הגנה על התקני מובייל, מדוע צריך את זה?

הקדמה

מאמר זה נועד להסביר בעברית ובאופן הכי פשוט והכי פחות טכנולוגי (כמה שניתן), עד כמה חשוב להגן על התקנים ניידים, בעיקר אלה הפועלים בארגונים ומהם הסיכונים שאנחנו והמידע חשופים אליהם.

אופיים של ההתקנים הניידים (מכשירי סמארטפון וטאבלטים) הוא כזה שיש בו ערבוב של מידע פרטי ומידע ארגוני ממקום העבודה המאוחסנים באותו התקן, התקנים שנמצאים במצב מקוון כל העת ובאופן שקוף לחלוטין מחוברים כל העת לרשת הזמינה והקרובה ביותר, מורידים ומעלים באופן תכוף עדכונים ומידע בכל פעם שמתאפשר ועל פי צרכיהם הרציפים של המשתמשים.

תצורה זאת הנה תצורה לא פשוטה מבחינת אבטחה ואם זה לא מספיק אז שפע האפליקציות הזמינות למשתמשים הנו עצום.

לצערנו, לא כל אפליקציה הנה מה שהיא מתיימרת להיות, ולמשתמשים קשה או כמעט בלתי אפשרי לזהות אפליקציות שהן מעשה נוכלות מתוחכם או כאלה שבנוסף למה שהן אמורות לעשות הן גם מבצעות עוד כמה "משימות נסתרות" כגון גניבת מידע מההתקן והעלאה שקטה שלו למקור הגניבה.

בנוסף, גם לא כל רשת היא באמת מה שהיא נראית, משתמשים נתקלים לעיתים קרובות ברשתות שמתחזות לרשתות לגיטימיות אבל בפועל מיירטות מידע או שאפילו משנות מידע שמשודר מן ואל ההתקנים הניידים.

אתגר נוסף הנן מערכות ההפעלה ואפליקציות לגיטימיות שהן בעצמן סובלות לעיתים מחולשות אבטחה, חולשות אלה מתגלות על ידי גורמים מיומנים שמצליחים לנצל אותן על מנת לגנוב או לשנות מידע ואף לשלוט באופן מלא ומרוחק בהתקנים.

מה הופך את ההתקנים הניידים לחשופים לסיכון?

בהשוואה למחשבים ניידים, להתקנים ניידים יש כמה מאפייני התנהגות שמגדילים באופן משמעותי את רמת הסיכון שלהם לחשיפה.

הדבר הראשון והבולט ביותר, התקנים ניידים תמיד דולקים ותמיד מקוונים (או מחפשים תווך) באינטרנט.

ללא שום התערבות של המשתמש, ההתקנים פועלים ברקע, מחפשים ומתחברים לרשתות בעלות מאפיינים התואמים לרשתות שהם הכירו בעבר, זאת אומרת שאם מישהו מתחזה לרשת שההתקן הכיר בעבר, הוא יתחבר אליה ברקע ובאופן אוטומטי.

בגדול, יש שלוש דרכים להתחזות לרשת אלחוטית:

- נתב שלא מוגדר כראוי עלול לאפשר לתוקף להשתלט עליו ואז ליירט או לשנות את התקשורת שעוברת דרכו
- גורם עויין שמחובר לרשת אלחוטית לגיטימית יכול לתקוף גורמים אחרים באותה רשת אלחוטית
- גורמים עויינים יכולים להקים רשת אלחוטית מזוייפת (רשת אלחוטית בשם של רשת אלחוטית לגיטימית) בעזרת כלים כגון Karma Go או Pineapple ואז ליירט את התקשורת שעוברת דרכם

התקנים ניידים שמחפשים רשתות אלחוטיות, משדרים חיפוש רשת בערך 10 פעמים בשנייה, ומתחברים מחדש (reconnecting) לרשת מוכרת בעלת האות החזק ביותר ברשימת הרשתות המוכרות שההתקנים שומרים, אות חזק וקרוב לרשת מוכרת שאיננה מאובטחת הנו מספיק עבור ההתקנים הניידים כדי לתעדף אותו על פני רשת מאובטחת יותר שאולי קיימת באזור.

