

שלדבריו יתפסו את הכותרות בתחום במהלך השנה הקרובה. "האירועים הגדולים התרחשו ב-2010 וב-2011, אבל יש עוד דברים שיתרחשו", אמר. "הפופולריות של ה'האקטיביסטים' תעלה. ההצלחה מזינה את עצמה והגלוריה פיקציה של ההתקפה, כמו גם התוצאות הנובעות ממנה, מייצרות את דורות ה'האקטיביסטים' הבאים. מגמה נוספת היא אבטחת מיחשוב הענן. מדובר בעוד מרחב קיברנטי ואנחנו לא יודעים מה קורה בו. עם זאת, אנחנו רצים ומעלים את כל החומר אליו. אם לקח לתחום כרטיסי האשראי לתקן את תקן ה-PCI שבע שנים, והוא עוד לא מומש לחלוטין, כמה זמן ייקח עד שזה יקרה גם בענן? ומה עם מובייל? כולנו משתמשים ביישומים ולא מפסיקים להוריד, אבל זו הרי עוד פלטפורמה עם מיליוני משתמשים שחשופה לחלוטין. ההגנות שלנו לשם יגיעו, אבל אנחנו עוד ממש לא שם".

### "עצרנו יותר מחצי מיליון התקפות ב-2011"

**מיכל בלושטיק-ברוורמן**, מנכ"לית RSA ישראל, התייחסה בנאומה להונאות הסייבר בתחום הפיננסי. לדבריה, "יש שלוש סוגי חברות מותקפות בעולם: חברות שהותקפו ומדברות על זה, כאלה שהותקפו ולא מספקות מידע וחברות שהותקפו ולא יודעות על כך".



אמנון בר לב

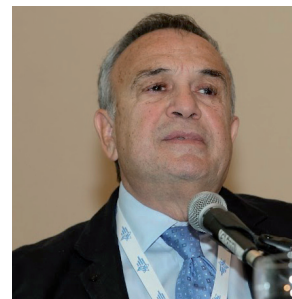


מיכל בלושטיק-ברוורמן

ישראל, להרוויח ולהתקדם הלאה". פרופ' בן ישראל, שהנחה את מושב הסייבר והיה הדובר הראשי בו, ציין שיש לישראל יתרון יחסי בהגנה נגד מתקפות סייבר, מאחר ש"מבחינה תקשורתית היא אי. אמנם יש לנו גבולות יבשתיים ארוכים, אבל לא חודרת מהם תקשורת. כל התקשורת מגיעה דרך שניים שלושה צינורות בים וכמה לוויינים. מכיוון שכך, יש לנו אפשרויות שאין בידי מדינה כמו צרפת או גרמניה. אם יש לנו מחשבים מספיק מהירים וחזקים אנחנו יכולים למנוע מעבר של חלק גדול מההתקפות שמגיעות מחו"ל, וזה יכול לשפר מאוד את הגנת הסייבר הלאומית".

### "מתקפות הסייבר יכולות לפגוע בחיים שלנו"

הוא התייחס גם לגישות שבהן צריך לנקוט כדי להילחם במתקפות סייבר. "לפי הגישה המסורתית, אבטחת מידע בסייבר צריכה להתבצע בשני צירים: האחד הוא דאגה לכך שלא ייכנסו דברים לרשת והשני הוא שברוך כלל, מה שצריך להגן עליו הוא המידע. זה נכון, אבל זה לא מקיף את כל הנזקים", אמר. לדברי פרופ' בן ישראל, "התקפת סייבר יכולה לפגוע בחיים שלנו, כי החיים שלנו כיום נשלטים בידי מחשבים. אני לא מתכוון למחשבים שיש לכל אחד בבית או לרשתות החברתיות, אלא לכך



