Infoblox

REPORT

Cybersecurity in healthcare:

What has changed two years on from WannaCry

Foreword from Victor Danevich, CTO Systems Engineering at Infoblox

In the two years since the WannaCry attack on the NHS, security investments in the healthcare industry have grown, emphasizing IT professionals deeper understanding of the importance of strong cybersecurity practices. While healthcare companies have become a more educated cybersecurity buyer, they face inherent roadblocks like the growth of internet connected medical devices and strict regulations that make their network more volatile and vulnerable to cyberattack.

Not to mention the type of data healthcare companies keep on record is extremely attractive to hackers today. While most IT professionals feel they have a strong cybersecurity posture, there is still room for growth, education, and increased attention on security best practices.

Overview

Following last year's "Cybersecurity in Healthcare: the Diagnosis" report, this study was commissioned to gain an understanding of how healthcare professionals around the world have adapted and evolved to protect themselves from cyber threats.

With extensive insights from healthcare IT professionals from across the US, UK, Germany and Benelux Union, Infoblox investigated the overall understanding of the threat landscape within healthcare, and touched on various organization's abilities to respond to these attacks.

Looking back over the past two years

Due to the massive amount of sensitive information, the healthcare industry has long been considered a prime target for cybercriminals. But with a recently heightened focus on IoT and digitalization within the industry, the past few years have seen a significant jump in healthcare-specific security vulnerabilities. According to a recent study in the Journal of the American Medical Association[1], the number of annual health data breaches have increased 70% to 344 over the past seven years, with 75% of the breached, lost, or stolen records – 132 million – being targeted by a "hacking or IT incident." On a global scale, researchers[2] recently found medical records of up to 140 million deceased patients on illicit market places on the dark web.

In May 2017, the infamous WannaCry ransomware attack devastated hundreds of thousands of computer networks, including that of the NHS, Britain's national health service. Unlike most major email-driven attacks, WannaCry was different in the fact that it was able to penetrate organizations through network vulnerabilities. In the end, the attack[3] caused more than 19,000 appointments to be cancelled, 200,000 computers to lock out, and cost the NHS over £92 million in damages.

A year after WannaCry, the General Data Protection Regulation, also known as GDPR, came into effect. The regulation aimed to replace the Data Protect Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, protect and empower all EU citizen's data privacy, and to reshape the way organizations across the region approach data privacy[4]. Under GDPR, organizations in breach could be fined up to 4% of annual global turnover or €20 million - whichever was greater.

[1] https://www.forbes.com/sites/michelatindera/2018/09/25/government-data-says-millions-of-health-records-are-breached-every-year/

[2] https://threatpost.com/deceased-patient-data-being-sold-on-dark-web/133871/

[3] https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Both WannaCry and GDPR marked a major moment in which organizations carrying data of any kind were made absolutely accountable for safeguarding consumer information. So almost two years from WannaCry - where does the healthcare industry stand when it comes to its cybersecurity?[4]

What has changed over the past two years?

Infoblox's research reveals that healthcare industry leaders have taken notice of major events such as WannaCry and have gone as far as to make cybersecurity a leading priority. The research reveals that 92 percent of IT professionals are now confident in their organization's ability to respond to a cyber-attack, compared to only 82 percent two years ago. Those within the United States are the least confident at 85 percent, while those within Benelux dominate in confidence at 98 percent.

Microsoft Windows 10, Mac OS X, and Linux lead as the top three operating systems currently being used for both internal networks and medical devices - a significant change from last year's reported operating systems which were Microsoft Windows 10, Microsoft Windows 7 and Microsoft Windows XP. The majority (87%) of IT professionals claim they can patch these systems, though the biggest proportion of respondents (24%) claim to only do this every two to three weeks. This is a change from last year's report, where the majority of respondents claimed to patch their systems every week (27%).

Concern around shadow IT

Three quarters (75%) of respondents claim they have a comprehensive overview of the total IT infrastructure, including all users, devices, applications and cloud services, at any time. That said, there is a slight doubt around the emergence of shadow IT - hardware or software that is not supported by the organization's central IT department[5] - with 17% considering it a point of concern.

According to Gartner, by 2020, around 30 percent of successful attacks on enterprises will be on their unsanctioned shadow IT resources[6]. With this in mind, many industry leaders have highlighted the importance of constantly monitoring network activity to avoid risk. According to the report, more than half (56%) of organizations have automated systems in place that actively scan their networks for suspicious activity, and around a third (31%) have their own Security Operation Centers (SOCs) for the same purpose. SOCs are particularly popular within Germany, with 44% of all healthcare organizations having one for the purpose of scanning suspicious activity.

