BIZCOMMUNITY

Ransomware is a business resilience issue, not an IT problem

By Kate Mollett

16 Sep 2022

Over the course of the last few years ransomware has increased considerably and this trajectory is set to continue. Data breaches and other security events pose significant risks to businesses because lost data represents not only lost business, but also compliance violations, damage to reputation, and typically a heavy financial burden in terms of recovery.

Source: © Daniil Peshkov– 123RF.com

Although ransomware affects IT infrastructure, the impact of an attack goes far beyond and stretches to every corner of a business. Ransomware is therefore a business resilience issue and not an IT problem, and organisations need to be data-ready to mitigate the risks and recover effectively.

The real cost of ransomware

The ultimate goal of ransomware is to extort money, and this is done by exploiting vulnerabilities in business-critical data, or data that is vital for operations, as well as sensitive data that contains Personally Identifiable Information (PII). Once the malware gains access to data, it will either delete, encrypt, or corrupt it, rendering business inoperable until they can regain access to this data.

Cybercriminals will hold the data to ransom and promise to give it back when the money is paid, but often this is not the case. Businesses that pay the ransom are often unable to fully recover the data, which leads to a host of other problems. In addition, the breach of compliance regulations and subsequent damage to reputation cannot be undone.

Threats both internal and external

This threat to data is a substantial business risk, and while often this is an external threat, data can also be vulnerable internally. Whether internal actors are acting intentionally with malicious intent, or data is accidentally leaked, exposed or

deleted, the result is the same. With ransomware, there is often a combination of both of these threat vectors. The malware originates externally, but it is propagated through the organisation inside. The impact to business can be massive, and any data breach needs to be treated as a disaster, with a proper disaster recovery strategy and plan in place.

Mitigating the risk

Dealing with the threat of ransomware, or the risk of any data loss event for that matter requires a strategic approach that leverages data governance to align the risk to the business value of data. It is essential to weigh up the cost of managing data versus the impact to business should something happen to that data, which will decide how this data should be treated. Critical and sensitive data have special requirements, and these need to form part of a data governance strategy.

Understanding the vulnerabilities and threats, developing policies and procedures to manage these, and educating people around them, are all essential steps as well. Having an incident response plan is vital, but importantly this plan must be evaluated before a problem occurs, to ensure it is robust and effectively handles the scenarios. Finally, all steps and decisions must be documented and auditable, so that in the event of a compliance breach, organisations can prove that they took all necessary steps to protect their data.

Plan for the worst

With the acceleration in the volume of ransomware attacks and other cyber threats, it is prudent to plan for the worst-case scenario. Using a best practice data management framework and designing data architecture around this can be invaluable. This includes immutable backups that cannot be infected by malware, and which can be used as restore points. In addition, organisations need to know what critical or sensitive data they have, where it is and why they are keeping it.

Permissions must also be addressed to ensure that only the right people can modify or delete data, and data should be continuously monitored for anomalies so that threats can be detected quicker before they can cause too much damage. The key is to have a plan, evaluate the plan, and then when an event occurs, go back to the plan to identify what went wrong and how this can be prevented in future. Data loss events are a matter of when, not if, and organisations need to be data-ready to ensure they can recover effectively.

ABOUT KATE MOLLETT

Kate Mollett is senior regional director at Commvault, Africa South and East.

- Modern data challenges demand advanced management platforms - 4 May 2023
- #BizTrends2023: The major trends to impact the data landscape in 2023 - 9 Jan 2023
- Ransomware is a business resilience issue, not an IT problem - 16 Sep 2022
- Big spike in ransomware attacks calls for adoption of backup-as-a-service - 14 Apr 2021
- Successfully managing risk in a digital world - 3 Jul 2019

View my profile and articles...