Trend Micro

HEALTHCARE in the Crosshairs

How ransomware and supply chains are putting patients at risk.

These are challenging times for global healthcare organisations (HCOs). COVID-19 put unprecedented pressure on a sector already struggling to manage the long-term impact of demographic change. Many responded by ramping up investment in digital technology. But while this has helped to support the transition to hybrid working, and the clearing of persistent patient backlogs, it has also dangerously expanded the cyber-attack surface.

Ransomware is arguably the biggest threat facing HCOs today. Many cybercrime groups showed their true colours during the pandemic by hitting hospitals already struggling with COVID-19. The sector remains a key target. But how exposed is it? How might supply chain weaknesses be making things worse? And where should HCOs focus their defensive efforts?

To find out more, Trend Micro recently commissioned global research, polling 145 business and IT decision makers in the sector.

Under pressure

Cyber-attacks are often discussed in abstract terms. Stolen data, breached systems and hijacked accounts all occur in the virtual or digital world. However, in healthcare, digital threats have a real-world impact. Our research finds that most (57%) responding HCOs have been compromised by ransomware over the past three years. And 86% of these organisations say these attacks affected them operationally–either by forcing them to stop completely (25%) or by disrupting some business processes (60%). It goes without saying that this poses a critical risk to patient safety.

Sometimes the victim organisation pulls the plug before ransomware spreads through the network. Sometimes it doesn't realise until it's too late, and many endpoints are infected. But whatever happens, recovery from such an incident can take a long time. On average it took most responding organisations days (56%) or weeks (24%) to fully restore operations.

Under pressure

Service outages, while important, are not the only impact of ransomware. Patient data is a highly regulated and attractive target for extortionists. That's why 60% of HCOs say that sensitive data was leaked by their attackers. This data exfiltration can increase the compliance and reputational risks associated with ransomware, and ramp-up investigation, remediation and clean-up costs.

Suppliers are risk

HCOs not only need to protect their own IT systems. Increasingly they need to tackle third-party risk that may come from an extensive ecosystem of suppliers and partners. Organisations as diverse as pharmaceuticals firms and cleaning contractors may have physical and/or virtual access to HCOs and their IT networks. But at the same time, they may not follow the same high standards of cybersecurity as those operating inside the HCO.

Respondents to our poll highlight this as a key challenge. Among the reasons given for ransomware compromise are lack of visibility across the ransomware attack chain (43%) and lack of visibility of attack surfaces (36%). A further 43% say their partners have made them a more attractive target for attack. It doesn't help that on average 52% of their supply chain partners are SMBs, which may have fewer resources to spend on security.

Room for Improvement

The good news is that plenty of HCOs are taking proactive steps to become more resilient. Most (95%) say they regularly update patches, while 91% restrict email attachments to mitigate malware risk. Many also use detection and response tools for their network (51%), endpoint (50%) and across multiple layers (43%). However, more can be done, including:

- Improved controls for remote desktop protocol (RDP) endpoints, which are a top-three access vector for ransomware. Nearly a fifth (17%) of respondents don't have any in place
- Better information sharing with supply chain partners. We found that many HCOs don't share any threat intelligence with partners (30%), suppliers (46%) or their broader ecosystem (46%)
- Improved collaboration with police, who can provide support and access to decryption tools. A third (33%) of HCOs don't share ransomware info with law enforcement
- Better detection across the cyber kill chain. Adoption rates of NDR, EDR and XDR are still too low. That's why detection rates languish for:
    - Lateral movement (32%)
    - Initial access (42%)
    - Use of tools like Mimikatz and PsExec (46%)

Despite these deficiencies, HCOs are confident about the future. Although most (77%) admit they are a target for ransomware going forward, many feel "optimistic" (25%), "motivated" (25%) and "calm" (19%) about tackling the challenge ahead. It is important that this confidence does not equate to a false sense of security. It should be of some concern that only 58% feel adequately protected, despite the large numbers that have been breached in the past and the significant investment made to address this issue.