במסלול ממשלה וביטחון שנערך במסגרת הכנס.

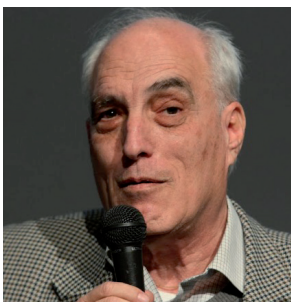
הוא המליץ לארגונים לעבור לענן מאובטח, שבמסגרתו מנטרים מפעילי הענן מפני חדירות מורכבות.

בדבריו מנה דולב את האתגרים שעימם צריכות חברות האבטחה להתמודד ב-2012. בין היתר, אמר, "זירת לוחמה היא א-סימטרית וגם האקר בודד יכול להסב נזק גדול; אין שום שליטה על העברת כלים או על העברת ושיתוף מידע בנוגע לכלי תקיפה באינטרנט; קשה עד בלתי אפשרי לאתר את המקום שממנו מבוצעת התקיפה; וקשה מאוד לאבחן ולהבין שהותקפת - החדירה לתוך המחשב יכולה להיות חשאית וללא שום יכולת גילוי. כיום, תקלה במערך המחשוב מטופלת על ידי ביצוע ניסיון החזרה לכשירות ותיקון התקלה ללא בחינת האירוע. כמו כן, הקושי לאתר את מקור התקיפה, שיכולה אף להיעשות דרך צד שלישי, ללא עקבות, מונע יכולת תגובה".

"תקיפות הסייבר הרב שלביות המתוחכמות ביותר בוצעו בשנה האחרונה על חברות אבטחה כגון RSA ודיגינוטר, והמידע שנגנב מהן שימש לבצע חדירות לגופים אחרים - גופים ביטחוניים וחברות כמו מיצובישי ולוקהיד-מרטין", אמר דולב. הוא קרא לאמץ את המודל שיושם בתהיל"ה, הכולל חוות שרתים או ענן מאובטח שמגן על הלקוחות - באותו המקרה מדובר היה במשרדי הממשלה. לדבריו, "ניתן כיום להקים מערך אירוח מאובטח למגזר הפרטי - לקחת את המודל שנבנה עבור הממשלה וליישם אותו עבור הסקטור העסקי".

איתי ינובסקי

ד"ר נמרוד קוזלובסקי



ד"ר יאיר שרן

"הנחת המוצא: ההגנות לא יעמדו בפני תקיפה"

איתי ינובסקי, יועץ לאסטרטגיית סייבר בחברת CXO, תיאר את השינויים שצריכה לעבור יחידת ה-CISO כדי לענות לאיומים החדשים, כך שתוכל לעסוק בתחומי הליבה שלה. בין אותם תחומים הוא מנה בקרות להכוונת הפעילות וההתנהגות האנושית, מדיניות, בדיקות רקע, בקרות שקשורות בטכנולוגיות (פיירוולים, אנטי וירוס ו-IPS), בקרות של תהליכים ותגובות לאיומים.

לדבריו, "הנחת המוצא של מי שעוסק בהגנה היא שכל אמצעי המניעה לא יעמדו, בסופו של דבר, בפני התקפה".

הוא קרא "להקים במגזר הציבורי גופים שונים - גוף העוסק בבקרות טכניות ומסמיך נאמני אבטחת מידע באגפים שונים של חברות; גוף העוסק בניסיון לבחון איך הארגון נראה מבחוץ; ויחידת מודיעין ומחקר שתעסוק בחקר אנומליות, הנדסה לאחור, איסוף מידע ומידול מתקפות סייבר, לרבות חקר מתקפות שאירעו ודרכי התגובה של הגופים שהותקפו".

"רמו"ט צריכה לשנות את מהותה"

עו"ד ד"ר **נמרוד קוזלובסקי**, מומחה לדיני מחשבים, אבטחת מידע ודואר אלקטרוני, דיבר על משבר האמון באבטחת המידע שהתגלה לאחר שמתקפות שנותרו ללא מענה חשפו שהחוליה החלשה היא האתרים האזרחיים המסחריים. לדבריו, "רמו"ט צריכה לשנות את מהותה ולהפוך לגוף שבודק את מוכנות החברות למתקפות באמצעות מתקפות פתע".

