Business Email Compromise Attack

อาชญากรรมไซเบอร์ที่องค์กรทั่วโลกพึงระวัง

*เมื่อต้นปีที่ผ่านมานอร์ทแคโรไลนา สหรัฐอเมริกา ได้รับผลกระทบจากการโจมตี **BEC Attack** ทำให้สูญเสียเงินมากกว่า 1.7 ล้านดอลลาร์สหรัฐ ซึ่งเป็นเพียงตัวอย่างหนึ่งในการโจมตีที่เพิ่มขึ้นและทวีความรุนแรงมากขึ้นด้วย*

การโจมตี Business Email Compromise Attack คืออะไร ?

BEC Attack หรือ Business Email Compromise Attack เป็นสิ่งที่อาชญากรไซเบอร์ผสมผสาน Social Engineering เข้ากับเทคนิคการ Phishing เพื่อหลอกบุคคลเป้าหมายที่อยู่ในองค์กรให้โอนเงินหรือหลอกเพื่อโจรกรรมข้อมูลต่างๆ โดยที่เหยื่อไม่รู้ตัว วิธีการที่ทำทั่วไป ได้แก่ การแฮ็คบัญชีอีเมล, การปลอมแปลงที่อยู่อีเมลของผู้บริหารระดับสูง, ลดความน่าเชื่อถือของอีเมล รวมถึงการปลอมแปลงอีเมลธนาคารและอีเมลนักกฎหมาย เป็นต้น

การโจมตี BEC Attack นั้นต้องกำหนดเป้าหมายและใช้เวลาค่อนข้างนาน ทำให้ในช่วงหลายเดือนที่ผ่านมาการโจมตีดังกล่าวจะมุ่งเน้นเป้าหมายไปที่องค์กรเดียวเท่านั้น และผู้โจมตีจะได้รับผลประโยชน์อย่างมากจากการก่ออาชญากรรม เรียกได้ว่าเป็นวิธีการที่แนบเนียนส่งผลให้การโจมตีดังกล่าวเพิ่มมากขึ้น ซึ่ง 53% ขององค์กรที่ถูกโจมตีทางไซเบอร์ในปีที่แล้วล้วนตกเป็นเหยื่อของการ Phishing ทั้งสิ้น

ในปัจจุบัน Phishing ถือเป็นปัญหาใหญ่ที่เกิดขึ้นในองค์กรและยังมีการโจมตีที่เพิ่มขึ้นทุกๆ ปี โดยจากทาง Sophos ได้มีการกล่าวว่า การโจมตีผ่านทางไฟล์ที่แนบมากับ E-mail ขององค์กรปัจจุบันมีมากถึง 66% ซึ่งส่งผลให้เกิดความเสียหายต่อองค์กรอย่างมาก และ 50% ของผู้ใช้งานคลิกลิงก์ที่ไม่รู้จักทำให้ Virus หรือ Scam เข้ามายังคอมพิวเตอร์ของคุณได้อย่างง่ายดาย ทำให้เกิดความเสี่ยงในการใช้งานไม่ว่าจะเป็นองค์กรขนาดเล็ก ขนาดกลาง หรือว่าขนาดใหญ่ก็ตาม

สนใจสมัครเป็นตัวแทนจำหน่าย หรือสอบถามเพิ่มเติมได้ที่

VSM 365 SD EBUSINESS SD EBusiness Co., Ltd.

328/3 ถนนลาดหญ้า แขวงคลองสาน เขตคลองสาน กรุงเทพฯ 10600

โทร : 02-8614600, แฟกซ์ : 02-4383100, อีเมล์ : salesorder@vsm365.com

ติดต่อฝ่ายขาย : 095-5365945, 061-5499391, 061-4951965, 064-7896519

ลดความเสี่ยงการโดนโจมตี

การโจมตีของ BEC Attack จะใช้ประโยชน์จากจุดอ่อนที่สำคัญที่สุดบนเครือข่ายความปลอดภัยทางไซเบอร์ จึงปฏิเสธไม่ได้ว่าเราทุกคนมีโอกาสตกหลุมพรางอีเมล, เอกสารและข้อมูลที่ถูกปลอมแปลง ไม่ใช่เพียงแผนกการเงิน ฝ่ายทรัพยากรบุคคลและผู้บริหารระดับสูงเท่านั้น สมาชิกทุกคนในทีมหรือบุคคลในองค์กรต่างเป็นเป้าหมายที่เป็นไปได้สำหรับการ BEC Attack แม้ว่าเหยื่อจะไม่ได้อนุมัติการชำระเงินจำนวนมากด้วยตัวเอง แต่พวกเขาอาจจะให้ข้อมูลหรือให้แฮกเกอร์เข้าถึงระบบบริษัทไปโดยไม่ได้ตั้งใจ

และนี่คือเหตุผลว่าการให้ความรู้และการอบรมแก่ผู้ใช้งาน ถือเป็นกุญแจสำคัญในการลดความเสี่ยงถูกโจมตี BEC Attack ด้วยการเพิ่มความรู้เกี่ยวกับปัญหาที่เกิดขึ้นและวิธีการสังเกตการสื่อสารที่น่าสงสัยต่างๆ จึงจะช่วยลดโอกาสในการถูกโจมตีได้นั่นเอง

Sophos สามารถป้องกันการโจมตี Business Email Compromise Attack และ Phishing อื่นๆ ได้

Sophos Phish Threat เครื่องมือที่ตอบโจทย์ในการตรวจสอบการใช้งานของผู้ใช้แต่ละส่วนในองค์กร เพื่อเจาะจงว่าผู้ใช้งานส่วนใดคือกลุ่มเสี่ยงในการโดนโจมตี ด้วยการจำลองสถานการณ์มากกว่า 500 การโจมตี Phishing ที่สมจริง เป็นการทดสอบการใช้งานของผู้ใช้ในองค์กรและรายงานผลการทดลองมายัง Sophos central ที่ระบุผู้ใช้งาน, อุปกรณ์ที่ใช้และรายละเอียดการทดสอบต่างๆ ให้ช่วยระบุจุดอ่อนความปลอดภัย พร้อมกับเสริมสร้างการป้องกันให้แก่องค์กรของคุณ ทำให้ผู้ใช้งานได้เรียนรู้เท่าทันสถานการณ์มากยิ่งขึ้น อีกทั้งยังสามารถรองรับได้มากถึง 10 ภาษา นอกจากจะประหยัดเวลาในการ Training แล้ว ยังประหยัดค่าใช้จ่ายและเพิ่มความปลอดภัยอีกขั้นให้แก่องค์กรของคุณอีกด้วย