Moshav Bnei Zion P.O.Box 151, 60910 Israel Tel. 972-9-7907000 Fax. 972-97442444

סיכום מפגש שולחן-עגול

BYOD – Bring your own device
MDM- Mobile device management

מנחים

סיגל רוסין

פיני כהן

לקוחות נכבדים שלום,

תודה על השתתפותכם במפגש שולחן עגול Round Table בנושא MDM–BYOD.

מצ"ב סיכום עקרי הדברים שעלו במהלך המפגש. במפגש עלו נושאים מהותיים שתומצתו בסיכום כפי שעלו. אין בסיכום זה המלצה גורפת ללקוחות אלא מתן פרספקטיבה והצגה של ההתלבטויות שעלו במפגש כלומר "מהשטח".
לדעת חברת STKI תחום מערכות המידע עומד לעבור מהפכה בכל מה שקשור להתקני הקצה. מהפכה לא פחות דרמטית מהמהפכה שעברנו לפני כעשרים שנה במעבר מהתקני הקצה של DIGITAL\MF ל- PC. נראה שארגונים "מרגישים" שמשהו חשוב קורה אך עדיין לא הפנימו לגמרי את גודל המהפכה ומשמעותה בהקשר של ניהול ותפעול המכשירים, פיתוח המערכות, הפצה התוכנה ועוד .
כסממן לכך שהשוק לא בשל ועדיין מתפתח באופן משמעותי, למרות שלקוחות רכשו כלי ניהול למובייל לפני שנתיים ונמצאים בשימוש ללא בעיות או תקלות מהותיות – עדיין מתבצעת כעת בחינה מחדש לנושא. ארגונים עדיין לא החליטו על מדיניות מסודרת של BYOD לפני בחירת המוצר לתמיכה במובייל. כמו כן, לפי מה שנראה מוצרי ניהול עמדות הקצה ינהלו גם את מכשירי המובייל.
בסוף המסמך ישנו מתווה בסיסי לכניסה לפרויקט בתחום זה.
בברכה,

סיגל רוסין
פיני כהן

תוכן עניינים

רקע 3
הבדלים בין כלי אבטחה וניהול למובייל 3
תוצאות סקר מקדים 5
מדיניות BYOD 8
תהליך הבחירה בכלי MDM 11
אבטחת מידע בכלי MDM 13
המלצות לכניסה לפרויקט 15
נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש 17

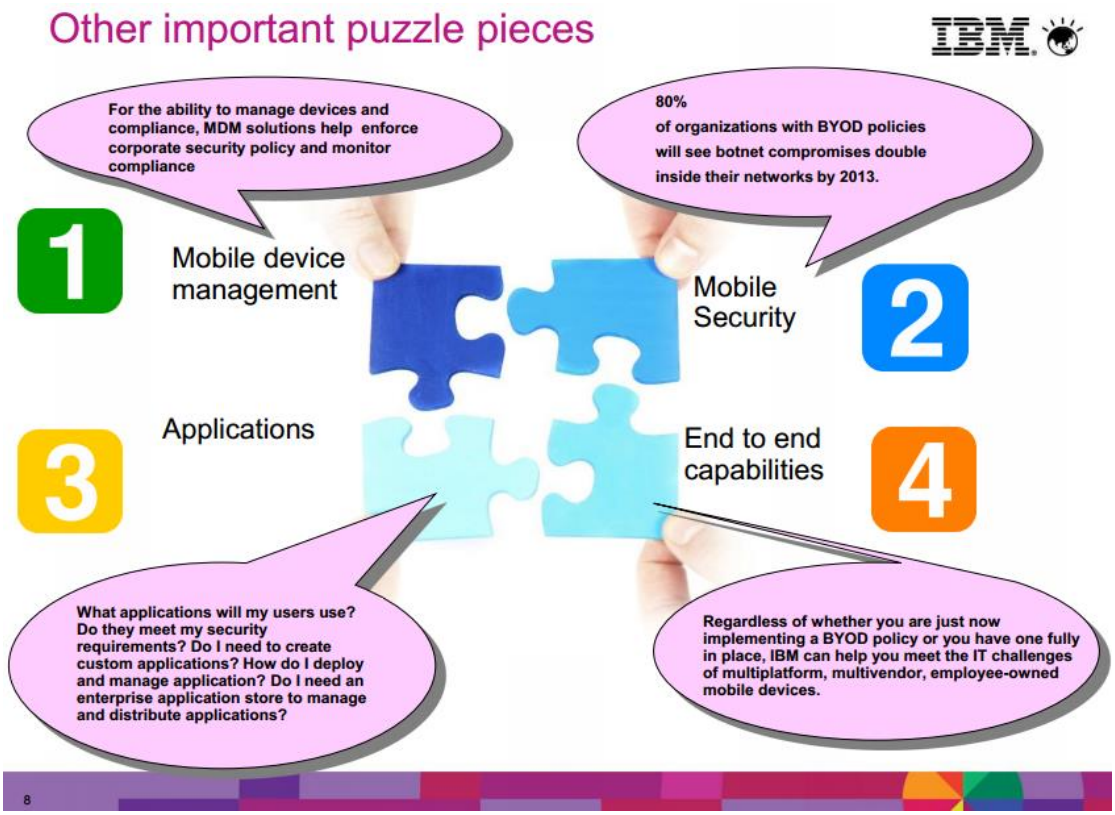
רקע

תופעת ה-BYOD (ר"ת Bring Your Own Device) הולכת ומתפשטת בארגונים. לפיכך נראה כי יותר עובדים רוכשים טלפונים חכמים, טאבלטים ואפילו מחשבים (מחשבי MAC), ומבקשים להשתמש בהם גם לצורכי עבודה. מגמות חדשות נוצרו ויש ליישם את מדיניות ה-BYOD דרך כלים לניהול המכשירים הנקראים MDM (ר"ת Mobile Device Management). כתוצאה מכך, ארגונים ישקיעו בפיתוח או ברכישת כלים לניהול המכשירים שבידי העובדים הכוללים השקעה בתחום האבטחה.

כלי ה- MDM משמשים הן ליישום מדיניות ה- BYOD והן לאבטחה ותמיכה במכשירים הנרכשים על ידי הארגון.

יש לציין כי רוב הלקוחות בשולחן עגול קיבלו סמארטפון מהעבודה לעומת טאבלטים שרכשו בעצמם.

הבדלים בין כלי אבטחה וניהול למובייל



מתוך:
http://www-935.ibm.com/services/multimedia/IBM_5_Steps_Mobile_Strategy_David_Merrill.pdf

Mobile Device Management - MDM- פתרון רב שכבתי המטפל בסוגיית הניהול, השליטה והבקרה, אבטחת המידע של המכשיר הנייד: device activation, enrollment, provisioning.

