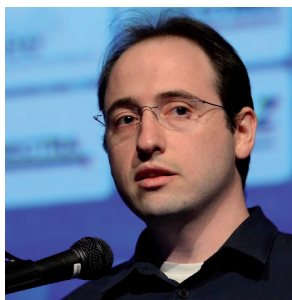


מדיניות מתאימה. אל תחכו. אל תעצמו עיניים".  
 רו"ח **דורון רונן**, נשיא האיגוד הישראלי לביקורת ואבטחת מידע (ISACA ישראל) התייחס גם הוא להשלכות של פרשיית חשיפת כרטיסי האשראי והמידע הפרטי של המשתמשים שאירעה לאחרונה.  
 "אין חסינות או הגנה מוחלטת מפני דליפת מידע, זה ברור לכולנו, וחשוב שגם האזרחים הפשוטים יהיו מודעים לכך, ושידעו שהם צריכים להגן על עצמם. צריך לחייב עסקים להגן על האתרים שלהם וחשוב שיהיה גוף ממשלתי שאחראי לכך. המסר שצריך לצאת מכאן הוא שאנחנו כאנשי מקצוע חייבים לחנך", אמר רונן.  
 לדבריו, "המשתמש חייב להיות מודע לאפשרות שהאתר לא מאובטח, אבל במקביל המגזר הממשלתי צריך לקחת אחריות כרגולטור ולהסמיך אתרים. אם יש הסמכה לאתר אני יכול, כמשתמש פשוט, להבין שמדובר באתר מאובטח ושאני יכול להשתמש בו. אם אין הסמכה, ואני בכל זאת משתמש, האחריות עליי".  
**אנדרי דולקין**, מנהל מחקר טכנולוגי ב-Cyber-Ark, הציג פתרון שמונע חיבורים לרשת עם הרשאות שמבוצעות על ידי אנשים לא מורשים שהשיגו את המידע.

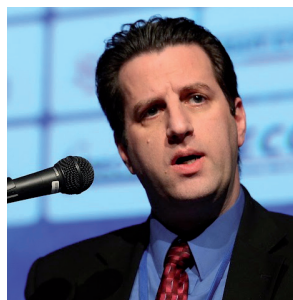
המידע ושפת הלוגיקה העסקית של הארגון. השילוב הזה יכול לעזור לסמנכ"ל הכספים לחשב את החשיפה שעלולה להיגרם לחברה כתוצאה מהתקפות על מערכות המידע הממוחשבות, כגון גניבת מידע, השחתת מידע, וידושים, סוסים טרויאניים, קוד זדוני ומעילות פנים ארגוניות. כימות סיכונים נכון יחסוך כסף לחברה ויגן עליה טוב יותר".  
 "שנת 2011, אמר מוזס, "הוכרזה בקרב אנשי אבטחת המידע כשנת התקפות הסייבר הבינלאומית. אין כמעט חברות חסינות לפריצה, אפילו חברות גדולות ופירמות בנקאיות ידועות נפלו קורבן. גם חברות קטנות מועדות למתקפות סייבר".  
 הוא סיים בהציגו טכניקות שונות לאיסוף מודיעין, דוגמת מקלדת "מטופלת", שיש בה שבר שמאפשר להאקרים להורות לה מה לכתוב ולפרוץ דרכה למערכות ה-IT הארגוניות.

**ההשפעה העסקית של התקפת סייבר**

"ההשפעה העסקית של התקפת סייבר נגזרת מערך הנכסים שאנחנו מחזיקים, ואנחנו צריכים להפעיל ניתוח שכולל הערכה לגבי המציאות הכלכלית, הפוליטית וכדומה - כדי לנסות להבין מהי הסכנה העסקית.



