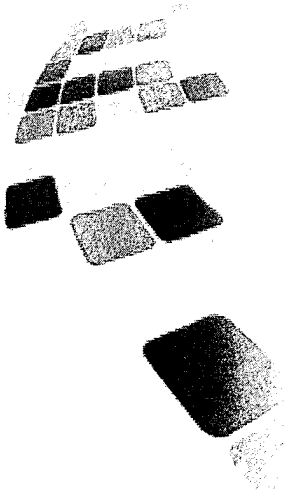
- בלמ"ס -

מדינת ישראל / שירות הביטחון הכללי

הרשות הממלכתית לאבטחת מידע



סקירת טכנולוגיות אבטחה

ל – Smartphones

1. מטרה

1) **למכשיר הנייד החכם – נקודת קצה נוספת ברשת ארגונית לתקשורת הסלולרית**, המאפשרת ליצור קשר זמין ומיידי בין כולם, יש כיום השפעה ניכרת על אופי ההתנהלות של כל ארגון. ארגונים נוטים להקצות מכשיר טלפון נייד לכל עובד. עובדים, מצידם, מעוניינים להשתמש במכשירים הניידים האישיים או הארגוניים שלהם , למטרות ארגוניות. היום קיימת מגמה ברורה של איחוד הטלפוניה הניידת עם מכשירי PDA וחיבורם לרשתות אלחוטיות שונות, על מנת לספק שירותי גלישה ושליחת דואר אלקטרוני באינטרנט יחד עם יכולת של שיתוף מידע ופעולות בין עובדים שונים בארגון. מגמה זו מסייעת להגדיל את הזמינות והיעילות של עובדי הארגון, אשר חלקם נמצאים בתנועה באופן מתמיד ובפיזור גיאוגרפי מקומי או מרוחק במסגרת עבודתם היומית.

2) ארגונים רבים כיום בוחרים להטמיע פתרונות קישור של טלפונים ניידים חכמים, דרך הרשת סלולרית, לרשת הארגון עבור סנכרון פריטי דואר אלקטרוני בזמן אמת וכן גישה למערכות פנימיות, באמצעות אפליקציות קישור מתאימות. הדואר האלקטרוני יכול להכיל מידע אישי, אך במידה רבה גם מידע ארגוני אשר רמת סיווגו יכולה לנוע בין רמת חסוי עסקי לבין רמת סיווג ביטחוני.

3) הפופולאריות ההולכת וגוברת של מכשירים אלה הפכה את "כדאיות" הפגיעה בהם לקוסמת יותר עבור גורמים עוינים ועל כן חייב ארגון לאמץ תפיסה הגנתית רחבה יותר עבור רכיבים אלה, כאשר ההתייחסות הטובה ביותר תהיה כאל <u>רכיבים ניידים המהווים נקודות כניסה ויציאה למידע ארגוני</u>. הקישור של מכשירים ניידים לרשת הארגון מטשטש את הגבולות בין השימוש האישי לזה הארגוני, בין מרכיבים בתוך הרשת הארגונית ומרכיבים מחוץ לרשת הארגונית, וכן את הגבול בין האזורים המאובטחים ברשת (לוגית או פיסית) לאלו שאינם מאובטחים כלל. בקישור זה משתבשת לחלוטין תפיסת ההגנה ההיקפית, כאשר וקטור התקיפה מתחיל במכשיר הנייד המשמש כנקודת קצה ברשת לכל דבר, אך קיים מחוץ לגבולות ההגנה הפיסיים של הארגון וכן מחוץ לגבולות ה – Perimeter ההיסטורי. לפיכך, תפיסת ההגנה גם צריכה להשתנות וליצור הגנה בשכבות וגם ברכיבים השונים, תרתי משמע, תוך כדי החלה של כלל היבטי אבטחת המידע המיושמים במחשבים הניידים המקושרים לארגון, גם על המכשירים הניידים.

4) מסמך זה מאפיין את הדרישות מהקישור, סיכונים קיימים, עקרונות אבטחת המידע ותאור דוגמא לפתרונות אבטחה כוללת שיש ליישם במידה ומקשרים את המכשירים הניידים של עובדי הארגון לרשת הארגון.

