

מסגרות אחוריה, שספקת מענה ארגוני-הגנתית. הכוון הראשי צריך להיות בראיה אזרחית כוללת".
לסום, ציין ד"ר סיבוני, "הרגע החמישית היא האימונים. יש ליצור מערכת ה小姑娘ת, הדרכות והסמכות של גורמים שונים, ליצור שתסייע לקידום התהום ברמת המדינה. מסגרת האימונים תכוון על ידי מי שיוביל את הגנה האזרחית בסיביר".

"הפריצות עברו תהליך של 'תיעוש' והפכו למתוחכם יותר"

"מעבר לכמות ההולכת וגדלה של הפריצות, מה שהשתנה הוא הפריצות עצמן. תמייד היו פריצות, אבל חל 'תיעוש' בתחום, אם בשל כניסה ארגוני פשע מאורגן ואם בשל כניסה מדיניות", כך אמר **דומניק סטורי**, מנהל טכנולוגי ראשי-ב-**SOURCEfire** לאזור EMEA (אירופה, המזרח התיכון ואפריקה). SOURCEfire מופצת בישראל על ידי מוביסק. "חלה עלייה מדרגה ברמת הפריצות ובמהותן", אמר סטורי. "יש פה בעיה: אין זה שארוגנים חכמים דוגמת סוני, גугл ו-RSA - שהיא בעצם חברות אבטחה מידע - נפרצו?"
הוא תיאר את התפתחות עולם המתקפות והנזקים, שכוללת כמה שלבים: מירוסים, מקרו וירוסים, תולעים והאקרים, רוגלוות ו-Kit Root. "כitos", לדבריו, "יש נזקים מורכבות ומתקפות ממוקדות ומתחמשנות". סטורי תיאר גם את שלבי הפעולות של האקרים: חקירות סביבת יעד המתתקפה, כתיבת הנזקה, בדיקה שהיא עובדת, משמע - גורמת את הנזק הנדרש מצד ההackers, התקפה ושליפת כמה שיטות נתוניות, מידע או כסף.
עוד שניינו שאוטו ציין הדברו הוא "המעבר מביצוע המתקפות על ידי בני תובי, שורצים לחבל תרילה, בשבייל החבלה עצמה, למתקפות ופריצות שהמניע שהן הוא כלכלי והן נעשות על ידי ארגוני פשע מאורגן, מדיניות וארגוני תח-מדינתיים. כל הגורמים האלה לא מעוניינים בחיפה ופועלים אחרית לחלוון - הם אנשי מקצוע לכל דבר ונניין. יש כיוון ארגונים שהם בבחינת 'ארגון אנטופרייז' של האקרים, שמנו להם לסתור לחדרו לארגונים".

איום נוסף אליו התייחס סטורי מגע מכיוון של המשותפים הארגוניים. "המשותפים מקליקים על קישורים, שחלקים זדוניים, כי הם רוצחים לדעת מה עמוד מחדרו כל אחד מהם", אמר. "הם לא עושים את החיבור הנדרש בין פתיחת הלינק להדבקת המחשב בנזקה. אסור לסגור על אוכלוסיות המקליקים".
הוא ציטט מחקר שלפיו 90% מהמשותפים בארגונים חוו ב-2012-2013 עד עשור מתקפות. "נדרש לחשב אחרת על אבטחת מידע", אמר סטורי. "אבטחת מידע זו לא בקשר גישה של המשותפים אלא הגנה מפני איום וניהול אבטחת האיום. יש לפשט את שרשות האבטחה ולהתעלם מרדעים מסוימים מימי דעת".

" אנחנו מכוונים לשוק הישראלי יזרחה "

ציוויליגר ציין שאחד ההבדלים בין סיביר לאבטחה הוא זהות הגורמים שמולם עובדים אנשי אבטחת המידע. "בשעתקי באבטחת מידע, דיברתי עם אנשי ה-IZ. בcut, בעסקים בסיביר, אני מדבר הרבה עם אנשי צבא ומודיעין", אמר.
לדבריו, "עולם הסיביר יושב מעל עולם אבטחת המידע ושונה ממנו במוכבות הטכנולוגית, ביצירתיות, בתחום, בכיסוי המערכת, במושביצה וברלונטיות".

