

# שכבת ההגנה שחסרה בארגונים

"כדי להתגונן, ארגונים חייבים לדעת האם עומדים לתקוף אותם או לא, ומהן התקיפות המבוצעות כרגע. דרוש להם מודיעין קיברנטי", אמר בועז דולב, Clear Sky ומנהל ממשל זמין לשעבר, במפגש פורום CISO ♦ גיא מזרחי, מנכ"ל סייבריה: "אותי מעניין מה מחפש מישהו שרוצה לתקוף מחוץ לארגון. לשם כך יש לייצר מודיעין איכותי ורלבנטי" ♦ ד"ר טל פבל, מומחה לאיומים מקוונים במזרח התיכון ומנכ"ל Middleeastern, דיבר על ההאקרים באזורנו

## יוסי הטוני

שלו מוכרת שירות חדש: מודיעין פרו-אקטיבי. "זו תופעה שהולכת ומתרחבת והיא תהיה על סדר היום ב-2013, קבע. סייבר, מרחב קיברנטי, אמר מזרחי, "הופיע לראשונה בספרות המדעית, ויש לו אינסוף הגדרות. כיום סייבר זה שישה מיליארד מכשירים מחוברים. יש מגוון איומים רחב בעולם הסייבר. אותי מעניין מה מחפש מישהו שרוצה לתקוף מחוץ לארגון. לשם כך יש להיטמע במרחב הסייבר, לאסוף מידע על חולשות אבטחה חדשות ודרכי התמודדות ולייצר מודיעין איכותי ורלבנטי, שמשלים את תמונת האיומים על ארגון מבחוח".

ד"ר טל פבל, מומחה לאיומים מקוונים במזרח התיכון ומנכ"ל Middleeastern, דיבר במפגש על ההאקרים באזורנו. לדבריו, מדובר על קבוצות שונות של האקרים, שפועלות במדינות שונות ואשר פרצו למוסדות וחברות ישראליות. "פריצות הן



ד"ר טל פבל

דבר שבשגרה. זה עניין של יום-יום. מדי יום נפרצים בארץ 15 עד 20 אתרים על ידי האקרים, אלא שהדבר זה לא מגיע לידיעת הציבור כי האתרים אינם משמעותיים".

הוא אמר כי בסוריה יש צבא סורי אלקטרוני, שמטרתו היא להיות מקביל לצבא הפיסי בזירה המקוונת. "לטענתם הם לא חלק רשמי מצבא אסד, ולא ממומנים על ידי הממשלה הסורית", אמר ד"ר פבל. "יש להם נוכחות יפה ברשת החברתית. מחקר שבוצע עליהם העלה, כי בעלי הדומיין הם חברה סורית שאחראית על ה-IT במדינה, מעין 'ממשל זמין'. הדפים שלהם משתנים כל פעם. באתר הם מתעקשים לומר כי הם לא שייכים לאף אחד".

עוד סיפר, כי בעזרת האקרים ערביים, הם מצליחים לשתול ידיעות כוזבות בסוכנויות הידיעות.

ד"ר פבל ציין את האירוע שקרה בתחילת החודש, שבמסגרתו גרמו האקרים סורים להשבתת הדואר האלקטרוני של מערכת עיתון הארץ. "מדובר בפעולת פשינג, שמבוססת על משלוח דואר אלקטרוני שמתחזה להיות מקורי. במקרה הזה, העובדים קיבלו הודעה ש-'נכתבה' כביכול על ידי המו"ל, עמוס שוקן. ההודעה נשאה את הכותרת 'חשוב' והפנתה ללינק למאמר שפורסם, לכאורה, בגרדיאן. מתקפה זו בוצעה בהמשך לפעולה עליה דווח באתר 'הצבא הסורי האלקטרוני' יום קודם לכן, בדבר פריצה והשחתה של כ-40 אתרים ישראליים - אתרים עסקיים ופרטיים בעלי חשיבות נמוכה".

מודיעין קיברנטי הוא הזרוע החסרה לארגונים כיום, על מנת לדעת האם עומדים לתקוף אותם או לא ומה הן התקיפות המבוצעות כרגע", כך אמר בועז דולב, מנכ"ל Clear Sky. דולב, מנהל ממשל זמין לשעבר, אמר את הדברים במפגש פורום CISO מקבוצת אנשים ומחשבים. המפגש נערך במלון שרתון בתל אביב, והנחה אותו אבי וייסמן, מנכ"ל שיא סקיוויטי.



בועז דולב

"ארגונים נדרשים לדעת ארבעה היבטים בהקשר לפריצה", אמר דולב: "מי תוקף את מערך ה-IT שלהם, מתי הייתה או תהיה התקיפה, באמצעות אילו כלים התקיפה מבוצעת ואילו פגיעויות מנוצלות במערכות על מנת

שהפריצה תהא קלה". הוא הסביר, כי "על כל אחד מהמימדים הללו יש לאסוף מידע. כדי לדעת איזה ציוד יש לבנק מסוים, יש לברר מהו בסיס הנתונים שלו. כדי לפרוץ לארגון, יש לברר מה סוג השרת שלו". הוא ציין, כי "יש לבדוק מי מתדפק' על שער הארגון, מי מנסה לפרוץ ועם אילו כלים - מתוך הבנה שככה אדע מי יתקוף".

עוד נדרש, אמר דולב, "לעין בפורומים של האקרים ובמקורות מידע גלויים - דוגמת המדיה החברתית, כדי לאתר דברים הקשורים לחברה מסוימת, שיייתכן שמדברים עליה". שכבת האבטחה המודיעינית, הסביר, "כוללת ייצור של מילון מונחים. יש להבין מה אנשי האבטחה עושים ולשנות המצב כיום, בו מנהל האבטחה בארגון שואל 'מי עשה לי מה?', אך אין לו היכולת להבין ההקשר הרחב יותר".

הוא סיכם באומרו, כי "קבלת שירות מודיעיני שכזה קשה ליישום ברמה פנים ארגונית. רק גוף המתמחה באיסוף מידע ובהבנה וניתוח שלו יכול לעשות זאת בצורה טובה. אנו מספקים שירות זה במשותף עם טרוג'נס".



גאי מזרחי

## מודיעין פרו-אקטיבי

גיא מזרחי, מנכ"ל סייבריה, סיפר כי החברה