

"זהות" - הגבול החדש

עודד צור, מנהל אבטחת מידע, חברת CA Technologies



עודד צור

נושא אחרון הוא הגבול הדק שבין שמירת האבטחה וחווית המשתמש - אנו נרצה שטכנולוגיה שנותנת מענה לאתגרים הנזכרים למעלה תהיה שקופה עד כמה שניתן ולא תפריע לחווית המשתמש - דוגמא לכך היא שאנו יכולים לעיתים לאפשר למשתמש לבצע פעולה אפילו ללא סיסמא - מכיון שהזיהוי הסביבתי שלו היה כה מובהק שאין צורך להקשות עליו. להיפך, נרצה לשפר לו את חווית השימוש.

אנו ב-CA Technologies מתמחים בנושא של ניהול זהויות והרשאות גישה על כל צדדיו.

ספציפית לעינינו ל-CA טכנולוגיה מעולם ה-FRAUD - הנותנת מענה ל-Risk Based Authentication הפתרון מתבסס על טכנולוגיה לזיהוי המכשיר (נייד או נייד) הנקראת Device DNA ובשילוב עם פרמטרים רבים סביבתיים נותן זיהוי חד ערכי שמהווה בסיס למתן ציון לסיכון של ההזדהות - מידע זה נאסף ללא הפרעה למשתמש ומועבר לאפליקציה כחלק מהזיהוי - שגם אם הוא נכון - אינו תמיד אותו זיהוי. כך שיתכן שאותו משתמש עשוי לקבל גישה שונה לאותו מידע בהתאם לסיכון המוערך באותו רגע.

זוהי דוגמא אחת מיני רבות, מהאופנים השונים בהם אנו מאפשרים לארגון להרחיב ולשפר את הגבול החדש הנקרא "זהות".

זהות היא הייצוג שלנו, משתמשי המחשב, לצורך שימוש ביישום כלשהו, בין אם שימוש ישיר במערכת ההפעלה או שימוש ביישום ארגוני כלשהו כדוגמת הדואר האלקטרוני שלנו או מערכת ה-ERP הארגונית וכאלה יש הרבה. בגדול, מספר הזהויות יכול להגיע למספר היישומים. לזהות שלנו הרשאות במערכות השונות והיא זו המבצעת "בשמנו" את הפעולות השונות במערכות השונות.

עד היום, הגבול עליו סמכנו היה הרשת. הושקע מאמץ רב בהגדרת הרשת, הגנה עליה ותחזוקה כזו שאיפשרה לנו להתייחס לעצם קיומה כמשהו שאפשר לסמוך עליו בקבלת החלטות לגבי זהות והרשאותיה. ברבות הימים איפשר לנו הארגון להיכנס כניסה מאובטחת מחוץ לארגון.

ל-CA Technologies

התמחות בפתרונות

ניהול זהויות והרשאות

גישה. החברה פיתחה

טכנולוגיה מעולם

ה-Fraud הפותרת את

סוגיית Risk Based

Authentication.

הפתרון מתבסס על

טכנולוגיה לזיהוי המכשיר

בשם Device DNA

היום, בעידן ה-Cloud, הרבה מהשירותים נצרכים על ידינו בין אם אנחנו בתוך הרשת או מחוצה לה. כך גם שותפינו, לקוחותינו וכלל ה-Eco System של הארגון שלנו.

במילים אחרות - הגבול עליו סמכנו עד היום טושטש כל כך שמבחינת אבטחה קשה לסמוך עליו.

ולכן, הגבול הבא הפך להיות הזהות עצמה.

כלומר, אנו צריכים להעמיק ולהרחיב את יכולותינו לנהל לזהות, להגן ולתת הרשאות לזהות היות שהיא הגבול החדש שלנו. אם נוסיף לכך את הכניסה של שימוש ברכיבים ניידים, טלפונים חכמים, iPads, טאבלטים וכד' - אלו מכניסים למשוואה גורם נוסף ה-Device.

עליו לנהל במובנים השונים, שהזכרו לעיל, את הזהות כשהיא

בהקשר של שימוש ב-Device - דוגמא - אין דינה של זהות שזוהתה בהצלחה כאשר היא משתמשת במחשב נייד של הארגון כדינה של אותה זהות שזוהתה באותה רמת הצלחה כאשר היא משתמשת בגלישה דרך טלוידיה חכמה או טלפון חכם - כלומר עלינו לזהות חד ערכית את הזהות ואת ה-Device. אם נרחיב את התסריט אין דינה של זהות שזוהתה בהצלחה כאשר היא משתמשת במחשב נייד של הארגון מביתו של המשתמש. כלומר גם מיקום יכול להוות פרמטר.

כלומר, קיים צורך להרחיב את יכולותינו בזמן האינטראקציה הראשונית עם המשתמש - קרי בזמן הזיהוי - ולקבוע מידת סיכון בשלב זה הנובעת מהשילוב של הזהות וה-Device והמיקום.

פן שלישי הוא המידע אליו מבקשת הזהות לגשת - האפליקציה, הקובץ, השרת המערכת וכד'.

משתמש המבקש לגשת למידע רגיש מאינטרנט קפה, גם אם זוהי בהצלחה לא ירשה לצפות במידע המחשש שמישהו יכול לצפות בו מעבר לכתפו.

