Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

The challenge for healthcare organisations to successfully scale their security

The healthcare industry is benefiting from increased use of digital systems and devices, leading to more efficient operations and better patient outcomes. However, the increased digitalisation of healthcare records and patient details means that healthcare organisations are ripe for cybercrime. In fact, health service providers consistently top the list of notifiable data breaches according to the Office of the Australian Information Commissioner. (1) This creates an urgent need for healthcare organisations to scale their security to provide better protections even as the industry suffers from an ongoing IT security skills gap, according to Wavelink.

Ilan Rubin, managing director, Wavelink, a Fortinet and Spectralink distributor, said, “One clear area of vulnerability in a medical setting is the use of medical devices that are connected to the internet. These devices are susceptible to targeted attacks by cybercriminals and they’re equally vulnerable to broad-scale attacks such as viruses and general malware. Considering the potential life-saving characteristics of medical devices such as pacemakers and defibrillators, it’s essential to ensure they’re adequately secured.

“Furthermore, patient details are increasingly being stored digitally on databases within healthcare organisations. This information can be used to blackmail patients who don’t want their employers to know about their health status, for example. Or, it could be used by cybercriminals to facilitate identity theft. And, holding healthcare information to ransom, for instance, can yield cyberattackers a lucrative income since the implicit urgency of accessing this information could potentially be lifesaving.”

Early in 2019, a ransomware attack on a Victorian private hospital locked doctors out of patient files for more than three weeks. The hospital paid the ransom but, as is often the case with ransomware attacks, some of the encrypted files remained unavailable. Ransomware can be delivered in various ways, including through compromised medical devices.

Ilan Rubin said, “It’s important for device manufacturers to be aware of the risks and build security in from the first stages of device development. It’s also essential to ensure that healthcare organisations are running the latest versions of software and apps, and are applying patches regularly to address known vulnerabilities. These are basic steps that need to happen no matter what.

“Following that, healthcare organisations need to ensure proper authentications are required to access devices, and they should only allow the minimum level of access and configuration required to limit the attack surface.

“The healthcare industry needs to avoid becoming complacent about security. To secure security investments from C-level decision-makers, it’s essential to highlight the risks to patient safety if devices and systems remain vulnerable.”

As well as hacking, human error remains a considerable threat to cybersecurity, accounting for 35 per cent of reported data breaches in the January-March quarter of 2019. This number was the highest for health service providers. (2)

Ilan Rubin said, “Awareness is a crucial aspect of maintaining cybersecurity at scale. People need to realise that everyone within an organisation plays a crucial role in keeping that organisation secure. Healthcare employees need to be aware of the specific threats, such as phishing, that rely on human error to succeed, and they need to understand how to combat these threats at the frontline. Furthermore, employees need to be educated about the proper processes for keeping information

secure, as well as the steps to take if information is accidentally accessed or released.

“When everyone takes information security personally and steps up to the challenge, the pressure on small IT teams is reduced somewhat. Then, IT teams can focus on more innovative and proactive security initiatives, improving overall security for the organisation.”

References:

(1) https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-quarterly-statistics-report-1-january-31-march-2019/
(2) Ibid.