Enabling Technologies:

The New Generation of Cloud Security

Chris Stegh,
CTO & VP of Strategy

Every day countless phishing emails make way to the inboxes of unsuspecting victims across the world. According to Verizon's 2017 data breach investigations report (DBIR), manufacturing companies are the most likely target to receive and click email messages that are phishing attacks. When companies transfer emails to the widely used cloud solution—Office365, Microsoft harnesses the potential of advanced security solutions for filtering out the known attacks and blocks them from showing up in the inbox. However, times have changed and attackers are wiser now. "Today, attackers send realistic looking emails with a link to webpage that has no virus and no malware," explains Chris Stegh, CTO and VP of Strategy, Enabling Technologies. "No antivirus or scanning services can determine these benign web pages are risky. But when the user clicks and is duped into logging into the attacker's page, the attacker captures the credentials and now owns the account. That's why 13 percent of manufacturing phishing messages are successful."Set against this backdrop is Florida-based Enabling Technologies. The company aims to empower clients with advanced security solutions in manufacturing—one of the highest phished industries.

After a risky email is received, Enabling Technologies' solution collects complete information about the end user—who received it, where the user logged in from, what tasks they are performing in the account, and other activities that identify behavior of an attacker.

Offered as a hosted managed service, Enabling Technologies' security solution relies on a few logging capabilities of Office 365. Customers can point their Office 365 logs to the Enabling Technologies' system via standard APIs, much in the way a SIEM works. Enabling's service is hosted in Azure and provided to the customer at a yearly service fee. Instead of customers relying on individual configurations in their tenant, Enabling's service improves each customers' outcome by learning from attacks reported in other customers' tenants. What is found with one customer immediately applies to others as well. With its breadth of experience, Enabling Technologies alleviates the administrative burden and lets clients focus on what's important. "We help customers do their share of responsibility in the cloud's shared responsibility model, which involves setting up the right protection like multi-factor authentication and single sign-on and detection of shadow IT," adds Stegh.

When it comes to sensing cyberattacks and automatically remediating them, companies either don't know they have been compromised or it takes them an awfully long time to identify it. What makes Enabling Technologies unique is its ability to sense a compromised account and then to immediately remediate the issue by shutting down the account and directing the real user to reset their password and take back control.

Drawing a complete picture of Enabling's capabilities, Stegh recalls an instance when the company assisted the IT team at Viewpoint, a global construction software developer. Viewpoint was facing frequent phishing scams targeting credential theft and business email compromise, which made Office 365 accounts vulnerable. Viewpoint today uses Enabling Technologies' PhishHunter service to take immediate action based on the logs created by Microsoft Cloud App Security (MCAS) and Advanced Threat Protection, identifying and mitigating attempted attacks. "With Enabling, we're being proactive, and are much more scalable. Now, we're dealing with email security only 5 percent of the time," said Chris Gielow, IT Director, Viewpoint.

Enabling Technologies recently introduced its latest solution, PhishHunter 2.0 —a solution that automatically detects and remediates attacks. The company's next big step is to improve the security of the customer data in Azure."We'll do that by collecting data about various application behaviors while they are running in the cloud, like how we alert and auto-remediate phishing attacks. We will perform the same sensing, detection, and remediation methods for breaches that could take over servers or data in Azure," concludes Stegh.