

כיצד להתמודד עם משבר הזהות בעולם הדיגיטלי

מאת: גלעד ירון, שותף ו-SECOZ CTO

משתמשים בלתי מנוהלים הינם בעלי המידע שהם מייצרים, ולמנהלי מערכות המידע יכולת פעולה מוגבלת לגבי צורת השימוש של משתמשים אלה, למעט מקרים בהם הם גורמים נזק ברור לארגון.

אין ספק כי המשתמשים הפנימיים של הארגון - עובדים קבועים, זמניים, ספקים, מתלמדים וכדומה, צריכים להיות מנוהלים בתוך הארגון. יש לבנות תשתית להזדהות, הרשאות וגישה למשאבי הארגון, ובכך להפוך אותם למשתמשים מנוהלים.

מי מנהל את המשתמשים הבלתי מנוהלים?

כיצד מנהלים את המשתמשים החיצוניים של הארגון? האם זה נכון והגיויני כי נחזיק מידע לגבי זהותם והנתונים הנדרשים עליהם, כגון כתובות, מקום עבודה, פרטים אישיים וכדומה? כיצד נעדכן את המידע? כיצד נאבטח אותו ולא נסתבך עם תביעות חוקיות שונות הדורשות שמירה על פרטיות?

רק לפני כמה שורות הפרדנו באופן חד משמעי את המשתמשים הפנימיים מאלה החיצוניים והצענו קשר בין המשתמשים הפנימיים והחיצוניים למשתמשים המנוהלים והבלתי מנוהלים. למרבה הצער, העולם בו אנו חיים אינו פשוט כל כך:

- ארגונים מאפשרים לאנשים לעשות שימוש בהתקנים שאינם נשלטים ואינם בבעלות הארגון. כך, אנשים עושים שימוש בטלפונים ניידים, טאבלטים או המחשב בבית.

- עובדים בתוך הארגון משתמשים במערכות מידע הנמצאות מחוץ לו - כגון Facebook או SalesForce.

- ארגונים משתמשים בשירותי ענן על מנת לבצע חלק משירותי המחשוב שלהם. המשתמשים שלהם יכולים להיות מנוהלים על ידי גורם אחר.

- משתמש אחד נזקק לשירותים הניתנים על ידי ארגונים שונים, למשל, משאבי אנוש של החברה מפנה אותך לקופת הפנסיה בה חשבוך מנוהל, סוכן הנסיעות מפנה אותך למלון וחברת התעופה וכן הלאה.

על מנת להתמודד עם אתגרים אלה, הוגדרו סטנדרטים המאפשרים תשאול לגבי זהות המשתמשים באופן אחיד ומאוברט, למשל, פרוטוקול Security Assertion Markup Language (SAML). באמצעות סטנדרטים אלה, עולם ניהול הזהויות הופך להיות יותר גמיש. ארגונים יכולים לנהל את חלק מן הזהויות או את כל הזהויות של המשתמשים שלהם מחוץ לגבולותיהם, ובאותה מידה לספק שירותי ניהול זהויות לחלק או לכל המשתמשים בארגונים אחרים.

סטנדרטים אלה קיימים זמן רב ומוצרים ותשתיות שונים מממשים אותם. בתקופה האחרונה אנו חווים פריחה של השימוש וההטמעה בסטנדרטים אלה ובפונקציונליות של תשתיות הניהול ואבטחת המידע, שנובעת מכך שכך המאזניים הולכת ומוטה יותר ויותר ממשקלם של כמות המשתמשים הבלתי מנוהלים שדורשים ניהול.

יש מקום לבדיקה, לחשיבה מחדשת ולשבירת מיתוסים בקרב הגורמים האחראיים על בנושא זה בארגונים.

