אאוץ! | מאי 2015

מרכז סליקה בנקאי בע"מ

שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע למשתמשי מחשב

OUCH!

בגיליון זה...

- האינטרנט של דברים (IOT)
- האתגרים של IOT
- להגן על התקני ה-IOT שלך

אינטרנט של דברים (IOT)

מהו האינטרנט של דברים (IOT)

עורך אורח

ג'יימס לין (@jameslyne) הוא ראש מחלקת מחקר האבטחה בחברת האבטחה Sophos. מצהיר על עצמו "חנון רציני", המומחיות הטכנית שלו משתרעת על פני מגוון של תחומי האבטחה. הוא מדריך מוסמך במכון SANS ולעתים קרובות מגיש חדשות בכנסים בתעשייה.

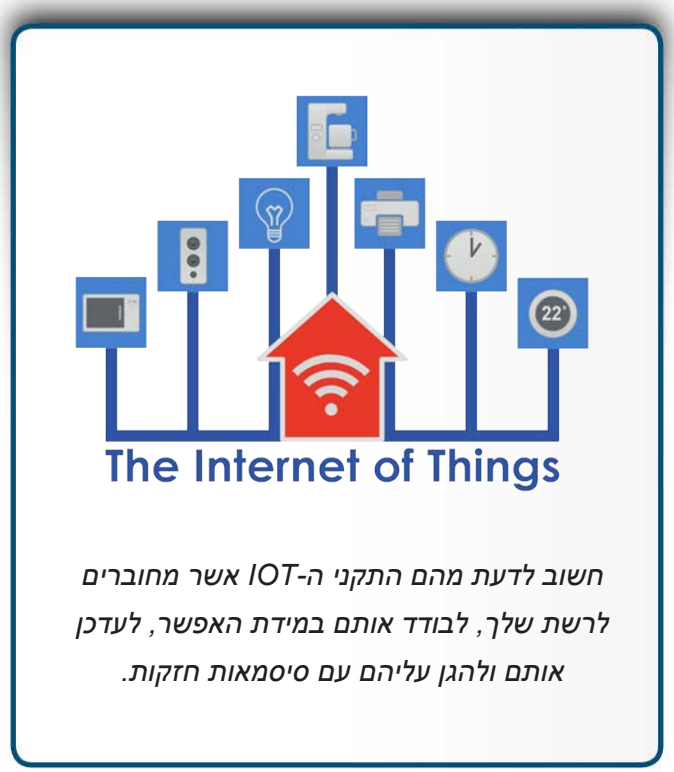
בעבר הטכנולוגיה הייתה יחסית פשוטה, אתה מחבר את המחשב לאינטרנט ומשתמש בו עבור הפעילות היומית שלך. אח"כ הטכנולוגיה התקדמה כשמכשירים ניידים נכנסו אל חיינו, מכשירים כגון טלפונים חכמים וטאבלטים. התקנים אלה שמים את הכוח של מחשבים שולחניים בכיסים שלנו. בעוד שהם הרבה יותר ניידים, מכשירים אלה הביאו בנוסף אתגרים אבטחתיים ייחודיים משלהם. עכשיו הקידום הטכני הגדול הבא הוא האינטרנט של דברים. האינטרנט של דברים, מקוצר לעתים קרובות ל-IOT (Internet Of Things), מדובר על חיבור מכשירים יומיומיים לאינטרנט, החל בפעמוני כניסה לבית, נורות חשמל, בובות צעצוע ותרמוסטטים. התקנים מחוברים אלה יכולים להפוך את חיינו להרבה יותר פשוטים - למשל להפעיל את האורות באופן אוטומטי כשטלפון מזהה שאתה מתקרב לבית. שוק ה-IOT נע בקצב מדהים עם מכשירים חדשים המופיעים מדי שבוע. עם זאת, כמו מכשירים ניידים, מכשירי IOT מגיעים עם בעיות אבטחה משלהם. בניוזלטר זה אנו נעזור להבין מהם הסיכונים ומה ניתן לעשות בכדי לאבטח את מכשירי ה-IOT, בבית שלך, ובסופו של דבר לשמור על המשפחה שלך.

