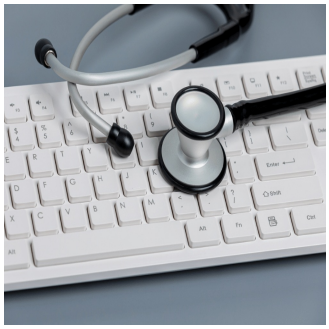
HealthManagement
Promoting Management and Leadership

Zero Trust Strategy: Cybersecurity Challenges for NHS



The recent cyberattacks on NHS Dumfries and Galloway and several London hospitals highlight the growing vulnerability of the UK healthcare system to cyber threats. The attackers claimed to have stolen three terabytes of data, underscoring the risks associated with such breaches. Ransomware and data theft present severe and persistent challenges for the NHS, emphasising the need for a cybersecurity approach that prevents attacks and effectively contains breaches. Zero Trust is emerging as a crucial strategy for safeguarding the NHS, shifting the focus from merely preventing unauthorised access to minimising an attacker's movement and impact within a compromised network.

Navigating Cybersecurity Challenges in NHS Organisations

The healthcare sector is an attractive target for cybercriminals due to its critical operations and the wealth of sensitive patient data. Ransomware attacks, particularly extortion-only variants, have become a preferred method for criminals. They aim to steal sensitive information for resale or blackmail and paralyse healthcare services to demand large ransoms. While the NHS maintains a firm stance against paying ransoms, the potential compromise of patient confidentiality and operational stability remains a severe concern.

As healthcare organisations continue to digitise and embrace new technologies, securing the infrastructure and data becomes more challenging. Traditional security measures often prove too rigid for the dynamic, cloud-led environments that NHS trusts now rely on. The situation necessitates a shift in strategy, where the focus moves from merely preventing attacks to assuming they are inevitable and strategically mitigating their potential damage.

Cloud Migration: Unveiling New Security Vulnerabilities

Cloud migration in healthcare has increased the efficiency and agility of patient care but has also introduced significant cybersecurity challenges. The NHS, like many healthcare organisations globally, has witnessed a rapid shift to cloud-based systems and digital records. However, this evolution has also expanded the attack surface, making cloud vulnerabilities a prime target for cyberattacks. Research from Illumio's Cloud Security Index reveals that 39% of healthcare institutions have experienced annual losses exceeding $1.1 million due to cloud breaches, with a global financial impact surpassing $2.5 million in total losses for the sector.

Healthcare facilities face unique challenges when addressing cybersecurity risks. Due to the critical need for system uptime, they rarely have the luxury to pause operations for maintenance or updates. Budgetary constraints further tighten the scope for cybersecurity investment. Consequently, healthcare providers are unable to tackle every potential threat comprehensively. Therefore, adopting an "assume attack" strategy becomes crucial for advancing towards a mature security posture. This strategy does not signal surrender; instead, it equips healthcare organisations to manage and contain threats effectively, focusing on minimising damage when unauthorised access occurs.

Advocating for Zero Trust in Healthcare

The Zero Trust approach, rooted in the principle of "never trust, always verify," offers a vital strategy for fortifying healthcare cybersecurity. Unlike traditional models that assume verified credentials equate to security, Zero Trust requires stringent, continuous authentication for all network access attempts. This dynamic approach ensures that the attacker's movements are restricted even if a network is breached, preventing further infiltration and data theft.

A core aspect of Zero Trust is Zero Trust Segmentation (ZTS), which applies micro-segmentation based on identity. For NHS staff, this ensures seamless access to necessary systems while maintaining robust security. ZTS aligns with NHS guidelines that advocate for segmentation based on five diagnostic pillars, making it an ideal approach for enhancing cybersecurity defences. By enforcing identity-based access checks for every network movement, ZTS blocks unauthorised entry into critical systems, much like restricting non-essential personnel from accessing operating rooms in a hospital. This ensures that sensitive data and critical assets are well-protected from potential breaches.

Implementing Zero Trust Segmentation provides healthcare institutions like the NHS with the necessary tools to isolate threats, preserve system

integrity, and protect patient privacy. The proactive breach containment approach of ZTS not only boosts cyber resilience but also ensures compliance with legal and regulatory standards, ultimately safeguarding the credibility and operational continuity of healthcare services. With consistent monitoring and updating of cybersecurity protocols, particularly in vulnerable areas like the supply chain, healthcare organisations can fortify their defences against cyberattacks. Adopting Zero Trust principles is crucial for the NHS to embrace a "never trust, always verify" mindset, essential for protecting patient information and maintaining uninterrupted care in an era of increasing cyber threats.

Source: **Health Tech Digital**
Image Credit: **iStock**

Published on : Mon, 7 Oct 2024