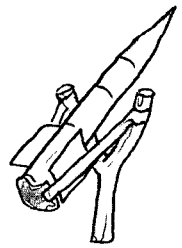

אמצעים נגד איומים של לוחמת־מידע

אל"מ (מיל') יעקב צור

לנוכח הדאגה השוררת במשרד ההגנה האמריקני מפני האיומים הגוברים הקשורים בלוחמת מידע, הוחלט שם על נקיטת צעדים שונים. צבא, שפעילותו תלויה במידה רבה בתפקודם של המחשבים ורשתות התקשורת, מוצא את עצמו חשוף יותר ויותר לתקיפה בתחום הזה, והתקיפה הזאת עלולה לשבש את תפקודו התקין, בכל הרמות, החל מרמת הלוחמים ומערכות הנשק, עבור דרך מערכות המודיעין ואמצעי השליטה והבקרה, וכלה בפיקוד הבכיר ביותר. מאמר זה ידון באמצעים שנוקט צבא ארצות־הברית כדי לקדם את פני הסכנה.

רמת מערכות הנשק

במשרד ההגנה הוקם ב־1995 "צוות אדום" (Red Team), המתמחה בתחום לוחמת המידע. תפקידו של הצוות לבחון מערכות ממוכנות חדשות, הנמצאות בפיתוח מבחינת ההיבט של חסינותן מפני מתקפה מסוג זה. נגד המערכות האלה מפעילים אנשי הצוות שיטות תקיפה וירטואליות, כדי לגלות בהן נקודות תורפה. הצוות הזה מרחיב כעת את שורותיו, ומוקמים צוותי־משנה, שיאפשרו להגביר את קצב הבדיקה של המערכות. נוסף על הצבעה על נקודות תורפה מציע הצוות פתרונות. הצוות משתמש במגוון שיטות תקיפה — הן בשיטות מסורתיות של לוחמה אלקטרונית והן בשיטות לא־שגרתיות וחדשניות בתחום לוחמת המחשבים. מובן, ששיטות הפעולה של אנשי הצוות

> צבא שפעילותו תלויה במידה רבה בתפקודם של המחשבים ורשתות התקשורת, מוצא את עצמו חשוף יותר ויותר לתקיפה בתחום הזה, והתקיפה הזאת עלולה לשבש את תפקודו התקין, בכל הרמות

חסויות, אך ידוע, כי רוב הציוד המשמש אותו נרכש בצורה מסחרית רגילה.

בחינה יסודית של מערכת נמשכת כשישה חודשים והעלות שלה היא בין 300 ל־500 אלף דולר. לא כל נקודת תורפה שמתגלית מחייבת פתרון טכני. לפעמים נמצא פתרון מבצעי על־ידי שיפור שיטות התפעול של האמצעי, ולפעמים ההערכה היא, שהסיכוי שהתוקף יפגע במערכת באמצעות נקודת התורפה הזאת הוא נמוך, ולכן מומלץ לא לשנות דבר. המטרה העיקרית היא לגלות ולהגדיר במדויק את נקודות התורפה החמורות, שחובה לטפל בהן. במקרה כאלה יש להוסיף לעיתים תקציב לפרויקט משום שבתוכנית המקורית אין כיסוי הולם לטיפול בבעיה שהתגלתה.

התקציב השנתי של "הצוות האדום" הוא מיליארד דולר. בתחילה, אנשי הצוות לא התקבלו תמיד בשמחה על־ידי מנהלי הפרויקטים, אולם לאחרונה יש הכרה בכך שמטרתם לסייע, ולא להציב קשיים, וקיימת נכונות רבה יותר להזמינם לשם בדיקת פרויקטים.

תקשורת בין מחשבים

במשרד ההגנה מוקמת תשתית הצפנה חדשה לאחר שהסתבר שוב ושוב, כי מערכות ההצפנה הקיימות, המשרתות משתמשים רבים ברשת, ניתנות לפריצה בקלות יחסית על־ידי מומחים. פיתוחה של המערכת הזאת (Public Key PKI – Infrastructure) יימשך כמה שנים, והעלות שלה לא פורסמה.

המערכת תכלול כמה רמות של הצפנה, שהגבוהה שבהן תתאים לתשדורות בסיווג "סודי ביותר". הטכנולוגיה הזאת תופעל ברשתות השונות של תקשורת מחשבים הן אלה הפנימיות (אינטרה־נט) והן אלה החיצוניות. המשתמשים השונים יקבלו הרשאות ברמת הסיווג ההולמת כל אחד מהם. הצדדים המוסרים והמקבלים מידע ברשת ישתמשו בקוד זיהוי לפני שישגרו מידע. הקוד ישמש כמעין חתימה אלקטרונית, וימנע דליפת מידע למי שאינו מורשה לקבלו.

מחשבים

רוב משתמשי המחשבים אינם מודעים לעובדה, שניתן לקלוט ממרחק, באמצעות ציוד מתאים (אמנם יקר מאוד), את המידע שמופיע על הצג שלהם. הדבר נעשה על־ידי קליטה של קרינת הרדיו הנפלטת מהצג ועיבודה לצורך שחזור המידע. התופעה מוכרת בשם Tempest Radiation, וארגונים שונים משקיעים כספים רבים כדי להתגונן נגדה. עד כה הדבר נעשה בעיקר באמצעות חומרת מיסוך וללא הצלחה יתרה.

לאחרונה הציעו מדעני מחשב מאוניברסיטת קיימברידג' דרך חלופית, באמצעות תוכנה ולא על־ידי חומרה. הרעיון התחיל דווקא מכיוון שונה — החוקרים ניסו להציע לחברת "מייקרוסופט" דרך להילחם במעתיקי תוכנה על־ידי כך שהצגים ישדרו

רוב משתמשי המחשבים אינם מודעים לעובדה, שניתן לקלוט ממרחק, באמצעות ציוד מתאים (אמנם יקר מאוד), את המידע שמופיע על הצג שלהם

במכוון את המספר הסידורי של התוכנה שבשימוש, וניידות מיוחדות יסיירו ברחובות ויאתרו את המשתמשים הפירטיים. מאוחר יותר הוביל המחקר לפתרון אפשרי להגנה מפני ציתות מרחוק לצגי המחשבים. החוקרים שמו לב, שהאותות הנפלטים מהמסכים הם בתדר גבוה — מעל 30 מגה־הרץ, והם פיתחו שיטה לסינון ולשינוי התדרים הגבוהים, כך שהאותות ייקלטו על־ידי המצותת בצורה מעוותת ובלתי ניתנת לשחזור. לאחר מכן פיתחו שיטות משוכללות נוספות, המבוססות על הוספה מכוונת של אותות, הגורמים לקליטה משובשת של המידע. ייתכן שיש בשיטות אלה צעד משמעותי בהתגוננות מפני דליפת מידע ממחשבים ומפני נפילתו לידי גורמים עוינים.

ביבליוגרפיה

Defense News, February 15, 1999, p. 28.

Defense News, January 11, 1999, p. 3

Scientific American, December 1998, p.21.