כמה עולה לחסל מנמ"ר?

מאת יהודה קונפורטס On 26 בפברואר 2017 @ 16:08 In אבטחת מידע וסייבר,בראש הכותרות,חדשות | No Comments

שרון נימירובסקי, מנכ"ל White Hat. צילום: פלי הנמר

"ב-2016, היקף פשיעת הסייבר העולמית המדווחת היה יותר מחצי מיליארד דולר, וכנראה שמדובר בסכומים הרבה יותר גבוהים", כך אמר **שרון נימירובסקי**, מנכ"ל חברת אבטחת הסייבר הישראלית **White Hat**. לדבריו, "סכום זה לא כולל את אלה שלא דיווחו על הפגיעה או שלא שילמו את הכופר, ולא מייצג את הנזק שנגרם למוניטין של הארגונים שנפגעו".

נימירובסקי דיבר במליאת היום השני של כנס המנמ"רים והמנכ"לים שערך באחרונה ביוהנסבורג פורום C3 מבית **אנשים ומחשבים**. מנחה הכנס היה **פלי הנמר**, יזם ומנהיג אנשים ומחשבים, והוא כלל שני ימי דיונים, שהשני ביניהם נערך בקמפוס המפואר של **Dimension Data**. המשתתפים הגיעו לשם כאורחי **MedOne** הישראלית, שמפיצה בארץ את מוצריה של החברה הדרום אפריקנית. בנוסף, נערכו במהלכו ארבעה פאנלים בהנחיית **רונן זרצקי**, יו"ר הפורום, שעסקו ברגולציה, התפוצצות מידע, רשתות חברתיות וסייבר וענן.

בדבריו ציין נימירובסקי כי "בשנה החולפת התחילו מסות של מתקפות כופר על מחשבים. התוקפים הצפינו מידעים וביקשו כופר עבור שחרורם. רק באחרונה הצטרפו סוגים חדשים של מתקפות כופר, בדמות ההתקפה על בית המלון באוסטריה, שבה ההאקרים נעלו את כל חדריו ודרשו כופר עבור שחרור האורחים".

"כדי לתקוף צריך לדעת רק לגלוש באינטרנט"

"בשנה הקרובה צפויות מתקפות כופר מגוונות שונות, כגון השתלטות על מוצרי אינטרנט של הדברים", הוסיף. "עקרונית, כל מי שמחובר לרשת הוא מטרה למתקפת כופר. בעבר הרחוק, לפני שלוש שנים, כדי לבצע תקיפות סייבר כאלה היה צריך במוח מיוחד, היה צורך בהאקרים עם IQ מאוד גבוה, ששקדו, למדו ופיתחו את יכולתם".

"כיום", ציין נימירובסקי, "כדי לתקוף בסייבר לא צריך לדעת כלום חוץ מלגלוש באינטרנט. מספיק שתיכנסו **לגוגל** (Google) ותקלידו את שלוש המילים הפשוטות: Download crime pack, ויש בידיכם ערכה מושלמת, שמאפשרת לכם לתקוף אחרים מבלי לדעת בכלל איך היא עושה את זה".

הוא דיבר גם על עולם הדארקנט וציין כי "כמות התכנים בו הוכפלה באופן אקספוננציאלי וניתן כיום לקנות שם את כל מה שנדרש לתקיפת סייבר כשירות (CaaS)". בהמשך הוא המחיש עד כמה קל לפרוץ לכל אתר, בעלות זולה מאוד: "אם תרצו לפרוץ ל**פייסבוק** (Facebook) או ל-Gmail, תצטרכו לשלם 150 דולר, מתקפת DDoS של 20 דקות תעלה לכם 1,200 דולר וחיסול של מנמ"ר – 12 אלף דולר".

"מנהלי הארגונים תקועים בכל הנוגע לסייבר"

נימירובסקי ייסד את White Hat לפני שלוש שנים והחברה מעסיקה כיום 34 איש, רובם לוחמי סייבר שעיקר עיסוקם הוא להגן על תאגידים מפני מתקפות אפשריות על מערכות המידע שלהם. בנוסף, עוסקת החברה בהפצת מידע רב לכלל האזרחים, כחלק מתרומה לקהילה, על מנת לשפר את רמת האבטחה.

מרבית הפעילות של White Hat היא מאחורי הקלעים ומתחת לרדאר, מטעמי סודיות מתבקשים. לטענת נמירובסקי, החברה עובדת עם מרבית הארגונים הגדולים במשק, כולל בנקים ומוסדות ממשלה, אזרחיים וביטחוניים.

לסיכום אמר נימירובסקי ש-"ה-IT הוא לב ליבו של הארגון והוא חשוף כל הזמן למתקפות סייבר. מרבית הארגונים תקועים: הם מנסים להילחם בסייבר בשיטות קונבנציונליות של אבטחת מידע, וזה לא תמיד נכון. אנחנו משרטטים עבור הארגון את מפת האיומים ונוכחים לדעת שמרבית מנהלי האבטחה לא מודעים לנושא".
