"Microsoft Office 365 packs strong cyber defense features — if set up correctly"

Dominic A. Paluzzi | Tuesday, June 18, 2019

With 155 million monthly active users, Microsoft Office 365 towers over other providers of cloud-connected efficiency software suites in terms of market share.

Because of its broad adoption, auditors and digital forensics say they face frequent security incidents related to the tool.

Though it offers enterprise customers robust cybersecurity measures, like multifactor authentication and free security assessments, these configurations are often missing, deactivated or not turned on by default, analysts say.

"Microsoft provides a lot of fantastic security features," said David Nives, managing director of cyber response services at KPMG, speaking at a panel during the NetDiligence Cyber Risk Summit in Philadelphia. "Like any solution, you need to tailor it to your needs and, unfortunately, not a lot of organizations take the time to do that, hence why we see as many incidents as we do."

For example, code logging is a key feature for digital forensics. It helps investigators track unauthorized data access more efficiently by narrowing the scope of an inquiry, said Devon Ackerman, associate managing director at Kroll, speaking at the summit.

Until recently, code logging on Microsoft's software package offered investigators step-by-step looks inside the system. But Microsoft recently nixed, relaunched, then nixed code logging once more.

"Logging for Office 365 is much more verbose," said Ackerman, when compared to the same capabilities in Google's G-Suite. "As massive as [Google] is, they're very infant in logging capabilities. We're better off dealing with an Office 365 breach."

That said, Microsoft is currently working on the feature.

"They realized they have a problem and they're fixing it," said Ackerman.

LIFE-SAVING SETTINGS

Multifactor authentication (MFA) is a key brick in Microsoft Office 365's firewall, especially in large and complex organizations that use it primarily for its email and productivity tools.

When it's not turned on, malicious actors have one less obstacle standing between them and valuable data or financial gain, said Dom Paluzzi, an attorney in the cybersecurity practice of Detroit-based law firm McDonald Hopkins, speaking at the summit.

Paluzzi said some clients experienced a breach because MFA wasn't activated. The clients then failed to enforce the security measure across the ecosystem and were later breached again in similar fashion.

"We've had repeat offenders," Paluzzi said.

Click here to read the full article from CIO Dive.

Dominic A. Paluzzi