IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Data Centre and Virtualization

Storage Must Form the Core of an Enterprise Cybersecurity Strategy

James (JT) Lewis

James (JT) Lewis
Director of Channels
EMEA and APJ
Infinidat

Biography

James (JT) Lewis is the Director of Channels EMEA and APJ at Infinidat (https://www.infinidat.com). He is an experienced international Sales Director with a proven track record in the enterprise IT, storage, and network security industries. His broad industry experience includes roles involving cyber security, Storage Area Networks (SAN), enterprise storage, IT service management, IT strategy, professional services, cloud computing and virtual computing environments.

Based in Frankfurt, JT has responsibility for Infinidat's EMEA and Asia Pacific regions, including Japan. JT served in the US Military before embarking on his technology sales career, more recently he worked for Data Interchange as Head of Channel Sales and was the Strategy and Growth Officer for Altdata Technology Solutions, focusing on the cyber security market. He also spent 15 years at EMC and RSA, based in London and Frankfurt, where he built up comprehensive experience in the recruitment, enablement, and leadership of channel partners and distributors.

JT blogs at https://www.infinidat.com/en/blog

Keywords Cyber resilience storage, Cyberattacks, Ransomware, Cyberthreats, Business threats, Data controls
Paper type Research

Abstract

Enterprise storage has become a main target of cybercriminals for the most damaging and hard-to-detect ransomware and malware attacks, so it's no wonder that in PwC's 24th Annual Global CEO Survey, leaders ranked cyberattacks second place amongst the most serious of all possible economic, social, political, business, and environmental threats. In this article, the author discusses some key features of enterprise storage that need to be in place to ensure cyber resilience against today's cybercriminals.

Introduction

Cyber security experts have estimated that global cybercrime costs will exceed 7.5 trillion Euros this year[1]. It's no wonder then that business leaders rank cyberattacks second place amongst the most serious of all possible economic, social, political, business and environmental threats. According to PwC's 24th Annual Global CEO Survey[2], ransomware attacks represented 12% of breaches of critical infrastructure in the last year. Enterprises run on data and when it's hacked or corrupted by cybercriminals, the disruption can topple an operation overnight, with multi-million Euro consequences.

The irony is that if the fallout from a cyberattack happened that quickly, it may be less problematic from which to recover. Remedial action should be started immediately and any damage minimized. The actual problem is much more insidious because when cyber attackers target an enterprise, they usually wait for almost six months before taking action. This increases their ransom power and without the right data controls, the victim's only option may be to concede to whatever financial demands are being made. In that timeframe, their primary data, the live data your business operations depend, on could have been exposed to all kinds of criminal activity.

For this reason, enterprise storage has become a main target of cybercriminals for the most damaging and hard-to-detect ransomware and malware attacks. One reason why enterprises still get trapped is because a cybersecurity strategy tends to focus on keeping criminals out in the first place, rather than accepting that attacks will most likely happen and there is an impetus for having a watertight strategy. The wolf will definitely keep knocking and will get inside your house.

So, what steps can you take?

Cybersecurity's emphasis must widen, to address three areas – detection, resilience and recovery – and plug the vulnerability gap that cybercriminals have been exploiting.

1. **Combining resilience** – the ability to instill defensive security measures to repel attacks:

2. **Detection** – the ability to know when data is corrupted and whether a known good copy of data is free of ransomware or malware; and

3. **Recovery** – the ability to bounce back and recovery with a known good copy of the data from cyberattacks, is the key to hardening storage infrastructure.

Converging cyber resilience, detection, and recovery on an integrated enterprise storage platform is an advancement over former siloed approaches that rely on disparate tools and technologies. It makes the cyber capabilities more air-tight and ensures a rapid recovery of data within minutes to thwart cybercriminals, nullifying ransom demands and minimizing downtime or damage to the business.

Immutable snapshots

There are some key features of enterprise storage that need to be in place to ensure cyber resilience against today's cybercriminals, all of whom are highly skilled technology experts. These include ensuring the immutable nature of the data, recovered from a copy you can trust. Air-gapping to separate the management and data planes to protect the data. A secure forensic environment, to analyze the data thoroughly and ensure the fastest recovery speeds possible is critical.

Immutable snapshots allow the end user to roll back the clock and recover guaranteed, uncorrupted copies of their data, before the execution of any malware or ransomware code introduced by an attacker. Immutable snapshots ensure data integrity because they prevent data copies from being altered or deleted by anyone. Even internal systems administrators are locked out of immutable snapshots manipulation. The enterprise can be confident that any disruption or damage caused by the intrusion is minimal.

Logical air gapping adds a further layer of security, by creating a safe distance between the storage management layer and the immutable snapshots. There are three types of air gapping. Local air gapping keeps the data on premises, remote air gapping makes use of a remotely hosted system and hybrid air gapping combines the two.

Fenced forensic environments help speed up the recovery process by providing a secure area to perform a post-attack forensic analysis of the immutable snapshots. The purpose here is to carefully curate data candidates and find a known good copy. The last thing an enterprise wants after an attack is to restore data infiltrated with malware or ransomware.

Once these core elements are present within your storage infrastructure, the whole restoration can progress like clockwork. It's why our focus as an organization is dedicated to educating IT leaders about the need for a convergent, tripartite approach. One that combining cyber resilience, detection, and recovery on a single storage platform. Reliance solely on backups and preventing attacks is no longer enough to secure storage systems.

Reference

[1] Morgan, S. (13 November 2020), Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] 24th Annual CEO Survey: A leadership agenda to take on tomorrow (2021). PWC. Available at: https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf