Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Why businesses must secure guest access and Internet of Things devices before it's too late

The need to comply with data breach legislation means Australian companies must be aware of their obligations and must ensure their own networks are fully compliant, along with the devices and applications of contractors, third parties, and guests that plug into the network. Internet of Things (IoT) devices pose a particular risk and must be explicitly secured, according to Wavelink.

Eligible Australian businesses must now report notifiable data breaches (NDB) to the Office of the Australian Information Commissioner (OAIC). The OAIC's first published quarterly report found 63 breach notifications were received in the first six weeks alone. (1) With the introduction of Europe's General Data Protection Regulation (GDPR) in May and other countries, including New Zealand, expected to introduce similar legislation, organisations need to comply with more regulations than ever. For example, GDPR affects companies in any country that does business with customers in Europe, which means many Australian companies could be subject to the legislation and some might not even know it.

Hugo Hutchinson, Wavelink's national business development manager for Fortinet, said, "Businesses can no longer remain stagnant and fail to act on security and compliance. Organisations of all sizes must ensure they're in line with the new legislation changes and perform due diligence to ensure their networks are protected. Security breaches affect a company's reputation and may result in significant consequences, with the cost and ramifications following a security breach potentially far more than the cost of initial investment in adequate protection measures.

"Organisations must also realise the value of the data they possess. Contractors, third parties, and guests plugging into the company's Wi-Fi network must be limited to accessing only the data they require. Everyone, including third parties, must comply with company security policies and practices."

The Internet of Things (IoT), which includes wearable technology, voice-activated devices, and smart appliances, present organisations with an additional level of concern. They don't tend to come with built-in security and can present a backdoor for cybercriminals to access company networks either to take over the device itself or as part of a larger attack.

Hugo Hutchinson said, "Schools and hospitals are subject to NDB requirements and they tend to be prolific users of IoT devices, as well as having hundreds of users, including guests, accessing their networks. These organisations must operate an appropriate security and compliance system otherwise they may held liable for any breaches that may occur."

Closing the gap created by IoT devices requires a solution that delivers visibility, segmentation, and protection throughout the entire infrastructure. It's essential to be able to see IoT devices on the network, then authenticate and classify them so they can be protected.

Hugo Hutchinson said, "Businesses shouldn't assume that IoT devices are inherently secure because they're not. Before connecting any IoT device to the network, businesses must change the default usernames and passwords at a minimum. From there, it's still crucial to implement a security solution that delivers visibility and control into what devices are connected and how they're being used."

Reference:

(1) https://www.oaic.gov.au/media-and-speeches/news/notifiable-data-breaches-first-quarterly-report-released