EINPRESSWIRE

Enterprise Storage and Backup Devices Average 14 Security Risks, Continuity Report Shows

Continuity announces "The State of Storage and Backup Security Report 2023"

NEW YORK CITY, NY, USA, March 22, 2023 /EINPresswire.com/ -- Continuity, a leading provider of cyber resilience solutions, today published the 2nd edition of "The State of Storage and Backup Security Report 2023." The research showed that an average enterprise storage and backup device has 14 vulnerabilities, three of which are high or critical risk that could present a significant compromise if exploited.

> "
> This research quantifies the high level of security misconfigurations and vulnerabilities in the average enterprise storage and backup system, and the importance of fixing them."
>
> *Gil Hecht, CEO of Continuity*

The findings underscore a significant gap in the state of enterprise storage and backup security, and shows how much it lags behind the security of other layers of IT. With the growing sophistication of data-centric attacks, the high volumes of data at risk and tightened regulations, enterprise storage and backup security clearly require urgent attention.

"Securing enterprise storage and backup systems has become a critical part of organizations' cyber resiliency strategies," said Dennis Hahn, principal analyst, Data Center Storage and Data Management for analyst firm, Omdia. "As important as rapid data recovery is to business continuity if data is lost or stolen, it is arguably even more important to protect data anywhere it lives and not let storage and backup systems themselves become an entry point for attack."

Key Findings
The second annual State of Storage and Backup Security Report assessed 245 environments with 8,589 storage and backup devices from leading providers including Dell, NetApp, Veritas, Hitachi Vantara, Pure, Commvault and others. Just over 60% of organizations were from the Banking sector. Other industries included Healthcare, Financial Services, Telecommunications, Media, Shipping Carriers and IT Services. Key findings include:

- A total of 9,996 discrete security issues (e.g., vulnerabilities and security misconfigurations) were detected, spanning more than 270 security principles that were not adequately followed
- On average, an enterprise storage and backup device has 14 security risks, of which three are of high or critical risk rating, meaning each would present a significant compromise if exploited. This finding is practically identical to last year's report, indicating little has been done to address this high-risk area
- While deployment of immutable storage is rising, this can lead to a false sense of security if not implemented properly, and unfortunately, the analysis detected a significant number of misconfiguration issues specific to these features
- Unpatched vulnerabilities in storage and backup systems are the main points of attack for most ransomware. Users are not aware of the fact that traditional Vulnerability Management tools do not cover those systems well

The top five security risks found in this year's analysis were:

1. Insecure network settings (use of vulnerable protocols, encryption ciphers, etc.)

2. Unaddressed CVEs

3. Access rights issues (over-exposure)

4. Insecure user management and authentication

5. Insufficient logging & auditing

The report provides additional details about these risks and recommends best practices for remediation. Other resources include the NIST SP-800-209 Security Guidelines for Storage Infrastructure, co-authored by Continuity, and a selection of practical guides on www.continuitysoftware.com.

“We conducted this research to offer greater insight into the scope of the problems in data storage and backup security,” said Gil Hecht, CEO of Continuity. “Not only did it help to quantify the high level of vulnerabilities and security misconfigurations in the average enterprise storage and backup system, it also underscores the importance of taking a proactive and automated approach to fixing them.”

Continuity's flagship product, StorageGuard, scans, detects and fixes security misconfigurations and vulnerabilities across storage and backup devices. StorageGuard gives customers complete visibility of security risks in their storage and backup environment, while hardening these critical systems and guaranteeing compliance with security regulations and industry standards.

The “State of Storage and Backup Security Report 2023" and more information about Continuity's StorageGuard are available online.

About Continuity
With the rise in cybersecurity threats, Continuity is the only solution provider that helps enterprises protect their data by securing their storage and backup systems. Continuity's StorageGuard provides organizations with visibility of all security misconfigurations and vulnerabilities in their storage and backup systems, while automating regulatory compliance.

Among Continuity's customers are the world's largest financial services firms and Fortune 500 enterprises, including six of the top ten U.S. banks. For more information, please visit www.continuitysoftware.com.

Elizabeth Safran
Montner Tech PR
2032269290 ext.
lsafran@montner.com
Visit us on social media:
Twitter
LinkedIn
Other

This press release can be viewed online at: https://www.einpresswire.com/article/623492720