Infoblox
CONTROL YOUR NETWORK

REPORT

Cybersecurity in healthcare:

The diagnosis

Foreword from Infoblox's Rob Bolton, Director of Western Europe

"The healthcare industry is facing major challenges that require it to modernise, reform and improve services to meet the needs of ever more complex, instantaneous patient demands.

Navigating digital transformation initiatives and delivering more personalised treatment plans requires fundamental changes both operationally and culturally.

At the core of every health service are the professionals – the doctors and nurses who work tirelessly to treat illness and improve lives. But with limited resources and mounting financial pressures, successfully delivering these new services can be a daunting task.

That's why driving digital transformation is so critical for improving healthcare services. From introducing paperless systems to allow the easy exchange of critical information, harnessing new technologies such as connecting medical devices to revolutionise healthcare delivery, to big data analytics to enable faster and more accurate diagnoses, and digitising health services will prove essential to maintain high quality services against a backdrop of both growing patient demand and complex IT environments.

However, as technology becomes more ingrained into core healthcare offerings, there is an increased threat of cyberattacks disrupting services, stealing sensitive patient data, and putting lives at risk.

As an example, the recent WannaCry ransomware attack demonstrated the extent to which the healthcare industry is at risk from the evolving cyber threat landscape, disrupting services at as many as 40 hospitals across 24 NHS Trusts in the UK.1 Security vulnerabilities discovered in connected medical devices, such as drug pumps and implantable heart devices, are also introducing new risks to both patients and hospital networks."

Overview

This report has been commissioned to gain a better understanding of whether the healthcare industry is adequately prepared to combat this evolving threat.

With extensive insights from healthcare IT and security professionals from across the US and UK, we investigated the growing cyber risk in healthcare, organisations' preparedness and the ongoing investment being made. We also provide practical recommendations about how health services can be properly prepared to mitigate this threat.

Cyber preparedness

The healthcare industry has become a prime target for cybercriminals. The sensitive information held by healthcare organisations is immensely valuable on the dark web, fuelling healthcare fraud in the US.

As cybercriminals increasingly shift to a ransom model rather than resale model for financial gain, the healthcare industry has also become a popular target for ransomware, with a recent Freedom of Information request indicating that a third of UK NHS trusts have been infected by ransomware.[2]

[1] http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack
[2] https://www.sentinelone.com/press/foi-request-reveals-30-nhs-trusts-victims-ransomware-attacks/

The severe disruption that can be caused to hospital operations and services by locking access to data, has been highlighted in high profile cases such as the Hollywood Presbyterian Medical Center, where the equivalent of $17,000 in bitcoin was paid to the hackers to regain control of the computer systems.

This growing cyber threat is weighing heavily on healthcare professionals with nearly a quarter (23 per cent) of UK healthcare IT professionals reporting that they are not confident in their organisation's ability to respond to a cyberattack. Confidence is much higher among US healthcare IT professionals, with just 12 per cent lacking confidence in their organisation’s ability to respond to a cyberattack.

Healthcare organisations are also preparing themselves for how they would respond to a ransomware attack. Of the healthcare IT professionals surveyed, 26 per cent reported that their organisation would be willing to pay a ransom in the event of a cyberattack. Of these, 85 per cent of UK healthcare IT professionals and 68 per cent of US healthcare IT professionals have a plan in place for this situation.

Conversely, one third of healthcare IT professionals do not know whether their organisations would be willing to pay a ransom in the event of a cyberattack.

At Logicalis, we have seen the last three attacks on our NHS customers happening late on a Friday afternoon. This is because attackers know there will be less staff around to respond and prevent an attack from spreading. A quick and decisive response to an attack can make the difference between a couple of hours work and the Chief Executive having to make a statement to the press.

Board level executives are being driven to ensure that their organisations have robust cybersecurity controls in place, both through government legislation such as GDPR and by educating themselves in understanding the reputational damage that a breach could cause. This is causing organisations to make significant investments in personnel and technology both in the private and public sectors.

