משחקי החתול והעכבר יימשכו

איליאס חנטזוס, סימנטק: "המצב הגיאו-פוליטי של ישראל משפיע על כמות מתקפות הסייבר עליה" ◆ המתקפות הן על התשתיות הלאומיות של ישראל והן על ארגונים בה, הן תוצאה של המצב בו היא נמצאת, אמר חנטזוס, מנהל תחום ממשלה בסימנטק לאזור EMEA ◆ לדבריו, "מה שנדרש מישראל הוא לחנך את האוכלוסייה בנושא מתקפות סייבר ולהגן על עסקים קטנים בינוניים" ◆ לדבריו, "אי אפשר להגן על הכול; ניסיון להגן על הכול מביא להגנה על כלום"

יוסי הטוני

"ישראל מצויה מבחינה גיאו-פוליטית במצב 'מעניין' - וזה משפיע על כמות המתקפות עליה, הן ברמת המדינה ומוסדותיה והן ברמת הארגונים שבה. המתקפות הן גם ברמת התשתיות הלאומיות הקריטיות וגם ברמת הארגונים", כך אמר **איליאס חנטזוס**, מנהל תחום ממשלה בסימנטק לאזור EMEA (אירופה, המזרח התיכון ואפריקה).

חנטזוס שימש בשנים האחרונות נציגה של סימנטק במוסדות השוק האירופי המשותף, ובמסגרת זו עסק בבניית יכולות מגננת סייבר ברמה הלאומית לכמה מדינות, שאת שמותיהן סירב לפרט. כמו כן, הוא עסק ביצירת שיתופי פעולה ברמת אבטחת המידע בין מדינות שונות ובשיתופי מידע בין גורמים בתעשיית אבטחת המידע - סימנטק וחברות אחרות, ובין מדינות וגורמי אבטחה ממלכתיים של מדינות.

"לישראל יש יכולות לא מעטות בתחום מגננת הסייבר ואני יודע שהיא בונה עוד ועוד יכולות", ציין חנטזוס. "כעת, מה שנדרש ממנה, כמו גם ממדינות אחרות, הוא לחנך את האוכלוסייה ולהגן על עסקים קטנים בינוניים. זאת, כיוון שכשליש מהפריצות לארגוני הענק והתאגידים מתחיל בפריצות לשותפים וספקים הקטנים יותר, שעובדים עם הגדולים".

הוא הוסיף כי "לפני חמש שנים, הסייבר היה בעיה טכנולוגית. דוגמאות לכך הן המתקפות על אסטוניה ב-2007 ועל גיאורגיה ב-2008, והופעת הנוזקה סטוקסנט באיראן. כיום הוא הפך למיינסטרים, לנושא פוליטי מהמעלה הראשונה, לנושא שיחה של מנהיגים. אצל מדינות רבות, המגננה מפני מתקפות קיברנטיות היא בתעדוף הראשון, לפני מתקפות טרור או בעיות של חדירת מהגרים בקנה מידה נרחב. ניתן לראות זאת ביוזמות, בפעילויות ובמימוש תכניות תוך תקצוב הולם בכל העולם - בארצות הברית, בבריטניה ובאיחוד האירופי בכלל. בנאט"ו הוקם מרכז לניהול משברים למגננה מפני מתקפות סייבר. זו דוגמה לשיתוף פעולה בין מדינתי, שכל החברות בו נהנות ממנו. כמו כן, יורופול, משרד המשטרה האירופי, עשה דברים ממש טובים במלחמתו בפורנוגרפיה של ילדים ובמיגור רשתות בוטנט. בשנים האחרונות הוא פועל בצורה משולבת, תוך תיאום מודיעיני בין סוכנויות המשטרה האירופיות, בתחום הסייבר. שיתופי הפעולה הם כורח המציאות, כי המדינות מבינות שמה שקורה היום למדינה אחת יקרה לשכנתה למחרת".