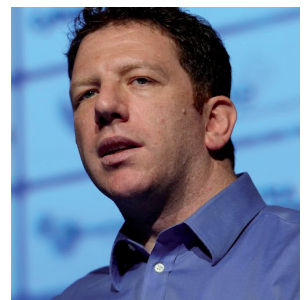
אנדרי דולקין



דורון רונן



עו"ד אביב אילון



אופיר זילביגר

לדבריו, "אחת הדרכים היא לא לתת לסיסמאות להגיע לתחנת הקצה. העובד מזוהה לפי פרופיל, פותחים בשבילו ששן שמתאים להגדרות העבודה שלו ועוקבים בזמן אמת כדי לדאוג אם הוא מבצע את מה שהוא אמור לבצע".  
 "בלי נקודת בקרה מרכזית, המשתמש מתחבר ישירות אל בסיסי נתונים וכדומה, וגם אם לא נגנבת הסיסמה, התוקף יכול לנצל את החיבור עצמו כדי לגנוב מידע. אבל עם בקרה מרכזית זה נמנע. והתוקף לא יכול לגשת ישירות לאף חלק במערכת המיושבת, כי מבוצע ניטור על החיבור בלבד ולא על המערכת כולה", אמר דולקין.  
**מני ברזילי**, מבקר מערכות מידע בבנק הפועלים, טען, כי "אנחנו חייבים לשנות את נקודת ההתייחסות שלנו. הסייבר הוא מקום שאנחנו נראים בו אחרת ופועלים בו אחרת. הפסיכולוגיה בו שונה וההיבטים החברתיים בו שונים. "מי שרוצה לעסוק בעולם הסייבר וגם באבטחת מידע צריך להבין דבר אחד: יש להשתחרר מקיבעונות העולם הפיזי ולחיות רק את העולם הווירטואלי", אמר.  
 לדברי ברזילי, "מדובר בהבדלים שיוצרים סוג חדש של פושעים ומגמות פשיעה. חייבים לשנות את הראייה ואת שאלות הבסיס. ככל שניטיב להבין מה נכון פה ומה נכון שם, איך העולם הזה עובד ואיך העולם הווירטואלי עובד - כך ניטיב להבין את העולם הזה ואת הסכנות שיש בו, אבל גם את הסיכויים שיש בו".

**ניהול סיכונים - תמיד**

"חברות צריכות לבצע ניהול סיכונים לא רק כשאומרים להן לעשות זאת, אלא באופן תקופתי. הן צריכות להבין, כי משבר הוא אינו אירוע

אנחנו צריכים לשאול עד כמה הארגון תלוי בתקשורת, עד כמה הוא תלוי בכוח אדם ולבדוק את הרגישות של כל ההיבטים האלה להתקפות סייבר", כך אמר **אופיר זילביגר**, מנכ"ל SECOZ, שהנחה את מסלול העסקים בכנס CyberSec 2012.  
 לפי זילביגר, התקפת סייבר משפיעה על ההיבט העסקי, התפעולי והאנושי של הארגון. "סייבר זה לא רק אבטחת מידע. ניהול של סיכונים סייבר יושב על עולמות סיכון שונים בארגון. מתודולוגיות לניהול סיכונים נותנות כלים להבנת רוחב החשיפה והתייחסות לאירועים שיכולים להתרחש, וצריך לבצע הקשרים נוספים בין העוסקים בסייבר, כי סייבר זה לא רק IT", הוא אמר.  
**עו"ד אביב אילון**, מומחה לדיני מחשב משרד עורכי הדין אילון ושות', הזכיר שהדבר הכי חשוב שעסק יכול לאבד זה כסף. "למה חשוב לנו לדעת אם לנהל סיכונים או לא? קודם כל, כי זה יעלה לכם הרבה מאוד כסף. ב-2012 הוגשו שתי תביעות, אחת על סך 13.5 מיליון שקלים נגד ויזה כ.א.ל ואחת על סך 10 מיליון שקלים נגד PCgames, בגלל חשיפת פרטי המשתמשים בפרשיית כרטיסי האשראי. גם אם התביעות לא מצליחות, הדבר הראשון שעושים הוא לשכור עורך דין וזה כבר אומר שהפסדתם כסף".  
 לדברי אילון, "צריך לדעת לשאול את כל השאלות הנכונות. קודם כל תדאגו שאם מישהו יבוא ויעשה ביקורת תוכלו להראות שלא עצמתם עיניים, שיש טכנולוגיה ומודלים שאתם פיתחתם או קיבלתם ממי שפיתח אצלכם את מערכת האבטחה. תשאלו למה אתם חשופים מבחינת חוקי שמירת המידע ואחר כך תבדקו היטב איפה אתם מעורבים מבחינת מקומות של שיתוף מידע ואיפה המידע מסתובב, ותפתחו