

אבטחת המידע, מנהלי הסיכונים ומנהלי הבקורות". לסיכום, הוא ציטט מספר קהלת פרק ט' פסוק 18: "טוֹבָה חֻכְמָה, מִכְּלִי קָרֶב; וְחוֹטָא אָחָד, יֵאָבֵד טוֹבָה הַרְבֵּה".

"על המנמ"רים להחדיר להנהלות שה-IT בליבת העסקים הארגונית"

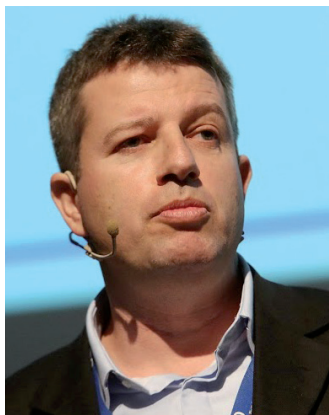
"ה-IT נתפס בארגון כמרכז עלות - וזה לא ככה. תפקידנו, המנמ"רים, הוא להילחם בתפיסה הזו ולהחדיר להנהלות שה-IT נמצא בליבת העסקים של הארגון", כך אמר **יוסי שנק**, סמנכ"ל תיקשוב בחברת החשמל.

שנק דיבר בפאנל שנערך במסגרת כנס של ISACA ישראל. מנחה הפאנל היה ר"ח **ירון פלד**, מנהל BDO זיו האפט וחבר הנהלת ISACA ישראל. לדברי שנק, "נדרש לנהל את ה-IT באופן מושכל, תוך מימוש תפיסת ממשל IT. בראייה כוללת, זה מוסיף לתקורה ולכן זה נתפס כמפריע. אבל אם עושים ממשל IT נכון, ממצבים נכון את גוף ה-IT בארגון ועובדים לפי מסגרת עבודה, למשל CobiT, מסייעים לעבודה ולתפעול התהליכים בצורה נכונה ויעילה, מאחר שהמסגרת מסייעת לעיצוב התהליכים".

הוא הגדיר את חברת החשמל כחברת "מיד-טק - לא לואו-טק ולא היי-טק. בארגונים כאלה ה-IT לא רק מסייע לליבה העסקית אלא הוא חלק ממנה. לכן, נדרש שה-IT של כל אחד מהם יעבוד על בסיס מסגרת עבודה. כך הוא יביא עוד תועלות והזדמנויות לארגון". "אני מתנגד בחריפות למשפט לפיו על ה-IT לעבוד בהלימה לעסק", סיכם שנק. "חברת החשמל היא ארגון גדול



יוסי שנק



ירון פלד

ומורכב, אבל מאוד פשוט - הוא מייצר חשמל. ה-IT שלנו תורם לעסק בדיוק כמו כל אגף אחר בחברה, וזה מובן וידוע".

"מסגרת העבודה מאפשרת ל-IT לעבוד בצורה כוללת"

עופר מיד'זנסקי, מנהל יחידת טכנולוגיות מידע ב-פז, ציין כי "כשישימנו את ממשל ה-IT בחברה הבנתי שאי אפשר ליישם את כל התהליכים על בסיס CobiT. בחרתי מסגרת תהליכית שכוללת יצירת



עופר מיד'זנסקי

עליו ועל חבריו מוטלות משימות והם נמדדים עליהן, גם אצלם קיימת תחרות פנים ארגונית על משאבים והם נדרשים ליעילות". לדבריו, חיי היום יום של התוקף הממוצע דומים למדי לאלה של כל אדם אחר: "הוא קם בבוקר, יש לו משימה לבצע, יעד מוגדר ומדיד, יש לו אתגר ועליו לבחון עד כמה הוא מממש אותו".

"המשאבים של התוקף מוגבלים, אין לו כל היכולות שבעולם", אמר דולב. "אין דבר כזה מגה תוקף, אחד שיש לו את כל סל היכולות. מכאן - חובה שהתקיפה תהיה מנוהלת, ולכן, בניגוד למה שחושבים, לא מדובר באנרכיזם. אם נבחן לעומק את התוקף נראה שהוא מחפש מיטוב של משאבים מול משימות. אין מצב שבו הוא יעשה הכול, כי הוא רוצה להיות יעיל".

