SANS SECURITY AWARENESS
שירותי בנק אוטומטיים בע"מ
מרכז סליקה בנקאי בע"מ
אאוץ! | ינואר 2018
עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

## בגיליון זה...

- הרשת האלחוטית שלך
- המכשירים שלך
- סיסמאות
- גיבויים

# יצירת בית מוגן סייבר

## סקירה כללית

לפני מספר שנים יצירת בית מוגן סייבר היה פשוט, ברוב הבתים היה רשת אלחוטית וכמה מחשבים. היום הטכנולוגיה הפכה מורכבת יותר והיא משולבת כחלק מהחיים שלנו, החל מהתקנים ניידים כגון קונסולת המשחקים, תרמוסטט הדוד ואולי אפילו המקרר שלך. להלן ארבעה שלבים פשוטים ליצירת בית מאובטח.

**עורך אורח**

מאט ברומיילי הוא מגיב לאירועי סייבר, הוא מסייע ללקוחות קטנים וגדולים להתמודד עם פרצות אבטחה וזליגת מידע. הוא גם מדריך SANS, ומלמד קורס FOR508, חקירות דיגיטליות ותגובה לאירועים. עקבו אחריו ב- @mbromileyDFIR.

## הרשת האלחוטית שלך

כמעט כל רשת ביתית מתחילה ברשת אלחוטית (Wi-Fi). זה מה שמאפשר לכל המכשירים שלך להתחבר לאינטרנט. רוב הרשתות האלחוטיות הביתיות נשלטות על-ידי נתב האינטרנט או נקודת גישה אלחוטית ייעודית נפרדת. שניהם פועלים באותו אופן על ידי שידור אותות אלחוטיים, ההתקנים בבית שלך מתחברים באמצעות אותות אלה. משמעות הדבר היא שאבטחת הרשת האלחוטית שלך היא חלק מרכזי בהגנה על הבית שלך. אנו ממליצים על השלבים הבאים כדי לאבטח את הרשת.

- שנה את סיסמת מנהל המערכת (Admin) המוגדרת כברירת מחדל לנתב האינטרנט או לנקודת הגישה האלחוטית. חשבון הניהול הוא מה שמאפשר לך להגדיר את ההגדרות הרשת האלחוטית.
- ודא שרק אנשים שאתה בוטח בהם יכולים להתחבר לרשת האלחוטית. בצע זאת על ידי הפעלת אבטחה חזקה. כיום, האפשרות הטובה ביותר היא להשתמש במנגנון האבטחה הנקרא WPA2. על ידי הפעלת אפשרות זו, נדרשת סיסמה כדי שאנשים יוכלו להתחבר לרשת הביתית שלך, ולאחר החיבור הראשוני, הפעילות המקוונת מוצפנת.
- ודא שהסיסמה המשמשת לחיבור לרשת האלחוטית שלך היא סיסמה חזקה ושהיא שונה מהסיסמה של מנהל המערכת. זכור, עליך להזין את הסיסמה פעם אחת בלבד עבור כל אחד מהמכשירים שלך, שכן הם שומרים את הסיסמה וזוכרים אותה.

# יצירת בית מוגן סייבר

- רשתות אלחוטיות רבות תומכות במה שמכונה "רשת אורח". זה מאפשר למבקרים להתחבר לאינטרנט, אבל מגן על הרשת הביתית שלך בכך שהם לא יכולים להתחבר לאף אחד מהמכשירים האחרים ברשת הביתית שלך. אם תוסיף רשת אורחים הקפד להפעיל את WPA2 וכן סיסמה ייחודית עבור רשת זו.

*עקוב אחר ארבעה שלבים פשוטים ליצירת בית מאובטח: לאבטח את רשת האלחוטית, לאפשר עדכון אוטומטי, להשתמש בביטוי סיסמה ייחודיים ולאפשר גיבויים.*

אינך בטוח כיצד לבצע פעולות אלו? שאל את ספק האינטרנט שלך או בדוק את אתר האינטרנט שלהם, לבדוק את התיעוד המצורף לנתב האינטרנט או לנקודת הגישה האלחוטית, או לעיין באתר האינטרנט שלהם.

