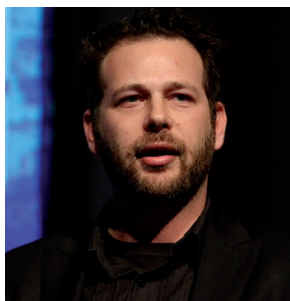


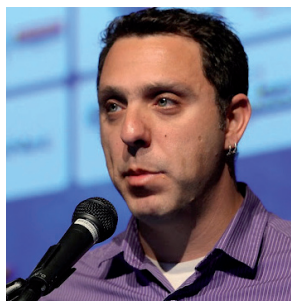
האבטחה הייחודית של NetWitness מרחיבה את הפתרונות של RSA לניהול סיכונים אבטחה בסביבות וירטואליות ופיזיות". הוא סיים בציינו, כי באוגוסט האחרון הוסיפה החברה רכיב חדש לקו המוצרים, NetWitness Panorama, "המספק יכולות ניתוח מתקדמות באמצעות שילוב והתכה של כלל מרכיבי המידע, הזמין מתעבורת הרשת של הארגון, לוגים ממקורות מידע שונים ברשת ומידע חיצוני מקהיליית אבטחת המידע. שילוב כלל מקורות המידע והיכולת לנתח את כל המידע בזמן אמת, מספקים כלים יעילים להתמודדות עם מתקפות מתקדמות שכלי אבטחת מידע מסורתיים אינם יעילים נגדם".

### ההגנה רב-שכבתית

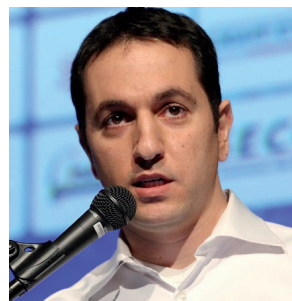
"הטכנולוגיה הולכת ומסתבכת. מיליוני שורות קוד נכתבות, מה שמביא לריבוי פרצות. ההגנה על מערכות המידע צריכה להיות רב-שכבתית", כך אמר **גיא לופו**, מנהל טכני אזורי בצ'ק פוינט. כדוגמה נתן לופו את סוני. לדבריו, החברה "נפגעה בצורה קשה ב-2011, ואחרי תחקיר התברר שהמערכת שלה שהותקפה לא הייתה מוגנת".



טל מוזס



גיא לופו



ציון זטלאובי



ד"ר גבי סיבוני

הוא אמר, כי המידע דולף בשל שני מימדים - האנושי והטכנולוגי. "בהיבט האנושי נעשה 'הינדוס חברתי' ברשתות חברתיות", ציין. "האקרים מזהים אנשים ולוונטיים בארגון, יוצרים עימם קשר ודרכם נכנסים לארגון. טעות נפוצה אחרת היא שפעמים רבות עובדים טוענים או מורידים קבצים שהם לא יודעים מה מקורם". "בעבר", הוסיף לופו, "דנו על הפיריורל כבסיס לכל אבטחת המידע בשנים אחרונות נכנסים כלים למניעת נזקות, אנטי וירוס, אנטי בוט ו-IPS, לצד כלי שו"ב". הוא ציין, כי ההגנה הרב שכבתית מטפלת בהיבטים כמו מניעת חדירת נזקות ומניעת כניסת דואר זבל. IPS הוא אחד ההיבטים הכי חשובים", אמר. "אנחנו מזהים פגיעויות וחוסמים אותן. צריך לוודא ולבקר של כל אחת מהמערכות לא תהווה פרצה". לדבריו, "יש לנו מנוע מתוחכם שבוחן את תקפות המידע שמגיע לארגון ובדק האם אנחנו תחת התקפה כלשהי". שכבה נוספת אותה ציין לופו היא האנטי בוט. "התחום עלה בשנתיים האחרונות", אמר. "בסופו של דבר, עם כל ההגנות, לעולם לא נהיה מוגנים ב-100%", סיכם. "תמיד תהיה נקודת תורפה שבאמצעותה ינסו האקרים לחדור. עם זאת, התקפות רבות היו יכולות להיחסם ולהימנע באמצעות המוצרים שלנו".

