אבטחת מידע 2012: עוברים לאבטחת ידע פרואקטיבית רב שכבתית

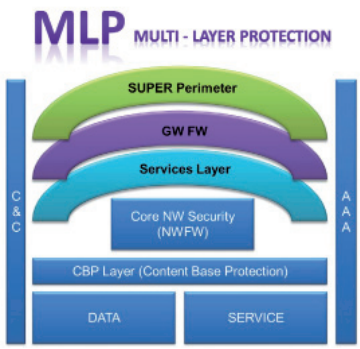
מאת: אורן ברט*

אורן ברט

בחודשים האחרונים נדמה שאנו שומעים כל העת על מתקפות סייבר, גניבות מידע וזהות, ופגיעה עיסקית ותפעולית בארגונים. התקפות תכופות אלו מעלות את השאלה האם הקידמה הטכנולוגית, היכולת הבלתי מוגבלת כמעט לנייד מידע ולהפיץ שירותים, והצורך לשתף משאבי ידע אינן למעשה גורם ישיר לפגיעה ברמת ביטחון המידע של כולנו והאם לא יווצר מצב שבו הגולם (הטכנולוגיה) יקום על יוצרו (האדם) בשל איבוד תחושת הביטחון בניהול חיינו מול הבנקים, אתרי הקניות, ספקיות שירותי האינטרנט שלנו ועוד.

האתגר האמיתי שעמד מאז ומתמיד בפני מנהלי מערכות המידע והממונים על הביטחון היה ועודנו ההגנה הארגונית על משאבי המידע ונכסי הידע. אך כיום נדרשת למעשה התייחסות חדשה ושונה לטווח האיום ולאמצעי ההגנה, היוצרת התאמה בין רמת האיום ולחשיבות הנכס עליו שומרים.

על בסיס אתגרים אלו פותח במטריקס קונספט אבטחתי מתקדם העונה על האתגרים של שנת 2012. מדובר בקונספט אבטחה רב שכבתי MLP- Multi Layer Protection הנותן מענה לשדרוג מערכות האבטחה מסורתיות והתאמתם לאיום המודרני.



ההגנה הרב שכבתית מקנה לארגון את היכולת להתמודד ישירות עם שמירה על הנכסים האירגוניים בדמות הידע והשירות, תוך מתן פתרונות טכנולוגיים נאותים לכל אחת משכבות ההתנהלות והתפעול במערכות השונות.

על פי התפישה הרב שכבתית, רכיבי ההגנה נפרסים על גבי מודל בן 7 שכבות הגנה כך שלמעשה נוצר מיתאם בין שכבת התקשורת, רמת האיום הנובע ממנה ואמצעי ההגנה הרלוונטי. ומצד שני מתאפשרת ההגנה הייעודית מותאמת לנכס המוגן, סוג התעבורה והאיום עליו.

למעשה נוצרו שלוש שכבות מידע חדשות בתפיסה הרב שכבתית:

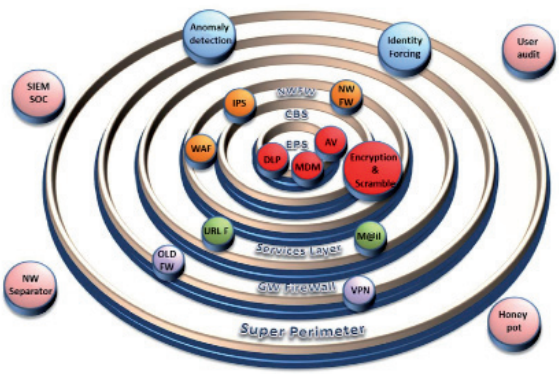
SUPER perimeter - הצורך בהפצת ידע ושירות גרם למעשה לכך שגבול הרשת (Perimeter) נמצא למעשה בכל מקום בו משתמש פוגש באפליקציה. מערך ההגנה נדרש אפוא לאפשר הגנה מול מתקפות לא מאופיינות (עדיין) על ידי משתמשים לא מוכרים מתוך רשתות ומערכות הפעלה לא ידועות. לצורך כך יש ליישם מערכי הזדהות קשיחה ורב ממדית, לצד איתור פעילויות לא שכיחות (Anomaly behavior) המצביעות בדרך כלל על איסוף מידע לקראת תקיפה (PreAttack Protection)

CBS - Content Base Security - שכבה זו מכילה כלי אבטחה ייעודיים המותאמים בצורה מיטבית לתכנים ולנכסים עליהן היא מופקדת כך שלמעשה יותאמו כלי האבטחה לסוגי התוכן כמו כלי הצפנה וערבול, כלי הפצת תוכן מאובטח וכד'.

Services layer - בעידן הידע והמידע נראה כי ה-DMZ (האזור המפורז ברשת) איבד את היכולת להוות שכבת חציצה ראויה שכן: אחידות הפתרון מייצר מפת דרכים כללית, המאפשרת לתוקף ידע קדומני ובנוסף - אין "חצי מאובטח". בנוסף, כידוע רוב האיום על המידע (כ-75% על פי מחקרים) נובע מתוך הרשת ונוצר על ידי המשתמש המורשה. למעשה אין בתשתית האבטחה המסורתית מענה נאות לאיום שכזה (רוב האבטחה מתרכזת בשער המידע האירגוני ומגינה מול העולם החיצון). כמענה לכך מכילה שכבה זו את כלל הכלים הנדרשים לצורך הפצת (PUBLISHING) מידע כמו: שרתי דואר קדמיים, שרתי פרוקסי ומסנני תוכן. בתצורה זו מתבצעת הסתרה מלאה של השירות החשוף והדרך ממנו לרשת הלגאסי, וכן מתאפשר להשוות את רמת ההגנה על התוכן מפני משתמשים חיצוניים ופנימיים כאשר הדרך אל התוכן עוברת תמיד דרך מערך קדומני "חשוף".

שימוש באמצעי אבטחה קיימים

שכבות ופתרונות אלו מתבססים כמובן על התשתית הקיימת ועושים שימוש באמצעי האבטחה הקיימים בארגון לצד הוספה של כלים ייעודיים ספציפיים. המענה לאתגר ההגנה בארגונים השונים בין אם אלו ארגוני הייטק, טלקום, גופי ביטחון ותעשייה, גופים ציבוריים וגופי שירותים, מתבסס אם כן על שימור התשתית הקיימת והוספת הרכיבים הנדרשים, זאת לאחר מיפוי הנכס האירגוני ומערך איתור הסיכונים. בצורה זו ניתן לשמר את רמת האבטחה בארגון מחד ומאידך אף למנף אץ רמת השירות הקישור והאמינות של הארגון אל מול קהל לקוחותיו.



באיור 2 ניתן לראות את מגוון הטכנולוגיות הקיימות ומיצובם בשכבות ההגנה עלפי תפישת MLP. טכנולוגיות בשכבות

*** הכותב הוא מנהל תחום אבטחת מידע בחטיבת מוצרי התוכנה של מטריקס. מטריקס מחזיקה בידע וביכולת ההטמעה וההתאמה של מערכות האבטחה לתפישת ההגנה האירגונית כולה ומייצגת את הטובים והמובילים שבייצרני הפתרונות כמו Gigamon, MaaS360, CRYPTZONE, SiteBlackBox, TrustWare, GED-I, Brillix, ועוד.**

matrix