

קו התפר בין סייבר אזרחי לצבאי

האיומים הפיסיים והקיברנטיים שמרחפים מעלינו באחרונה, חייבים לחזק את שיתוף הפעולה בין המערכות האזרחיות והצבאיות ♦ ההבדל היחיד בין הסייבר הצבאי לסייבר האזרחי, הוא שהצבאי לא רק מגן על הרשתות הצבאיות - אלא גם יוזם ותוקף, בעוד שתפקידו של הסייבר האזרחי הוא להגן על הרשתות ולמנוע התקפות ואיומים שונים ♦ הצבא צריך לסייע לגופים האזרחיים להתגונן טוב יותר מפני איומי סייבר, ואילו התעשיות האזרחיות יכולות לסייע לצה"ל להיערך טוב יותר לעימות הבא

להגן על הארגון האזרחי מפני אסונות - ולא רק מתקפות סייבר. כפי שכבר נכתב במדור זה יותר מפעם אחת, במגזר האזרחי הפך הסייבר לשם קוד לכל נושא האבטחה וההגנה על המידע.

איציק מלאך - חבר הנהלת בנק לאומי ומפקד ממר"ם לשעבר, ויוסי שנק - מנמ"ד חברת החשמל, אמרו בכנס כי הגנה מפני סייבר אינה הגנה על תשתיות מיחשוב בלבד, אלא הגנה על מידע, שבהיבט הפיננסי הוא אחד הנכסים החשובים ביותר שיש לארגונים. שם המשחק הוא המשכיות עסקית: כאשר יש מצב חירום, תפקידה של המערכת הבנקאית הוא לאפשר המשך פעילות, כדי לא לפגוע בלקוחות. גם חברת החשמל יודעת היטב שפגיעה בתשתיות שלה, פירושה פגיעה אנושה בתשתיות המידע של מדינת ישראל - שהשבתתן פירושה שיבוש החיים במדינה. האויב הרי יודע היטב שלא חייבים טילים כדי לפגוע בישראל.

האם הסקטור האזרחי מסוגל להגן על עצמו מפני איום הסייבר לבד - ללא סיוע של גורמי צבא וממשלה? למרות שזו התפיסה ששולטת כיום, היו לא מעט דוברים בכנס שסברו כי הגיע הזמן לשנס מותניים ולהתחיל לעשות. גם בנק, רשת קמעונאית או בית מרקחת, יכולים להיות קריטיים בשעת חירום - והתאום ביניהם הוא צו השעה.

שיתוף הפעולה בין הצבא לסקטור הפרטי בא לידי ביטוי, בין היתר, בפתרונות הטכנולוגיים שצה"ל מאמץ כדי לתקשר את היחידות שלו. זה היה נושא שבו עסקו חלק גדול מהמרצים שהגיעו לאירוע מטעם החברות הטכנולוגיות הפועלות בשוק. הם הציגו פתרונות דטה-סנטר, תקשורת, מערכות שו"ב ועוד - שטובים גם למשימות צבאיות וגם לסקטור האזרחי, הן להמשכיות עסקית בשעת חירום והן להגנה מפני סייבר.

השורה התחתונה: האיומים הפיסיים והקיברנטיים שמרחפים מעלינו באחרונה, חייבים לחזק את שיתוף הפעולה בין המערכות האזרחיות והצבאיות. הצבא צריך לסייע לגופים האזרחיים להתגונן טוב יותר מפני איומי סייבר, ואילו התעשיות האזרחיות יכולות לסייע לצה"ל להיערך טוב יותר לעימות הבא.

יהודה קונפורטס

הכנס הלאומי לתיקשוב ולמגזר הביטחון, CSIsrael, אירח דוברים לובשי מדים לצד דוברים שהגיעו על אזרחי, אבל לבשו מדים בעברם, כל אחד בתקופתו, במשך שנים רבות. חלקם הגדול היה קצינים בכירים במילואים ביחידות הקשר והתקשוב. השילוב הזה, של צבא ואזרחות, היה אחד הנושאים המרכזיים בכנס, ובעיקר בהקשר לנושא שמעסיק אותנו יותר מכל באחרונה: הסייבר.