2. רקע

1) אחת מהתעשיות בעלות קצב החדירה הגבוה ביותר בשוק היא תעשיית הטלקום אשר מיקדה בשנים האחרונות את מירב המאמץ לפיתוח מואץ של שוק הטלפוניה הניידת המבוססת על תשתית תקשורת סלולארית, אשר שינתה ללא הכר את האופי בו אנשים יוצרים קשר זמין ומיידי.

2) התקשורת הסלולארית הפכה להיות גורם חשוב ולעיתים אף מכריע בחיי היום יום ועל כן יש לה השפעה ניכרת על אופי ההתנהלות של הארגון.

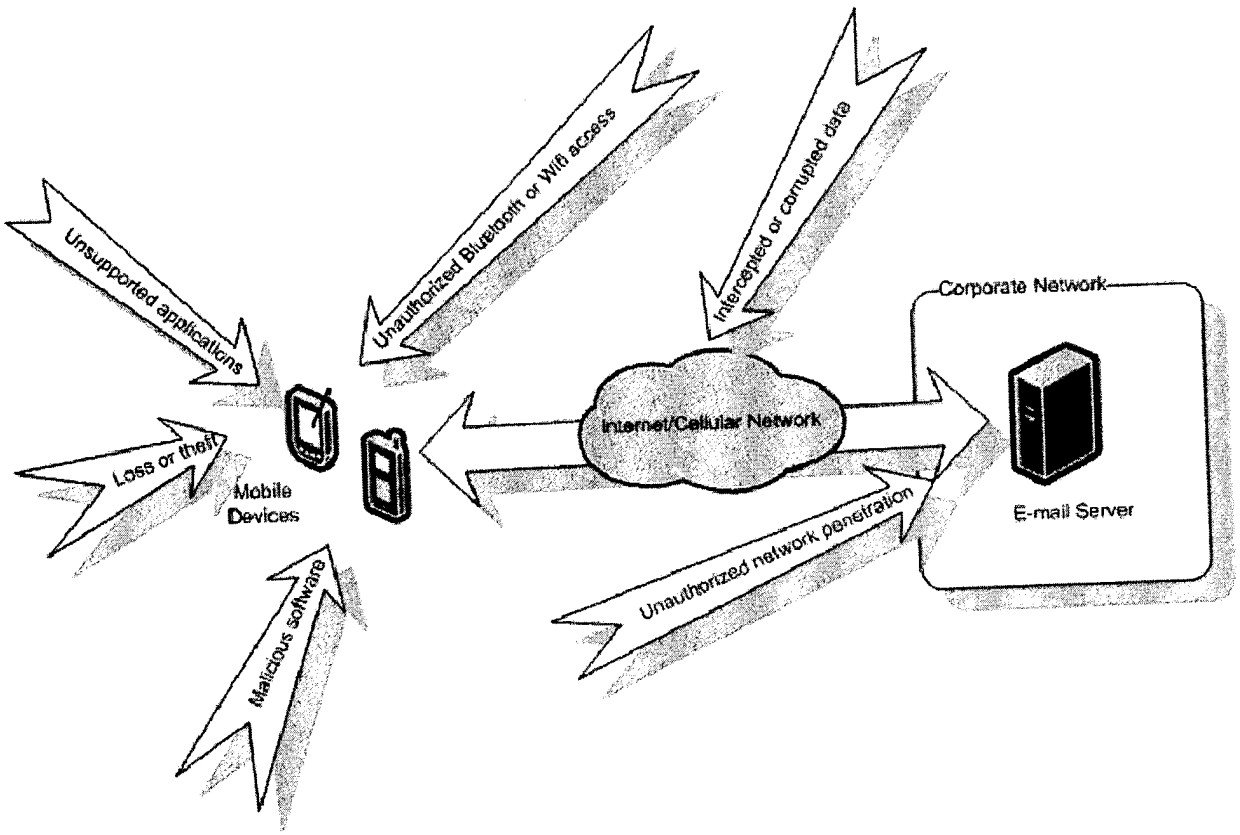
3) ארגונים בוחרים לשלב מכשירים ניידים המשלבים קישוריות לארגון עבור סנכרון של דואר אלקטרוני או גלישה מאובטחת ברשת האינטרנט.

