

גופים גדולים, מדינות או ארגוני פשע, אוספים מודיעין רב, מחפשים פריטי מידע מאוד מסוימים, מבצעים את המתקפות שלהם בעקביות ולא מתייאשים עד שהם פוגעים במטרה."

הוא ציטט את אחד המחקרים שהעלה שבכל המקרים שנבדקו, המתקפות בוצעו על אף שתוכנות האנטי וירוס של הארגונים היו פעילות ומעודכנות. "הסיבה לכך היא שלא היה לאותם ארגונים המענה הנדרש למתקפות שהאנטי וירוס לא זיהה". סימסולו הוסיף, כי "בכל תקיפה מתוחכמת נעשה שימוש בגניבת הרשאות חזקות".



אלעד סימסולו

סייבר-ארק היא חברה ישראלית שמפתחת טכנולוגיית כספות וירטואליות. לדברי סימסולו, "בנקים, חברות ביטוח וארגונים נוספים אימצו את הכספות שלנו. בנוסף, אנחנו מציעים פתרונות לשמירה מאובטחת של קבצים בארגון והעברת קבצים בטוחה בין ארגונים או בין הארגון לספקים וללקוחות. מוצר נוסף שלנו הוא שרת סיסמאות שמציע פתרון לבעיית ניהול הסיסמאות בארגון ברמת תשתיות המיחשוב, רכיבי הרשת והיישומים. בקרה מלאה יכולה לבלום חלק גדול מהמתקפות על הארגון ובמתקפות שמצליחות - לצמצם מהותית את הנזק".

לעקוב אחר פעילותם של המורשים לכניסה

"ארגונים משקיעים משאבים רבים בבקרת גישה ובשאלה מי נכנס למערכות ה-IT הארגוניות, אולם לא משקיעים מספיק משאבים בשאלה מה עשו המשתמשים בתוך המערכות לאחר שהותר להם להיכנס", כך אמר אריק קשה, מנהל מכירות לאזור EMEA ב-ObservelT.

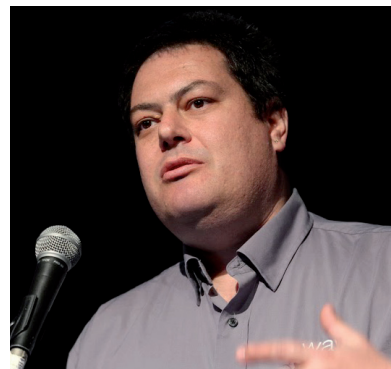


אריק קשה

החברה, ציין קשה, היא השלישית במהירות הצמיחה שלה בישראל וחוותה גידול של 3,500% בפעילותה בחמש השנים האחרונות. מספר הלקוחות שלה עומד על 700 לקוחות. לדבריו, "במקום לנטר את מערכות ה-IT אנחנו מנטרים את האנשים ועוקבים אחר פעילותם".

ObservelT פיתחה מערכת ניטור והקלטה ייחודית, "שמספקת יכולת צפייה מלאה בהתנהלות המשתמשים ובפעילותם המתבצעת על שרתים ותחנות, בלי תלות בצורת החיבור לשרתים - בין אם דרך חיבור מקומי, תחנת קצה מרוחקת, טרמינל סרבר או כל תוכנת חיבור וניהול מרוחק", אמר קשה.

לדבריו, "אנחנו מאפשרים צפייה מאובטחת ומוגנת בכל הקלטה המאוחסנת במערכת, על ידי שימוש במערכת של הרשאות מודולרית. בזכות העובדה שהמידע מאונקס בצורה מרכזית יש לנו יכולת לבצע חיפושים נרחבים, על פי מדדים רבים, כמו: שם המשתמש, שם היישום, שם השרת, טווחי תאריכים, שמות קבצים או פעולות כמו מחיקת קבצים



אדי אלמר

מיקרוסופט מאחר שלעומת iOS ואנדרואיד, יש לה ניסיון באבטחת הנתונים שבמחשב. הוא ציין ש"המערכת מאפשרת למשתמשי הארגון לעבוד מרחוק בלי שום חשש ולהיפטר מהסיסמאות. החומרה שנמצאת בטאבלט מאבטחת אותו, התוכנה שלנו מנהלת אותו. המשתמש יכול לגשת למשאבים הארגוניים

כרצונו. כמו כן, כאשר המכשיר אובד, הוא יודע למחוק את עצמו אוטומטית, בניגוד למכשיר טלפון שאובד. יש לו גם יכולת לחסום את עצמו מיידית. בנוסף, ה-PIN שמשמש את המחשב לזיהוי שייך רק לו עצמו".

להקשיח את ציוד הקצה

דביר גורן, ה-CTO של חברת כלקום, הציע להקשיח את המחשבים, הטלפונים ושאר ציוד הקצה כדי להתמודד עם מתקפות הסייבר. הוא דיבר על המתקפות שחוותה ארצות הברית ב-2012, בהסתמך על דו"ח שהוצא בנושא. "המטרה שלהן הייתה יצירת כאוס", ציין. "מניתוח המידע ניתן לראות שהמקור של 90% מהן הוא בסין ולאחר מכן ברוסיה, באיראן ובפעולות שבוצעו על ידי האקרים שמזוהים עם אל קאעידה.



דביר גורן

המסקנה של הדו"ח היא שהמתקפות הצליחו עקב החלשת מערכות ההגנה ואי עדכון שלהן ומאחר שככלל, התוקפים הכינו היטב את המתקפה".

גורן הוסיף, ש"ממשל אובמה הטיל על המשרד האמריקני לביטחון פנים לרכז את תחום אבטחת המידע, להגיש המלצות, להטיל רגולוציות ולפקח ישירות על הנושא. גרטנר המליצה

בעקבות כך לארגונים להקשיח את תצורת ה-IT ואת הציוד שלהם, כדי להתכונן למתקפות חיצוניות, לאחד כוחות בין מחלקות אבטחת המידע למחלקות תפעול ה-IT לצורך פיתוח מדיניות, לימוד התהליכים הטמעות התקנים ולבצע ניהול ומעקב אחר שינויי קונפיגורציות. כל כניסה של כל משתמש, אפילו מורשה, צריכה להיות מתועדת".

כן הוא אמר, כי כלקום פיתחה מוצר בשם CHS שנועד לענות על הדרכים החדשות להקשחה כפי שהוצעו על ידי המשרד האמריקני לביטחון פנים.

"האקרים נמצאים במחשב הארגון כשנה וחודשיים לאחר שנפרץ"

"האקרים שפורצים למחשב ארגוני שוהים בו במשך כשנה וחודשיים, וליתר דיוק - 416 ימים, לאחר שנפרץ. מדובר בתקופת נצח", כך אמר אלעד סימסולו, מנהל פרויקטים בסייבר-ארק. לדברי סימסולו, "התוקפים השתנו: הם מתקדמים, ממומנים על ידי