In case of emergency

Though confidence is at a two-year high, organisations are still lagging in responsive planning. At the moment, almost a quarter (23%) of global IT leaders have no plan in place in the event of a cyber-attack.

Many IT leaders are also still unsure whether or not to pay ransom to attackers. According to the report, twenty-four percent would be completely unwilling to pay ransom in the event of a cyber-attack. And of those who would be willing to pay ransom, only 32% have an actual plan in place - this is a significant drop in comparison to the previous report, where 77% claimed they were willing and had a plan in place.

[4] https://eugdpr.org/

[5] https://searchcloudcomputing.techtarget.com/definition/shadow-IT-shadow-information-technology

[6] https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_-swg

Greater investment

More healthcare organizations (28%) are spending between 11 and 20 percent more on cyber-security than in 2017, with the top three investments being anti-virus software (59%), firewalls (including next generation firewalls) (52%), and application security (51%). Additionally, employee education has grown in popularity, with investment 10 percent higher in 2019 than in 2017. The reason for this has much to do with improving email hygiene in an effort to avoid phishing scams and the delivery of ransomware.

Connected devices

Healthcare IT professionals are addressing the growing adoption of the Internet of Things (IoT) and as a result the number of security policies in place for new connected devices has increased from 85 to 89 percent, with fewer respondents doubting the effectiveness of these policies (9% in 2019 compared to 13% in 2017).

The majority of connected devices now run on Microsoft Windows 10 (66%), with the popularity of Linux (33%) and Mac OS X (31%) growing significantly since 2017. Reassuringly, the number of devices running on Windows XP, which has been unsupported since 2014, has fallen from one in five to one in ten.

Country specific concerns

United States: The FDA released a medical device security playbook in October 2018, to help device manufacturers and healthcare organizations identify security vulnerabilities in medical devices. According to the report, 61 percent are confident that this is an effective security policy for the healthcare industry, 16 per cent are not confident, and almost a quarter (23%) are unfamiliar with or do not know about the policy.

Germany: Hospitals in Germany that have more than 30,000 inpatient cases per year come under the “Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" - also known as KRITIS - a regulation for determining critical infrastructures under the BSI Act, and have to report their IT security measures to the BSI until June 2019. According to the report, 66 percent of respondents believe it’s a step in the right direction, but many believe that it should include smaller hospitals (64%) and regional conditions (61%). As a result of KRITIS, the majority of organizations have taken it into account, with 57 percent claiming they’ve made internal changes as a result.

Benelux: In Benelux, the NCSC opened zorg-CERT in January 2018 to support healthcare institutions in times of cyber incidents. According to the report, it hasn’t exactly caught on as intended. Most respondents claim to have never contacted them (42%) and 20 percent have been in touch but have not used their services. Only 21% have used them and are in regular contact over security issues.

United Kingdom: WannaCry had a devastating influence on the global security landscape – especially within the UK. According to the report, only 4% of organizations have not adjusted their security procedures almost two years later. Unsurprisingly, most IT professionals have increased security software (63%) and upgraded all systems to the most recent operating systems (42%). On the positive side, many within the healthcare sector have even gone so far as to adopt two-factor authentication (41%), increased securities around information within the supply chain (40%) and increase employee education (39%).

Conclusions and recommendations

There’s no debating that the WannaCry attack was a wake-up call to healthcare providers around the world. And as we move forward and continue to digitalize, there is the possibility of such attacks continuing to grow.

It's encouraging to see healthcare organizations across the globe taking action in the form of increased cybersecurity spending, managing connected devices, and educating employee security protocols.

By taking such precautions, healthcare IT providers are right to be more confident about their ability to tackle threats to their network. They mustn't become complacent, though, and must continue to think strategically about ensuring the security of their networks and – most importantly - the safety of their patients.

Monitor for shadow IT

With such a potential for devastation, organizations must be able to identify what malicious activity looks like within their network and have a plan in case of emergency.

With threat intelligence-based DNS Security solutions, the vulnerable network infrastructure itself can be weaponized to recognize 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.

Have a plan in place

Since its inception, GDPR has resulted in over 200,000 cases reported and more than €50 million in fines. To avoid being subjected under penalties, IT leaders within healthcare organizations must keep up the momentum and continue to have top of the line security defences.

If they are unfortunate enough to be attacked, a plan of action must be put in place - whether they're willing to pay a ransom or not. Minimizing disruption will be key to ensuring that healthcare organizations can continue providing essential services to patients, and every effort should be made to make the response as quick and streamlined as possible.

Methodology

Infoblox commissioned the survey among 600 healthcare IT professionals in the UK, US, Germany, and Benelux Union (150 respectively in each region). The research was conducted in February 2019 by polling company Censuswide, an international research organization.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com