אאוץ! | אוגוסט 2018

עלון מודעות אבטחת מידע למשתמשי מחשב

התקני בית חכם

מה הם מכשירי בית חכם?

באופן מסורתי, רק כמה מהמכשירים בבית שלך יכולים להתחבר לאינטרנט, כגון המחשב הנייד, הטלפון החכם או קונסולת המשחקים. עם זאת כיום, יותר ויותר מכשירים מתחברים לאינטרנט, החל בנורות שלך והרמקולים של הטלוויזיה שלך, מנ־עולים על הדלת ואפילו המכונית שלך. בקרוב, כמעט כל מכשיר בבית שלך יכול להיות מחובר לאינטרנט. התקנים מחוברים אלה נקראים לעתים קרובות בשם Internet of Things (IoT) האינטרנט של הדברים או התקני בית חכם. בעוד שהתקנים מחוברים אלה מביאים הרבה נוחות, הם גם מביאים סכנות ייחודיות.

מה הבעיה?

ככל שיותר מכשירים מחוברים לרשת של הבית שלך, יותר סיכוי שדברים ישתבשו. האקרים יכולים להשתלט על ההתקנים שלך ולתקוף אחרים, ספקים יכולים לאסוף מידע נרחב על הפעילויות שלך, או שהמכשירים שלך עלולים להפוך לנגועים ולנעול אותך מחוץ לבית. רבות מהחברות המייצרות מכשירים אלה אינן בעלות ניסיון בתחום האבטחה הקיברנטית ורואות את ההשקעה בביטחון כעלות נוספת. כתוצאה מכך, רבים מן המכשירים שאתה רוכש אין בהם או יש מעט אבטחה מובנית. לדוגמה, להתקנים מסוימים יש סיסמאות ברירת מחדל ידועות או שאינך יכול לעדכן או להגדיר אותן.

כיצד אוכל להגן על עצמי?

אז מה אתה יכול לעשות? אנחנו בהחלט רוצים שתמנף התקנים מחוברים, בבטחה ובביטחון. התקנים אלה יכולים לספק תכו־נות נהדרות שהופכות את החיים שלך לפשוטים יותר. בנוסף, ככל שהטכנולוגיה גדלה, ייתכן שאין לך ברירה אלא להשתמש במכשירים חכמים. הנה הצעדים העיקריים שאתה יכול לנקוט כדי להגן על עצמך.

חבר רק את מה שאתה צריך: הדרך הפשוטה ביותר לאבטח התקן היא לא לחבר אותו לאינטרנט. אם אינך זקוק שהמכשיר שלך יהיה מקוון, אל תחבר אותו לרשת ה- Wi-Fi שלך. האם אתה באמת צריך טוסטר ששולח לך הודעות לטלפון שלך?

דע מה חיברת: אילו מכשירים יש לך מחוברים לרשת הבית שלך? לא בטוח או לא זוכר? כבה את הרשת האלחוטית שלך וראה מה לא עובד עוד. זה לא ימצא את כל המכשירים, אבל אתה תהיה מופתע כמה מכשירים שכחת.

התמד לעדכן: בדיוק כמו המחשב והתקנים הניידים שלך, חשוב מאוד לשמור על עדכניות של כל המכשירים שלך. אם למכשיר שלך יש אפשרות לעדכן באופן אוטומטי, הפעל אותה.

סיסמאות: שנה את הסיסמאות במכשירים שלך למשפט-סיסמה ייחודי וחזק שרק אתה יודע. סביר להניח שתצטרך להזין אותם פעם אחת בלבד. לא זוכר את כל משפטי הסיסמה שלך? אל תדאג, גם אנחנו לא יכולים. שקול להשתמש במנהל סיסמאות כדי לאחסן את כולם בצורה מאובטחת.

אפשרויות פרטיות: אם ההתקן שברשותך מאפשר לך להגדיר אפשרויות פרטיות, להגביל את כמות המידע שהוא אוסף או משתף. אחת האפשרות היא פשוט להשבית כל יכולות שיתוף מידע.

ספק: קנה את המכשירים שלך מחברה שאתה מכיר וסומך עליה. חפש מוצרים התומכים באבטחה, כגון אפשרות להפעלת עדכון אוטומטי, שנוי סיסמת ברירת המחדל ולשנות את הגדרות הפרטיות.

מקשיב תמיד: אם מכשיר יכול לקבל פקודות קוליות הוא מקשיב ללא הרף. לדוגמה, מכשירי Alexa ו- Google Home יכולים להקליט שיחות רגישות. חשוב על כך כאשר אתה קובע היכן למקם את המכשירים בביתך ובדוק את אפשרויות הפרטיות.

רשת אורח. שקול לשים את המכשירים הביתיים החכמים שלך ברשת "WiFi" נפרדת, במקום ברשת ה- WiFi הראשית שבה אתה משתמש עבור המחשבים והתקנים הניידים שלך. בדרך זו אם מכשיר חכם נגוע, המחשבים או המכשירים הניידים שברשת הראשית שלך נשארים בטוחים.

אין סיבה לפחד מטכנולוגיות חדשות, אבל חשוב להבין את הסיכון שהן מציבות. על ידי נקיטת צעדים פשוטים אלה תוכל לעזור ליצור בית חכם הרבה יותר מאובטח.

עורכת אורחת

רוברט מ. לי (@RobertMLee) הוא מדריך מוסמך של SANS ומחבר הספר FOR578 – מודיעין סיכוני סייבר ו- ICS515 - הגנת מחשוב פעילה ותגובות לאירועים. רוברט הוא גם מנכ"ל ומייסד של חברת אבטחת סייבר תעשיתית Dragos.

מקורות

משפטי סיסמה: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_he.pdf

מנהלי סיסמאות: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_he.pdf

אבטחת הרשת הביתית שלך: https://www.sans.org/sites/default/files/2018-01/201801-OUCH-January-Hebrew.pdf

יצירת בית מוגן סייבר: https://www.sans.org/u/GEL