OUCH! נובמבר 2014

הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- הנדסה חברתית
- איתור / עצירת מתקפת הנדסה חברתית
- מניעת התקפות עתידיות

הנדסה חברתית

סקירה

אנשים רבים מאמינים (בטעות) שהאקרים משתמשים רק בכלים ושיטות מתקדמים על מנת לפרוץ למחשבים, חשבונות ומכשירים ניידים של אנשים. זה פשוט לא נכון. האקרים למדו שאחת הדרכים הקלות ביותר לגנוב את המידע שלכם או לפרוץ למחשב שלכם היא על ידי הטעייתכם. בניוזלטר זה אנו נלמד איך שיטות כאלו של מתקפות הנקראות הנדסה חברתית עובדות ומה ניתן לעשות על מנת להתגונן מפניהן.

עורכת אורחת

אליסה טורס (Alissa Torres) היא מדריכת SANS מוסמכת, המתמחה בחקירת מחשבים ומענה לאירועים. הנסיון התעסוקתי שלה כולל עבודה בצוותי אבטחת מידע פנימיים, בצוותי תגובה וכחוקרת אירועי מחשב. ניתן למצוא אותה בטוויטר כ **@siberor**.

הנדסה חברתית

הנדסה חברתית היא סוג של מתקפה פסיכולוגית כאשר התוקף מוליך אתכם שולל לבצע משהו שהוא מעוניין שתבצעו. הנדסה חברתית קיימת כבר אלפי שנים. הרעיון להונות ולרמות מישהו הוא לא חדש. עם זאת, האקרים למדו ששימוש בטכניקה זו באינטרנט הוא יעיל מאוד ויכול לשמש לתקיפת מליוני אנשים. הדרך הפשוטה ביותר להבין כיצד הנדסה חברתית עובדת היא להסתכל על דוגמאות כלליות מהעולם האמיתי.

אתם מקבלים שיחת טלפון ממישהו שמתחזה לעובד של חברת תמיכת מחשבים, ספק האינטרנט שלכם או אולי מהתמיכה הטכנית של מיקרוסופט. המתקשר מסביר שהם זיהו שהמחשב שלכם מתנהג בצורה מוזרה (כמו לסרוק את האינטרנט או לשלוח ספאם -דואר זבל) והוא מאמין שהוא נגוע בפוגען. הוטל עליו לחקור את הנושא ולעזור לכם לאבטח את המחשב שלכם. ואז הוא משתמש במושגים טכניים שונים ומוביל אתכם בצורה מטעה ומבלבלת על מנת לשכנע אתכם שהמחשב שלכם נגוע.

לדוגמא, הוא עלול לשכנע אתכם לבדוק האם קבצים מסויימים נמצאים על המחשב שלכם, ואף יסביר כיצד למצוא את הקבצים האלו. כאשר אתם מאתרים את הקבצים האלו, המתקשר ישכנע אתכם שהקבצים האלו הם ההוכחה שהמחשב שלכם נגוע, כאשר בפועל אלו קבצי מערכת הנמצאים על כל מחשב ממוצע. ברגע שהוא שכנע אתכם שהמחשב שלכם נגוע, הוא ילחץ עליכם לגשת לאתר האינטרנט שלהם ולקנות את תוכנת האבטחה שלהם או יבקש

© The SANS Institute 2014

הנדסה חברתית

מכם לתת לו גישה מרחוק למחשב שלכם כדי שהוא יוכל לתקן אותו. עם זאת, התוכנה שהם מוכרים היא למעשה נוזקה. אם אתם קונים ומתקינים את התוכנה לא רק שהם הצליחו לרמות אתכם ולהדביק את המחשב שלכם, אלא שגם שילמתם להם כדי לעשות זאת. אם אתם נותנים להם גישה מרחוק למחשב שלכם כדי לתקן את זה, הם בפועל הולכים להשתלט עליו ולהדביק אותו.

