Business Email Compromise

Business Email Compromise (BEC) หมายถึงการโจมตีผ่านอีเมลเพื่อหลอกให้สูญเสียรายได้ผ่านทางอีเมล โดยนอกเหนือจากการหลอกลวงทางอีเมลแล้วอาจมีการใช้วิธีเพิ่มเติมเพื่อเร่งรัดให้เหยื่อตกใจและรีบดำเนินการเพิ่มเติมด้วยการโทรศัพท์ ตัวอย่างสถานการณ์การโจมตีแบบ BEC มี 5 สถานการณ์ดังต่อไปนี้

สถานการณ์ที่ 1 เหยื่อของการโจมตีในลักษณะนี้มักเป็นองค์กรที่มีซื้อของกับคู่ค้าจากต่างประเทศ ซึ่งผู้โจมตีจะทำอีเมลปลอมใบแจ้งหนี้หลอกให้เหยื่อเชื่อว่ามีการเปลี่ยนแปลงเลขบัญชีจนเหยื่อหลงโอนเงินไปยังบัญชีของผู้โจมตี

สถานการณ์ที่ 2 ผู้โจมตีจะปลอมเป็น CEO หรือผู้บริหารลำดับสูงตำแหน่งอื่นๆ ขององค์กรแล้วทำการส่งอีเมลสั่งพนักงานว่าให้โอนเงินด่วนเพื่อทำกิจกรรมบางอย่าง โดยอีเมลของ CEO อาจถูกแฮกมาก่อนแล้ว หรือผู้โจมตีใช้วิธีปลอมแปลงอีเมล

สถานการณ์ที่ 3 อีเมลของบุคลากรที่เป็นผู้ติดต่อธุรกิจถูกแฮก ทำให้ผู้โจมตีสามารถส่งอีเมลหาลูกค้า ขององค์กรว่ามีการเปลี่ยนแปลงให้โอนเงินไปยังบัญชีอื่นๆ เพื่อชำระค่าสินค้า

Support : support.th@nit.co.th
Sales : rung@nit.co.th
Mobile : 081=985-6916
Web : www.netinfortech.co.th
Line : nit.sharetech

สถานการณ์ที่ 4 ผู้โจมตีติดต่อมายังองค์กรโดยหลอกว่าตัวเองเป็นทนายหรือที่ปรึกษาด้านกฎหมาย หลอกว่าสามารถช่วยเหลือองค์กรด้านกฎหมายได้ แล้วกดดันให้เหยื่อโอนเงิน เพื่อดำเนินการด่วน

สถานการณ์ที่ 5 ผู้โจมตีแฮกเข้าถึงบัญชีอีเมลของพนักงานในองค์กรแล้วหลอกสอบถามเพื่อจารกรรมข้อมูล

ShareTech Mail Server ได้เร่งพัฒนาเพื่อป้องกัน BEC จนสำเร็จในปีที่ผ่านมา โดยมีระบบป้องกันหลักดังต่อไปนี้

- การตรวจสอบอีเมลขาเข้า ตั้งค่าอีเมลให้ถูกต้อง (SPF,DKIM,DMARC) เพื่อป้องกันการได้รับอีเมลปลอม

- ระบบพิสูจน์อีเมล (Email Validation) ว่าเป็นอีเมลที่ไม่ปลอม เพื่อยืนยันว่าส่งออกไปจากองค์กรของท่าน

- มี Sandstorm ไว้คอยตรวจสอบและป้องกันอีเมล์ที่ส่งเข้ามาในองค์ว่ามีการซ่อนเร้น Script (Malware, Virus) มาเพื่อหลอกลวงเอาข้อมูล

- ระบบคัดกรองไฟล์โดยแยกตามชนิดได้เช่น PDF, XLXS, DOCS, TXT ให้รับได้เฉพาะผู้บริหารยกเว้นพนักงาน เราเรียกว่า (Mail Audit and Filtering)

- มีระบบ OTP (One Time Password) โดยจะส่ง OTP ไปที่ Mail และ LINE เพื่อพิสูจน์ตัวตนก่อนใช้งานเว็ปมล (Webmail) ขององค์กร จากภายนอก เหตุผลหลักเพื่อป้องกัน เราอาจจะ Password หลุด ด้วยเหตุผลใดๆก็ตาม เราจะยังมีระบบ OTP กั้นไว้อีกชั้น

- มีระบบตรวจสอบการรับส่งที่ผิดปกติ (Mail Log, Abnormal Traffic SMTP, Firewall)