אבטחה בנייד, באפליקציות ובאינטרנט של הדברים

הגנה על נתונים ומכשירים בכל העולם

לנוכח העלייה הדרמטית במספר הגורמים הזדוניים שפועלים באינטרנט כמו גם במתקפות סייבר במימון מדינות, האבטחה של המוצרים והשירותים שלנו חשובה לא פחות מהיעילות שלהם. אנחנו ב-Google משקיעים מאמצים מיוחדים בהגנה על אנשים, ארגונים וממשלות – ופועלים כדי להעמיד את הידע שלנו לרשות הציבור, להעצים אנשים להתמודד עם סכנות הסייבר המתפתחות מהר מתמיד ולקדם אבטחת סייבר ברמה הגבוהה ביותר, במטרה ליצור עולם בטוח יותר לכולם.

לכן, חשוב לנו להקדים תרופה למכה ולהמשיך לפתח את פתרונות האבטחה שלנו כדי להתמודד עם מפת האיומים המשתנה מדי שעה. חשוב במיוחד לאבטח אפליקציות ומכשירים שמחוברים לאינטרנט, כדי שהלקוחות שלנו יוכלו להשתמש במכשירים באופן מאובטח ולשלוט במידע.

האתגר

לצורך להיות מחוברים כל הזמן יש מחיר

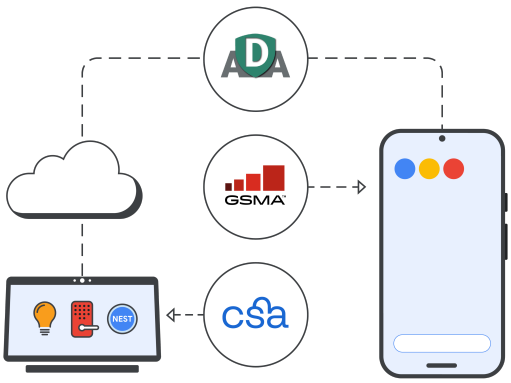
חלק גדול מחיי היום-יום שלנו מתנהל בסמארטפון, באפליקציות ובמכשירים שמחוברים לאינטרנט. אנחנו מבלים יותר ויותר זמן באינטרנט ומשתפים יותר ויותר מידע אישי וחשוב, כמו פרטי חשבון בנק או מידע רפואי. וזאת בדיוק הסיבה שפושעי סייבר מתוחכמים מגבירים את ההתקפות על המכשירים האלה, כדי להשיג מידע רגיש.

יותר מכשירים, יותר מידע ונתונים, יותר איומים

לפי ההערכות, יש כיום בעולם 17 מיליארד מכשירים עם חיבור אינטרנטי, ממדפסות ועד שלטים לפתיחת שערים. כל אחד מהם פועל על תוכנות (שחלקן תוכנות בקוד פתוח) שאפשר לפרוץ אליהן בקלות.[1] בסך הכול, מספר המכשירים עם חיבור אינטרנטי שנמצאים בסיכון כמעט הכפיל את עצמו ב-2020.[2]

- למרות שאנחנו מחוברים למספר הולך וגדל של מכשירים עם חיבור אינטרנטי, לא קיים עדיין תקן גלובלי למדידת איכות האבטחה של המוצרים המחוברים. זה אומר שהצרכנים נאלצים לקבל החלטות לא מושכלות בקשר לאבטחה.
- בדיוק כמו שיש לצרכנים זכות לדעת מה מכילים מוצרי המזון או חומרי הניקיון שהם קונים, כך יש להם זכות לשקיפות בקשר למוצרים הדיגיטליים שלהם.
- מכשירים ניידים הם כר פורה נוסף לתקיפות אחרות, והחיבור בין המכשירים מגדיל את הצורך לשקיפות בקנה מידה רחב בכל הקשור לאבטחה. לכן אבטחת המערך הכולל של המכשירים המחוברים חשובה לא פחות מאבטחת הרשתות והמערכות.

שיתוף הפעולה שלנו עם ארגונים בתחום



הפתרון שלנו

אנחנו ב-Google מקדמים את האבטחה והשקיפות של המכשירים המחוברים שלנו באמצעות אבטחה בנייד, באפליקציות ובאינטרנט:

אבטחה בנייד

Android, מערכת ההפעלה שלנו בקוד פתוח, נשענת על גישה רב-שכבתית לאבטחה כדי להגן על המכשירים הניידים:

