Deep Dive Into Business Email Compromise (BEC) and Best Practices To Reduce the Risk of BECs

PONDURANCE

In the evolving landscape of cybersecurity, recent findings from the Pondurance DFIR team shed light on significant vulnerabilities and trends in Business Email Compromise (BEC) incidents. Alarmingly, 92% of all BECs involved accounts that had multifactor authentication (MFA) enabled, while 97% were compromised through sophisticated phishing kits designed to exploit man-in-the-middle software for token capture.

Moreover, none of the BEC incidents had conditional access controls properly optimized, and 78% lacked the necessary monitoring configurations, such as foreign travel alerts, geoblocking, and impossible travel detection. The process of resetting or locking user accounts demands multiple touchpoints to ensure the revocation of active sessions and tokens, especially as Microsoft rapidly updates its security protocols. These insights underscore the need for heightened awareness and robust security measures in the fight against cyber threats like BEC. Below are some of the best practices to help you defend against emerging threats.

Best Practices To Reduce Likelihood of BEC



- ☐ **Phishing awareness and training –** Implement a training and awareness program. Identify and increase focused training for phish-prone and high-value target groups. Then consider increasing the frequency of testing for those groups.

- ☐ **Email protection –** Fully leverage E5 modules for email (Microsoft Defender for Office 365, Advanced Threat Protection) to determine if common attack identifiers can be filtered prior to end-user delivery to reduce the likelihood of attack. Also use E5 for postincident forensics for precision details on actions of the attacker.

- ☐ **Web browsing protection –** Leverage DNS filtering to limit user access to malicious domains that may be hosting phishing infrastructure.

- ☐ **Endpoint protection –** Consider evaluating other EDR options to leverage behavioral analysis for specific user groups and proactively block or alert on suspected malicious sites.

- ☐ **Access controls –** Utilize principle of least privilege to limit access and permissions to only what is absolutely needed by the user to complete the job. Ensure no gaps with MFA — and don't rely on it as a silver bullet. General access policies lead to broad risk. Lock down access via VPN.

- ☐ **Incident response –** Develop a formal incident response program and procedures and consider a company tabletop exercise focused on a phishing-initiated incident.

- ☐ **Phish reporting and response**
  - Implement a risk-rating program (alongside phishing training) that rates phish-prone users as high risk
  - Limit access of high-risk users
  - Monitor the activity of those users more closely
  - Prioritize the need for users to report attempts (real or training) to a common internal security email

- ☐ **Continuous monitoring –** Conduct architecture reviews to ensure email protection, browser, and endpoint alerting options are all properly ingested. Make sure that any changes or new tech is added.

Copyright © 2025 Pondurance. All Rights Reserved.