OUCH! אוקטובר 2014

הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

חמישה צעדים על מנת להישאר מאובטח

סקירה

ככל שהטכנולוגיה מקבלת תפקיד מרכזי יותר בחיינו, כך גם גדלה המורכבות שלה. בהתחשב במהירות שבה טכנולוגיה משתנה, להישאר מעודכן בהנחיות האבטחה עלול להיות מבלבל. נראה שתמיד יש הנחיה חדשה לגבי מה שצריך או לא צריך לעשות. למרות זאת, בעוד הפרטים כיצד להישאר מאובטח עשויים להשתנות עם הזמן, יש מספר דברים בסיסיים שניתן תמיד לעשות על מנת להגן על עצמכם. ללא קשר לאיזו טכנולוגיה אתם משתמשים או היכן אתם משתמשים בה, אנו ממליצים על חמשת צעדי המפתח הבאים.

עורך אורח

לני זלצר (Lenny Zeltser) מתמקד באבטחת תפעול ה – IT של הלקוחות ב NCR ומלמד «לוחמה בנוזקות» (Malware Combat) בארגון SANS. לני פעיל בטוויטר כ **@lennyzeltser** וכותב בלוג אבטחה ב **blog.zeltser.com**.

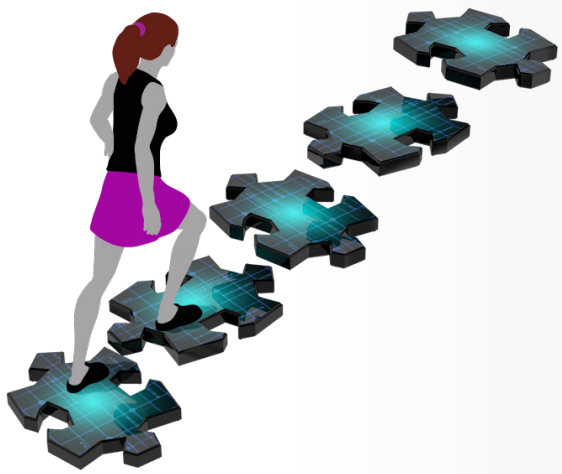
חמשה צעדי המפתח

כל אחד מחמשת הצעדים מהווה סקירה על קצה המזלג. כדי להעמיק בכל צעד, יש לפנות לחלק המקורות בסוף הניוזלטר הזה.

1. **אתם**: בראש ובראשונה זכרו שטכנולוגיה לבד לא יכולה להגן עליכם. תוקפים למדו שהדרך הקלה ביותר לעקוף את מרבית מערכות ההגנה היא לתקוף אתכם. אם הם רוצים את הסיסמה שלכם או פרטי כרטיס האשראי, הדבר הקל ביותר הוא לשטות בכם ולגרום לכם למסור את המידע הזה. לדוגמא, הם יכולים להתקשר אליכם ולהתחזות לאנשי התמיכה הטכנית של מיקרוסופט ולטעון שהמחשב שלכם נגוע, כאשר בפועל אלו פושעי סייבר שרוצים שתתנו להם גישה למחשב שלכם. או שאולי שישלחו אליכם דואר אלקטרוני המסביר שלא היה ניתן להעביר את החבילה שלכם ויבקשו מכם ללחוץ על קישור כדי לוודא את הכתובת שלכם, כאשר בפועל הם רוצים שתבקרו באתר זדוני שיסייע להם לפרוץ למחשב שלכם. לבסוף, ההגנה הטובה ביותר נגד תוקפים היא אתם. היו חשדניים, כך שעל ידי שימוש בהגיון בריא תוכלו לאתר ולעצור את מרבית המתקפות.

2. **עדכון**: וודאו שהמחשבים, המכשירים הניידים, האפליקציות וכל דבר אחר שלכם שמחובר לרשת מריץ את הגרסה האחרונה של התוכנה. פושעי סייבר מחפשים באופן עקבי אחר פגיעויות בטכנולוגיות שאתם משתמשים

חמישה צעדים על מנת להישאר מאובטח



על ידי ביצוע חמשת הצעדים האלו אתם תעשו קפיצת מדרגה בהגנה על עצמכם תוך שימוש בטכנולוגיה העדכנית ביותר.

