

עלייתו של המשתמש: "הבא את הזהות שלך"

הזהויות הדיגיטליות הן קו ההגנה החדש שמגשר בין אבטחה מוכוונת (No) לבין אבטחה מוכוונת שליטה וידע (Know)

מאת עווד צור, מנהל תחום אבטחת מידע ב-CA Technologies ישראל

משמעות אליהן, משמשות להגדרת האינטראקציות עם הארגון והכנת פרופילים. ושלישית, הדגש בתחום הזהות מושם כיום יותר על התנהגות ואחריות, וכוחות על שם משתמש וסיסמה.

עם זאת, יש מי שיטענו כי השינויים מתרחשים בקצב מהיר מדי. חלק מהמבקרים טוענים כי לא ניתן לבטוח בזהות שמקורה באתר של מדיה חברתית. אולם, ניתן להיעזר במספר גדל והולך של שירותים שמחשבים את מידת האמון שניתן לתת בזהויות אלה ומגדירים סף לקבלתן. אתרים אלה מגדירים, למשל, שאם משתמש מסוים עושה שימוש באותה זהות ב-Facebook במשך חמש שנים, וצבר היסטוריית תקשורת מספיק ארוכה, סביר להניח שהיא אינה מזויפת. למעשה, מאחר שהחברות של המדיה החברתית מיישמות אמצעים רבים לבקרה על החשבונות שיוצרים המשתמשים, קשה יותר ליצור זהות מזויפת באתרים של מדיה חברתית מאשר בתהליך רישום שבו פותחים חשבון חדש וייחודי כדי לקבל שירות נתון.

מהסקר של Quocirca עולה כי המגמה של 'הבא את הזהות שלך' (BYOID) לא תהיה מוגבלת לעולם של הצרכנים הפרטיים בלבד, ותתפשט גם לעובדים שיוכלו, למשל, לעבור ממשרה למשרה עם הזהות שלהם, כשם שהם עוברים כבר היום עם הטלפון החכם ועם אמצעי גישה נוספים.

יש, כמובן, גם 'אבל'. אם האתרים של המדיה החברתית משמשים כמקור לזהויות, על הארגונים להתייחס לכך בצורה נבונה. מחלקות השיווק לא יכולות לצפות, משתמשים מאתרי מדיה חברתית, שהם צד שלישי, יבצעו המרה ישירה לזהות ביישומי הארגון שלהן; אי אפשר גם לצפות מהמשתמשים שייכנסו פעם אחר פעם או ימלאו אותם נתונים באותם תפסים שוב ושוב.

ניהול הזהויות והגישה בארגון המורחב

המשתמשים זקוקים יותר מאי פעם לגישה ליישומים של שותפים (שותפים עיסקיים של הארגון אליו הם ניגשים) - למשל כדי לבצע בדיקה צולבת של היסטוריית אשראי מול צד שלישי בחברה שמספקת שירותים פיננסיים, או כדי להשתמש ביישומי ענן דוגמת Salesforce.com. ברבים מאתרים אלה דורשים להזין שם משתמש וסיסמה לצורך אימות זהות, אך המשתמשים נרתעים מהנטל הכרוך בשם משתמש נפרד, ובסיסמה נפרדת, לכל יישום. החוויה הטובה ביותר היא כניסה אחודה וחלקה (SSO - Single sign-on) שאינה תלויה בבעלות על היישום.

בתהליך של הכניסה האחודה אפשר להשתמש בזהויות מכל מקור - ובכלל זה רשתות חברתיות. השיווק במדיה חברתית הופך לשיטת שיווק מקובלת. היכולת להשתמש בצורה בטוחה בזהויות שהונפקו על ידי ספקי זהות מהימנים מהמדיה החברתית, דוגמת Facebook או Google, מאפשרת לעסקים להכניס את המשתמשים בכניסה אחודה וחלקה לאתרי השיווק שלהם. לאחר שהמשתמשים נכנסו למערכת של העסק, קל יותר ליישם מסעות שיווק בהתאמה אישית בניסיון להמיר אותם למערכות בחברות העסקיות צריכים להכיר בכך שהתמורה להשקעה במערכות לניהול הזהויות והגישה אינה באה לידי ביטוי אך ורק באבטחה משופרת. התמורה מתבטאת גם בכך שהמערכות פותחות ללחץ הדדמנויות עסקיות. הכרת המשתמשים על סמך הזהויות הדיגיטליות שלהם, על מנת למצוא

פתאום כולם בעניין: מבקשים ליצור קשר עם אנשי מקצוע בעולם באמצעות LinkedIn? אתם יכולים, אם רק תרצו, להשתמש בחשבון Facebook כדי להיכנס ל-LinkedIn. מבקשים למצוא מוזיקה מתאימה ב-Spotify? היכנסו באמצעות Facebook. אפילו בממשלת בריטניה שוקלים לאפשר לאזרחים להשתמש בזהויות מהרשת החברתית כדי לגשת בצורה בטוחה לשירותים ציבוריים במסגרת תוכנית של Identity Assurance (IDA). מגמה זו מכונה 'הבא את הזהות שלך' (Bring Your Own Identity - BYOID) והיא עומדת להפוך לנחלת הכלל.



עווד צור

בחברות העסקיות צריכים להכיר בכך שהתמורה להשקעה במערכות לניהול הזהויות והגישה אינה באה לידי ביטוי אך ורק באבטחה משופרת. התמורה מתבטאת גם בכך שהמערכות פותחות ללחץ הדדמנויות עסקיות. הכרת המשתמשים על סמך הזהויות הדיגיטליות שלהם, על מנת למצוא את הפוטנציאל עד תום, היא אבן הפינה של השליטה באינטראקציות בין עסק נתון לעולם החיצון

בסקר שהזמינה לאחרונה חברת CA Technologies על ידי חברת המחקר Quocirca נמצא, בין השאר, כי ב-27 אחוזים מבין החברות המסחריות משתמשים במדיה חברתית כמקור לזהויות של צרכנים. על פי פירמת Gartner (Gartner Inc), עד סוף שנת 2015 יתבססו 50 אחוזים מהזהויות החדשות של לקוחות בענף הקמעונאות על זהויות מהרשתות החברתיות, בהשוואה לפחות מ-5 אחוזים כיום. לצד טכנולוגיות ה-federation והמיחשוב הנייד, תהיה לאימוץ זהויות מהרשתות החברתיות השפעה חשובה על התחום של ניהול הזהויות והגישה (IAM) משנת 2013 והלאה, על פי האנליסטים.

קל להבין מדוע. ראשית, כשמאפשרים לצרכנים להיכנס לאתרים מאובטחים תוך שימוש בזהויות של Facebook, LinkedIn, Twitter או רשתות חברתיות אחרות, מסייעים להם להתגבר על 'עייפות הכניסה' (Login fatigue) הנובעת מהצורך לזכור מספר רב מדי של שמות משתמש, סיסמאות ותשובות לשאלות אבטחה. אפשרות זו מצמצמת את הטרדה ומשפרת את חוויית המשתמש במהלך ההרשמה של הלקוח ובכניסות הבאות שלו. שנית, מחוץ לתחומי הארגון נוצרות זהויות רבות יותר ונשמרים פרטי זהויות רבים יותר. זהויות אלה, וההתנהגויות