מעריב nrg

מי שולט במרחב הסייבר

תקיפת סייבר, כמו במקרים שישראלים תקפו אתרים בערב הסעודית, היא הפעלת כוח מסוכנת שצריכה להתבצע רק על ידי גורמים מוסמכים

גבי סיבוני | 13/2/2012 17:20

תגיות: מלחמת הסייבר

אירועי השבועות האחרונים העלו לראש סדר היום הציבורי את החשיפה של חברות ופרטים ישראליים לתקיפת מחשבים. אף כי היקף הנזק בתקיפות האחרונות היה מצומצם, הרי שאלה מצביעות על שאיפה גוברת של גורמים עוינים להרחיב את השימוש במרחב הסייבר נגד יעדים ישראליים.

הגדיל לעשות אחד מאנשי הדת המוסלמיים כאשר אמר שיש צורך לאחד את מאמצי התקיפה במסגרת תוכנית לג'יהאד אלקטרוני נגד ישראל.

בכל הנוגע לכושר ההגנה מפני תקיפת סייבר, ניתן לחלק את ישראל לשלוש קבוצות. הראשונה הינה ארגוני הביטחון: צה"ל, ארגוני קהיליית המודיעין וכדומה. הצורך של הארגונים להגן על הנכסים הביטחוניים מחייב אותם להשקיע משאבים רבים כדי למנוע אפשרות חדירה לא מורשית למערכות המחשוב והמערכות המבצעיות.

השנייה הינה תשתיות לאומיות קריטיות. זו כוללת סקטורים אשר פעילותם חיונית לתפקוד המדינה, לדוגמה אספקת חשמל, מים וכדומה. סקטורים אלה פועלים תחת הנחיה ובקרה של הרשות לאבטחת מידע. לאור זאת, ניתן להעריך שההשקעה המוסדרת והמכוונת של שתי הקבוצות האלה מצמצמת, אף אם לא מבטלת, את היכולת של גורמים עוינים לגרום נזק של ממש.

לא כך הדבר בקבוצה השלישית הכוללת את כל שאר משתמשי הרשת - ארגונים ועסקים. זוהי הקבוצה הפגיעה ביותר, שבה כושר ההגנה מפני תקיפת סייבר נקבע על ידי שיקולים עסקיים-כלכליים הנגזרים בדרך כלל משיקולי רווח והפסד בטווח הקצר.

באירוע התקיפה האחרון היו אלה בעיקר נזקים תדמיתיים, אולם אין ערובה לכך שהתקיפות הבאות לא יכוונו למערכות תפעוליות של חברות שהגנתן אינה מספקת ושהפגיעה בהן תהיה משמעותית יותר.

פעולה עצמאית של אזרחים הינה בניגוד לחוק

התקיפות האחרונות הציפו תופעה חמורה נוספת: אזרחים ישראלים תקפו בתגובה אתרים בערב הסעודית ופרסמו פרטי כרטיסי אשראי של אזרחים ערבים. תקיפות אלה קיבלו תהודה תקשורתית רבה. זאת בלי לתת את המשקל הראוי לחומרת התופעה ולהשלכות המסוכנות שלה על הביטחון הלאומי של מדינת ישראל.

יש להפנים את העובדה שתקיפת סייבר הינה הפעלת כוח לכל דבר ועניין, וככזו-היא עלולה לגלוש גם להפעלת כוח פיזי. הפעלה של כוח מורשה בחברה דמוקרטית יכולה להתבצע רק על ידי גורמים מדיניים מוסמכים. פעולה עצמאית של אזרחים הינה בניגוד לחוק.

חובה על רשויות המדינה למנוע אירועים כאלה בעתיד ולפעול בהקדם כדי לאכוף מרות על פרטים וקבוצות
הפועלים בניגוד לחוק.

התמודדות מדינת ישראל עם אתגרים אלה מחייבת פעולה בשלושה ממדים: הגנה, חקירה ותגובה. דומה שהדרך היעילה לשפר את כושר ההגנה של חברות וארגונים שאינם מוגדרים

כתשתית לאומית קריטית, הינה באמצעות השימוש בחוק רישוי עסקים, תוך קביעת מספר מדרגות לעסקים המחויבים לעמוד בדרישות הגנה מינימליות.

בצורה כזו לכל תחום עיסוק תיקבע רגולציה להגנה מחייבת בהתאם למדרג שנקבע. באשר לממד החקירה, כיום אין בנמצא גורם מוגדר שתפקידו לחקור אירועי תקיפה של אזרחים או חברות ועסקים. לכן ניתן להניח שאירועי התקיפה האחרונים לא נחקרו בצורה שיטתית על ידי גורמים המוסמכים לכך מתוקף תפקידם.

לא ברור מי האחראי

באשר לתגובה התקפית, לא ברור מי האחראי במדינת ישראל לקבוע את מדיניות התגובה ההתקפית ולהגיב (אם בכלל) לתקיפות כדוגמת האחרונות.

היעדרה של מסגרת הפעלת כוח (שאינה ביטחונית) בתחום הסייבר מייצר חלל שאליו נכנסים אזרחים הפועלים בצורה עצמאית ולא חוקית. החוסר במסגרת לאומית שתוכל לקבוע את מדיניות ההגנה, לחקור אירועים ואף להגיב להם במקרה הצורך, הינו בולט לעין.

המענה לצורך הזה יכול להינתן בכמה דרכים: הרחבת הסמכויות והמשאבים של הרשות לאבטחת מידע או של משטרת ישראל. המטה הלאומי לסייבר יכול אף הוא לרכז את הנושא ולהגיש המלצות. בכל מקרה, השארת המצב הקיים עלולה לגרום אובדן שליטה במרחב הסייבר.

הכותב הוא אל"מ במיל', ראש התוכנית ללוחמה קיברנטית במכון למחקרי ביטחון לאומי