

מערכות נשק ושליטה נחשפות לעיוותי מידע, השבתה או מניעת שירות. אבטחת מידע היא רכיב חשוב אך חלקי במארג המגוון של האמצעים והיכולות בהגנת המערכת.

ברט אמר עוד כי "התפיסה ההגנתית צריכה להיות רב מרחבית, שיוצרת את המגננה הקיברנטית. המשימה במגננה הקיברנטית היא לאפשר המשך פעולה רציף ותקין של נכסים ומערכות שירותים לקיומה של המסגרת המתגוננת. איך עושים זאת? יש כמה אתגרים: אחד איתור של האיום מוקדם ככל האפשר, זיהוי וקטורים רב מרחביים וקבלת החלטות נכונות במרחב".

"המשימה היא לתת בידי המנהיגים את היכולת לדעת, להחליט ולפעול" סיכם ברט. לדבריו, המענה לאיום הקיברנטי הוא "מענה דיסציפלינארי, השומר על נכסי הארגון והמשאבים שלו, ונעזר במודיעין".

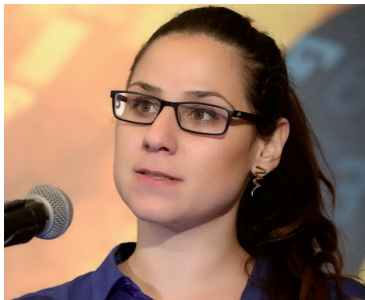
ניצנים ראשונים של תקיפות מכשירים ניידים

"מערכות מיחשוב שמטפלות בנושא הביטחון יהיו בין הנושאים שיעסיקו את עולם האבטחה ב-2014. זאת, לצד הגברת המודעות לשמירה על הפרטיות, התקפות על מערכות פיתוח תוכנה, התקפות על מכשירים ניידים וכמובן - נושא הסייבר", כך אמרה בכנס **איילת סאחנתו**, מומחית לאבטחת מידע.

לדבריה, "המתקפות על המובייל יהיו לא רק ברמת הארגון אלא גם מתקפות על מכשירים אישיים של משתמשים, שרבים מהם לא מודעים לסכנות. אנחנו רואים כבר ניצנים ראשונים של התקפות כאלה".

"2013 הייתה מעניינת",

סיכמה סאחנתו את השנה. "עסקנו בה רבה בתחום הסייבר ושמענו על אתגרים במגמת ה-BYOD. אם נאפיין את התחזיות לשנת 2014, הרי ללא ספק זו תהיה שנת ההאקינג - לא רק על תשתיות אלא על כל המערכות משובצות המחשב. למעשה, שום



איילת סאחנתו

דבר לא יהיה מוגן". היא ציטטה דו"ח של גרטנר לפיו "לא משנה מה תעשו, היכן שיש כסף ינסו לפגוע בכך, היכן שיש מידע תמיד יימצא מישהו שיאתר את החולשות והנוזקות שלכם".

"יש להגן על הקובץ - באמצעות הפלטפורמה"

דובר נוסף בכנס היה **יוסי שני**, יועץ לאבטחת מידע, שדיבר על החשיפה הבלתי מוגבלת כמעט של קבצי מידע ויישומים שאנחנו משתמשים בהם יום יום למתקפות קטלניות, מבלי שאיש ירגיש.



יוסי שני

"הקובץ הוא יחידת המידע שעליה יש להגן", אמר. "הוא יכול להכיל מידע רגיש ואחת המטרות של תקיפה על רשת היא לשים יד על המידע הזה". הוא הדגים פריצת יחידות מידע תמימות לכאורה באמצעים שזמינים באינטרנט. "בין היתר, ניתן למצוא מפענח אותות וידיאו שמתקן

בתוך כבל מסך ומאפשר לקרוא את כל הקבצים שיש על הצג, שניתן לרכישה ב-30 דולר בלבד. אמצעים יקרים יותר הם מערכות להשתלטות

האיומים הולך ומשתנה, אמר שנהב, היא הנוזקה פליים, שבחינת התפוצה שלה העלתה כי לאחר השכיחות הרבה ביותר, באירן, היו ישראל והרשות הפלסטינית בעלי השכיחות השנייה בתפוצתה.

מגמה נוספת שתורמת אף היא לגידול באיומים, אמר שנהב, "היא ההסתמכות על הטלפונים הסלולריים כאמצעי זיהוי. שילוב זה, של פתיחת הארגונים ליותר מערכות, לצד ההסתמכות על הסלולר כאמצעי זיהוי, כאשר מנגד יש עלייה תלולה בכמות נוזקות שבסלולר - היא בפירוש קריאת השכמה לארגונים. חלה עלייה מדאיגה בכמות הנוזקות המיועדות למכשירי טלפון ניידים מבוססי מערכת ההפעלה אנדרואיד, כאשר במקביל - מכשירים אלה הולכים ונהיים נפוצים יותר ויותר".

מגמות נוספות שאותן ציין הן "המעבר לעבודת בתצורת מיחשוב ענן, המהווה גם היא סכנת אבטחה שיש להתייחס אליה. וזאת לצד השימוש הוותיק למדי בשיטות של הינדוס חברתי לטובת גניבת נתונים, עסקיים או אחרים, שווי כסף".

"יש תמיד לזכור כי התוקף נמצא בעמדה של יתרון", סיכם שנהב, "טרור קיברנטי הוא איום ממשי על החיים של כולנו. אנו בחברת הייעוץ קומודו מבינים היטב את האמירה, ומפתחים מוצר לניטור ולהגנה על מרחב הסייבר - CYSNIFF - מערכת מודיעין והתראה בזמן אמת על תקיפות סייבר. המערכת מהווה שכבה עבה של הגנה קיברנטית עבור ארגונים בארץ ובעולם. המערכת

תספק מידע - מבעוד מועד - על מתקפת סייבר שעתידה להתרחש, וכן תתריע על תקיפות המתרחשות ברגעים אלו ממש. כך, ניתן יהיה למזער את הנזק שבמתקפה".

"הלוחמה הקיברנטית הורגת"

"לוחמה קיברנטית אינה וירטואלית, זוהי מלחמה שמפעיל אותה מי שיש לו יעדים, והיא הורגת אנשים. צריך להתייחס אליה בהתאם לכך", כך אמר **אורן ברט**, מנהל תחום מערכות הגנה בסייבר בתעשייה הצבאית.



אורן ברט

לדברי ברט, "מאחר שמדובר בשדה קרב לכל דבר, ניתן להכריע את הקרב או להתגונן, ובמסגרת זו מבצעים פעולות שמיוחסות לנושא הסייבר. לכן, חשוב להגדיר בבירור את המושגים ולהבחין בהבדלים ביניהם: הסייבר הוא לא שדה קרב אלא מרחב בו מתנהלת קישוריות בין מערכות

תקשוב ומערכות ושירותים פיזיים. שדה הקרב הוא השדה הקיברנטי". הוא ציין כי "במלחמה קיברנטית, כמו במלחמה קינטית, הפגיעה בבני אדם ובנכסים היא משמעותית. התוקף מתכוון לפגוע בנכס לאומי קריטי תוך שילוב של מספר יעדים, מטרות ואמצעים. לכן, המערכות הקריטיות חשופות לקיום הלאומי, מעבר לשאלה של אבטחת מידע. למשל,