הוא כינה את טכנולוגיות התקיפה בהן משתמשים ההאקרים "סקסיות, מדהימות. אלא שמי שיוודע לא יספר עליהן וטכנולוגיות עבר דוגמת סטוקסנט, שיש כאלה שאוחזים במידע עליהן - זה כבר לא רלוונטי. חנות הצעצועים של התוקף משתנה באופן תדיר, כאשר החלק המשמעותי בה הוא חשאי ולא ניתן לניבוי. אי אפשר לחזות את מגמות התקיפה". הוא הוסיף כי "השיח על תקיפה הוא בעייתי, אנשים שנוטים לשוחח על כך נלחמים את המלחמה הקודמת".

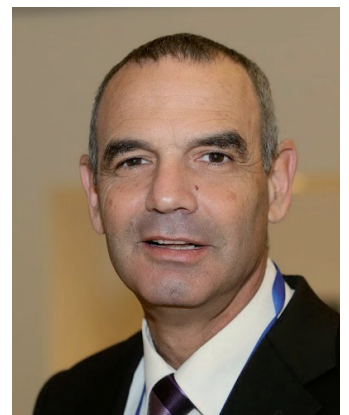
דולב סיכם באומרו כי "השאיפה האולטימטיבית של התוקף היא לקדוח בנקודה הנכונה. הוא רוצה לעבוד באופן מקצועי, שהמשאבים שלו יהיו הטובים ביותר. לכן דרושה מולו ההגנה הטובה ביותר".

"ההגנה הקיברנטית צריכה להיות טורפת, מיירתת, חכמה וממזרית"

"הסייבר שובר פרדיגמות שהכרנו בעולם הלחימה הקלאסי. בניגוד לעולם הפיזי, המשפט 'ההגנה הטובה ביותר היא ההתקפה' לא רלוונטי בו, כי אין בו מצב של התקפה. בסייבר, ההגנה הטובה ביותר היא ההגנה", כך אמר **ארז קריינר**, נשיא Five C. לדבריו, "ההגנה הקיברנטית צריכה להיות אקטיבית, טורפת, מיירתת, חכמה ובעלת מימד ממזרי, שישפר את המצב בארגון".

קריינר, עד לאחרונה ראש רא"ם, הרשות לאבטחת מידע בשב"כ, דיבר בכנס.

"ישראל היא מדינה קטנה בשכונה קשה. בנוסף, הגבולות הווירטואליים קשים להגדרה. לכן, כל מודל הביטחון הלאומי שישראל נשענת עליו קורס בעולם הווירטואלי: קשה להשיג בעולם הזה את ההרתעה, ההתראה וההכרעה", אמר קריינר. "הסיבה לכך היא שבסייבר אין שטח. ככלל, הוא שובר פרדיגמות: ניתן לתקוף טיל עם וירוס אבל לא ניתן



ארז קריינר

ההיפך. זהו כרטיס בכיוון אחד. אפשר לתקוף את העולם הקינטי בנשק קיברנטי, אולם אי אפשר לתקוף את העולם הקיברנטי בנשק קינטי. בנוסף, שכפול וירוסים הוא פעולה זולה, בעוד שיקר לשכפל טילים".

"היבט נוסף", לדבריו, "הוא שהחזית בשדה הקרב הקיברנטי אינה בחזית הפיזית, אלא בכל מקום. לא לחינם אמר ויליאם לין, לשעבר סגן שר ההגנה האמריקני, שהאיום הקיברנטי הוא האיום החמור ביותר על ארצות הברית. אפגניסטן ועיראק רחוקות, הסייבר נמצא להם בתוך הבית".

קריינר ציין כי שאלה נוספת שעולה היא על מי מוטלת האחריות לבצע את ההגנה הטובה ביותר בסייבר שהיא, כאמור, ההגנה עצמה. "לא הצבא ולא המשטרה יגנו על ארגון כלשהו מפני מתקפות סייבר", אמר. "רק הארגון יגן על עצמו ולכן, האחריות מוטלת אך ורק על מנהלי