פתרון MDM מאפשר התקנת יישומים ותוכנות באופן מבוקר, התייחסות מיוחדת לדירוגי אבטחה ומידור, סיסמת הזדהות, השתלטות מרחוק, הפצה של אפליקציות ארגוניות, איתור פריצה במכשיר ומחיקת מידע ממכשיר גנוב.

פתרונות אלו קיימים בפלטפורמת ניהול מהענן software as a service SAAS , או כאופציה של מערכת המוטמעת ומותקנת בארגון on premise, בד"כ בין ה- Exchange server ל FW.

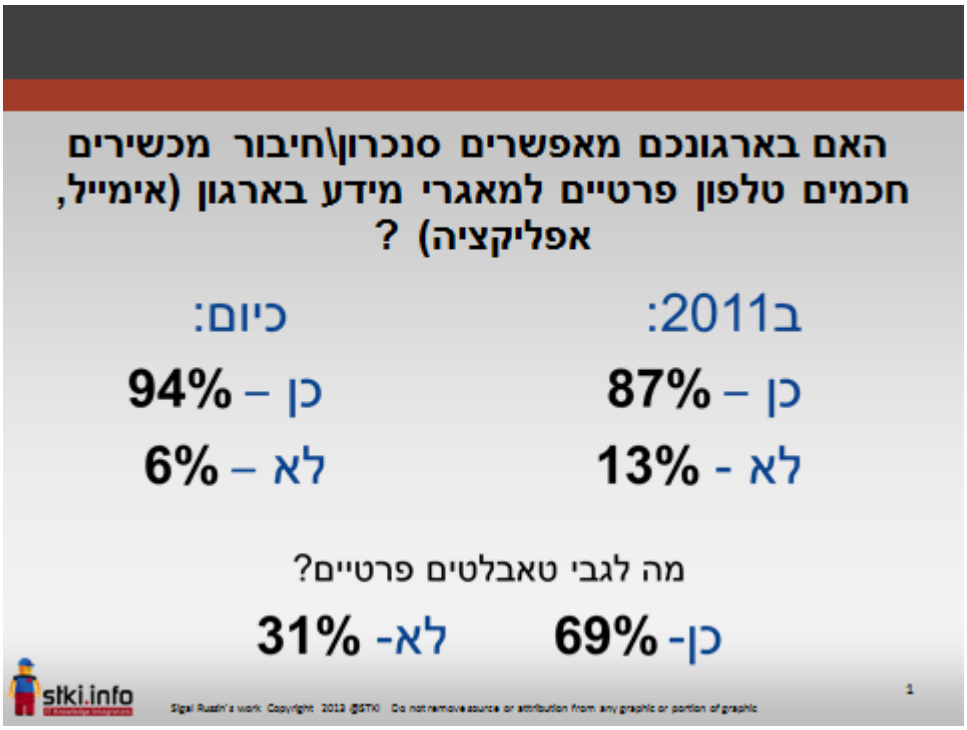
סיגל – דבר שלא הבנתי – האם הפצת התוכנה למכשיר הנייד (חנות האפליקציה או דרך אחרת של הפצה) זה חלק מ- MDM או MAM?

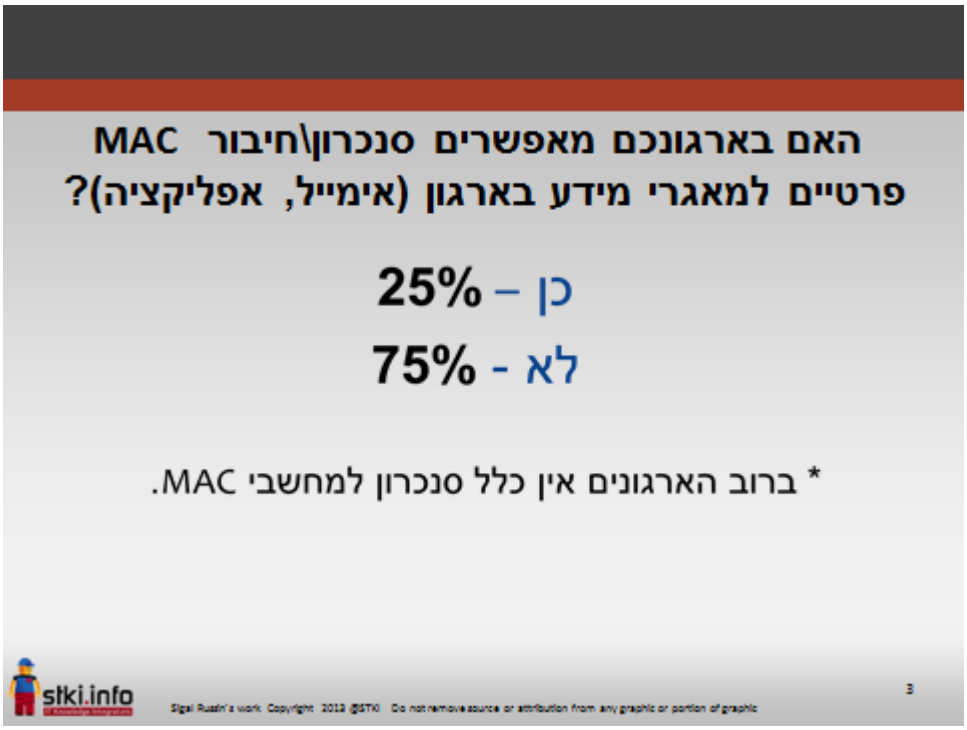
Mobile Application Management -MAM- תוכנה או שירותים האחראים על הקצאה, ניהול ובקרת גישה לאפליקציות שפותחו על ידי הארגון. כלומר, כל אפליקציה ארגונית במכשיר נעטפת על ידי שכבת הגנה ואבטחה ספציפית לה. ישנה התמקדות באפליקציה עצמה: אספקת האפליקציה למכשיר (דרך MARKET), רישוי, תצורה, תחזוקה, מעקב אחר השימוש ואכיפת מדיניות לאותה אפליקציה.