בהן. כאשר הם מאתרים חולשות אלו, הם משתמשים בתוכנות מיוחדות כדי לנצל חולשות אלו ולפרוץ לאיזו טכנולוגיה שאתם משתמשים בה כולל הרשת, המחשב או המכשירים הניידים שלכם. בינתיים, החברות שיצרו את הטכנולוגיות שאתם משתמשים בהן עובדות קשה על מנת לשמור אותן מעודכנות. ברגע שמתגלה פגיעות, הם מייצרות תיקון לפגיעות זו ומשחררות אותו לציבור הרחב. על ידי ווידוא שהמחשבים והמכשירים הניידים שלכם מעודכנים, אתם מפחיתים את מספר הפגיעויות הידועות ומקשים מאוד על מישהו לפרוץ אליכם. כדי להישאר מעודכנים אפשרו עדכונים אוטומטיים כשזה אפשרי. כלל זה תקף כמעט לכל טכנולוגיה המקושרת לרשת כולל טלביזיות אינטרנט, מוניטורים לתינוקות, נתבים ביתיים, קונסולות משחק ואף המכונית שלכם יום אחד. עם מערכת ההפעלה של המחשב שלכם או המכשיר הנייד או כל טכנולוגיה אחרת שאתם משתמשים בה אינה נתמכת יותר ולכן לא תקבל עדכונים, אנו ממליצים להשיג גרסה עדכנית שנתמכת.

3. **סיסמאות**: הצעד הבא בהגנה על עצמכם מערב שימוש בסיסמה ייחודית וחזקה לכל אחד מהמכשירים שלכם, חשבונות מקוונים ואפליקציות. מילות המפתח פה הן חזק ו ייחודי. סיסמה חזקה משמעותה סיסמה שאינה ניתנת לניחוש בקלות ע»י האקרים או הכלים האוטומטיים שהם מפעילים. במקום שימוש במילה בודדת, השתמשו בביטוי סיסמה ארוך המורכב ממספר מילים עם סימנים מיוחדים הפזורים אקראית. ייחודי משמעותו שימוש בסיסמה שונה עבור כל מכשיר או חשבון מקוון. בדרך זו אם סיסמה אחת נחשפת כל שאר המכשירים והחשבונות שלכם בטוחים. מתקשים לזכור את כל אותן סיסמאות חזקות וייחודיות? אל דאגה, גם אנחנו. לכן אנו ממליצים על שימוש במנהל סיסמאות, אפליקציה מיוחדת לסמארטפון או המחשב שלכם שמאחסנת בצורה מאובטחת ומוצפנת את כל הסיסמאות שלכם. לבסוף, אם מי מהחשבונות שלכם תומך בהזדהות דו שלבית, אנו ממליצים בחום לאפשר זאת תמיד מאחר שזו אחת מהשיטות החזקות ביותר לשמור על החשבון.

4. **הצפנה**: צעד שלישי שאנו ממליצים עליו הוא שימוש בהצפנה. הצפנה מוודאת שרק אתם או אנשים שאתם סומכים עליהם יכולים לגשת למידע שלכם. מידע יכול להיות מוצפן בשני מצבים: במנוחה ובתנועה. הצפנת מידע במנוחה משמעותה הגנה עליו בזמן שהוא מאוחסן כקבצים כמו בדיסק הקשיח או בזכרון נייד שלכם.

חמישה צעדים על מנת להישאר מאובטח

מרבית מערכות ההפעלה מאפשרות לכם להצפין את המידע שלכם באמצעות הצפנת דיסק מלאה (Full Disk Encryption). אנו ממליצים שתאפשרו זאת בכל מקום שזה קיים. הצפנת מידע בתנועה משמעותה הצפנת המידע בזמן שהוא משודר מהמחשב או המכשיר שלכם לאחרים לדוגמא בזמן שאתם גולשים לאתר הבנק שלכם. דרך פשוטה לוודא אם הצפנה עובדת היא לוודא ששורת הכתובת של האתר מתחילה ב https ושציור של מנעול קטן סגור מופיע לידה.

5. **גיבוי**: לעיתים, לא משנה כמה זהירים אתם, אחד מהמכשירים או החשבונות שלכם עלול להיפרץ. אם זה המצב, לעיתים קרובות האפשרות היחידה שלכם לוודא שהחשבון או המכשיר שלכם נקי מנוזקות היא למחוק אותו לחלוטין ולבנות אותו מחדש. התוקף אפילו עלול למנוע מכם גישה לקבצים האישיים שלכם, תמונות ומידע נוסף האגור במכשיר או בחשבון שנפרצו. האפשרות היחידה עשויה להיות שיחזור הכל מהתחלה מגיבוי. וודאו שאתם מגבים את המידע שלכם על בסיס קבוע ובדקו שניתן לשחזר את המידע במקרה הצורך. מרבית מערכות ההפעלה והמכשירים הניידים תומכים בגיבוי.

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

מתקפות דיוג על דואר אלקטרוני: http://www.securingthehuman.org/ouch/2013#february2013
שמירה על מחשב הלוח שלכם (טאבלט) מאובטח: http://www.securingthehuman.org/ouch/2013#december2013
סיסמאות חזקות: http://www.securingthehuman.org/ouch/2013#may2013
מנהלי סיסמאות: http://www.securingthehuman.org/ouch/2013#october2013
אימות בשני שלבים: http://www.securingthehuman.org/ouch/2013#august2013
הצפנה: http://www.securingthehuman.org/ouch/2014#august2014
גיבויים: http://www.securingthehuman.org/ouch/2013#september2013

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