4) המכשירים הניידים יכולים להיות משולבים במערכת ה – Email בארגון על ידי שימוש בחבילת תוכנה בשם Microsoft Exchange ActiveSync אשר קיימת לה בשרת ה – Microsoft Exchange הארגוני. פלטפורמה זו מאפשרת קבלת דואר אלקטרוני בזמן אמת עד למכשיר הסלולר וללא השהיה כמעט. המכשיר הנייד הינו מכשיר חיצוני אשר מתחבר לרשת הארגון למטרת סנכרון מידע ופרטי דואר משרת הדואר. הסיכונים נובעים בעיקר ממאפייני המכשיר הנייד ואופן השימוש בו. המכשיר הנייד מתפקד למעשה כמחשב נייד ממוזער. על כן היבטי אבטחת המידע אמורים להיות זהים לאלו אשר מיושמים במחשבים הניידים המקושרים לארגון.

5) מכיוון שהמידע עובר דרך הרשת הציבורית ישנה חשיבות רבה לאבטח את הקישור בין המכשיר הנייד לשרת הדואר. שליחת נתונים לא מוצפנים עלול לאפשר לגורם חיצוני להאזין לתקשורת (Man in the Middle).

3. מתאר האיומים

<u>שרטוט סכמטי המתאר את מגוון האיומים</u>



קישורים חדשים – סיכונים חדשים

סיכוני אבטחת המידע נובעים בעיקר ממאפייני המכשיר הנייד ואופן השימוש בו. המכשיר הנייד מתפקד למעשה כמחשב נייד ממוזער.

<u>להלן מגוון הסיכונים הקיימים בקישור זה:</u>

- ממשקי הסנכרון - המכשירים הניידים מכילים יכולות קישור אלחוטי לטווח קצר באופן מובנה, ממשקי הכניסה והיציאה כמו InfraRed, Bluetooth ו- Wi-Fi, אשר נועדו להחלפת מידע באופן מהיר עם רכיבי קצה אחרים. <u>ממשקים אלו יוצרים סיכונים רבים:</u>
  - דלף מידע מהמכשיר- **פגיעה בחיסיון המידע הארגוני.**
  - גישה לא מורשית למכשיר ולרשת הארגון דרך הממשקים - **פגיעה באמינות.**

- השתלת סוסים טרויאניים ותוכנות זדוניות על המכשיר ובמשאב ברשת אשר מאפשרים שליטה מרחוק, גישה מלאה למידע ופגיעה כללית במשאב - **פגיעה באמינות, זמינות וחיסיון מידע ארגוני.**

- תוכנות פוגעניות - הטלפונים הניידים החכמים מכילים מערכת הפעלה ייעודית אשר מאפשרים להם להריץ יישומים שונים (לדוגמא Java , Office) וטיפול בקבצי אודיו, ווידאו ותוכן. המכשיר הנייד עלול להיות חשוף לתוכנות זדוניות כגון וירוסים וסוסים טרויאניים. המזיקים מופצים בכמה דרכים: ע"י הודעות מולטימדיה (MMS), הודעות קצרות (SMS), דרך חיבור ה- Bluetooth, תוכנות אשר מותקנות ממקור לא ידוע, גלישה והורדת קבצים ברשת האינטרנט ודרך תשתיות הדואר האלקטרוני. <u>המזיקים מכוונים לבצע את הדברים הבאים:</u>
  - לשתק את הטלפון – **פגיעה בזמינות.**
  - לחשוף מידע ארגוני ולשדרו הלאה - **פגיעה בחיסיון המידע הארגוני.**
  - ליצור מתקפות DoS (Denial of service) על תשתיות הארגון - **פגיעה בזמינות הרשת.**

