לקוח נכבד,
ה"אשליה" כי מערכות מחשב מרכזיות הינן מאובטחות וחסינות בפני כל סיכון, הינה דעה רווחת בקרב חברות רבות. אולם המציאות מוכיחה כי גם במערכות המחשוב הנ"ל נדרשת השקעה רבה על מנת לתכנן ניהול סיכונים נכון ולייצב מערך תקין של אבטחת מידע.

בחברת סקיוריטרי קיים הידע בתחום ניהול הסיכונים של מערכות מחשב מרכזיות ובכך אנו יכולים לתרום מניסיוננו הרב על מנת ליצור מודלים המותאמים אישית לארגון בעל מערכות מחשוב כאלו.

בהמשך, מצורף המאמר " ניהול הסיכונים במערכות מחשב מרכזיות " להעשרת הידע בנושא.
לקבלת פרטים נוספים ופניות בנושא, ניתן ליצור עימנו קשר בכתובת
Info@securitree.co.il .

אביאת בר
מהנדסת אבטחת מידע

ניהול הסיכונים במערכות מחשב מרכזיות

מאת: צביקה גורן, יועץ אבטחת מידע בכיר ומרכז נושא DRP

בחברת סקיוריטרי.

מה לא עשו להם ?

ביכו אותם! נפרדו מהם לשלום ! "קברו" אותם ! הספידו אותם ! הכשירו את הקרקע למחליפיהם !

מי הם ???

כן, מדובר באותן חיות פרהיסטוריות, ה"דינוזאורים" הזקנים, המחשבים "האימתניים" אשר מטילים את חתיתם על כל האקר אומלל, ואלה החוסים בצילם של "ענקי" הרשת הידועים כשרתי Microsoft.

ובכל זאת, מי הם ?

אנו מדברים על מחשבי ה-Mainframe לסוגיהם השונים, מחשבי AS/400 ויורשיהם מסדרת iSeries, שרתי UNIX הנמנים על חברות IBM, SUN ו-HP ועל "חיות" אחרות בקטגוריה זו !

מרב "חיות" אלו נחשבו עד לעבר הלא כל כך רחוק כמערכות מאוד מאובטחות וכמעט "בלתי חדירות" !

והיום ?

הפתיחות ההולכת וגדלה של מערכי המחשוב הארגוניים בפני האינטרנט ובפני העולם הרחב, חשפו גם את מערכות המחשב המרכזיות בפני סיכונים המאיימים על שלמות וזמינות המידע האגור בתוכן.

ו"הדאגה" ?

זו קיימת היום בארגונים רבים בתחום אבטחת המידע והיא לא פסחה גם על מערכי המחשוב המרכזיים, ובפרט מאז נפתחו מערכים אלו לסוגי/שירותי תקשורת שונים (TCP/IP, FTP, TELNET וכיו"ב).

והפתרון ?

תכנון "חכם", יעיל ועניני לניהול הסיכונים ואבטחת המידע במערכות המחשוב המרכזיות של הארגון, תוך כדי שילוב של אמצעי אבטחה ובקרה מתקדמים המשלימים את מערכי האבטחה הקיימים.

והדרישות ליישום ?

היכרות וניסיון מעמיקים עם מערכי האבטחה בסביבות המחשוב המרכזיות לסוגיהן השונים, כמו גם הידע המתאים לתפעול והטמעה של אמצעי האבטחה המובנים והנלווים אל סביבות העבודה הנ"ל.

ובכל זאת, מה צריך לעשות ?

תכנון ליישום מודרג בשלבים של אבטחת המידע המלווה ב"תוכנית עבודה" ובאבני דרך לביצוע המטלות השונות, מהווים תנאי הכרחי לניהול "חכם" של הסיכונים ואבטחת המידע במערכי מחשוב מרכזיים.

ומה ב"תוכנית העבודה" ? מה מייחד אותה בסביבות מחשוב מרכזיות ?

מערכות מחשב מרכזיות שהנן מטבען ריכוזיות מאופיינות על ידי מגוון רחב של סביבות עבודה, ממשקים ושירותים המרוכזים על גבי פלטפורמת מחשוב מרכזית אחת ויחידה.

לפיכך קיימת חשיבות רבה לתכנון מסודר, מודרג ויעיל ליישום ולייצוב של אבטחת המידע, וזאת תוך כדי פגיעה מינימאלית בפעילות המחשוב השוטפת המקיפה בדרך כלל את כל פעילויות הארגון.

להלן הנושאים להכנת "תוכנית עבודה" המיועדת לשיפור אבטחת המידע במערכות מחשב מרכזיות:

- "צילום" מצב אבטחת המידע הקיים.

  מיפוי תשתיות, ניטור ממשקים, סיקור הגישה בתקשורת, יישום במערכת ההפעלה, ארגון מסדי הנתונים, האבטחה ברמת האפליקציות, הפרדת סביבות העבודה, תהליכי הגדרת המשתמשים והבקרות הכלליות והייעודיות בכל הרמות.

- איתור סיכונים ונקודות כשל באבטחה

  סיווג וניתוח הממצאים, איתור וזיהוי הסיכונים ומיפוי נקודות הכשל במערכים שנסקרו.

- ניתוח הסיכונים וקביעת תיעדוף לטיפול

  ניתוח הסיכונים שאותרו מהיבט של מקור הסיכון ודרגת ה"חומרה" שלו,ותיעדוף הנושאים לטיפול מהיבטים של עלות-תועלת.

- עיצוב פתרונות ותכנון לו"ז לשיפורים

  תכנון לביצוע שיפורים מידיים, עיצוב פתרונות בשיתוף גורמים בארגון, תכנון לשיפור בשלבים וקביעת אבני דרך ולו"ז ליישום.

- ליווי, סיוע ובקרה בהטמעת הפתרונות

  יישום פתרונות נקודתיים שביצועם מהיר, סיוע להטמעה בשלבים של פתרונות מורכבים וליווי ובקרת פתרונות המיושמים על ידי גופים חיצוניים.

- **תיעוד ותכנון לתפעול הפתרונות שעוצבו**

תיעוד של פתרונות מורכבים באמצעות מסמכים מפורטים, ליווי של תכנון לביצוע ואבני דרך ליישום באמצעות מסמכים מלווים והכנת הנחיות ומדריכים לפתרונות המערבים את ציבור המשתמשים.

- **תפעול, תחזוקה ובקרת האבטחה בשוטף**

הכנת מדיניות ונהלי אבטחה המותאמים לשינויים שבוצעו, והכנת תוכנית ליישום בקרה שוטפת ותהליכים לאיתור ותגובה של אירועים חריגים.

ביצוע השיפורים במערכי האבטחה של מערכות מחשב מרכזיות על ידי גורמים לא מיומנים, או כאלה שהכרותם עם סביבות העבודה הנ"ל הנה מועטה, יש בה כדי לפגום במארג האבטחה הסופי ולגרום להווצרותם של פרצות וחשיפות במערך זה הנובעים מפער הידע ומהעדר מודעות נכונה.