



בניין המשרדים של סימנטק בפאתי דבלין, בו ממוקם ה'חדר המזוהם'

"השוק השחור העתידי במידע הוא רק עניין של זמן"

ג'ון שרטטה את ההתקדמות של הרעים למיניהם במהלך שני העשורים האחרונים: בתחילה היו מחשבים אישיים ושרתים, ואז נולדו הווירוסים. לאר מכן, עם התפשטות האינטרנט ותחילת המסחר המקוון, החלו מתקפות מניעת שירות, DoS, מתקפות מניעת שירות מבזרות, DDoS, וגניבת זהויות. התקופה הנוכחית, אמרה, המתאפיינת במיחשוב נייד ובמיחשוב ענן, מגלמת בחובה איומים מסוג נזקות מתוכחמות, והדבקת תלפונים חכמים דרך עולם המובייל והרשתות החברתיות. השלב הבא בעולם המיחשוב, אמרה ג'ון, הוא M2M, מכשיר למכשיר, אינטרנט של דברים וטכנולוגיות מיחשוב לביש. פה האיומים, לדבריה, יגיעו משני כיוונים, טרוריסטים מקוונים, והאקרים העובדים עבור ארגוני פשע מאורגן. אלה וגם אלה יפעלו בכמה דרכים - גניבת מידע אישי ומסחר בו, מה שיביא לעוד ועוד אובדן של הפרטיות, מינופולציה על המידע, על מנת להניב ממנו רווח כלכלי, ופגיעה בתשתיות לאומיות קריטיות, תוך שימוש ברכיבים המקושרים החדשים כמחשבי זומבי, לצורך תקיפה, או שימוש פעילויות שונות. בסופו של דבר, אמרה ג'ון, "הצורך באבטחת מידע, הגנה מפני מתקפות סייבר ושמירה על הפרטיות - שלוש המגמות הללו תתאחדנה, כי יש להן אותו יעד".

"צריך לאבטח את הסביבה הטכנולוגית החדשה, בדיוק כמו שצריך לאבטח את זו הקיימת", אמרה ג'ון, "אלא שכבר כיום זה לא נעשה, או שנעשה בצורה חלקית. צריך להגיע למצב הדומה לזה הקיים במכונית - שבו אף אם היא יכולה מבחינה מכנית להגיע ליותר מ-220 קמ"ש - היא תמנע זאת מנהג. ככה צריך לשמור על המידע החדש".

שאן ג'ון: "משקפי גוגל הם בסך הכל הרחבה של מכשיר הטלפון הנייד, רכיב שהוא בעצמו אינו מאובטח. כבר לפני חצי שנה גילינו נזקות לעולם זה"

מחיישנים המחוברים לנעלי הריצה, ועד לחיישנים המודדים את הדופק, המליחות ושאר נתונים פיזיים, בעת עריכת ספורט למשל. מיחשוב לביש יהיה 'שער הכניסה' הבא של ההאקרים. כל פריטי המיחשוב הליביש, הקיימים והעתידיים, חסרי רכיבי אבטחת מידע ולכן פוטנציאל הנוזקות שיודבקו אליהם, נזקות שייקח זמן למצוא להן הטלאה - הוא פוטנציאל גדול, והוא ימומש על ידי ההאקרים".

כך, אמרה, "משקפי גוגל הם בסך הכל הרחבה של מכשיר הטלפון הנייד, רכיב שהוא בעצמו אינו מאובטח. כבר לפני חצי שנה גילינו נזקות לעולם זה".

הבעיה, לדברי ג'ון "נובעת מהעובדה כי כאשר מוצר טכנולוגי בא לעולם, המהנדסים שתכננו אותו חשבו על פונקציונליות, ועל ידידותיות למשתמש, אולם ברוב המקרים, לא חשבו על היבטי אבטחת מידע והגנה על הפרטיות. לכן, אם כבר הוטמעו יישומי אבטחת מידע, הם הוטמעו בשולי הייצור של המוצר, או בסופו, ולא כחלק מובנה בהליך הייצור. כאשר חברה מתכננת פריט מיחשוב לביש, היא חושבת על היבט ה'קוליות' והאופנתיות - ולא על היותו מאובטח או לא".

מגמה נוספת הצפויה לקרות בשנתיים-שלוש שנים הקרובות, אמרה ג'ון, "היא האגירה הבלתי פוסקת של נתונים. ככל שיהיו יותר רכיבים ממוכשרים ומקושרים, הם ייצרו יותר מידע. ה- Big Data הזה יהיה צריך להיות מטופל. המדובר על המון פרטים אישיים, שלצד בעיית אבטחת המידע, משקף בעייה של אובדן פרטיות. למשל, אם מישהו נוטל תרופות מסוימות, אבל מסתיר את עובדת היותו חולה ממקום העבודה. בשל כך, ערך המידע שייצבר - יעלה, ויש להניח כי המידע הזה ייגנב בשלב כלשהו, ויימכר בשוק השחור, בשל הערך הכספי הגלום בו. זה לא יקרה מחר - אבל בטוח יקרה מחרתיים".