- גניבת המכשיר הנייד - תעשיית הטלקום פועלת במרץ על מנת לשווק טלפונים ניידים אשר להן שתי תכונות עיקריות: הוספה מתמדת של תכונות, קישוריות ויכולות מעבד לטלפון הנייד ומזעור של המכשיר עצמו עד למשקלים של כ- 100 גרם. תכונות אלה הופכות את המכשיר מצד אחד ליותר יקר ומצד שני מגדיל את הסיכוי לגניבתו כאשר ברוב המקרים מכוון הגנב לשתי מטרות: מכירת המכשיר עצמו לקבלת רווח כספי, והעתקה של נתוני ה – SIM או הזיכרון, כמו פרטי הזדהות מול המפעיל הסלולרי, פרטי הזדהות מול תשתיות הארגון, רשימות מספרי נמענים, הודעות טקסט, יומן שיחות, קבצי תמונה וקול, יומן פגישות וכדומה, ואף של נתוני טלפון כגון פרטי הזדהות הייחודיים מול המפעיל הסלולרי. נתוני ההזדהות השונים יאפשרו לתוקף:
  - להתחזות לגורם מורשה ברשת – **פגיעה באמינות.**
  - לחשוף מידע רגיש נוסף – **פגיעה בחיסיון מידע ארגוני.**
  - לשנות מידע רגיש ואף לחדור לשרתים בתוך הרשת הארגונית – **פגיעה בזמינות שירותים ופגיעה בחיסיון מידע ארגוני.**

- חשיפת מידע רגיש בתווך התקשורת החיצונית – המידע עובר דרך הערוצים הבאים, בהם הוא חשוף להאזנה: רשת התקשורת הקווית הציבורית של ספק התקשורת המרחבית, רשת התקשורת של הספק הסלולרי, רשת התקשורת הסלולרית. במקרה זה מדובר בסיכונים הבאים:
  - חשיפת פרטי הזדהות והתחזות – **פגיעה באמינות.**
  - חשיפת מידע ארגוני – **פגיעה בחיסון מידע ארגוני.**

4. תיאור הפתרון

עקרונות ודרישות לאבטחת שימוש ב – Smartphones.

ארגונים כיום מעוניינים לאפשר גישה של מכשירים ניידים למשאבים ברשת הארגון. לפיכך, הם בוחנים פתרונות **לניהול ואכיפה מרכזיים** של מדיניות של ניהול, בקרה , תפעול, תחזוקה ואבטחת מידע במכשירים הניידים. פתרונות ארגוניים לניהול מכשירים ניידים, פתרונות ה – Mobile Device Management – MDM, מתפתחים לאפשר ניהול ובקרה אחר מכשירים ניידים מסוגים שונים. אתגרי הניהול של המכשירים הניידים גדלים עם הזמן, יחד עם הגידול בכח העיבוד ובזיכרון שלהם, אשר גורר את הפיכתם למכשיר הקישוריות העיקרי של עובדי הארגון (במקרים מסוימים כתחליף למחשב הארגוני שלהם). תשתיות מאובטחות שהוקמו בעבר עבור מערכות הפעלה כמו BlackBerry או Symbian צריכות לתמוך היום במערכות הפעלה חדשות, רבות ושונות, כמו IOS מבית Apple או Android מבית Google.

<u>להלן פירוט של שלל תכונות אבטחת המידע הנדרשות בקישורים של Smartphones לרשת הארגונית:</u>

