45084378-9	11/2014	גלובס - כותרת	עמוד 23	1	10.55x31.27
טלדור מערכות מחשבים - 3710					

הקמת רשות הסייבר

/ אריה רימיני

טרור לכל דבר

ראש הממשלה בנימין נתניהו הכריז לאחרונה כי יקים רשות לאומית להגנה אופרטיבית בתחום הסייבר (רשות הסייבר). על־פי ההצהרה, מטרת הרשות היא "לחבר בין המרחב האזרחי לעולם הביטחוני". צעד כזה נשמע כנדרש וכחשוב. התקפות סייבר הן טרור לכל דבר ועניין; לכן, הטיפול בהן זה מעניינה ומאחריותה של המדינה. יחסית לגודלה, ישראל עומדת בפני התקפות רבות יותר מאשר מדינות אחרות בעולם. ההתקפות המאסיביות על ישראל נובעות הן בשל היותה מרכז מחלוקת מבחינה פוליטית־ביטחונית, והן גם בשל היותה מרכז פיתוח טכנולוגי מהמובילים בעולם. וכך ישראל, על הארגונים הביטחוניים והעסקיים שבה, היא מטרה עבור מדינות רבות, שחומדות את הידע שלה. על מנת לעמוד איתנים מול התקפות מצד מדינות וארגונים, יש לפעול ברמה הלאומית.

ניהול נושא הסייבר מאפשר למדינה להגיב במקומות שבהם ידיהם של הארגונים כבולות מבחינה כלכלית וחוקית. לעיתים, הגנות מסוימות ברשת דורשות גם פעולות המכוונות נגד ההאקרים המעוניינים לפרוץ אותה. הארגון כשלעצמו מוגבל, מפני שהוא כפוף לחוקי המדינה שאוסרים עליו להפעיל פעילויות שונות. זאת, להבדיל מיכולותיו של האקר אנונימי. לעומת זאת, מדינה יכולה להגן על עצמה בכל האמצעים. ממש כמו הגנה על גבולות יבשתיים וימיים, על מדינה לאתר ולהגדיר את הגבולות הדיגיטליים שלה, ולסכל כל סוג של חדירה לגבולה.

חרף הצהרתו של ראש הממשלה, אין בישראל כיום גוף לאומי בעל אחריות ביצועית על תחום הסייבר. הארגונים העסקיים לומדים את נקודות־החולשה של אבטחת הרשת שלהם בעקבות התקפות שכבר קרו, ומקימים חומות־הגנה פרטניות, בהון עתק, שאינן יכולות להגן עליהם באופן מלא מפני פרצות. בנוסף, עלויות עתק אלו, המושקעות בהגנה על הארגון, מועמסות על לקוחות החברות, ומקבלות ביטוי לדוגמה בעמלות הבנקים.

מדי שנה גדל הביקוש בארגונים לפרויקטים בתחום הסייבר ב־30%־50%. מספר זה צפוי לגדול עוד יותר, עקב העלייה ברמת התחכום של התוקפים, התואמת את התפתחות הטכנולוגיה. היות שבישראל לא קיימת הגנה כוללת ולא למידה ברמה הלאומית, כל ארגון נמצא לבדו במערכה. זהו מצב בעייתי מאוד, שכן איתנות לאומית וכלכלית, נמדדת גם באיתנות הגופים העסקיים שפועלים בה.

על רשות הסייבר שתוקם כעת, יהיה לקבל אחריות אקטיבית ולפעול בתחום הסייבר. בהיעדר פעולה מצידה, רשות זו תהפוך לעוד רגולטור ותו לא. דבר שלא יענה על הצורך להתמודד עם האיומים בתחום הסייבר. הגוף היחיד שיכול לתת מענה אופרטיבי בהגנה לאומית כוללת, מבחינה ביטחונית, אזרחית ועסקית כאחד, הוא גוף המורכב הן מהשב"כ והן מגופי התקשורת הפועלים כיום בישראל. שילוב היכולות של גופים אלה, יביא מצד אחד למיפוי מקצועי ומדויק של התחום, באמצעות הידע ומיקומו בתווך של חברות התקשורת והאינטרנט; ומצד שני, ליכולת לפעול ולהגיב, להגן ולסכל, באמצעות יכולותיו וחופש פעולתו של השב"כ.

על הגוף המשולב להקים מרכז בקרה ושליטה אשר ינטר את כל התקפות הסייבר על אזרחים וארגונים בישראל. כמו כן, עליו לפעול כמעין "משמר הגבול" במרחב הקיברנטי בשיתוף־פעולה עם ספקיות האינטרנט השולטות בשערי הגבול של רשת האינטרנט הישראלית. על ספקיות האינטרנט להיות מתואמות עם מרכז השליטה ובקרה כדי לדווח על כל ניסיון תקיפה של כל ארגון ואזרח כדי לאפשר הגנה אפקטיבית ורוחבית. ספקיות האינטרנט צריכות לתת הגנה לאזרחים ולארגונים מפני חדירות זדוניות, באופן שיספק מענה ל־70%־80% ממתקפות הסייבר, ולהותיר 20%־30% מההגנה על הארגונים עצמם.

ישראל היא מטרה עבור מדינות רבות, החומדות את הידע שלה. העלייה ברמת התחכום של ההאקרים דורשת גוף משולב של השב"כ וספקי התקשורת

הקמת רשות לאומית להגנה אופרטיבית בתחום הסייבר היא צעד מבורך והכרחי היום. נקווה כי רשות זו תשכיל להוציא את הדברים מהכוח אל הפועל. אי אפשר להמשיך לדבר רק ברגולציה. הגיע הזמן לפעול, להוביל, לקדם ולהגן אקטיבית מפני האיומים והמלחמות של ימינו. ●

הכותב הוא מנכ"ל טלדור