# להפוך מאומת סטארט-אפ לאומת סייבר

## ח"כ מאיר שטרית: "העולם אינו ער דיו לסייבר ולבעיות שהוא יוצר" ♦ "האיום הגרוע מכל הוא האקר שמשתלט על מערכות לאומיות קריטיות וסוחט מדינה", אמר ח"כ שטרית, לשעבר יו"ר ועדת המדע והטכנולוגיה של הכנסת וכיום מועמד לנשיאות, בוועידת InfoSec של אנשים ומחשבים ♦ כרמי גילון: "רק גישה פרואקטיבית תמנע התמודדות בלתי פוסקת מול האיומים המשתנים"

יוסי הטוני, יהודה קונפורטס, צבי קצבורג ואבי בליזובסקי > צילום: קובי וניב קנטור

"ישראל, יותר ממדינות רבות בעולם, מצויה תחת מגוון רחב של איומים קיברנטיים. האיום הגרוע מכל הוא של קבוצת האקרים שמשתלטת על מערכות IT של תשתיות לאומיות קריטיות וסוחטת את המדינה", כך אמר ח"כ **מאיר שטרית**, יו"ר סיעת התנועה. לדבריו, "העולם אינו ער דיו לסייבר ולבעיות שהוא יוצר: כיום אפשר למוטט מדינה באמצעים קיברנטיים בלבד".

ח"כ שטרית, לשעבר שר הפנים ויו"ר ועדת המדע והטכנולוגיה, וכיום מועמד לנשיאות המדינה, היה אורח הכבוד בכנס Infosec 2014 של אנשים ומחשבים, שנערך במרכז הכנסים אווניו שבקריית שדה התעופה. לכנס הגיעו מאות מקצועני אבטחת מידע, והנחה אותו פלי הנמר, יזם ומנהיג אנשים ומחשבים.

לדברי ח"כ שטרית, "כל עולם ה-IT מתמקד באבטחת מידע וסייבר - ובצדק: זה התחום המדאיג ביותר את המדינות בעולם. אין ספק שלתופעת המיחשוב ההולכת וגדלה יש יתרונות גדולים בכל היבט שהוא", ציין. "אולם לצד היתרונות יש לאינטרנט גם צד אפל, בעל חסרונות. שדה הקרב המודרני עבר שינוי: על מנת לכבוש מדינה לא צריך מטוסים, ספינות קרב וחיל שריון, ואפילו לא חייל אחד. כל מה שצריך זה מחשב ומקלדת. המתקפות במימד הסייבר הופכות להיות דבר שכיח, שקורה על בסיס יומיומי, והן הולכות ומתפתחות עם הזמן, בצורה שגוברת פלאים".

ח"כ מאיר שיטרית

### להשתלט על מדינה

"אחת המטרות של ההאקרים היא לתפוס שליטה על מדינה, משום שכך הם יכולים לדרוש ממנה כל דבר", הוסיף ח"כ שטרית. "אם האקר משתלט על אתרי תשתית של מדינה, הוא יכול למוטט מערכות שלמות שלה. אם האקר יוכל לחדור ולהשתלט על מערכות תחבורה ורמזורים, ולהפעיל אותן כך שכל הזמן יהיה רמזור ירוק, הוא יגרום לאלפי תאונות ולאנדרלמוסיה שלמה".

"ואולם מערכות התחבורה הן רק טיפה בים", אמר, "יש חשש להשבתת משאבות מים, לחבלה בתחנות כוח ואנרגיה, ואפילו בתחנות כוח גרעיניות. ניתן לגרום לכל מערכת שנשלטת על ידי מחשבים נזקים חמורים, גם אם המערכת עצמה אינה ממוחשבת".

הוא ציין לחיוב את החלטת הממשלה להקים מטה קיברנטי לאומי, שכפוף ישירות לראש הממשלה. "הרבה גופים עוסקים בנושא הסייבר הלאומי, זרועות ביטחון שונות, ודרוש גוף שישים את הדברים תחת קורת גג אחת". הוא ציין גם את רא"ם (הרשות הלאומית לאבטחת מידע) שבשב"כ, ש"מטרתו היא להתמודד מול איומי הסייבר העיקריים על ישראל, להגן על התשתיות הלאומיות והמיחשוב הממשלתי".

ח"כ שטרית נתן כדוגמה את התולעת סטוקסנט, שפגעה במערכות הבקרה של הצנטריפוגות באחד ממתקני הגרעין של איראן והביאה להרס של יותר מ-1,000 מהן. "סטוקסנט היא דוגמה קלאסית ליכולת לפעול בעולם הסייבר. אין בצנטריפוגות שנפגעו שום מחשב, אלא הן מבוקרות על ידי המערכת שלה נגרם הנזק. נזק גדול, לשמחתנו". לדבריו, "המקרה הזה מלמד שנדרש ליצור מערכת הגנה, שפועלת לאורך זמן ובעקביות. בחלוף הזמן הסתבר שסטוקסנט היא תולעת מאוד מתוחכמת, שיודעת לפגוע רק ביעד שאליו היא מכוונת. התולעת עשתה עבודה מתוחכמת ויצרה תחושה שדבר אינו מוגן".

עוד אירועי סייבר שציין השר לשעבר הם 13 המתקפות על נאס"א, שבהן היא הודתה, שגרמו לה לאובדן חלק מהקודים לשליטה בחלליות שלה, והפריצה ללוקהיד מרטין, שבמסגרתה נגנבו מהתאגיד הביטחוני מסמכים של מטוס הקרב F-35. "האמריקנים אמרו שזו פעולה של הסינים, שכן נדרשה עבודה בת שנתיים של 400 איש כדי לבצע את המתקפה, ואין גורם כלשהו שאינו מדינה, ושאינו סין, שיכול להפעיל אופרציה שכזו", אמר.

### "צריך אקו-סיסטם שלם"

ח"כ שטרית ציין, כי יש כמה חסמים לטיפול בהגנה בעולם הסייבר, בהם העדר או מיעוט רגולציות, העדר חקיקה בתחום וההתקדמות המהירה מאוד בו. "בעוד שבכלל העולם הטכנולוגי השינויים אורכים שנים, בסייבר, דור חדש של איומים מופיע מדי שנה וחצי", אמר.

"דרוש אקו-סיסטם שלם על מנת לטפל ולהתגונן מפני מתקפות סייבר", לדברי ח"כ שטרית. "יש צורך לבצע פעולות בכמה שדות, ובעיקר בתעשייה, בביטחון ובחינוך, כמו גם שתהיה כוננות ממשלתית באופן כללי. המגזרים השונים צריכים לשלב ידיים לטובת העניין".

"ישראל היא המדינה המותקפת ביותר בעולם, אבל גם אחת משלוש המדינות בעלות רמת ההגנה הגבוהה ביותר בתחום בעולם, לצד פולין ושבדיה. לשמחתי, ישראל נערכת למתקפות סייבר, היא עברה שינוי אקספוננציאלי בהשקעות ובתשומת הלב הנדרשת להגנה על תשתיות ומערכות. סייבר הוא לא רק מחשבים, כל מאגרי המידע הם יעד למתקפה. על ישראל להפוך מאומת סטארט-אפ לאומת סייבר", סיכם ח"כ שטרית.

### גישה פרואקטיבית לאיומים המשתנים

"איומי אבטחת המידע והסייבר משתנים כל הזמן. לכן נדרש לטפל באיומים בגישה פרואקטיבית, על מנת שלא להתמודד כל הזמן עם האיומים המשתנים ולהתאים עצמך אליהם. אם הארגון בא מוכן מראש