RocketCyber

Business Email Compromise:

An Essential Component of Your Layered Security Strategy

The Importance of Layered Security

Security experts know no single cyberdefense can stop every kind of threat.

That's why the most secure organizations rely on a layered security strategy: If one layer fails, there are multiple protections in place to stop diverse attacks. In the same way that a castle relies on stone walls, armed guards, and a moat to keep out invaders, layered cybersecurity builds defenses on top of one another. And because email scams are growing increasingly prevalent, one of these layers should focus specifically on business email compromise.

Business Email Compromise: A Rising Threat

Business email compromise (or BEC) attacks are nothing new. Hackers have always tried to insert personal information into scam emails to catch recipients off guard. What's new, however, is how sophisticated BEC attacks have become and how often they succeed — and with catastrophic consequences.

Consider today's most common BEC scheme. An email arrives with an invoice from a trusted vendor and a brief note about updating a payment address. Everything appears as normal, so the payment is sent to the new address ... where it's stolen by thieves who promptly disappear.

BEC schemes take many forms. Yet collectively, they represent a small percentage[1] of the total number of attacks: In 2019, the FBI received 467,361 internet and cybercrime complaints, with only 23,775 involving BEC. Despite being relatively rare, however, BEC schemes are extremely *costly*. The FBI blames them for **$1.7 billion in losses in 2019 — around half the $3.5 billion in total losses that year.**

By far, BEC scams are the most damaging and effective type of cybercrime. The average attack results in $75,000 in losses, compared to just $500 for phishing attacks and $4,400 for ransomware.[2] And because these attacks are carefully designed to avoid raising red flags, they're also the hardest to stop. Targets almost inevitably become victims — unless they have a layer of their security stack equipped to stop BEC.

Avoiding the Most Sophisticated Security Scams

Education and training can help users spot scam emails. But they'll always miss some — and that's especially true for well-disguised BEC scams. Technology can provide multiple layers of additional security that rise to the occasion when frontline efforts fail:

1. Multifactor authentication: Hackers will often break into email accounts to harvest details to use in BEC schemes, so encourage clients to use multifactor authentication to keep prying eyes out of their messages. Making it harder to carry out BEC attacks makes a company look less appealing as a target.

2. Conditional policies: BEC attacks originate from across the globe. Help clients set up conditional access so that, for example, only users in the U.S. can access email accounts. This puts one more obstacle between hackers and the valuable information inside the inbox.

3. 24/7 monitoring: The final and most important layer scours for early warnings that BEC schemes have (once again) tricked an unsuspecting recipient into enabling an attack. Constant security monitoring, 24/7 and 365 days a year, reveals red flags as soon as they appear so clients can prevent or minimize the consequences of BEC.

Organizations can handle steps one and two on their own, but make no mistake: Hiring a security team to work round the clock is a different story. Without monitoring, clever BEC schemes have little standing in the way of a huge payday.

Why not equip your clients with 24/7 monitoring by security veterans to ensure peace of mind?

Start a free trial of RocketCyber Managed SOC to see what it's all about, or simply schedule a live demo with our dedicated cybersecurity team.

https://www.rocketcyber.com/sign-up

https://www.rocketcyber.com/product-demo

Sources

1. https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120
2. https://www.zdnet.com/article/fbi-bec-scams-accounted-for-half-of-the-cyber-crime-losses-in-2019/

RocketCyber