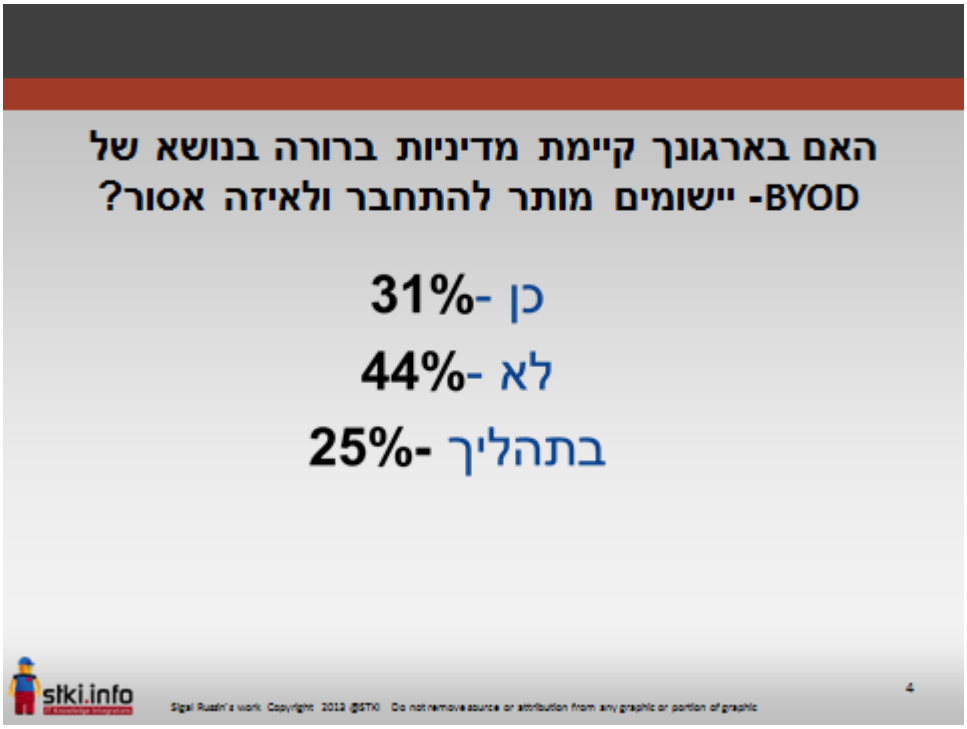
כמו כן, ישנה יכולת למחוק אפליקציות ארגוניות ונתונים מהמכשיר של משתמש קצה ולמנוע גישה עתידית לאפליקציות ארגוניות ומידע השייך אליהם מבלי לגעת פיזית במכשיר.

Secure Data Container- אפליקציה צד שלישית הפועלת כממשק וירטואלי נפרד של "מחסן" אפליקציות, הכולל סיסמת אימות, הצפנה ואבטחה של האימייל הארגוני, היומן ואפליקציות ארגוניות. נקראת גם sandbox. כל האינטראקציה בין המשתמש לארגון מתחרשת בתוך הקונטיינר המוצפן הזה. למעשה זהו חלק ארגוני נפרד במכשיר מהמידע הפרטי הנשלט ומנוהל על ידי מדיניות ארגונית של IT. אפליקציות הנמצאות מחוץ לקונטיינר לא יכולות לגשת לנתונים בתוך. לדוגמה, משתמש לא יהיה מסוגל לגזור ולהדביק מידע מדואר אלקטרוני שהתקבל בקונטיינר לדוא"ל המקומי של המכשיר.

