

סייבר טרור - המפציץ החמקן החדש

הללו אינה מציאותית. כמובן שניתן להגיע לרמות הגנה ובקרה טובות מאלו הקיימות כיום מבלי לפגוע בנגישות למערכות אלה, אולם גם אמצעים כאמור לא יבטיחו הגנה טוטאלית מפני מתקפות סייבר-טרור.

אם נרד לרגע לרמת המיקרו, אין ספק שמוצרי אבטחת מידע, כמו אנטי-וירוס, פיירוול, anti malware וכו' עושים עבודה טובה בלחוסם איומים סייבר-טרור מוכרים, ואף מתעדכנים במהירות בנוגע לאיומים חדשים שכבר היכו בזירות אחרות. אולם למוצרים אלה אין את היכולת לחזות מתי ואיך תתרחש ההתקפה הבאה. לחלק מסוגי המתקפות אין פתרון מדף שיאפשר למנמ"ר לישון בלילה בשקט.

בנוסף, כל ארגון פועל בסביבה עסקית שונה, ועל כן מתאר האיומים העומדים בפתחה של חברה אחת אינו דומה לאתגרי אבטחת המידע של חברה אחרת. כך למשל, ארגון כגון תחנת כוח או מתקן התפלה עשוי להיות תחת איום טרור בהיותו חלק מהתשתית הלאומית של מדינת ישראל; האחר, למשל בנק או חברת ביטוח, כפוף לרגולציה שמחייבת התנהלות לפי דרישות קפדניות; והשלישי, ספק מזון למשל, חושש מגניבת מידע וריגול תעשייתי.

כדי למנוע מתקפה אפשרית על מערכות המידע יש צורך בשירותיו של גוף המתמחה במגוון רחב של דיסציפלינות אבטחה. חברות אבטחה מסוג זה יגיעו בעיקר מהעולם האפליקטיבי, עם ניסיון בפיתוח תוכנה והבנה אמיתית בכל רמות ה-ICT שבארגון - מהרמה האפליקטיבית דרך מערכות האחסון, התקשורת והסיסטם. לגוף אבטחת מידע מתמחה מסוג זה יש את היכולת לאפיין את חליפת האבטחה הנכונה ללקוח, תוך שילוב מוצרים, שירותי-ענן, שירותי PS, צוותי יועצים ומומחים במספר דיסציפלינות. כל זאת, במטרה לתת מענה הוליסטי בכל הרמות ללקוח. ספק אבטחת מידע שכזה יקח אחריות כוללת למספר רב של מערכות ושירותים, ויחד עם קבלני משנה מתמחים, ימנף את הידע הרב שברשותו ולטובת מתן ערך מוסף וייחודי ללקוחות.

ובחזרה לרמת המאקרו: לטעמי, אין מקום שהממשלה תיטול את האחריות לאבטחת תמנון המערכות הפרטיות, הממשלתיות, הצבאיות והחברתיות בתוך רשת האינטרנט ורשתות הסלולר. על המגזר הפרטי והאזרחים להבין שאחריות לאבטחת נכסינו הווירטואליים כגון זהות, מידע, כסף, מוניטין, פרטיות, קניין רוחני ועוד, חלה עלינו ועל אותם גופים עסקיים אתם אנו באים במגע.

איש מאתנו לא היה רוצה לותר על החופש ונחות הגישה למידע ושירותים שהמערכות הללו מעניקות לנו. אולם בעשור הנוכחי נהיה חייבים להפנים את האחריות שיש לנו כמשתמשים וכארגונים לשמור ולהגן על נכסינו הווירטואליים במערכות אלו. כפי שהובהר, אין די בטכנולוגיות לבדן כאמצעי הגנה. מודעות גבוהה לאיומים העומדים בפתח, יחד עם איפיון נכון של האיומים תהווה בסיס איתן למערך אבטחת מידע אפקטיבית כנגד סייבר טרור.

