Newsletter #3

לקוח נכבד,

תחום אבטחת המידע הפך להיות נושא עיקרי בתכנון ויישום טכנולוגיות בקרב חברות רבות. מערך אבטחה יעיל בסביבות הקיימות כיום, דורש הרבה מעבר להרצת אפליקציות אנטי-וירוס והתקנת חומות אש (Firewalls). עליו לכלול בנוסף הכשרה והדרכת משתמשים ואנשי מערכות מידע.

אחת ההתמודדויות העיקריות של אנשי ה IT זה עם כמות העדכונים הרבה הנובעים רובם מאיומי אבטחה חדשים . ניהול ובקרה של עשרות ומאות השרתים ותחנות העבודה בארגון . ללא כל ספק שמירה על רמת עידכונים גבוהה במערכות הינה גורם מפתח לאיכות אבטחת המידע בארגון .

על מנת לספק פתרון לניהול Patches בארגון חברנו כשותף עסקי לחברת Patch Link, הנחשבת בצדק, לחברה המובילה בעולם בתחום של Patch Management. מוצרי Patch Link תומכים ומנהלים את כל סביבות מיחשוב ומערכות האבטחה בארגון.

אנו שמחים להציע את מוצרי Patch Link הכוללים במידת הצורך גם תמיכה טכנית והטמעה .

בהמשך, מצורף המאמר "ניהול עדכונים" להעשרת הידע בנושא.

לקבלת פרטים נוספים ופניות בנושא, ניתן ליצור עימנו קשר בכתובת Info@securitree.co.il .

אביאת בר
מהנדסת אבטחת מידע

ניהול עדכונים (Patch Management)

מאת: איזק קרמונה, מהנדס אבטחת מידע בכיר בחברת סקיוריטרי.

ניהול עדכונים הוא אחד המשימות החשובות ביותר לעבודת ניהול רשתות נכונה. משימה זו, מורכבת מסריקה ומיפוי המערכות ברשת, מציאת עדכונים (patches) חסרים, והטמעתם ברגע שהם מתפרסמים והופכים זמינים. אי ביצוע פעולה זו גורמת לפגיעה כפולה ברשת: כעת לא רק שהמפגע כבר קיים, הוא גם התפרסם ברבים. הפרסום יגרום להאקרים ולכותבי הוירוסים לנסות ולנצל פרצה קיימת על ידי יצירת התקפות מכוונות עבורה.

פעמים רבות, כשלו מנהלי רשתות בעדכוני מערכות המחשוב שלהם. דוגמא לכך ניתן לראות בתקופה של השנתיים האחרונות, כאשר תולעי המחשב, כגון ה-Slammer, שצץ בינואר 2003, התפשטו במהרה באינטרנט בעקבות ניצול של חורי אבטחה שהתפרסמו.

מאחר ומערכות המחשוב לא עודכנו, הייתה הפגיעה בהן, בלתי נמנעת. עד לא מזמן, הסיבה העיקרית לכך הייתה שפעולת עדכון הגרסאות הייתה משימה מסורבלת ומרתיעה. אך עם הופעתם של כלים אוטומטיים מתוחכמים לניהול עדכוני תוכנות, חל שינוי בנושא.

עדכון מערכות מחשוב הוא רק חלק מאסטרטגית האבטחה הכוללת בארגון, אך ללא ספק זהו הנושא החשוב ביותר. כאשר נגשים לכתוב נוהלי אבטחת מידע לחברה, חלק מהנוהל צריך להיות מוקדש לתהליך והשיטה של ניהול עדכונים. אף על פי שקיימות דרכים רבות לאבטחה ולהגנת מערכות המחשוב מפני ניצול חורי האבטחה, המטרה הסופית היא תמיד להביא את כל המחשבים למצב עדכני ככל שניתן. יעד זה הוא בר השגה רק על ידי עדכון של כל הטלאים האבטחתיים במערכות.

