Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Why organisations need to reassess their email security architecture

Whether through phishing attacks or brute force hacking, email remains one of the key attack vectors used by cybercriminals, leaving many organisations hugely vulnerable because they don't have adequate protection in place. The latest industry data shows that 94 per cent of malware was delivered by email (1), demonstrating the crucial importance of securing this business-critical function, according to Wavelink.

Email scams cost Australian businesses more than $60 million in 2018 according to Scamwatch. (2)

Ilan Rubin, managing director, Wavelink, a Fortinet distributor, said, "These attacks are both sophisticated and hard to detect, as they rely to a large extent on human error. The more protections organisations can put in place to secure email, the less likely they will be to fall victim to email-related cyberattacks."

Moving to the cloud has delivered significant agility, flexibility, and financial benefits for organisations but it can also create risk if not properly secured. Email has been caught up in the move to cloud, which makes sense considering the high storage requirements and relative maturity of email. However, this means that, sometimes, email security is getting lost in the shuffle.

Organisations need to reassess their email security architecture. Key areas that need to be addressed include:

- **Attachment-based advanced threats:** in these threats, users are tricked into clicking onto an attachment such as a fake invoice. Once launched, the attachment delivers malware into the network. Businesses require solutions that offer network sandboxing, and content disarm and reconstruction services.
- **URL-based threats:** users are tricked into clicking onto a link that takes them to a spoof website where they're told to enter their credentials. Once they do that, the cybercriminals have their username and password, which they can then use to access further parts of the network or essential accounts such as business banking or other mission-critical applications. Businesses need URL rewriting and time-of-click analysis, and web isolation services.
- **Social engineering threats:** cybercriminals are becoming increasingly good at impersonating colleagues and managers, instructing staff members to do things like purchase iTunes gift cards, change the payment details for key invoices, or transfer large sums of money to other accounts. Because the email seems so authentic, users often fall for them. To avoid this, businesses can benefit from display name spoof detection, domain-based message authentication, reporting and conformance on inbound email, lookalike domain detection, and anomaly detection.

Ilan Rubin said, "Organisations shouldn't necessarily avoid moving their email infrastructure to the cloud. Instead, they just need to ensure that they've put the right protections in place to avoid falling victim to these scams and hacks.

"It's important to note that protecting against cyberthreats involves creating a series of rules that will need to be fine-tuned; and as a result users may notice some effects on performance. However, this is the price that organisations need to pay to avoid letting the cybercriminals win. It's a constant battle in which some false positives are far preferable to the alternative, which is a data breach or compromised system."

References:

(1) https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/
(2) https://www.scamwatch.gov.au/news/australian-businesses-hit-hard-by-email-scams