HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 3 • € 22

ISSN = 1377-7629

AI: Opportunities, Capabilities and Limits

THE JOURNAL 2022

Henrique Martins et al.
Hospitals-on-FHIR: Preparing Hospitals for European Health Data Space

Rafael Vidal-Perez
Artificial Intelligence and Echocardiography: Are We Ready for Automation?

Konstantinos Petsios et al.
Artificial Intelligence in Radiology: Realities, Challenges and Perspectives from a Tertiary Cardiac Centre in Greece

Sai Pavan Kumar Veeranki et al.
Learning From Each Other: An Artificial Intelligence Perspective in Healthcare

Elmar Kotter
Integrating Decision Support and AI in Radiology

†Werner Leodolter
Clinical Decision Support – Benefits and Application in Healthcare

9 771377 756005 07

Cybersecurity:

Preventing the Worst-Case Scenario

What Can the NHS Learn from Public Sector Supply Chain Attacks?

Jonathan Lee I UK Director of Public Sector Relations I Sophos I UK

As organisations become increasingly connected through technology, there is a rising threat of becoming collateral in cyberattacks. It is imperative to evaluate the security practices and stances taken within any third-party organisation involved.

Key Points

- The NHS plans to launch 42 Integrated Care Systems (ICS) across England this year.
- The goal will be to share resources, drive efficiency and improve healthcare provision.
- While this is likely to increase collaboration, it also creates a greater attack surface area for cybercriminals.
- The NHS should take heed and evaluate the security practices and stances taken within any third-party organisation they work with.

In July of this year, the NHS plans to launch 42 Integrated Care Systems (ICS) across England. The NHS states that these Integrated Care Systems will be "new partnerships between the organisations that meet health and care needs across an area, to coordinate services and to plan in a way that improves population health and reduces inequalities between different groups". Ultimately, the goal will be to share resources, drive efficiency and improve healthcare provision.

While we believe this will be an incredibly effective framework, the increased collaboration between healthcare organisations comes at a cost. This newfound interconnectedness creates a greater attack surface area for cybercriminals and makes individual organisations more susceptible to supply chain attacks.

In 2021, we saw a number of devastating ransomware attacks that impacted not just the victim organisation, but all those in its supply chain. Most memorable of these was Kaseya. Attackers exploited a vulnerability in its software in July 2021 against MSPs and their customers, meaning about 1,500 SMEs were impacted by the attack.

When you consider the role of the NHS, a similar attack on an ICS could have dire consequences.

As plans for this framework are put in motion, the NHS should take heed of attacks like Kaseya to avoid a similarly devastating supply chain attack on these critical services, and consider the following steps.

Safeguarding Your Business Against Third-Party Attacks

As organisations become increasingly connected through technology, leveraging shared applications and infrastructure to enable more seamless integration, there is a rising threat of becoming collateral in cyberattacks – even when your organisation isn't the one getting hit. Not only may you depend on software or solutions that have been knocked offline, but when you connect your IT infrastructure with another organisation it's very possible for a criminal to move laterally through your partner or supplier's network and make its way to yours.

For that reason, it is imperative that NHS IT leaders rigorously evaluate the security practices and stances taken within any third-party organisation they work with. This can generally be done by asking a list of security-related questions about their practices and control environment, either as part of the procurement process or with existing suppliers.

Once assured of your partner's security posture, it's integral that NHS bodies adopt best practice when allowing contractors or third parties onto their network. Operate under the principle of zero trust: trust nothing, verify everything. As individual users and their devices join the network, it's important that they aren't just given all the implied trust and access that usually comes with this. It might feel like a daunting task, but is one that will pay dividends in the long-run – and there are a wealth of solutions on the market to simplify and manage this process.

Operate under the principle of zero trust: trust nothing, verify everything

Protect Yourself, Protect Your Supply Chain

You pose as much of a risk to your partners and supply chain as they pose to you. Not only do you have to think about the importance of robust cybersecurity for the health of your organisation, but all of those that could likely be impacted if you fall foul of an attack. In the case of these ICSs, each organisations security posture will be integral to patient safety. Cybercriminals tend to go after privileged access accounts, which act like a master key that can unlock every door in a technology environment. In an interconnected environment, it's these accounts that pose the greatest risk and so need to be given additional layers of protection. Applying Privileged Access Management enables organisations to safeguard accounts with special access or advanced capabilities, by monitoring them and putting enhanced controls in place such as multi-factor authentication, regular password changes or password vaults.

Likewise, adding layers of security at each access point is essential to deterring or impeding an attack effectively. One common misconception organisations have is that if they have an antivirus or antimalware solution in place, then they are protected. The reality, however, is quite different. On its own, it's unlikely that a single security solution will block an attack. When combined, each layer works in concert to plug any possible flaws or gaps in your defences – so the more layers you have in place, the more likely you are to prevent an attacker from getting in.

The nature of today's threat landscape means that it's no longer a viable option to sit back and hope for security solutions to block or detect malicious behaviour on the network. In many instances, an attacker will be lurking within the IT infrastructure undetected for days or even weeks before deploying ransomware. Actively threat hunting means you have a greater chance of neutralising a cybercriminal before they can release the payload.

In It Together

This might feel out of reach for many healthcare organisations whose IT teams are already under immense pressure to keep things going. We're increasingly seeing interest from public sector organisations for third-party support, which will help them monitor their environments and respond to threats as they see them. For these newly instated ICSs, managed security services will be an invaluable resource – enabling them to focus on the day-to-day with the peace of mind that cybersecurity experts are on-hand at all times.

Working together offers great opportunities to drive efficiencies, but this must extend to a collaborative effort towards implementing a robust cybersecurity posture. There are clear, simple steps an organisation can take to secure itself – as well as those it works with – and in light of recent third-party attacks, this is essential.

Conflict of Interest

None. ■