יולי 2024
תמוז התשפ"ד

המלצות להנהלות הציבור בשימוש בתגי איתור

רקע

בשנים האחרונות, צברו אביזרי איתור ומעקב אחר מיקום ("תגי איתור"), כגון אלו הנמכרים על ידי אפל, סמסונג, Tile, גוגל וחברות נוספות, פופולריות רבה. תגי איתור אלו מאפשרים לבעליהם לעקוב אחר מיקום חפצים אליהם הוצמדו, כמעט בכל מקום בארץ ובעולם.

בכדי לאפשר את יכולת איתור התג, ספקים כמו אפל, סמסונג,[1] וגוגל החלו לפרוס **רשתות מעקב לא מקוונות** (OF - Offline Finding)[2] בקנה מידה רחב מאוד וזאת כדי לנטר מכשירים המנותקים מרשת האינטרנט. רשתות מעקב אלו משתמשות בטכנולוגיות תקשורת למרחקים קצרים כגון Bluetooth Low Energy (BLE) או Ultra-Wideband (UWB) להעברת הודעות ופרסומות למקלטים קרובים (כגון טלפונים חכמים). המכשירים המקבלים תקשורת זו, מאפשרים לייצר דוחות מיקום לשרתים שבשליטת ספק השירות.
יודגש כי רשתות מעקב לא מקוונות של היצרניות חולקות שתי תכונות מפתח: השימוש בתקשורת להעברת נתונים לטווח קצר בין התקנים (למשל, בין המכשיר הסלולרי לתג האיתור), ובעיקר, רשת נרחבת של מכשירים ניידים המחוברים בניהם והמכונים "מכשירי מוצא" המעבירים מידע מיקום לשרת הנשלט על ידי הספק.
הרעיון הבסיסי הוא די פשוט: כאשר מכשיר (אבוד) מאבד את חיבור האינטרנט שלו, הוא מתחיל לשדר משואת איתות ייחודית המשתמשת בתקשורת למרחקים קצרים הנקלטת על ידי מכשירי מוצא קרובים המשתתפים ברשת המעקב הלא מקוונת. מכשירים אלה מעבירים את משואת האיתות ואת המיקום בו הוא נמצא לשרת הספק.

מכשירים ניידים כגון טלפונים חכמים וטאבלטים מגיעים לרוב גם עם תכונה נוספת הנקראת **רשתות חיפוש מכשירים**. תכונה זו המאפשרת לבעלים שלהם למצוא את המכשירים כשהם אובדים, וזאת באמצעות שימוש בפורטל אינטרנטי שמסופק על ידי החברות. כדי שתכונה כזו תעבוד, הבעלים נדרשים לאשר שיתוף המיקומים של המכשיר מעת לעת עם הספק. דוגמאות בולטות לתכונה כזו של איתור מכשיר אבוד (רשתות חיפוש מכשירים): Find My Device של גוגל, Find My Mobile (FMM) של סמסונג ו- Find My של אפל.

[1] https://www.researchgate.net/publication/364771539_Privacy_Analysis_of_Samsung's_Crowd-Sourced_Bluetooth_Location_Tracking_System

[2] רשתות מעקב לא מקוונות הן רשתות אשר מאפשרות למכשיר במצב לא מקוון לחשוף את מיקומו לצורך אחזור מידע על מיקומו ואיתורו, וזאת על ידי מכשירים קרובים אשר שולחים אותות לשרת.

הדרישה הבסיסית בכדי שתכונה כזו תעבוד היא שהמכשיר חייב להיות מחובר לרשת האינטרנט בכדי שיוכל לשלוח את דוח המיקום שלו לשרת הספק, למקרה שבעליו מסמן את המכשיר ככזה שאבד. לעתים קרובות תכונה זו מגיעה עם תכונות נוספות כגון השמעת קול במכשיר, נעילת המכשיר או מחיקת הנתונים שלו מרחוק.

