הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- בדיקות מקדימות
- מכשיר שאבד / נגנב
- גישה ל – WiFi
- מחשבים ציבוריים

להשאר מאובטח בדרכים

סקירה

בניוזלטר זה אנו נסקור כיצד ניתן להתחבר בצורה מאובטחת לאינטרנט ולבצע מטלות כאשר אתם בנסיעה.

עורך אורח

סטיב ארמסטרונג (Steve Armstrong) הוא המנהל הטכני של CyberCPR בחברת Logically Secure. הוא מדריך מוסמך של SANS ובעבר כתב קורסים ב – SANS. הוא פעיל בטוויטר כ **@Nebulator** ובגוגל פלוס כ **+SteveArmstrongSecurity**.

בדיקות מקדימות

בעוד שהרשת שלכם בבית או בעבודה מאובטחת, כאשר אתם בנסיעה אתם תמיד צריכים להניח שכל רשת שאתם מתחברים אליה אינה מאובטחת. לעולם אינכם יודעים מי עוד מחובר אליה וכיצד הוא מאיים עליכם. נקיטת מספר אמצעים בטרם יציאתכם לנסיעה יכולה לסייע לכם לשמור על המידע שלכם מאובטח:

- זהו את המידע שאינכם זקוקים לו במכשירים שאתם לוקחים אתכם והסירו אותו בצורה מאובטחת. פעולה זו תפחית משמעותית את ההשפעה במקרה שהמכשיר שלכם יאבד, ייגנב או יוחרם בידי פקידי מכס או אנשי אבטחת גבולות. אם זוהי נסיעת עבודה, נסו לקבל מכשיר חליפי ייעודי לנסיעות.
- בנסיעה לחוץ לארץ בדקו באיזה חשמל ובאילו שקעים משתמשים במדינת היעד. ייתכן שתזדקקו למתאמים על מנת לטעון את המכשירים שלכם. בנוסף בידקו את התוכנית הסלולרית שלכם. לרוב ספקי סלולר גובים סכומים גבוהים עבור שימוש בנתונים בחוץ לארץ, וייתכן שתרצו להשבית את תקשורת הנתונים כאשר אתם בחוץ לארץ או לעבור לתוכנית מיוחדת.
- התקינו תוכנה שמאפשרת לעקוב מרחוק אחרי המכשיר שלכם ואף למחוק אותו מרחוק במקרה שהוא נגנב או אובד. בהרבה מכשירים ניידים יש יכולת כזו מובנית וייתכן שרק תצטרכו להפעיל אותה (זכרו שתכונה זו זקוקה לחיבור אינטרנט במכשיר).

© SANS Institute 2015

להשאר מאובטח בדרכים

יום או יומיים לפני הנסיעה:

- עדכנו את המכשיר שלכם, אפליקציות ואנטי-וירוס וודאו שאתם מריצים את הגרסאות האחרונות.
- הפעילו את כל הגדרות האבטחה במכשיר שלכם, למשל הפעלת חומת אש (FireWall).
- נעלו את כל המכשירים הניידים שלכם עם סיסמה חזקה. בצורה כזו, אם תאבדו את המכשיר או שיגנבו אותו מכם, לא יוכלו לגשת למידע עליו.
- הצפינו את כל המכשירים שלכם כך שבמקרה של אובדן או גניבה לא ניתן יהיה לגשת לנתונים שלכם. חלק מהמכשירים (אייפון לדוגמה) עושים זאת באופן אוטומטי ברגע שמגדירים סיסמה.
- גבו את כל המכשירים שלכם. בצורה זו, אם משהו קורה להם בזמן שאתם בנסיעה, עדיין יהיה ברשותכם את המידע שלכם.

המפתח להשאר מאובטחים בזמן נסיעה הוא לאבטח את המכשירים שלכם לפני עזיבת הבית, לשמור עליהם מאובטחים פיזית, לדעת היכן הם בכל רגע ולהצפין כל תקשורת מול האינטרנט.

