Brands must consider protecting customers from cyber attacks

South African public and private sector organisations have fallen victim to a range of sophisticated cyberattacks over the last year and have resulted in reputational damage, loss of productivity and finances.

Heino Gevers, cybersecurity specialist at Mimecast

Most organisations have to protect against a growing list of attacks including phishing, ransomware, impersonation fraud and insider threats. IT security teams are often overwhelmed and under-resourced, making it increasingly difficult to detect and defend against cyberattacks. Many end-users remain unaware of how to identify and stop incoming threats, which only adds fuel to the fire.

Looking beyond the perimeter to protect customers

But beyond protecting their own organisations from these attacks, security leaders need to take an expanded view that protects their customers too.

Heino Gevers, a cybersecurity specialist at Mimecast, warns that organisations can no longer rely on their customers being cyber aware when it comes to malicious emails exploiting their brand.

“In the past, service providers tended to pass the buck when their customers fell victim to a scam impersonating them. It was easy to blame the individual’s misfortune on their own poor cyber awareness. But as cyberattacks have become more sophisticated, the buck now stops with the brand.”

Gevers adds that organisations are no longer excused from looking beyond their own security perimeter to protect customers and partners.

“It’s surprisingly easy for attackers to impersonate a brand on the internet. Even an unsophisticated attacker can register a domain similar to a well-known brand and draw customers, partners and the public to it. Because there’s an underlying level of trust in the brand they are impersonating, there is an elevated risk of customers clicking on a link that deploys malware to their device, or sharing personal information that is used later for financial gain.”

Wait...is that the real Facebook?

19 Feb 2020

Holistic protection and resilience is essential

Gevers says nine out of ten cyberattacks globally use email as the primary attack channel.

“Business email can be used to give criminals access to confidential information, gain control over an organisation’s IT assets and disrupt business operations”.

He advises that organisations employ a cyber resilience strategy by implementing effective security controls to detect and protect against a cyberattack, advanced archiving and business continuity tools to ensure productivity during an attack, and the ability to quickly recover data and restore business systems in the wake of an effective cyber attack.

“Effective security controls must include protection from external threats at the email perimeter and internal threats within the network and organisation. They then need to look beyond the perimeter to ensure their brand isn’t being impersonated to target external email users like customers.”

While it might seem obvious, there are still some organisations that aren’t protecting themselves from emails containing malicious links or malware within attachments.

Employees must be educated about mobile cyber threats

Doros Hadjizenonos 13 Feb 2020

“First and foremost, organisations need to implement effective controls at the perimeter to detect phishing, spear-phishing and malware attacks. But it doesn’t stop there. Criminals often try to bypass perimeter security by using a compromised employee’s account or social engineering to transmit email from an internal network, which can then expose organisations to immense risk. All it takes is for one employee to click on a malicious link or open a compromised attachment to put the entire network at risk. Regular awareness training should be the norm for South African organisations to ensure their

employees have the knowledge to identify and avoid risky behaviour."

Protecting an organisation from brand impersonation is then the third and often overlooked step to ensuring pervasive protection.

“Organisations should look at tools such as DMARC to protect the domains owned by the organisation from impersonation and fraud. This should be supported by the ability to proactively hunt for domain and brand abuse, and the power to take down fraudulent sites aiming to exploit customers and partners. Unfortunately cyberattacks like this leverage and can ultimately destroy value and trust that a brand owner may have taken years or decades to build. So, it’s really in the interest of the brand to take the correct measures to prevent this from happening."

For more, visit: https://www.bizcommunity.com