

- אנשים ומחשבים - פורטל חדשות היי-טק, מיחשוב, טלקום, טכנולוגיות - <http://www.pc.co.il>

## "דליפת מסמכי ה-CIA משפיעה על כל ארגון וממשלה בעולם"

מאת [אבי בליזובסקי](#): On 9 במרץ 2017 @ 10:18 In [אחד על אחד - ראיון השבוע, דעות וניתוחים, כתבות ראשיות](#) | [No Comments](#)



שרון נימירובסקי, מייסד ומנכ"ל White Hat. צילום: יח"צ

### השבוע נחשפו ב-ויקיליקס שיטות ההאזנה של ה-CIA. מה בדיוק הודלף?

"ל-CIA יש שמות קוד לפרויקטים. במסגרת [פרויקט בשם Vault 7](#)<sup>[1]</sup>, סוכנות הביון הפעילה מיקור-חוץ של האקרים. הספקים שלה בתחום העסיקו 5,000 עובדים שעסקו במשימות המחקר של ה-CIA - מספר המעיד על השקעה עצומה. אחת המשימות הרבות של הצוות הייתה בניית בנק יכולות תקיפה המבוססות בעיקר על חולשות שקשורות למתקפות יום אפס. הם עברו על כל המכשירים האפשריים - מחשבים, טלפונים, טלוויזיות חכמות ומערכות אינטרנט של הדברים - ועל בסיס החולשות האלה בנו קודים שבעזרתם הם יכולים היו לתקוף ולהשתלט על תחנות עבודה, סמארטפונים - הן iOS והן אנדרואיד (Android) - וטלוויזיות חכמות, במטרה להאזין להם".

### מה במכשירים עצמם מאפשר ל-CIA ולגורמים אחרים להאזין להם?

"בטלוויזיות החכמות הם יכולים להאזין למיקרופון, שמובנה בטלוויזיה גם כשהיא כבויה, בטלפונים החכמים הם יכולים לצותת לווטסאפ (WhatsApp) ולטלגרם (Telegram) ולקרוא את ההודעות לפני שהן עוברות את תהליך ההצפנה, וב-Windows הם יכולים לגרום להתפשטות של נזקות בין מחשבים".

### האם מיקור-חוץ הוא החוליה החלשה?

"כן, אבל אי אפשר לעשות את זה אחרת. גם בישראל הדברים נעשים במקרים רבים במיקור-חוץ, כי אי אפשר להחזיק את כמות כוח האדם שדרושה כדי לעקוב אחרי נזקות ומתקפות כאלה ולתקן את הנזקים שהן יוצרות כשהן פוגעות, בגלל אילוצים תקציביים. גם בארץ נעזרים בגופים חיצוניים, כולל מערכת הביטחון. במקרים כאלה, כולם תומכים על סודיות, וכך היה גם במקרה של ה-CIA, אבל כנראה שמישהו שם סרה, החליט שיש כוח גדול מדי במקום אחד והחליט להדליף את זה, מתוך רצון ליצור שיח על כך, כמו גם על ההאקרים והיכולות שלהם".

### האם היכולת של ה-CIA נפגעה ובכלל, מי יושפע מההדלפה?

"היכולת של ה-CIA עדיין קיימת, אבל ארסנל הכלים שלהם נחשף. יש לכך השפעה על כל ארגון וממשלה בעולם. הסיבה היא שעכשיו כל ארגון, כל ממשלה וכל חברה יודעים שהאיום עליהם גדל. עלה לאוויר מסמך עם חולשות, כך שיכולים לראות אותו גם פושעים בתחום הסייבר ומדינות עוינות".

### כיצד המנמ"רים צריכים להיערך?

"התובנה המרכזית שניתן להסיק מהאירוע היא שארגונים צריכים לעשות שינוי בתוכניות העבודה שלהם ולשים את נושא עדכוני התוכנה במקום גבוה בסדר העדיפויות, מכיוון שאפשר לנצל חורים רבים שלא היו ידועים קודם לכן. אם ארגונים עדכנו את התוכנות שלהם עד עכשיו 'בנחת' ודחו עדכונים למערכות הפעלה ולשרתים, כעת ביצוע עדכונים 'לאורך השנה' יהפוך ל-'לחודש הקרוב'".

---

Article printed from <http://www.pc.co.il>: טלקום, מיחשוב, טלקום, טכנולוגיות:

URL to article: <http://www.pc.co.il/editorial/236724/>

URLs in this post

[1] פרויקט בשם 7 Vault: <http://www.pc.co.il/featured/236687/>

אנשים ומחשבים © 2014 - כל הזכויות שמורות