- אבטחה רב-שכבתית
  - בזכות הפעלה מאומתת והגנות כמו חזרה למצב הקודם ואיפוס להגדרות המקוריות, הגרסה של Android תמיד הכי עדכנית והכי בטוחה.
  - השימוש בקוד אימות (PIN) ובאימות ביומטרי מגן מפני פריצות.
  - השירות 'איפה המכשיר שלי' מאפשר לאתר את המכשיר או למחוק אותו אם הוא נגנב או אבד.
- הגנה על הזהות והסיסמה
  - אפשרויות ושירותים כמו אימות דו-שלבי, שימוש במפתח האבטחה המובנה של הטלפון ומנהל הסיסמאות מגינים על חשבון Google מפני פריצות.
  - בדיקת האבטחה וההגנה המתקדמת, שזמינה לשימוש שומרות על התקינות והאבטחה של המכשיר.
- הגנה מפני פישינג
  - האפליקציות והמכשירים של Google עוזרות לזהות ולמנוע הונאות והתקפות פישינג.
  - הגלישה הבטוחה של Google מגינה על יותר מ-5 מיליארד מכשירים בעולם.

אבטחה באפליקציות

מניעת תוכנות זדוניות בהתקנת ברירת המחדל (Out-of-the-box) מגינה מפני אפליקציות לא בטוחות, והמידע בקשר לאבטחת המידע מעניק למשתמשים שקיפות כשהם מורידים אפליקציות.

- חנות Google Play: כלי זיהוי המבוססים על למידת מכונה ואנליסטים בשר ודם בודקים את כל האפליקציות לפני שהן זמינות להורדה. בחלק של אבטחת המידע מוסבר אילו סוגים של נתונים ומידע האפליקציות אוספות ולצורך מה המידע הזה משמש.
- Google Play Protect: יותר מ-125 מיליארד אפליקציות נסרקות מדי יום, ואם מזוהים סיכוני אבטחה, התראות נשלחות והאפליקציות מוסרות או מושבתות.
- ברית ההגנה על אפליקציות (ADA): Google חברה לשותפות מובילות מתחום זיהוי האיומים בנייד כדי להקים את ברית ההגנה על אפליקציות, שמגינה על משתמשי Anrdoid מפני אפליקציות שעלולות להיות זדוניות בעזרת שיתוף פעולה מודיעיני ותיאום פעולות הזיהוי.

אבטחה באינטרנט של הדברים

סימוני האבטחה באינטרנט של הדברים מספקים מידע ברור בקשר לנוהלי הפרטיות והאבטחה במכשיר, למשל אילו נתונים ומידע נאספים.

- אנחנו מאמינים בחמישה עקרונות מרכזיים למוסכמות של סימוני אבטחה באינטרנט: סימון בזמן אמת, מוסכמות הערכה, נקודות בסיס לאבטחה לצד גמישות, שקיפות רחבה ותמריצי אימוץ.
- אנחנו פועלים יחד עם הברית לתקני קישוריות (Connectivity Standards Alliance) (CSA) ועם ברית GSM (GSMA) כדי ליצור תוכנית אישור כלל-ענפית אחידה לדרישות הרגולטוריות הקיימות והעתידיות.

העקרונות שלנו

אנחנו ב-Google מיישמים 3 עקרונות מרכזיים לקידום האבטחה והשקיפות במכשירים המחוברים שלנו:

הגנת עומק: אנחנו משתמשים במספר שכבות בארכיטקטורת האבטחה, שפועלות יחד כדי ליצור חומת מגן חזקה, יעילה ותקינה כל הזמן.

פתיחות ושקיפות: בלב החזון שלנו ניצבת שקיפות. אנחנו מאמינים ששיתוף מידע וידע עם משתמשי הפלטפורמה שלנו לצורך חיזוק ההגנה מאפשר למערכת הקוד הפתוח שלנו להיות יותר מאובטחת מאשר מערכת סגורה.

המיטב של Google יחד עם מומחים בתחום: צוותי מומחים מכל רחבי Google ומהתחום משתפים פעולה כדי לשמור על האבטחה של מיליארדי משתמשים.

אפליקציות

סימוני אבטחה באינטרנט של הדברים: העברת השליטה לידי הצרכנים

ללא סימונים מוסכמים לאבטחה באינטרנט של הדברים, ליצרני המכשירים אין תקן גלובלי שמנחה אותם. גם למשתמשים אין את השקיפות שמגיעה להם, והם לא יודעים אם המכשירים מגינים על המידע שלהם. כלל השחקנים בתחום צריכים לחבור יחד כדי לקדם את האבטחה באינטרנט של הדברים ולהחזיר את השליטה לידי הצרכנים. באמצעות התהליכים והשותפויות שלנו אנחנו עובדים על פיתוח מוסכמות לסימוני אבטחה באינטרנט של הדברים.

