אאוץ! | דצמבר 2016

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

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- **המידע שלך**
- **מחיקת המכשיר**
- **כרטיס אחסון / סים (SIM)**

כיצד להחליף את המכשיר הנייד שלך באופן מאובטח

סקירה כללית

מכשירים ניידים, כגון טלפונים חכמים, שעונים חכמים ומ־חשבי לוח, ממשיכים להתקדם ולהתחדש בקצב מדהים. כתוצאה מכך, אנשים מחליפים את המכשירים הניידים שלהם לעתים קרובות ולפעמים אפילו מדי שנה. לצערנו אנשים רבים זורקים את המכשירים שלהם ללא תשומת לב לנתונים האישיים אשר שמורים במכשיר הנייד. בעלון זה נתאר את סוגי המידע האישי אשר עשויים להימצא במכשיר הנייד שלך ואיך אתה יכול למחוק אותם בצורה מאובטחת לפני זריקתו, החלפתו או החזרתו של המכשיר. אם המכשיר הנייד שלך ניתן לך על ידי מעסיקך, או שיש בו נתונים ארגוניים, הקפד לבדוק עם הממונה עליך את תהליכי הגיבוי והשמדת הנתונים על פי הנהלים בארגון לפני ביצוע השלבים הבאים.

עורך אורח

הת'ר מהליק (**@HeatherMahalik**; **+HMahalik**) מדענית בעלת הכשרה משפטית, מובילה את מאמצי הזיהוי הפלילי עבור חברת ManTech. היא מובילה ואחת ממחברי הקורס של מכון SANS, חקירות מחשב מתקדמות למכשירים ניידים ומדריכה בקורס ניתוח וחקירות מחשב של מיקרוסופט (FOR408). היא כותבת בבלוג **smarterforensics.com**.

המידע שלך

מכשירים ניידים מאחסנים מידע רגיש, הרבה יותר ממה שאתה משער, במיקרים רבים אפילו יותר מהמחשב שלך. מידע אופייני יכול לכלול:

- איפה אתה גר, מקום העבודה שלך ומקומות שאתה מרבה לבקר
- פרטים אודות אנשי הקשר מספר הכתובות והיישומים שלך ,כולל משפחתך, חברים ועמיתים לעבודה
- היסטוריית שיחות הכוללת שיחות נכנסות, יוצאות ושיחות שלא נענו
- הודעות SMS, הודעות קוליות ומולטימדיה
- הודעות צ'אט בתוך אפליקציות כגון: שיחות צ'אט מאובטחות, משחקים ומדיה חברתית
- היסטוריית מיקום מבוססת קואורדינטות של GPS או אנטנות סלולאר
- היסטוריית הגלישה באינטרנט, היסטוריית החיפוש, עוגיות ודפי מטמון
- תמונות אישיות, קטעי וידאו, הקלטות שמע ודואר אלקטרוני
- סיסמאות שמורות אשר מספקות גישה לחשבונות אישיים, כגון לבנק או לדוא"ל שלך
- גישה לתמונות שלך, קבצים או מידע המאוחסן בענן
- מידע בריאותי כגון גילך, קצב הלב, לחץ דם ואף דיאטה.

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

כיצד להחליף את המכשיר הנייד שלך באופן מאובטח

מחיקת המכשיר

כפי שהבנתם, ככל הנראה יש כמות עצומה של מידע רגיש במכשירים הניידים. לא משנה באיזה צורה תיפטרו מהמכשיר הנייד, כגון לתרום אותו, להחליף אותו בחדש, לתת אותו לבן משפחה אחר, למכור אותו או אפילו לזרוק אותו, דבר ראשון שעליכם לעשות הוא למחוק את כל המידע הרגיש במכשיר הנייד. זה קצת קשה לתפיסה, אבל מחיקה רגילה של הנתונים לא מספיקה, ניתן לשחזר אותם בקלות באמצעות כלים חינמיים מאינטרנט. עליכם למחוק באופן מאובטח את כל הנתונים במכשיר, תהליך הנקרא wipe (להשמיד מידע). תהליך זה משכתב ומחליף את כל המידע על מנת להבטיח שלא ניתן לשחזר את המידע. זכרו, כשלב ראשון לפני השמדת המידע יש לגבות את כל הנתונים, כך שתוכלו בקלות לבנות מחדש את המכשיר החדש שלכם.