משתמשים גם נוהגים להתחבר ידנית לרשתות המכילות בשמן את המילה Free, וכך הופכים את עצמם למטרות.

כאשר משתמש מתחבר לרשת מתחזה כזאת, כל המידע המשודר ניתן לניטור, האזנה, שינוי והקלטה והמשתמש עלול בלי ידיעה גם לאשר קבלת תעודה דיגיטלית משירות מזויף שיאפשר התקשרות ברשת "מוצפנת מאובטחת" מול Man in The Middle (MITM).

אבטחת מידע בתקשורת של ההתקנים הניידים הנה סיפור מורכב לאור הכמות ומגוון האפליקציות שבאופן תדיר מחפשות עדכונים להורדה ומשדרות מידע ופרטי משתמשים לשרתים ושירותים ברקע.

אפליקציות אלה לעיתים קרובות נבנו לספק ביצועים מקסימליים על חשבון אבטחה ומייצרות זרם מידע עשיר מאוד ליירוט ולשינוי.

המציאות העגומה היא שיש סיכוי גבוה שמשתמש יתקין אפליקציה או פרופיל זדוני על ההתקן וזאת בגלל שמרבית המשתמשים לא יצליחו לזהות מתי מדובר באפליקציה שהגיעה ממקור לגיטימי ומתי לא.

כברירת מחדל התקני אייפון/אייפד והתקני אנדרואיד יכולים להתקין אפליקציות רק מהחנויות הרשמיות (Apple, Google Play).
במכשירי אפל יש צורך בפריצת המכשיר (Jailbreak) כדי להתקין אפליקציות ממקור אחר, במכשירי אנדרואיד ניתן להגדיר באופן קבוע או חד פעמי את האפשרות להתקנה ממקור שאיננו החנות הרשמית של גוגל.
מקור האפליקציה הנו חשוב ביותר מכיוון שמרבית התוכנות הזדוניות מגיעות ממקורות שאינן החנויות הרשמיות.
נושא לא פחות חשוב הוא שמירה על מערכת הפעלה מעודכנת ואפליקציות מעודכנות, עדכונים אלה, בעיקר עדכוני האבטחה מטפלים בחולשות שנתגלו מאז העדכון האחרון והטיפול בהן מקשה על מנצלי חולשות אלה.
כשמדובר בהתקנים ניידים, האבטחה הפיסית חשובה לא פחות, לעיתים מספיק שההתקן נמצא בידיים "הנכונות" לזמן קצר כדי להתחיל הסתננות.

מדוע יש צורך בהגנה על התקנים ניידים?

התקנים ניידים מכילים כיום אפליקציות, מסמכים, חשבונות משתמשים, דואר אלקטרוני, תמונות וכד', מידע מהסוג שלא נועד לגישה שאיננה מוגבלת ולכן ההתקן חייב להיות מוגן מפני גישה או שימוש שאינם מורשים.
את המידע שמגיע בתצורות ופורמטים שונים ניתן לחלק בגדול לשני סוגים: מידע ארגוני, מידע אישי.
מידע ארגוני הנו מידע הקשור לעסקי הארגון, חשיפה של מידע כזה יכולה לפגוע בעסקי הארגון ואף עלולה לגרום למידע רגיש להגיע למתחרים, מידע כזה בדרך כלל יכלול נכסי מידע (IP), מידע על לקוחות, סודות מסחריים וכד'.
ואם זה לא מספיק רגיש, הרי שמידע ארגוני כולל גם פרטי גישה למידע ארגוני נוסף כגון פרטי חשבונות משתמש או פרופיל VPN או לפעמים אפילו ממש רשימה או בסיס נתונים של חשבונות משתמש וסיסמאות שישמשו לאחר מכן לצורך דריסת רגל בתוך הרשת הארגונית.
סיסמאות כאלה יכולות להופיע במכשירים במספר רב של תצורות, החל מאפליקציות לניהול סיסמאות, דרך קובצי טקסט ועד להודעות קוליות.
המידע האישי, מבחינה טכנית דומה מאוד למידע הארגוני, אבל חשיפתו עלולה לפגוע בבעל ההתקן בעצמו.