זה קרא למנהלי האבטחה בארגונים "להיות ערוכים מבעינים ומחוז. עליהם לחשוב 'חוץ' ולא רק 'פנס'. נדרש מודיעין איכון: לדעת מה מתכוונים שם בחוץ, מה הם יודעים על הארגון, מה מפרסמים בדשות החברתיות ומה כותבים בכך האפל של הרשות".

"הבין העוצמה של ההתקפה הממוקדת המתמשכת"

"יש להבין את העוצמה של ההתקפה הממוקדת המתמשכת (APT)," הוסיף זיליגר. "היא מופעלת לזמן קצר, עלולה להסב נזק רב במאםך רק". לדבריו, "יש לצפות את הבלתי צפוי, להבין שמתפקידות APT 'תפורות' על הלוקוח".
זיליגר ציין ש"על מנהל אבטחת המידע לדעת לעומק גם לרוחב, לעומד בדרישות וגולטרויות, לנאל אירופים - והפעם ברכזונות, לעבד בצדדים, שמשלב את אנשי האבטחה הפיזית, אבטחת המידע, אנשי המשכויות העסקית, ה-IZ והמנהלים העסקיים. יש לנאל את הסיכון תוך תדעוו, ולעשות זאת במוגבלות זמן ותקציב".

"אתמול היה טוב ויהיה עוד יותר מחר"

"מבחן הגנת הסיביר בישראל, אתמול היה טוב ויהיה עוד יותר מחר", כך אמר אל"ם (מיל') ד"ר גבי סיבוני, ראש התוכניות הלאומית לSİיבר במכון למחקרי ביטחון לאומי, ISSN. לדבריו, "אנחנו נמצאים בעיצומו של תהליך ועលינו כל הזמן להשתכלל בתהום. יש לתת מענה על הכל, ישראל נמצאת במצב מיוחד במיוחד בתחום סיוכנים, היא אטרקטיבית לתקיפות ולכך, יש להיערך ברמה הלאומית".

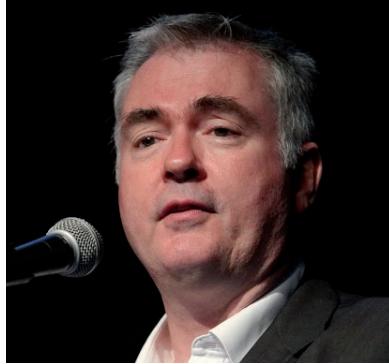
בראצתו תיאר ד"ר סיבוני את בנין הכוח בתחום הסיביר במדינה, שלדריו מושתת על חמשרגלים. "הרגע הראשונה היא התרבות, האסטרטגיה, הדזוקטינה", אמר. "יש

לגבש תורה לאומית להגנת הסיביר האזרחית. במסגרת זו, יש לטפל בכמה היבטים: למשל להחליט מי נדרש להיות מוגן, מה המדרגות של החומרה, איזו תקינה קבוע, להחליט מהם הארגונים שהיו תחת המטריה של ההגנה, אילו כללים יחולו. יש לקבוע תורدة הגנה אזרחית".

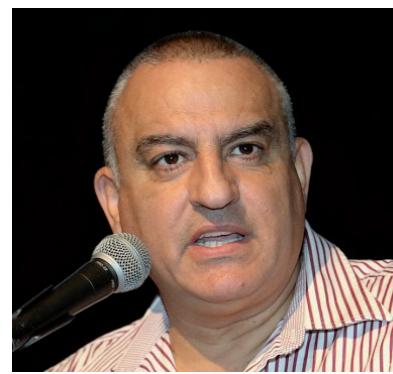
"הרגע השני היא פיתוח כוח אדם", הוסיף. "יש לפתח הון אנושי בתחום הסיביר, להביא להקמת מוסדות אקדמיים, להכשרה בתחום. למדינה יש כלים לעודד תמייה בתהליכי הscrda שכאללה".

"רגע הנוסף היא אמצעים ופיתוח טכנולוגיה תומכת", המשיך ד"ר סיבוני. לדבריו, "אף שמדובר בשוק חופשי, על המדינה להכוון פיתוחים בשוק, לאור תורدة הגנה בסיביר".

הוא הוסיף, כי "הרגע הבלתי הבהיר הוא היבט הארגוני - איך מסדרים את הארגונים העוסקים בתחום ואני אחראי על מה. כאשר מארגנים הגנה אזרחית בסיביר צריך להיות איגום של הגופים העסקיים בתחום. נדרשת



דומניק סטורי



גבי סיבוני