המלחמות הינן חלק בלתי נפרד מההיסטוריה האנושית. מאז ומתמיד נלחמו בני האדם על משאבי טבע, כסף, נכסים, מידע, כוח פוליטי, שליטה בצירי מסחר ועוד. סיבות אלו שרירות גם כיום, אלא ששדה הקרב כיום הפך לרחב ומאתגר הרבה יותר. עם ההתפתחות הטכנולוגית המהירה במאה ה-21, חל גידול מדאיג גם בהיקף האיומים והסכנות. למעשה, אל אמצעי הלחימה והטרור הקלאסיים שהתבססו על חניתות, קליעים וחומרי נפץ, התווסף "מפציץ חמקן" - הסייבר-טרור.



רוני קהת, מנהל תחום סייבר - טלדור תקשורת

הסייבר טרור מסוכן לא פחות מכלי נשק קלאסי. הוא ממנף את הכפר הגלובלי שהאינטרנט והטלפון הסלולרי יצרו, כדי לפגוע במערכות מחשוב קריטיות ולשבש עד כדי סכנת חיים את חיי האזרח התמים במדינה מודרנית. כיום יכול כל האקר בגיל העשרה לשלוח "טילי שיוט" מצד אחד של העולם לעבר מערכות מחשוב בבנקים, חברות תקשורת, תשתיות קריטיות ועוד, ולהביא לקריסתם. הסייבר טרור מנוצל גם לריגול ולאיסוף מידע אשר יכול להיות שימושי מאד גם בשדה הקרב הקלאסי.

נראה שהמורכבות ההולכת וגדלה של מערכות מידע, היא עקב האכילס שלהן. עם התקדמות הטכנולוגיה הוקמו בשנים האחרונות מערכות מתקדמות להעברת כספים, מידע וסחורות וכן פותחו אמצעים טכנולוגיים המאפשרים שליטה טובה יותר על הסביבה שבה אנו חיים. המערכות הללו, הכוללות אפליקציות, תקשורת, ואמצעי שליטה ובקרה, הפכו ליעד למתקפות סייבר-טרור העשויות לשבש מהותית את שגרת חיינו.

- את סוגי המערכות הטכנולוגיות הללו ניתן לחלק לקטגוריות הבאות:
1. מערכות שבאחריות הרשויות והמדינה כגון מערכת בקרת התנועה והרמזורים, מערכות בקרת חשמל ומים, מערכות סעד, מערכות התרעה לאומיות, מערכות צבאיות ועוד.
 2. מערכות שברשות ארגונים פרטיים, כגון מערכות פיננסים וביטוח, מערכות לפיתוח והפצת תרופות, מערכות סחר ועוד.
 3. מערכות חברתיות כגון רשתות חברתיות, דואר אלקטרוני, בלוגים ועוד.

את המערכות האלו ניתן לדמות למספר תמונים המקושרים אחד לשני במספר זרועות: האזרח מתחבר ממערכת פרטית למערכת ממשלתית, המערכת הממשלתית מתחברת ומקבלת מידע ממערכות של ארגונים פרטיים, המערכות הצבאיות מקבלות מידע ומודיעין ממערכות שאף הן מקושרות למערכות פרטיות וכן הלאה. המערכות מזינות האחת את השנייה והרשת ממשכה לגדול ולהסתעף.

מכיוון שקיימת תנועה מתמדת של מידע, כספים ונתונים בין המערכות, הגבולות בין המערכות השונות הולכים ומטשטשים. ב"שטחים האפורים" שבין המערכות מתמקמים שודדי הדרכים של הרשת ומציבים מארבים למידע ולמשתמשים, מתוך מטרת פוליטיות (טרור), מניעים פיננסים (הונאה וגנבה של כסף וסחורות), ריגול צבאי או מסחרי או מסיבות אידאולוגיות (אקטיביזם חברתי).

מכיוון שמדובר ברשתות פתוחות המחברות אחד לשנייה קשה מאוד לבקר ולאבטח סביבה כה מורכבת ודינמית המשתנה ללא הפסקה. הציפייה שרשות ממשלתית כזו או אחרת, תקים מנגנונים שיגנו על כלל המערכות

