"מאז תולעת הסטוקסנט – כל רכיב בעולם חשוף למתקפת סייברה"

מאת אבי בליזובסקי
רביעי, 11 יוני 2014 00:29

פרופ' יצחק בן ישראל

במסגרת מושב המועצה הלאומית למחקר ופיתוח של משרד המדע בכנס הרצליה בנושא חדשנות ישראלית בסייבר, אמר היום (שני) יו"ר סוכנות החלל הישראלית האלוף (מיל.) פרופ' יצחק בן ישראל: "מאז אירוע הסטוקסנט בצנטריפוגות בכור הגרעיני באיראן ישנן שלוש אמיתות שצריך להיפתר מהם ומהר: ראשית, שאיומים בסייבר הם רק איום למידע – סטוקסנט פגעה במכונות פיסיות וצנטריפוגות בכור גרעיני. שנית, מחשבים זה לא רק על השולחן במשרד ובבית זה גם סלולרי, רמזורים, הפסקת חשמל ועוד. היום כמעט כל מכשיר חשוף. בנוסף, הצינור לתקיפה אינו מוגבל לאינטרנט בלבד – מתקן הפיקוח על הצנטריפוגות באירן כלל לא היה מחובר לרשת, לא פנימית ובטח לא לרשת האינטרנט העולמית ובכל זאת הותקף. זה אפשרי החל מהחומרה שנרכשה וכלה בעדכון תכנה או בהחדרת וירוס באמצעות דיסק און קי."

ראש מו"פ המנהל פיתוח אמל"ח במפא"ת תא"ל איתן אשל, אמר כי ככל שגבולות החיים והמרחב הקיברנטי הולכים ומטשטשים אנו פגיעים יותר להתקפות. "אנו מחברים עצמנו לדעת ועומדים בפתחם של חיים במציאות רבודה: שימוש במטבע הוירטואלי ביטקוין, שימוש במדפסות תלת מימד לייצור אובייקטים והתלות בדאטה שחלק גדול ממנו נמצא על ענן הופך את חיינו למרחב לחימת סייבר". אשל הדגיש כי כלי התקיפה הם חינמיים ברשת ואין צורך במשאבים גדולים כדי לבצע תקיפה.
ד"ר טל שטיינהרץ, CTO, טכנולוג ראשי במטה הסייבר הקבירנטי הלאומי במשרד רוה"מ סיפר על פיתוח באוניברסיטת בן גוריון בו מנסים לפתח פיוז מכני שיאפשר למכונה לזהות שהיא מותקפת. לדבריו: "הגנה לאומית בסייבר מייצרת למדינה מנוע צמחיה כלכלי. מדובר בשוק המוערך בכ-60 מילארד דולרים ובסוף הכל נבנה על האנשים". שטיינהרץ הוסיף כי ישראל מעצמה בתחום ושווי השוק שלה בתחום שווה לכל העולם כולו יחד להוציא את ארה"ב.

אסתי פשין, ראש מנהל מערכות סייבר בתעשייה האווירית הסבירה מדוע ההאקר יכול לנצח: "בסייבר קל לייצר זהויות בדויות. הקמנו זהות בדויה בפייסבוק ותוך 48 שעות היו לה 150 חברים. הזמינו אותה למסיבות. רכלו עליה. התלוננו עליה. שנית, מדובר באטה עצום במיוחד ובנוסף, רוב התעבורה מוצפנת והחברות הללו מבכרות את פרטיות המשתמשים על פני ביטחון של מדינות. הרעים מנצחים. הרבה יותר קל לתקוף מלהגן. אכן אנחנו רואים שכמות ההתקפות רק עולה."

"המפתח להתמודדות הוא חדשנות, לקחת טכנולוגיות בנות 60 שנה ולהסב אותן לעולם הסייבר. צריך לייצר שיתופי פעולה עם סטארטאפים. אנחנו רואים עצמנו כמבוגר אחראי שצריך לסייע ליזמים צעירים. אנחנו צריכים האקרים טובים כדי ללמוד להתגונן ולכן אנחנו חייבים להקים עוד מרכזי מו"פ במסגרתם יתפתחו האקרים טובים. "

{loadposition content-related}

מאת אבי בליזובסקי
רביעי, 11 יוני 2014 00:29