מפתחים אפליקציות מובייל ארגוניות? כדאי להכיר את Workspace ONE SDK

כולם הולכים למובייל

כמעט בכל ארגון כיום מתבצע פיתוח אפליקציות להתקנים ניידים עבור עובדי הארגון, גישה מהתקנים ניידים למערכות הארגון משפרת את ביצועי הארגון ומאפשרת להגיב במהירות וביעילות לצרכי הלקוחות, הספקים וההנהלה.

ומה עם אבטחת הנתונים וניהול האפליקציות?

בתהליך הפיתוח של האפליקציות הניידות נהוג בדרך כלל להתמקד בפונקציונאליות ובחוויית המשתמש כשהיבטי הניהול והאבטחה בדרך כלל אינם מטופלים מתוך הנחה שזה יטופל במסגרת תשתיות האבטחה של הארגון.
הנחה זו הנה הנחה מוטעית ומגיעה מתפיסת עולם מיושנת של פיתוח אפליקציות מסורתיות הפועלות ברשת הארגונית.
כשמדובר באפליקציות הפועלות על התקנים ניידים שמתקשרים על בסיס רשתות ציבוריות ומאפשרים למשתמשים להתחבר בכל עת מכל מקום, נדרשים היבטי אבטחה, הזדהות וניהול מתאימים, כאלה שיגנו על המידע אך לא יפגעו בחוויית השימוש.
לצורך מימוש אפליקציה ארגונית ניידת, הארגון צריך לשקול מעבר לפונקציונאליות ולחוויית המשתמש, גם את ההיבטים הבאים:

- App Config – ניהול הגדרות תצורה, היכולת להפיץ להתקנים אפליקציות עם הגדרות מסויימות מראש (בגון שם שרת, Port, דומיין וכד') והיכולת להפיץ הגדרות עדכניות Over The Air, המציאות היא שמערכות מחשב משתנות לעיתים תכופות והארגון חייב יכולת להפיץ עדכוני הגדרות למכשירים שיכולים להמצא בכל מקום ובכל עת
- App Passcode – החלת מדיניות קוד בכניסה לאפליקציה, כולל אפשרות למימוש זיהוי ביומטרי מעל הקוד לצורך חווית משתמש נוחה יותר, מדיניות זו מונעת גישה בלתי מורשית לאפליקציה במקרה ואדם לא מורשה הצליח להגיע למכשיר ארגוני שאיננו נעול
- App Tunneling – מימוש VPN אוטומטי ייעודי רק לנתוני אפליקציה ספציפית, VPN מסוג זה פועל בלי התערבות המשתמש ומבטיח שרק מידע שרלוונטי לאפליקציה יעבור דרך ה – VPN ולא כל שאר המידע שהמכשיר משדר
- Encryption – הצפנת מידע אפלקיטבי על המכשיר נחוצה למקרה של גניבת מכשיר וגישה למערך האחסון שלו
- Managed Open In – ניהול היכולת לשתף מידע מתוך האפליקציה כדי למנוע שיתוף מידע באמצעות אפלקציות שאינן מורשות לשיתוף מידע ארגוני (כגון Gmail וכד')
- Prevent App Backup – מניעת גיבוי אוטומטי של מידע מתוך האפליקציה (גיבוי מכשיר של גוגל, סמסונג, אפל וכד'), בלי מדיניות כזו, נתוני האפליקציות של הארגון עלולות להגיע לשרתים של גורמים רבים ושונים
- Prevent Copy and Paste – מניעת העתק הדבק של נתונים מתוך האפליקציה החוצה לשמירת המידע הארגוני בתוך מערכות הארגון בלבד
- Prevent Screenshot – מניעת צילומי מסך בתוך האפליקציה, מניעת הוצאת מידע באמצעות צילומי מסך
- Single Sign On Certificate Authentication – הזדהות מבוססת תעודות המבטיחה הזדהות חזקה

- Single Sign On NTLM / Basic – הזדהות מבוססת NTLM או HTTP Basic מול שרתי WEB ומערכות ארגוניות
- Single Sign On OpenID Connect – הזדהות באמצעות OpenID Connect (OIDC) לצורך הזדהות מול שירות Identity Provider (IDP)
- Single Sign On SAML – הזדהות באמצעות SAML מול שירות Identity Provider
- Users and Groups Management – יכולת של אפליקציות ליצור, למחוק, לעדכן ולקרוא משתמשים וקבוצות בארגון

האתגר

פיתוח יכולות מסוג זה עבור האפליקציות הארגוניות יאריך את זמני הפיתוח באופן משמעותי ויחייב התמחויות פיתוח שבדרך כלל אינן קיימות בצוותי הפיתוח הארגוני.

בנוסף פיתוח יכולות כאלה באופן ייעודי עבור כל אפליקציה יסבך את הפיתוח, יגרור בעיות אמינות וקושי רב לשמור על עדכנות מול טכנולוגיות האבטחה המתעדכנות חדשות לבקרים.

ואם זה לא מספיק, הרי שארגונים רבים פועלים תחת תקינות מסוימות (GDPR, HIPAA וכד') ופיתוח יכולות ניהול ואבטחה התואמים לדרישות אלה הנו אתגר גדול אף יותר.

אם כך כיצד מתמודדים עם האתגר?

כשמדובר בארגונים (הרבים במקרה זה) שבהם מיושם פתרון VMware Workspace ONE (Airwatch), הפתרון מאוד פשוט.

VMware מספקת ללקוחותיה קיט פיתוח ייעודי Workspace ONE Software development Kit, שמבוסס על קבוצת ספריות קוד המאפשרות למפתחים בארגון ליישם בכל אפליקציה שהם מפתחים את היכולות המצוינות במסמך זה בתוך דקות.

התוצאה, תהיה אפליקציות ארגוניות ברמת אנטרפרייז שניתן לנהל ולאבטח אותן באמצעות ממשק הניהול של Workspace ONE בדיוק כפי שמנהלים את האפליקציות האחרות של VMware (Boxer, Secure Content Locker וכד').

מעוניינים בפרטים ומידע נוסף בנושא?

פנו אלינו, **מוביסק טכנולוגיות** שמובילה משנת 2011 את נושא הניידות הארגונית בישראל.

חברת מוביסק מתמחה מיום הקמתה בתכנון, יישום ותחזוקת פתרון VMware Workspace ONE ואחראית למרבית בסיס ההתקנות הגדול בישראל עם מאות התקנות בארגונים המובילים בארץ.

info@mobisec.co.il