inhouse.

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. Professional cloud providers employ small armies of highly skilled security experts who are likely to be significantly more proficient and up to date with the latest issues than IT people employed directly by a shipping line.

Most in-house IT teams are extremely competent, but it isn't their full-time job to keep data safe. Cloud professionals stake their reputation and their business on maintaining security and so it is vital that their skills are fully comprehensive and up to date. 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 silly.

Added to this, your cloud provider will be able to offer you a failsafe 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.

Hackers are growing in number and sophistication to maintain pace with our ever-increasing reliance on IT. They are driven by a combination of ego and cash. Fortunately, shipping and logistics are fairly low on their target list, but even so, a successful penetration will have far-reaching consequences. Applying a few rules and standards alongside the introduction of holistic staff training will go a long way to keeping your data safe and building resilience into your business.