הנחיות לעבודה בסביבה מאובטחת – איך להימנע מווירוסים / דויד שליט

לאחר כמה מקרים של וירוסי מחשב שאירעו ברפתות בעת האחרונה, ובעקבותיהם נותרו אנשים ללא אפשרות שחזור מידע, אני רוצה לתת כמה עצות למניעה ועבודה מודעת לבעיות אבטחה. בבקשה קראו את ההמלצות והיעזרו באיש מקצוע כדי ליישמן.

1. גיבויים: יש לדאוג לגיבוי יומי מסודר למדיה חיצונית או ל"סינכרון לענן" [פרטים בהמשך]
2. לדאוג להתקין תוכנת אנטי-וירוס. האנטי-וירוס חייב להיות בגרסה מעודכנת והוא חייב להתעדכן כל העת.
3. להנחות את המשתמשים במחשבי הרפת לא לפתוח מיילים ממקור שאינו ידוע או מיילים המכילים קישורים שנראים חשודים או לא ברורים.
4. להנחות את המשתמשים במחשב לא לגלוש לאתרים מפוקפקים
5. פיירוול מקומי על המחשב פועל

ועכשיו ארחיב קצת לגבי כל נושא. רצוי גם להתייעץ עם איש הרשת או מי שמטפל לכם במחשבים על מנת לקבל עזרה בהתקנות וביישום הנקודות שהעליתי:

1. גיבויים: נעה מאפשרת לבצע גיבויים אוטומטיים לשני יעדים. כדאי להגדיר יעד אחד שיהיה דיסק חיצוני שאפשר יהיה לנתקו בסוף יום העבודה מהמחשב ולקחת הביתה. זאת על מנת שאם המחשב ייפגע מווירוס, המידע שעל הדיסק הנייד לא יפגע ביחד עם כל המחשב. דרך נוספת היא שימוש בכלי סנכרון לענן כמו Dropbox או Google drive בכל אחת משתי האפשרויות, יש להירשם לשירות [בחינם] ואח"כ להוריד את תוכנת הסינכרון למחשב. בסיום ההתקנה, יש להפנות את הגיבוי של נעה גם לתיקייה המסתנכרנת לשירות שהתקנתם [דרופבוקס או גוגל דרייב]. כדאי להיעזר לשם כך באיש מקצוע.

2. תוכנת אנטי-וירוס חייבת להיות מותקנת על המחשב אבל בנוסף חשובים שני דברים: 1. שהתוכנה עצמה מעודכנת לגרסה האחרונה שלה. שימו לב, יכול להיות שמותקן על המחשב אנטי-וירוס אבל בגרסה ישנה. חשיבות העדכון של גרסת התוכנה עצמה הוא קריטי, שכן "המנוע" מתעדכן ומתאים את עצמו לאיומים חדשים כל הזמן. 2. שמתבצעים

עדכונים אוטומטיים כל העת. העדכונים האלה מכילים "עדכוני חתימות" לווירוסים חדשים שצצים ולכן חשוב לדאוג שיהיה עדכון.
מומלץ בנוסף לתוכנת האנטי-וירוס להוריד תוכנה לזיהוי והתרעה מפני תוכנות זדוניות כגון Malwarebytes

3. וירוסים מגיעים אל המחשב מכמה מקורות, בניהם אימיילים. ראשית מיילים ממקור לא ידוע – לא לפתוח. במיוחד אם לא מצפים למשהו. מיילים חשודים ינסו לפתות את המשתמש לפתוח קובץ או ללחוץ על קישור המוביל.. אל אתר נגוע בווירוס ומדביק את המחשב. אז ההנחיה היא לא לפתוח קבצים המצורפים למייל. במיוחד קבצים עם הסיומת exe או bat, ובמיוחד אם המייל מגיע ממקור לא ידוע.
מיילים ממקור ידוע הם בעיתיים יותר כי אנחנו נוטים לסמוך על אנשים המוכרים לנו. אבל ייתכן שמייל נגוע נשלח אלינו בשמו של מישהו מוכר לנו כתוצאה מווירוס.. לכן, אם מקבלים מייל ממקור ידוע והוא מכיל טקסט לא מתאים, או חשוד, או מכיל קישורים שנראים לנו לא מתאימים לאותו אדם – שוב, לא לפתוח.

4. גלישה לאתרים מפוקפקים – אתרי סקס, אתרים של תוכנות לא חוקיות, אתרים לצפייה ישירה בסרטים וסדרות, אתרי הימורים – כל אלה הם אתרים המועדים לפורענות ויש להנחות את המשתמשים שלא יגלשו אליהם. כמו כן, תוכנות להורדות טורנטים [כמו uTorrent] ולשיתוף קבצים, הן תוכנות שחשוב להרחיקן ממחשב שנמצא עליו חומר חשוב. בנוסף – הורדה של תוכנות לא חוקיות הן מקור לבעיות כי הן מכילות לעיתים וירוסים שונים הנמצאים ב key generator הנועדו כדי "לפרוץ" את התוכנות, או אף בתוכנות עצמן. וככלל – במחשב הרפת צריכות להיות מותקנות מעט תוכנות, ורק אלו המשמשות את צרכי הרפת.

5. פיירוול מקומי – פיירוול מקומי קיים כחלק מתוכנת האנטי-וירוס, וגם כחלק מ windows. כדאי להפעיל אותו.