



26.04x14.82	1	עמוד 12	הארץ - סייבר	11/05/2021	77236426-7
ODI מנכ"ל ODIX חברת טייבראורן איתן - מנכ"ל - ODIX - 20934					

כן ניתן להגן על הדוא"ל הארגוני

הדוא"ל הוא נתיב החדירה העיקרי של נוזקות ופשינג לארגונים. רק שילוב נכון בין שכבות של פתרונות אבטחה שונים עם הדרכת העובדים להיגינת סייבר, יפחית משמעותית את הסיכון להיפגע מהתקפות זדוניות החודרות לארגון דרך הדוא"ל

אל"מ (במיל) ד"ר אודן איתן



אודן איתן | צילום: תומר שלום

הדוא"ל הפך מזמן לנשמת החיים של התקשורת העולמית, בעיקר בסביבה העסקית. לכן לא מפתיע שלפי רוח פרצות האבטחה של וריזון לשנת 2020, 94% מההתקפות התוכנה הזדוניות מגיעות דרך הדוא"ל. הגנה אפקטיבית על הדוא"ל הארגוני מפני איומים ונוזקות יכולה לעשות את ההבדל בין "עסקים כרגיל" לבין כותרות ראשיות על פריצה לארגון ונוק כספי ותרמית עצום. לפיכך חשוב להגן על שער הכניסה לדוא"ל (gateway) מפני כל סוגי האיומים, ידועים או לא ידועים - או שההשלכות עלולות להיות הרסניות.

כיצד אם כן ניתן להגן על הדוא"ל הארגוני? התהליך אולי נראה מורכב, אך ניתן לשפר את אבטחת הדוא"ל באופן ניכר על-ידי שליטה בזרימת הקבצים המאושרים, שילוב של מספר שכבות הגנה והגבלת גישות ארמין למירע חיוני. פלטפורמות אבטחת סייבר הקיימות בשוק - כגון אנטי-וירוס, SEG, או Sandbox - מעניקות הגנה מפני נוזקות נפוצות ואיומי סייבר ידועים, ולכן מהוות את לב ליבה של מדיניות אבטחה יעילה בדוא"ל. אולם, מידת ההצלחה של מערכות אלו תלויה

פרצות אבטחה ברמת המערכת.

אם רק יקפידו על ערכון תכוף של טכנולוגיות למניעת התקפות סייבר, צוותי IT יוכלו למקד את תשומת ליבם במילוי פערי האבטחה ושיפור המודעות לאבטחה בארגונם. זוהי נקודה חשובה, מפני שאבטחת הדוא"ל תלויה במידה רבה באנשים שמשתמשים בו. סיכול ניסיונות פשינג מסתכם בסופו של דבר בהחלטה של העובד הבודד אם ללחוץ על הקישור או לא, ולכן הדרך להגן על הארגון מפני כמה משיטות הפריצה הנפוצות ביותר, היא להדריך את העובדים היטב למודעות סייבר ולשלב זאת עם טכנולוגיות מניעה מתקדמות, הממועדות את משטחי התקיפה שהארגון חשוף אליהם.

מיגון הדוא"ל הארגוני מפני תקיפה עתידית צריך להיות רומה להכנה לקראת סופת חורף: רייבוי שכבות הוא המפתח. הארגון צריך לשלב שכבות של מספר מערכות וטכנולוגיות אבטחת דוא"ל שונות, אשר יחדיו ייצרו מודל שיכול לבודד את פלטפורמת הדוא"ל מכל סוג של מתקפת סייבר.

כלי אבטחה מסורתיים כגון אנטי-וירוס, מערכות SEG, שירותי PKI ושירותי זיהוי מנהלים, אמנם מהווים יסוד איתן לאבטחת דוא"ל בסיסית, אך זהו רק שלב ראשון באבטחת הדוא"ל הארגוני. פתרונות

נייטיב ברמה מקומית - כגון Microsoft EOP, או Microsoft Defender (ATP) - פותחו במטרה לסיפק שכבת מניעה ראשונה בפני האיום המתרחב של תוכנות זדוניות ידועות. כלים אלה עושים עבודה ראויה להקטנת הסיכון, אבל הוכח כי יעילותם משתפרת ככל שמשלבים אותם עם פתרונות צד שלישי, כגון פתרונות הלבנת קבצים בגישת CDR, אשר מבצעים "פידוק והרכבה מחדש" של התוכן שמגיע בדוא"ל ומשאירים את רכיבי הנוזקה בחוץ. רק כאשר הפתרונות הללו משולבים ברמת נייטיב - כמו למשל במקרה של FileWall עם סכיבת מיקרוסופט 365 - הם מפחיתים בצורה משמעותית ביותר את האיום על משתמשי הקצה בארגון.

בין אם בארגון יש עשרה עובדים או 1,000, הצורך להגן על הדוא"ל שלהם הוא קריטי וברור. רק שילוב נכון בין שכבות של פתרונות אבטחה שונים עם הדרכת העובדים להיגינת סייבר, יפחית משמעותית את הסיכון להיפגע מהתקפות זדוניות החודרות לארגון דרך הדוא"ל.

המחבר הוא מנכ"ל חברת ODIX המפתחת פתרונות אבטחה לנישורול וירוסים ונוזקות מקבצים ארגוניים. לשעבר מפקד יחידת מצויב בצה"ל