

לתקיפה לא חייב להיות באינטרנט. יש דרכים רבות להדביק, למשל חומרה, עדכוני תוכנה או דיסק און קי".

"אנחנו נמצאים בעיצומה של המהפכה", סיכם פרופ' בן ישראל. "ככל שנהיה תלויים יותר במחשבים ייווצרו נקודות תורפה רבות יותר בכל שטח בחיים שלנו, כולל יכולת לפגוע במערכות חיוניות".

### "אנו פגיעים יותר כי אנו מחברים עצמנו לדעת"

"ככל שגבולות החיים והמרחב הקיברנטי הולכים ומטשטשים, אנו פגיעים יותר להתקפות, כי אנו מחברים את עצמנו לדעת", כך אמר תת-אלוף **איתן אשל**, ראש מ"פ במפא"ת (המנהל למחקר ופיתוח אמל"ח ותשתית טכנולוגית), משרד הביטחון.



תת-אלוף איתן אשל

"מדי שנה אנו חושפים את עצמנו ליותר מתקפות סייבר. אנו עומדים בפתחם של חיים במציאות רבודה: שימוש במטבע הווירטואלי ביטקוין, שימוש במדפסות תלת מימד כדי לייצר אובייקטים והתלות בדטה, שחלק גדול ממנה נמצא על ענן. כל זה מייצר מצב בו הכל מחובר עם הכל, והסייבר הופך למרחב של לחימה".

"אנו כבר עשרות שנים נמצאים בהגנה, מאז שהמחשב הראשון נכנס לחיינו. פעם זו הייתה אבטחת מידע, היום זו הגנה בסייבר", הוסיף תא"ל אשל, "מרחבי האיום השתנו, למרחק הגיאוגרפי משמעות. התקיפה היא קלה, כי היא נעשית עם כלי תקיפה חינוניים, מה שלא דורש משאבים גדולים על מנת לתקוף. יש א-סימטריה בין המגן לתוקף: כי התוקף עשוי לזהות ביתר קלות את חולשות המגן. פוטנציאל התקיפה גדל: האימונים יכולים לפעול על ישומים, מערכות הפעלה, חומרות. היום אפילו בקר בלואו-טק חשוף למתקפות. לצד כל אלה, יש את הגורם האנושי".

ומה לגבי שיטות ההגנה הקיימות? כאן יש לתא"ל אשל הסבר מפורט: "מבטיחים על ההגנה כעל הגבולות, יוצרים גדרות, עם Firewall, מנגנוני זיהוי ועוד, אבל זה לא מספיק מול כמות עצומה של חורים. תוקף שחודר - שוהה תקופה ממושכת עד שהוא מתגלה".

בנוסף, חידד, "קשה לנטר את כל התוקפים, כל הזמן מנסים לייצר מלכודות דבש, אולם עדיין, התוקפים מוסווים". לכן, אמר, "על מנת להתמודד עם המצב החדש, מערכות ההגנה הולכות לכיוון מודיעיני, עם אי ודאות גדולה, תוך התייחסות להיבט של 'אני לא יודע מה אני יודע'. אנו הולכים למצב בו הרשת משתנה, מה שדורש ניהול של רשת דינמית". תא"ל אשל סיים באומרו כי "יש לנו שיתוף פעולה הדוק עם התעשייה. הקמנו קרן לפני שלוש שנים. כשהתחלנו, עבדנו מול ארבע חברות - היום אנו עובדים מול יותר משלושים חברות, והנתון הזה גדל. אנו במפא"ת נמצאים בקשר עם כל הגופים העוסקים בתחום - עם מחלקת הגנה בסייבר באגף התיקשוב, עם גורמי מודיעין, עם התעשיות. יש פה יתרון יחסי אדיר במשק: אנו מקבלים את כוח האדם הטוב ביותר".

מדבריה של **אסתי פשין**, ראש מנהל מערכות הסייבר של התעשייה האווירית-אלתא, בכנס הרצליה.

"ההאקר הוא הבעיה שלנו", אמרה פשין. "יש שלוש סיבות מדוע הוא מנצח: ראשית, יש את בעיית הזהויות הבדויות. בסייבר קל ליצור זהויות שכאלה. היה מקרה בו יצרנו בחורה אנגליה ממוצא צרפתי. בתוך 48 שעות היו לה 100 חברים שהזמינו אותה למסיבות ושאלו אותה שאלות. הדמות התפתחה ברשת כאמיתית. הבעיה השנייה היא ה-Big Data, מאחר שריבוי המידע מקשה לאתר טרנזקציות. עוד אתגר הוא שרוב עולם הסייבר מוצפן. מרבית התעבורה בסייבר נשלטת על ידי תאגידים ואלה מעדיפים את צרכי הביטחון של המדינות על פני הגנת הפרטיות של המשתמשים".

היא ציינה כי "הסייבר הוא לא בהכרח מהפכה - הוא התפתחות פרקטיקות קודמות, למשל מתחום הלוחמה האלקטרונית. זה מרחיב את היכולות שלנו. אחד הדברים שאנחנו מנסים לעשות הוא לקחת שדות פעילות קודמים ולהעתיק את הפעילות שמבוצעת בהם לשדה הסייבר". "התעשייה מבינה כי המפתח להתמודדות בסייבר הוא חדשנות", הוסיפה פשין. "יש בישראל סצנה מדהימה של סטארט-אפים. התעשייה האווירית משתפת פעולה עם סטארט-אפים ומשמשת להם מעין 'אחות גדולה'. אנחנו מסייעים לסטארט-אפיסטים להגיע לשוקים חדשים, עוזרים להם בהתקנת המוצרים שלהם ולוקחים על המוצרים הללו אחריות".



אסתי פשין

פשין ציינה כי התעשייה האווירית הקימה שני מרכזי מ"פ חיצוניים לה, שעוסקים בסייבר - "האחד הוא מרכז מ"פ שהקמנו עם סייבריה, שמשמש כמרכז הנגשת הסייבר של התעשייה האווירית, לטובת צרכים מודיעיניים והגנתיים. השני הוא מרכז שהקמנו בסינגפור".

### "ישראל מקדמת את עצמה בתחום הסייבר"

פרופ' בן ישראל אמר, כי "שתי מגמות בולטות בשנים האחרונות הן שישראל ביצעה מהלכים רבים כדי לקדם את עצמה בתחום הסייבר ושלאט לאט מחלחלת בעולם ההכרה שסייבר הוא לא רק אבטחת מידע". הוא ציין כי "אנחנו משתמשים במחשבים באופן אינטנסיבי מזה שנים רבות ותמיד היה צריך להגן על המידע שנמצא בהם, אלא שמאז סטוקסנט התברר שיש שלוש אמיתות, פרדיגמות שמהן נדרש להיפטר מהן: הראשונה היא שאיום סייבר הוא איום על המידע. סטוקסנט גרמה לנוק פייז, לפגיעה בצנטריפוגות. ניתן לפגוע גם בדברים אחרים, למשל מערכות חשמל, רכבות או רמזורים. התובנה הזו מחלחלת לתודעת העולם. הפרדיגמה השנייה היא שמחשב זה לא רק מה שאנחנו קוראים לו מחשב. גם הטלפונים והבקרים, למשל אלה שמבקרים את מהירות סיבוב הצנטריפוגות באיירן, הם מחשבים. יש להסתכל על המונח 'מחשב' במובן רחב יותר. הפרדיגמה השלישית והמפתיעה ביותר היא שהמקור