

שיתופיות וקישוריות בירוק זית

ארנון זו-ארץ, קבוצת אמן: "ה-IT מאפשר לצה"ל להיות צבא אחד, מבוסס שיתופיות וקישוריות" ♦ "אחד האלמנטים שמאפשרים זאת הוא היכולת של ה-IT שקיימת כיום לספק קישוריות ושיתופיות", אמר תא"ל (מיל) זו-ארץ, סמנכ"ל לקוחות המגזר הביטחוני בקבוצת אמן ולשעבר קצין קשר ותיקשוב ראשי של צה"ל ♦ "בנוסף, קיימת היכולת לספק תשתית רחבת פס, בעלת יכולת קצב ותקשורת מהירים, יחד עם מערכות מרובות יישומים, וכל זאת לצד אבטחת מידע ברמה גבוהה", ציין

יוסי הטוני

היתוך של המידע."

"חידרות לארגונים מצליחות ב-79% מהמקרים"

"הנחת העבודה היא שחידרות לארגונים מצליחות ב-79% מהמקרים. לכן, נדרש למפות את רשתות התקשורת והמחשבים בהיבט האיומים, לקבל עליהן 'בינה עסקית', על מנת לייצר הגנה טובה יותר", אמר **רועי חרמוני**, מנהל לקוח תיקשוב בסיסקו ישראל.

לדברי חרמוני, התפיסה של סיסקו דורשת שינוי התנהגותי בהיבט ההגנה ומדברת על איסוף נתונים הרצים על פני הרשתות, במטרה למפות את האיומים ולהיערך אליהם טוב יותר. הוא ציין שיש לסיסקו מרכז עצבים בתחום אבטחת המידע. "רוב תעבורת האינטרנט עוברת דרך ציוד של החברה ויש לנו חיישנים



רועי חרמוני

בכל העולם", ציין. "המידע על תעבורת הרשת מרוכז במרכז העצבים, שרואה תמונה עולמית של התקפות וסיכונים המתפתחים ברשת."

"על ארגונים להבין שסייבר זה לא פרויקט שעיקרו ברכישת מוצר זה או אחר", הוסיף חרמוני. "סייבר הוא גישת אבטחת מידע והגדרת מדיניות המוחלטות על כל מקטעי הרשת בהתאמה, המאפשרת גמישות ושינויים של סיכונים ואכיפות". לדבריו, "האתגר האמיתי בגיבוש תפיסת סייבר הוא ריבוי יצרני אבטחת המידע המוטמעים ברשת. יש לחלקם מנגנוני אבטחה שונים, חלקם סגורים להתממשקות חיצונית, חלקם מיושנים ועוד. עובדה זו מאוד מקשה על היכולת לקבוע מדיניות ולאכוף אותה ביעילות. אתגר נוסף הוא ריבוי צורות הגישה לרשת - למשל, רכזים קבועים וניידים, פיזיים ווירטואליים."

לאורך זמן, ציין, "לא יהיה מנוס מפתרון המורכב מעמדה רזה ומרוחקת, או כמה עמדות, שעובדות מול המחשבים המאובטחים במרכז הנתונים."

איחוד תשתיות תקשורת

בהיבט ההתייעלות, אמר חרמוני, החברה מובילה זה ארבע שנים את תפיסת איחוד התשתיות במרכזי המיחשוב, על בסיס תקנים. "איחוד תשתיות זה מאפשר חסכון מיידי בהוצאות כבילה ומחברים אופטיים יקרים, צמצום כמות ציוד התקשורת ב-50% על ידי איחוד מתגי ה-LAN וה-SAN למכונה אחת עם יכולות משולבות", אמר. הוא ציין ש"הטכנולוגיה אף מאפשרת איחוד מערכות הניהול והקטנת התקורה הדרושה בניהול שני מערכי תקשורת קריטיים בנפרד."

חרמוני נתן כדוגמה את הבית הלבן, שהשתמש במערכת שיחות ועידה בווידיאו במהלך המבצע לחיסול אוסמה בן-לאדן. לדבריו, "כמות

הטכנולוגיה התפתחה וה-ICT נמצא כיום במצב בו הוא מאפשר לארגונים, ובתוכם ארגוני ענק כצה"ל, להיות צבא אחד, מבוסס שיתופיות וקישוריות", כך אמר תא"ל (מיל) **ארנון זו-ארץ**, סמנכ"ל לקוחות המגזר הביטחוני בקבוצת אמן.

זו-ארץ, לשעבר קצין קשר ותיקשוב ראשי של צה"ל, השתתף ברב-שיח בנושא תיקשוב צבאי שהתקיים לקראת כנס C5Israel 2012. הכנס ייערך ב-18 ביולי במרכז הכנסים אווניו שבקריית שדה התעופה. מנחה רב-השיח היה **יהודה קונפורטס**, העורך הראשי של אנשים ומחשבים.



תא"ל (מיל) ארנון זו-ארץ

לדברי זו-ארץ, "יש כמה אלמנטים שמאפשרים להביא את הארגון להיות ארגון אחד, שלא כבעבר. אחד מהם הוא היכולת של ה-IT שקיימת כיום לספק קישוריות ושיתופיות. בנוסף, קיימת היכולת לספק

תשתית רחבת פס, בעלת יכולת קצב ותקשורת מהירים, יחד עם מערכות מרובות יישומים, וכל זאת לצד אבטחת מידע ברמה גבוהה."

הוא ציין, כי צה"ל פועל בשני וקטורים, שבחלקם הם מנוגדים. אחד מהם הוא העובדה שהטכנולוגיה ממשיכה לספק את היכולת לשפר את האפקטיביות המבצעית - משמע, שיתופיות בין זרועות 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-IT 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."

עלייה בחשיבות הסייבר

בשל הצורך ביציבות ובהמשכיות הפעילות של המערכות, ובראשון המערכות המבצעיות, עולה חשיבות המימד של הסייבר, לדבריו. "זהו המימד החמישי, שנוסף ליבשה, ים, אוויר וחלל", אמר. "בעולם הסייבר אין הבדל בין המוכנות של בנק, חברת חשמל או צבא. מדובר באותו איום, באותו עולם ובאותן דרכי התמודדות."

האתגר, אמר זו-ארץ, הוא לייצר תמונת מצב בזמן אמת, גם של עולם הסייבר, תוך קבלת נתונים מחיישנים חיצוניים ופנימיים. "כיום יש מערכות שליטה ובקרה על מערכי התקשורת, על ה-IT, על כוחותינו ועל האויב, אולם אין שליטה ובקרה לסייבר. זה האתגר - ליצור חדר מצב סייברי, שבו יוכלו להחליט אילו פעולות מיחשוב נדרש לעשות, תוך