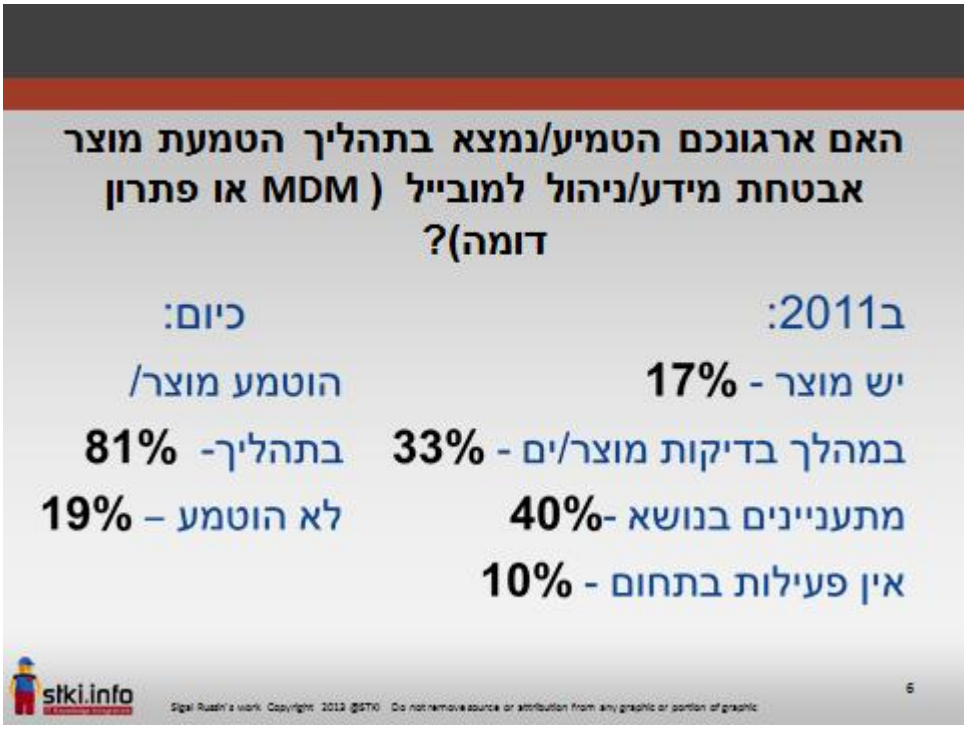
תוצאות סקר מקדים

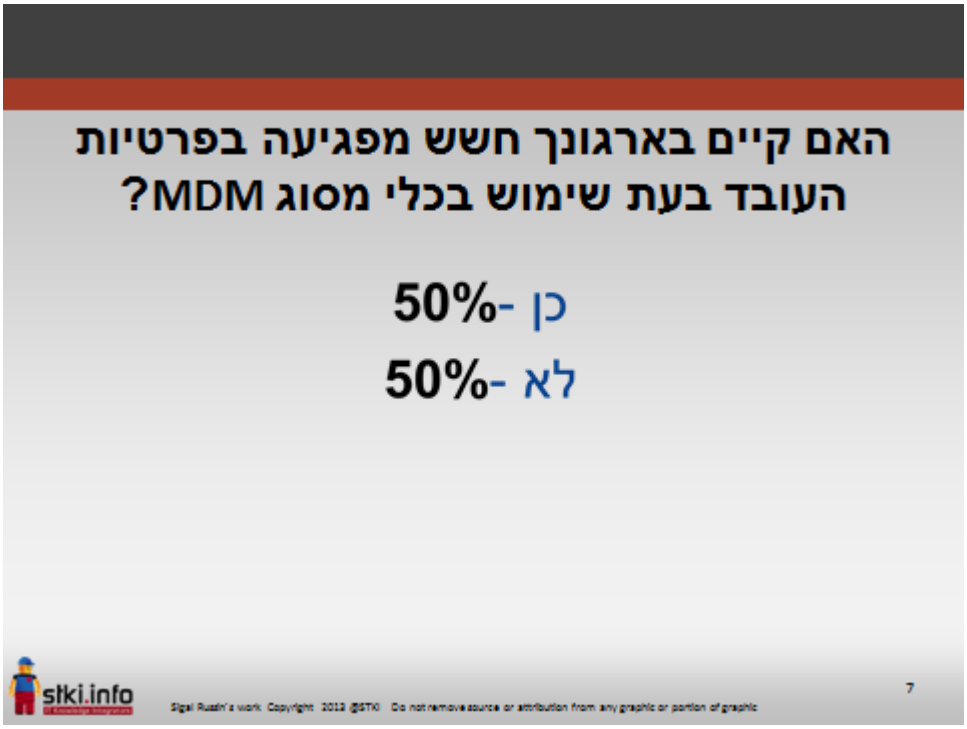





האם בארגונך קיימת מדיניות ברורה בנושא של
BYOD- יישומים מותר להתחבר ולאיזה אסור?
כן -31%
לא -44%
בתהליך -25%
stki.info
4

לשם מה לדעתך חשוב יישום גישת BYOD
בארגונך? (ניתן יותר מתשובה אחת)
63% יעילות העבודה ותפוקת הארגון
50% חדשנות הארגון והמשכיות עסקית
25% חסכון כלכלי לצוות ה IT ולארגון
69% שיפור שביעות רצון העובדים
19% שליטה ותחזוקה טובה יותר של עמדות הקצה
6% אחר
stki.info
5


האם ארגונכם הטמיע/נמצא בתהליך הטמעת מוצר אבטחת מידע/ניהול למובייל (MDM או פתרון דומה)?
ב2011:
יש מוצר - 17%
במהלך בדיקות מוצר/ים - 33%
מתעניינים בנושא -40%
אין פעילות בתחום - 10%
כיום:
הוטמע מוצר/
בתהליך- 81%
לא הוטמע – 19%
stki.info
Sigal Russin's work Copyright 2013 @STKI Do not remove source or attribution from any graphic or portion of graphic
6


האם קיים בארגונך חשש מפגיעה בפרטיות העובד בעת שימוש בכלי מסוג MDM?
כן -50%
לא -50%
stki.info
Sigal Russin's work Copyright 2013 @STKI Do not remove source or attribution from any graphic or portion of graphic
7

מדיניות BYOD

לקוח סיפר כי תהליך ה BYOD החל לפני שנתיים כאשר החליפו תשתיות בארגון. בעקבות כך הארגון רצה להגדיל את שירותי המובייל לעובדים. מטרת הארגון הייתה לחשוף את השירות למובייל בצורה מאובטחת כך שתהיה שמירה על המידע העסקי במכשיר העובד והפרדה בין המידע הפרטי.

הארגון רצה לשלוט על המידע שניתן לראות דרך המובייל.

בהתחלה השירות כלל רק חברי הדירקטוריון ואז הורחב לעובדים נוספים בהתאם לרגולציה PCI 357.

הארגון חיפש מוצר אשר מפריד בין המידע העסקי למידע הפרטי במכשיר. לדוגמה, מחיקת המידע העסקי בלבד מרחוק ללא נגיעה במידע הפרטי. כמו כן, המוצר צריך לספק תמיכה במספר מערכות הפעלה, שליטה מרחוק, דואר אלקטרוני ושירותי WEB מאובטחים.

בהתחלה הארגון השתמש רק בבלאקברי ולאט הרחיב את התמיכה במערכות הפעלה נוספות. לפי הארגון, בלאקברי קשה לתפעול והתמיכה בארגון הייתה בעייתית. המחיר של בלאקברי יקר. לכן, הארגון חיפש כלי זול, קל לתפעול, מאובטח העומד בדרישות ברגולציה.

באותו הזמן הארגון בדק מספר פתרונות לפי כגון : סיטריקס וDME, אך היו להם בעיות בניהול משתמשים ותצורה.

הארגון החליט על GOOD היות והכלי זה עמד ברוב דרישות הארגון לפני שנתיים היות והוא תרם לאבטחת המידע באימייל הארגוני. התעבורה מוצפנת ועוברת דרך שרתים NOC של GOOD (כמו רשת blackberry).

הלקוח תיאר את הכלי : sandbox- ניהול המכשיר מרחוק, הצפנה, ניתן להכתיב מדיניות על המכשיר, הכל בהתאם לדרישות וצרכי ארגון. בנוסף, ניתן למחוק רק מידע ארגוני, ניתן לנעול מכשיר מרחוק ולנהל אותו מרחוק כמו כלי MDM - היו מעט יכולות למוצר בהיבט של ניהול ושליטה. הארגון החליט לוותר על עולם זה לטובת אבטחת מידע וחשיפת המידע הארגוני.

הארגון התחיל רק בסנכרון וניהול המייל הארגוני. במידה ואין גישה לרשת הארגונית לא ניתן לעבוד עם המייל הארגוני. הכי חשוב הוא השימוש באימייל ארגוני ותמיכה שלו בכל מגוון מערכות ההפעלה.

כמו שצוין לארגון היה בלאקברי – מכשיר מאובטח אך GOOD נתנו את האופציה לאבטחה גם במערכות הפעלה שונות מבלאקברי. הארגון מאפשר BYOD לכולם בין אם זה ספק או עובד המביא איתו מכשיר פרטי והארגון מאפשר לו דואר אלקטרוני ארגוני. היות והארגון מחויב להפרדת רשתות מבחינת הרגולציה GOOD נתן מענה לנושא זה .

כיום (לאחר שנתיים) עולם ניהול המובייל השתנה ויש עוד מוצרים. הספקים צריכים לתמוך בכל מערכת הפעלה ועדכונים שיוצאים וקיימים בשוק. לפני שנתיים מגוון המוצרים לא היה רב. כיום GOOD מותקן בארגון על 250 מכשירים. לפי הארגון, נחשב מוצר יקר. יש לGOOD יכולת הפצה פנימית של אפלקיציות או מדיניות וניתן להפיץ בצורה אוטומטית לכל המכשירים. ניתן לעבוד בפורטל ארגוני לעובדים דרך דפדפן מאובטח. אך הדפדפן לא תומך activeX.

הלקוח טען כי בשנה וחצי האחרונות הייתה לGOOD בעיה בעברית, הכל הפך לג'בריש. הייתה בעיה בהקלדה ועריכה ימין-שמאל. לקח ל GOOD הרבה זמן לפתור את הבעיה. אך, כעת בגרסה האחרונה הכל תקין וניתן לעבוד בעברית.

