עלון מודעות אבטחת מידע למשתמשי מחשב

הונאת המנכ"ל

מה זה הונאה מנכ"ל / BEC?

תוקפי סייבר ממשיכים לפתח התקפת דוא"ל בשם הונאת המנכ"ל, או פגיעה בדוא"ל של עסקים (BEC). התקפת דוא"ל היא התקפה ממוקדת, שמטעה את הקורבן לבצע פעולה שהוא או היא לא צריכים לבצע. ברוב המקרים הרעים רוצים להשיג כסף. מה שעושה את ההתקפות האלו למסוכנות הוא המחקר ועבודת הרקע שהתוקפים עושים לפני שליחת ההתקפה דרך הדוא"ל. כמו כן, קיים קושי אבטחתי טכנולוגי להפסיק או למנוע את ההתקפות האלו, משום שאין קבצים נגועים בדוא"ל או קישורים זדוניים שניתן לזהות.

הנה דוגמא לתהליך ההתקפה, תוקף הסייבר משתמש באינטרנט וברשתות החברתיות על מנת לחקור וללמוד את הקורבן המיועד, אנשים אשר יש להם אינטראקציה עם הקורבן. לדוגמה, אם הם סימנו אותך, הם ילמדו ויגלו מי הבוס שלך בעבודה או אולי סוכן נדל"ן שאתה עובד עמו. לאחר מכן, התוקף ישלח דוא"ל לכתובת הדואר שלך, מעמיד פנים שהוא אחד מהאנשים האלה. הודעת האימייל דחופה, מחייבת אותך לנקוט פעולה באופן מיידי, כגון טיפול בחשבונית, בשינוי למי אתה משלם או לשכנע אותך להשיב ולצרף מסמכים רגישים. התקפת הדוא"ל עובדת על ידי הפעלת לחץ לגרום לך לעשות את מה שהם רוצים. הנה שתי דוגמאות כיצד התקפה כזו יכולה לפעול.

העברה בנקאית: פושעי הסייבר רודפים אחרי הכסף. הם חוקרים את החברה שאתה עובד בה, כגון זיהוי מי עובד בהנהלת חשבונות או מי אחראי על העברות כספים ותשלומים. הפושעים מעצבים ושולחים דוא"ל לאנשים אלו ומעמידים פנים שהם הבוס שלהם או מנהל בכיר בחברה. דוא"ל אומר להם שיש מצב חירום ונדרש להעביר כסף באופן מידי לחשבון בנק חדש. האימייל מלחיץ אותם לעשות טעות ובמציאות הם שולחים כסף לפושעי הסייבר.

הונאת כח אדם: פושעי סייבר רוצים להשיג מידע אישי של אנשים לצרכי הונאות וסחיטה. אחת הדרכים המהירות ביותר להגיע לזה היא לגנוב את המידע של כל העובדים בחברה. פושעי סייבר יזהו מי עובד במחלקת משאבי אנוש. לאחר מכן הם שולחים דוא"ל מזויפים לאנשים אלו, מעמידים פנים שהם מנהלים בכירים או אולי מישהו מהמחלקה המשפטית. האימיילים יוצרים סיפור מזויף דחוף, שיש צורך להעביר מידע על כל העובדים בחברה ויש להגיש אותו מיד. אנשי מחלקת משאבי אנוש חושבים שהם שולחים את המסמכים הרגישים למנהל הבכיר, כאשר במציאות הם שולחים אותם לפושעי הסייבר.

הגן על עצמך

אז מה אתה יכול לעשות כדי להגן על עצמך? השכל הישר הוא ההגנה הטובה ביותר שלך. להלן הרמזים הנפוצים ביותר שניתן לחפש.

דוא"ל הוא קצר ומאוד דחוף (לעתים קרובות רק כמה משפטים), החתימה רושמת שהדוא»ל נשלח ממכשיר נייד.

יש תחושה חזקה של דחיפות, לוחצים עלייך להתעלם או לעקוף את המדיניות של המעסיק. תמיד פעל לפי מדיניות עבודה והנהלים, גם אם הדוא"ל נשלח מהבוס שלך או אפילו מנכ"ל.

הודעת האימייל קשורה לעבודה, אך משתמשת בכתובת דוא»ל אישית, כגון @gmail.com או @hotmail.com.

נראה דוא"ל מגיע ממנהל בכיר, עמית לעבודה או ספק שאתה מכיר או עובד איתו, אבל הטון של ההודעה לא נשמע מתאים להם.

הוראות לתשלום שונות מהוראות תשלום דומות שקיבלת בעבר, כגון בקשה לתשלום מיידי לחשבון בנק אחר.

אם אתה חושד שמישהו סימן אותך בעבודה, יש להפסיק את כל האינטראקציה עם התוקף ולדווח לממונה שלך. אם אתה חושד שמישהו סימן אותך בבית או שנפלת קורבן להעברה בנקאית שנעשתה, מיד לדווח על כך לבנק שלך, ואז למשטרה.

עורך אורח

דון קאונדר הוא סוכן מיוחד לשעבר של ה- FBI, עם מעל ל-22 שנות וותק בזיהוי פלילי דיגיטלי ופשע דיגיטלי. לאחרונה הוא מתאם פעילות בין ארגונים אשר נפגעו מפעולות סייבר בוושינגטון די.סי. הוא מספק הכשרה ומבצע מחקר דיגיטלי פלילי וחקירות סייבר. @don_cavender

https://www.linkedin.com/in/donald-cavender

מקורות

הנדסה חברתית: https://www.sans.org/u/HE3

עצור את הדיוג: https://www.sans.org/u/HE8

עצור את התוכנה הזדונית: https://www.sans.org/u/HEd

נעל את הכניסה שלך: https://www.sans.org/u/HEi