

כיצד ליצור תמונת מצב לאומית לאירועי אבטחת מידע וסייבר

התפתחות הרשת והשימושים בה בשנים האחרונות הביאה לגידול בחשיבות של צוות תגובה לאירועי אבטחת מידע וסייבר, CERT - כך אמר שוקי פלג, מנהל מערך אבטחת המידע של ממשל זמין במשרד האוצר ומי שעומד בראש הצוות הרלוונטי בישראל ♦ לדבריו, "מטרת ה-CERT הלאומי היא לספק עדכון שוטף לציבור, לממשלה, למערכת הביטחון ולמגזר הרלוונטי על אודות אירועי אבטחה שקרו או צפויים לקרות"

יוסי הטוני

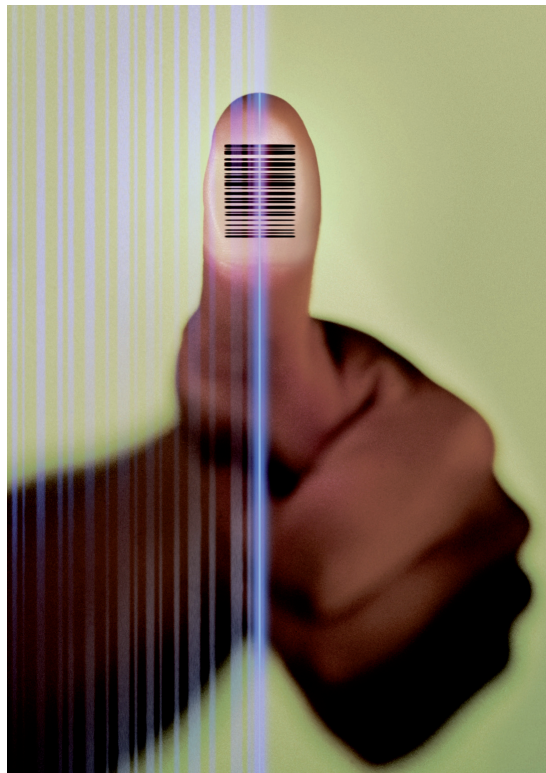
"יש ל-CERT הישראלי שיתופי פעולה עם ארגוני CERT בעולם, גופי בטחון בישראל, חברות טכנולוגיה ישראליות, האוניברסיטאות וגופי המחקר וכן עם מיזמים ממשלתיים, המטה הקיברנטי הלאומי וגופי CERT נוספים בארץ. המטרה היא להעשיר ככל הניתן את המידע ולשתף אותו בין הגופים", אמר.

פלג צופה, כי בעתיד יהיו גופי CERT מגזריים, למשל בתחומי האנרגיה, המים, החשמל, גופי CERT שח ספקיות תקשורת ואינטרנט, במגזר הפיננסי ובקרב המכללות והאוניברסיטאות מעליהם יהיו, לדבריו, ארבעה גופי CERT - תשתיות לאומיות, אזרחי, אקדמי וממשלתי - ומעליהם יהיה ה-CERT הלאומי. "בעבר, ה-CERT הממשלתי הפעיל מערכות אבטחת מידע להגנת רשתות, שרתים וקישורי אינטרנט של משרדי ממשלה", ציין פלג. "כיום הוא עוסק בסיוע לתכנון מערכות המטפלות באבטחת מידע ובהגנה על הפרטיות, לצד מניעת כוונות זדוניות. הדבר נעשה על בסיס ניטור מתקדם, יכולות מניעה ויכולות התאוששות. היעד, שמימושו כבר מתחיל, הוא להיות חוליה מקשרת בין אזרחים ועסקים, כשה-CERT הלאומי יהווה מצרף של כל המגזרים, תוך שיתוף מידע רב ככל האפשר".

SOC-I SIEM

אופיר זילביגר, מנכ"ל SECOS, ציין שהחברה עוסקת מזה יותר מעשור בבניית מערכי ניהול אבטחת מידע וניהול אירועי אבטחה, SIEM (Security Information and Event Management) וכן בבניית SOC (Security Operation Center) - מרכז תפעול אבטחת מידע בארגונים. לדברי זילביגר, "התהליך הינו מורכב וכולל כמה מרכיבים, כאשר סביבם יש שני מערכים - SIEM טכנולוגי ו-SOC המשמש כמערך ארגוני. השלבים הם: הגדרת היעדים שנדרש לממש בעת בניית המערכים הללו; ניתוח חוקים עסקיים על בסיס סיכונים; בניית פרופיל שימוש; חיפוש חוקים על פני השטח; בחירת טכנולוגיה ריאלית תוך מימוש ראייה כוללת; ולבסוף - מימוש בפועל".

חשיבות ה-CERT (Computer Emergency Readiness Team), צוות תגובה לאירועי אבטחת מידע וסייבר, גדלה בשנים האחרונות בשל התפתחות הרשת והשימושים בה. נדרש ליצור תמונת מצב לאומית לאירועי אבטחת מידע וסייבר, כך אמר **שוקי פלג**, מנהל מערך אבטחת המידע של ממשל זמין במשרד האוצר. לדבריו, תמונת המצב הלאומית תיווצר מחיבור חלקי הפאזל של גופי התגובה השונים במגזרי המשק השונים.



פלג דיבר בפני פורום CISO של אנשים ומחשבים, שהתכנס במלון שרתון בתל אביב. מנחה המפגש היה **אבי וייסמן**, מנכ"ל שיא סקויריטי. "מטרת ה-CERT הלאומי היא לספק עדכון שוטף לציבור, לממשלה, למערכת הביטחון ולמגזר הרלוונטי אודות אירועי אבטחה שקרו או צפויים לקרות, דוגמת מתקפות עתידיות או נזקות", ציין פלג, שעומד בראש הצוות. הוא הוסיף ש"ה-CERT הלאומי הוא הגורם המתווך בין ציבור המשתמשים לגופי אבטחת המידע העוסקים בתחום בשגרה ובחירום". פלג ציין, כי מדי שבעה מפיצים אנשי הצוות דו"ח אירועי אבטחת מידע לממשלה. התפקידים אותם עושה גוף התגובה, אמר פלג, הם היערכות לשינויים טכנולוגיים, איתור אירועי אבטחה, לדעת איך לטפל בהם, במידה שקרו, וכן לנתח ולשנות התנהגויות בעקבות אותם אירוע.

כיום, הוסיף, גוף התגובה הלאומי משמש זרוע בפועל של משרדי ממשלה בממשל זמין, אולם "זה ישתנה וה-CERT הלאומי יהפוך לצוות תגובה לאומי, עם יכולות שיתוף מידע דו-כיווניות לכלל הגורמים". הוא ציין, כי קיים בארץ CERT נוסף, זה של מחב"א (ר"ת מרכז חישובים בין אוניברסיטאי), והוא אחד הגופים הרלוונטיים הראשונים בעולם בתחום האקדמיה. "עם זאת", אמר פלג, "לא נערך כיום שיתוף פעולה בין שני הגופים ויש לשנות מצב זה". לדבריו, מספר גופי התגובה הללו בעולם עומד על כמה מאות וחלקם מאוגדים תחת מסגרות-על-של הגופים המערביים, הערביים והאסייתיים.