הלקוח טוען שיש עוד בעיות עם המוצר (לדוגמה, אין תמיכה בwindows phone 8) ולכן החליטו כעבור שנתיים לפתוח את הדיון מחדש לבחירת כלי מתאים לניהול מכשירי BYOD.

לקוח אחר תיאר כי מדיניות הBYOD מנטרת את כל מכשירי הארגון בין אם זה עובדים בכירים המביאים מכשירים שונים- יש לבדוק אם המכשיר מקבל מדיניות ואז יכול להסתנכרן לארגון.

מכשירי IOS מקבלים טוב את הpolicy שנקבעה לעומת מכשירי אנדרואיד זה שונה וצריך לשים לב לנושא הtouchdown -הצפנה. מאד מתסכל את העובדים קוד לפתיחת המכשיר אך יש ליצור מודעות בקרב העובדים בנושא האבטחה, אובדן או גניבת מכשיר.

הלקוח בחן את airwatch וגילה כי המוצר לא מנהל תוכן של מייל ארגוני. כיום, הארגון כבר משתמש בגרסה החדשה של zenprise שהיום חלק מסיטריקס. רוב העובדים משתמשים בnative client.

אפליקציות WEB ארגוניות ניתן גם לפתוח דרך zenprise. הארגון כבר מיישם את zenprise שנתיים- הם היו הראשונים בארץ בנושא. הם עובדים כל הזמן בנושא מול המחלקה המשפטית.

בנוסף, יש ל zenprise גם מודל DLP למובייל. הארגון כבר יצא לדרך עם פרויקט של שילוב סביבת הפיתוח לאפליקציות ארגוניות דרך עטיפה של אבטחה, תווך מוצפן והפצה למכשירים בעזרת MDM.

לקוח נוסף מספר כי נושא המובייל מגיע ממחלקת הייצור ולא מאבטחת מידע. האבטחה היא רק חלק מהתמיכה במובייל. כל הנושא התחיל מהדרג הגבוה בו המנהלים עשו שימוש בבלאקברי ורצו ליישם מכשירים חדשים. בהתחלה היה צריך להחליט אם זה רק לשם סנכרון אימייל ארגוני או תמיכה כוללת בכל מכשירי BYOD.

הארגון החליט שהחיבור לאימייל הארגוני הינו רק למכשירי הארגון. אם העובד רצה מייל ארגוני במכשירו הוא היה צריך לקבל אישור מהמנהלים ולקבל מכשיר ארגוני.

בהתחלה היישום היה רק על מכשירי הארגון עקב תאימות מכשירים ומערכות הפעלה. כך הייתה אחידות. אך הדרישה השתנתה ויש לתמוך בסוג המכשיר ומערכת ההפעלה והאבטחה בהתאם. נושא להתמודדות הארגון:

התמיכה במגוון סוגי גרסאות ומערכות הפעלה מעבר לבעיית חווית משתמש. יש מערכות הפעלה כמו אנדרואיד בהם הסיכון לוירוס יותר גבוה.

הסבירות בניהול סיכונים- ככל שיש יותר מכשירים המחוברים לארגון כך הפרצה לאבטחה גודלת והסיכון עולה.

תפיסת המשתמש- אם זה מכשיר עסקי מודעות המשתמש יותר גבוהה. אם המכשיר פרטי קשה למצוא מדיניות היות וקיים נושא פרטיות העובד. קשה לסמוך על העובד אם מאבד את המכשיר או המכשיר נשאר ללא נעילה.

תיקון מכשיר BYOD- ישנם הרבה ספקי סלולר בשוק, על העובד לגשת למרכז שירות לתיקון המכשיר.

עדיין לא קיים בארגון מדיניות BYOD. הכל תלוי במחלקה משפטית בין אם השימוש לאותו עובד במכשיר פרטי או עסקי. רצו לממש את המדיניות שיש בלפטופ פרטי או PC על מובייל אבל נמצאים רחוק מזה.

תהליך הבחירה בכלי MDM

לקוח תיאר כי עובד כיום עם 2 סוגי פתרונות למובייל: כלי של sandbox וכלי לאבטחה והצפנת האימייל הארגוני. הלקוח טוען כי GOOD לא עובד תקין עם גלקסי נוטס 2 וקשה למוצר לעמוד בתאימות למערכות ההפעלה.

בGOOD אם המכשיר נגנב או הולך לאיבוד ניתן להפעיל wipe ולמחוק מידע מרחוק- הכל בהתאם למדיניות. ניתן להפעיל מחיקה אוטומטית אחרי מספר הקשות של סיסמא.

לקוח אחרבחן לפני 3 שנים כלי MDM ובדק את GOOD. הלקוח ציין כי זהו לא כלי MDM אלא כלי secure קונטיינר ארגוני מופרד. הארגון מתעניין בדעה של העובדים ונוחות העבודה שלהם דרך הכלי. חשוב לו זמני תגובה מהירים. כל הנושא עלה עם יציאת ווינדוס מובייל לשוק ותמיכה בactive sync באייפון. הדרישות גם במקרה זה הגיעו מההנהלה. אנדרואיד לעומת זאת בהתחלה לא תמך בactive sync .

תהליך בדיקת כלי MDM היה ארוך ומייגע. באותו זמן בשוק היו מספר מתחרים לא בשלים. לעומת היום שיש מאות כלי MDM- כל אחד מציע פתרון. הכל התחיל עם ניהול בלאקברי - ניהול roaming כלים שיודעים להתמודד ונתנו רישיונות לאפליקציות. מי שנתן בזמנו פתרון היה Zenprise.

הכלי הוטמע על אלפי מכשירי אנדרואיד. תהליך בקשת הסנכרון מתחיל מהעובד - self service בקשה לסנכרון מייל בוחרים סוג מכשיר ופועלים על פי הוראות העובד פותח BPM בהתאם לאותו המכשיר והגרסה.

לפני הסנכרון למכשיר BYOD על העובד לחתום כי הוא לא פורץ את מכשירו אחרת שירותי MDM יבוטלו. כלומר, הכלי יודע לזהות פריצה ולהתריע על כך. לפי המדיניות, לא מפעילים שירותי location בגלל פרטיות העובד.

הארגון מתייחס לכל המכשירים כפרטיים ולא תומך בהפרדה בין הסביבה הפרטית לעסקית. חובה ניהול של קוד על המכשיר.

לקוח נוסף סיפר כי בהתחלה היה היו רק מכשירי בלאקברי לשכבת ההנהלה הבכירה, והסנכרון לאימייל הארגוני עבד דרך active sync והתאים לתנאי לרגולציה. השינוי בארגון התחיל דרך סמארטפונים חדשים שצצו בשוק כדוגמת אייפון. מי שהתחיל ללחוץ על נושא התמיכה במכשירים שונים הייתה ההנהלה. לכן, הIT נאלץ להתמודד עם מערכות הפעלה שונות וגרסאות חדשות. בהמשך הדרישה לניהול מכשירי המובייל באה מעובדי קבלן שקיבלו

מכשירים מהחברות שלהם. מנהלי הארגון דרשו כי יהיה חיבור לאימייל הארגוני לעובדים אילו לשם יעילות העבודה.

