

מסגרת אחודה, שמספקת מענה ארגוני-הגנתי. הכיוון הראשי צריך להיות בראייה אזורית כוללת.

לסיום, ציין ד"ר סיבוני, "הרגל החמישית היא האימונים. יש לייצר מערכת הכשרות, הדרכות והסמכות של גורמים שונים, ליצור שתטיע לקידום התחום ברמת המדינה. מסגרת האימונים תכונן על ידי מי שיוכל את ההגנה האזורית בסייבר".

## "הפריצות עברו תהליך של 'תיעוש' והפכו למתוחכמות יותר"

"מעבר לכמות ההולכת וגדלה של הפריצות, מה שהשתנה הוא הפריצות עצמן. תמיד היו פריצות, אבל חל 'תיעוש' בתחום, אם בשל כניסת ארגוני פשע מאורגן ואם בשל כניסת מדינות", כך אמר **דומיניק סטורי**, מנהל טכנולוגי ראשי ב-SOURCEfire (אירופה), המזרח התיכון ואפריקה. SOURCEfire מופצת בלעדית בישראל על ידי מוביסק. "חלה עליית מדרגה ברמת הפריצות ובמהותן", אמר סטורי. "יש פה בעיה: איך זה שארגונים חכמים דוגמת סוני, גוגל ו-RSA - שהיא בעצמה חברת אבטחת מידע - נפרצו?"

הוא תיאר את התפתחות עולם המתקפות והנוזקות, שכוללת כמה שלבים: וירוסים, מקרו וירוסים, תולעים והאקרים, רוגלות ו-Root Kit. "כיום", לדבריו, "יש נוזקות מורכבות ומתקפות ממוקדות ומתמשכות (APT)". סטורי תיאר גם את שלבי הפעילות של ההאקרים: חקירת סביבת יעד המתקפה, כתיבת הנוזקה, בדיקה שהיא עובדת, משמע - גורמת את הנזק הנדרש מצד ההאקרים, התקפה ושליפת כמה שיותר נתונים, מידע או כסף.



דומיניק סטורי

עוד שינוי שאותו ציין הדובר הוא "המעבר מביצוע המתקפות על ידי בני נוער תאבי תהילה, שרוצים לחבל בשביל החבלה עצמה, למתקפות ופריצות שהמניע שלהן הוא כלכלי והן נעשות על ידי ארגוני פשע מאורגן, מדינות וארגונים תת-מדינתיים. כל הגורמים האלה לא מעוניינים בחשיפה ופועלים אחרת לחלוטין - הם אנשי מקצוע לכל דבר ועניין. יש כיום ארגונים שהם בבחינת 'ארגוני אנטרפרייז' של האקרים, ששמו להם למטרה לחדור לארגונים".

איום נוסף אליו התייחס סטורי מגיע מכיוונו של המשתמשים הארגוניים. "המשתמשים מקליקים על קישורים, שחלקם זדוניים, כי הם רוצים לדעת מה עומד מאחורי כל אחד מהם", אמר. "הם לא עושים את החיבור הנדרש בין פתיחת הלינק להדבקת המחשב בנוזקה. אסור לסמוך על אוכלוסיית המקליקים".

הוא ציטט מחקר שלפיו 90% מהמשתמשים בארגונים חוו ב-2012 מתקפה אחת ומעשרת האחוזים הנותרים, 66% חוו שתי מתקפות או יותר ו-20% - עד עשר מתקפות.

"נדרש לחשוב אחרת על אבטחת מידע", אמר סטורי. "אבטחת מידע זו לא בקרת גישה של המשתמשים אלא הגנה מפני איומים וניהול אבטחת האימונים. יש לפשט את שרשרת האבטחה ולהתעלם מרעשים מסיחי דעת".

## "אנחנו מקווים שהשוק הישראלי ירתח"

SOURCEfire, ציין סטורי, "עוסקת בפיתוח ובמכירת פתרונות לאבטחת רשתות מחשבים ומערכות מידע בזמן אמת. פתרונות החברה כוללים

זילביגר ציין שאחד ההבדלים בין סייבר לאבטחה הוא זהות הגורמים שמולם עובדים אנשי אבטחת המידע. "כשעסקתי באבטחת מידע, דיברתי עם אנשי ה-IT. כעת, בעוסקי בסייבר, אני מדבר הרבה עם אנשי צבא ומודיעין", אמר.