אמנם נהוג להפריד בין הסייבר הצבאי לבין זה האזרחי, אולם מרוב ההרצאות ניתן נהיה להבין, שההפרדה הזו היא טקטית - כי בסופו של יום הכל מתנקז לאנשים, לאזרחים, לעסקים ולתשתיות. ההבדל היחיד בין הסייבר הצבאי לסייבר האזרחי, הוא שהצבאי לא רק מגן על הרשתות הצבאיות - אלא גם יוזם ותוקף, בעוד שתפקידו של הסייבר האזרחי הוא להגן על הרשתות ולמנוע התקפות ואיומים שונים. אגב, היה מי שהציע בחצי חיוך לשבור את הפרדיגמה הזו, ולאפשר גם לסקטור האזרחי לבצע התקפות סייבר כלפי גורמי אויב.

את צה"ל ייצג ראש אגף התיקשוב, אלוף עוזי מוסקוביץ', שהייתה זו הופעתו הראשונה בפורום זה, בתפקידו כראש האגף. האלוף מוסקוביץ' הסביר למאות המאזינים שהגיעו כדי לשמוע אותו, כי התיקשוב הצה"לי מתייחס לסייבר ברצינות רבה, אולם היערכות אליו היא חלק בלתי נפרד מהיערכות לאיומים אחרים, שמשמעותה המשך העמקת חדירת מערכות המידע ליחידות הצבאיות, ובפרט לדרג הלוחם - ברמה הכי פרטנית. גם כאן שם המשחק הוא קישוריות.

האלוף אמר, שהחלום שלו הוא שהמ"פ בשטח יוכל לדבר בצורה מאובטחת עם הטייס שממריא למשימה מבצעית בגזרה שלו. אנחנו עדיין לא שם, אבל אין ספק שתנופת העשייה בשנים האחרונות, ותוכניות העבודה שהאלוף הציג, הפכו את הצבא ליותר דיגיטלי ויותר חכם.

איום הסייבר, הסביר האלוף מוסקוביץ', מבוסס על העדר ידע ועל חוסר היכולת לדעת מראש על ההתקפה המגיעה. על כן, המאמצים מתרכזים בהגנה מפני חדירות וביזום התקפות, כאשר התשתית האנושית היא חלק בלתי נפרד מהמלחמה הקיברנטית הזאת.

גם הדוברים האזרחיים באירוע התייחסו לפתרונות שונים, שנועדו

מחיישנים חיצוניים ופנימיים. "כיום יש מערכות שליטה ובקרה על מערכי התקשורת, על ה-T, על כוחותינו ועל האויב, אולם אין שליטה ובקרה לסייבר. זה האתגר - ליצור 'חדר מצב סייברי', שבו יוכלו להחליט אילו פעולות מיחשוב נדרש לעשות, תוך היתוך של המידע."

"אם פורץ יתאמץ עוד ועוד - בסוף הוא יצליח"

"אנו, בבנק לאומי, גורסים כי כאשר גורם כלשהו מבקש לחדור - אם הוא יתאמץ עוד ועוד, בסופו של דבר הוא יצליח. לכן, נערכנו ואנו ממשיכים להיערך על מנת להגביה את החומות ככל הניתן. לשם כך פיתחנו והטמענו יכולות הגנה", כך אמר **איציק מלאך**,



תטי אלוף (מיל) ארנון זו ארץ

מהם הוא העובדה שהטכנולוגיה ממשיכה לספק את היכולת לשפר את האפקטיביות המבצעית - משמע, שיתופיות בין-זרועית בין חילות היבשה, האוויר והים, בכל היבטי שיתוף חוזי ועבודה משותפת לאיתור ולפגיעה במטרות. זאת, על מנת לקבל את היתרון היחסי הטמון בכל זרוע וזרוע. "צה"ל טבע את המונח 'לדעת ראשון, להחליט ראשון, לפעול ראשון', וה-10 הוא זה שמקנה לו יתרון יחסי בשדה הקרב המודרני", אמר זו ארץ. "מנגד, הצבא פועל על בסיס המתווה של ועדת ברודט, שקבעה שעליו לצמצם את עלות הקיום השוטף שלו ולהפנות משאבים לבניין הכוח". הוא סיכם באמרו, כי נדרש לייצר תמונת מצב בזמן אמת, גם של עולם הסייבר, תוך קבלת נתונים