29 מאי, 2014
כ"ט אייר, תשע"ד
תקמ. 2014-1772

לכבוד:
מרב קדם, מנהלת מינהל הרכש הממשלתי
משרד האוצר

הנדון: **הוספת שירותי ניהול ואכיפת מדיניות במכשירים ניידים במסגרת הארכת ההתקשרות במכרז ממם-1-2010 - רכישת מוצרי MDM במסגרת המכרז המרכזי**

רקע

1. לאחרונה עלה צורך לספק פתרונות בתחום ניהול מרכזי של מכשירים ניידים, אשר יאפשרו בין היתר אבטחת הדואר הארגוני, היומן הארגוני, רשימת אנשי הקשר האירגונית וקבצים, מניעת הצורך לשמירת סיסמת הארגון על המכשיר, ניטור ודיווח על מצב מדיניות האבטחה של המכשיר וזיהוי מכשיר פרוץ, אפשרות לזיהוי התנהגות חשודה של מכשירים אירגוניים המחוברים למערכת, אפשרות לסיסמה על המכשיר שאינה תואמת לסיסמת הארגון של המשתמש, אכיפת מדיניות אבטחת מידע ארגונית כולל מנגנון לטיפול בהפרת מדיניות, תמיכה בהפצת יישומים והסרתם, תמיכה באפליקציות ארגוניות, וכן תמיכה בהפצת תוכן ארגוני, הגבלתו והסרתו.
2. מוצרי Mobile Device Management - MDM כוללים יכולות של:
   1) כלי לניהול מדיניות ותצורה למכשירים ניידים – טלפונים חכמים ומחשבי לוח מבוססי מערכות הפעלה של טלפונים חכמים.
   2) פתרון ארגוני שיאפשר שימוש במכשירים ניידים באופן מאובטח לשם גישה וסנכרון של משתמשי הארגון הניידים לנתונים של הארגון כגון דואר, יומן ואנשי קשר.
3. הצורך בפתרון MDM קיבל מישנה תוקף במהלך 2012 עם התרחבות תופעת ה- Bring Your Own Device - BYOD שהולכת ומתפשטת בארגונים, עובדים רוכשים טלפונים חכמים ומחשבי לוח ומבקשים להשתמש בהם גם לצורכי עבודה**.** פתרון MDM ארגוני צריך לתת מענה הן למכשירים בבעלות הארגון והן למכשירים בבעלות משתמש הקצה.
4. פתרון MDM מאפשר התקנת יישומים וסנכרון נתונים באופן מבוקר תוך כדי התייחסות לרמות אבטחה ומידור הנאכפות על מכשיר הקצה**.** יישום MDM מאפשר בין היתר אכיפת סיסמת הזדהות, השתלטות מרחוק, הפצה של אפליקציות ארגוניות ומחיקת אפליקציות ומידע ממכשיר גנוב**.**

מטרת המסמך

5. המסמך מהווה כלי עזר למינהל הרכש הממשלתי במסגרת קבלת החלטות בדבר:
   1) הרחבת ההתקשרות עם חברות הסלולר, במסגרת מכרז ממם 1-2010 בנדון, בפטור ממכרז, לצורך אספקת מוצרי MDM**.**
   2) הגדרת השירותים שיסופקו במכרז המרכזי הבא שייכתב לאספקת שירותי סלולאר.

מצב קיים

6. בשוק הישראלי קיימת חדירה כמעט מלאה של שימוש במכשירים ניידים חכמים ושימוש בהם לסנכרון דואר יומן ואנשי קשר. החדירה הרחבה הזאת מביאה לדרישה מצד משתמשי המכשירים החכמים להרחבה של השירותים הניתנים לאפליקציות אירגוניות נוספות (מעבר לסנכרון דואר יומן ואנשי קשר).
7. על פי נתונים מסקר הנעשה על ידי STKI:
   שימוש במוצרי MDM עבר את רף ה 80% בשוק הישראלי בשנת 2013.
   בשנת 2011 - 17% מהארגונים קיים מוצר MDM.

בשנת 2013 - 81% מהארגונים הוטמע או בתהליך הטמעת מוצר MDM.

8. כיום, ארגונים לעתים קרובות "תופרים" יחד מספר פתרונות נקודתיים כדי לאפשר פתרון ניידות. לעתים קרובות, פתרונות נקודתיים אלו מגיעים ממורשת המחשוב הנייח ואינן מותאמים לניידות, מה שמוביל לחוויית משתמש ירודה ופתרון יקר שלא מנוצל כיאות.
9. יחד עם הרחבת החדירה של פתרון ה-MDM בארגונים השונים, מתרחב ה-MDM גם ביכולותיו- מתפקיד הגדרת המדיניות האירגונית לשימוש במכשירים ניידים לתפקיד ניהול כל החלק הנייד של הארגון. בכך, מאפשר ה- MDM לארגון להפוך להיות "ארגון נייד" כמתחייב מהשינויים הטכנולוגיים ומדרישות העולות הן מצד העובדים והן מצד הלקוחות.