יצרניות מכשירים ניידים יצרו ממשק בין רשתות המשמשות לחיפוש מכשירים לבין רשתות מעקב לא מקוונות (OF). ממשק זה מאפשר למצוא מכשיר נייד שאבד גם כאשר אין לו חיבור לרשת האינטרנט.
בעוד שניתן להשתמש בממשק בין הרשתות בכדי לאתר מכשירים חזקים יחסית כמו טלפונים חכמים ומחשבים ניידים, **המוצר המשמעותי והנפוץ כתוצאה מיצירת הממשק הוא תג האיתור**.
בתגי איתור אלו מוטמעים מקלט, משדר, מיקרו-מעבד וסוללה באריזה קומפקטית וניתן לחבר אותן לאובייקטים פיזיים (למשל, ארנק, מזוודה, חיית מחמד). הפופולריות של תגי האיתור נובעת מהעלות הנמוכה שלהם (בדרך כלל מתחת ל-30$) וכן מהזמינות הרחבה של רשתות לא מקוונות המופעלות על ידי מכשירים "מתנדבים" שיכולים לזהות אותם. מכירות תגי האיתור המשולבות לשנת 2023 של אפל, סמסונג ו- Tile עולות על 100 מיליון יחידות.[3]
הרשות להגנת הפרטיות ניתחה מסמכים רלוונטיים של החברות המייצרות תגי איתור ומסמכים של חברות המספקות רשתות חיפוש מכשירים ורשתות לא מקוונות, וגיבשה סדרה של המלצות לשימוש בטוח ומאוזן תוך שמירת על פרטיות המשתמשים. יובהר כי המסמך אינו מבקש למנוע את השימוש בתגי איתור, אלא לתת כלים להתנהלות נכונה של המשתמשים בהיבטי פרטיות.

<u>איסוף נתונים אישיים למטרות שימוש בתגי איתור</u>

פרוטוקולי המעקב תוכננו כדי להבטיח רמה מסוימת של שמירה על פרטיות המשתמש מפני מעקב על ידי הספק. עם זאת, נראה כי מנגנוני פרטיות כאלה עומדים בסתירה לתופעה של מעקב מבוסס תגי איתור, שבו תוקפים משתמשים בתגים אלו בכדי לנטר את תנועותיהם. מקרים פליליים רבים מסוג זה דווחו, והחברות נאלצו לבצע התאמות על מנת לאפשר זיהוי של תגים זדוניים.
מעצם טיבן, תגי איתור אוספים מידע אישי רב המשמש לצורך איתור ומעקב. ניתן לסווג את המידע שנאסף על ידי תגי איתור ורשתות "חיפוש מכשירים" באופן הבא:
<u>נתוני מכשיר</u>:

- מזהה ייחודי – לכל תג איתור יש מזהה ייחודי שמבדיל אותו מאחרים.
- רמת סוללה – עוזרת להעריך את הפונקציונליות ואת תוחלת החיים של תג האיתור.

[3] Caleb Naysmith. Apple AirTags and Bluetooth Trackers Are Officially a Billion-Dollar Industry. Yahoo News, December 2022.

- מצב קישוריות – מציין האם תג האיתור נמצא בטווח Bluetooth או רשת נתמכת אחרת.

<u>נתוני מיקום</u>:

- מיקום – זוהי פונקציית הליבה, והדיוק יכול להשתנות בהתאם לטכנולוגיה שבה נעשה שימוש (Bluetooth, UWB וכו'). הרשת Find My של אפל משתמשת במכשירים אחרים של אפל בקרבת מקום כדי להעביר באופן אנונימי את מיקומו של תג האיתור, ומציעה רשת צפופה יותר. רשתות ה-SmartTag של Tile וסמסונג מסתמכות יותר על תשתית משלהן וקישוריות בלוטות'.
- חותמת זמן – מספקת תיעוד של מתי נאספו נתוני המיקום.

חשוב לציין כי רשתות חיפוש מכשירים מאחסנות בדרך כלל נתוני מיקום לתקופה מוגבלת, תוך הקפדה על מדיניות הפרטיות של החברות. במסגרת זאת, למשתמשים יש בקרה על הנתונים הנאספים, השימוש שנעשה ואמצעי אבטחה כדי למנוע גישה לא מורשית לנתונים אלה.