המידע האישי יכול לכלול אנשי קשר, מידע על זהות, מידע רפואי, מידע פיננסי, כתובות ומידע על בני משפחה ועוד מידע שמאפשר באופן אגרגטיבי להוביל להתחזות ואף לגניבת זהות.
הנגישות למידע ולמשאבים קיימת ונוחה כיום, סיסמאות מאוחסנות בהתקנים, אפליקציות מבצעות הזדהות אוטומטית (Auto Login) ואפליקציות לניהול סיסמאות מציעות את הסיסמה המתאימה לכל אפליקציה ובקונטקסטים שונים.

בנוסף לעיתים מידע אישי רגיש עלול לכלול מידע משותף כך שחשיפה של מידע רגיש מהתקן אחד עלולה לחשוף מידע על בני משפחה אחרים.

בשורה התחתונה, התקנים ניידים מכילים מידע רגיש רב ובאופן טבעי מושכים אליהם את גנבי המידע וגורמים נוספים, ומרבית בעלי ההתקנים הניידים לא מבינים תמיד את המשמעות של גניבת או שינוי המידע שברשותם.

כיצד נגנב מידע ממכשירים?

גניבת מידע, על ידי התגברות על מערכות למניעת דלף מידע ועקיפת מנגנונים לאכיפת והגבלת שימוש (המיושמות בארגונים) יתבססו בדרך כלל על עבודה מבפנים, בדרך כלל על ידי משתמש לגיטימי בעצמו או מנהל מערכת וכד' שהתפתו לנצל את מעמדם לגניבת מידע.

הטעיית המשתמש להתקנת פרופיל זדוני, תוכנת Malware או אפליקציה שעברה אריזה מחדש (repackaged) כדי שישמשו אחר כך לצורך שידור או ייצוא מידע או ניטור והקלטת מידע או אפילו יאפשרו לתוקף להיות בעמדת Man in The Middle, הן פעולות שיבוצעו בדרך כלל על ידי גורם חיצוני המנסה להשיג גישה.

בלי קשר לגורם התוקף, חיצוני או פנימי, אחזקה פיסית של ההתקן (גניבת ההתקן) הנה הדרך הטובה ביותר לאיסוף מידע.

שתי הדרכים הטובות והיעילות ביותר להתמודד עם גניבת ההתקן הן: סיסמה חזקה בכניסה להתקן והצפנת ההתקן.

על פי מחקרים, רק על 50% מההתקנים מופעלת סיסמת כניסה ומתוכם, 77% הם התקנים עם סיסמת פין של 4 ספרות, המשמעות היא שכחצי מההתקנים פתוחים לחלוטין ומרבית האחרים מוגנים בפין קוד של 4 ספרות בלבד.

הצפנת מכשירים הנה ברירת מחדל במכשירי אפל וניתנת ליישום (וצריכה להיות מיושמת) בהתקני אנדרואיד, כ – 97% מההתקנים הניידים בעולם מבוססים על שתי מערכות הפעלה אלה, הצפנת המידע המאוחסן במכשיר מקשה באופן קיצוני ביותר על היכולת הריאלית לפענח את המידע שמאוחסן בו.

גם מכשירים בעלי סיסמה חזקה בכניסה שהופעלה בהם ההצפנה, עדיין נמצאים בסיכון בגלל ווקטורים נוספים של תקיפה בעקבות חולשות במערכות הפעלה ואפליקציות ורשתות אלחוט מתחזות וזדוניות.

ולכן חשוב מעבר לסיסמה חזקה והפעלת ההצפנה, גם להקפיד להשתמש באפליקציות שמגיעות מהחנויות של אפל וגוגל, עדיף כאלה עם דירוג גבוה, הקפדה על עדכניות של מערכת ההפעלה והאפליקציות שבשימוש והתחברות לרשתות מוכרות ובטוחות בלבד.
מערכת הפעלה שאיננה מעודכנת מכילה חולשות, ויש מי שעוקב באופן תדיר אחר גילויי חולשות כאלה, ולאחר שהוא מוצא את הדרך לנצל אותן, אותם מכשירים שלא עודכנו הופכים להיות המטרות הקלות יותר עבורו.