אנחנו לא רצים בעצמנו בתוך המחשבים, מערכות התקשורת, הכספומטים, הקופות הרושמות וכל אותן המערכות אלקטרוניות המודרניות המלוות אותנו על כל צעד ושעל בחיינו הפרטיים ובמקומות העבודה שלנו. הזהות הדיגיטלית שלנו מייצגת אותנו בכל הפעולות הללו. זהות דיגיטלית הינה תחליף לדרכון עם תמונה. היא מייצגת את האנשים המסתתרים מאחורי הרשתות והמחשבים בדומה לימים בהם הכירו כולם את כולם וקיימו עסקים פנים אל פנים.

ניהול הזהויות הדיגיטליות בצורה שתבטיח את אמינות הנתונים, זמינותם ואבטחתם ותצמצם את הסיכון כי מתחזים חורשי רעה יגנבו זהות לא להם, הינו אתגר סבוך העומד בפני ארגונים המעניקים שירותי מחשב לעובדיהם וללקוחותיהם (ואיזה ארגון אינו כזה בעולם המודרני?).

קיצור תולדות הזמן

בתחילת עידן המחשבים כלל עולם המחשוב מחשבים מרכזיים אשר הוזנו באמצעים כגון כרטיסים מנוקבים. הזהויות שנוהלו במחשבים אלה היו של קומץ מפעילים והמפתחים שלהם.

עם תחילת עידן המחשוב המבוזר, נוספו למערכות משתמשים עסקיים העובדים עליהן באופן ישיר. היות ומשתמש אחד יכול היה לעבוד על יותר ממערכת מידע אחת, נוצר הצורך להגדיר משתמשים בכל אחת מן המערכות הללו.

על מנת לייצל את תהליך ניהול המשתמשים על מערכות אלה החלו להתפתח ארכיטקטורת מחשוב שונות המקלות על ניהול זהויות המשתמשים. ניתן להתייחס לשתי תצורות מרכזיות בתחום זה:

1. אחסון מרכזי של זהויות המשתמשים אליו פונות אפליקציות בארגון על מנת לוודא את זהות המשתמש ואת הרשאות שלהם. מערכות אלו מכונות ספריות. דוגמה נפוצה לארכיטקטורה כזאת הינה מערכת Active Directory.

2. מערכות רבות מנהלות את המשתמשים שלהן באופן עצמאי. מערכות לניהול משתמשים מרכזי מאפשרות הגדרת המשתמשים דרך מקום מרכזי אחד. מערכת הניהול המרכזית יוצרת קשר עם כל אחת מן המערכות ומייצרת את המשתמשים עליהן.

במקביל, עם התפתחות האינטרנט, המשתמשים לא תחומים יותר בחצרות הארגון. משתמשים יכולים לעבוד מכל מקום ברחבי העולם ובכל זמן. יכולים להיות אלה המשתמשים הפנימיים של הארגון, לקוחותיו או ספקיו.

בעולם כל-כך מורכב, איך יודעים מי זה מי?

משתמשים מנוהלים ובלתי מנוהלים

מנקודת מבט הארגון, ניתן לחלק את עולם הזהויות לשני חלקים - משתמשים מנוהלים ומשתמשים בלתי מנוהלים.

משתמשים מנוהלים הם אלה שעליהם ניתן לאכוף את מדיניות הארגון לכל פרק הזמן בו הם עושים שימוש ברשת הארגון. צוות מערכות המידע המקומי שולט על כל התקן שברשותם ובאפשרותו לחסום את הגישה לכל משאב ברשת כאשר הוא מזהה התנהגות בלתי נאותה. המשתמשים המנוהלים אינם בעלי המידע אותו הם שומרים מקומית או ברשת הארגון. משתמשים בלתי מנוהלים חיים בעולם אחר לחלוטין. אלו הלקוחות או השותפים העסקיים העושים שימוש בשירותים אותם הארגון מציע, או הקורא שורות אלה בעת שהוא צורך שירות בארגונים אחרים.

SECOZ
BUSINESS & INFORMATION SECURITY ADVISORS