42553998-5	22/05/2014	הארץ - סייבר	עמוד 13	1	26.09x31.14
טלדור מערכות מחשבים - 3710					

פניו החדשים של האויב הקיברנטי

זירת האיומים בעולם הקיברנטי הנוכחי מחייבת ארגונים להיערך מחדש, מאחר ומוצרי המדף הוותיקים, מבוססי החתימות, אינם מסוגלים להגן עוד מפני מתקפות Zero Day אשר גורמות לנזק מערכתי גדול לארגונים ולממשלות

טירן לוי, מנכ"ל טלדור תקשורת גלאסהאוס

טירן לוי

Taldor
we deliver IT
GLASSHOUSE
INFRASTRUCTURE :: OPTIMIZED

לפני כחודשיים וחצי ערכה יחידת שייטת 13 של צה"ל פשיטה מוצלחת ומתוקשרת על אוניית הנשק האירנית Klos-C. בעקבות הפשיטה, מספר רב של אתרי אינטרנט בישראל הותקפו על-ידי קבוצות אנטי- ישראליות ופרו-פלשתיניות, תחת הכותרת OP-Israel. קמפיין דומה התרחש גם בשנה שעברה ופגע במספר לא מבוטל של אתרים ישראלים, שלא השכילו להיערך לכך בהתאם ולנקוט באמצעים חיוניים להגנת הרשתות ואתרי האינטרנט שלהן.

טכנולוגיות הסוואה

בשנים האחרונות מסתמנת מגמת שינוי במערכה הקיברנטית. פניהם של התוקפים השתנו וכך גם מניעיהם וכלי התקיפה בהם הם עושים שימוש. כעת אנו נמצאים בתחילתה של תקופה חדשה בעולם אבטחת המידע ולוחמת הסייבר. ילדים שתוקפים אתרים ממסדיים לשם השעשוע, אינם מהווים עוד את האיום המרכזי והמשמעותי הקיים לחברות וארגונים שונים. מתקפות אלה גרמו אמנם לנזקים אדירים ולבלבול בקרב קהילות מודיעין רבות, אולם עידן זה תם ונשלם. עם סיומה של תקופה זו הפכו מוצרי אבטחת מידע, שנולדו בסוף שנות ה-80' של המאה הקודמת, ללא רלוונטיים כנגד האתגרים החדשים של לוחמת הסייבר.

התוקפים הפועלים כיום משנים את פניהם באמצעות טכנולוגיות הסוואה ופולימורפיזם. טכנולוגיות העבר, המבוססות על חתימות לצורך איתור וחסימת מתקפות סייבר, לרוב אינן מספיקות על מנת להתמודד לבדן כנגד האיום החדש. הדבר דומה לחייל אמריקאי במלחמת וייטנאם שכל שנדרש ממנו היה לזהות ולפגוע בלוחם וייטקונג לבוש מדים בהירים, סנדלים וכובע קסקט. כבר אז זה עבד בצורה חלקית, ודי ברור שכל ניסיון להשתמש במתודה זו ככלי לזיהוי טרוריסטים ברחבי העולם, נדון לכשלון. במלחמות כיום, הן הצבאיות והן הקיברנטיות, האוייב מזוהה על-פי מודיעין מקדים. לאחר מכן הוא עובר הפללה ובהמשך נעשים ניסיונות לנטרלו.

במילים אחרות, בעולם הקיברנטי ובעולם מתקפות הסייבר ארגונים כיום נדרשים להיערך מחדש, זאת מאחר ומוצרי המדף הוותיקים מבוססי החתימות, אינם מסוגלים להגן עוד, מפני מתקפות Zero Day אשר גורמות לנזק מערכתי גדול לארגונים ולממשלות.

דוגמא לחוסר היכולת של ארגון להתמודד עם מתקפת סייבר של הדור החדש ניתן למצוא באוקטובר האחרון, אז נסגרו מנהרות הכרמל למשך כ-20 דקות ויצרו עומס אדיר ופקקי תנועה ענקיים בכבישי חיפה. מומחים דיווחו ל-AP כי סוס טרויאני הוחדר למערכות הבקרה וגרם לשיבושים קשים שהביאו לסגירת הכבישים. ניתן להניח שמערכות ההגנה הקונבנציונליות הקיימות בארגונים בכלל ובמנהרות הכרמל בפרט, אינן ערוכות לזהות מקורות תקיפה שאינם מוכרים וידועים מראש.

הידע הקיים אינו מספיק

דוגמא נוספת שהובילה בשנה שעברה למעצרם של חמישה אנשים בניו ג'רזי, מקורה בפריצה לארגונים עולמיים כגון נאסד"ק ו-7-Eleven וגניבת פרטים של כ-160 מיליון פרטי כרטיסי אשראי. מדובר במתקפות שנמשכו מספר שנים וכללו שתילת תוכנה מקומית במחשבי אותם ארגונים ואיסוף פרטי אשראי מהרשת הארגונית. בכל אותו זמן, לא איתרו מערכות ההגנה המקומיות את התוכנה שהושתלה וכך נעשתה הפעולה ללא הפרעה משך זמן רב. תוצאות הפריצות הללו נאמדו בנזקים של מאות מיליוני דולרים וכן נזקים אדירים במוניטין ארגוני ובעלויות ביצוע עסקים באמריקה.