וקטורים נפוצים של מתקפות וכיצד ניתן לצמצם את הסיכון

התקנים ניידים הנם התקנים שפגיעים למתקפות מסוגים שונים, מתקפות אלו יכולות להיות פיזיות, מתקפות רשת, ניצול חולשות ומתקפות Malware וקוד זדוני אחר.
בפסקאות הבאות נסקור מספר תרחישים נפוצים וכיצד ניתן להקטין את הסיכון.

אבטחה פיזית
כשמדובר בווקטורים שונים של מתקפות, המיקום הנו מרכיב חשוב שלעיתים איננו מוערך מספיק.

מערכות ניהול התקנים (MDM/EMM/UEM) מסוגלות לאכוף מדיניות שונה על התקנים בהתאם למיקום שלהם וכך לטפל בתרחיש הפשוט ביותר, כשהתקן נמצא בסביבה עוינת המערכת מזהה את מיקומו ומכילה עליו סט של מגבלות וחוקים שיקשו מאוד על תקיפתו גם אם המכשיר נפל לידיים הלא נכונות, כשההתקן יצא מהסביבה העוינת המערכת תזהה שוב את מיקומו ותסיר את המגבלות והחוקים שהגבילו את פעולתו.

התקן שנפל לידיים הלא נכונות הנו הסיכון הגבוה ביותר וגם מכשיר שנעול בפין קוד של 4 ספרות עדיין נמצא בסיכון, התקן כזה ניתן לפריצה באמצעות רכיבים כגון IP-BOX או USB Rubber Ducky שיחוברו להתקן הנייד, רכיבי USB אלה מזדהים כמקלדות חוקיות וניתן באמצעותם לבצע תהליך Brute Force (פריצה באמצעות ניסוי כל הקומבינציות האפשריות) לפריצת התקן עם פין קוד בן 4 ספרות בפחות מ – 17 שעות וזאת בהתחשב באופן שבו מערכות הפעלה מגיבות לפין שגוי, אנדרואיד דורש השהייה של 30 שניות לאחר הקשת קוד שגוי והתקני אפל עד לגרסה 9 ניתן לאתחל חשמלית את המכשיר לאחר 5 ניסיונות כושלים ואז לנסות שוב.

מכיוון שמספר הקומבינציות האפשריות בפין בן 4 ספרות איננו גדול יחסית, ווקטור מתקפה כזה הנו ריאלי בעיקר כשמדובר בהתקן רגיש של מטרה מתוכננת (בעל התקן שסומן מראש כמטרה) ולא התקן אקראי שנמצא או נגנב.
העלאת הרף של הפין קוד ל 6 ספרות במקום 4 ספרות, מעלה את הקושי לקומבינציה אחת מתוך מיליון במקום אחת מתוך עשרת

אלפים, שינוי קטן כזה הופך את המתקפה להרבה פחות ריאלית אם כי עדיין מעשית.
כדי להתגבר על הקושי בהקלדת פין קוד ארוך, ניתן להשתמש בפתרון ביומטרי שמקטין את הסיכוי לפרוץ פיזית להתקן, אבל יש לזכור שהתקנים בבעלות פרטית המקושרים למערכות מידע ארגוניות , עלולים להיות התקנים שמכירים יותר מטביעת אצבע אחת (בגון בני משפחה נוספים) וכאן קיימת חשיפה וסיכון למידע הארגוני כשמדובר במערכות שמקבלות טביעת אצבע המוכרת בהתקן.

מומלץ להשתמש במערכת ניהול ההתקנים הארגונית (MDM/EMM/UEM) כדי לאכוף מדיניות מחיקת התקן (מחיקת כל המידע הארגוני) במקרה של מספר ניסיונות פין קוד שגויים (בדרך כלל 10 ניסיונות) וכן לרענן את הנהלים מול משתמשי הארגון לגבי חובת דיווח מידי על אובדן או גניבת התקן.
לארגון עצמו צריך גם להיות נוהל ברור כיצד מטופל התקן שדוח כגנוב (בהנחה שקיימת מערכת לניהול התקנים), מה זמן התגובה למשלוח פקודה Over The Air (OTA), האם מיד נועלים מרחוק? האם מיד מוחקים מידע ארגוני (Enterprise Wipe) או שמבצעים למכשיר אתחול מלא להגדרות יצרן (Reset to factory default).

