

השיח, כי "קיימים נושאים רבים שנדרש להתייחס אליהם בתחום הסייבר לפני שרוכשים כלים".

לדבריו, "נדרש ליישר קו בהיבט מדיניות האבטחה ועשיית סדר במגוון נושאים, שלכאורה אינם מתקשרים ישירות לעולם הסייבר, אך יכולים לעשות 'רעש', להשרות חוסר ודאות ואף להוות פרצת אבטחה, אם הם לא מנוהלים ולא נשלטים".



דניאל ברודנר

בין שאר הפעילויות של CA, אמר ברודנר, "אנחנו מתמחים בניהול זהויות והרשאות. הפתרון שלנו מאפשר שליטה בגישת המשתמשים דרך 'כספת סיסמאות' בצורה מאובטחת ומתועדת. בנוסף, המערכת מאפשרת הגנה נקודתית על מאגרי המידע הרגישים בארגון. CA מספקת כיסוי מקיף של הטיפול במשתמש, מרמת גרעין מערכות ההפעלה (Kernel) ועד הגישה המאובטחת לחשבון או ליישומים השונים במערכות ה-IT של הארגון. במסגרת הפתרון, המיועד לארגוני אנטרפרייז, ניתן לקבוע מדיניות אבטחת מידע ארגונית ולהפיץ אותה בלחיצת כפתור אחת לשרתים הרלוונטיים בארגון".

"אין לנו מספיק ידע על המתקפות הקיברנטיות"

"אין לנו מספיק ידע על המתקפות הקיברנטיות. עלינו להיערך להתקפה הבאה וחלק מההיערכות כולל מידע אודותיה", כך אמר **צביקה חורובסקי**, מנהל מגזר הביטחון בנס ישראל.

בהתייחסו לסייבר ואבטחת מידע אמר חורובסקי, כי "ישראל הינה מדינה עתירת טכנולוגיות. הפער הוא בידע לגבי המתקפה הבאה ולא זאת שהייתה. מקור הבעיה נובע מכך שהדברים אינם תלויים בנו. אנחנו חשופים ומזמינים התקפות, ואין לנו דרך להגיע לאלפי הבודדים והמתארגנים".



צביקה חורובסקי

הוא הוסיף, כי "המשק הישראלי נשען במידה רבה על עולם הסייבר, הן במגזרים הפיננסי והפרטי והן במערכות הביטחוניות. לכן, חייבים לראות את מתקפות הסייבר ברמה של בעיה לאומית. לשם כך אמנם הוקמו גופים לאומיים, אבל יש לקבוע אסטרטגיה לאומית

ללוחמה בעולם הקיברנטי. לכן, יש לשלב כוחות בין מגזר העסקי למגזר הביטחוני, למשל באמצעות הקמת מרכז שליטה ובקרה משותף, תוך תיאום ושיתוף ידע ברמה הלאומית". הוא ציין שמערכת שליטה ובקרה שכזו קיימת "באזרחות". חורובסקי הביא כדוגמה מערכת שליטה ובקרה לטיפול במפולות שלגים בשווייץ. "מיד עם היוודע אסון הטבע", אמר, "המערכת יודעת להפעיל את כלל גופי החירום הנדרשים ויכולה לתת למפקדים ולמנהלים בשטח תמונת מצב שכוללת את מיקומם ופועלם. על המגזר הביטחוני לבנות או לרכוש מערכת מקבילה לה".

לדבריו, במערכת הביטחון יש מאות אלפי משתמשים וכבר קיימות טכנולוגיות בשלות שיכולות לשמש את הארגונים הללו. חורובסקי אמר שהדבר נכון בעיקר בעולם הדאטה סנטר. "המטרה היא לייעל לא רק כדי לאפשר גידול של יותר חומרה, אלא לאפשר צמצום של ההוצאות הישירות; לאפשר להגדיל את יכולות הייצור על ידי הגדלת מרכז הנתונים; לאפשר שינוי תמידי של הטכנולוגיה לטובת מימוש של תהליכים עסקיים חדשים; להביא לשיפור האבטחה; ולספק יכולות ההתאוששות של מרכז הנתונים", הסביר. "בדרך זו ניתן להביא לשיפור איכות השירות ללקוח הסופי".

