אאוץ! | מרץ 2017

מרכז סליקה בנקאי בע"מ שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

שימוש באפליקציות באופן מאובטח

סקירה כללית

עורך אורח

ג'וש רייט הוא המנהל הטכני שלCounter Hack ומדריך בכיר של מכון SANS. הוא המחבר של קורס SEC575: אבטחת התקנים ניידים, פריצה אתית וחשיפת פריצות ברשתות אלחוטיות. ניתן לעקוב אחריו בטוויטר **@joswr1ght**.

מכשירים ניידים כגון טאבלטים, סמארטפונים ושעונים חכמים הפכו לאחת מהטכנולוגיות העיקריות שאנו משתמשים בחיינו האישיים והמקצועיים. מה שמייחד את המכשירים הניידים הן מיליוני האפליקציות שאנו יכולים לבחור להתקין בהם. יישומים אלו מאפשרים לנו להיות פרודוקטיביים יותר, מאפשרים תקשורת מיידית ושיתוף עם אחרים, מאפשרים ללמד ולחנך או סתם להשתמש בהן בשביל הכיף. עם זאת, עם העוצמה של כל היישומים הללו באים סיכונים. הנה כמה צעדים שניתן לנקוט שיעזרו לך להשתמש בבטחה ולהפיק את המרב מהיישומים.

הורדת אפליקציות

הצעד הראשון הוא לוודא שאתה תמיד מוריד יישומים ניידים ממקור בטוח ומהימן. פושעי סייבר מנצלים את כישוריהם ביצירה והפצת יישומים ניידים נגועים שנראים לגיטימיים. אם תתקין אחד מהיישומים הנגועים אלה, הפושעים יכולים לקבל שליטה מלאה על ההתקן הנייד שלך. הורדה והתקנה של אפליקציות מחנויות ידועות וממקורות אמינים מקטינה את הסיכוי של התקנת אפליקציה נגועה. אתה אולי לא מודע שמותג המכשיר שאתה משתמש בו קובע את האפשרויות השונות להורדת אפליקציות.

עבור מכשירים של חברת אפל כמו אייפד או אייפון, ניתן להוריד אפליקציות לנייד מ- App Store של אפל. היתרון הוא שאפל עושה בדיקה ביטחונית של כל היישומים הניידים לפני שהם נעשים זמינים לציבור. חברת אפל לא יכולה לתפוס את כל האפליקציות הנגועות, אך סביבה מנוהלת עוזרת להפחית בשיעור ניכר את הסיכון בהתקנת אפליקציה נגועה. בנוסף, אם אפל מוצאת אפליקציה החשודה כנגועה בחנות שלה היא תסיר את האפליקציה מהנייד במהירות. טלפון נייד מבוסס "חלונות" משתמש באותה שיטה וגישה של יישומים מנוהלים.

שימוש באפליקציות באופן מאובטח

מכשירים ניידים עם מערכת הפעלה מסוג אנדרואיד שונים משאר המכשירים. אנדרואיד נותן לך גמישות רבה יותר ויכולת להוריד אפליקציה לנייד מכל מקום באינטרנט. עם זאת, עם גמישות זו גדלה צריכה לבוא אחריות גדולה. אתה צריך להיות יותר זהיר לגבי אלו אפליקציות תורידו ותתקינו משום שלא כל האפליקציות נבחנות. לחברת גוגל יש חנות אפליקציות סלולריות בדומה לחברת אפל, המכונה Google Play. היישומים אשר אתם מורידים מהחנות של גוגל עברו בדיקות אבטחה בסיסיות. עקב כך, אנו ממליצים להוריד יישומים עבור המכשירי אנדרואיד רק מהחנות של גוגל. הימנעו להוריד אפליקציות למכשירי אנדרואיד מאתרים אחרים, פושעי הסייבר יכולים בקלות ליצור ולהפיץ יישומים זדוניים, ולגרום לכם בדרכי מרמה להדביק בנוזקה את המכשיר הנייד שלכם. כאמצעי הגנה נוסף, כאשר הדבר אפשרי מומלץ להתקין אנטי וירוס במכשיר הסלולארי.

המפתח לשימוש באופן מאובטח באפליקציות במכשיר הנייד הוא להתקין אפליקציות רק ממקורות מהימנים, להתקין עדכונים זמינים, ולהעניק את ההרשאות הנדרשות לאפליקציה.

