

הכלל מחוץ לגבולות הצבא, על מנת לקדם את הנושא של חמש יחידות סייבר בתלמידי תיכון. זאת לצד קידום פרויקט 'מגשימים', שהצריך עזרה פיזית של אנשי מטה הסייבר הצבאי. הם עשו זאת מטעמי ציונות בלבד."

וייסמן המשיך בדברי השבח. "הגוף השני שלו אני רוצה להודות הוא משטרת ישראל. קראתם על מה שהמשטרה עשתה בדארקנט, זו עבודת פרך. זו עבודה מבריקה שכוללת את לכידתם של אנשים מושחתים, סוטים וגנבים. על זה אני רוצה לומר למשטרת ישראל כל הכבוד."

"הטכנולוגיה מגיעה מהעובדים"

"מערכות לניהול התקנים ניידים הן כיום חלק ממערך אבטחת המידע הארגוני ואסור לוותר עליהן", כך אמר **יניר בן נון**, מנהל מכירות ניהול ואבטחת מכשירים ניידים בחברת אינפורמט. הוא נימק זאת בכך ש"אנחנו נמצאים בעידן שבו אנשי ה-IT כבר לא דוחפים טכנולוגיה לארגון אלא הטכנולוגיה מגיעה מהעובדים, שמחליפים טלפונים, מחשבים וטאבלטים בקצב מטורף, מביאים את המכשירים לארגון ומעמיסים אותם במידע שלו"

הוא ציין שבחמש השנים האחרונות גדלה מכירת המכשירים החכמים פי 10 - מ-120 מיליון מכשירים ב-2007 ל-1.2 מיליארד אשתקד - וש"רבים מהם משמשים לעבודה ולגישה למידע הארגוני". לדבריו, "העובדה שהעובדים יהיו זמינים ויוכלו לתת מענה מחוץ לארגון נשמעת רעיון מעולה, אבל יש בכך לא מעט סיכונים שלא



יניר בן נון

נותנים עליהם את הדעת ושצריכים לקחת אותם בחשבון כשמאפשרים למשתמשים לשים מידע ארגוני על המכשירים שלהם". בין אותם סיכונים מנה בן נון "גניבה או איבוד של מכשיר כאשר כל המידע הארגוני חשוף; רוגלות ווירוסים שעלולים לשאוב מידע וסיסמאות מהמכשיר; יישומים מתחזים שנטען שהם עושים משהו אחד ובפועל עושים משהו אחר; פרסומות מתחזות המובילות לקישורים שמכילים קוד עוין; רשתות אלחוטיות מתחזות, שבעליהן פורצים למכשירים המחוברים לרשת וגונבים מידע; סיכון שגלום בארנק הדיגיטלי, שללא הגנות מתאימות עלול לעלות לארגון ולמשתמש הרבה כסף; ואפילו כספומטים מתחזים". עוד אמר בן נון, ש"כדי להגן על המידע הארגוני על הארגונים להחזיר את השליטה אליהם ולרכוש מערכות התקנים ניידים. יש כיום 60 חברות שמציעות פתרונות בתחום, מסוגים שונים. אין פתרון קסם שמתאים לכולם. זה משהו שתלוי במדיניות החברה וצריך לקחת זאת בחשבון בעת בחירת הפתרון". הוא פירט וציין ש"על הפתרון שייבחר לאפשר שימוש גמיש ונוח עם המכשיר, למזער את הגישה למידע רגיש, לכלול מדיניות סיסמאות והצפנת התיווך, לחסום גישה ולמחוק מידע מהמכשיר במהירות, גם אם הוא לא מחובר לרשת, לקבוע תנאים בהם ניתנת למכשיר האפשרות להתחבר למידע ולקבוע מדיניות למניעת דליפת מידע."

"להקשיח את הציוד כדי להתמודד עם מתקפות סייבר"

אדי אלמר, סמנכ"ל פיתוח עסקי בחברת Wave, הציג מערכת לניהול טאבלטים מבוססי חלונות 8. לדבריו, Wave מעדיפה לעבוד עם סביבת



משה מורדגשטרן

את המחשב הפורט שלו ננעל תוך 12 שניות - הדברים פסקו באופן מיידי", הסביר. לדבריו, "בינתיים XOR התפרקה ובפרק זמן מסוים נשארנו בלי תמיכה. למזלנו, אורן הלוי - יוצא חברת XOR ובעלים של Wise-Mon - קנה את הזכויות של מוצר ה-SWAT תוך התחייבות לשמור את המוצר ולהמשיך לתת שירות ברמה גבוהה".

הוא המשיך ואמר, כי "הלוי וצוותו חזרו לצוות חברת החשמל, נכנסו לאתר, יישרו קו והעמידו את המוצר בחזית התחום. במהלך שנת 2010 נחתם הסכם ארוך טווח למתן שירותים ותמיכה במוצר, כשברקע קיימת דרישה של גורמי אכיפת אבטחת מידע בחברה, כמו גם דרישות בשוק, לשדרג את המוצר כך שיתאים לדרישות האבטחה של היום. הלוי הצליח לעזור לנו לערוך את התאמת ציוד הקצה - הגענו למצב שאנחנו יכולים לדבר עם כל ציוד קצה שמחובר לרשת התקשורת, לרבות כל הציוד של סיסקו וג'וניפר, מחשבים, שרתים, מדפסות, שעוני נוכחות, מכונות אוכל ומסופונים של קוראי מונים, שגם להם פוטנציאל להחדרת וירוסים לרשת. הטמענו את מנוע התאימות לרגולציות של Wise-Mon, וכך אנו מפעילים ברשת מוצר NAC מלא".

ניתוח קוד לגילוי פגיעויות

מתי סימן, מנהל טכנולוגיות ב-Checkmarkx, הציג את מערכת ניתוח קודי התוכנה כדי לגלות פגיעויות. במערכת מתוארת כל אפשרות למתקפה, זאת בעזרת תרשים זרימה שמסביר כיצד הקוד העוין פוגע.



מתי סימן

המערכת בוחנת את כל הפגיעויות הללו. לעתים קרובות היא מגלה שאותה שורת קוד היא שגורמת לרבים מהן - וכך ממקדת את פעולת המתכנתים.

"תודה למשטרה"

אבי וייסמן, מנכ"ל See Security ויו"ר הפורום הישראלי לאבטחת מידע, הקדיש את הרצאתו למתן ציון לשבח לכמה מהגופים העוסקים באבטחת מידע ביום יום. "אני מבקש להגיד תודה למטה הסייבר הצה"לי על פעילות יוצאת מן



אבי וייסמן