Digital Whisper
Technologic Papers

תפיסות אבטחה במציאות משתנה

נכתב ע"י יובל סיני

הקדמה

החל משנת 2001 החלו להתגלות בעולם המחשוב סוגי התקפות מסוג חדש, אשר חלקן סווגו באופן מוטעה כתקיפות וירוסים. הסיבה הרווחות להכרה בסוגי התקיפות הנ"ל כתקיפות וירוסים נעוצה בעובדה כי לכלי התקיפה ישנם מאפיינים של וירוסים, אך לא בכך מסתיים הדבר. כלי התקיפה החדשים חשפו יכולות חדשות הכוללות ביצוע Sniffing ברמה גבוהה, גישה ל-Kernel Level המחייבת הבנה גבוהה של ארכיטקטורת מערכת ההפעלה המתוקפת, והכרה מאפייני השימוש של הסביבה המותקפת. קרי, מדובר בהתקפות אשר הותאמו באופן ייעודי לסביבה המותקפת.

עם זאת, מרבית סביבת ה-IT לא נחשפה באופן פומבי לסוג התקיפות הנ"ל, למרות שכבר בשנת 2004 החלו להצטבר תלונות במשטרת ישראל על ניסיונות ריגול תעשייתי מצד ארגונים שונים.

שנת 2010, היוותה שנה מכוננת, ובשנה זו נחשפה תוכנת ה"סטוקסנט", אשר שילבה יכולות Rootkit מובנים. לאחרונה התגלתה תוכנת Flame, אשר חלק מהמבנה הלוגי שלה שיקף את היכולות של תוכנת ה-"סטוקסנט", דבר המציג בפנינו כי דור חדש של תוכנות תקיפה נחשף.

במאמר, נושא הדיון לא נועד לעסוק בצורה פרטנית בסוגיית תוכנות התקיפה הנ"ל, וזאת מכיוון שרבים וטובים כתבו ויכתבו על תוכנות התקיפה הנ"ל. קל וחומר כי המידע הרשמי הקיים ברשות הציבור הינו מוגבל, מסווג בחלקו ונוטה לדעתי לדיסאינפורמציה במידה מסוימת.

לפיכך, השאלה שמאמר זה בא להעלות לדיון: האם תפיסות האבטחה הקיימות כיום עונות לצרכי הביטחון של הארגונים השונים, או שמא, תפיסות האבטחה מחייבות בחינה ובנייה מחדש.

תפיסות אבטחה מסורתיות

את מנגנוני האבטחה המסורתיים ניתן לחלק למספר תתי מנגנון עיקריים:

1. מידור
2. כלי אבטחה
3. כוח אדם
4. תקינה, חוקים ונהלים

מידור

המידור נעשה על סמך סיווג מוקדם של מידע, מסמכים ושירותים, וזאת באמצעות יצירת פרופיל תוכן. לאחר יצירת פרופיל התוכן, מוגדר פרופיל גישה, אשר קובע איך, מי, מתי, ומה מותר לו לבצע בעת הגישה למידע/מסמכים/שירותים. כחלק מהליך הגישה מקובל לשלב הליך Audit פרטני, אשר מאפשר לעקוב אחר ביצוע גישה ושינויים.

כלי אבטחה

תחת כלי האבטחה ניתן למנות רכיבים אבטחת מידע נפוצים, כדוגמת Firewall, Antivirus, IDS/IPS, WAF (Web Application Firewall), DF (Database Firewall), Proxy, DLP (Data Leakage Prevention) ועוד.

ראוי לציין כי קיימים כיום בשוק מגוון רב של ויצרנים פתרונות, כאשר מרבית היצרנים טוענים כי הם אלו אשר נותנים את הפתרון הראוי ביותר ללקוחותיהם.

כוח אדם

כוח האדם אשר מוקצה לתחום אבטחת מידע כולל את מנהל אבטחת המידע (CISO), וצוות אבטחת המידע. עם זאת, בארגונים רבים מקובל להגדיר כי צוות אבטחת המידע הינו צוות התקשורת ו\או הסיסטם. מטרת צוות אבטחת המידע הינה לתפעל את תשתית אבטחת המידע. בנוסף, מנהל אבטחת המידע (CISO) אשר אמור לשבת מחוץ לגוף מערכות המידע (וזאת על מנת למנוע ניגוד אינטרסים), מוכפף פעמים לגוף מערכות המידע, למרות שהוא זה אשר אמור להנחות ולבקר את פעילות גוף מערכות המידע בארגון. בנוסף, בארגונים ציבוריים רבים מקובל כי "ועדת היגוי" מנחה את פעילות אבטחת המידע.

