Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Organisations are still not getting cybersecurity fundamentals right

Most IT security professionals are well aware that the most important aspects of cybersecurity boil down to human actions. It's possible to have the most sophisticated and expensive cybersecurity tools in place and still suffer a major breach due to human error. One of the most basic of these errors is failing to install patches to close security gaps, according to Wavelink.

Ilan Rubin, managing director, Wavelink, a Fortinet distributor, said, "The fundamentals of cybersecurity include installing patches as soon as they become available, educating employees regarding their role in keeping the organisation secure, and keeping systems secure with multifactor authentication. However, it's literally shocking how many organisations fail to manage even these basic tasks, creating a significant risk that their organisation will fall victim to an attack."

Research shows that nearly 60 per cent of organisations that suffered a data breach in the two years between 2016 and 2018 fell victim to a known vulnerability with patches available. These organisations could have avoided being breached simply by installing the patches as soon as they became available. And, the evidence suggests that many of these organisations are aware of this, with 39 per cent of respondents to the survey saying their organisations were aware that the breaches were linked to known vulnerabilities. (1)

Ilan Rubin said, "These numbers are worrisome because it shows that breaches aren't happening because of sophisticated attacks, advanced tactics, or innovative techniques. Instead, they're happening because CISOs and CSOs aren't getting the fundamentals right. And, given the speed with which cybercriminals create exploits the moment a vulnerability becomes known, it's essential for organisations to be on top of patching."

In addition to patching, there are other cybersecurity fundamentals that can mitigate the risk of a cyberbreach, yet many organisations are ignoring or neglecting them. These include:

1. Adopt the Australian Signal Directorate (ASD) Essential Eight: this is a priority list of risk mitigation strategies to protect organisations against a range of adversaries. Patching is one of the Essential Eight, along with application whitelisting, restricting administrative privileges, using multifactor authentication, and backing up data daily.

2. Implement continuous security awareness campaigns: 34 per cent of notifiable data breaches were caused by human error from April to June 2019, demonstrating the crucial importance of providing ongoing security education for employees. (2) By reducing human error, organisations can dramatically reduce the incidence of successful cyberattacks.

3. Adopt a next-generation firewall (NGFW): NGFWs combine traditional firewalls with additional filtering functionalities, which can help compensate for unpatched systems.

4. Apply a rigorous and autonomous approach to web application vulnerability management: by applying machine learning to detect and block attacks, organisations can reduce their reliance on manual resources and improve accuracy.

5. Employ multifactor authentication: requiring more than just a password to access mission-critical systems makes it harder for these systems to be hacked.

6. Backup data: to ensure business continuity, organisations should back up their data based on

criticality and service level agreements.

Ilan Rubin said, “Organisations need to re-examine their approach to the fundamentals of cybersecurity and make sure they have basic security hygiene measures in place. Getting the basics right can pay huge dividends. For example, in many cases of attacks, the patches have been available for more than a year yet the organisations haven’t applied them. This creates unnecessary risk for the organisation and effectively negates any investment made in sophisticated cybersecurity solutions. It’s a bit like locking the back door while leaving the front door wide open. Employing these six cybersecurity fundamentals can help close and lock that front door.”

References:

(1) https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
(2) https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/