17.52x31.51	1	עמוד 27	הארץ - the marker	06/04/2016	52683717-9
חברת White ha - 15079					

הנזק העיקרי מאיומי מתקפת הסייבר על ישראל מחר: פאניקה והוצאות מיותרות

האיומים הקוליניים של קבוצות האקרים שונאי ישראל הסתיימו בשנים האחרונות בנזקים מינוריים ● חברות האבטחה נערכות למתקפה השנתית ב-7 באפריל ומרעננות את הנחיות הביטחון, אך בענף אומרים: "הווירוסים שפוגעים בישראל בכל יום גרועים פי כמה"

אליחי וידל

במדי שנה בשלוש שנים האחרונות, מחר, 7 באפריל, יציינו ההאקרים שונאי ישראל את יום הזעם שלהם נגד המדינה. המבצע, שזכה לשם Opisrael, אמור לבלול תקיפות סייבר נרחבות ומתוזמנות נגד ישראל. ביום זה מבטיחים האקרים מקבוצת אנונימוס לתקוף כל מחשב ישראלי אפשרי, אתרים פרטיים, חשבונות מייל, שרתים ארגוניים וגופים פיננסיים וממלכתיים.

למרות האיומים וההפחדות, "השלל" שהצליחו ההאקרים לרשום לזכותם בשנים האחרונות לא היה רב, ואפילו די עלוב. בשנה שעברה למשל, נרשמו ניסיונות תקיפה של אתרי רשויות, ספקיות שירותי אינטרנט, גופי חינוך ואקדמיה, גופים משפטיים ופיננסיים. כפי שמצד התוקפים מדובר ביום חג, כך זוהי שעתן היפה של חברות אבטחת הסייבר, שמעמידות את שירותיהן הטובים לרשות הנפגעים ומפעילות חמ"לים לסיוע, כמו לקראת מבצע צבאי.

מבדיקה שערכו בחברת White-Hat עולה כי ב-2015 נחשפו למתקפה כמה מאות כתובות מייל ממשלתיות, עשרות כרטיסי אשראי שפרטי בעליהן נחשפו, כמה אלפי כתובות אי־מייל, מגורים ומספרי טלפון, עשרות רבות של מיילים וסמאות מוצפנות של המכון הישראלי ליצוא ושיתוף פעולה בינלאומי, השירות המטאורולוגי ובנק ישראל, וכן עשרות פרופילים בפייסבוק של עסקים ואנשים פרטיים שהכילו סיסמה.

האקר של אנונימוס. שעתן היפה של חברות הסייבר צילום: אי־אף־פי

בחברת האבטחה Secoz ציינו לקראת האירוע כי גם באירועים קטנים ומציקים, שכביכול נראה שאינם גורמים לנזק גדול, יכולים להתחבא אירועים מורכבים יותר שייכנסו לפעולה בעיתוי אחר לגמרי. מסיבה זו, לדבריהם, כדאי לוודא שכל התוכנות מעודכנות, שהורדו טלאי אבטחה מעודכנים, שתוכנות ההגנה פועלות באופן תקין וכלל, שהעובדים מכירים את כללי הבסיס ואינם פותחים קבצים או לינקים שנשלחו ממקורות בלתי מזוהים, שלא מעבירים סמאות בטפסים ייעודיים.

בחברת MadSec מיפו לקראת האירוע את הקבוצות העיקריות שמתכננות את התקיפה. בין היתר ניתן למצוא בהן את AnonGhost – קבוצה של האקרים המזהים את עצמם כתומכי דאע"ש ומתמחים בהשחתת דפי הבית של אתרים רבים. לרוב, מטרות הקבוצה הן אמריקאיות וישראליות, וביוני 2015 הם רשמו לעצמם הישג עם השחתת עמוד הבית של אתר הבית הלבן. ארגון נוסף בשם Fallaga Team הוא קבוצה של האקרים תוניסאיים התוקפת אתרים תוניסאיים, צרפתיים וישראליים. לפי MadSec, זו קבוצה דתית המתנגדת לכל גילוי חילוניות ואתאיזם במדינות האיסלאם, אך אינה קשורה לדאע"ש.

החידוש: תקיפת רשתות ביתיות

גם בחמ"ל של רדוור מצאו זווית חדשה לקראת המתקפה של השנה: פריצה לראוטרים (נתבים) ביתיים ולהשתלטות על רשתות Wi-Fi ביתיות. מתקפה כזאת מאפשרת השתלטות על הנתב הביתי שדרכו נגנבים מידע ונתונים אישיים העוברים ברשת הביתית, או ביצוע השתלטות נוחה יותר על ציוד הקצה המחובר אליו – כמו מחשבים, טלפונים חכמים, טאבלטים, טלוויזיות חכמות, מצלמות ומדפסות.

עם זאת, לדעת מנכ"ל אקספריס סייבר, אלי כהן, הפגיעה האמתית באיומי ההתקפה של אנונימוס היא דווקא בהיערכות אליה ובפאניקה שהיא יוצרת בקרב הארגונים. חברות משקיעות הון תועפות בהגנה מפני ההתקפה, שתוצאותיה ברוב המקרים מזעריות – ובכך מצליחים לפגוע ולשבש שלא במידה את המשק הישראלי.

"אירועי סייבר קורים כל הזמן", אומר כהן. "רק בשבועות האחרונים משתוללים וירוסים של כופרות, שפוגעות בעשרות אלפי מחשבים בישראל בכל יום. הנזק שנוצר בווירוסים הללו הוא פי כמה מהנזק שייווצר לארגונים ולאנשים פרטיים ב-7 באפריל".

לדבריו, סביר להניח שחלק מהארגונים הקטנים שאינם יכולים להרשות לעצמם רכישת מוצרי אבטחה מתקדמים, יתעוררו עם אתר אינטרנט עם כתובות נאצה, וירוס כופרה או מייל זדוני שנשלח לאנשי הקשר. כשבאמת רוצים לגרום נזק לתשתיות ולמדינה עושים זאת מתחת לרדאר, ולא מפרסמים זאת חודש לפני ביוטיוב".

המודעות לאיומי הסייבר היא ההגנה הטובה ביותר

אף שהנזקים שהצליחו ההאקרים להסב לאינטרנט הישראלי בשנים הקודמות היו מזעריים עד כדי בלתי מורגשים, האיומים ב-7 באפריל הם זמן מצוין לרענן הנחיות הביטחון ברשת – מעין יום מודעות ארצי, בחסות אנונימוס.

כך תמזערו את הסיכון בגופים פרטיים ובארגונים

1. ודאו בכל התחנות והשרתים בארגון כי גרסת האנטי וירוס מעודכנת לזאת החדשה ביותר.
2. נקו חוקי פורוורד של המיילים.
3. אל תפתחו מיילים שהגיעו משולח לא מוכר.
4. הימנעו משימוש במיילים אישיים במחשבי הארגון.
5. אל תתקינו בדפדפן תוכנות או תוספים בלתי מאושרים.
6. דווחו על כל אירוע או חשד לאירוע אבטחת מידע.

כך תגנו על הנתב הביתי

1. שנו את הסיסמה בנתב, או הוסיפו סיסמה אם הנתב פתוח לאינטרנט.
2. מינעו כניסה לנתב דרך האינטרנט.
3. התקינו עדכוני אבטחת מידע שהפיצה יצרנית הראוטר, כדי לחסום את הראוטר מפני השתלטות מרחוק.
4. אם הנתב שייך לחברת תקשורת או ספקית אינטרנט, בצעו את ההתאמות הנדרשות באמצעות שירות התמיכה.