ניסים בר אל



פרופ' יצחק בן ישראל

היא סיפרה שב-2011 הייתה RSA ישראל אחראית למניעת גניבות בשיעור של יותר משלושה מיליארד דולרים ושמרזז הפיקוד שלה, שעובד מסביב לשעון, עצר יותר מחצי מיליון התקפות. "מדובר בהתקפות שכל הזמן הולכות ונעשות מתוחכמות יותר", אמרה. "שרשרת האספקה בעולם הסייבר בנויה כבר על אנשים מקצועיים ולא על ילדים בני 16. האנשים שמפתחים הם טכנולוגיים. אנחנו מפתחים תוכנה וגם הם מפתחים תוכנה". היא הוסיפה, כי "יש קבוצה אחרת של פושעים, שרוכשת את הכלים האלה ומשתמשת בהם כדי לבצע גניבות. כמוכן שעבור זה צריך שוק ויש הרבה מאוד מקומות באינטרנט בהם מציעים למכירה, רוכשים, מייצעים ומוכרים שירותים. זה מוכיח שיש צורך בהגנה רב שכבתית ובמעקב קבוע".

### אסטרטגיה לאבטחת מידע

הבעיות באבטחת המידע נובעות הן מהממד האנושי והן מהממד הטכנולוגי. **אמנון בר לב**, נשיא צ'ק פוינט, אמר שהממד האנושי לא פחות חשוב מהטכנולוגי. לכן, הוא מציע לנקוט אסטרטגיה שמורכבת מכמה צעדים. "קודם כל, צריך להגדיר מדיניות, ולא משנה אם מדובר במדינה, חברה או אדם בודד. צריך להגדיר מי יכול ומורשה להגיע לאן ולמה, להיצמד לכך ולעשות זאת באופן פשוט וברור", אמר. "בנוסף, יש להסביר את המדיניות, לוודא שמשמשים בטכנולוגיה ושעושים זאת בתהליך העבודה השוטף. גם בצבא וגם בבית פרטי, למשל, צריך לייצר רצף של הגנות שיעבדו ביחד. זה מאוד חשוב, כי ההתקפות כיום מאוד מורכבות". הוא הביא כדוגמה לכך את סטוקסנט. "זו הפעם הראשונה שבה ראיתי שבמקום לשלוח מטוסים כדי להפציץ השתמשו בתולעת

שכל המערכות החיוניות שלנו נשלטות על ידי עשרות מערכות מבוקרות מחשוב. כל מי שיודע לחדור אליהן ולהשתיל את התוכנה הנכונה יכול לגרום נזק לחיים שלנו. לדוגמה, הנזק האמיתי זה לא אם מישוה ייכנס למערכת המחשוב של הרכבת כדי לגנוב מידע, אלא ייכנס למערכת הרובוטית של הרכבות ויגרום להן במקום לא להתנגש אלו באלו כן לעשות זאת ואז הנזק הוא בבני אדם".

למרות כל אלה, אמר פרופ' בן ישראל שהמדינה יחסית ערוכה לאיומי הסייבר מכיוון שהיא עוסקת בזה שנים רבות מאוד. "העניין של הסייבר די עתיק יומין, למעשה. מדינת ישראל ומערכת הביטחון מתעסקים בזה כבר כ-20 שנים", סיפר. "כבר לפני 10 שנים הגיע העניין עד לרמת הממשלה עם התוכנה שנקודת התורפה של המדינה היא בכלל במשק האזרחי, בתשתיות של ייצור חשמל ומים וגם בבורסה, ולא דווקא במערכות הביטחון. כבר לפני 10 שנים הוקמה הרשות לאבטחת מידע בשב"כ שאמורה להגן על מספר תשתיות קריטיות שבלעדיהן לא ניתן לתאר חיים תקינים במדינה".

### "השיא באירועי אבטחת המידע - מאחורינו"

התקפת התולעת סטוקסנט לפני כשנתיים העירה את תחום אבטחת המידע בעולם הסייבר והקפיצה את המודעות והעיסוק בו מאות מונים קדימה. כיום, יש צורך להשתמש בהגנות מרובות שכבות כדי להתמודד עם סכנות הסייבר, החל בקביעת מדיניות ברורה וכלה בשימוש בכלים חדשניים, ואפילו התקפיים. זה היה הקו המאחד של כל הנואמים במושב הסייבר של הכנס.

**ניסים בר-אל**, מנכ"ל יושב ראש קומסק, התייחס לחלק מהמגמות