אאוץ! | ינואר 2017

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

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- מהי הנדסה חברתית
- זיהוי / עצירת התקפות הנדסה חברתית

הנדסה חברתית

סקירה כללית

טעות נפוצה בנוגע לתוקפי הסייבר היא, כי הם משתמשים רק בכלים וטכניקות מתקדמים ביותר כדי לפרוץ למחשבים או לחשבונות של אנשים. זה לא נכון. תוקפי סייבר למדו כי לעתים קרובות הדרך הקלה ביותר לגנוב את המידע שלך, לפרוץ לחשבונות שלך או להדביק המערכות שלך היא פשוט לגרום לך לעשות טעות. בעלון זה תוכל ללמוד כיצד התקפות אלה, הידועות בשם הנדסה חברתית עובדות ומה אתה יכול לעשות כדי להגן על עצמך.

עורך אורח

ג'יימס לין (@jameslyne) הוא מדריך SANS מוסמך וראש מחלקת מחקר ב- Sophos. הוא מנתח את היצירות החדשות והאיכותיות ביותר של פושעי סייבר. הוא גם המחבר של מספר קורסים ב SANS : Metasploit (SEC580) והנדסה חברתית (SEC567).

מהי הנדסה חברתית

הנדסה חברתית היא התקפה פסיכולוגית, התוקפים משתמשים בטריקים על מנת לשכנע אותך לעשות משהו שאתה לא צריך לבצע. הרעיון של הנדסה חברתית הוא לא חדש, הוא קיים כבר אלפי שנים. תחשוב על רמאים או נוכלים, עצם הרעיון זהה. הטכנולוגיה של היום כל כך הרבה יותר יעילה עבור התוקפים משום שאתה לא יכול לראות אותם פיזית, הם יכולים בקלות להעמיד פנים ולהתחזות למישהו אחר, הם יכולים לתקוף מיליוני אנשים ברחבי העולם, כולל אותך. בנוסף, תקיפות מסוג הנדסה חברתית יכולות לעקוף טכנולוגיות אבטחה רבות. הדרך הפשוטה ביותר להתגונן היא להבין את ההתקפות האלו ובכך להגן על עצמך מפניהם. שים לב לשתי דוגמאות מהעולם האמיתי.

אתה מקבל שיחת טלפון ממישהו שטוען שהוא מחברה לתמיכת מחשבים, ספק שירותי האינטרנט שלך או אולי מהתמיכה הטכנית של מיקרוסופט. המטלפן מסביר שהמחשב מפעיל סורק אשר סורק את האינטרנט, הם מאמינים שהמחשב נגוע והם רוצים לעזור לך לאבטח את המחשב. לאחר מכן הם משתמשים במגוון של מונחים טכניים ובכך הם מצליחים לשכנע אותך כי המחשב נגוע. לדוגמה, הם עשויים לבקש ממך לבדוק אם יש לך קבצים מסוימים במחשב שלך וללוות אותך לאורך התהליך על איך למצוא אותם. כשאתה מאתר את הקבצים, המתקשר מבטיח לך כי הקבצים האלו הם הוכחה כי המחשב נגוע, כאשר באמת קבצים אלה הם קבצי מערכת וניתן למצוא אותם בכל מחשב בעולם.

הנדסה חברתית

השכל הישר הוא ההגנה החזקה ביותר שלך בזיהוי והפסקת התקפות מסוג הנדסה חברתית.

ברגע שהם רימו אותך להאמין כי המחשב שלך נגוע, הם לוחצים אותך לקנות את תוכנות האבטחה שלהם או לתת להם גישה מרחוק למחשב שלך, כך שהם יכולים לתקן את זה. עם זאת, התוכנה שהם מוכרים היא למעשה תכנית זדונית. אם אתה רוכש ומתקין את התוכנה, הם שכנעו אותך להדביק את המחשב שלך ובנוסף אתה שילמת להם לעשות את זה. אם אתה נותן להם גישה מרחוק למחשב שלך, הם ישתלטו על המחשב, יגנבו את הנתונים שלך, או שהם ישתמשו במחשב עבור צרכיהם.

