שלום רב,

<u>הוראות התגוננות מפני תכנות כופרה</u>

לאחרונה נכרת עליה חדה במגוון ובכמות האיומים הדיגיטליים המודרניים. בלטה במיוחד מתקפת הסייבר העולמית אשר זכתה לכינוי **WannaCry**. וירוס כופר זה **(Ransomware)** גרם לנזק רב למערכות ממוחשבות במדינות רבות בעולם, ובין היתר נפגעו ושותקו בתי חולים ברחבי בריטניה, חברת השליחויות האמריקאית Fedex, בנק BBVA הספרדי, מערכת הרכבות במספר ערים בגרמניה, אוניברסיטאות ועוד.

רוב מקרי ההידבקות מקורם בפתיחת קישורים או קבצים בהודעות דואר זדוניות. ברגע שמשתמש נפגע בווירוס כופרה, מנגנון הווירוס ינסה להצפין קבצים בכל מקום שלמשתמש יש זכות כתיבה אליו. למעשה אין דרך לתקן את הקבצים שהוצפנו ובהנחה שלא רוצים לשלם למבקשי הכופר, הדרך היחידה לחזרה לשגרה היא החזרת הקבצים מגיבוי.

WannaCry התבסס על פרצת אבטחה במנגנון שיתוף הקבצים של מיקרוסופט. מיקרוסופט אומנם שחררה תיקון לפרצה עבור מערכות הפעלה מודרניות בעדכונים השוטפים, אך למערכות הפעלה ישנות (כדוגמת Windows XP ו Windows Vista) שלא נתמכות על ידי מיקרוסופט זה מכבר, שוחררו תיקונים לפרצה רק לאור הפרסומים, ממש יום יומיים לפני ההתפרצות.

אנחנו בערדום נערכנו ונערכים כל העת לשלל המתקפות. בכל זאת, לא נוכל לעשות זאת בלעדיכם. בידכם לסייע למניעת התפרצות הווירוס בארגון.

<u>דרכי התגוננות ברמת המשתמש</u>:

אל תפתחו קבצים המצורפים למיילים חשודים או לא מוכרים –לעולם אל תפתחו קבצים המצורפים להודעות דואר אלקטרוני אם אינכם בטוחים במאה אחוז מהי התשובה לכל אחת מהשאלות הבאות:

- ✓ מי הוא השולח?
- ✓ מה הוא שלח?
- ✓ מדוע הוא שלח את ההודעה אליי?

אם יש ספק ולו הקטן ביותר, יש למחוק ללא פתיחת ההודעה והקבצים המצורפים.

<u>דרכי התגוננות ברמת הארגון</u>:

- ✓ אנו מפעילים במבואות הדואר שלנו (זהו מעגל ההגנה ההיקפי) כלי סינון, אך חשוב לדעת כי הצלחתם בעצירת מפגעים כאלו אינה מוחלטת. לפעמים מסתננות הודעות שבעיני מנגנון סינון כזה, נראות כהודעות תמימות.
- ✓ אנו דואגים כי מערכות ההפעלה יהיו מעודכנות.
- ✓ אנו דואגים לשגרת גבוי כולל בדיקה תקופתית של שחזור יזום.
- ✓ על מנת לצמצם את מימדי ההיפגעות, חשוב להקפיד על מדיניות שאינה ליבראלית במתן הרשאות כתיבה לתיקיות ברשת למשתמשים. דהיינו יש לצמצם ככל הניתן את הרשאות הכתיבה של משתמשים למקומות שונים, כך משתמש שנפגע בווירוס כופר, ידביק רק את רשימת המקומות המצומצמת שיש לו הרשאת כתיבה אליהם.

בברכה,

יוסי מורחי
מנהל תפעול - שרותי תקשוב ערדום

שרותי ערדום תקשוב
◄ד.נ חבל אילות 88820 ► ◄ טל: 08-6355755 ◄► פקס: 08-6355770 ►
E-mail: yossim@ardom.net