לא משנה באיזה מכשיר אתם משתמשים, צעד נוסף שאתם יכולים לבצע הוא להימנע מאפליקציות חדשות לגמרי, מספר הורדות נמוך או שיש להם מעט מאוד הערות חיוביות. ככל שאפליקציה כבר בעלת וותק וזמינה, יותר אנשים ירשמו הערות חיוביות, כך ניתן להניח כי האפליקציה לא נגועה ואפשר לסמוך עליה. בנוסף, יש להתקין רק את היישומים הדרושים לך ולשימושך. שאל את עצמך, האם אני באמת צריך את היישום הזה? כל אפליקציה היא פוטנציאל לנקודות תורפה חדשות בנוסף לשימוש במידע הפרטי שנמצא על המכשיר. אם אתם מפסיקים להשתמש באפליקציה, עליכם להסיר אותה מהמכשיר הנייד (ניתן תמיד להתקין אותה בחזרה מאוחר יותר, במידה ואתה מוצא את הצורך לכך). בנוסף, לא מומלץ לפרוץ את המכשיר הנייד. תהליך הפריצה גורם להתקנה של יישומים לא מאושרים או שינויים בהגדרות המכשיר. זה לא רק עוקף או מבטל את בקרות האבטחה המובנות של היצרן בתוך המכשיר הנייד, אלא לעתים קרובות גם פוגע באחריות המכשיר ולא ניתן לקבל תמיכה מהיצרן.

הרשאות

לאחר התקנת אפליקציה ממקור מהימן, יש לוודא שהאפליקציה מוגדרת בבטחה ושומרת על פרטיותכם. תמיד תחשבו לפני שאתם מאפשרים גישה מאפליקציה לנייד, אתם רוצים להעניק לאפליקציה את ההרשאה שהיא רוצה, האם האפליקציה באמת צריכה את זה? לדוגמה, יישומים מסוימים רוצים להשתמש בשירותי מיקום גיאוגרפי. אם אתם

שימוש באפליקציות באופן מאובטח

מאפשרים לאפליקציה תמיד לדעת את המיקום שלכם, אתם יכולים לאפשר ליוצר של אפליקציה לעקוב אחר התנועות שלכם, נביא גם בחשבון שיוצר האפליקציה יכול למכור את המידע הזה לאחרים. אם אינכם מעוניינים להעניק את ההרשאות, יש לדחות את בקשת ההרשאות או לחפש אפליקציה אחרת שעונה על הדרישות שלכם. זכרו, יש הרבה אפשרויות שם בחוץ.

עדכוני אפליקציות

אפליקציות, בדומה לתוכנות מחשב ומערכת ההפעלה, יש לעדכן כדי להישאר מעודכנים. פושעי הסייבר מחפשים ומאתרים חולשות ביישומים ובאפליקציות. לאחר מכן הם מפתחים התקפות אשר מנצלות חולשות אלה. המפתחים שיצרו את האפליקציות משחררים עדכונים על מנת לתקן את החולשות הללו ולהגן המכשירים שלכם. מומלץ לעדכן את האפליקציות במכשיר לעיתים תכופות ככל שניתן. רוב המכשירים מאפשרים להגדיר את עדכוני המערכת באופן אוטומטי. אנו ממליצים על הגדרה זו. אם הדבר אינו אפשרי, אז אנחנו ממליצים לכם לבדוק לפחות אחת לשבועיים עדכונים לאפליקציות שלכם. לבסוף, כאשר היישומים שלכם מעודכנים תמיד חשוב לוודא שאתם מאמתים את ההר־שאות שהאפליקציות עשויות לבקש.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

הנדסה חברתית:	https://securingthehuman.sans.org/ouch/2017#january2017
כיצד להיפטר מהמכשיר הנייד:	https://securingthehuman.sans.org/ouch/2016#december2016
אבטחת מחשב הלוח החדש שלך:	https://securingthehuman.sans.org/ouch/2016#january2016
ארכיון & תרגומים:	https://securingthehuman.sans.org/ouch/archives
קורס אבטחת התקנים ניידים:	https://sans.org/sec575

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר


securingthehuman.sans.org/blog


/securethehuman


@securethehuman


securingthehuman.sans.org/gplus