אבטחת התקשורת

בגדול, החברה הרעים מנסים בדרך כלל להתמקם תקשורתית בין ההתקן לבין שירות הקצה אליו ההתקן מתחבר (שרת דואר, שרת אפליקציה ארגוני, שרת אפליקציה ציבורי כגון בנק, חברת ביטוח וכד').
הגישה הקיצונית אומרת לסגור את יכולת האלחוט בהתקן כך שהתקשורת תעבור רק בתווך הסלולרי, תווך שיותר קשה להתחזות אליו.
דרך נוספת היא להעביר את כל התקשורת מההתקן דרך תווך Tunnel VPN מלא (יצירת רשת וירטואלית פרטית מוצפנת בין ההתקן לבין שרת או שירות היעד) שיגן מפני יירוט או שינוי המידע בזמן התקשורת, הבעיה שגם לתצורה זו יש לא מעט חסרונות כגון צריכת סוללה בהתקן, עלולה להיות השפעה (האטה) על קצב התקשורת ועל צריכת רוחב הפס בארגון, בנוסף נדרשת תחזוקת מערכת למימוש ה – VPN וישנם גם היבטי פרטיות שונים.
לבן נהוג להשתמש באחת או בשתי הדרכים הבאות גם יחד:
המערכות המובילות לניהול התקנים מציעות כיום את האפשרות ל Per App VPN או Micro VPN שבעצם נפתח ונסגר אוטומטית בעת הפעלת אפליקציות שהארגון מגדיר כרגישות, בתוך התווך הזה משודר רק המידע הספציפי של האפליקציה ולא כל תשדורת ההתקן, יש לזכור שבהתקן פרוץ (Jailbreak, Rooted) אדם מיומן מספיק יכול להפעיל אפליקציות אחרות על ההתקן שיעבדו תחת ה VPN של אפליקציה לגיטימית ולמעשה יקבלו גישה לגיטימית לרשת הארגונית ועוד בתווך מוצפן כך שגם התוקף יהיה מוגן מפני גילוי, זוהי סיבה נוספת מדוע הארגון חייב לנקוט ביד קשה כשמדובר בהתקנים פרוצים, לגבש נוהל ברור ולהשתמש במערכת ניהול ההתקנים הארגונית כדי לבצע מידית ניתוק של ההתקן או מחיקתו מרחוק.
אפשרות שניה, קיימת במערכות מתקדמות ביותר להגנה על התקנים ניידים, מערכת כזו מסוגלת לזהות התחברות לרשת שאיננה בטוחה וברקע לבצע מעבר שקט לעבודה בתצורת VPN, תצורה זה תמשיך להגן על המידע מפני יירוט או שינוי גם אם הרשת זוהתה כרשת שאיננה בטוחה.
פתרון מסוג זה יאפשר זיהוי של רשת מתחזה או כזו שמבצעת מניפולציה כלשהי לתקשורת בין המכשיר לבין שרת או שירות היעד ומיד יבצע מעבר לתווך VPN שימנע מהרשת המתחזה את היכולת להגיע אל המידע.
פתרון הגנה כזה, יזהה גם התחזות לרשת סלולארית, מתקפה מסוג זה אפשרית לביצוע וממקמת את התוקף בדיוק במקום שבו הוא רוצה להיות (Man in The Middle) אך מערכות הגנה מתקדמות מסוגלות לזהות את הרשת כמתחזה ולהעביר את התקשרות באופן אוטומטי לתווך VPN וכך להקשות כמעט באופן מוחלט על התוקף להגיע אל המידע.

Malware

מתקפות Malware מגיעות בצורות ובפורמטים רבים ושונים שצריך לגלות ולעצור.
במקרה זה, הגילוי הוא האתגר האמתי בגלל שזיהוי מבוסס חתימה (כפי שמקובל בווירוסים מסורתיים) איננו יעיל וזאת מכיוון שניתן בקלות לעדכן אפליקציות או לבצע Repackaging ואז ה – Malware מקבל חתימה אחרת לגמרי.