תמיד תזכרו שהנדסה חברתית אינה מוגבלת לשיחות טלפון בלבד. היא יכולה להתבצע כמעט עם כל טכנולוגיה כולל מתקפות דיוג בדואר אלקטרוני, סמס, פייסבוק, טוויטר ושיחות אונליין. המפתח הוא לדעת ממה להזהר.

ללמוד כיצד למנוע, לזהות ולעצור מתקפות הנדסה חברתית זה אחד הצעדים היעילים ביותר שאתם יכולים לנקוט על מנת להגן על עצמכם.

זיהוי / מניעת מתקפות הנדסה חברתית

הדרך הפשוטה ביותר להמנע ממתקפות הנדסה חברתית היא להפעיל הגיון בריא. אם משהו נראה חשוד או מרגיש לא טוב, זו עשויה להיות מתקפה. כמה אבני בוחן כלליות לאיתור מתקפות הנדסה חברתית הן:

- מישהו נותן לכם תחושה של דחיפות גדולה. אם אתם מרגישים שאתם תחת לחץ כדי לקבל החלטה, היו חשדניים.
- מישהו מבקש מידע שלא אמורה להיות לו גישה אליו, או שהוא היה אמור כבר לדעת אותו.
- משהו שהוא יותר מדי טוב כדי להיות אמיתי. דוגמא נפוצה היא קבלת הודעה על זכיה בלוטו למרות שמעולם לא השתתפתם בהגרלה.

אם אתם חושדים שמישהו מנסה להפוך אתכם לקורבן של מתקפת הנדסה חברתית אל תיצרו קשר איתו יותר. אם זה מישהו שמתקשר אליכם לטלפון, נתקו את השיחה. אם זה מישהו שמושחח איתכם אונליין, נתקו את הקשר. אם זה דואר אלקטרוני שאינכם סומכים עליו, מחקו אותו. אם ההתקפה קשורה לעבודתכם, דווחו על האירוע למרכז התמיכה או מחלקת אבטחת המידע באופן מיידי.

מניעת התקפות הנדסה חברתית עתידיות

למזלנו יש צעדי מנע שניתן לנקוט בהם על מנת למנוע את חשיפתכם למתקפות הנדסה חברתית עתידיות:

© The SANS Institute 2014

הנדסה חברתית

- **אף פעם על תחלקו סיסמאות**: אף ארגון לא ייצור אתכם קשר ויבקש את הסיסמה שלכם. אם מישהו מבקש מכם את הסיסמה שלכם, סימן שזו מתקפה.

- **אל תחשפו יותר מדי מידע**: ככל שהתוקף יודע עליכם יותר, כך קל לו יותר להוליך אתכם שולל. אפילו שיתוף מעט מידע עלול להוביל עם הזמן לקבלת תמונה מלאה עליכם. ככל שתחשפו פחות מידע על עצמכם, כולל במדיה חברתית, חוות דעת, פורומים ורשימות תפוצה, כך יפחת הסיכוי שתותקפו.

- **וודאו את אנשי הקשר שלכם**: לעיתים אתם תקבלו פניה מהבנק שלכם, חברת כרטיסי האשראי, ספק הסלולר או האינטרנט או כל ארגון אחר שיש לכם קשרים איתו בנסיבות לגיטימיות. אם יש לכם ספק לגבי לגיטימיות הפניה או הבקשה, בקשו מהאדם בצד השני לשמו ולשלוחת הטלפון שלו. לאחר מכן מיצאו את הטלפון של הגוף שהתקשר אליכם (למשל באתר האינטרנט של אותו גוף). בצורה זו, כאשר אתם מתקשרים לאותו גוף, אתם יודעים שאתם באמת מדברים איתם. למרות שזה נראה כמו טירחה, שמירה על הזהות שלכם והמידע האישי שלכם בהחלט מצדיקים את המאמץ הנוסף.

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

התקפות דיוג בדואר אלקטרוני: http://www.securingthehuman.org/ouch/2013#february2013

התנהלות בטוחה במדיה חברתית: http://www.securingthehuman.org/ouch/2013#march2013

המנעות מתרמיות: http://www.onguardonline.gov/topics/avoid-scams

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.