נהלי מחשוב ואבטחת מידע – הנחיות למניעת הדבקה בווירוס כופר

לכבוד
עובדי המועצה

הנדון: איך להימנע מהדבקה בווירוס כופר

מהו וירוס כופר ?

לאחרונה מתקבלים חדשות לבקרים חדשות אודות תקיפות וירוס כופר של ארגונים ואנשים פרטיים. הווירוס תוקף את מחשבי המשתמש / המשתמשים ומצפין את כל הקבצים של המשתמש במחשב ובתיקיות השיתוף (בכונני רשת, דיסק און קי וכו') בהם יש למשתמש הרשאות. בסוף ההליך מתקבלת הודעה על המסך המודיעה לקורבן כי עליו לשלם כופר במטבע ביטקויין (מאות דולרים עד אלפי דולרים) תוך כמה שעות ואם לא – החומר כולו יישאר מוצפן לעולם.
הווירוס משתמש בחולשות של המשתמש / הארגון ומגיע דרך קבצים מצורפים לדוא"ל או קבצים נגועים בדיסק און קי אשר בהם קיים סקריפט (קוד תוכנה המופעל ללא התקנה) המריץ את מנגנון ההצפנה המובנה של מערכת ההפעלה windows. הקבצים מוצפנים במפתח קוד הצפנה הידוע לתוקף בלבד והוא דורש עבורו כסף.

הנחיות למניעה מהדבקה בווירוס כופר

1. אל תפתחו קבצים המצורפים לדוא"ל חשודים או לא מוכרים – לעולם אל תפתחו קבצים המצורפים להודעות דואר אלקטרוני אם אינכם בטוחים במאה אחוז מהי התשובה לכל אחת מהשאלות הבאות:
   a. מי הוא השולח?
   b. מה הוא שלח?
   c. מדוע הוא שלח את זה אליי?

השתלטות על חשבונות דואר אלקטרוני במטרה להפיץ הונאות רשת היא לא דבר נדיר. לכן העובדה שאתם כביכול מכירים את השולח לא מספיקה על מנת להבטיח שהקובץ המצורף הוא לא וירוס. דבר ראשון, יש להסתכל מהי כתובת הדוא"ל של השולח ולקרוא את נושא ההודעה. אם משהו נראה חשוד, פעלו בזהירות – עדיף למשל שתיצרו קשר עם השולח על מנת לוודא אם הוא אכן שלח לכם את ההודעה ומה מכיל הקובץ המצורף.
מקרים שממש צריכים לעורר את חשדכם הם לגבי אנשים שאינכם נמצאים איתם בקשר שפתאום שולחים לכם

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

נהלי מחשוב ואבטחת מידע – הנחיות למניעת הדבקה בווירוס כופר

כל מיני הודעות וקבצים מוזרים, או למשל לגבי הודעות שמתחילות ב"בהמשך לשיחתנו", "בהמשך לבקשתך" למרות שמעולם לא דברת או פנית לאותו אדם.

אחד מהתקפות ה Ransomware הגדולות ביותר הדביקו מאות, ואפילו אלפי משתמשים, באמצעות תכתובת דואר אלקטרוני המתחזה לשירות Fax to Mail - שירות שמעביר פקסים שנשלחים אליכם ישירות לתיבת הדואר האלקטרוני). הקורבנות שקיבלו את המייל לחצו על הקובץ המצורף, למרות שרבים מהם לא ציפו לקבל דואר אלקטרוני ומעבר לכך – רבים מהם כלל לא היו מנויים לשירות כזה!

2. אל תלחצו על קישורים מפוקפקים – למרות שרוב מתקפות הכופר מקורן בקבצים המצורפים להודעות דואר אלקטרוני, קיימות שיטות התקפה נפוצות נוספות. אחת מהן היא לכלול קישורים בתוך הודעת המייל, שיובילו את הקורבן לאתר שמבצע את התקנת התוכנה הזדונית משרת מרוחק. בדומה לסעיף 1, אם אינכם יודעים מי שלח לכם את הקישור ולמה – אל תלחצו עליו.

