BIZCOMMUNITY

Guarding against cyberattacks in the shipping and logistics sector with an effective recovery strategy

By Kate Mollett

27 Jun 2022

The shipping and logistics industry is increasingly a target of cybercrime and ransomware attacks, a trend that has accelerated in recent years. The reason for this is simple - these companies store and process a wealth of personal information that is immensely valuable, so a successful attack can be a highly profitable exercise. However, the damage these attacks cause financially and reputationally can be catastrophic. Companies need to implement leading-edge ransomware recovery and ransomware protection to enable them to protect and recover data quickly, minimising damages and loss.

Source: Martin Dambroldt via Pixabay

The shipping and logistics industry is increasingly a target of cybercrime and ransomware attacks, a trend that has accelerated in recent years. The reason for this is simple – these companies store and process a wealth of personal information that is immensely valuable, so a successful attack can be a highly profitable exercise. However, the damage these attacks cause financially and reputationally can be catastrophic. Companies need to implement leading-edge ransomware recovery and ransomware protection to enable them to protect and recover data quickly, minimising damages and loss.

An industry under siege

There are many examples of cyberattacks and data breaches across the shipping and logistics sector, from companies of all sizes. There were also several high-profile data breaches in 2020 and 2021, which have shone a spotlight on this industry under siege. In April 2020, Mediterranean Shipping Company was the victim of a malware attack that caused an outage to the company's website and customer portal. In June, global conglomerate Maersk reported a cyberattack that caused in excess of $300 million in losses. CMA CGM was attacked in September, with a breach that impacted its peripheral servers.

This trend accelerated into 2021. In September, CMA CGM was hit again, this time with an attack targeting customer information. In November, shipping giant Swire Pacific Offshore (SPO) fell victim to a cyberattack that caused a significant data breach that resulted in the loss of confidential proprietary commercial information and personal data.

In December, US logistics company D.W. Morgan exposed over 100GB of sensitive data on clients and shipments, including financial, transportation, shipping and personal details. Also in December, Hellman Worldwide Logistics was targeted by RansomEXX ransomware, and more than 70GB of stolen data, including customer names, user IDs, email addresses and passwords, was leaked.

Does not discriminate based on size

While the examples above are of large multinational shipping and logistics conglomerates, cyberthreats affect providers of all sizes across the supply chain. A case in point is a malware attack on a third-party supplier for Canada Post in May 2021, which resulted in a data breach impacting 950,000 parcel recipients. Another example is a ransomware attack on a small trucking company in the US, which could potentially have taken down the entire business.

The reality is that cybercrime does not discriminate based on size, and all organisations throughout the supply chain need to take the relevant steps to protect data and ensure the ability to recover from an attack. While digital transformation can improve efficiency in the logistics sector, it can also introduce vulnerabilities if data security is not prioritised.

A multi-layered approach

Data security is a vital tool to protect against ransomware, and it needs to take the form of a multi-layered defence to guard on multiple levels, build on a zero-trust framework for advanced security, that should be flexible and scalable to meet digital transformation goals.

The first step is to identify, assess and mitigate risk exposure, including implementing tools like multi-factor authentication and dual authorisation. Data then needs to be locked and hardened, using air gapping and immutable copies of data, to reduce the attack surface and better safeguard data. Clean backup copies help to minimise risk as well as the downtime associated with a data breach. Active monitoring and advanced threat and anomaly provide early warning alerts of suspicious and malicious activities.

Finally, consistent recovery processes need to be put into place across all data and workloads to restore wherever the data is needed. Solutions should also actively work to avoid ransomware file reinfections by deleting suspicious or unnecessary files from backups, isolating suspect backup copies, and enabling restoration to a safe location.

With the increasing number of attacks on the shipping and logistics sector, protecting data is essential. What is arguably more important, however, is the ability to recover quickly in the event of an attack. Extended downtime and continued exposure can end up costing millions, and the reputational damage can be severe, not to mention regulatory penalties associated with leaked personal information. Having an effective recovery strategy and the right tools in place is critical to protecting organisations in this vulnerable industry.

ABOUT THE AUTHOR

Kate Mollett, Regional Director at Commvault Africa