בהודעה שפרסמה לאחרונה Gartner בוועידה לניהול סיכוני אבטחת מידע, המליצה חברת המחקר לארגונים להיערך אחרת מבחינת טכנולוגיות ההגנה והידע האנושי שברשותן, על מנת להצליח להתמודד עם הסוג החדש של המתקפות. ב-Gartner הצביעו בעיקר על בעיה בטכנולוגיות הקיימות שאינן מכסות את כלל המתקפות ובעיקר אינן מספיקות על מנת להתמודד עם מתקפות Zero Day. כמו כן, Gartner ציינה בנוסף, כי מרבית הידע הקיים כיום בצוותי אבטחת המידע איננו מספיק על מנת להתמודד עם אירועים מתקדמים בתחום אבטחת המידע.

כל ארגון שמבין, כי עליו להתגונן ממתקפות עכשוויות, ובין היתר ממתקפות Zero Day, מחוייב להסב נתח מההשקעה במוצרים קונבנציונליים להשקעה במוצרים מתקדמים בעלי יכולות המתאימות למתקפות המתקדמות. בנוסף, על כל ארגון להסב שעות עבודה מטיפול שוטף במוצרים קונבנציונליים (הגדרות, תקלות, חוקים ועוד), לטובת תחקור אירועים אנומליים ברשת הפנימית והחיצונית באמצעות המוצרים המתאימים לכך.

ניטור פעילות חריגה

מבחינת סט המוצרים הנכון להתגוננות מפני מתקפות העת החדשה, יש לתת דגש מיוחד על מוצרים הנותנים Visibility (ניראות) על המתרחש ברשת התקשורת. בתחנות הקצה ובשרתי הארגון, יש לבחון הטמעת מוצרים המנטרים פעילות החורגת מהשגרה, הן ברמת תעבורת רשת התקשורת והן ברמת מערכות ההפעלה בתחנות הקצה. לעניין זה, רק למערכות המבינות את המתרחש ברמת מערכת ההפעלה והליבה יש את היכולת לזהות אירועים הקשורים לפעילות של rootkit (רכיב זדוני שהתקין עצמו בליבת מערכת ההפעלה כך שמנועי אנטי-וירוס אינם יכולים לזהות אותו) ואף פעילות של Bot'ים (תוכנות זדוניות שמתקינות עצמן על מחשבים ומאפשרות לשולחיהן שליטה מלאה על המחשב הנדבק) מתוחכמים.

כמו כן, רק מערכות המבינות התנהגות פרוטוקולי תקשורת גלויים ומוצפנים, יזהו אנומליות שימוש שיובילו למתקפה בהסתברות גבוהה.

לבסוף, יש לבנות בצוותים המקומיים את מיומנויות הניתוח וההבנה של אירועי רשת ואירועים על תחנות הקצה לצרכי הסקת מסקנות, הלבנת תהליכים לגיטימיים והתראה ממוקדת בעת זיהוי חריגות, או אירועים בעלי אופי זדוני. ארגוניים שאין ברשותם יכולות כאלה, או צוותים מתאימים לצורך ביצוע משימות אלה, צריכים להסתייע בשירותי PS (Professional services) של מומחי אבטחת מידע חיצוניים ברמה רבעונית לפחות.

הכותב הוא מנכ"ל טלדור תקשורת גלאסהאוס
לפרטים נוספים ניתן לפנות לטלדור תקשורת גלאסהאוס 03-9298944
cyber-info@taldor.co.il

להסב 20% מתקציב אבטחת המידע לטכנולוגיות חדשניות

לאור כל האיומים שתוארו לעיל נשאלת השאלה, אם כן, מהם המשאבים הכספיים הנדרשים להגנה מיטבית מפניהם וכיצד יכולים ארגונים במציאות פיננסית לא פשוטה לגייס אותם? התשובה לכך פשוטה למדי - על הארגון להסב לפחות 10%-20% מתקציב אבטחת המידע לכיוון טכנולוגיות חדשניות, וביתרת התקציב למקסם את יכולות הטכנולוגיות הקיימות וכן את היכולות המקצועיות של האמונים על טכנולוגיות אלה.

בתקופה זו, כאשר ארגונים נמצאים תחת מגבלות תקציביות בשל התנאים הכלכליים המאתגרים בעולם, חשוב מאד לזכור שהמלחמה הקיברנטית הולכת ומתעצמת וכל קיצוץ בטכנולוגיות ובכלים עדכניים לאבטחת מידע יכול להיות הרה אסון ולהביא לקריסת הארגון ועסקיו. לאור זאת, מומלץ לכל ארגון לעשות בדק בית ולהקדיש את הנחוץ על מנת שלא לאפשר, בין היתר, לקבוצות קיצוניות להופכו לבשר התותחים של מדינת ישראל ועל גבו להתהולל בהצלחת הפגיעה ביישות הציונית, ולא פחות חשוב - להגן על הארגון עצמו מפני מתקפה אפשרית.