

2014: לצפות את הבלתי צפוי

מהי מגמת ה-BYO? איך תשפיע הפסקת התמיכה ב-Windows XP על עולם אבטחת המידע? ומהו המודל שלפיו עובר שוק ההאקינג לעבוד? ♦ מערכת אנשים ומחשבים קיבצה את האיומים המרכזיים השנה, על פי התחזיות של חברות אבטחת המידע

יוסי הטוני

חסינה לניהול סיכונים ויצירת יכולת תגובה מהירה ויעילה יותר.

מה יקרה בתחום ההינדוס החברתי?

הינדוס חברתי (Social engineering) "על סטרואידיים", או תקיפת הגורם האנושי, הוא מגמה שתמשך השנה. על פי חוקרי סייבר ארק, הנדסה חברתית, כלומר - עבודה מול הגורם האנושי, הייתה תמיד אחד הכלים הטובים העומדים לרשות תוקפי סייבר כדי לפרוץ הגנה היקפית. ממיילים מזויפים ועד לאתרים מזויפים, תוקפים משתמשים בטבע האנושי כדי לעקוף אותה ולהחדיר את הנוזקה ישירות לרשת הארגון. "ב-2014 נראה עוד התקפות הינדוס חברתי מסוגים שראינו ב-2013, למשל מתקפה ממוקדת שכוונה לעובדי IO גברים, שהשתמשה ברשתות חברתיות בפרופילים מזויפים של נשים מושכות, המתחזות לעובדות חדשות המבקשות עזרה, כמו גם הצעות עבודה מזויפות ושיחות טלפון מצידי ראשים כדי לבקש מידע", על פי סייבר ארק. "אסטרטגיה נוספת

היהו המגמות הבולטות בעולמות אבטחת המידע בסייבר ב-2014? איזו מהן תשפיע יותר על אבטחת המידע ועל חיינו בשנה הבאה? מערכת אנשים ומחשבים קיבצה את סביבת האיומים המתקדמים בשנה שנפתחה.

על פי מאות מנהלי אבטחת מידע בארגונים, החברים ב-ISF (Information Security Forum), מגמת ה-BYO ("הבא את המשהו שלך") היא האיום האבטחתי המרכזי שבפניו הם יתמודדו השנה. מגמת ה-BYO היא הרחבה של המושג שהיה שגור בשנה החולפת - BYOD ("הבא את המכשיר שלך"). הצפי הוא, שהשנה ירחיבו המשתמשים ויכניסו לארגונים לא רק את המכשירים החכמים שלהם, אלא גם את חשבונות הדואר האלקטרוני ואת הקבצים שלהם שמתארחים בענן. בגלל הגידול באיום יגדלו הסיכונים - ניהול כושל של המכשיר עצמו, מניפולציה חיצונית על נקודות תורפה בתוכנות ופריסה של יישומים עסקיים שאינם מאובטחים. המענה למגמה זו, על פי הארגון, הוא היערכות של הארגונים, בניית גישה