מחזור ההתקפות והעדכונים

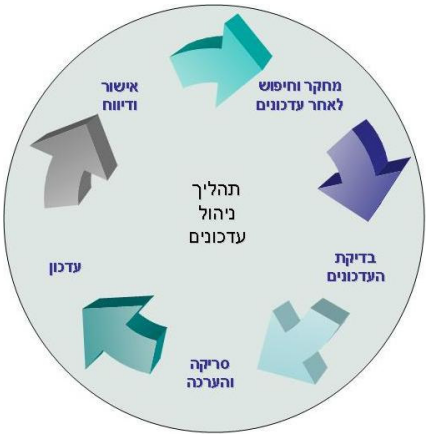
עדכון מערכות הוא צורך ידוע בתחום המחשוב כל יום מתפרסמים באגים חדשים המצריכים את תשומת לבינו. בין החברות קיימות גישות שונות בטיפול עדכוני האבטחה השונים. ישנם ארגונים שיתקינו מראש כמה שיותר עדכונים. אחרים יתמקדו רק במערכות החשופות לאינטרנט הנמצאות בסיכון גבוה. יהיו כאלו שיחכו עד שההתקפות יחלו ואז ינקטו בפעולות קיצוניות כמו ניתוק או כיבוי המערכות הנגועות. כאמצעי בקרה חלופיים, יהיו חברות שיבחרו לנהל פתרונות אבטחה משלימים בכדי להגן על המערכות מפני איומים פוטנציאלים.

בלי קשר לשיטות ההגנה, ניתן לומר כי אנו מתקרבים מאוד לנקודת רתיחה של מחזור בלתי נפסק של התקפה ועדכונים. במקרה הטוב אנו נמצא בשגרת פעילות חוזרת היעילה במקצת, לאור העוצמה של בעיית העדכונים הקיימת. במקרה הגרוע, נתעלם מהבעיה, ובכך נאפשר להתקפות להגביר את יעילותן ולהתפשט בכל מקום בארגון ובאינטרנט.

המתקיפים, בדרך כלל, הם אופורטוניסטים. הם סורקים את האינטרנט במטרה לגלות מערכות פגיעות וברוב המקרים הם מנצלים את הפרצות על ידי כלי פריצה הנמצאים באתרי ההאקרים. Code Red, Nimda ו- Slammer לדוגמא, אלו הן פרצות שהופצו כתוצאה מניצול הפרסום בתרי האינטרנט, של חורי אבטחה קיימים, בכדי לגרום נזקים למערכות המחשוב.

כיום, הארגונים יכולים להימנע במידה רבה מרוב האיומים, על ידי עדכונים פשוטים של המערכות בארגון. אך המילה "פשוט" היא בעצם בלשון המעטה, כי הרי ברור שהמספר הרב של העדכונים הדרוש בסביבות מורכבות של ארגונים היום, יוצר צורך חזק של כלי אוטומטי כלשהו בכדי להתגבר על תהליך העדכון המסורבל.

ניהול עדכונים ממוכן



מספר פרצות התוכנה המתפרסמים מידי שבוע הגיע לקרוב ל- 80. עקב קבלת מספר כה רב של פרצות, הפך ניהול העדכונים למעשה, להיות מדע מדויק. ניהול עדכונים אינו מבצע חד פעמי, אלה סידרה של צעדים ומהלכים מתמשכים במטרה להביא את סביבת המחשוב למצב העדכני ביותר מבחינת אבטחת המידע. התהליך הבסיסי מתואר בדיאגראמת "תהליך ניהול העדכונים" שלפנינו.

נעמוד על כל אחד מהתהליכים:

- מחקר וחיפוש לאחר עדכונים

מומלץ כי עדכון חדש יותקן בכל המערכות הקיימות בארגון, אך המספר הרב של חורי האבטחה הקיימים דורש תהליך של מחקר שיקבע האם עדכון מסוים אכן נדרש. במסגרת תהליך זה יש לבצע מעבר דקדקני בין כל גרסאות חדשות, service packs ותיקונים זמניים כדי להחליט אילו מהם רלוונטיים/ מתאימים לארגון.

