# דו"ח האיומים: החמרה במצב אבטחת המידע; ישראל - "במקום טוב באמצע"

מספר הפריצות, כולל פריצות הענק, וכמות גניבות הזהויות עלו ב-2013 בצורה דרמטית - כך מגלה דו"ח האיומים השנתי של סימנטק * בישראל המצב קצת יותר טוב, עם שיפור קל במספר מתקפות הנוזקות לעומת הרעה בכמות הספאם שנשלח

ישראל נמצאת "במקום טוב באמצע" בדירוג רמת אבטחת המידע באינטרנט של סימנטק, אותו פרסמה במסיבת עיתונאים שערכה בדבלין, בירת אירלנד. לעומת זאת, בכלל העולם המצב מדאיג: ב-2013 חל גידול דרמטי במספר הפריצות, כולל אלה שמוגדרות "פריצות ענק".

על פי ענקית אבטחת המידע, ישראל דורגה במקום ה-43 ברשימת המדינות שסבלו מתקיפות הנוזקות הרבות ביותר - שיפור קל , של 0.3%, לעומת המקום ה-39 ב-2012 (ככל שהדירוג נמוך יותר הוא נחשב טוב יותר). לעומת זאת, בהיקף הספאם שנשלח לכתובות בארץ חלה הרעה של 0.7% - מהמקום ה-36 למקום ה-28. ישראל הגיעה למקום ה-48 בהיקף אתרי הפישינג - שיפור של 0.2% בהשוואה למקום ה-35. בהיקף רשתות Bot היא דורגה במקום ה-19, המהווה שיפור של 1% לעומת המקום ה-16 ב-2012.

הדו"ח מעלה כי מספר פריצות הענק (Mega breaches) גדל בשנה החולפת מאחת לשמונה והמגמה צפויה להימשך השנה. מספר אירועי הפריצות הכללי זינק ב-62%. עוד עולה מהנתונים כי ב-2013 נגנבו 552 מיליון זהויות ופרטים אישיים של משתמשים ולקוחות לעומת 93 מיליון בשנה שלפני כן. החוקרים כתבו כי "נתון זה מוכיח שפשעים מקוונים מהווים איום אמיתי ומזיק על צרכנים ועסקים כאחד".

הנתונים הראו שהרעים למיניהם - האקרים, פושעים קיברנטיים בשירות ארגוני פשע, האקטיביסטים (שילוב של המילים האקרים ופעילים פוליטיים) והאקרים בשירות מדינות - ביצעו ב-2013 את סדרת הפריצות המזיקה ביותר של תקיפות סייבר בהיסטוריה המקוונת. על פי חוקרי סימנטק, חל שינוי בהתנהגות המקוונת של אותם רעים והם פעלו לביצוע יותר פריצות ענק שנפרשות על פני חודשים מאשר פריצות "קטנות", עם הישגים לטווח קצר מועד. בכל אחת משמונה פריצות הענק לנתונים נגנבו עשרות מיליוני רשומות ופרטים אישיים.

הארגונים שסבלו ביותר מנחת זרועם של אותם רעים מגיעים ממגזרי הבריאות, החינוך והממשלה - 58% מכלל הפריצות. אלא שהרגולציות החמורות הקיימות במגזרים אלה הביאו לכך שרק 1% מהזהויות נגנבו. לעומת זאת, ארגונים מהמגזר הקמעונאי, שהיוו רק 5% מסך הפריצות, תפסו נתח של 30% מכלל גניבות הזהויות, מאחר שהם מאובטחים פחות.

**האיומים גוברים, לפחות לפי סימנטק (צילום: פלי הנמר)**

עוד גילו חוקרי סימנטק, כי כמות המתקפות נגד אתרים צמחה השנה משמעותית השנה - מ-464,100 ל-568,700 בכל יום. מדובר בזינוק של 23% לעומת 2012.

## יותר פריצות ממוקדות ומתקפות יום אפס

מספר מתקפות יום האפס צמח בשנה החולפת ביותר ממחצית ונתון חמור יותר מעלה שמשך מציאת ההטלאה צמח אף הוא ועמד על 19 ימים. אחד מכל שמונה אתרים בעולם מכיל נוזקה שעדיין לא הומצא טלאי לתיקונה.

כמו כן, הדו"ח מעלה כי ההאקרים למיניהם ביצעו השנה 91% יותר מתקפות ממוקדות מאשר ב-2012 והזמן הממוצע של כל מתקפה גדל פי שלושה - משלושה ימים לשמונה ימים. היעדים העיקריים למתקפה היו עוזרים אישיים למנכ"לים, סמנכ"לים ומנהלים בכירים בארגונים, ואנשי יחסי ציבור. הפושעים הקיברנטיים ניצלו אותם כקרש קפיצה להגעה לאישים בעלי פרופיל גבוה, למשל ידוענים או אנשי עסקים בכירים. המגזר שחווה את מספר המתקפות הממוקדות הרב ביותר ב-2013 היה המגזר הממשלתי, שדורג רביעי ב-2012.

נתון נוסף מעלה, שבעוד שהייתה "יציבות" בכמות הארגונים הקטנים והגדולים שהותקפו, הרי כמות ארגוני הביניים שהותקפו עלתה מ-50% ל-61%. סימנטק מגדירה ארגון ביניים ככזה שמעסיק בין 250 ל-2,500 עובדים.

ענקית אבטחת המידע ציינה, כי המתקפה האופיינית אינה מסובכת טכנולוגית ופועלת בשני שלבים: משלוח מייל ובו הודעה הכרוכה בביצוע פעולת תשלום ולאחר מכן "פולו-אפ" של ההאקר, שמזדהה כעוזר המנכ"ל או כאיש הכספים של הארגון וקורא לנמען לבצע את פעולת התשלום במהירות. המייל שנשלח מכיל קישור ללינק שמכיל נוזקה או כולל דרישה למילוי פרטים אישיים, כגון מספר תעודת זהות ומספר ביטוח לאומי (בארצות הברית).

**יוסי הטוני**