"הסתבר שהמחשבה שלפיה השוק יסדיר את האבטחה, משום שגופים יתהדרו בכך שהם מוגנים על מנת למשוך אליהם עוד לקוחות, לא עבדה. אין לאתרים מוטיבציה לעסוק כלל באבטחת מידע", אמר. "לכן, אני מציע לשנות את החוקים כך שיגדירו עונשים כבדים על מי שלא מתכונן למקרי תקיפה כאלה ולחייב את החברות לדווח על מקרי פריצה. הפחד מעונשים אלה, כמו גם הפחד מאובדן המוניטין, יגרום לחברות לבצע את ההשקעה הדרושה באבטחת האתרים".

כמו כן, הציע עו"ד ד"ר קוזלובסקי לישראל להצטרף לאמנה הבינלאומית לפשעי מחשב - אמנת בודפשט משנת 2001. כך, לדבריו, תוכל המשטרה לקבל סיוע ממשטרות אחרות בעולם בפענוח הפשעים הללו, שרובם בינלאומיים.

"בעתיד, האקרים יחדרו למוח שלנו"

"כיום מדברים על עולם שבו הסודות הכי פרטיים שלנו יכולים להיות ברשות כל אחד שהיה רוצה לדעת. בעתיד, האקרים לא יחדרו דווקא למערכות מחשב אלא גם למוחות שלנו, למחשבות של כל אחד מאיתנו", כך אמר ד"ר **יאיר שרן**, מנהל המרכז הבינתחומי לניתוח ותחזית טכנולוגית באוניברסיטת תל אביב.

הוא חזה, כי הפרטיות תיעלם בעתיד. "תארו לעצמכם את העולם בשנת 2030, שבו קוראים מחשבות ומצלמים מעבר לקירות, עולם שיכול להיות שאין בו כבר טעם לדבר על הגנת מידע, כי ממילא, כל המידע יהיה פרוץ", אמר.

כמו כן, הוא דיבר על האיומים הקיימים כיום ואמר, כי "האיום הכי מטריד מביניהם הוא היכולת של ארגוני טרור לחדור לכורים גרעיניים ולגרום לתאונות או התפוצצויות גרעיניות באמצעות חדירה למערכות השליטה והבקרה". "בהקשר הזה חשוב להתכונן לכלי נשק חדש - רובוטיקה", המליץ ד"ר שרן. "הרובוטים יוכלו בעתיד לעשות אמנם את עבודות הבית ולטפל בילדים או בהורים קשישים, אבל יש להם גם את הצד השלילי, מאחר שגם הטרוריסטים יוכלו לעשות בהם שימוש. כבר כיום אנחנו עדים לקלות הבלתי נסבלת של רכישת רובוטים ולאפשרות לחבר להם חומרי נפץ וחומרים רעילים, ולפזר אותם היכן שרוצים".

זהירות - נחילי רובוטים

"צריך להיזהר במיוחד מנחילי רובוטים", הוסיף. "כל רובוט בנחיל יכול להיות קטן מאוד ולשאת מעט מאוד חומר נפץ, אך במספרים גדולים, ועם יכולת התקשורת בין הרובוטים לבין עצמם ובינם לבין המפעיל, ניתן לגרום נזק גדול לאויב".

תחום נוסף המהווה מקור לדאגה, לדברי ד"ר שרן, הוא הננו-טכנולוגיה. "היא מאפשרת כיום להפוך כל מערכת להרבה יותר קטנה מאשר בעולם שאנו מכירים. כמו כן, היא מאפשרת לפתח חומרים עמידים ומה שיותר גרוע - חומרים שלא ניתנים לגילוי על ידי שום סנסור". בתחום החומרים המתוכנתים הוא ציין שיש שריג משובץ מערכות מחשב זעירות שיכול לשנות את עצמו על פי פקודה ואמר, כי בעתיד, "ניתן יהיה להבריח כלי נשק שנראים כצעצועים תמימים ומשנים את צורתם לאחר המעבר".

"עולם הביולוגיה מתפתח לכיוון של ביולוגיה סינתטית, קרי: היכולת