

מאומת סטארט-אפ למעצמת סייבר

"ישראל מובילה את הגנת הסייבר בעולם, יש בה 200 חברות בתחום וצריכות לקום נוספות", אמר רמי אפרתי, ראש אגף בכיר במטה הקיברנטי הלאומי ♦ לדבריו, נושא הסייבר היה מוזנח במשך שנים, עד שהוקם המטה, שנועד לשמור על המגזר האזרחי ♦ ארז קריינר, לשעבר ראש רא"ם בשב"כ: "הגנת הסייבר הטובה ביותר היא ההגנה"

יוסי הטוני < צילום: קובי קנטור

הוא ציין כי אחת הדרכים לקדם את תחום הגנת הסייבר היא באמצעות תקנים ורגולציות: "בעולם מתחיל להתפתח התקן להגנת הסייבר 27032, שמבוסס על תקן האבטחה 27001. אנחנו מצויים בתהליכי עבודה מול מכון התקנים הישראלי ובניית תקנים לתחום".

לסיכום, פנה אפרתי לנוכחים באולם ואמר: "עליכם להיות מתריעים בשער מול המנהלים שלכם ולהראות עד כמה איום הסייבר משמעותי לחברה ומה יש להבין בו. נדרש לשתף פעולה על מנת לבחון מה ניתן לאמץ כדי לקדם את הגנת הסייבר ברמה הלאומית".

"ההאקרים אינם אנרכיסטים, אלא אנשי מקצוע"

"בניגוד לדימוי של ההאקר שתוקף בלחימת סייבר כאנרכיסט שקם בצהריים ומעשן ג'וינט, בפועל מדובר באדם שעובד ברצינות, כמו בכל ארגון. על מנת להבין את דרכי פעולתו יש לבחון אותו במשקפיים סוציולוגיים ולא טכנולוגיים. צריך להבין מה המניעים והמשאבים שלו, ומתי הוא מגיע למקסום יכולותיו", כך אמר נתן דולב, אנליסט בסייברארם ולשעבר בכיר בשב"כ.

דולב, שבתפקידו האחרון בשב"כ עסק במודיעין קיברנטי, דיבר בכנס. על מנת להמחיש את פעולת תוקף הסייבר דימה אותו דולב לבעלים של מקדחה שאינה עושה רעש, שהסוללה שלה לא נגמרת, אשר הבעיה שלו היא שהקיר אותו עליו לקדוח על מנת להגיע לאוצר גדול ועובי המקדחה הוא רק מילימטר אחד. לדבריו, "בפני תוקף הסייבר עומדים שני מכשולים: בטכנולוגיה ובנגישות. פתרנו את המכשול הטכנולוגי בעזרת המקדחה ואת בעיית הנגישות - בעזרת העובד. השאלה היא כיצד מתקדמים משם".



נתן דולב

"שם המשחק הוא מודיעין בסייבר", ציין. "מדובר בדבר נגיש. ניתן להשיג מידע רב על אמצעי ההגנה רק ממודיעין גלוי ותוקף בעל סבלנות, זמן וכסף יגיע אליו. כמו כן, קל להשיג מודיעין על מערכות אבטחה - פשוט קונים אותן. זו רק שאלה של כסף. לאחר הקנייה, ההאקר חוקר את מערכת ההגנה כמשתמש וכך מבין איך היא פועלת. התצורה של המערכת בארגון אחד דומה משמעותית לתצורה בארגון שני".

"טכנולוגיות התקיפה של ההאקרים - סקסיות"

דולב עמד על הדימוי שיש להאקרים - כשל אנרכיסטים - ואמר שהוא "פנטסטי אבל לא תואם למציאות. בסופו של דבר, התוקף רוצה להיות מקצועי, מה גם שהוא לא פועל לבד, אלא בתוך מסגרת ארגונית. גם

לא לחינם ישראל כונתה אומת הסטארט-אפים, אלא שעכשיו נדרש להעביר אותה לשלב הבא: לנצל את ההון האנושי שקיים בארץ ולהפוך את ישראל לאומת ההגנה מפני מתקפות סייבר. יש בארץ כבר 200 חברות שעוסקות בתחום", כך אמר רמי אפרתי, ראש אגף בכיר במטה הקיברנטי הלאומי שבמשרד ראש הממשלה.

אפרתי דיבר בכנס של ISACA ישראל, הסניף המקומי של האיגוד העולמי לביקורת ואבטחת מערכות מידע. הכנס, בהפקת אנשים ומשבים, התקיים במרכז הכנסים אווניו, והנחה אותו רמי ניסן, חבר הנהלת ISACA ישראל ויו"ר ועדת הכנס. לדברי אפרתי, "דלויט הנפיקה אמנת שירות בינלאומית בנושא הסייבר ואני 'מת' לאמץ אותה, מאחר שנושא אמנת שירות בסייבר הוא חשוב. אם תהיה בישראל אמנת סייבר לאומית, כזו שלא מעוגנת בחוק, בגולציה או בתקנים - זה יהיה דבר מדהים". הוא ציין כי ב-1 בינואר

יחגוג המטה הקיברנטי הלאומי את יום הולדתו השני. "הוא הוקם לאחר עבודת מטה בת שנה בהשתתפות כ-100 מקצוענים בתחום", אמר אפרתי. "המטה בונה את תפיסת ההגנה הלאומית של ישראל נגד מתקפות סייבר ולאחר מכן מוודא שבונים תשתיות לאומיות על מנת שישראל תהיה מעצמת סייבר. הוא בא למלא את הצורך בהעלאת רמת אבטחת המידע של ישראל ולוודא שהמדינה ערוכה ומוכנה היטב במגזר האזרחי. שנים רבות איש לא דיבר כאן על הגנת סייבר למגזר זה ולפתע, בתהליך ממושך, אנחנו מאוד מתקדמים בכך".

אפרתי אמר שהסניף הישראלי של ISACA הוא "שותף חשוב להכנסה, הטמעה וטיפול בהגנת הסייבר בישראל. מסגרת העבודה CobIT5 היא אחד הדברים החשובים שקרו לקידום התחום. זה לא עוד אמירה כללית, אלא מרכיב מרכזי בתהליך ההגנה".

שיתוף פעולה בסייבר בין חברות

"ישראל מובילה את תעשיית הסייבר ברמה הבינלאומית", הוסיף. "הפיכה שלה לאומת סייבר תיצור הדמנות עסקית חשובה. יש להקים חברות נוספות בעלות שם בתחום הסייבר ולשתף פעולה בין חברות, כי אין אחד שיוודע את הכול".

ככלל, הוסיף אפרתי, "הסייבר כולל תחומי משנה רבים: הגנה מפני סוסים טרויאניים ומתקפות מסוג APT, ניתוח מתקפות, צפי ומודיעין סייבר, אבטחת מידע בעולם המובייל ועוד. הכסף בתחום זה נמצא במדינות שונות ובראשון ארצות הברית, ולשם יש לכוון את הפעילות".