אאוץ! | יולי 2016

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

עלון מודעות אבטחת מידע למשתמשי מחשב

OUCH!

בגיליון זה...

- מה היא הונאת המנכ"ל?
- הגן על עצמך

הונאת המנכ"ל

מה היא הונאת המנכ"ל?

פושעי סייבר הם ערמומיים - הם כל הזמן מוצאים דרכים חדשות על מנת להשיג את מבוקשם. אחת השיטות היעי לות ביותר היא להציב למטרה אנשים כמוך. תוקפי סייבר למדו כי אנשים ללא מודעות אבטחה הם החוליה החלשה ביותר בכל ארגון, הם שכחו כי אנשים בעלי ידע באבטחה כמו קוראי OUCH! יכולים להיות ההגנה הטובה ביותר של ארגון.

עורך אורח

אנגילה פאפאס (Angela Pappas), מנהלת הדרכות אבטחת מידע ומודעות בתומסון רויטרס. בתפקידה, אנגילה היא אחראית על תכנית השגריר, למידה אלקטרונית וחינוך עובדים על התחזות.

פושעי סייבר פיתחו התקפה חדש בשם הונאת המנכ"ל, הידוע גם בשם ירוט דוא"ל עסקי (BEC - Business Email Compromise). בהתקפות אלו, פושע הסייבר מתיימר להיות מנכ"ל או מנהל בכיר אחר מהארגון שלך. הפושעים שולחים מייל לאנשי צוות כמוך על מנת להטעות אותך ולגרום לך לעשות משהו שאתה לא אמור לעשות. התקפות אלו יעילות במיוחד משום שפושעי הסייבר מבצעים את מחקרם לפני ההתקפה. הם מחפשים אתרי אינטרנט של הארגון לקבלת מידע כגון היכן הוא ממוקם, מי המנהלים שלך, וארגונים אחרים אשר אתה עובד איתם. בעזרת מידע זה הם לומדים כל שביכולתם על עמיתיך לעבודה באתרים כמו לינקדאין, פייסבוק או טוויטר. ברגע שהם יודעים את המבנה הארגוני של אירגונך, הם מתחילים לחקור ולהציב מטרות כגון עובדים ספציפיים. הם בוחרים את המטרות שלהם בקפידה על מנת להשיג את מטרתם הספציפית. במידה ופושעי הסייבר מחפשים כסף, הם יכולים להציב למטרה את הצוות במחלקת הנהלת החשבונות. אם הם מחפשים מידע אישי על עובדים, הם יכולים להציב למטרה את מחלקת משאבי אנוש. אם הם רוצים גישה לשרתי מסד הנתונים, הם יכולים להציב למטרה עובד במחלקת תשתיות.

ברגע שהם קבעו את מטרתם ואת מי עליהם לתקוף, הם יתחילו לעצב את המתקפה. לרוב הם ישתמשו בדיוג ממוקד (spear phishing). התקפת דיוג (phishing) מבוצעת כאשר התוקף שולח דוא"ל אל מיליוני אנשים במטרה להטעות אותם לביצוע פעולה, למשל פתיחת קובץ מצורף נגוע או ביקור באתר זדוני. דיוג ממוקד מאוד דומה להתחזות, עם זאת, במקום לשלוח דוא"ל גנרי למיליוני אנשים, הם שולחים דוא"ל ממוקד ומותאם אישית למספר קטן מאוד ונבחר

© SANS Institute 2016

הונאת המנכ"ל

הונאת המנכ"ל היא התקפה חזקה שיכולה לעקוף את רוב מנגנוני ההגנה. בסופו של דבר אתה ההגנה הטובה ביותר שלנו.

של אנשים. מייל מסוג דיוג ממוקד מאוד מציאותי וקשה מאוד לזיהוי. לעתים קרובות הדואר האלקטרוני יגיע ממישהו שאתה מכיר או עובד עמו, כגון קולגה לעבודה או אולי אפילו הבוס שלך. הדוא"ל נראים מציאותיים ככל הניתן, הם יכולים להשתמש באותה שפה או בסלנג אשר הקולגות שלך משתמשים בהם, הם יכולים להשתמש בלוגו של הארגון שלך או אפילו לזייף את החתימה הרשמית של מנהל בכיר בארגון. דוא"ל אלו לעתים קרובות יוצרים תחושה עצומה של דחיפות, דורשים ממך לנקוט בפעולה מיידית ולא לספר לאף אחד. המטרה של פושעי הסייבר היא לגרום לך לעשות טעות. הנה שלושה תרחישים נפוצים:

