אאוץ! | באוקטובר 2016

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

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- אתה
- סיסמאות
- עדכונים
- גיבויים

ארבעה שלבים להשאר בטוח

סקירה כללית

בזמן שהטכנולוגיה לוקחת תפקיד חשוב יותר בחיינו, כך גם גדלה מורכבותָ. בהתחשב כמה מהר חלים שינויי טכ־ נולוגיה, שמירה על ייעוץ אבטחתי יכול להיות מבלבל. זה נראה כאילו תמיד יש הנחיה חדשה על מה שאתה צריך או לא צריך לעשות. עם זאת, בעוד שהפרטים של איך להישאר מאובטח עשויים להשתנות עם זמן, יש דברים בסיסיים שאתה תמיד יכול לעשות כדי להגן על עצמך. לא משנה מה הטכנולוגיה שאתה משתמש או איפה אתה משתמש בה, אנו ממליצים על ארבעת השלבים העיקריים הבאים. כדי ללמוד עוד על כל אחד מהשלבים הבאים, עיין בסעיף "מקורות" בסוף עלון זה.

עורך אורח

ריאן ג'נסון מתמקד בלהבטיח שארגונים יהיו מוכנים להגיב לפריצה בלתי נמנעת ומלמד חקר תעבורה רשתית מתקדם במכון SANS. ריאן פעיל בטוויטר כ- @ForensicRJ.

1. **אתה**: בראש ובראשונה, יש לזכור כי טכנולוגיה לבדה לא תוכל להגן עליך לגמרי. תוקפים למדו שהדרך הקלה ביותר לעקוף אפילו את טכנולוגית האבטחה המתקדמת ביותר היא לתוקף אותך. אם הם רוצים את הסיסמה, כרטיס אשראי או מידע אישי, הדבר הכי קל לתוקפים לעשות הוא להערים עליך לתת להם את המידע הזה. לדוגמא, הם יכולים להתקשר אליך להתיימר להיות תמיכה טכנית של מיקרוסופט בטענה כי המחשב שלך נגוע, כאשר במציאות הם רק פושעי סייבר שרוצים שתיתן להם גישה למחשב שלך. או אולי הם ישלחו לך דוא"ל שמסביר שלא ניתן היה למסור את החבילה שלך ולבקש ממך ללחוץ על קישור כדי לאמת את כתובת המשלוח שלך, כאשר במציאות הם הטעו אותך לבקר באתר זדוני כדי לפרוץ למחשב שלך. כך התקפות כגון כופר או הונאה המנכ"ל מתחילות. בסופו של דבר, ההגנה הטובה ביותר נגד תוקפים היא אתה. היה חשדן. באמצעות שכל ישר אתה יכול לזהות ולעצור רוב ההתקפות.

2. **סיסמות**: השלב הבא כדי להגן על עצמך כרוך באמצעות סיסמא חזקה וייחודית עבור כל ההתקנים שלך וחשבונות מקוונים. מילות המפתח כאן הן חוזק וייחודיות. סיסמא חזקה פירושה שלא ניתן לנחש אותה בקלות על ידי האקרים

© SANS Institute 2016

ארבעה שלבים להשאר בטוח

או על ידי התוכנות האוטומטיות שלהם. נמאס לך לזכור סיסמאות מורכבות וקשות וקשה להקליד? נסה להשתמש בביטוי סיסמא במקום. במקום מילה אחת, להשתמש בסדרה של מילים שקל לזכור, כגון "איפה הקפה שלי?". ככל שמשפט הסיסמה ארוך יותר כך הוא חזק יותר. סיסמה ייחודית אומר שימוש בסיסמה שונה עבור כל התקן וחשבון מקוון. בדרך זו, אם סיסמא אחת נפגעת, כל החשבונות וההתקנים האחרים שלך עדיין בטוחים. קשה לזכור את כל סיסמאות חזקות וייחודיות אלו? אל תדאג, גם אנחנו לא יכולים. לכן מומלץ להשתמש במנהל סיסמאות, זה יישום מיוחד עבור הטלפון החכם או מחשב שלך שיכולים לאחסן בצורה מאובטחת את כל הסיסמאות שלך בצורה מוצפנת.