1. **אכיפת הצפנת התקשורת בין ה - Smartphone לרשת הארגון - הצפנת הקישור בין המכשיר הנייד לרשת הארגון הכרחית על מנת למנוע האזנה לתקשורת וגניבת מידע.** המידע אשר עובר בתווך התקשורת הינו רגיש וחשיפתו לגורם זר עלולה לחשוף מידע רגיש כגון שמות משתמשים, סיסמאות, כתובות דוא"ל ומבנה הארגון. <u>להלן חלופות להצפנת תווך התקשורת:</u>
   - **א.** שילוב עם יכולות הצפנת מובנות במערכת ההפעלה התומכות באלגוריתמי הצפנה תקניים וחזקים (לדוגמא AES).
   - **ב.** יישום של פרוטוקול הצפנה יעודי התומך באלגוריתמי חצפנה תקניים וחזקים (לדוגמא AES).
2. **אכיפת הצפנת מידע בתוך ה – Smartphone** - המכשיר הנייד מתפקד למעשה כמחשב נייד ממוזער ומשמש לשמירת פריטי דואר, פגישות, אנשי קשר ומסמכים. מידע זה מסווג כרגיש וחשיפתו עלולה להזיק לארגון. במידה והמכשיר נגנב או אבד ישנה סכנה שתבוצע גישה למידע אשר שמור במכשיר הנייד. **ברוב המכשירים הניידים כיום, הצפנת המידע אשר שמור במכשיר הנייד מתאפשרת על ידי שימוש בתוכנת צד שלישי בלבד.** <u>להלן חלופות קיימות להצפנת המידע במכשיר הנייד:</u>
   - **א.** הצפנת מידע ארגוני בלבד (תוך יצירת מעטפת בינו לבין מידע פרטי).
   - **ב.** הצפנת כל המידע שבזיכרון המכשיר הנייד.
   - **ג.** הצפנת מידע בכרטיס הזיכרון החיצוני.
3. **אכיפת הזדהות בהדלקת ה - Smartphone, לרבות מדיניות סיסמאות, בהתאם למדיניות הארגונית.**
4. **אכיפת נעילה אוטומטית של ה - Smartphone לאחר פרק זמן ללא שימוש.**

5. **אכיפת מדיניות התקנה ופעילות של תוכנות ב – Smartphone.**
   א. בקרה על שימוש בתוכנות.
   ב. הפצת תוכנות - יכולת לנהל ולתמוך באפליקציות ניידות, לרבות הטמעה, התקנה, עדכונים, מחיקה וחסימה.
   ג. אכיפת מדיניות WhiteList או BlackList.
   ד. בקרה על הורדת תוכנות, בדיקתן ועדכונן כולל עדכוני אבטחה.
   ה. חיווי וניטור - Audit trail/logging.
6. **אכיפת בקרת ממשקים חיצוניים של ה – Smartphone.**
   א. ממשקי תקשורת (Bluetooth ,WiFi).
   ב. מצלמה.
7. **אכיפת מדיניות בקרה מרחוק של גישה למידע -** המכשיר הנייד אינו נמצא תמיד בטווח העין שלנו. עובדה זו מאפשרת לגורם זר על ידי כמה לחיצות להעתיק, למחוק, לצפות במידע אשר מאוחסן במכשיר או אפילו להתקין תוכנה זדונית, כל זאת ללא ידיעתנו. **יש להגדיר נעילה אוטומטית של המכשיר לאחר מספר דקות של אי פעילות, בכדי למנוע גישה במקרה שהמכשיר אינו בטווח העין שלנו או נגנב כאשר היה דלוק. יש לאפשר מחיקה מרחוק של המידע במכשיר לאחר גניבתו.** <u>להלן חלופות קיימות בנושא זה:</u>
   א. Device Remote Wipe.
   ב. Remote Lock.
8. **ניהול רשימות מלאי של כלל ה - Smartphones.**
   א. Inventory – זיהוי של פרטים על המכשיר: מספר טלפון, מערכת הפעלה, פרטי משתמש, שיוך לרשת הארגון, פעילות מכשיר.
   ב. "Jailbreak" detection – זיהוי מערכות הפעלה פרוצות במכשירים הניידים.
   ג. Provisioning – יכולת לאכוף מדיניות גישה למשאבים.
   ד. חיווי של שינויי הגדרות במכשיר הנייד לאורך זמן .
9. **יישום אמצעים למציאת ה - Smartphone הנייד בעת הצורך.**
10. **תמיכה במערכות הפעלה מגוונות של מכשירים ניידים.**
11. **הזדהות של ה – Smartphone עם תעודה דיגיטלית מול השרת** – כולל הפצה של תעודות דיגיטליות.
12. **הצפנת תווך התקשורת בין השרת ל – Smartphone.**
13. **בקרת גישה של ה – Smartphone אל משאבים ברשת** – כתלות ב – Policy Compliance של המכשיר ובהרשאות המשתמש.

