Three Common Email Security Mistakes That MSPs Make

Businesses have come to rely on cloud email and file-sharing applications for communication and productivity. But too often, they assume these platforms' built-in security delivers enough protection against email-borne threats.

The reality is quite different.

While the built-in protection of platforms such as Microsoft Office 365 and Google Drive catches some threats, it is not designed to detect the myriad unknown dangers that amount to 95 percent of all cyber threats in the wild, according to Trend Micro research.

Businesses need an added layer of protection for email and file-sharing platforms. But most organizations don't realize this need until it's too late, and their systems have already been breached.

That's why MSPs and IT service providers should be proactive in educating customers about email threats — and how to defeat them. In so doing, providers position themselves to generate new recurring revenue. But they must avoid three common mistakes providers make regarding email security:

1. Failing to educate customers
Surprisingly, not all MSPs and IT service providers are aware of the need to add a layer of protection to cloud email platforms. Like their customers, many believe built-in controls get the job done.

This being the case, providers fail to educate customers on the dangers of email-born threats, leaving them susceptible to malware infections through phishing and spam, fraud, spying and information theft. Providers must make clear that an attack caused by one user's bad decision to click an infected URL or attachment can bring an organization to its knees and have long-term repercussions: The City of New Orleans is still reeling from a December 2019 ransomware attack that cost the city over $3 million.

2. Placing too much faith on end-user training
There's no question users need education on safe security practices to avoid infecting their own computers and their network. Phishing is effective because it preys on users' trust and curiosity to deliver ransomware and other forms of malware: consider that in 2018, credential phishing tactics accounted for 40 percent of all high-risk email threats. But you can't stop phishing by merely telling users not to click a link or attachment; someone is always going to do it.

Because training alone cannot fully address security risks, providers should introduce solutions to customers that stop threats *before* they reach users. They should also teach users to spot threats before clicking infected links and attachments.

3. Leaving service revenue on the table
Providers can build various services around security, including assessments that show how many threats their cloud platforms miss, as well as simulations that determine how many end users fall for phishing scams.

Assessments can lead to other, ongoing services, including awareness and training programs to help users avoid and report email threats. These services create new revenue streams and stickiness with customers.

Trend Micro's Approach

Increased customer reliance on cloud email makes these platforms a bigger target for hackers. MSPs can minimize the target with the right solutions and services to protect customers. Trend Micro's email security solution is easy to set up; it has direct APIs for various cloud applications, and it employs advanced features such as machine learning and Writing Style DNA to identify and stop phishing and other threats. Secure your email — and your company's future — today.