התוקפים עלולים לשלוח מיילים המתחזים לשירותים מוכרים כמו PayPal, אתר הבנק שלכם ועוד, ועליכם להיות ערניים מאוד על מנת להבחין שמדובר בהתחזות, אבל אם יש אפילו ספק קל שבקלים – אל תלחצו! נושא המייל, כתובת המייל של השולח, תוכן ההודעה ואפילו שם הקובץ המצורף – כל אלה יכולים לעורר חדש, ואם אכן התעורר חשד עדיף להתקשר לשירות הלקוחות של הגוף שכביכול שלח לכם את ההודעה, מאשר ללחוץ על הקישור ולהצטער.

3. שמרו על מערכת הפעלה, תוכנות ואפליקציות מעודכנות – עדכוני תוכנה הם חיוניים במלחמה נגד תוכנות זדוניות. האקרים רבים מנצלים פירצות אבטחה ידועות במוצרי תוכנה ומצליחים באמצעותם לחדור למחשבים ולפגוע במשתמשים. כאשר מתגלה פרצה בתוכנה כלשהי, לרוב היצרן דואג להפיץ תיקון. אך כל עוד התוכנה המותקנת במחשב לא עודכנה, הפרצה עדיין קיימת. התוכנות החשובות ביותר לעדכון הן מערכת ההפעלה שלכם, תוכנת הג'אווה, הדפדפנים, תוכנת הפלאש וכן תוכנת האנטי וירוס וחומת האש.

בנוסף, ולא פחות חשוב, עליכם לוודא שהתוכנות המותקנות במחשב שלכם או במחשבי העסק שלכם הן חוקיות ואותנטיות – גם אם מדובר בתוכנה חינמית. תוכנות לא חוקיות לרוב מכילות פרצה שמאפשרת להתגבר על נושא הרישוי ולכן הן משמשות כר פורה להאקרים כדי לפוגע באותם משתמשים. כמו כן לרוב תוכנות אלה לא מתעדכנות באופן שוטף מה שמגדיל עוד יותר את הסיכוי שהם מכילות פרצה אבטחה מסוכנת.

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר

נהלי מחשוב ואבטחת מידע – הנחיות למניעת הדבקה בווירוס כופר

4. ודאו שקיימת תוכנת אבטחה על כל מחשב – קיימת חשיבות עליונה בשימוש בתוכנת אבטחה – במיוחד בהקשר של תוכנות כופר. תוכנת אבטחה יכולה למנוע מהקוד הזדוני לפעול ולהדביק את המחשב שלכם – בתנאי שהיא מעודכנת ומוגדרת כראוי. בהרבה מבתי העסק שנדבקו בתוכנות כופר נתגלה שלא היה קיים אנטי וירוס על כל התחנות ברשת, מה שאפשר לתוכנת הכופר להצפין קבצים בשרתים של החברות שנפגעו.

גם באנדרואיד - פתרון אבטחה הוא לא בלעדי למחשבים אישיים. עם התפתחות הנוזקות למערכות ההפעלה הסלולאריות, כמו ה – SimpLocker תוכנת הכופר הראשונה למכשירי אנדרואיד, חיוני להתקין תוכנת אבטחה גם על טאבלטים וסמארטפונים.

חשוב לוודא שתוכנת האנטי וירוס שלכם בתוקף, שהיא מעודכנת בחתימות הווירוסים העדכניות ביותר ושהיא מוגדרת בצורה נכונה.

5. בצעו גיבוי תקופתי לכל המידע שלכם – ככל שהעולם הופך טכנולוגי יותר, כך גיבוי הופך לדבר חיוני יותר – בין אם בבית או בעסק. עסקים וחברות גדולות כבר הכירו מזמן בצורך בגיבוי והנסיבות, לצערנו, מכתיבות לנו מציאות שבה כל אדם צריך לעשות גיבוי של המידע שלו – לכל צרה שלא תבוא.

במקרה של תוכנות כופר החשיבות של גיבוי עולה בעשרות מונים, כיוון שהדרך הבטוחה היחידה להשיג בחזרה את המידע המוצפן שלכם היא באמצעות שחזור מתוך הגיבוי. גם משתמשים שבחרו לשלם את הכופר גילו שאין הבטחה שהמידע יוחזר אליהם, ולכן גיבוי הוא הפתרון היחיד למקרה שהותקפתם על ידי תוכנת כופר.

בברכה,

אריאל הידליסהיימר
מנכ"ל המועצה

בית חשמונאי ד.נ שמשון 9978900
טל. 08-9274040
פקס. 08-9247115
www.gezer-region.muni.il
מועצה אזורית גזר