תקינה, חוקים ונהלים

השימוש בתקינה נועד לייצר Framework תשתיתי אשר יאפשר את יישום אבטחת המידע בארגון באופן מיטבי. תחת התקינה ניתן למנות את תקן FISMA, ISO 27001 ועוד.

החוקים (ותקנות העזר) נועדו לקבע מדיניות אבטחת מידע ראויה, כפי שהמדינה רואה אותה. תחת קטגוריה זו ניתן לראות את פעילותה של הרשות למשפט, טכנולוגיה ומידע (רמו"ט) בישראל, וכן חוקים נוספים כדוגמת חוק המחשבים, התשנ"ה - 1995, חוק הגנת הפרטיות, התשמ"א - 1981 ועוד.

הנהלים בתחום אבטחת מידע אשר משמשים את הארגון לצורת הטמעה בפועל של תפיסת אבטחת המידע, אמורים להיגזר מ"מדיניות אבטחת מידע" של הארגון.

תפיסות אבטחה במציאות משתנה

ניתן לפתח דיון פילוסופי ארוך בסוגיה, אך במבחן המציאות - תפיסות האבטחה המסורתיות אינן מספקות את המענה, וזאת מכיוון שהלכה למעשה נזק רב נגרם לארגונים רבים כתוצאות מדור חדש של כלי תקיפה, ואף כיום לא ניתן מענה הולם לגבי מרבית האיומים.

המונח "מציאות משתנה" מהווה למשנתי את המרכיב היסוד, אשר מהווה את עקב אכילס של תחום אבטחת מידע. תחת המושג "מציאות משתנה" ניתן למנות את הצורך להתמודד עם איומים חדשים, אך גם עולה הצורך למנות מרכיבים נוספים אשר לא זכו להתייחסות והכרה בעבר. "גמישות ארגונית" הינה צורך קיומי כיום לארגונים. לא מעט ארגונים מוכנים להקריב את "אבטחת המידע" לטובת הישרדות ו\או הגדלת רווחים. מרכיב נוסף שלא זכה להכרה והתייחסות הינו הפיכת גוף מערכות המידע לגוף שירותים, הנמדד ע"פ יחס עלות\תועלת. בנוסף, מגבלות תקציב מחייבות הערכות שונה, ביחוד לאור העובדה כי הצרכים הארגונים גדלים במקביל, תוך אימוץ טכנולוגיות חדשות, כדוגמת "הענן".

עם זאת, רבים נותן לייחס את האשמה להעדר יכולת להתמודדות עם ה"מציאות המשתנה" לצד הטכנולוגי בלבד. לפיכך מן הראוי לבצע בחינה מחודשת בארבע רמות לפחות:

1. חינוך
2. הצד האנושי
3. הצד המשפטי
4. הצד הטכנולוגי

חינוך

מרכיב החינוך אמור להוות נתבך משמעותי בתפיסת אבטחת המידע של ארגונים פרטיים וציבוריים. חשיבות החינוך נעוצה בכך כי אין יכולת מעשית לסגור את כל חורי "אבטחת המידע" בארגון, וכי התוקפים מנצלים כשלים אנושיים לשם ביצוע התקפות. לפיכך, תפקיד החינוך להעלות את המודעות לקיומם של איומים מצד אחד, ומצד שני לשנות תפוסי עבודה אשר ידועים כבעייתים. עם זאת, ללא עיגון החינוך בהתאם ל"מדיניות אבטחת מידע" נאותה, וללא הדרכת העובדים לגבי ההשלכות הפרקטיות של התנהלות לא נכונה, הסבירות להצלחת הטמעת תפיסות ראויות הינה נמוכה. קל וחומר כי שיטת "ההפחדה" אשר תפסה לה מקום חשוב בעבר, אינה משפיעה כיום על גורמי ההחלטות בארגון. אי לכך, נוכל להסיק כי תחום אבטחת המידע חייב כיום להיכלל ב"תרבות הארגונית", ולא לעמוד כתחום נפרד.