<u>הסיכונים לפרטיות</u>

תגי איתור נמצאים בשימוש נפוץ, דבר שמרחיב למעשה את השימוש בתשתיות איתור ומעקב. על כן, קיים חשש שמידע אישי הכולל גם נתוני מיקום אשר נאגרים במערכות אלו, ייזלוג לידי צדדים שלישיים או שיעשה בו שימוש שחורג מן המטרות אשר לשמו נאסף המידע האמור, באופן הפוגע בפרטיות המשתמשים.[4]

כאמור, שימוש בתגי איתור מספק גישה למיקום המשתמש, המייצר, בין היתר, "שובל דיגיטלי" של נתוני מיקום, העלולים לחשוף מידע רגיש על אורחות חייו והרגליו של אדם. עובדה זו מגבירה את איום וסיכון אבטחת המידע, ומעלה את החשש כי המידע שייאסף במסגרת השימוש יתורגם לכדי פגיעה בפרטיות בדרך של מעקב.

<u>נבקש להציג מספר נקודות מרכזיות שבהן הפוטנציאל לפגיעה בפרטיות המשתמשים גדל</u>:

1. נקודות תורפה ביישום פרוטוקול – פגיעויות בפרוטוקולי הרישום של תגי איתור, שיטות ההצפנה להפקת מזהים ייחודיים למכשירים שאבדו, והפרוטוקול לדיווח של מכשירי המוצא. כל אלה עלולים להיות מנוצלים על ידי גורמים זדוניים ולסכן את אבטחת המידע.
2. מעקב לא רצוי – רשת החיפוש הלא מקוון (OF) עלולה להיות מנוצלת לרעה לצורך מעקב לא רצוי אחר אדם או חפץ, על ידי גורם אחר מלבד ספק השירות. הדבר מהווה סיכון לפרטיות ולביטחון של אנשים שעלולים להיות במעקב ללא הסכמתם.

[4] https://www.prnewswire.com/news-releases/parks-associates-32-of-smart-tag-owners-report-using-the-device-to-track-another-person-without-their-knowledge-301603454.html

3. נכונות ושלמות נתוני מיקום – קיימת אפשרות של גורם שלישי שאינו המשתמש או החברה, לזייף דוח מיקום של מכשיר שאבד, ולהוות סיכון לנכונות ושלמות נתוני המיקום ברשת החיפוש הלא מקוון (OF).

סיכונים אלה מדגישים את הפוטנציאל למעקב לא מורשה, פגיעה בפרטיות ובעיות בנכונות ושלמות הנתונים ברשת החיפוש הלא מקוון (OF), דבר שמעלה את הסכנה לשליטה במידע האישי ולאבטחתו.

<u>המלצות להתנהלות הציבור בעת שימוש בתגי איתור</u>

להלן יוצגו המלצות הרשות להגנת הפרטיות בנושא. ההמלצות מבוססות, בין היתר, על העקרונות והכללים שהוצגו קודם לכן:

- <u>הבינו את הגדרות הפרטיות</u> – בדקו את הגדרות המכשיר שלכם כדי ללמוד כיצד נאספים ומשתמשים בנתוני מיקום. לעתים קרובות אתם יכולים לבחור להשבית לחלוטין את מעקב המיקום או לאפשר זאת רק תוך כדי חיפוש אחר תגי איתור.
- <u>שימו לב להרשאות</u> – בעת התקנת אפליקציות ניהול מכשירי איתור ומעקב, שימו לב להרשאות המיקום שהן מבקשות. העניקו גישה רק אם הדבר חיוני לפונקציונליות של תג האיתור.
- <u>הקפידו על עדכוני תוכנה</u> – ודאו שהמכשירים ואפליקציות האיתור שלכם מעודכנים בתכונות האבטחה העדכניות ביותר ובתכונות השמירה על הפרטיות.
- <u>השתמשו בשיתוף זמני (אם זמין)</u> – מספר רשתות חיפוש מכשירים מציעות תכונות של שיתוף מיקום זמניות. נצלו אותן עבור מצבים ספציפיים במקום להעניק גישה קבועה.
- <u>היזהרו מעוקבים לא ידועים</u> – אם אתם מוצאים תג איתור לא ידוע המחובר לחפצים שלכם, פנו לרשויות אכיפת החוק.