למזלנו בשנים האחרונות הטכניקות לזיהוי Malware נמצאות בהתפתחות מתמדת, ואלגוריתמים המבצעים ניתוח התנהגות משמשים לזיהוי פעולות אפליקטיביות שאינן "ראויות" וכן לבניית טבלאות מוניטין לאפליקציות.

מערכות ההפעלה עצמן עלולות אף הן להקשות במידה מסוימת על היכולת לזהות מתקפת Malware, כמו לדוגמה ההפרדה שמערכות אפל מבצעות בין אפליקציות שונות (Sandboxing), הפרדה שמגיעה מתפיסת אבטחה גבוהה, היא בעצמה מגבילה אפליקציות של הגנה ומונעת מהן את היכולת לזהות התנהגות חריגה של אפליקציות אחרות.

לבן, קו ההגנה הראשון והמשמעותי ביותר הנו אכיפת הורדת אפליקציות רק מהחנויות הרשמיות (Google Play, Apple App Store), לחנויות אלה יש תהליך סינון שמקטין את הסיכוי להימצאותו של קוד זדוני בתוך אפליקציה לגיטימית לכאורה.
מרבית המתקפות של Malware ותוכנות זדוניות מגיעות מהורדות שאינן מהחנויות הרשמיות.
בנוסף, חשוב ביותר להשתמש במערכות הגנה מתקדמות, כאלה שיכולות לזהות Malware גם אם הוא נמצא בחנות הרשמית של היצרנים ולמנוע את הורדתו אל ההתקן.

מלבד אפליקציות שמכילות קוד זדוני, התקנים ניידים פגיעים גם לפרופילים זדוניים, פרופילים אלה הנם קובצי הגדרות שיכולים להכיל סטים של הגדרות שיאפשרו לפגוע בהתקן, ליירט ממנו מידע ואף להשתלט עליו, כל מה שצריך זה למצוא דרך לגרום למשתמש הקצה ליזום הפעלה של התקנת הפרופיל ואת זה עושים באמצעות שיטות פיתוי שונות (Phishing) כגון מסרונים הכוללים לינק ומבקשים מהמשתמש ללחוץ על הלינק להסרה מרשימה או מיילים מפתים שמציעים הטבה כלשהי בלינק המצורף וכד', כל לחיצה כזו תפעיל הורדת קובץ XML קטן שירד אל ההתקן בתוך שבריר שניה ויכול פוטנציאלית לעורר מהומה גדולה.
גם כאן קיימים שני מרכיבים, חינוך המשתמשים ושימוש במערכת הגנה מתקדמת שתמנע את ההורדה בעת לחיצה על הקישור.

ואם זה לא מספיק, הרי שכיום חלק ממתקפות ה – Malware על התקנים ניידים הנם מתקפות כופרה, כאלה שנועלות את ההתקן הנייד עד לתשלום דמי כופר, גם כאן חינוך משתמשים לא ללחוץ על קישורים המגיעים ממקורות חשודים או שאינם מוכרים ביחד עם מערכת הגנה מתקדמת להתקנים ניידים, כזאת שמנתחת התנהגות ובודקת קישורים עוד לפני ההורדה יקטינו באופן משמעותי את הסיכוי להיפגע.

