Politicians are Noticing Health Care Data Breaches

URL:https://www.americanthinker.com/articles/2025/09/microsoft_s_next_security_breach.html

Published: September 27, 2025

Situation: Politicians are increasingly aware of healthcare data breaches, as highlighted in an article by Julio Rivera.

Senator Ron Wyden has accused Microsoft of "gross cybersecurity negligence" for compromising nearly six million patient records in the recent Ascension Health incident. A contractor clicked a malicious Bing link, exploiting Microsoft's outdated RC4 encryption, which was left enabled by default.

This vulnerability enabled hackers to escalate privileges and compromise Microsoft Active Directory, resulting in widespread network disruption. The article criticizes Microsoft's decisions to prioritize backward compatibility over security, fostering national risks in an IT ecosystem dominated by a monoculture. It lists several breaches:

1) 2023 Storm-0558 breach linked to Chinese actors in Exchange Online

2) 2024 SharePoint flaw allowing persistent intrusions

3) CrowdStrike's 2024 update bricked millions of devices

These failures highlight how Microsoft's focus on convenience has exposed its customers in critical sectors to increasingly severe cyber threats.

Task: Healthcare providers, patients, and regulatory authorities must become aware of vulnerabilities exposed by major shared cloud service providers to proprietary patient records. With breaches becoming more frequent and costly, there's an urgent need to

address the risks of outsourcing sensitive information to environments with opaque operations, shared tenancy, and unverified controls.

Action: Healthcare providers, financial institutions, and government agencies should evaluate their outsourced IT infrastructure. The dangers of entrusting proprietary data to unknown engineers in undisclosed locations, governed by varying standards and laws, are mounting. Based on the business risks and bad publicity, it makes sense to repatriate data to private, secure on-premises data centers.

Result: More companies are shifting their critical infrastructure back in-house to enable direct employee oversight, thereby reducing exposure to vendor lock-ins and opaque adherence to best practices and regulatory compliance rules.

Zerowait's Approach

Zerowait's on-premises infrastructure engineering and SimplStor hardware solutions offer the ideal answer for enterprises seeking proprietary on-premises AI deployments. SimplStor systems provide customized storage and computing with high reliability, data sovereignty, low latency, and enhanced security.

1) Zerowait's on-premises solutions eliminate cloud data transfer risks, keeping proprietary information local and under complete control.
2) Simplstor.com hardware offers high-security encryption and air-gapping, preventing remote hacks common in Azure, AWS, and Google Cloud.
3) Avoid regulatory fines from international data flows by using Zerowait to ensure compliance with local laws.
4) Reduce downtime from cloud breaches with SimplStor's redundant, offline backups for quick recovery.
5) Cut costs on cloud subscriptions while enhancing security against phishing and misconfigurations via Zerowait's customizable systems.

Want to know more? Contact Zerowait today!

Email: engineering@zerowait.com
info@zerowait.com
TEL: (302) 996-9408
Web: www.zerowait.com
www.simplstor.com