בעת החלפת המכשיר הנייד שלך, ודא לבצע איפוס להגדרות יצרן, להסיר את ה-SIM ואת כרטיסי הזיכרון במידה והם נמצאים במכשיר הנייד.

הדרך הקלה ביותר להשמיד את המידע מהמכשיר באופן מאובטח היא להשתמש באופציית "איפוס להגדרות יצרן". זה יחזיר את המכשיר למצב בו הוא היה כאשר רכשתם אותו לראשונה. מצאנו כי איפוס להגדרות היצרן מספק שיטה בטוחה ופשוטה להסרת הנתונים מהמכשיר הנייד. פונקציית האיפוס להגדרות היצרן משתנית בין מכשירים; המפורטים להלן הם הצעדים עבור שני המכשירים הפופולריים ביותר.

- Apple iOS התקנים: הגדרות | כללי | איפוס | מחק את כל התוכן וההגדרות
- התקני אנדרואיד: הגדרות |כללי | גיבוי ואיפוס |שחזור נתוני יצרן

למרבה הצער, מחיקת נתונים אישיים מטלפון Windows אינה פשוטה כמו איפוס להגדרות יצרן. מחקרים נוספים מתנהלים על שיטות המחיקה בכדי להבטיח שהנתונים האישיים שלכם אכן נמחקים מהמכשיר. אם עדיין יש לכם שאלות על איך לבצע איפוס להגדרות יצרן, מומלץ לבדוק בהוראות ההפעלה שלך או באתר האינטרנט של היצרן. זכרו, מחיקה פשוטה של הנתונים האישיים שלכם אינה מספיקה משום שניתן לשחזר בקלות את הנתונים.

כרטיסי SIM & חיצוניים

בנוסף לנתונים המאוחסנים במכשיר, יש לשקול מה לעשות עם כרטיס הסים (Subscriber Identity Module). כרטיס הסים מיועד לבצע חיבור סלולארי ו/או נתונים למכשיר הנייד. בעת ביצוע איפוס להגדרות יצרן במכשיר, כרטיס הסים שומר מידע על החשבונות המשתמש שלכם. אם אתם נשארים עם אותו מספר טלפון ועוברים למכשיר חדש, עליכם לדבר עם ספק השירות של הטלפון החדש על העברת כרטיס הסים שלכם. אם הדבר אינו אפשרי, למשל

כיצד להחליף את המכשיר הנייד שלך באופן מאובטח

הטלפון החדש משתמש בכרטיס סים בגודל שונה, עליכם לשמור על כרטיס הסים הישן שלכם, לגזור אותו פיזית או להשמיד אותו לחלוטין על מנת למנוע מאדם אחר להשתמש בו.

לבסוף, חלק מהמכשירים הניידים מנצלים כרטיס זיכרון נפרד לצורך אחסון נוסף, כרטיס SD (Secure Digital). כרטיסי אחסון אלו בדרך כלל מכילים תמונות, אפליקציות ותוכן רגיש אחר. חשוב לזכור להוציא את כל כרטיסי האחסון החיצוניים מהמכשיר הנייד לפני שתיפרדו מהמכשיר (במכשירים מסוימים, כרטיסי הזיכרון עשויים להיות מוסתרים בתוך תא הסוללות של המכשיר, אולי מתחת הסוללה). ניתן להשתמש בכרטיסים אלו שוב ושוב בהתקנים ניידים חדשים, כמו כן, הם יכולים לשמש לאחסון גנרי במחשב עם מתאם USB. אם שימוש חוזר בכרטיס הזיכרון אינו אפשרי, אז בדיוק כמו כרטיס הסים הישן שלך, אנו ממליצים לך להשמיד אותו פיזית.

אם אתה לא בטוח לגבי כל אחד מהשלבים המכוסים בגיליון זה, מומלץ לקחת את המכשיר הנייד שלך לחנות שקנית אותו ולהיעזר בטכנאי מיומן. לבסוף, אם אתה רוצה לזרוק את המכשיר הנייד שלך, אנו מבקשים ממך לשקול לתרום אותו. יש הרבה ארגוני צדקה מעולים המקבלים התקנים ניידים משומשים.

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

אבטחת מחשב הלוח החדש שלך:	https://securingthehuman.sans.org/ouch/2016#january2016
גיבוי ושחזור:	https://securingthehuman.sans.org/ouch/2015#august2015
קורס Smartphone Forensics מתקדם:	https://sans.org/for585
ארכיון עלון אאוץ:	https://securingthehuman.sans.org/ouch/archives

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

