OUCH! ינואר 2015

הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- סקירה
- השגת אפילקציות
- הרשאות
- עדכון אפליקציות

שימוש מאובטח באפליקציות מובייל

סקירה

עורך אורח

כריס קרוולי (Chris Crowley) הוא יועץ עצמאי, מדריך SANS מוסמך וכותב קורסים. הוא פעיל בטוויטר (**@CcrowMontance**) ובגוגל פלוס (**+ChrisCrowley**).

מכשירים ניידים כגון טאבלטים וטלפונים חכמים נהיו אחת מהטכנולוגיות העיקריות שאנו משתמשים בהן גם בחיינו הפרטיים וגם בחיינו המקצועיים. מה שהופך את המכשירים הניידים לכל כך רב תכליתיים הן מליוני האפליקציות שאנו יכולים לבחור. האפליקציות מאפשרות לנו להיות יותר יעילים, לתקשר ולשתף מידע עם אחרים באופן מיידי, ללמוד ולתרגל או סתם להנות. עם זאת, עם העוצמה של כל אפליקציות המובייל מגיע גם סיכון. הנה מספר צעדים שאתם יכולים לנקוט על מנת לתחזק ולהשתמש באפליקציות המובייל שלכם בצורה מאובטחת.

השגת אפליקציות מובייל

הצעד הראשון הוא וידוא שאתם תמיד מורידים אפליקציות ממקומות מוסמכים ומאובטחים. זכרו, כמעט כל אחד יכול לייצר אפליקציות מובייל כך שאתם צריכים להיות זהירים מהיכן אתם משיגים את האפליקציות. פושעי סייבר שיפרו את יכולותיהם ביצירת והפצת אפליקציות נגועות שנראות לגיטימיות. אם אתם מתקינים אחת מתוכנות נגועות אלו על המכשיר שלכם, פושעים אלו יכולים להשתלט עליו כולל קריאת הדואר האלקטרוני, האזנה לשיחות וגניבת אנשי הקשר שלכם. על ידי הקפדה על הורדת אפליקציות רק ממקומות ידועים שניתן לסמוך עליהם אתם מפחיתים את הסיכון להתקין תוכנה נגועה. מה שייתכן שאינכם מבינים הוא שסוג המכשיר שברשותכם מגדיר את האפשרויות שלכם.

עבור מכשירים של חברת 'אפל' כמו iPad ו iPhone אתם יכולים להוריד אפליקציות רק מסביבה מנוהלת - ה App Store. היתרון הוא ש›אפל' מבצעת בדיקות אבטחה הן לאפליקציה והן למפתחים שלה. אמנם ›אפל‹ לא יכולה לאתר את כל האנשים הרעים או את כל האפליקציות הנגועות, אבל סביבה מנוהלת זו מסייעת להפחית משמעותית את הסיכון של התקנת אפליקציה נגועה. בנוסף, אם 'אפל' מוצאת אפליקציה בחנות (store) שהם מאמינים שהיא נגועה, הם מסירים אותה באופן מיידי. חלונות (Windows Phone) משתמשת בשיטה דומה לניהול אפליקציות.

שימוש מאובטח באפליקציות מובייל

מכשירים ניידים עם מערכת ההפעלה אנדרואיד הם שונים. אנדרואיד מאפשרת לכם יותר גמישות על יד האפשרות להוריד אפליקציות מכל מקום באינטרנט. עם זאת, עם גמישות זו באה גם יותר אחריות. אתם חייבים להיות יותר זהירים לגבי אילו אפליקציות אתם מתקינים מאחר שלא כולן נבדקות. גוגל אכן מחזיקה חנות אפליקציות מנוהלת (Google Play) שדומה לזו של 'אפל'. האפליקציות שמורידים מהחנות של גוגל עוברות בדיקה בסיסית. לכן, אנו ממליצים להוריד אפליקציות למכשירי אנדרואיד רק מהחנות של גוגל. המנעו מהורדת אפליקציות אנדרואיד מאתרים אחרים מאחר שכל אחד, כולל פושעי סייבר, יכול בקלות ליצור ולהפיץ אפליקציות זדוניות ולגרום לכם להדביק את המכשיר שלכם. כהגנה נוספת, שקלו להתקין אנטיוירוס על המכשיר הנייד שלכם.

המפתח לשימוש מאובטח באפליקציות לנייד הוא התקנת אפליקציות רק ממקורות מהיימנים ושמירה על האפליקציות מעודכנות תוך וידוא ההרשאות שהן דורשות.