לפי אותו לקוח, סמארטפון הוא סוג מכשיר מתחום המחשוב ויש להתייחס אליו כמו מחשב נייד. הארגון ניסה לתרגם מדיניות למכשירי המובייל בהתאם לרגולציה והבין שקשה כי רוב המכשירים לא מוצפנים וכל מכשירי שייך למדיניות של מערכת הפעלה אחרת. לדוגמה, IOS קיימת הצפנה והיא פריצה לעומת, אנדרואיד שאין הצפנה ולכן יש להשתמש ב-Touchdown(הצפנה לסנכרון אימייל, אנשי קשר וכדומה באנדרואיד). במידה ועובדים רצו הצפנה במכשיר האנדרואיד שלהם הם שילמו פרטית עבור פתרון לRMS העולה בסביבות 170 ₪.

יש עובדים שויתרו על ההצפנה במכשיר נייד. האם הארגון הסכים שיקבלו מיילים פנימיים אפילו שאין הצפנה? נראה מוזר...

הארגון חיפש פתרון MDM לשם אבטחה malware בו תהיה מדיניות ארגונית מופרדת הכוללת הגנה, הצפנה, נעילה, מחיקה מרחוק של מידע.

כיום, הארגון מאפשר חיבור מכשירים פרטיים דרך החתמת העובד על נוהל בו מוסכם כי יותקנו אמצעי הגנה על המכשיר ואם יקרה משהו המידע ימחק מרחוק. בהסכם, העובד חייב לדווח על אובדן מכשיר. באם ישנה בעיה טכנית העובד לא יגיע אל הארגון אלא יטפל פרטית. כיום אין לארגון פתרון הצפנה אלא רק פתרון זמני והם מחפשים עדיין מענה. הארגון ניסה ליישם Sybase afaria של SAP אך הפרוייקט לא צלח.. כמו כן, הארגון בחן מוצר MDM הנקרא FAMOC http://www.fancyfon.com/ אך הוא לא ענה על כל צרכי הארגון. הארגון ניסה ליישם כלי בשם Letmobile .

זהו פתרון לסנכרון והצפנת המייל הארגוני היות ושום מידע לא יורד למכשיר. התצוגה הינה דרך ה-web ולא ירד שום מידע לענן חיצוני. ניתן לסנכרן גם אופליין. אך לפי הלקוח הייתה בעיה בחוויית המשתמש בהצגת מסמכים. הספק ישב אצלהם 4 חודשים להרמת המערכת אך לא הצליח.

בימים אלה הארגון עובר POC עם airwatch. זהו פתרון עובד SSL VPN למייל דרך wifi . ניהול האימייל הארגוני דרך השימוש בקליינט המובנה של כל מכשיר (לא כל כך מאובטח). התווך מוצפן וההזדהות היא עם מנגנונים שהארגון הגדיר לעצמו.

לקוח אחר תיאר כי יש להבין איפה ההבדל בין מכשיר ארגוני לפרטי, גם אם העובד חתם ואישר איפה ההגבלה ואיזה נהלים על הארגון לקבוע. לכן יש לקבוע במדיניות: כמות המכשירים, תפיסת העובד לגבי מכשיר פרטי או ארגוני, מערכות הפעלה, פריצה במכשיר, עדכון גרסאות ועוד.

כיום הארגון מממש (מעל שנה) ומיישם GOOD גם על מכשירים פרטיים- סה"כ יותר מ1000 מכשירים כולל טאבלטים. יש הפרדה בGOOD בין המידע בפרטי של העובד למידע

העסקי. זה תורם לארגון עקב יישום הפרדת רשתות. על העובד לשמור על המכשיר ולהיזהר מאובדן. בדומה לתפיסה הנהוגה בלפטופים (השארה ברכב או פתוח).

יש לציין כי לפי הלקוח כל המחלקות בארגון מבקשות יישום BYOD . הארגון בוחן דוחות שימוש בGOOD בקרב העובדים. לא נערך סקר של העובדים לפני הטמעת הכלי ועובדים התלוננו על פתיחת מסמכים בעברית, איטיות, קושי לדעת אילו אפליקציות פותחות סוגי מסמכים.

הארגון אפשר 2 אפליקציות בסיסיות איתם ניתן לפתוח מסמכים ארגוניים. הכל תלוי במדיניות שהארגון קבע לעצמו. אם הארגון אפשר לעובד להוריד אפליקציה לצפייה במסמכים שלו- אילו יהיו רק המסמכים הפרטיים.

בנוסף, הארגון נמצא בתהליך הטמעת אנטי וירוס-סימנטק למובייל. הארגון כל הזמן בקשר עם ספקים ויועצים לגבי נושא האבטחה במובייל אך עדיין בודק את הנושא.

במידה ויש בעיות טכניות למכשיר BYOD העובד הולך למרכז שירות בו מוחקים לו את GOOD מהמכשיר לצורך תיקון.

אבטחת מידע בכלי MDM

לדעת אחד הלקוחות, הבעיה בGOOD הינה חווית המשתמש. למשל, לקוח תיאר כי לא הצליחו לעשות attach לתמונות מהמכשיר לאימייל הארגוני. לכן, המוצר לא נבחר. הארגון הסתכל על אבטחה מאשר על חווית המשתמש. GOOD לא מאפשר למידע חיצוני (פרטי) כמו תמונות להיכנס למידע הארגוני וזה יוצא בעיה. הארגון טוען כי מטרתו היא לנהל מידע עסקי במובייל הכולל שליטה מרחוק, תחזוקה, הפצה,ועוד. העולם ילך לניהול תחנות קצה וכלי ה- MDM לאט ייעלמו.

בעיות נוספות הקיימות במוצר: באנדרואיד נושא הmalware בא לידי ביטוי דרך התקנת אפליקציות מהMARKET. האם הפוגען יכול להיכנס למוצר sandbox כמו GOOD? לקוח אחר ציין כי GOODלא מזהה jailbreak של אייפון לדוגמה.

אחד הלקוחות הזהיר בשימוש VPN מלא במכשיר היות ואין שליטה על תוכנות ריגול למיניהם. בתוך התווך המאובטח הכל פתוח ויכול לחדור לשם וירוס.יש להגביל לפי סגמנט. כמו כן, יש בעיה עם הורדת אפליקציות מהmarket באנדרואיד שנגועות באנטי וירוס ואנטי וירוס לא מצליח לזהות זאת. אנטי וירוס למובייל כולל עלויות גבוהות של ביצועים. אם יש אנטי וירוס לעמדות קצה כדאי לבדוק אם קיימים רישיונות חינם למובייל.