העברה בנקאית - פושעי סייבר רודפים אחרי הכסף. משמעות הדבר שהם יחקרו וילמדו עובדים בעלי גישה לכספים, מקורות מימון, או צוות הנהלת החשבונות של הארגון. הפושעים יעצבו וישלחו דוא"ל אשר מתיימר להיות מהמנהל של הנמען, הדוא"ל אומר לנמען שיש מקרה חירום ושעליו להעביר כספים באופן בהול לחשבון מסוים.

הונאת מידע אישי - פושעי הסייבר רוצים לגנוב מידע אישי על הקולגות שלך על מנת שיוכלו להתחזות לעובדים עבור הונאות שונות. הם יחקרו את הארגון, ימצאו מי מטפל במידע על עובדים, למשל, מישהו ממחלקת משאבי אנוש. משם, פושעי הסייבר ישלחו דוא"ל מזויפים אשר מתיימרים להיות ממנהל בכיר או אולי עובד במחלקה משפטית, בדרישה לקבלת מסמכים מסוימים באופן מיידי.

התחזות לעו"ד - לא כל הונאת המנכ"ל כרוכה רק בדוא"ל, ניתן להשתמש בשיטות נוספות כגון הטלפון. בתרחיש זה, הפושע יתחיל את ההתקפה על ידי שליחה של דואר אלקטרוני אשר מתיימר להיות ממנהל בכיר, המנהל יכתוב לך כי עורך הדין שלו יתקשר אלייך בעניין דחוף. הפושע יתקשר לקורבן ויציג את עצמו כעורך הדין של המנהל. הפושע יוצר תחושה עצומה של דחיפות. בזמן השיחה הפושע והקורבן מדברים על נושאים רגישים וסודיים. תחושה זו של דחיפות וסודיות גורמת לקורבן להישאב לתוך המשחק באופן מיידי.

הונאת המנכ"ל

הגן על עצמך

אז מה ניתן לעשות בכדי להגן על עצמך ועל הארגון שלך? היגיון בריא הוא ההגנה הטובה ביותר. אם קיבלת הודעה מהבוס שלך או קולגה וזה לא נשמע או מרגיש נכון, זה יכול להיות התקפה. הרמזים יכולים לכלול תחושה אדירה של דחיפות, חתימה לא נראית תקינה, טון דיבור לא צפוי, או שהשם של שולח הדוא"ל שונה מהשם של שהאדם שמתקשר אליך. עוד רמז יהיה כאשר התוקף מתקשר ממספר טלפון או כתובת דואר אלקטרוני שמעולם לא ראית קודם, או אולי שהם משתמשים בכתובת דוא"ל דומות מאוד אבל לא בדיוק אותו הדבר כמו קולגות לעבודה או אפילו המנהל שלך. במקרה של ספק, התקשר לאדם למספר טלפון מהימן ומוכר, בנוסף תציע לפגוש אותם פנים אל פנים וכך תוכל לאמת שהם אכן שלחו את הדואר האלקטרוני (לא לבקש פגישה באמצעות הדואר האלקטרוני, אלא בטלפון). לעולם לא לעקוף מדיניות אבטחה או נהלים. בארגון שלך יש מדיניות ונהלים לצורך העברת כספים או מסירת חומר סודי. בק שות המנסות לעקוף את הנהלים האלו, צריכות להיחשב לחשודות, יש לאמת לפני ביצוע הפעולה. אם קיבלת בקשה כזו, ואתה לא בטוח מה לעשות, פנה לממונה עליך, למחלקת התמיכה או לצוות אבטחת מידע מייד.

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

הנדסה חברתית:	https://securingthehuman.sans.org/ouch/2014#november2014
דיוג:	https://securingthehuman.sans.org//ouch/2015#december2015
מהי תוכנה זדונית:	https://securingthehuman.sans.org/ouch/2016#march2016
אימות בשני שלבים:	https://securingthehuman.sans.org/ouch/2015#september2015
העצה היומית:	https://www.sans.org/tip-of-the-day

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Securing The Human, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה ouch@securingthehuman.org.

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

© SANS Institute 2016