

אומרים כי אני אינני אני

אבטחה וניהול זהויות: טכנולוגיות חדשות לאימות זהות ♦ אבחן מקרוב את הזהויות: למרות שרבים מתארים מציאות קשה, הרי שחלו כבר שיפורים רבים

טום קילין *

השתלט אפילו על הסיסמאות החזקות והמוגנות ביותר. את העניינים מסבכות עוד יותר הנחיות מחמירות ליצירת סיסמאות והחלפתן. זה היה יכול להיות משעשע, אלמלא הנחיות אלה היו מקשות על המשתמשים לבצע את עבודתם.

מה היה קורה אילו היינו מצליחים לפשט את העניינים עבור המשתמשים, ובה בעת לקבל החלטות אמינות יותר ביחס לזהות? מה אם המערכות של אימות הזהות היו חשופות פחות להונאות, גם במקרים שבהם נוכלים הצליחו לשטות במשתמשים ולהניח יד על הסיסמה שלהם?

היום אני מבקש לבחון מקרוב את הזהויות. למרות שרבים מתארים מציאות קשה, הרי שחלו כבר שיפורים רבים מאז העידן העתיק שבו אימות הזהות התבסס על חותמות ייחודיות וכריות שעווה, שיטה שחשפה את משתמשיה לזיופים רבים. בעידן שלנו, שבו אנו משתמשים במגוון רחב בהרבה של כלים - מסרים מיידיים, עצמת מיחשוב בלתי מוגבלת בענן, צגי מגע גדולים בכל כיס ותיק - כיצד יתכן שאימות הזהות עדיין נחשב לבעיה? קודם כל, צריך לקחת בחשבון את ההיקף העצום. כשישה מיליארד מכשירים מחוברים כיום לאינטרנט, וממדיה של המגמה המכונה



ניתן בהחלט לתכנן פתרונות שנסמכים על ארכיטקטורה חסונה וכוללים את כל שלושה היסודות של אימות הזהות (מה שאתה יודע, מה שיש לך, מה שאתה). בוועידת המפתחים של אינטל (Intel Developer Forum) שנערכה בספטמבר 2012, הציג מנהל הטכנולוגיה הראשי של אינטל, ג'סטין רטנר, מערכת שמשלימה את הסיסמאות הנפוצות והאסימטריות המקובלים, ומבוססת על שיטה איתנה יותר.

ג'סטין הציג משתמש שניגש למכשיר ונעזר בחיישנים ביומטריים כדי לאמת זהות של משתמש אחר בצורה מקומית. לאחר מכן מאשר המשתמש הראשון לספקית שירות שהזהות של המשתמש השני אומתה בהצלחה. לדעתו, יהיה זה נפלא אם פתרונות אמינים כאלה יזכו לאימוץ נרחב, משום שקשה לפרוץ אותם, קל לנהל אותם ואפשר להרחיב אותם כך שיטפלו בכמויות גדולות של משתמשים. וחשוב מכל - מנקודת המבט של המשתמשים, קל להשתמש בהם.

למרות שחברות מסוימות מציעות חלקים מהפאזל, הרי שהגורמים המעורבים עדיין מתקשים לחרוג מהגישות המקובלות לאימות זהות. התקדמנו אמנם לא מעט מעידן החותמות, אך נותרה לנו עדיין כברת דרך בלתי מבוטלת.

* טום קילין, מנהל טכנולוגיות ופרייקטים להגנת סייבר, אינטל

"אינטרנט של הדברים" (internet of things) רק יילכו ויתרחבו - על פי ההערכות, כ-50 מיליארד מכשירים יהיו מחוברים לאינטרנט עד שנת 2020. אפילו היינו מצליחים להנפיק לכל משתמש אנושי חותמת ייחודית וכרית שעווה, הרי שעדיין נתקשה להתמודד עם מיליארדי המכשירים שאינם מסוגלים להשתמש בחותמת. ספקיות השירות הגדולות מזהות כיום בשניות ספורות משתמשים רבים מכפי שאנשי חצר המלכות זיהו לאורך כל חייהם.

גם הסיכונים גוברים בהתאם. בעולם שנסמך על החלטות זיהוי שמתקבלות באופן אוטומטי, היכולת של הנוכלים לנצל פרצות ולזהות נקודות תורפה משתפרת כל העת. על פי ההערכות, היקף הנוזקים שנגרמים לחברות כתוצאה מפשיעה מקוונת ברחבי העולם מגיע לטריליון דולרים. למשתמשים שמגלים נטיות פרנואידיאליות, יש סיבות טובות לחשש.

נבחן, אם כן, את המצב מנקודת המבט של המשתמשים. הם מתאמצים לזכור כל הזמן שמות משתמש וסיסמאות בחשבונות מרובים - הן עסקיים והן אישיים. השם של המורה בכיתה א', חיית המחמד הראשונה, המכוננית הראשונה. הודעות SMS עם סיסמאות חד פעמיות. ועדיין אי אפשר לתת אמון ולהיות בטוחים משום שתוכנה זדונית מתוחכמת עלולה