<u>המלצות למשתמשי מערכת הפעלה IOS (אפל)</u>

<u>הכירו את צפצוף ה-AirTag</u>[5] – צפצוף זה מציין ש-AirTag ללא בעלים נמצא בקרבת מקום, או באחד החפצים שלכם. אם אתם מקבלים התראה המזהירה אתכם לגבי AirTag קרוב, אל תתעלמו ממנה.

<u>דעו כיצד לזהות AirTag</u> – אם תמצאו AirTag שאינו שלכם, ויש לכם אייפון, היכנסו לאפליקציית "מצא את המכשיר שלי", לחצו על "פריטים" ולאחר מכן החליקו למעלה עד שתראו את האפשרות

[5] השם המסחרי של תג האיתור שפיתחה אפל.

"זהה פריט שנמצא". הכלי הזה מאפשר לכם לסרוק את ה-AirTag על ידי החזקתו ליד הטלפון שלכם. לאחר מכן, הוא יציג את המספר הסידורי של ה-AirTag ואת ארבע הספרות האחרונות של מספר הטלפון של הבעלים, דבר שיכול להיות שימושי עבור המשטרה.

שקיפות מעקב אחר אפליקציות (רלוונטי ל- IOS 14.5 ואילך) – תכונה זו דורשת מאפליקציות לקבל את הסכמתכם המפורשת לפני שהן עוקבות אחריך. הדבר מסייע למנוע איסוף נתונים שאינו קשור לתפקוד מכשיר האיתור והמעקב.

הגדרות פרטיות עבור רשתות Find My – בתוך הגדרות > פרטיות > שירותי מיקום > Find My, אתם יכולים לנהל את האופן שבו נתוני מיקום ממכשירי אפל ומ-AirTags נאספים ומשותפים. אתם יכולים לבחור:

- מצא את האייפון שלי – שליטה בשיתוף המיקום עבור האייפון עצמו.
- מצא את הרשת שלי – ניהול שיתוף מיקום עבור מכשירי אפל אחרים.
- פריטים – ניהול שיתוף מיקום עבור AirTags או אביזרים תואמים אחרים.

אופטימיזציה של הפרטיות באמצעות AirTags:

- התראות – אפשרו הודעות עבור "AirTag נמצא זז איתך". במיוחד למקרה בו קיימת התראה על AirTag לא ידוע המלווה אותך תקופה ממושכת. זה יכול להצביע על שימוש לרעה פוטנציאלי.
- הגדרות שיתוף – מאפשרת שליטה ברשימת האנשים שיכולים לראות את המיקום של ה-AirTags שלך. הענק גישה רק לאנשים מהימנים שבאמת צריכים למצוא אותם.
- שיתוף זמני (רלוונטי ל- IOS 16 ואילך) – אם זמין, השתמשו בתכונות שיתוף מיקום זמניות במקום להעניק גישה קבועה.

המלצות למשתמשי מערכת הפעלה אנדרואיד

זיהוי מעקבי מיקום לא רצויים (DULT) – תכונה חדשה יחסית (רלוונטי לאנדרואיד 6.0 ואילך) שיכולה לזהות התקני מעקב בלוטות' לא ידועים בקרבתכם. תכונה זו יכולה לעזור לזהות עוקבים שעלולים להשתמש בתגי איתור למטרות זדוניות.

שימוש מאובטח ב"מצא את המכשיר שלי" – שלטו בהגדרות חשבון גוגל שלכם בכדי לנהל את האופן שבו נאספים נתוני מיקום שלכם ונעשה בהם שימוש. אתם יכול לגשת להיסטוריית המיקומים ולבחור למחוק אותה.

אימות דו-גורמי (2FA) – אפשרו אימות דו-גורמי בחשבון הגוגל שלכם בכדי להוסיף שכבת אבטחה נוספת. הדבר מקשה משמעותית על גישה לא מורשית לנתוני "מצא את המכשיר שלי".