

הכלל מוחזק לגבולות הצבא, על מנת לפחות לפזר 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".

וישמן המשיך בדבריו השבח. "הגוף השני שלו אני רוצה להזכיר הוא משטרת ישראל. קראתם על מה שהמשטרה עשתה בדארקנינג, זו עבودת פרך. זו עבודה מבריקה שכוללת את לכידתם של אנשים מושחתים, טוטמים וגבנים. על זה אני רוצה לומר למשטרת ישראל כל הכבוד".

### "הטכנולוגיה מגיעה מהעובדים"

"מערכות לנויה התקנים נידים הן כולם חלק ממערך אבטחת המידע הארגוני ואסרו לוותר עליון", כך אמר **יירן בן נון**, מנהל מכירות הchn מרכז מושגים. הוא נימק זאת בכך כי ניהול ואבטחת מכשירים נידים בחברת אינפומט. הוא נימק כי "אנו נחננו ונמצאים בעידן שבו אנשי ה-IT כבר לא דוחפים טכנולוגיה לארגון אלא הטכנולוגיה מגיעה מהעובדים, שמהליפים טלפונים, מחשבים וטאבלטים בקצב מטורף, מביאים את המכשירים לארגון ומעמיסים אותם במידע שלו".

הוא ציין שבמחשש הchn האخرונות גדרה מכירת המכשירים החכמים פי 10 - מ-120 מיליון מיליארד ב-2007 ל-1.2 מיליארד אשתקד - ו"רבים מהם משמשים לעובדה ולגישה למידע הארגוני".

לדבריו, "העובד שהעובדים יהיו זמינים וככלו לתת מענה מוחזק לארגון נשמעת רעיון מעוללה, אבל יש בכך לא מעט סינוונים שלא



יירן בן נון

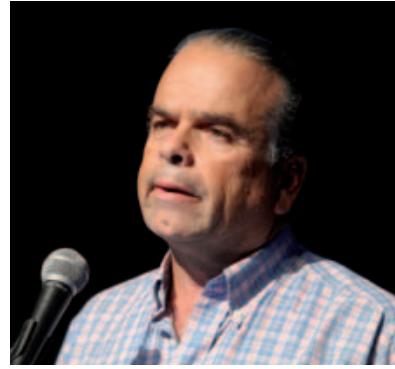
נותנים עליהם את הדעת ושציריכים לקחת אותם בחשבון כפתרונות למשתמשים לשימוש מידע ארגוני על המכשירים שלהם". בין אותם סינוונים מהן נון "גנבה או איבוד של מכשיר או אשר כל המידע הארגוני; חסוף; רוגלוות וירוסים שעולמים לשאוב מידע ו시스템אות מהמכשיר; ישומים מהזרים שנשען בהם עושים משהו אחד ובפועל עושים משהו אחר; פרסומות מתחזות, שבעליהם פורצים למכשירים המוחברים לרשות אלחוטיות מתחזות, סיכון שלגים בארכון הדיגיטלי, שלא הגנות מתאימות וגונבים מידע; סיכון שלגים ולשימוש הרובה כסף; ואפקיל כספומטים מתחזים".

עוד אמר בן נון, ש"כדי להגן על המידע הארגוני על הארגונים יש כוון להחזיר את השליטה אליהם ולרכוש מערכות התקנים נידים. אין פתרון קסם 60 חברים שמצוינות פתרונות בתחום, מסוגים שונים. אין פתרון קסם שמתאים לכלום. זה משווה שתלו במדיניות החבורה וצריך לקחת זאת בחשבון בעת בחרית הפתרון". הוא פירט וציין "על הפתרוןшибחר לאפשר שימוש גמיש ונוח עם המכשיר, למזער את הגישה למידע דריש, לכלול מדיניות סיסמאות והצפנה התווין, להסיט גישה ולמחוק מידע מהמכשיר במהירות, גם אם הוא לא מחובר לרשת, לקבוע תנאים בהם ניתנת למ哂יר האפשרות להתחבר למידע ולקבוע מדיניות למניעת דליפת מידע".

### "להקשייח את הציד כדי להתמודד עם מתקפות סייבר"

**אדֵי אלמור**, סמנכ"ל פיתוח עסקית בחברת Wave, הציג מערכת לניהול טאבלטים מבוססי חלונות 8. לדבריו, "Wave מעדיפה לעבוד עם סביבת

את המחשב הפרט שלו ונעל תוך 12 שנים - הדברים פסקו באופן מייד", הסביר. לדבריו, "ביןתיים XOR התפרק ובערך זמן מסוים נשארנו בלי תמייה. למזלנו, אורן הלוי - ייצא חברה XOR ובבעליהם של Mon - קנה את הזכיות של מוצר ה- SWAT תוך התchingות לשמר את המוצר ולמשר לחתה שיטות ברמה גבוהה".



משה מורגנשטרן

הוא המשיך ואמר, כי "הלו וצוותו חזו לצוות חברת החשמל, נכנסו לאלה, יישרו קו והעמידו את המוצר בחזית התהום. במהלך שנת 2010 נחתם הסכם ארוך טוח למתן שירותים ותמיכה במוצר, כשברקע קיימת דרישת של גומי אכיפה אבטחת מידע בחברה, כמו גם דרישות בשוק, לשדרוג את המוצר כך שתיארים לדרישות האבטחה של היום. הלו הצליח לעוזר לנו לעזרן את התאמת ציוד הקצה - הגענו למצב שאנו חנו יוכלים לדבר עם כל ציוד קטן שמחובר לרשות התקשות, לרבות כל הציוד של סיסקו וג'ונייפר, מחשבים, שרתים, מדפסות, שעוני נוכחות, מכונות אוכל ומסופונים של קוראי מונחים, שוגם להם פוטנציאלי להחדרת וירוסים לרשota העמנו את מנוע התאמיות לרוגლציות של Wise-Mon, וכן אנו מפעלים בראש מוצר NAC מלא".

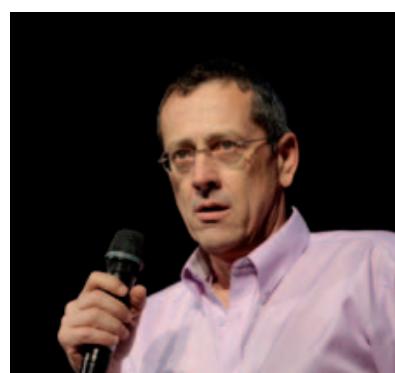
### ניתוח קוד לגילוי פגיעויות

**מוני סימן**, מנהל טכנולוגיות ב-Checkmarkx, הציג את מערכת ניתוח קודי התוכנה כדי לגלוות פגיעויות. במערכת מתואמת כל אפשרות למתקפה, זאת בעזרת תרשימים זורמה שմסביר כיצד הקוד העוין פוגע. המערכת בוחנת את כל הפגיעה הלא. לעיתים קרובות היא מגלה שאוותה שורת קוד היא שגורמת לריבים מהן - וכך מקדמת את פעולות המתכנתים.



מוני סימן

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



אבי וייסמן