הצד האנושי

לא פעם עולה האמרה כי "המשאב האנושי" הוא המשאב החשוב ביותר בארגון. עם זאת, הנהלות גופים רבים מזניחים את הצד האנושי, למרות שהוא קו ההגנה הראשון של הארגון. בנוסף, הנהלות רבות מנסות להתעלם מן העובדה כי חלק ניכר מהתקיפות מקורן מעובדים ממורמרים ו\או ספקים חיצוניים. לפיכך, נדרש שינוי חשיבתי לגבי תפקיד העובדים בארגון, והתגמול אשר מגיע להם. לדוגמא, מצב שבו עובדים אינם מקבלים את זכויותיהם מחוק, מעלה את הסבירות לקיומה של מתקפה פנים ארגונית. לפיכך, קיומה של "תרבות ארגונית" הוגנת מסייע לארגון בצמצום חשיפתו לאיומים שונים, וזאת ללא השקעת כספים על פתרונות אשר לגביהן אין כל הוכחת הצלחה בפועל.

הצד המשפטי

הריבון אשר מהווה את הסמכות המשפטית במדינה חייב לבחון את החוקים הקיימים, ולהתאימם ל"מציאות המשתנה" תוך שמירה של מסגרת ליברלית בחברה. דוגמא בולטת לכך הינו חוק המחשבים, התשנ"ה-1995 אשר לא עודכן בצורה משמעותית למעלה מ-17 שנה. אף ניסיונות חקיקת חוקי "אח הגדול" אינם יעילים משמעותית, וזאת מכיוון שבשלב זה האכיפה אחר יישום הולם של חוקים אלו אינה קיימת כלל. כלומר, מצד אחד המדינה מנסה ליישום חוקים "דרקוניים", אך מצד שני, החוקים עצמם יכולים לגרום לנזק בלתי הפיך. לפיכך, ישנו צורך במעקב ציבורי הולם לשם קיומה של מערכת איזונים הולמת, אשר תוכל לשמר תפיסת אבטחת מידע הולמת, תוך שמירה של זכויות הפרט. בנוסף, נדרשת הקניית סמכויות אכיפה והרתעה הולמות לגופים ציבוריים כדוגמת הרשות למשפט, טכנולוגיה ומידע (רמו"ט), אשר בשלב זה אינם יכולים לבצע פעולות אכיפה משמעותיות עקב מגבלות משפטיות ופוליטיות שונות.

הצד הטכנולוגי

הצד הטכנולוגי מהווה לדעתי את נקודת הכשל החשובה ביותר, אשר לא זכתה להתייחסות הולמת מתחילת עידן המחשוב. יצרנים רבים מצהירים בריש גליי כי הפתרונות אשר ברשותם הינם הטובים ביותר, תוך הצמדת מסמכים ומחקרים רבים אשר מגבים את טענותיהם.

לפיכך, חלה חובה על הארגון לבדוק את טענות היצרנים, ולא להיצמד ליצרן כזה או אחר. בנוסף, חלה חובה על הארגון להימנע מלהתפזר ליישום טכנולוגיות מיצרנים רבים, דבר המקשה על הליכי ההטמעה והתחזוקה וכדומה. עם זאת, חלה חובה נוספת על הארגון, ולמרות קיומה, היא לא זכתה מעולם להתייחסות.

החובה אותה אני מעלה לדיון הינה הדרישה מספקי פתרונות אבטחת המידע לספק פתרונות איכותיים ואוניברסליים, ולא להסתמך על מצגות היצרן וספקיו. קרי, סביר להניח כי ארגונים רבים אשר יבצעו חשיבה מחודשת בתחום זה יוכלו לאתר כי ברשותם פתרונות אבטחה מידע רבים, אשר אין ביכולתם לספק מענה לשאלה הפשוטה: מי ביצע Logon, לאן הוא ניגש, מתי הוא ניגש, ומהי הפעולה אשר בוצעה. בנוסף, רבים יגלו כי כשלי אבטחת המידע נמצאים בתוך המוצרים עצמם, דבר הכולל את הצורך להשתמש בפתרונות רבים ומסובכים, בכדי להגיע למעטפת אבטחת מידע סבירה בארגון.

סיכום

המאמר כלל סקירה קצרה של תפיסות אבטחה מסורתיות תוך קיום דיון ראשוני בסוגיית הלימת תפיסות אבטחה ל"מציאות המשתנה".

אין מטרת המאמר לספק "פתרון קסם" לבעיות השונות, אלא מטרתו לפתח דיון בשיח הציבורי אשר יאפשר התמודדות נאותה יותר עם איומים חדשים בתקופתנו.

מקורות ביבליוגרפיים

בילורובסקי א. (2007). שימוש בתקשורת אלקטרונית לצורך ניטור (Monitoring) ביחסי "עובד מעביד".

כהן א. (2005). הותר לפרסום: פרשת ריגול במחשבי חברות מהגדולות במשק נשלף ב-2 יוני, 2012 מ:

http://www.ynet.co.il/articles/1,7340,L-3089971,00.html