This has had the knock-on effect of creating a massive shortage in skilled staff; it is estimated that there will be a global shortage of 1.8 million cyber security professionals by 2020. This has made it very difficult for public sector organisations to recruit and retain sufficiently skilled and trained staff. Many organisations are overcoming this problem by engaging specialist Managed Security Services companies. These providers tend to specialise in each of the various areas of cybersecurity and work as an extension of an internal IT team when there is an incident. This allows an organisation to be assured that sufficient resources are available to respond to an attack at any time of the day or night. The added bonus being that internal staff can be protected from the accusation of insider attacks, as access to sensitive data is being monitored by an external team with no access to the organisational data themselves.

At Logicalis we are seeing our NHS customers challenged with increased demands for the protection of sensitive data in line with GDPR compliance, as well as increased data usage to drive efficiencies in delivering care whilst having to reduce budgets. To help address these challenges, we work closely with our NHS customers to ensure that their existing security solutions are being fully utilised, correctly configured and are providing the maximum protection available, before suggesting they invest in new solutions. We see the technology from Infoblox providing a significant step forward in a customer’s security posture, without increasing staff workloads.

Dangerous operating systems

Hospital networks have a wide range of IT and medical devices operating on the network. From MRI scanners and internet connected medical equipment, to tablets and desktop PCs, these devices pose diverse security challenges to the IT team.

A significant security concern, as highlighted by the recent WannaCry ransomware attack, is ensuring that all the different operating systems upon which these run on are secure and updated.

When asked about which operating systems are running on their network, more than 22 per cent of healthcare IT professionals surveyed reported the presence of Windows 7, the operating system exploited in the WannaCry attack.

Similarly, 20 per cent reported that Windows XP is running on their network, which has been unsupported since April 2014.[3] This has meant that no security updates have been created and pushed out for the Windows XP operating system other than in extremely rare circumstances, such as in the aftermath of WannaCry.

With the cyber threat landscape evolving dramatically fast, it is essential that IT and security professionals patch everything as soon as possible when new threats are discovered. This poses a significant challenge and risk to those organisations still running outdated operating systems, including Windows XP, as the patches aren't produced and so the devices cannot be updated to patch security flaws, leaving them open to attack.

While Microsoft advised all organisations running Windows XP to update to a modern operating system, such as Windows 10, certain institutions fear that specialised legacy software will not run on the more modern releases. For fear of disruption to patient care, many hospitals and health centres have therefore continued using these outdated operating systems.

These dangerous, outdated operating systems also power some medical equipment, such as MRI scanners, which have a shelf life spanning decades and are more difficult to update and/or patch. Nearly one in five healthcare IT professionals reported that medical devices on the network are currently running on Windows XP.

This poses a significant risk as legacy equipment running on vulnerable operating systems can be exploited by malware on the network, which may have been introduced from a simple USB or phishing attack, to communicate back to its Command and Control (C&C) server to whom it can exfiltrate data using the network's Domain Name Server (DNS).

To the same end, seven per cent of IT professionals don't know what operating systems their medical devices are running on. As with outdated operating systems, without an understanding of what operating system the device is running on, it is impossible for the IT and/or security team to proactively patch it.

Even when the operating system these devices are running on is known, 15 per cent of healthcare IT professionals surveyed reported that they either can't or don't know if they can update these systems. In larger organisations, with more than 500 employees, this figure rises to 26 per cent.

However, those that can patch these systems are quite effective in doing so, with 57 per cent of healthcare IT professionals patching systems at least once a week.

[3] https://www.microsoft.com/en-gb/windowsforbusiness/end-of-xp-support

Cybersecurity policies

Further to the traditional IT and legacy medical equipment on the network, a wealth of new connected devices are being introduced to hospital networks around the world. Over 20 per cent of the healthcare IT professionals surveyed reported having over 5,000 devices on their network at the time of the survey, rising to 37 per cent in organisations with over 500 employees.

Each new connected device acts as an exploitable endpoint for the network, massively increasing the attack surface area. The FDA has also cited numerous cases of connected medical devices that are vulnerable to hacking and manipulation, potentially putting patients' safety at risk. In some cases, such as the Hospira's Symbiq medication infusion pump, the FDA advised caregivers to stop using the pump entirely.[4]

Security policies for IoT devices should assure the authentication layer of an IoT device, which is used to verify the identify information of that entity; its authorisation controls manage the device's access across the network fabric, and ensure IT teams have complete visibility and control over the entire IoT ecosystem and its data.

However, 15 per cent of UK healthcare IT professionals and 11 per cent of US healthcare IT professionals don't believe that their current security policy for newly connected devices is effective. This could suggest that hospitals and health centres are rapidly adopting new connected devices without due care and attention towards security policies.

