proofpoint.

SERVICES BRIEF

BEC and EAC Workshop

Prevent business email compromise and email account compromise

Key Benefits

- Get the education and tools you need to prevent and deal with BEC and EAC incidents
- Leverage the knowledge and expertise of some of the world's top security experts
- Receive a sample project plan containing milestones to implement a comprehensive BEC and EAC strategy

Compromised email and business email accounts are large and growing problems. They are difficult to detect and prevent, especially with legacy tools, point products and native cloud platform defenses.

A business email compromise (BEC) attack is an email cyber crime scam in which an attacker targets a business to defraud the company. BEC takes aim at organizations of all sizes across every industry around the world. These kinds of scams have exposed organizations to billions of dollars in potential losses.

An email account compromise (EAC) attack, or email account takeover, is a related threat that is only getting more widespread in this era of cloud-based infrastructure. EAC is often associated with BEC because compromised accounts are used in a growing number of BEC-like scams. EAC is also the basis for other kinds of cyber attacks.

The Proofpoint BEC and EAC Workshop will cover Proofpoint's people-centric approach and best practices to protect your people from these threats. Your company will gain all the knowledge, education and tools it needs to prevent and deal with any BEC or EAC attack.

Who Facilitates the Workshop

The Proofpoint Professional Services Team facilitates the workshop. This team includes some of the world's leading mail experts. It has helped more than 1,500 organizations around globe evolve their mail architectures. Our clients include some of the smallest companies and some of the world's largest, including Microsoft and Google G Suite customers. We have helped these companies improve their security postures. With extensive hands-on experience leading customers through major security implementations, our consultants can offer invaluable insight to help prevent and protect your organization from BEC and EAC threats.

What to Expect from this Workshop

The workshop involves three phases. Each is described in this section.

Preworkshop data collection

You'll complete a preworkshop questionnaire. Then you'll return it to Proofpoint. The information you provide ensures that your consultant has a basic understanding of your mail environment before the workshop even begins.

Facilitated workshop

The table below shows a typical agenda.

Workshops comprise two interactive sessions. The facilitated portion is spread across one or two days. And it can be delivered remotely or at your location. The facilitated workshop is an interactive session focused on understanding and recognizing BEC and EAC attacks. It covers the potential impact to your organization and comes up with strategies for combating this type of threat. This discussion covers both infrastructure and the end-user experience.

Postworkshop documentation

As applicable, the Proofpoint consultant will review and provide input on your final BEC and EAC strategy and design. You will also receive a sample project plan containing the relevant milestones to implement a BEC and EAC strategy.

What is Required of You

Your team's commitment throughout the process is needed to ensure success. Before the workshop, identify the key stakeholders in this process. These include technical influencers and members of the leadership team. They typically include management sponsors responsible for corporate information security. They also include technical leads from messaging and security teams and identity-management or directory-services teams and service owners.

What is Outside the Scope of the Workshop

Hands-on work related to the implementation of the BEC and EAC prevention.

Agenda

Part 1: Technical overview

- What is BEC (Impostor Email) and EAC?
  - Domain Spoofing
  - Display Name Spoofing
  - Look-alike Domains
  - Compromised Accounts
  - Data Exfiltration
  - Phishing
  - Malware
  - Password Spray
- Strategies for Combating BEC and EAC
  - Email Authentication
  - Impostor Classifier/Stateful Composite Scoring Service
  - External Warnings
  - Threat Response Auto-Pull (TRAP)
  - Multifactor Authorization

Part 2: Facilitated discussion

- Strategies for Combating BEC and EAC (Continued)
  - Cloud Account Defense
  - Cloud Access Security Broker
  - Browser Isolation
  - Email Gateway Rules
  - Targeted Attack Protection
  - Internal Mail Defense
  - Multifactor Authentication
- Planning and Implementation
  - Sample Implementation Timeline
  - Anti-Spoof & Email Authentication Data Analysis
- Questions and Open Discussion

LEARN MORE

For more information, visit **proofpoint.com**.