דרך נוספת להקטנת הסיכוי לגניבת מידע ארגוני באמצעות Malware היא שימוש באפליקציות קונטיינר לצורכי הארגון, אפליקציות אלה פועלות בתוך אזור תחום ומוצפן (קונטיינר), כל המידע שהן מייצרות או שומרות נשמר גם הוא מוצפן ובתוך אותו אזור שמופרד לחלוטין מכל האפליקציות האחרות על ההתקן בלי יכולת לתקשר איתן או להעביר אליהן מידע, המשמעות היא שבמידה וקיימת אפליקציה "סוררת" אחרת על ההתקן, היא לא תוכל לשלוף מידע ארגוני רגיש, ליירט אותו או לשנותו.
אפליקציות קונטיינר הן בדרך כלל אפליקציות "מנוהלות" הפועלות תחת מערכת לניהול התקנים (EMM/UEM) שיכולות לנהל אותן, ז"א לאכוף עליהן מדיניות שימוש כגון מניעת העתק/הדבק, מניעת צילום מסך או שיתוף מידע וכד'.
יתרון נוסף וחשוב בשימוש באפליקציות קונטיינר, מכיוון שהאפליקציה מופצת אל ההתקנים על ידי מערכת לניהול התקנים ומכיוון שהמידע שהיא מייצרת נשמר ביחד אתה בקונטיינר, הרי שמחיקת האפליקציה מרחוק על ידי הארגון מבטיחה שגם המידע שייצרה לא יישאר על ההתקן וגם הוא יוסר עמה ביחד.

הגנה ארגונית על התקנים ניידים

הגנה על התקנים ניידים בארגונים קיימת מזה שנים רבות אם כי באופן מפתיע עדיין לא כל הארגונים מתייחסים באותו כובד ראש להתקנים הניידים כפי שהם מתייחסים למחשבים השולחניים וזאת למרות שההתקנים הניידים כיום נגישים למערכות הארגון.
הגנה נכונה ומלאה מבוססת על כמה רבדים שמטפלים בהיבטים השונים של האיומים.

חינוך משתמשים
שגיאות משתמשים, פזיזות בלחיצה על קישורים, מסירת שם משתמש וסיסמה, אחסון סיסמאות באפליקציות חינמיות לניהול סיסמאות, נעילת מכשיר עם פין בן 4 ספרות, הפעלת היכולת להורדת אפליקציות מכל מקור, התחברות לכל רשת פתוחה ועוד המון פעולות שמשתמשי הארגון מבצעים יום יום הן פעולות תמימות אך ברמת סיכון גבוה, חשיפה אחת מוצלחת תאפשר

להשתמש במידע שנשלף מההתקן או בהתקן עצמו לפריצה קלה אל מערכות המידע והרשת הארגונית.
הארגון חייב לבצע פעולות סדירות להעלאת המודעות של עובדי הארגון על ידי שימוש בלומדות, ימי עיון והדגמות חיות שמבוצעות על ידי פורצים מנוסים מחברות המספקות שירותי אבטחת מידע.

מערכות לניהול התקנים

מערכות לניהול התקני קצה (MDM/EMM/UEM) הנן קו ההגנה המרכזי בתחום מניעת דלף מידע, גם המערכות המתקדמות ביותר בתחום זה לא יגנו על ההתקנים מפני אפליקציות או פרופילים זדוניים, מפני רשתות מתחזות וכד' אבל בעזרת סט חוקי מדיניות שהן אוכפות על ההתקנים הן יצליחו לצמצם את הסיכוי לדלף מידע בזכות מספר פעולות חשובות כגון, מניעת התחברות של התקנים פרוצים, מניעת התחברות של התקנים שאינם מורשים או שאינם עומדים במדיניות הארגון (גרסת מערכת הפעלה, התקנים ללא תוכנת הגנה מוכרת וכד'), אכיפת שימוש באפליקציות קונטיינר מנוהלות לשימוש מול מערכות הארגון, אכיפת שימוש ב – Per App VPN או Micro VPN בעת הפעלת אפליקציה רגישה, החלת מדיניות למניעת העתק/הדבק, שמור בשם..., פתח באמצעות... וכד', החלת דרישה להזדהות חזקה ופקטור הזדהות נוסף מותנה סיטואציה וכד', הנגשה מאובטחת של מידע ארגוני, אכיפת פין קוד ארוך או שימוש בטביעת אצבע, נעילה ומחיקת התקנים מרחוק במקרה של אובדן או חריגה ממדיניות וכד'.
מערכות אלה יודעות לפעול באינטגרציה עם מערכות הגנה מפני איומים ולבצע פעולות שונות על התקנים בעת זיהוי איום.