## המכשירים שלך

השלב הבא הוא לדעת אילו מכשירים מחוברים לרשת הביתית האלחוטית שלך ולוודא שכל המכשירים האלה מאובטחים. זה אמור להיות פשוט כאשר יש לך מחשב או שניים. עם זאת היום כמעט כל דבר יכול להתחבר לרשת הביתית שלך, כולל טלפונים חכמים, טלוויזיות, קונסולות המשחקים, צגים לתינוק, רמקולים, אפילו המכונית שלך. לאחר שזיהית את כל ההתקנים ברשת הביתית שלך, ודא שכל אחד מהם מאובטח. הדרך הטובה ביותר לעשות זאת היא להבטיח שיש לך עדכונים אוטומטיים מופעלים בכל מכשיר אפשרי. תוקפי סייבר כל הזמן מוצאים חולשות חדשות במכשירים שונים ומערכות הפעלה. על ידי הפעלת עדכונים אוטומטיים, המחשב וההתקנים שלך מפעילים תמיד את התוכנות העדכניות ביותר, מה שהופך אותם להרבה יותר קשים לפריצה.

## סיסמאות

השלב הבא הוא להשתמש בסיסמה חזקה וייחודית עבור כל אחד מהמכשירים והחשבונות המקוונים שלך. מילות המפתח כאן הם חזקות וייחודיות. נמאס לך מסיסמאות מורכבות שקשה לזכור וקשה להקליד? גם לנו. במקום זאת, השתמש במשפט-סיסמה. זהו סוג של סיסמה המשתמשת בסדרה של מילים שקל לזכור, כגון "איפה הקפה שלי?" או "ארץ נהדרת – כוכב נולד - אבודים". ככל שהמשפט שלך ארוך יותר, כך הוא חזק יותר. סיסמה ייחודית פירושה שימוש בסיסמה אחרת עבור כל מכשיר וחשבון מקוון. בדרך זו אם אחת מהסיסמאות נפגעת, כל שאר החשבונות וההתקנים שלך עדיין בטוחים. לא זוכר את כל הסיסמאות החזקות והייחודיות האלה? אל תדאג, גם אנחנו לא יכולים. לכן אנו ממליצים להשתמש במנהל סיסמאות, שהיא תוכנת אבטחה מיוחדת המאחסנת את כל הסיסמאות שלך בצורה מאובטחת.

# יצירת בית מוגן סייבר

לבסוף, הפעל אימות דו-שלבי בכל עת, במיוחד עבור החשבונות המקוונים שלך. אימות דו-שלבי הוא הרבה יותר חזק. הוא משתמש בסיסמה שלך, אך גם מוסיף שלב שני, כגון קוד שנשלח אל הטלפון החכם או יישום בטלפון החכם שיוצר את הקוד עבורך. אימות דו-שלבי הוא כנראה הצעד החשוב ביותר שניתן לנקוט כדי להגן על עצמך באינטרנט וזה הרבה יותר קל ממה שאתה חושב.

## גיבויים

לפעמים, לא משנה כמה זהיר אתה, אתה עלול להיפרץ. אם זה המקרה, לעתים קרובות הדרך היחידה שאתה יכול לשחזר את המידע האישי שלך היא לשחזר מהגיבוי. ודא שאתה עושה גיבויים קבועים של כל המידע החשוב וודא שאתה יכול לשחזר מגיבוי. רוב המכשירים הניידים תומכים בגיבויים אוטומטיים לענן. עבור המחשבים ייתכן שיהיה עליך לרכוש סוג של תוכנת גיבוי או שירות, במחיר נמוך יחסית ופשוט לשימוש.

## 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

משפטי סיסמה: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_he.pdf

מנהל הסיסמאות: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201709_he.pdf

אימות שני גורמים: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201712_he.pdf

גיבויים: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201708_he.pdf



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