לקוחות רבים נתקלים בקושי של תפעול המכשיר ובעיות טכניות. האם האחריות חלה על הservice desk בארגון או ספקי השירות מהם המכשיר נמכר. רוב הארגונים הIT אחראי רק על סנכרון לאימייל הארגוני. פתרון שנקרא selectivewipe מוודא יש policy שמחייב למחוק מידע אם הולכים לתקן את המכשיר אצל ספק שירות.

לקוח מהמגזר הביטחוני אפשר BYOD והחליט על סגירת המצלמה במובייל ואפשר רק סנכרון יומן ואימייל. עקב תמיכת הארגון במובייל כמות התקלות שנפתחות לאייפון לעומת אנדרואיד הוא 1 ל10 פניות לHD. יש כ- 1500 מכשירים מנוהלים.
השאלה מי מנהל את הMDM?נושא המדיניות הוא בידי אבטחת מידע ותפעול המוצר הוא בידי מחלקת תפעול HD.

לקוח אחר מתאר כי הארגון עושה שימוש באפליקציות ארגוניות בסיסיות כגון :יומן, אימייל, אנשי קשר. כל מי שרוצה לסנכרן אפליקציות אילו עובד אך ורק מול GOOD. הארגון חסם סנכרון מובייל דרך המחשב. ניסו להתקין אנטי וירוס לאימייל הארגוני עם lacon security אך המוצר לא הצליח לזהות אם נכנס וירוס למייל הארגוני דרך GOOD. כיום גם נושא האפליקציות העסקיות הארגוניות כגון salesforce CRM נבדקות דרך מוצר של סיטריקס.
נושא האפליקציות הארגוניות יותר רגישה היות וישנה פחות הגנה עליהם ולכן יש להתאים כלי המספק הגנה ואבטחה לאפליקציות כולל ניהול מרחוק שלהם.
חווית משתמש בGOOD היה פחות מהותי לארגון. כל נושא ניהול מסמכים, אפליקציות, מיילים- משתמש לא מרוצים וטוענים כי רוצים שכל האפליקציות הארגוניות יהיו חלק מהטלפון שלהם ולא סביבה ארגונית מבודדת. כמו כן GOOD לא מזהה keylogger.

לקוח נוסף מספר כי חיפשו במשך שנתיים מוצר לניהול המובייל. המון מוצרים קיימים אך לא עושים כל מה שהארגון דורש. קיימים סיכונים תפעוליים של אבטחת מידע בהטמעת מוצר. נושא הBYOD מחולק לקביעת מדיניות ותפעול המוצר. הארגון לא הצליח בהטמעת afaria Sybase. הארגון התחיל עם עבודה דרך active sync אך נפסל בבדיקת חדירות לארגון ואבטחה ולכן חיפשו מוצר sandbox המבצע הפרדה לפי מדיניות. לכן, הארגון בחן את GOODו DME. מאד חשוב לארגון חווית המשתמש. לכן, נתנו לקבוצת מנהלים בכירים לנסות לעבוד עם DME . מנהלים התאכזבו מGOOD בגלל נושא העברית, סוללה נגמרת במהירות וגם delayבזמן תגובה.
גם ב DME היו בעיות תחילה והתגברו עליהם. כיום (לאחר שנה) הארגון עם 500 מכשירים ארגוניים מנוהלים ושוקל לקנות עוד 30 רישיונות של DME . המוצר כולל קלות ופשטות. מכשיר פרוץ לא יתחבר כלל לארגון – אלא יינעל. המשתמשים מודעים לנושא.
גם בארגון יש בעיות אך עשו סקר סיכונים לפני בו נסגרו פערי האבטחה וpenetration test. הספק תפר את הפתרונות שהארגון רצה לדוגמה, גאווה בצד שרת.
הטאבלטים בארגון עובדים עם סיטריקס. כרגע הארגון מחליף את סביבת הטרמינל של סיטריקס ושוקל אם להמשיך עם DME בגלל עלות הרישיונות והתפעול. היות וzenprise נרכשה ע"י סיטריקס שוקלים את הנושא למעבר לטרמינל בארגון שישמש גם במובייל. DME די דומה לGOOD. רק בGOOD אין התרעה על סנכרון לוקאלי דרך המחשב ולכן אפשר להעתיק אנשי קשר ולסנכרן יומן.

לקוח אחר בחן את airwatch והנושא נפל עקב בעיה כספית וחוסר זמינות של תמיכה טכנית במוצר. החברה רצתה מוצר on premise וairwatch הכל עובר דרך ענן. הענן של airwatch אין 100% זמינות לפי החוזה. כיום רץ כ4 חודשים zenprise. כיום יש 4000 מכשירים תומכים ומוסיפים עוד 100. Zenprise מבוסס על ענן של אמזון ולכן יש 100% זמינות.

הארגון ערך סקר משתמשים לבדיקת בעיות ביצועים. הלקוח ציין כי יותר קל להטמיע באייפון מאשר באנדרואיד. רוב המכשירים שהארגון מחלק הם גלקסי 3. יש בעיה מבחינת דחיפת הפרופיל אך touchdown פותר את זה.

יתרון של airwatch מול zenprise הינו נושא התעודות והתקנתם בקלות במכשיר.

הארגון לא עובד עם VPN אלא עם MDM למייל הארגוני וסיטיריקס לכל שאר האפליקציות.

המלצות לכניסה לפרויקט

שלב ראשון: הכנת מסמך מדיניות BYOD בארגון העונה על צרכי הארגון והעובדים. במסגרת המסמך יש להתייחס לפחות לנקודות אלו:

- אילו אפליקציות ארגוניות כל משתמש יכול להיחשף?
- הרשאות גישה פר עובד או פר מחלקה למשאבי הארגון.
- הסכם או נוהל בו העובד חותם כי מאשר לארגון להתקין תוכנות ארגוניות במכשירו הפרטי.
- מכשירים שיתחברו לארגון: מערכות הפעלה מאושרות, גרסאות, סוגי מכשירים (טאבלטים).
- רישיון תוכנה/ אפליקציה ארגונית- מה על הארגון לעשות במידה וירצה להתקין תוכנה על מכשיר העובד?
- תמיכה בכמות מכשירים נוספים- האם יש להגדיל כ"א?
- הגבלת שימוש בפונקציות המכשיר כגון זיהוי קולי, WIFI חיצוני ועוד. כל אלה יכולות לפגוע במידע הארגוני הקיים על מכשיר העובד.
- במידה ועובד IT פגע לא במכוון במכשיר פרטי BYOD- מי ישלם על עלות התיקון?
- בעיה טכנית במכשיר BYOD- למי על העובד לפנות? מרכז שירות או IT בארגון?
- הוספת מדיניות ה BYOD כחלק ממדיניות אבטחת המידע הארגונית למובייל.
- יישום הכלי רק לעובדי הארגון? עובדי outsourcing ? ספקים העובדים עם הארגון וניגשים למאגרי מידע ארגוניים?
- במידה וישנה רגולציה פיננסית על הארגון המפרידה בין מידע הארגוני על המכשיר למידע הפרטי של העובד יש לציין זאת במדיניות ולבחון בהמשך כלים מתאימים.

