MSP Barracuda
Your journey, secured.

CASE STUDY

AI-based security alleviates MSP's email security headaches

TTG Services Managed.

Based in Powell, Ohio, TTG is a seasoned voice, data, and mobile managed services provider, dedicated to improving the ecosystem of its customers' communication, data, and network security infrastructure. The company's telecom experts provide infrastructure connectivity, planning, installation, and maintenance services to ensure optimal performance.

In 2019, TTG expanded its services offerings through the acquisition of technology solution provider Rampart, a company with more than 20 years' experience in IT. While TTG continues to adapt and grow, its consultative approach and commitment to earning its customers' trust through client advocacy and value-added partnering remains unchanged.

High-risk clients need more protection

Many of TTG's clients are in **regulated industries such as healthcare and financial services, which not only puts them at high risk for cyberattacks, but they also have the added burden of compliance**. One of TTG's clients, a recruiter of healthcare professionals, had another security challenge.

"Unlike some companies that deal mostly with known vendors and customers, recruiters very frequently communicate with strangers," says Don Ribar, Partner at TTG. "They receive unsolicited emails and phone calls regularly, which makes it much harder to block spam using basic filtering techniques."

Often, customers and prospects don't want to talk about security until they have an incident, he adds. "People see Home Depot or Equifax in the news, and they think, 'Why would anyone care about my relatively small company?" says Ribar. "The reality is that SMBs are often cybercriminals' most appealing targets, because they're typically under-protected."

Profile

- Website: www.ttginc.net
- Employees: 17
- Specializations: Voice, data, and mobile managed services, telecom expense management, web and mobile app development services, and hosting services

Challenge

With phishing attacks getting more sophisticated, TTG needed to add additional layers of protection to the security services they offered customers.

Solution

TTG added Barracuda Essentials and Barracuda Sentinel to its security offering mix to:

- Set rules that trigger alerts when sensitive info is sent outside an organization
- Provide email encryption, data archiving, and recovery capabilities
- Better detect malicious emails before they reach their intended target

Results

Using Barracuda Essentials and Sentinel, TTG was able to:

- Minimize the amount of phishing emails and social engineering attacks that reach a customer's inbox
- Drive efficiency by eliminating the need to look through spam emails manually

One of TTG's customers was almost victimized by a sophisticated social engineering scam. "The attacker compromised the business owner's email credentials and gathered information about the company over a long period, possibly months," says Ribar. "While the owner was out of the office, the broker received an email that purported to come from the client requesting funds to be wired to a foreign bank for a business investment. Luckily, the company's policy required a verbal confirmation due to the requested amount. After that close call, the client was much more receptive to reviewing security policies and investing in better security."

Implementing solutions to fit customers' needs

TTG's multi-layered approach includes dark web scanning, phishing training, advanced spam filtering, and leveraging AI-based products. "We use solutions like Barracuda Essentials to protect our Office 365 clients. **Essentials can set rules that alert staff before an email containing personally identifiable information (PII) is sent outside the organization.** It also enables email encryption for times when it's necessary to email sensitive information without fear of the message being intercepted. The solution also includes data archiving and recovery capabilities that meet much higher SLA standards than what's included with Office 365."

> "AI-based security tools like Barracuda Sentinel learn communication patterns within an organization and can pick up on subtle differences between authentic and fake emails."

"Hackers will hunt social media sites like LinkedIn to gather names, titles, and other personal details of employees within an organization," says Ribar. "Then, they'll spoof an email address and use personal information to fool recipients into thinking a request for sensitive information is from a trusted source. AI-based security tools like Barracuda Sentinel can learn communication patterns within an organization and are able to pick up on subtle differences between authentic and fake emails. For example, a message might be flagged by Sentinel because the perpetrator addressed the recipient by a last name and not a first name, which is not how two peers typically address each other. It also might flag requests for an unusual action, such as sending money to a new vendor."

Adaptability of solutions makes MSP's life easier

Not only are TTG's clients now better protected against a wide array of phishing attacks, but the MSP is also using many of the same tools to protect and secure itself internally. "We received an email containing an invoice that looked like it was from a vendor we work with regularly, but it was actually the work of a bad actor," says Ribar. "**Tools like Essentials and Sentinel minimize the number of phishing emails that make it to our inboxes and it makes it harder for cybercriminals to carry out social engineering attacks successfully.**"

Despite advances in AI and machine learning, there's still a vital human element needed for email security, adds Ribar. "We were able to work with the Barracuda MSP team to customize Essentials, so that we could allow the right level of messages in. What's nice about Sentinel is that it can 'learn' and adapt on its own. It saves a lot of time compared to looking through spam emails manually and relying on employees to filter out the phishing attacks on their own."

Learn more about Essentials

barracudamsp.com/product-details/email-security

Learn more about Sentinel

barracudamsp.com/product-details/spear-phishing

MSP Barracuda
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.
@BarracudaMSP | LinkedIn: BarracudaMSP | blog.barracudamsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com