מערכות להגנה מפני איומים

מערכות אלה הנן מערכות הגנה שפועלות במספר מישורים בו זמנית על מנת להתמודד עם האתגר הגדול והוא זיהוי מתקפה, כדי להצליח במשימתן מערכות אלה משתמשות בכל הדרכים האפשריות, החל משימוש במנגנונים לזיהוי חתימה שמזהים חתימה של תוכנה או פרופיל זדוני, דרך אלגוריתמים לניתוח התנהגות אפליקטיבית שמזהים התנהגות שאיננה סבירה, ממשיך ביכולת לזהות חולשות במערכות הפעלה ואפליקציות, יכולת ניתוח פעולות בתקשורת (הרבה מהן באופן פרואקטיבי) כדי לזהות רשתות מתחזות או כאלה שמנסות לבצע מניפולציה כלשהי בנתונים ועד להתבססות על בסיסי מידע גלובאליים המכילים את כל הסיכונים הידועים.
מערכות אלה נדרשות לבצע מספר רב של פעולות וזאת בלי לפגוע בחוויית השימוש בהתקנים או בצריכת הסוללה או משאבי הרשת.
המוצרים המובילים בתחום עושים את זה בצורה מרשימה כבר כמה שנים טובות, המוצרים המובילים יודעים לא רק לזהות אלא גם להתמודד עם האיומים ולחסום אותם או לעבוד באינטגרציה מלאה עם מערכות לניהול התקנים ולפעול ביחד איתן על מנת להגן מפני התקיפה.
המוצרים המתקדמים מאוד בתחום משמשים בעצמם כל אחד כסנסור לאירועי אבטחת מידע וכל חשיפה שהם מזהים מספקת מידע חשוב שמשודר למרכז איסוף המידע של היצרן, מרכז זה הנו מרכז ניתוח מודיעין חשוב שמבצע על המידע ניתוחים ואגרגציות נדרשות ויכול להסיק מכל פיסת מידע מסקנות ולהסיק סיכונים פוטנציאליים, לאחר שהמידע מעובד, מרכז המודיעין מעדכן את יתר ההתקנים וכעת כולם מודעים לחשיפה החדשה שהתגלתה.

מרכזי בקרה SIEM SOC

משום מה, בארגונים רבים שיש בהם מרכזי בקרה לאירועי אבטחת מידע (SIEM SOC) עדיין מערכות הגנה להתקנים ניידים לא קיימות או שאינן מחוברות למרכז הבקרה וזאת למרות שכל מערכות ההגנה מותאמות לכך.
כמות ההתקנים הניידים בארגונים איננה נופלת מכמות המחשבים, וחלק גדול מהם מחוברים למערכות המידע הארגוניות, כפי שתואר כאן התקנים אלה נמצאים ברמת סיכון גבוהה ביותר ולכן ההגנה עליהם נדרשת וחיבור מערכות ההגנה של התקנים אלה למרכז בקרת אירועי אבטחת המידע הנו מאיר עיניים ומספק מידע רב, מידע שכיום איננו קיים ברשות הארגון והוא עיוור לחלוטין למתרחש בהתקנים הניידים בארגון.

מוביסק טכנולוגיות

מוביסק טכנולוגיות, חברת מומחים הפועלת משנת 2011 ומתמחה בתכנון, הקמה ותחזוקת מערכות לניהול והגנה על התקני הקצה.

מומחי החברה הנם בעלי ניסיון עצום במימוש מערכות EMM/UEM, פתרונות וירטואליזציה, פתרונות להגנה על התקני קצה ומימוש בפועל של תשתית לסביבת עבודה דיגיטלית, לכל סוגי ההתקנים, מחשבים שולחניים וניידים, טלפונים חכמים, מחשבי לוח ולכל מערכת הפעלה נפוצה Windows, MAC OS, Chrome OS, iOS, Android.

מוביסק מספקת שירותים ליותר מ – 90 ארגונים מובילים בישראל והנה שותפה של היצרנים המובילים בתעשייה כגון VMware, Symantec, Checkpoint, SentinelOne, Blackberry.

לפרטים נוספים ולקבלת ייעוץ מהחברה המנוסה והמקצועית ביותר בתחום זה בישראל, צרו קשר: info@mobisec.co.il