כובע לבן ואביר לבן נלחמים בהתקפות סייבר

תקשורת פשיעת סייבר נגד טרור ביטחון מודיעין עוד... ישראל גאו פוליטיקה חדשות טכנולוגיה טכנולוגיות חדשות אבטחת סייבר סייבר
תוכנה רשתות

Jun 14, 2018

This post is also available in: English (אנגלית)

איומי הסייבר על חברות, ארגונים ותשתיות ישראליים מתרבים מיום ליום. רשות הסייבר הלאומית מנסה לרכז את המאמץ נגד האיום הזה ולצורך כך היא משתמשת בקבלני משנה, חברות סייבר שעל כל אחת מהן הוטלה המשימה להגן על מגזר קריטי מסוים.

אחת מהחברות האלה היא White Hat. מנכ"ל החברה, שרון נימירובסקי, אומר כי האקרים מעדיפים לחדור למפעלי תעשייה באמצעות ספקי רכיבים ונותני שירות כמו רואי-חשבון ועורכי-דין.

החברה מתל-אביב הקימה יחידת מודיעין עלית המספקת אבטחת סייבר לארגונים פרטיים – ובעתיד גם למדינות. "יש לנו מרכז מודיעני שמנטר איומים מכל הסוגים ובכל הרמות. אנחנו פועלים בנושא הזה כמו יחידת עילית צבאית למניעת פיגועי סייבר", אומר המנכ"ל בראיון ל -i-HLS.

לדבריו, כיום האקרים יכולים גרום נזקים ברכוש ובנפש כמו צבאות, שעושים שימוש בכל נשק מסוגים שונים. "האקרים מסוגלים כיום לגרום לתקלות במפעלים כימיים המאחסנים כמויות גדולות של חומרים מסוכנים ובצורה כזו להביא לאסונות בקנה מידה נרחב".

ישראל, אומר נימירובסקי מאוימת לא מעט בגלל המצב באזורנו והכוחות שלוקחים חלק בעימות. לדבריו, האיומים גוברים משבוע לשבוע ובכל פעם מומחי החברה נתקלים בסוגים חדשים של איומים. "האויב הבלתי-נראה הזה מתוחכם ופעל בדרכים מגוונות כדי לגרום נזק".

לדבריו, רשות הגנת הסייבר שהקימה הממשלה נעזרת כיום בחברות פרטיות כדי לגלות איומים מתפתחים ולמנוע אותם. "עלינו הטילו את הטיפול במגזר מסוים. אני כמובן לא יכול לחשוף מהו, אבל מדובר במגזר שיש בו פוטנציאל גדול לנזקים".

מנכ"ל החברה אומר כי לעתים מתגלה איום מתפתח אבל הבעיה היא שלא ברור כלל מתי האיום יצא לפועל והיכן. "אנחנו פועלים בעולם בו הרבה דברים אינם ברורים מייד, לכן צריך להפעיל מערך מודיעין שיצמצם את סימני השאלה, שבמקרה הזה יכולים להיות קריטיים".

לדבריו, אנשיו מגלים איומים שכבר מצויים למעשה ב"חצר" של הלקוח המאוים. "באמצעות חדר המלחמה שאנו מפעילים בתחום המודיעין אנחנו מסוגלים לתת ללקוח התראה שמישהו עומד לתקוף אותו דרך פרצה מסוימת".

כל זה נעשה, לדברי נמירובסקי, על ידי מערכת שלמה של סימולציות התקפה, שבאות לחשוף את נקודות התורפה של הלקוח בכל אחת מהמערכות המקוונות שלו.

"אנחנו לא מחכים שמשהו יקרה כדי להפיק לקחים. אנחנו מנסים להקדים תרופה למכה, והמכות בתחום הזה יכולות להיות כואבות מאוד ועם נזקים אדירים"

חברת White Hat מפעילה כיום מערך חיפוש איומים המכונה "אביר לבן". מערך זה פעיל בתחום הרשתות החברתיות למיניהן, ומאתר תחילה איום אפילו בשלב התכנון. "הבעיה היא שיש המון מידע ולכן המערכת שלנו היא מערכת ביג דאטה מתוחכמת, שיודעת לחשוף את המידע הרלבנטי".

לצורך השיטוט הזה בעולם הרשתות החברתיות, מפעילה החברה "מודיעין אנושי" שהוא למעשה שימוש באמצעים טכנולוגיים שמתחזים למודיעין המבוסס על אדם.

"כל עובד שלנו מפעיל סוכנים מעין אנושיים כאלה, המשוטטים ברחבי הרשת ומנסים לאתר סימנים מקדימים לפעילות סייבר עוינת".

הוא מסביר כי אחת השיטות המקובלות כיום אצל האקרים היא לתקוף דרך ספקי משנה של חברות. "המידע הרגיש ביותר מצוי אצל הספקים ודרכם ניתן להגיע לצמתים הקריטיים."

לדברי מנכ"ל החברה, "אם תצא לפועל תקיפה ממומנת על ידי מדינה, ברוב המקרים לא יהיה ניתן לזהות אותה. רמת המשאבים שיושקעו בה היא כל כך גדולה, שיהיו משאבים רבים מאוד שיוקדשו להסתרתה".

להרשמה לניוזלטר.