8. סיכום

- **תכנון ההגנה המשולבת**

על מנת לתכנן את פתרון האבטחה בקישור המכשירים ניידים לרשת הארגון נדרש להכיר את טכנולוגית הקישוריות, הסיכונים הקיימים, תשתיות הארגון, מנגנוני ההגנה המובנים והדרישות של הארגון. נדרש פתרון הגנה משולב, בצד המכשיר הנייד, בתווך התקשורת ובתוך הרשת הארגונית. הפתרון צריך להיות מנוהל ממקום אחד מרכזי אשר גם יתריע בעת זיהוי של אירועי אבטחת מידע.

- **ההגנה מפני האיום הנייד**

אבטחת המידע בפתרון קישור המכשיר הנייד לרשת הארגונית מתחלקת לשלושה נושאים עיקריים:

- **הגנה על המכשיר הנייד** - המכשיר הנייד מתפקד למעשה כמחשב נייד ממוזער ומשמש לשמירת פריטי דואר, פגישות, אנשי קשר ומסמכים. במידה והמכשיר נגנב או אבד ישנה סכנה שתבוצע גישה למידע הרגיש אשר שמור במכשיר הנייד. נדרש ליישם הצפנה של כל המידע החסוי, לרבות זה השייך למערכת ההפעלה, השמור בזיכרון המכשיר. כמו כן, נדרש לשמור על עדכניות מערכת ההפעלה ועדכוני האבטחה, להטמיע ולנהל תוכנת אנטי וירוס במכשיר, ליישם הזדהות משתמש מתאימה למכשיר, יחד עם נעילה אוטומטית, ליישם נעילת ממשקים וליישם חיווי של פעולות.

- **הגנה על רשת הארגון** - נדרש להפריד שירותים ראשיים (קישור בין המכשיר הנייד לרשת) ומשניים (העברת פרטי דואר וגלישה למערכות) על ידי הטמעה של פתרון Gateway תקשורתי ואפליקטיבי ב – DMZ בין המכשיר הנייד לשרת הדואר הארגוני. נדרש גם ליישם בקרת תכנים וסינון מזיקים בתהליך העברת המידע (והקבצים) בשני הכיוונים בין הרשת הפנימית למכשיר החיצוני. כמו כן, נדרשים הדברים הבאים: שמירה של עדכניות מערכת ההפעלה ועדכוני האבטחה הרלוונטיים של שרת ה – Gatway, שרת הדואר הארגוני ושרתים נוספים בפתרון, הקשחה של מערכת ההפעלה ושירות הדואר, הטמעה וניהול תוכנת אנטי וירוס (רצוי לשלב אפליקציות של יצרנים שונים ברכיבים שונים בפתרון) והפעלת חיווי על פעולות שונות במערכת.

- **הגדרת מדיניות אבטחה בפתרון** מאפשרת ניהול מרכזי, שליטה והחלת מדיניות אחידה לכלל המכשירים הניידים בארגון והיא הכרחית, על מנת להבטיח שהנתונים במכשיר הנייד לא ידלפו לגורמים אחרים או שלא תבוצע פגיעה בארגון דרך המכשיר הנייד. כמו כן, יש לוודא כי המדיניות לא תוכל להשתנות על ידי

המשתמש. הגדרות המדיניות חייבת לכלול את הדברים הבאים: אכיפה של הצפנת תווך חזקה, נעילת המכשיר הנייד, אכיפת מדיניות סיסמת ההפעלה, הגבלה ובקרת פעילות אפליקציות במכשיר הנייד, בקרה ואבטחת ממשקי ה – Bluetooth, Wi-Fi, Infra-Red. כמו כן, נדרשת הצפנת המידע השמור על המכשיר הנייד, בקרה על הגלישה ועל הורדת קבצים ואפליקציות מהאינטרנט, בקרת פעילות שירותי ה – SMS וה - MMS.

- **הגנה על הקישור בין המכשיר הנייד לרשת הארגון** - נדרשת הצפנת תווך התקשורת בין המכשיר הנייד ל – Gateway באמצעות אלגורימי הצפנה תקניים ותקפים, וכן מימוש תהליכי הזדהות חזקים בין המכשיר הנייד והמשתמש ל – Gateway.