HealthManagement
Promoting Management and Leadership

Building Cyber Resilience in Healthcare: Lessons from CrowdStrike

Healthcare institutions are increasingly dependent on robust cybersecurity measures to protect sensitive patient data and maintain the integrity of critical systems. The recent CrowdStrike outage highlighted the vulnerabilities that even the most advanced security solutions can face. It serves as a stark reminder that control failures can occur at any time, not just during major events. Cyber resilience in healthcare must focus on control efficacy, bypass elimination, and vulnerability management as critical strategies to ensure continuous protection.

Understanding Cyber Resilience in Healthcare

Cyber resilience refers to an organisation's ability to withstand and recover from adverse cyber events. For healthcare providers, this means having the capacity to maintain patient care and protect sensitive data, even when security controls fail. The healthcare sector is no stranger to these challenges, often relying on downtime procedures and incident response plans to mitigate the impact of system failures. However, many organisations overlook a critical question: How resilient are we if one of our cybersecurity tools or controls fails?

This question becomes even more pressing considering that security controls can fail frequently, not just in extraordinary circumstances. For instance, a firewall might malfunction, or a zero-day vulnerability could expose systems to attackers. Therefore, healthcare organisations must develop security architectures that account for potential control failures, ensuring they are prepared for any eventuality.

Measuring Control Efficacy

A common pitfall in cybersecurity is focusing solely on the existence of controls rather than their efficacy. While industry standards provide a baseline for security controls, they often emphasise having the controls in place rather than how well they perform. For example, simply having a firewall does not guarantee protection if the firewall rules are not effectively preventing data exfiltration or unauthorised access.

Healthcare organisations should adopt evidence-based security practices to evaluate the effectiveness of their controls against specific attacker techniques. This involves regularly testing controls and adjusting them to address any identified weaknesses. Such measures are crucial, as studies have shown that specific controls, like Endpoint Detection and Response (EDR) systems, are only effective about 39% of the time. By improving the efficacy of controls, organisations can enhance their resilience to attacks.

Eliminating Bypass Techniques

Even the most robust security tools can be bypassed by skilled attackers. Common bypass techniques include booting into safe mode to disable EDR or using DNS tunnelling to mask command and control traffic. Therefore, healthcare organisations must identify potential bypass methods and implement measures to counteract them.

For instance, practical steps include disabling the ability to use commands that could boot systems into safe mode or applying egress filtering to block unauthorised outbound communications. By proactively addressing these vulnerabilities, healthcare organisations can ensure that attackers must contend with the full strength of their security controls rather than finding easy ways around them.

Enhancing Vulnerability Management

Traditional vulnerability management often focuses on identifying and patching software vulnerabilities. While this is a critical aspect of security, healthcare organisations should also consider compensating controls—additional security measures that can mitigate the impact of a

vulnerability if it cannot be patched immediately. For example, the Log4J vulnerability could be mitigated by implementing egress filtering to block the necessary outbound communications required for its exploitation.

By expanding the scope of vulnerability management to include such compensating controls, healthcare organisations can build a more resilient security posture. This approach is particularly vital given the increasing prevalence of zero-day vulnerabilities that may not have immediate patches available.

In conclusion, building cyber resilience in healthcare is not just about having the right tools in place but also ensuring they work effectively and can withstand various attack methods. By focusing on control efficacy, eliminating bypass techniques, and enhancing vulnerability management, healthcare organisations can create a robust defence against cyber threats. As the digital landscape evolves, so must the strategies and architectures that protect patient data and maintain the integrity of healthcare systems. The stakes are high, and the need for resilient security architectures has never been greater.

Source: **Healthcare IT News**

Image Credit: **iStock**

Published on : Thu, 1 Aug 2024