### "כימות סיכונים נכון חוסך כסף"

"הוצאות אבטחת המידע אינן תקורה מיותרת, אלא ערך עסקי אמיתי לארגון", אמר **טל מוזס**, מנהל חברת הקטיקס, ארנסט אנד יאנג ישראל. "די אם נזכור שהעלות של גניבת מידע או התקפת סייבר יכולה להגיע לעשרות מיליוני דולרים כדי להבין שמוטב להשקיע את הכסף במניעה מראש ולא בתיקון בדיעבד", הוא ציין, כי "נוצר אתגר חדש - לשלב בין שתי שפות: שפת אבטחת

ועם ארגונים ממשלתיים, על מנת לקבל מידע ולהגיע ביחד לתמונת מצב אמיתית".

בלוך סיכם בציינו, כי "הפתרון של קבוצת אמן מבוסס על הפקת לקחים ויישומם, תוך שילוב ידע ודיסציפלינות צבאיות ושל תעשיות ביטחוניות, על עולם אבטחת המידע הקלאסי. כך ניתן לבנות יחד עם הארגון את תפיסת אבטחת המידע. לאמן יש פתרון מעטפת לתחום הסייבר, שכולל ניתוח אסטרטגי, מודיעין 'מחוץ לגדר' והנדסת מערכות פיתוח וטכנולוגיות".

### "שכבה שלמה של ארגונים לא מוגנים"

"יש זיקה הדוקה בין תחום הסייבר לחוסן ולביטחון הלאומי של מדינת ישראל. בישראל יש שכבה שלמה של ארגונים שאינם מוגנים מפני מתקפות סייבר", אמר אל"מ (מיל') ד"ר **גבי סיבוני**, ראש תכנית המחקר "צבא ואסטרטגיה" במכון למחקרי ביטחון לאומי. לדברי ד"ר סיבוני, תחום הסייבר מטופל או לא מטופל בשלושה מרחבים. האחד, הארגונים הביטחוניים, צה"ל, קהילת המודיעין

והתעשייה הביטחונית. "הם בדרך כלל מוגנים מפני מתקפות קיברנטיות", ציין. המרחב השני, לדבריו, הוא התשתיות הלאומיות הקריטיות, "שבעבר נדרשו להגנה פיזית וכיום ניתן לתקוף אותן תקיפה קיברנטית". המרחב השלישי, לדברי ד"ר סיבוני, הוא "רוב רובו של המגזר האזרחי, בו פעולות חברות אזרחיות וגם פרטים. הם חשופים באופן טבעי למתקפות קיברנטיות. יש שכבה שלמה של ארגונים שלא מוגנת כיאות בתחום. כל הקשור לצנעת הפרט ולהיבטי השמירה על המידע - אינו מטופל". "יש פה בעיה שאסור לתת לה להימשך", אמר ד"ר סיבוני, "לתוקפים קל לתקוף מערכת לא מוגנת, אתרי תדמית ואתרי חדשות - ובכך הם עלולים להסב נזק רב למדינה. לכן, על המדינה להוסיף סעיף בחוק רישוי עסקים ולטפל בנושא. נדרש לקבוע מי יהיה הרגולטור לתחום זה, ולהכניס לתוך החוק את היבטי אבטחת מידע. המטה הקיברנטי הלאומי יכול לסייע ולהגדיר אילו תנאים צריך להכתיב לאילו סוגי עסקים הרכב. יש להוציא הנחיות מפורטות לתחום. אסור שתחום תגובת הנגד למתקפה יישאר פתוח לשני הצדדים, ושארזרחים יפעלו באופן בספונטני".

**ציון זטלאובי**, מנהל קדם מכירות אזורי ב-RSA, אמר בכנס, כי "הנחת העבודה לפיה ארגונים נדרשים לעבוד היא שהם מותקפים, מחשביהם גנועים ועליהם לאתר את הפרצות ולהגן עליהם". הוא הציג את כלי NetWitness של החברה, המספק לדבריו "רשת נייטר אבטחה ופלטפורמת ניתוח. כך ארגונים יכולים להבין את הפעילות המתרחשת ברשתות שלהם. בין היתר, מספקת החברה פתרונות לבעיות אבטחת מידע כמו אימונים פנימיים, תוכנות זדוניות, הונאה, ריגול והדלפות מידע". לדברי זטלאובי, NetWitness הגדירה מחדש את נוף האבטחה, וסיפקה פתרון כוחני לארגונים המחפשים להשיג הבחנות מיידיות ובהירות מדויקת לנוכח איומי הסייבר הקשוחים ביותר. יכולות ניתוח רשתות