GETTING AHEAD OF FUTURE ATTACKS

A.J Thompson, CCO, Northdoor says that the UK public sector needs to look to third party IT consultants to help secure supply chains

Digital Health and Care Wales (DHCW) has predicted that, due to increasing global conflict, an increase in cyber-attacks is inevitable. The public health department said that threat actors won't be looking to just extort money, but will be looking to cause damage by bringing down systems.

The statement follows a recent ransomware attack on several major London hospitals. King's College Hospital, Guy's and St Thomas', including the Royal Brompton and Evelina London Children's Hospital and other primary care services were all affected. GP services across the Bexley, Greenwich, Lewisham, Bromley, Southwark and Lambeth boroughs were also impacted by the attack.

The cyber-attack applied to hospitals partnered with third party pathology service provider, Synnovis. The cyber incident had a significant impact on the delivery of services, including blood transfusions and test results. It also led to procedures being cancelled or redirected to other NHS hospitals.

Ransomware-as-a-service

The attack is thought be part of a ransomware-as-a-service (RaaS) campaign, where attackers bought information on the dark web around vulnerable suppliers, which if attacked, could affect critical national infrastructure in the health service. The attack service itself was provided by a Russian-based company called Qilin. The threat actors told the BBC via an encrypted messaging platform, that it targeted Synnovis as a way to punish the UK for not doing more to help in an unspecified war.

RaaS is a cyber-crime business model in which a ransomware group sells its code or malware to other hackers, who then use it to carry out their own attacks. It is a particularly dangerous, if not highly successful business model as it lowers the bar for entry into cyber-crime. Threat actors with sparse technical knowledge can carry out cyber-attacks without having to develop their own malware. Ransomware developers can also increase their profits by packaging their tools and services to sell to hackers without having to manually attack services themselves.

The cost of a breach

Healthcare services are generally targeted due to their integral function to society, the sensitive data their systems hold and their increase in IoT adoption. IBM's 2023 Cost of a Data Breach report has highlighted the increasing cost for organisations that suffer a data breach in the sector. The report found that the average cost of a data breach is now at $10.93m. This represents an increase of 53.3% since the 2020 report. In fact, healthcare has had the highest average cost of a breach for 13 years.

This is some way above the average cost of a data breach across all sectors, which sits at $4.45m and highlights how impactful breaches on healthcare organisations are. Healthcare is top of the average cost for a breach when compared to other verticals – and by some margin. The next on the list is the financial sector at $5.90m, followed by pharmaceuticals at $4.82m. There are a number of reasons for the huge difference in the cost. The sector is highly regulated, which increases the cost and is considered by most governments as a critical infrastructure.

The nature of the data held by healthcare organisations means that it is an incredibly tempting target for criminals. In the US, March 2024 set a new record for healthcare breaches according to the HIPAA Journal. 93 breaches of 500 or more records were reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). This is a 50% increase from February 2024 and a 49% increase year-on-year from March 2023. This marked the highest number of breaches reported in a single month before the COVID-19 lockdown in 2020.

> "THREAT ACTORS WITH SPARSE TECHNICAL KNOWLEDGE CAN CARRY OUT CYBER-ATTACKS WITHOUT HAVING TO DEVELOP THEIR OWN MALWARE."

It's clear that the sector is in the sights of cyber-criminals. The nature and perceived value of the data, as well as some of the vulnerabilities that the sector experiences (particularly third party supply chain attacks), means that healthcare organisations have to do more to protect themselves.

Phishing and stolen or compromised credentials

The IBM report also found that phishing and stolen or compromised credentials were the two most common initial attack vectors across all verticals. We have seen cyber-criminals use increasingly sophisticated phishing attacks to target employees, who are often considered the 'weakest link' in the security defences of a company. This is reflected in the report, with phishing attacks responsible for 16% of breaches and stolen -

or compromised credentials responsible for 15%.

These were followed by cloud misconfiguration at 11%, followed by business email compromised at 9%. The public sector, therefore, has to ensure that the weakest link in their defences is strengthened considerably. The nature of the most recent phishing attacks means that employees have little chance of being to filter out legitimate messages and malicious emails and need help in doing so. This is important in healthcare where downtime can have a huge impact on frontline services.

> **SUPPLY CHAIN ATTACKS ARE WITHOUT A DOUBT A BUSINESS-CRITICAL ISSUE, ESPECIALLY WHEN PATIENTS ARE BEING PUT AT RISK.**

2024 trends

IBM's X-Force Threat Intelligence Index 2024 has found that the use of stolen credentials to access valid accounts surged by 71% over the previous year and represented 30% of all incidents responded to in 2023, tied with phishing as the top infection vectors. The report also found three major trends that CISOs needs to be aware of. Firstly, there has been a sharp increase in abuse of valid accounts, with a focus on logging-in rather than hacking-in. This highlights the ease of obtaining valid credentials as opposed to exploiting vulnerabilities or staging phishing campaigns.

The timing and shape of the impact of GenAI on cybersecurity has also been cited in the report. With the public sector and other organisations under pressure to adopt AI, the rush to implement it is overtaking the ability to fully understand the cybersecurity risks. Once AI adoption is widespread, the public sector will need to prioritise security defences that can adapt to AI cybersecurity threats.

Third party IT consultants can help

The level of damage associated with supply chain attacks on critical infrastructure and healthcare services has never been higher. Supply chain attacks are difficult to detect, especially in large organisations that have many partners and suppliers. Public sector organisations and their partners and suppliers need to understand that just because defence systems were previously validated, doesn't necessarily mean they are secure now. With the public sector also facing restraints and cuts, rigorously assessing partners and suppliers may not be something that can be undertaken in-house.

Supply chain attacks are without a doubt a business-critical issue, especially when patients are being put at risk. With internal teams unable to cope with the workload they have, the public sector needs to turn to qualified, third party IT consultants who can supplement internal teams. Third party IT consultants can provide

a 360-degree, 24/7 overview of the supply chain, giving a comprehensive view of where vulnerabilities lie. This allows public sector organisations to have urgent conversations with partners and suppliers to shut the vulnerabilities before they are exploited by cyber-criminals.

RaaS-based and other supply chain attacks are extremely lucrative and therefore are not going to go away any time soon. Getting ahead of any future attacks using threat intelligence will be crucial for the public sector. Effective prevention, detection and response technologies implemented by third party IT consultants will enable the public sector to proactively defend against an attack. •