היבט נוסף בו הצבא נדרש לתת את הדעת, לדבריהם, הוא הצורך בתכנון המשכיות עסקית (BCP). הם אמרו, כי "צה"ל צריך לתעדף את המערכות השונות אותן נדרש לגבות ולשחזר. הבנקים כבר בוחנים את הנושא לעומק, וכעת, גם הצבא נדרש לביצוע פעולות דומות. צריך



עמרי הולצמן

לגבש את המסקנות הנובעות מהתוויית תכניות להמשכיות עסקית בטרם האסון ולא לאחריו".

עוד ציינו כרמי והולצמן, כי לענף הכחול יש יכולות בתחום ממשל, זו, יכולות הכוללות אפיון של התהליכים שנדרשים בטרם מימוש פרויקטים בתחום.

הפוטנציאל בהתייעלות אנרגטית

"מערכת הביטחון כולה נשענת על אמצעי תיקשוב המרוכזים ברובם במרכזי מיחשוב או בחדרי שרתים. בעולם זה, אפקטיביות מבצעית משמעה שרידות והתייעלות, שהם התוצר של התייעלות אנרגטית. בעידן של מחסור תקציבי, לא בטוח שמערכת הביטחון עיכלה מה גדולה הפוטנציאל לחיסכון בתחום זה, אם כי המודעות לכך בצה"ל גבוהה מאוד", כך אמר **שלום אביטן**, סמנכ"ל הטכנולוגיות של אלכסנדר שניידר. "כל קילוואט של עומס זו עולה למערכת הביטחון בין 8,000 ל-16 אלף שקלים בשנה, תלוי במידת היעילות האנרגטית של חדר השרתים", אמר



שלום אביטן

אביטן. "באולם שרתים בגודל של מגה-וואט, ויש לא מעט כאלה ואף גדולים יותר, מדובר על הוצאה כספית שנתית שנועה בין 8-16 מיליון שקלים, רק על סעיף החשמל. הכפלת הנתון ב-20 שנים ובכמות חדרי השרתים במגזר הביטחוני מביאה להבנת הפוטנציאל לחיסכון הגלום בתחום, כאשר

מדברים על תכנון והקמה של מרכז מחשבים חדש", הוסיף.

למרות הנתונים הללו, אמר, הרכישה של האמצעים המשפיעים על היעילות או אי-היעילות האנרגטית מבוצעת תוך דגש על חיסכון בהוצאה הראשונית ולא בהוצאות התפעול, שמהוות את המרכיב המכריע שבעלות הבעלות הכוללת (TCO). "בגלל מפרטי התכנון, משרד הביטחון מעדיף לחסוך 1,000 שקלים במחיר הקנייה במקום לחסוך עשרות אלפי שקלים לאורך שנים", אמר אביטן. "אולם, לצד זה, כאמור - המודעות בצבא לפוטנציאל החיסכון ברמה האנרגטית גבוהה מאוד, ללא ספק יותר מאשר במגזר האזרחי. עם זאת, הדרך בה נכתבים המפרטים, לצד הביורוקרטיה שבמערכת הרכש, לא מאפשרים לקצינים בעלי שאר רוח ויוזמה להוביל מהליכים מרחיקי לכת של חיסכון".

אביטן ציין ארבעה איומים בפניהם ניצבים הגורמים הביטחוניים: לוחמת סייבר, רעידות אדמה, EMP (פעימה, פולס אלקטרו-מגנטי, משמע - קרינה הנוצרת מפיצוץ אלקטרו-מגנטי, בעיקר פיצוץ גרעיני או אי יציבות, תנודות, של שדה), וכן איום מפני טילים או רקטות. "יש לאלכסנדר שניידר ידע רב באמצעי מיגון למרכזי מיחשוב מפני איומים אלה", ציין. ככלל, אמר, "התעשייה בארץ מצויה בראשית הדרך לבחינת האיומים הללו. ניתן להגיע לרמות מיגון גבוהות, ובהשקעה זעומה. ראוי שקברניטי המדינה יתנו את הדעת לתחום".

"ליישר קו בהיבט מדיניות האבטחה"

דניאל ברודנר, יועץ אבטחת מידע בכיר ב-CA ישראל, אמר ברב-