צורך ממשלתי

10. עד לפני מספר שנים סנכרון דואר יומן ואנשי קשר למכשירים ניידים נעשה באופן כמעט בלעדי באמצעות מכשירי בלאקברי, טלפון חכם שניתן על-ידי הארגון לשכבת הנהלה מצומצמת- בעל מנגנון אבטחת מידע מובנה. עם יציאת טלפונים חכמים חדשים כדוגמת אייפון החלו הארגונים ליישם מוצרי MDM כדי לענות על דרישות אבטחת המידע שהיו מובנות בפתרון הבלאקברי.
11. המגזר הממשלתי בדומה לשוק העולמי בכלל והישראלי בפרט עבר משימוש בבלאקברי לשימוש במכשירים ניידים אחרים. הכניסה המסיבית של מכשירים חכמים החלה באמצע 2013 לאחר עדכון ההתקשרות האחרונה של הממשלה עם חברת פלאפון. כתוצאה מכך, החלה דרישה של משתמשי קצה לסנכרון שירותי דואר, יומן ואנשי קשר למכשירים החכמים. יחד עם זאת, לא סופק פתרון לאבטחת שירותים אלו ויישומים נוספים באמצעות המכשירים החכמים. שירותי האבטחה שניתנו במכשירי הבלאקברי אינם קיימים במכשירים החכמים שזכו במכרז המרכזי.
12. ודוק, בעוד שבעת הגישה למשאבי הארגון דרך מחשב ארגוני נייח נדרשת הזדהות לפחות ברמת משתמש וסיסמה, וישנם אף משרדים ממשלתיים הדורשים הזדהות באמצעות כרטיס עובד- הגישה לאותו מידע דרך טלפונים חכמים ומחשבי לוח ללא MDM מתבצעת ללא שום הזדהות.
13. המצב הקיים יכול לגרום לדליפת מידע רגיש מהארגון כתוצאה מאובדן מכשיר נייד או בהיעדר השגחת בעליו.
14. לאור האמור לעיל, ובשים לב לצורך המיידי שהתעורר, נבחנו האפשרויות להתקנת יישומים וסנכרון נתונים באופן מבוקר, באמצעות MDM.

הפתרון הטכנולוגי הנדרש

15. לצורך הגנה על המידע הארגוני נדרש מענה של פתרון הגנה משולב הכולל:
   1) **הגנה על המכשיר הנייד**: המכשיר הסלולארי הינו מחשב נייד קטן לכל דבר, עליו נשמרים מסמכי דואר, יומן ואנשי קשר. במקרה של אובדן או גנבה של המכשיר קיימת סכנה שתבוצע גישה למידע הרגיש שאגור במכשיר הנייד. לצורך כך, נדרש ליישם פרוטוקול הצפנה של המידע החסוי השמור בזיכרון של המכשיר, שמירה על עדכניות מערכת ההפעלה ,עדכוני אבטחה, יישום הזדהות משתמש למכשיר ועוד.
   2) **הגנה על תווך התקשורת וקישור המכשיר הנייד לרשת הארגונית**: נדרש להפריד בין שירותים ראשיים (שירותים שלא קשורים לארגון) ושירותים משניים (העברת פרטי דואר וגלישה למערכות ארגוניות) על ידי הטמעה של פתרון gateway (שער כניסה לרשת הארגונית) בין המכשיר הנייד לשרת הדואר הארגוני. כמו כן, חשוב ליישם פיקוח ובקרת תכנים וסינון מזיקים בתהליך העברת המידע בין הרשת הארגונית למכשיר הנייד ולהיפך ואף רצוי להפעיל חיווי על פעולות שונות במערכת.
   3) **הגנה בתוך הרשת הארגונית**: ניהול מרכזי והחלת מדיניות אחידה לכלל המכשירים הניידים בארגון ללא יכולת של המשתמש לשנות את ההגדרות. המדיניות צריכה לכלול אכיפה של הצפנת התווך, נעילת המכשיר, אכיפת סיסמה, הגבלת פעילות אפליקציות במכשיר, אבטחת התקני הקישור, בקרה על גלישה והורדת קבצים ואפליקציות ועוד.

סיכום

16. הצורך ביישום MDM במגזר הממשלתי הינו כיום מיידי, והוא התחדד במהלך 2013, עם כניסתם המסיבית של הטלפונים החכמים למשרדי הממשלה. צפוי כי הארגונים ימשיכו לתמוך במשתמשים ניידים והתקנים ניידים, ולכן מידע ארגוני ימשיך להיות נגיש לאותם משתמשים באמצעות המכשירים הניידים.
17. צפוי כי הצורך בפתרון MDM שיענה לצרכים השונים של המשתמשים יוסיף ויגבר בהיעדר סטנדרטיזציה

במכשירים הניידים, ובשל העובדה שיהיו למשתמשים פרופילי ניידות שונים ודרישות שונות לגישה ליישומים ולמידע.

18. יש לגבש מענה עתידי לצורך הממשלתי הברור- הן פונקציונלי והן מכרזי. לצורך כך, יש לספק פתרון ניידות כולל העונה על הצרכים העסקיים ותואם את מדיניות אבטחת המידע של הארגון.
19. הכללת שירותי MDM כחלק בלתי נפרד מהמכרז הסלולרי וכדרישת סף להגשת מועמדות במכרז תמנע את המצב הקיים לפיו משרדי הממשלה מאפשרים חיבור בלתי מאובטח של המכשיר הנייד לארגון. אמליץ לפיכך שבמכרז הסלולרי הבא דרישות האבטחה, לרבות אספת מוצרי MDM, יהיו תנאי סף במכרז.
20. קשה להפריז בעוצמת הסיכון למידע השמור במכשירים החכמים של משתמשי הארגון, בהיעדר מוצרי MDM המוטמעים בו. ממשלת ישראל נמצאת בפיגור משמעותי אחר ארגונים שאינם ממשלתיים, שהקדימו להטמיע מוצרי MDM ופעלו למקסם את ההגנה על המידע הארגוני השמור במכשירים הניידים.

גדעון קונפינו
מנהל חטיבת אבטחת מידע וסייבר
התקשוב הממשלתי

העתקים:
רז הייפרמן, מ"מ הממונה על התקשוב הממשלתי
רווית קורן, מנהלת ההקמה, אגף התקשוב הממשלתי
ניסים בן צרפתי, מינהל הרכש הממשלתי
בני בקשי, מנהל הרשת הממשלתית, מינהל הרכש הממשלתי