AL2025_22 How Microsoft 365 Backups Store Risks for Future Attacks (24th March 2025)

Description

As organizations migrate their operations to the cloud, ensuring robust security measures in cloud environments has become crucial. Microsoft 365 (M365) remains a widely adopted productivity suite; however, depending solely on its built-in security mechanisms, it can expose organizations to significant cyber risks. A recent study by the Acronis Threat Research Unit revealed alarming security vulnerabilities in M365 backups, highlighting the potential dangers posed by malicious URLs and embedded malware that persist in backup data.

Attack Details

The Acronis Threat Research Unit analyzed over 300,000 M365 user seats from a pool of 1.2 million to assess the effectiveness of Microsoft's built-in security protocols. The findings were concerning:

- **More than 2 million malicious or suspicious URLs**: These links could lead to phishing sites, malware downloads, or other cyber threats.
- **Over 5,000 instances of malware**: Ranging from spyware and ransomware to trojans, these threats could compromise business operations and data integrity.

The study underscores the limitations of M365's default security settings, which may fail to detect and remove malicious content before it is stored in backups. Since Microsoft follows a **shared responsibility model**, where it secures the infrastructure but leaves data protection up to organizations, companies must take proactive measures to safeguard their cloud environments.

Remediation

To mitigate the risks associated with compromised M365 backups, organizations should implement a multi-layered security approach:

1. **Deploy Advanced Backup Solutions: Use** security-enhanced backup tools that scan and remove threats before data is stored.
2. **Implement Advanced Email Security:** Leverage email filtering solutions that detect and block phishing attempts and malicious attachments.
3. **Secure Collaboration Apps:** Ensure real-time malware scanning and threat detection within M365 applications such as Teams and SharePoint.
4. **Conduct Regular Security Audits:** Periodically assess backup environments for vulnerabilities and unauthorized access attempts.
5. **Enable Multi-Factor Authentication (MFA):** Strengthen access controls with MFA to prevent unauthorized logins.
6. **Employee Awareness Training:** Educate staff on recognizing phishing emails and suspicious activities to reduce the risk of compromise.
7. **Incident Response Plan:** Develop a structured incident response plan to quickly address and mitigate breaches before they escalate.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

Acronis. (3 C.E., March 24). Hidden Threats: How Microsoft 365 Backups store risks for future attacks. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/hidden-threats-how-microsoft-365-backups-store-risks-for-future-attacks/

Microsoft 365 Backup Risks: Uncovering Hidden vulnerabilities. (2025, March 24). Retrieved from Windows Forum. https://windowsforum.com/threads/microsoft-365-backup-risks-uncovering-hidden-vulnerabilities.357775/