

סייבר טרור וסקרי סיכונים - על קצה המדלג

כפיר אלפנדרי, מנהל תחום תקשורת נתונים ואבטחת מידע ב-Dell ישראל

בטיפול באיום מסוים. בשלב "הטיפול" מכינים תוכנית מסודרת לכל איום. מטעם הדברים לא נוכל להתגונן מפני 100% מהאיומים, אולם נוכל לסנן את המוץ מהתבן ולהתגונן מפני האיומים אשר לאחר המיפוי וההערכה שביצענו מהווים את פוטנציאל הנזק הגדול ביותר לצד הסתברות סבירה למימוש האיום.

שלב הטיפול אינו פשוט. על פי רוב, לכל טיפול באיום פוטנציאלי ישנו תג מחיר הכולל את עלות מערכת האבטחה, הדרכה, הכשרה והתרגול לאורך שנים. תג המחיר של מערכות אבטחה ותשתיות אבטחה יכול בקלות להוות סעיף מרכזי בתקציב הארגון ומכאן גם חשיבות ההוצאה הכספית בשיקולים למימוש מלא או חלקי של מערכת ההגנה.

אחת השיטות המאפיינות אנשי כספים הינה רכישת ביטוח עבור סיכון מסוים, בדרך כלל כאשר ההסתברות לסיכון היא קטנה מאוד לצד פוטנציאל נזק עצום. דוגמה לשימוש בביטוח על מנת להעביר את הסיכון לחברה המבטחת יכולה להיות "רעידת אדמה", פוטנציאל נזק עצום לצד הסתברות נמוכה. אולם רכישת ביטוח לא תסייע מפני העברת הסיכון בגין פריצה או ביצע התקפת סייבר טרור למתקן קריטי, היות וקשה מאוד לכמת ולשער את פוטנציאל הנזק העקיף אשר יגרם מחדירה למתקן בסדר גודל זה. (כפיר - זה לא עומד בסתירה לתהליך שתיארת קודם?)

האמת נמצאת באמצע בין העברת סיכון, לבין התמודדות עם קשת האיומים על הארגון. מיפוי כלל האיומים בשיטה שהודגמה מראה את כלל המפה, ומהווה בסיס לתהליך קבלת החלטות ניהולית על דרכי ההתמודדות.

הכותב הינו **אלפנדרי כפיר** (CISSP, CRISC, CISM, PMP), בעל תואר ראשון בבילוגיה ומדעי המחשב, ותאר שני במנהל עסקים. אשר מנהל את תחום תקשורת הנתונים ואבטחת המידע בחברת DELL ישראל.



אלפנדרי כפיר

הקדמה הטכנולוגית
הביאה תלות
וחיבוריות מלאה
עם מערכות מחשב
ותקשורת נתונים,
לסביבות הקריטיות
ביותר במדינה לדוגמה
רשת מסחר בורסאית,
רשתות תחבורה,
ורשתות בקרה נוספות
אשר אמונות על
מתקנים קריטיים כגון
הולכת חשמל, גז מים
ותחנות שאיבה.

מאז ומתמיד הייתה אבטחת המידע בארגון נושא חם. פריצות מתוחכמות שהתבססו על ניצול חולשות אבטחה, או פשעים ממוחשבים שהניבו לפורץ "כבוד רב" התחלפו בהתקפות מורכבות הרבה יותר ומתוחכמות ברמה חסרת תקדים, המבוצעות על ידי גופים בסדר גודל עצום ליצירת "סייבר טרור". התקפות אלה מכוונות בדרך כלל נגד תשתיות קריטיות ברמה המדינית ומהוות סיכון של ממש בהשבתה או פגיעה באורך החיים לא פחות ממתקפת טילים "קונבנציונאלית".

הקדמה הטכנולוגית הביאה תלות וחיבוריות מלאה עם מערכות מחשב ותקשורת נתונים, לסביבות הקריטיות ביותר במדינה לדוגמה רשת מסחר בורסאית, רשתות תחבורה, ורשתות בקרה נוספות אשר אמונות על מתקנים קריטיים כגון הולכת חשמל, גז מים ותחנות שאיבה.

מערכים קריטיים אלה למרבה ההפתעה לא היו מוגנים בעבר ברמה הגבוהה ביותר או באמצעות המוצרים הטכנולוגיים המתקדמים ביותר. מדובר על פי רוב, על רשתות ישנות אשר אופן בנייתם לא כלל שימת לב מיוחדת לאבטחת המתקן בכל רמה שהיא. הדגש היה על עבודה אופרטיבית ותקינה בלבד. ברבות השנים מתקנים אלה אשר אפיינו בעיקר את שוק הבקרה (ולא את שוק ה-IT "הטכנולוגי") הפכו להיות הרשתות הקריטיות ביותר אשר מהוות תשתית לאומית למדינה ויעד מועדף להתקפות סייבר.

בשל הפער הרב בין חשיבות המתקן לחיים היום יומיים של אזרחי המדינה ובשל הסיכון הגלום בתצורת אבטחת (או אי אבטחת) מתקנים מעין אלה, יש לבצע בדיקה מחדש של כלל הפתרון בכל שכבות התקשורת והאבטחה. בדיקה כזאת נחוצה על מנת לנסות ולמזער את הסיכון הפוטנציאלי מקשת האיומים מצד אחד, ומצד שני להכין מראש את התרחישים שנועדו להתמודד עם מקרה של ניצול חולשה או זליגת מידע קריטי.

תקצר היריעה במאמר קצר להסביר את תהליך ניהול הסיכונים הכולל גודל וגבולות הגזרה של כלל הסיכונים. אולם נוכל בהחלט להבין כיצד מתבצע תהליך מעין זה. ראשית, מתבצע מיפוי כולל של כלל הסיכונים היכולים להוות איום על מתקן קריטי שכזה, האיומים לאו דווקא נופלים בקטגוריית "אבטחת המידע", אלא מדובר על ניהול ורישום מדויק של "כלל הסיכונים המאיימים על מתקן קריטי", לאחר מכן מתבצעת הערכת נזק פוטנציאלית לכל סיכון מידה והאיום יתממש, ולבסוף הערכת הסיכוי למימוש איום מסוג זה.

בשלב הרישום לדוגמה, ניתן בהחלט להניח כי רשת בקרת תחבורה הינה מערכת אשר התקפת סייבר עליה עלולה להסב נזק גדול מאוד לשגרת החיים היום יומית. בשל העובדה כי ישראל נחשבת למדינה הסובלת מהתקפות סייבר טרור ישנו סיכוי סביר שתשתית מסוג זה עוברת דרך קבע ניסיונות חדירה על בסיס יום יומי. מצידו השני של המטבע, נפילת מטאור על מרכז הבקרה הראשי הינו בעל פוטנציאל נזק לא פחות גדול, אולם הסבירות לכך נמוכה משמעותית. בשלב זה יש צורך לשלב כמה שיותר בעלי תפקידים מתוך הארגון לצורך הכנת הרשימה.

לאחר הכנת הרשימה, ניתן לדרג את הסיכונים על ידי הערכת פוטנציאל הנזק לצד ההסתברות למימוש האיום. בדרך כלל ישנו סולם מספרי אשר נותן ערך מספרי לפוטנציאל הנזק, וערך מספרי להסתברות המימוש, הכפלה של ערכים אלה תיתן ערך אשר לכאורה הינו חסר משמעות מבחינה מספרית, אולם מהווה סולם מספרי לתיעדוף (Prioritization)