מכשיר שאבד / נגנב

בזמן הנסיעה שלכם, יש לדאוג לאבטחה הפיזית של המכשיר. לדוגמא, אף פעם אל תשאירו את המכשירים שלכם ברכב במקום בו העוברים והשבים יכולים לראות אותו, מאחר שגנבים פשוט ירסקו את שמשת המכונית וייקחו כל דבר בעל ערך שהם יראו. אחת האפשרויות היא להשתמש בכבל נעילה כך שתוכלו לנעול פיזית את המכשירים שלכם (בעיקר מחשב נייד) כאשר אתם עוזבים אותם. אמנם להיות קורבן לפשע הוא אכן סיכון, אך מה שאנשים פחות יודעים הוא שיש סיכוי גדול יותר לאבד את המכשיר מאשר שהוא ייגנב. לפי מחקר בן עשר שנים של חברת ווירזון (Verizon) הסיכוי לאבד מכשיר הוא פי 15 מאשר שהוא ייגנב. המשמעות היא שתמיד צריך לחזור ולוודא שהמכשיר שלכם איתכם בזמן נסיעה כמו לאחר בדיקת ביטחון בשדה התעופה, ביציאה ממונית או מסעדה, כאשר אתם עוזבים את המלון או לפני שאתם יוצאים מהמטוס.

גישה ל – WiFi

הגישה לאינטרנט בזמן נסיעה נעשית פעמים רבות באמצעות חיבור לרשתות WiFi ציבוריות כמו במלון, בבית קפה או בשדה התעופה. הבעיה עם רשתות ציבוריות היא לא רק העובדה שלעולם אין וודאות מי באמת הקים אותן, אלא גם העובדה שאתם לא יודעים מי מחובר אליהן. ככאלו יש להתייחס אליהן בחשדנות. למעשה זו אחת הסיבות מדוע נקטתם אמצעי זהירות עוד בטרם יצאתם לנסיעה שלכם. בנוסף, WiFi משתמש בגלי רדיו כדי לתקשר עם נקודת

© SANS Institute 2015

להשאר מאובטח בדרכים

הגישה לרשת האלחוטית. המשמעות היא שכל אדם עם קירבה פיזית אליכם יכול פוטנציאלית ליירט ולהאזין לתקשורת זו. לכן, אם אתם אכן משתמשים ברשתות WiFI ציבוריות אתם צריכים לוודא שכל התקשורת שלכם מוצפנת. לדוגמא, כאשר גולשים לאתרי אינטרנט יש לוודא שכתובת האתר מתחילה ב https:// ושליד הכתובת יש ציור של מנעול סגור. בנוסף, ייתכן שאתם משתמשים בחשבון רשת וירטואלית פרטית (Virtual Private Network – VPN) שמצפין את כל התקשורת שלכם. ייתכן שהנושא הוגדר לכם על ידי מקום העבודה או שניתן לרכוש שירות VPN לשימושכם הפרטי. אם אתם חוששים שאין באזורכם נקודות WiFi שניתן לסמוך עליהן אתם יכולים לשקול להפעיל גישת WiFi בטלפון הנייד שלכם. (אזהרה – כמו שציינו קודם זה עלול להיות יקר כאשר נוסעים לחוץ לארץ).

מחשבים ציבוריים

אל תשתמשו במחשבים ציבוריים כמו מחשבים בלובי של מלונות, ספריות או בתי קפה. אין לכם מושג מי השתמש במחשבים אלו לפניכם וייתכן שהם הדביקו את המחשב הציבורי הזה לפני כן בטעות או שבכוונה. כאשר זה אפשרי, השתמשו אך ורק במכשירים שיש לכם שליטה עליהם ושאתם סומכים עליהם לכל פעילות באינטרנט. אם בכל זאת אתם חייבים להשתמש במחשב ציבורי אל תשמשו בשום שירות שמחייב לבצע לוגין או להקיש סיסמה שלכם.

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

סיסמאות:	http://www.securingthehuman.org/ouch/2013#may2013
אימות בשני צעדים:	http://www.securingthehuman.org/ouch/2013#august2013
הצפנה:	http://www.securingthehuman.org/ouch/2014#august2014
אבטחת הטאבלט החדש שלכם:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

OUCH! מפורסם ע"י SANS Securing The Human ומופץ תחת רשיון Creative Commons BY-NC-ND 4.0. אתם חופשיים להפיץ את הניוזלטר הזה או להשתמש בו בתוכנית העלאת המודעות שלכם כל עוד שאינכם עורכים שינויים בניוזלטר. לתרגום ומידע נוסף אנא צרו קשר ב ouch@securingthehuman.org

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
צוות העורכים: ביל ווייימן, וולט סקריבנס, פיל הופמן, בוב רודיס.