- **בדיקת עדכונים**

ברגע שהעדכון זוהה כרלוונטי לארגון, יש לבצע שלב בדיקות על מנת להעריך את השפעתו בסביבת המחשוב הקיימת. בסביבות קטנות, הבדיקה תהיה לרוב פשוטה כמו התקנת העדכון בקבוצת מחשבים מבוקרת ושימוש בו בעבודה יומיומיות למשך מספר ימי מעקב. בסביבות מסורבלות יותר, משך תהליך הבדיקה במעבדות, יכול להגיע לשבועות עד שהוא נמצא מתאים להתקנה בכל הארגון.

- **סריקה והערכה**

מכיוון שסביבות המחשוב הן ברובן מורכבות ודינאמיות, קשה מאוד לאתר מערכת שבה נחוץ עדכון מסוים. השלב הבא הוא ביצוע סריקה של מערכות המחשוב, על מנת להעריך כל אחד מהם בנפרד ולזהות את כל אותן המערכות הדורשות עדכונים נוספים ודחיפות העדכון בהן, היא גבוהה.

- **עדכון**

לאחר שלושת השלבים שצוינו לעיל, ניתן לבצע עדכון למערכות ע"פ הממצאים שנמצאו קודם לכן. העדכון הוא בדרך כלל התהליך שצורך זמן רב יותר מכל שאר התהליכים בשרשרת. שלב זה הינו השלב המכריע בהגנה על הארגון.

- **אישור ודיווח**

השלב האחרון הוא אישור ביצוע על התהליך כולו. האישור מבטיח כי המערכות והאפליקציות הדורשות עדכונים, אכן עודכנו בהצלחה. שלב זה מספק את הביטחון שתהליך העדכונים אכן הסתיים כראוי.

כל השלבים של ניהול עדכונים שתוארו לעיל מצריכים משאבים רבים. מיכון של התהליך מקטין את כמות השעות הכולל הדרוש לניהול התהליך עד לסיומו. יתרונות היעול הם דבר ברור מאוד למנהלי תשתיות שאחראיים לעדכון מערכות המחשוב בארגון. מעבר מתהליכי אד הוק או תהליכים ידניים למערכת ממוכנת מספקת יתרונות משמעותיים ביותר.

נסכם ונאמר כי כיום ניתן למצוא הרבה מערכות מורכבות ומסורבלות וחורי האבטחה הם רבים מידי בכדי שארגון בעל מערכות אלו, יוכל לבצע הטמאה ידנית של העדכונים. לא

ניתן יותר לצפות מאפליקציות בסיסיות שפותחו בתוך הארגון לבצע את עדכון טלאי האבטחה כראוי. חברות צריכות כלים אוטומטיים שידווחו למנהלי ה-IT באופן מיידי, בעת

שנמצאה מערכת שאינה מעודכנת ומהווה בכך סיכון אבטחתי לארגון. מנהלים צריכים כלים שיעזרו להם לזהות את אותן מערכות המצריכות עדכונים בדרגות סיכון שונות ובנוסף, להשתמש בכלים שיתופיים לניצול ותאום משאבים באופן יעיל יותר.

חברות שיש להן תהליך עדכוני מערכות שהוא מובנה וממוכן, מבטיחות רמת אבטחה גבוהה יותר, מצמצמות בהוצאות לטיפול בהתקפות וירוסים ומגדילות את פריון העבודה באמצעות זמינות גדולה יותר של המערכות. הן גם חוסכות אלפי שעות עבודה שנתיות, מקטינות את כמות התביעות הקשורות לאבטחה ורוכשות יותר אמון בקרב השותפים, הספקים והלקוחות.