Investing against the threat

[4] https://www.cnbc.com/2015/08/03/citing-hacking-risk-fda-says-hospira-pump-shouldnt-be-used.html

In response to the growing threat, 85 per cent of healthcare organisations surveyed have increased their cybersecurity spending over the past year; 12 per cent of organisations increased their cybersecurity spending by over 50 per cent.

Of the security investments made, getting the basics right appears to be the priority with traditional security solutions. Anti-virus software and firewalls were the most popular investments for cybersecurity spending in the healthcare industry (60 per cent and 57 per cent respectively).

However, the rise in malicious activity has also led many healthcare organisations to invest in other cybersecurity solutions. Half of organisation have invested in network monitoring to identify malicious activity on the network; one third have invested in DNS security solutions, which can actively disrupt Distributed Denial of Service (DDoS) attacks and data exfiltration; and 37 per cent invested in application security to secure web applications, operating systems and software.

Encryption is being deployed more regularly in the US than UK, with half of US healthcare IT professionals reporting that their company invests in encryption software, compared to 36 per cent of those in the UK.

Similarly, roughly one third of healthcare IT professionals indicated that their company is investing in employee education, email security solutions and threat intelligence (35 per cent, 33 per cent and 30 per cent respectively), with just one in five healthcare organisations investing in biometrics solutions.

Conclusions and recommendations

With the increasing number of attacks on healthcare organisations, it's essential that CIOs and IT leaders strategically plan their cybersecurity defences to protect both patient and employee data, and against disruption to services.

Across the UK and US, healthcare IT professionals are facing growing challenges in securing their networks and devices, with our research highlighting diverse issues ranging from vulnerabilities in medical devices to outdated operating systems and unenforceable security policies. However, cybersecurity investment is increasing across the board, providing the opportunity for great improvement if deployed effectively.

Based on the research and Infoblox's extensive knowledge of the cybersecurity challenges that healthcare IT professionals are facing, we recommend the following next steps:

Know your network

Understanding what devices are on your network and what operating systems those devices are running on is essential to ensure that vulnerable endpoints are patched and not leaving healthcare organisations exposed.

Organisations must also be able to identify what malicious behaviour looks like on their network to identify when cyberattacks are underway. With network monitoring, IT professionals can be notified in real time of any anomalous behaviour on the network that may be an indicator of malicious activity.

With threat intelligence-based DNS Security solutions, the vulnerable network infrastructure itself can be weaponised to recognise and block DNS traffic to and from known malicious domains using reputation lists and signature detection. It can also identify legitimate traffic, enabling the detection of exploits and data exfiltration.

Controlled chaos is better than disruption and destruction

Our research demonstrated that a significant number of healthcare organisations have both IT and medical devices on their networks that run on the outdated Windows XP, introducing unnecessary risk to their network since Microsoft stopped supporting the operating system in April 2014.

While there is a valid concern in many organisations that many critical software and applications may no longer work on new operating systems, healthcare IT professionals must introduce a plan to update operating systems to supported versions. This may cause short-term issues in terms of the running of certain software and/or devices, however, but it is better to manage that anticipated inconvenience, rather than wait until it is maliciously exploited as this will ultimately result in a far greater cost to the organisation, either through significant disruption of services or the loss of sensitive data.

Have a plan

As cybercriminals see greater reward driven from ransom over resale, ransomware attacks will continue to increase and healthcare organisations have clearly already been identified as popular targets.

Organisations need a plan of action to deal with a ransomware attack, whether they wish to pay or not. Minimising disruption will be key to ensuring that healthcare organisations can continue providing essential services to patients, and every effort should be made to make the response as quick and streamlined as possible.

Strategic cyber spending

Healthcare organisations are spending more on cybersecurity, but it is essential that this additional budget is spent strategically. Firewalls and anti-virus are not effective in defending against new IoT threats, for example. Therefore, CIOs and IT managers need to plan their cyber defences to protect against evolving threats, such as through DNS security and threat intelligence

Methodology

Infoblox commissioned the survey among 305 healthcare IT professionals in the UK and US (152 and 153 respectively in each region). The research was conducted online by polling company Censuswide, an international research organisation, in July 2017.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com

Infoblox