Agile software testing pioneer slams the door on C-level email attacks

AI-powered Sentinel thwarts spear-phishing and fraud attacks against senior staff and lets IT team sleep at night.

TRICENTIS

A literal wake-up call

Andreas Gross reached groggily for the ringing phone by his bed, noting that it was a little past midnight. He was not surprised when he found himself talking to one of the executives at his company. The executive had received a suspicious email, and was now worried that by opening the email he may have done something wrong.

It wasn't the first such call, and Gross doubted it would be the last. Tricentis, where Gross serves as VP of IT, had been suffering a rash of sophisticated, highly targeted spear-phishing attacks, most of them aimed at C-level executives. While none of these attacks had so far been successful, Gross knew it was only a matter of time.

As a leading global provider of continuous-testing tools for enterprise Agile and DevOps teams, Tricentis boasts a list of customers that include some of the world's largest, most tech-integrated enterprise-scale organisations. The potential costs of a successful attack—which could expose critical, highly confidential customer data to criminal hackers—was incalculable. Gross knew that something had to be done to harden Tricentis' email security.

Profile

- Based in Vienna, Austria
- Offices across EMEA, APAC, and North America
- Global market leader in automated continuous testing for software and DevOps

Challenges

- C-level executives receiving frequent fraudulent spear-phishing attacks
- Following transition to Office 365, wanted to enhance native security features

Solutions

- Barracuda Sentinel
- Barracuda Essentials for Office 365
- Barracuda Message Archiver

Results

- Mitigated risk to C-suite and other staff from account-takeover and spear-phishing/whaling attacks
- Implemented protection against domain spoofing
- 200% increase in spam detection
- Boosted compliance with tamper-proof email archiving

Getting serious about Office 365 security

Tricentis is heavily invested in the cloud, and had made an early transition to Microsoft Office 365. “Microsoft has its own native security capabilities built into Office 365 of course, but these are just ‘OK’ and we needed a higher level of protection,” says Gross. “We were actively engaged in transitioning into a more mature, less risk-tolerant organisation.”

Once the onslaught of spear-phishing attacks got rolling, Gross turned to a trusted security consultant for advice, and was told to have a look at Barracuda’s offerings.

> “We looked at Mimecast and Proofpoint offerings as well, but our initial impression was that Barracuda Essentials had a more robust feature set.”
>
> **Andreas Gross**
> VP IT
> Tricentis

The personal touch

By coincidence, Gross and some of his team were heading to San Francisco on business, and Barracuda seized the opportunity to arrange a meeting at the company’s Campbell, CA headquarters. “Just the fact that Barracuda was willing to act so fast was impressive,” says Gross. “We met with senior engineers and product managers, and it was clear they were very focused on our specific needs. That level of attention meant a lot to us.”

Barracuda quickly set up a proof-of-concept trial with Essentials for Office 365 and helping Gross’ team tune the settings. But because spear-phishing was such a salient issue for Tricentis, they also suggested Barracuda Sentinel, which uses artificial intelligence to spot anomalous communications that indicate malicious intent.

The Barracuda team began by running Barracuda Email Threat Scan—a free service available to the public that uses Sentinel technology to scan Office 365 email inboxes to find all the malicious emails they contain. “That was sobering,” says Gross. “We had no idea that so many potentially damaging threats were just sitting there in our inboxes, totally undetected. We were immediately convinced that Sentinel was the anti-phishing solution we needed.”

Results and lessons learned

“We tested Barracuda Essentials and Sentinel together, and they worked extremely well. Going into full production was very fast—Sentinel in particular took us only two hours to set up, and we got great support from Barracuda’s product experts. We also deployed Barracuda Message Archiver to give us a fail-safe email audit and discovery process that is compliant with our regulatory obligations.”

The effect of deploying Barracuda was immediate, drastically reducing instances of attempted phishing, fraud, and account takeover attacks, and delivering a significant overall improvement in email security. The IT team also reported a 200% rise in the number of detected spam emails.

> “Essentials and Sentinel together are a really strong combination.”
>
> **Andreas Gross**
> VP IT
> Tricentis

“Now I can get a good night’s sleep without C-level colleagues contacting me about real or perceived attacks. Sentinel has also given us new visibility into domain settings across the organisation, which helps us ensure the integrity of our email communications.” Gross and his team were also very favourably impressed at the personal attention they received throughout the process. As he puts it, it was “a perfect deal from beginning to end.”

Learn more about Barracuda Sentinel, Barracuda Essentials and Barracuda Message Archiver

barracuda.com/products/sentinel
barracuda.com/products/essentials
barracuda.com/products/messagearchiver

Barracuda
Your journey, secured.