לדבריו, "עולם הסייבר יושב מעל עולם אבטחת המידע ושונה ממנו במורכבות הטכנולוגית, ביצירתיות, בתחכום, בכיסוי המערכת, במוטיבציה וברלוונטיות".

הוא קרא למנהלי האבטחה בארגונים "להיות ערוכים מבפנים ומבחוץ. עליהם לחשוב 'חוק' ולא רק 'פנים'. נדרש מודיעין איכותי: לדעת מה מתכננים שם בחוץ, מה הם יודעים על הארגון, מה מפרסמים ברשתות החברתיות ומה כותבים בצד האפל של הרשת".

## להבין העוצמה של ההתקפה הממוקדת המתמשכת

"יש להבין את העוצמה של ההתקפה הממוקדת המתמשכת (APT)", הוסיף זילביגר. "היא מופעלת לזמן קצר, עלולה להסב נזק רב במאמץ קטן". לדבריו, "יש לצפות את הבלתי צפוי, להבין שמתקפות APT 'תפורות' על הלוקח".

זילביגר ציין ש"על מנהל אבטחת המידע לדעת לעומק וגם לרוחב, לעמוד בדרישות רגולטוריות, לנהל אירועים - והפעם ברצינות, לעבוד בצוות, שמשלב את אנשי האבטחה הפיזית, אבטחת המידע, אנשי ההמשכיות העסקית, ה-IT והמנהלים העסקיים. יש לנהל את הסיכון תוך תעדוף, ולעשות זאת במגבלות זמן ותקציב".

## "אתמול היה טוב ויהיה עוד יותר מחר"

"מבחינת הגנת הסייבר בישראל, אתמול היה טוב ויהיה עוד יותר מחר", כך אמר אל"מ (מיל') ד"ר **גבי סיבוני**, ראש התוכנית הלאומית לסייבר במכון למחקרי ביטחון לאומי, NISS. לדבריו, "אנחנו נמצאים בעיצומו של תהליך ועלינו כל הזמן להשתכלל בתחום. יש לתת מענה על הכול. ישראל נמצאת במצב מיוחד מבחינת סיכונים, היא אטרקטיבית לתקיפות ולכן יש להיערך ברמה הלאומית".

בהרצאתו תיאר ד"ר סיבוני את בניין הכוח בתחום הסייבר במדינה, שלדבריו מושתת על לחמשרגלים. "הרגלה ראשונה היא התורה, האסטרטגיה,



גבי סיבוני

הדוקטרינה", אמר. "יש

לגבש תורה לאומית

להגנת הסייבר האזורי.

במסגרת זו, יש לשלב

בכמה היבטים: למשל,

להחליט מי נדרש להיות

מוגן, מה המדרגיות של

החומרה, איזו תקינה

לקבוע, להחליט מהם

הארגונים שיהיו תחת

המטרייה של ההגנה, אילו

כללים יחולו. יש לקבוע

תורת הגנה אזורית".

"הרגל השנייה היא

פיתוח כוח אדם", הוסיף.

"יש לפתח הון אנושי לתחום הסייבר, להביא להקמת מוסדות אקדמיה, להכשרה בתחום. למדינה יש כלים לעודד תמיכה בתהליכי הכשרה שכאלה".

"רגל הנוספת היא אמצעים ופיתוח טכנולוגיה תומכת", המשיך ד"ר סיבוני. לדבריו, "אף שמדובר בשוק חופשי, על המדינה להכווין פיתוחים בשוק, לאור תורת ההגנה בסייבר".

הוא הוסיף, כי "הרגל הרביעית היא ההיבט הארגוני - איך מסדרים את האנשים העוסקים בתחום ומי אחראי על מה. כאשר מארגנים הגנה אזורית בסייבר צריך להיות איגום של הגופים העוסקים בתחום. נדרשת