

מורכבות שכוללות מכוונות וירטואליות, חיבורי רשתות מורכבים ורשתות גדולות", אמר פישר. פישר סיכם באומרו, כי "כשמסתכלים על הנושא בעיניים פקוחות לומדים שאפשר להתמודד עם הדברים האלה, ואז זה כבר לא כל כך מפחיד".

### "פיירול הוא כמו גבינה"

**ברוך טי**, מנהל אזורי בכיר לאזור המזרח התיכון ואפריקה בתופין מערכות, הציג את הפתרון שמציעה החברה שלו לסתימת חורים שנובעים מחוקים שונים שפוערים ערוצי מעבר בפיירול. "פיירול הוא כמו גבינה שהחורים בה הולכים ומתרחבים, וכשחורים מתרחבים נכנסים מזיקים. פותחים יותר מדי ערוצים, יש עוד ועוד חוקים, ויש חוקים מוצללים שלא ממוקמים היטב ויש גם חוקים שלא נמצאים יותר בשימוש ושכחו למחוק אותם", אמר טי. לדבריו, "אנחנו רוצים לדעת מה החורים וכך להגביר את האבטחה שלנו, כי אנחנו יודעים איפה החורים ואיך לסתום, או לפחות להקטין אותם. אנחנו מאפשרים לכם לקבל תמונה של כל הרשת שלכם, כולל כל החיבורים, הממשקים ונקודות האבטחה. אנחנו יכולים לספר לכם על כל

חריג, אלא אנחנו חשופים אליו בכל רגע נתון, ומה שיעשה את ההבדל הוא איך אנחנו מבצעים את ניהול הסיכונים. היעדר ניהול סיכונים נכון יכול להוביל לאסון, כשלפעמים אי אפשר להחזיר את הגלגל אחורה", כך אמרה **רונית קריספין**, יועצת לניהול סיכונים ומשברים ומבקרת פנים ממשדר 1Risk 1Solution, במסלול העסקים בכנס.

לדבריה, אסור לחברות להיות מופתעות. "זה צריך להטריד אותנו שיש עוד חברות שמופתעות ממשברים ומכך שמתקפים אותן. צריך להבין שתוקפים אותנו כל הזמן ולפעמים מצליחים ולפעמים לא, והשאלה היא איך אנחנו מתכוננים לכך", היא אמרה.

**אפרים אקרלינג**, סמנכ"ל ומנהל אגף מערכות מידע באליהו חברה לביטוח, הציג במסלול העסקים את ההתכוננות של החברה למשבר שיכול להתרחש עקב התקפת סייבר. "בחברת ביטוח יש כספים של לקוחות ואנחנו צריכים לשמור היטב על המידע של הלקוחות בהתאם לחבות העסקית ולרגולציה".

לדבריו, "כל פתרון שאני מאמץ עבור אליהו צריך לתמוך בעסקים של החברה ואני מנסה למצוא דברים קיימים ולא להמציא דברים חדשים". "אנחנו מחויבים להמשכיות עסקית, והמשכיות עסקית זה לא רק



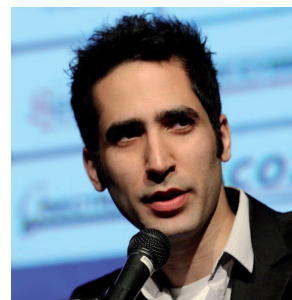
יוסי פישר



אפרים אקרלינג



רונית קריספין



מני ברזילי

שינוי שקורה, וגם מי ניגש, מתי ניגש ואפילו מאיזה ממשק".

**מיכאל מומצ'ונלו**, ה-CTO של Light Cyber, אמר כי "המשפט דע את האויב ודע את עצמך ולא תובס גם במאה קרבות, מייצג את האמונה שלנו, לפיה הדרך להתמודדות עם האיומים של השנתיים האחרונות היא זיהוי המתקפות כשהן מתרחשות ברשת שלנו".

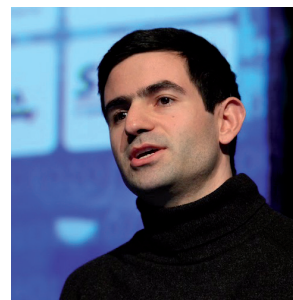
הוא הוסיף, כי "אנחנו מציעים ניתוח אוטומטי שמטרתו למצוא את כל המחטים בערמות השחת. האם אתם מכירים את מבנה הרשת? את כל השרתים ומי משתמש בהם? מהן המערכות הקריטיות ומהן השגרות להתחברות מהבית? ומה קורה אם מזהים גניבת מידע?". לדבריו, "אנחנו צריכים להגיע למצב של עליונות ידע, ואסור לוותר על כך למרות הקשיים, כי ידע הוא כוח והוא עוזר לזהות תקיפות ולהתמודד עם האיום".

### "להקשיח סטנדרטים כדי להגן על המידע"

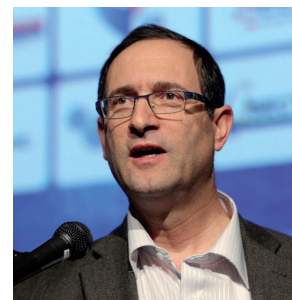
"חברות האבטחה בישראל צריכות לשים לב שהן הפכו ליעד תקיפה, כדי להגיע דרכן ללקוחות שלהן. החברות הללו צריכות להקשיח סטנדרטים כדי להגן על המידע שלהן", כך אמר **בועז דולב**, מנכ"ל חברת Clear Sky. דולב, לשעבר מנהל תהיל"ה-הממשל זמין במשרד האוצר, דיבר



בועז דולב



מיכאל מומצ'ונלו



ברוך טי

טכנולוגיה או שירות, זה גם פיזי, מה קורה כשביט אליהו מפסיק לעבוד. יש לנו אתר חירום עם רפליקציה מלאה, כולל חומרה ותוכנה, הכל כפול ובשרידות מלאה. אנחנו גם משתמשים במספר חברות שמנסות לפרוץ למערכת שלנו ומספקות דו"חות כדי שנדע מה צריך לתקן ומה לבדוק".

**יוסי פישר**, דירקטור מכירות למזרח התיכון ב-SafeNet, הזכיר את החשיבות של הגורם האנושי, והסביר מדוע חשוב להצפין את המידע בעסק.

לדבריו, "יש הרבה סוגים של מתקפות ורק אמת אחת: אין מקום שיש בו בני אדם שהוא לא חשוף להתקפות. צריך לחשוב על מה שקורה אחרי. מה יקרה אחרי שפורצים וגונבים מאיתנו את המידע. לנו הרי חשוב שהמידע שייצא החוצה לא יהיה שמיש, והדרך היחידה היא להצפין את המידע במרכז הנתונים, וזה מה שאנחנו עושים, הצפנות בסביבות