עדכון חדשות סייבר יומי 14/06/2018

בארץ ובעולם

1. משרד האוצר האמריקאי הודיע כי הוא מטיל סנקציות על שתי חברות אבטחת מידע ישראליות, שלטענתם שיתפו פעולה עם הרוסים במהלך מתקפת סייבר כנגד ארה"ב. חברות אבטחת מידע אלו מחזיקות משרדים ברוסיה, ומעתה כל נכסיהם בארה"ב יוקפאו ויאסר על תושבים אמריקאים לבצע עסקאות עם חברות אלו (haaretz).

2. נחשפה פרצת אבטחה חמורה בחברת "אוטומציה החדשה" המפעילה את מערכי המחשוב והשירותים המקוונים של מס' רשויות מקומיות ומועצות דתיות. פרצה זו חשפה עשרות מאגרי מידע המכילים פרטים רגישים, תשלומי דוחות חניה, קבלת היתרי בנייה ועוד (calcalist).

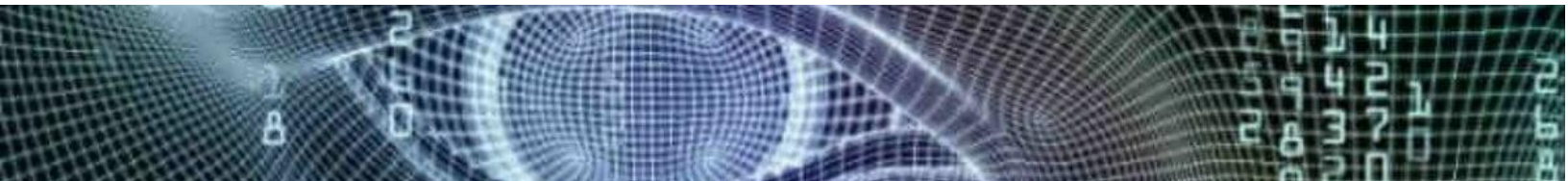
3. ארגון FS-ISAC מקים פלטפורמה חדשה המכונה CERES ותאפשר שיתוף מידע בין בנקים מרכזיים, רגולטורים ועוד. הפלטפורמה תאפשר לבנקים לשתף את שיטות עבודתם, להפיץ התרעות מפני מתקפות סייבר ועוד. (businesstimes)

4. לאחר שחוותה פריצה לחברה בשנת 2015, חברת האלקטרוניקה הבריטית Dixons Carphone הודיעה כי בשנה שעברה חוותה פריצה נוספת למערכותיהם, במהלכה נחשפו פרטים של כ-5.9 מיליון לקוחות הכוללים פרטים אישיים וכרטיסי אשראי. לדברי החברה, לא ניתן לעשות שימוש ברוב כרטיסי האשראי ללא קוד המשתמש. (bleepingcomputetr)

5. נחשף כי האפליקציה הרשמית של הליגה הספרדית לכדורגל, אשר הורדה למעלה מעשר מיליון פעמים, מפעילה את המיקרופון ומיקום המשתמש מרחוק. לטענת מנהלת הליגה, הם עושים שימוש בתכונות אלו על מנת לבדוק האם המשתמש נמצא בקרבת משחק, או במקום פומבי. (geektime)

טכנולוגיה

6. חוקר אבטחה מחברת Vertek חשף מעל ל-34 מיליון כתובות דוא"ל שהודלפו משרת השליטה והבקרה של הבוטנט Trikbot. לדבריו של החוקר, היה ניתן לגשת לשרת בעקבות שינוי הגדרות אשר אפשרו לכל משתמש לגשת לכתובת השרת ולחשוף מידע זה. (bleepingcomputer)



7. סטודנטים למדעי המחשב מהטכניון חשפו פגיעות בעוזרת הווירטואלית של מיקרוסופט-מערכת קורטנה. הסטודנטים הצליחו להשתלט על מחשב נעול ולהוריד אליו קובץ חיצוני שבאמצעותו קיבלו גישה לכל הפונקציות. מיקרוסופט מיהרה לתקן פרצה זו. (haaretz)

8. חברת אפל הודיעה כי היא תשנה את הגדרות האייפון על מנת להקשות על החוק אשר מאפשר פריצה למכשירים לצורכי חקירה. (reuters)

9. חוקרי אבטחת מידע מקספרסקי מדווחים כי קבוצת התקיפה Emissary Panda המזוהה עם ממשלת סין נחשפה בעקבות מתקפת סייבר שהתרחשה במהלך חודש מארס השנה. לדבריהם, המתקפה החלה בשנת 2017, והייתה ממוקדת למדינות במרכז אסיה. לדבריהם, התוקפים עשו שימוש בשיטת התקיפה Watering hole באמצעות הוספת סקריפט זדוני באתרים ממשלתיים. אינדיקטורים רלוונטיים בקישור. (securelist)