דוגמה נוספת היא התקפה הדוא"ל שנקראת הונאת המנכ"ל, אשר לרוב מתרחשת בעבודה. התוקף מבצע מחקר אודות מקום העבודה שלך, מזהה את שם הבוס שלך או עמית לעבודה. התוקף שולח דוא"ל מזויף אשר מתיימר להיות מאותו מכר אשר שולח את הדוא"ל אלייך. הדוא"ל מבקש ממך לבצע פעולה בדחיפות, כגון ביצוע העברה בנקאית או שליחת מידע רגיש. לעיתים קרובות מיילים אלה מעמידים פנים שיש מקרה חירום המחייב פעולה דחופה מצידך שכלולה לעקוף נהלי ביטחון קבועים, למשל הם עשויים לבקש ממך לשלוח את המידע הרגיש ביותר לחשבון האישי @gmail.com. מה הופך את ההתקפות הממוקדות האלו למסוכנות במיוחד,זה שהתוקף מבצע מחקר לפני הפעולה. בנוסף, טכנולוגיות אבטחה כמו אנטי וירוס או חומת אש לא יכולות לזהות או לעצור התקפות אלה כי אין תוכנות זדוניות או קישורים זדוניים מעורבות.

זכור, תקיפות מסוג הנדסה חברתית כמו אלה אינם מוגבלים רק בשיחות טלפון או בדואר אלקטרוני; הם יכולים לקרות בכל צורה שהיא למשל הודעות טקסט לטלפון שלך, במדיה חברתית או אפילו פנים מול פנים. המפתח הוא לדעת מה לחפש, אתה ההגנה הטובה ביותר שלך.

גילוי / עצירת תקיפות מסוג הנדסה חברתית

למרבה המזל הדרך לעצור התקפות אלו היא פשוטה, אתה יכול לחשוב - שכל ישר הוא ההגנה הטובה ביותר שלך. אם משהו נראה חשוד או לא מרגיש נכון, זה יכול להיות התקפה. הרמזים הנפוצים ביותר להתקף הנדסה חברתית כוללים:

הנדסה חברתית

- מישהו יוצר תחושה עצומה של דחיפות, הם מנסים להאיץ בך לעשות טעות.
- מישהו מבקש מידע שאין לו צורך לגישה אליו או שהוא כבר צריך לדעת, כגון מספרי החשבון שלך.
- מישהו מבקש את הסיסמה שלך, אף ארגון לגיטימי לא ישאל אותך על זה.
- מישהו לוחץ עליך לעקוף או להתעלם מתהליכי אבטחה מקובלים בעבודה.
- משהו טוב מכדי להיות אמיתי. לדוגמא אתה מקבל הודעת הזכייה בלוטו או אייפד, למרות שלא נרשמת להגרלה.
- אתה מקבל הודעת דוא"ל מוזר מידיד או עמית לעבודה, המכיל נוסח שלא נראה כמו שהם בדרך כלל שולחים. ייתכן כי תוקף הסייבר פרץ לחשבון שלהם ומנסה להונות אותך. כדי להגן על עצמך, ודא בקשות כאלה על ידי יצירת קשר עם החבר בדרכים שונות כגון פנים אל פנים או בטלפון.

אם אתה חושד שמישהו מנסה להערים או להטעות אותך, יש להפסיק את ההתקשרות עם אדם זה. אם ההתקפה קשורה לעבודה, הקפד לדווח על כך למוקד התמיכה שלך או צוות אבטחת מידע. זכור, שכל ישר הוא לעתים קרובות ההגנה הטובה ביותר שלך.

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

דיוג:	https://securingthehuman.sans.org/ouch/2015#december2015
הונאת המנכ"ל:	https://securingthehuman.sans.org/ouch/2016#july2016
כופר:	https://securingthehuman.sans.org/ouch/2016#august2016
אאוץ ארכיון:	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