שלב שני: חינוך ומודעות העובדים בחיבור למשאבי הארגון בעזרת מכשירים פרטיים.

- שימוש במכשיר BYOD הכולל מידע ארגוני בקרב החיים הפרטיים- לדוגמה גישה לילדים, העברת מידע מהמייל הארגוני למייל הפרטי וכדומה.
- במקרה של גניבה או אובדן מכשיר עם גישה למשאבי הארגון על העובד להודיע ישירות לארגון.

- התקנת אפליקציות היכולות לפגוע במכשיר ופעילותו.
- שימוש בסיסמאות על המכשיר.
- תרגול העובדים במקרה וישנה פגיעה של אחת האפליקציות במכשיר- מה עלול לקרות למכשיר ולארגון?

שלב שלישי: סריקת כלי אבטחה למובייל המתאימים לארגון.

- האם דרוש כלי לניהול מכשירי BYOD או לניהול אפליקציות ארגוניות על המכשיר?
- הצפנת המידע הארגוני על המכשיר כולל התווך לארגון.
- סקר בקרב העובדים על מספר כלים שנבחרו והשימוש בהם למען חווית משתמש תקינה.
- בדיקת ביצועי המכשיר עם יישום הכלי הנבחר- האם זה משפיע?
- תמיכה בכלי הנבחר- תמיכה בארץ או בחו"ל, זמינות, תנאי חוזה.
- שימוש בכלי המותקן on premise או החיבור לארגון עובר דרך ענן חיצוני.
- תמיכה באפליקציות ארגוניות במספר גרסאות ומערכות הפעלה.
- האם נדרש חיבור VPN לארגון לשם גישה לאפליקציות ארגוניות? או לסנכרון אימייל ארגוני?
- גרסאות לא נתמכות או מכשירים מיושנים- האם על העובד לקנות מכשיר חדש? או על הארגון לספק לו? האם הכלי הנבחר תומך בכל הגרסאות?
- התקנת הכלי במכשירים- הספק, צוות ה IT או כל עובד בעצמו?
- התייחסות לרגולציה פיננסית במידה וקיימת בארגון בהתאמה לכלי אבטחה למובייל.
- שמירה על פרטיות העובד ובמידע האישי שלו במכשיר.

שלב רביעי: בחירת כלי אחד או יותר (בהתאם לארגון) לניהול ואבטחת המובייל.

- יישום הכלי כפיילוט על מספר עובדים בארגון.
- יצירת APPSTORE ארגוני בו כל האפליקציות הארגוניות יופיעו- האם נדרש בארגון?
- תחזוקה- כמות התקלות בHD גדלה/ קטנה כתוצאה מהכנסת הכלי לארגון.
- במידה ואכן הכלי הצליח כפיילוט- יישום הכלי בכל הארגון.
- תקלות קריטיות בגישה למידע הארגוני דרך המכשיר-כוננות ארגונית, טיפול מהיר בתקלה.
- לאחר מספר חודשים, סקר בקרב העובדים על השימוש בכלי והתמיכה בו.
- כל חצי שנה, לבדוק נהלים ארגוניים בקרב העובדים לגבי מדיניות BYOD שהוגדרה ויישומה דרך כלי האבטחה למובייל. במידה ויש שינוי כלשהו יש להוסיף למדיניות הקיימת ולנסות לבדוק אם הכלי תומך בשינויים.

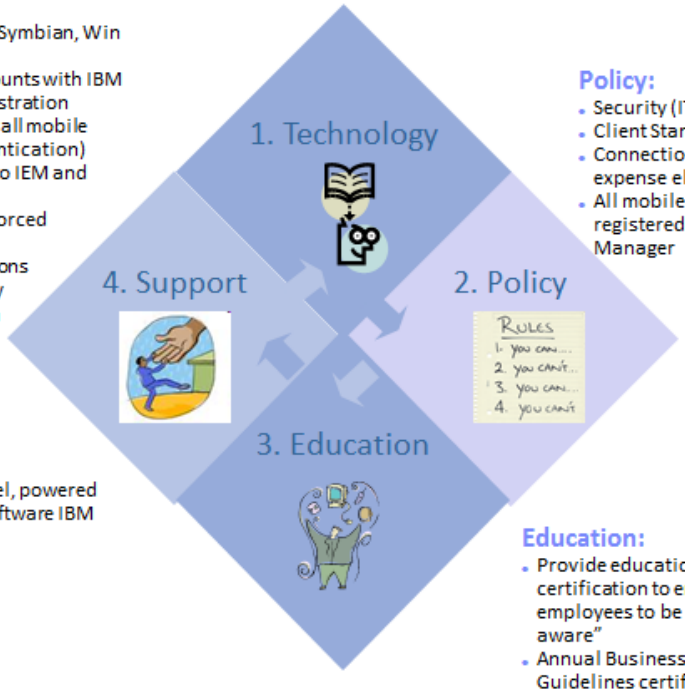
קישור ל case study של IBM:

http://www.esl.dk/media/35735/Fredag%20Carsten%20B%20Andersen%20Personally-owned%20devices%20at%20IBM%20(ISACA).ppt

Addressing the challenges with a four-pronged approach

IBM

Technology:
- Sunset legacy devices (Symbian, Win Mobile)
- Cross link Traveler accounts with IBM Endpoint Manager registration
- Digital Certification for all mobile devices (1st step authentication)
- Cross link digital certs to IEM and network access
- WiFI protection via enforced registration
- Containerization solutions
- Remote wipe capability
- Enable and deploy high value applications



Policy:
- Security (ITCS300)
- Client Standard
- Connection tools and service expense eligibility (CIO 128)
- All mobile devices must be registered in IBM Endpoint Manager

Support:
- Self-support model, powered by IBM's social software IBM Connections

Education:
- Provide education and certification to enable employees to be "security aware"
- Annual Business Conduct Guidelines certification
- "Ask the experts"

11

© 2012 IBM Corporation

נספח מיוחד התייחסות ספקים ויצרנים לנאמר במפגש