איך מדינה צריכה להתגונן מפני מתקפות קיברנטיות?

"הגנה מפני מתקפות קיברנטיות היא לא לרכוש מוצר אבטחה א' ולהטמיע מוצר אבטחה ב'. מדובר על שילוב של אנשים, תהליכים וטכנולוגיה, ונדרש לטפל בכל שלושת הרכיבים. הטכנולוגיה לכשעצמה לא תועיל בעת מתקפה אם, לדוגמה, לא יטופל היבט חינוך האוכלוסייה.

"ברמה הלאומית, נדרש טיפול בשני מימדים. אחד מהם הוא הגנה על ממשל זמין ומגוון הפעילויות המקוונות של האזרחים, גם לא אלה שברמה הממשלתית, כגון שירותי בנקאות אלקטרוניים או זימון תורים לקופת חולים. זאת, תוך הבטחה שהשירותים הללו מסופקים ושמעטפת אבטחת המידע שנבנתה עליהם לא פוגעת בטיב השירות. המימד השני הוא הגנה על התשתיות הלאומיות הקריטיות. על הגורמים הממונים על האבטחה ברמת המדינה לבצע תעדוף: מה יותר חשוב - הבנקים או חברות הטלקום וספקיות האינטרנט? אם ספקית האינטרנט תיפגע, הבנקים לא יוכלו לתפקד. אם מערכת החשמל תקרוס, כמה זמן בתי החולים יוכלו לעבוד על גנרטורים. המדינה צריכה לבצע מיפוי יסודי של כלל התשתיות הלאומיות הקריטיות בה ולהחליט על תעדוף שלהן".

איליאס חנטזוס

היית מעורב בבניית יכולות למגננת סייבר ברמה הלאומית. מה נדרש לעשות בתחום זה?

"אשיב ברמה הגנרית. פיתוח יכולות נגד קיברנטיות דורש לבנות ארגון או להוסיף את היכולות הללו לארגון קיים. מדובר בבניית תהליכים, עם החלטה מי עומד בראש הפירמידה ומקבל החלטות. צריך להגיע למצב בו המדינה ערוכה מפני המתקפות וכשהן מגיעות, היא יכולה להכיל את האירוע, להגיב, לנהל ולצמצם ככל הניתן את הפגיעה - ובמהירות. יש לוודא מה נגנב. יש לברר האם הפריצה הייתה למטרות חבלה, משמע - פוליטית, או למטרת תועלת פיננסית.

"התעדוף הוא מילת המפתח. כיום כבר ברור שאי אפשר להגן על הכול. ניסיון להגן על הכול מביא להגנה על כלום. אחר כך יש לטפל במשולש: רכיבי מיחשוב-בקרת זהויות-מידע. הרכיבים הם הצלע הפחות חשובה במשולש.

"כמו כן, יש להיערך למצב שבו אתה יודע שתותקף, אבל אתה לא יודע על ידי מי, מתי ואיך. נדרש ניטור של מערכות ה-IT מסביב לשעון. יש להקים חדר מצב עם בניית תרחישים ולצידם סדרת תגובות".

"אנחנו מתמודדים כבר שני עשורים עם וירוסים", סיכם חנטזוס. "כעת הרעים עלו שלב. יש בכך גם מן החיוב, כי הנושא נכנס לשיח הפוליטי. יתרון נוסף, אציין בחיוך, הוא שאנחנו נמצאים בזירה טובה מבחינה עסקית. צפויות לנו עוד שנים רבות של עבודה".

מי ינצח בסוף - הטובים או הרעים?

"אני לא יודע ומקווה, כמובן, שהטובים. אני מעריך שמשחקי החתול והעכבר יימשכו, ועל כל יכולת מתקפה חדשה תיבנה יכולת נגד. תהליך נוסף שיקרה הוא הפיכת הסייבר לבעל ממדים צבאיים".