על ידי ביצוע ארבעת שלבים עיקריים אלו, תוכל לקדם בהרבה ולהגן על עצמך תוך מינוף הטכנולוגיה העדכנית ביותר.

לבסוף, אחד הצעדים החשובים ביותר שאתה יכול לנקוט כדי להגן על כל חשבון הוא לאפשר אימות דו-שלבי. סיסמאות לבד כבר לא מספיק כדי להגן על חשבונות, כולנו צריכים משהו חזק יותר. אימות בשני שלבים הוא הרבה יותר חזק. הוא משתמש בסיסמא, אך גם מוסיפה שלב שני, או משהו שאתה (ביומטריה), או משהו שיש לך (כגון קוד שנשלח הטלפון החכם או אפליקציה בטלפון החכם שלך שמיוצרת את הקוד בשבילך). הפעל אפשרות זו על כל חשבון שניתן, כולל במידת האפשר לאפליקציה לניהול הסיסמאות. אימות בשני שלבים הוא כנראה הצעד הבודד החשוב ביותר שאתה יכול לנקוט כדי להגן על עצמך וזה הרבה יותר קל ממה שאתה חושב.

3. **עדכונים**: ודא שהמחשבים שלך, מכשירים ניידים, אפליקציות וכל דבר אחר המחובר לאינטרנט מריץ את הגירסה האחרונה של התוכנה. פושעי סייבר מחפשים כל הזמן נקודות תורפה חדשות בתוכנה להשתמש בהתקנים שלך. כשהם מגלים פגיעויות, הם משתמשים בתוכנות מיוחדות כדי לנצל אותן ולפרוץ את המכשירים שאתה משתמש. בינתיים, החברות שיצרו את התוכנה למכשירים אלו עומלים קשה לתקן את הפגיעויות על ידי שחרור עדכונים. על ידי הקפדה להתקין עדכונים אלה על המחשבים והמכשירים הניידים, אתה מקשה בהרבה עבור מישהו לפרוץ למכשיריך. כדי להישאר מעודכנים, צריך פשוט לאפשר את תכונת העדכונים האוטומטיים בכל הזדמנות אפשרית.

© SANS Institute 2016

ארבעה שלבים להשאר בטוח

כלל זה חל על כמעט כל טכנולוגיה מחוברת לרשת, כולל טלוויזיה מחוברת לאינטרנט, צגים להשגחה לתינוקות, נתבים ביתיים, קונסולות משחק או ביום מן הימים אולי אפילו המכונית שלך. אם מערכות ההפעלה או המכשירים שלך ישנים וכבר לא נתמכים עם עדכוני אבטחה, אנו ממליצים לך להחליף אותם בחדשים ונתמכים.

4. **גיבויים**: לפעמים, לא משנה כמה זהיר אתה, אתה עשוי להיפרץ. במקרה כזה, לעתים קרובות האפשרות היחידה שלך כדי לוודא שהמחשב שלך או המכשיר נייד נקי מתוכנות זדוניות הוא למחוק אותו לחלוטין ולבנות אותו מחדש מאפס. התוקף עלול גם למנוע ממך גישה לקבצים האישיים שלך, תמונות ומידע נוסף המאוחסן על המערכת הפרוצה. במקרים רבים, הדרך היחידה להחזיר את כל המידע האישי שלך היא מגיבוי. ודא שאתה מבצע גיבויים סדירים של כל מידע, חשוב לוודא שאתה יכול גם לשחזר מהם. רוב מערכות ההפעלה למכשירים ניידים תומכות בגיבויים אוטומטיים. בנוסף, אנו ממליצים לך לשמור את הגיבויים בענן או בהעתק לא מקוון כדי להגן עליהם מפני תוקפי סייבר.

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
מנהלי סיסמאות:	https://securingthehuman.sans.org/ouch/2015#october2015
טיפי אבטחה יומיים:	https://securingthehuman.sans.org/ouch/2015#september2015
משפטי הזדהות:	https://securingthehuman.sans.org/ouch/2015#april2015
גיבויים:	https://securingthehuman.sans.org/ouch/2015#august2015

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