על מנת להפחית את הסיכון שלכם אפילו יותר, המנעו מאפליקציות חדשות לגמרי שמעט אנשים הורידו אותן, או שיש להן מעט חוות דעת חיוביות. ככל שהאפילקציה זמינה זמן רב יותר, או שיש עליה יותר חוות דעת חיוביות, כך ניתן לסמוך יותר על אפליקציה הזו. כמו כן, התקינו אך ורק את האפליקציות שאתם זקוקים להן. שאלו את עצמכם, האם אני באמת זקוק לאפליקציה הזו? לא רק שכל אפליקציה מעלה את הסיכון להדבקות אלא גם מעלה את הסיכון לפגיעה בפרטיות. אם אתם מפסיקים להשתמש באפליקציה, הסירו אותה מהמכשיר הנייד שלכם (אתם תמיד יכולים להוסיף אותה בחזרה בשלב מאוחר יותר אם אתם מגלים שאתם אכן זקוקים לה).

לבסוף, אתם עשויים להתפתות לפרוץ את המכשיר שלכם (jailbrake במכשירי 'אפל' ו root במכשירי אנדרואיד). זהו תהליך פריצה למכשיר המאפשר, בין השאר, להתקין אפליקציות לא מאושרות או לשנות תכונות קיימות במכשיר. אנו ממליצים בחום להמנע מכך, מאחר שפעולה כזו בעיקר עוקפת או מבטלת את מרבית מערכות ההגנה של המכשיר ועלולה לפגוע באחריות על המכשיר.

הרשאות

לאחר שהתקנתם אפליקציה ממקור מהיימן, הצעד הבא הוא לוודא שהגדרות האבטחה שלה שומרות על פרטיותכם. התקנה או הגדרה של אפליקציות לרוב דורשת שאתם תעניקו הרשאות מסוימות. תמיד הפעילו מחשבה לפני מתן הרשאה לגישה, האם האפליקציה אכן זקוקה להרשאות אלו על מנת לבצע את המשימה שלשמה היא נועדה. לדוגמא,

שימוש מאובטח באפליקציות מובייל

חלק מהאפליקציות דורשות גישה למיקום שלכם. אם אתם מאפשרים לאפליקציה תמיד לדעת את המיקום שלכם, ייתכן שאתם מאפשרים לכותבי האפליקציה לעקוב אחרי התנועות שלכם וייתכן שהם אפילו ימכרו מידע זה לאחרים. אם אתם לא מעוניינים לאפשר לאפליקציה הרשאה שהיא מבקשת, חפשו אפליקציה דומה שעומדת בדרישות שלכם. זכרו, יש לכם אפשרויות רבות. מכשירי 'אפל' מאפשרים לשנות חלק מההרשאות בזמן ההגדרה או הריצה כמו גישה למידע על המיקום שלכם. מכשירי חלונות ואנדרואיד שונים, מאפשרים רק בחירה בהכל או לא כלום, זאת אומרת אם אתם לא מאפשרים את כל ההרשאות המבוקשות, אתם לא יכולים להתקין את האפליקציה.

עדכון אפליקציות

אפילקציות לנייד, ממש כמו מערכת ההפעלה של המחשב או המכשיר הנייד שלכם, זקוקות לעדכונים. פושעים מחפשים בעקביות חולשות באפליקציות. לאחר מכן הם מפתחים התקפות על מנת לנצל חולשות אלו. הכותבים של האפליקציות שלכם מעדכנים את האפליקציות על מנת לתקן חולשות אלו ולהגן על המכשיר שלכם. ככל שתדירות בדיקת העדכונים והתקנתם תהיה גבוהה יותר, כך מצבכם יהיה טוב יותר. מרבית הפלטפורמות מאפשרות להגדיר את מערכת ההפעלה והאפליקציות לעדכונים אוטומטיים. אנו ממליצים על הגדרה זו. אם זה לא אפשרי, אנו ממליצים שתבדקו לפחות אחת לשבועיים עדכונים לאפליקציות שלכם. יש להקפיד שבזמן העדכון אתם מוודאים מהן ההרשאות שהאפליקציה מבקשת.

למדו עוד

הרשמו ל OUCH! הניוזלטר החודשי למודעות אבטחת מידע, גשו לארכיון OUCH!, בקרו אותנו ב http://www.securingthehuman.org ולמדו עוד על פתרונות מודעות אבטחת מידע של SANS.

מקורות

הנדסה חברתית:	http://www.securingthehuman.org/ouch/2014#november2014
להפטר מהמכשיר הנייד שלכם:	http://www.securingthehuman.org/ouch/2014#june2014
אבטחת הטאבלט החדש שלכם:	http://www.securingthehuman.org/ouch/2013#december2013
מושגי אבטחה נפוצים:	http://www.securingthehuman.org/resources/security-terms
SEC575:	http://www.sans.org/sec575