- בראש ובראשונה, אנחנו משקיעים במחקרי אבטחה חיצוניים כדי להצביע על נקודות חולשה אפשריות (מכשירי Google Nest משתתפים בתוכנית התמריצים של Google לזיהוי נקודות חולשה ואנחנו מספקים תמריצים לחוקרי אבטחה מחוץ ל-Google שמזהים נקודות חולשה).
- אנחנו גם שולחים תיקוני באגים קריטיים לפחות חמש שנים אחרי ההשקה.
- כל המכשירים שלנו שפותחו החל מ-2019 משתמשים בהפעלה מאומתת כדי לוודא שהתוכנה הנכונה פועלת והגישה מוגנת. לדוגמה, מכשירי Google Nest מאומתים באמצעות תקני אבטחה של צד שלישי שמקובלים בתחום, כמו אלו שפותחו על ידי NIST, ETSI ו-ISO.

התקנים האלה, ומחזור החיים שלנו לפיתוח תוכנות (SDLC), מצמצמים את הסיכוי שצרכנים ייחשפו לנוהלי אבטחה גרועים וסוללים את הדרך לאינטרנט פתוח ובטוח יותר.

ההשקעות ואבני הדרך שלנו בתחום

2007 – **הקמת הגלישה הבטוחה** – כדי להתריע באופן יזום בפני המשתמשים כשהם נכנסים לאתרים מסוכנים ולהגן כיום על יותר מ-5 מיליארד מכשירים.

2010 – **השקת דוח השקיפות של Google** – כדי להראות איך המדיניות והפעולות של ממשלות ושל המגזר העסקי משפיעות על הפרטיות, האבטחה והגישה למידע באינטרנט. ב-2018 הוספנו דוח שקיפות ספציפי ל-Android.

2017 – **השקת Google Play Protect** – הפתרון למניעת תוכנות זדוניות שנמצא כיום בשימוש הכי רחב, עם סריקה של יותר מ-125 מיליארד אפליקציות ביום ביותר מ-3 מיליארד מכשירים.

2019 – **הוספת מפתח אבטחה** – חלק מובנה ב-Android, והחל מ-2020 גם ב-iPhone.

2022 – **הוספת סעיף על אבטחת מידע ל-Google Play** – כדי לתת לאנשים יותר מידע על הדרך שבה האפליקציות אוספות ומשתפות את המידע של המשתמשים ומגינות עליו. יצרנו גם את המערכת הראשונה לחלוקת תגים לאפליקציות שביצעו בדיקת אבטחה בלתי תלויה בעזרת הברית להגנה על אפליקציות.

2023 – **מפתחות גישה: הדרך לעתיד ללא סיסמאות** – לאחר עשור של קידום תקנים פתוחים בעזרת ברית FIDO וגורמים טכנולוגיים מובילים בעולם, יצאנו לדרך עם תמיכה נרחבת במפתחות גישה.

הגישה שלנו

מחויבות לעולם דיגיטלי פתוח ומאובטח

ככל שיהיו יותר נתונים ביותר מכשירים המחוברים לרשתות שונות, כך הבעיות והחששות שקשורים לאבטחה יגדלו. באמצעות פיתוח המוצרים שלנו, קריטריונים לשקיפות ושותפויות בתחום, אנחנו עוזרים לקדם עתיד שבו המכשירים המחוברים יהיו מאובטחים.

אחד מעקרונות היסוד באסטרטגיית פיתוח המוצרים שלנו הוא שמירה על כך שהמוצרים יהיו מאובטחים כברירת מחדל. הגלישה הבטוחה, Google Play Protect ומפתחות האבטחה המובנים מגינים על מכשירים ניידים ואפליקציות, ושומרים על רמת האבטחה הגבוהה ביותר במוצרים שלנו.

בזכות פתיחות ושקיפות בנוגע לדרך שבה אנחנו מתמודדים עם בעיות ושיתוף מידע בקשר לאבטחת המכשירים המחוברים, אנחנו עוזרים לשמור על חופש הבחירה בתהליכי האבטחה. אנחנו מאמינים שמערכת בקוד פתוח יכולה להיות יותר מאובטחת מאשר מערכת סגורה בזכות גישה שכבתית לאבטחה.

בעזרת שיתוף הפעולה עם CSA, הברית להגנה על אפליקציות ו-GSMA, אנחנו שואפים לקדם אבטחת סייבר ברמה הגבוהה ביותר, למען אינטרנט בטוח ועתיד בטוח לכולם.

חרטנו על דגלנו להעלות את הרף בכל הקשור לאבטחת המכשירים המחוברים ולהתוות את הדרך לסביבה בטוחה יותר באינטרנט לכולם, בכל מקום בעולם. למידע נוסף על הפעילות של Google בכל הקשור לאבטחת המכשירים המחוברים: g.co/connecteddevicesafety

מקורות מידע: [1] CNBC Cyber Report, Jan 9, 2023, [2] What is an IoT Attack? The Ins and Outs of IoT Security, July 20, 2021