בעיות עם IOT

כוחו של IOT הוא שרוב המכשירים יחסית פשוטים. לדוגמה, אתה פשוט מפעיל את מכונת הקפה שלך והיא מבקשת להתחבר לרשת Wi-Fi הביתית. לפשטות זו יש מחיר. הבעיה הכי גדולה עם התקני IOT היא שחברות רבות שמייצרות אותן הן ללא שום ניסיון עם אבטחת מידע, המומחיות שלהם היא בייצור מכשירי חשמל ביתים או אולי הם חברת הזנק המנסה לפתח מוצר בדרך היעילה והמהירה ביותר, כגון Kickstarter. ארגונים אלה מתמקדים ברווחים, לא אבטחת מידע או סייבר. כתוצאה מכך, מכשירי ה-IOT שנמכרים היום הם עם מעט או ללא אבטחה מובנית בכלל. לדוגמה, יש מספר סיסמאות ברירת המחדל אשר ידועים, אולי אפילו פורסמו באינטרנט, אשר לא ניתן לשנותם. בנוסף, למספר רב

אינטרנט של דברים (IOT)

של התקנים אין אפשרות או יכולת לשנות את ההגדרות ברירת המחדל, אתה תקוע עם מה שנשלח. כדי להחמיר את המצב, קיים קושי רב בעדכון מוצרים אלו, ואפילו חוסר היכולת להתעדכן בכלל. כתוצאה מכך, התקני IOT אשר אתה משתמש בהם עלולים להיות לא מעודכנים במהירות, עם נקודות תורפה ידועות אשר לא ניתן לתקן, מצב זה משאיר אותך פגיעה לצמיתות.



חשוב לדעת מהם התקני ה-IOT אשר מחוברים לרשת שלך, לבודד אותם במידת האפשר, לעדכן אותם ולהגן עליהם עם סיסמאות חזקות.

הגנה על התקני ה-IOT שלך

אז מה אפשר לעשות? אנחנו בהחלט רוצים לעזור לך למנף את העוצמה של מכשירי ה-IOT בצורה מאובטחת וביעילות. התקנים אלה יכולים לספק תכונות נפלאות שהופכות את החיים ליותר פשוטים, לעזור בחסכון כספי, ואולי לשפר את רמת האבטחה הפיסית של הבית שלך. בנוסף, ככל שהטכנולוגיה מתפתחת ומשתפרת אין ברירה אלא לרכוש או להשתמש במכשירי IOT. הנה כמה צעדים שניתן לנקוט כדי להגן על התקני IOT שלך ועל עצמך.

- **תחבר רק את מה שאתה צריך**: הדרך הפשוטה ביותר לאבטח מכשיר IOT היא לא לחבר אותו לאינטרנט. אם אתה לא צריך שהמכשיר יחובר לאינטרנט, פשוט לא לחבר אותו לרשת האלחוטית.
- **רשת אלחוטית נפרדת**: אם אתה צריך שהתקני ה-IOT שלך יהיו באינטרנט, שקול ליצור רשת אלחוטית נפרדת רק בשבילם. יש נתבים אשר יכולים ליצור רשתות אלחוטיות נוספות, כגון רשת אורחים. אפשרות נוספת היא לרכוש נקודת גישה לאינטרנט אלחוטית נוספת (נתב) רק עבור מכשירי ה-IOT. דבר זה שומר על התקני ה-IOT ברשת מבודדת ונפרדת, הם לא יכולים לשמש תוקף אשר רוצה לפגוע או לתקוף מחשבים והתקנים ניידים המחוברים לרשת האלחוטית הראשית שלך - הרשת הביתית (עד היום זהו תחום ההתעניינות העיקרי של פושעי סייבר).
- **עדכן במידת האפשר**: בדיוק כמו המחשבים והתקנים ניידים, חשוב לשמור על התקני IOT שלך מעודכנים. אם למכשיר ה-IOT שלך יש את האפשרות להתעדכן באופן אוטומטי, יש לאפשר זאת.

שירותי בנק אוטומטיים בע"מ

מרכז סליקה בנקאי בע"מ

אינטרנט של דברים (IOT)

- **סיסמאות חזקות**: חשוב לשנות את כל הסיסמאות במכשירי ה-IOT שלך, סיסמה ייחודית וחזקה אשר רק אתה יודע. קשה לך לזכור סיסמה ארוכה ומסובכת? אל תדאג, גם אנחנו לא יכולים. יש שקול להשתמש במנהל סיסמאות כדי לאחסן אותם בבטחה.
- **הגדרות פרטיות**: אם מכשיר ה-IOT שלך מאפשר לך להגדיר ולהגביל את הפרטיות, מומלץ להגביל את כמות המידע שהוא חולק. אפשרות אחת היא פשוט להשבית את יכולות שיתוף המידע של המכשיר.
- **שקול החלפה**: בשלב מסוים ייתכן שתרצה להחליף את מכשיר ה-IOT, כאשר למכשיר שלך יש יותר מדי נקודות תורפה ידועות שלא ניתן לתקן או שישנם מכשירים חדשים יותר עם הרבה יותר הגדרות אבטחה מובנות.

אין הגדרה אשר מתאימה לכל המכשירים, שווה לבדוק שיטות עבודה מומלצות ופרסומים על איך לאבטח את מכשירים אלו. למרבה הצער רוב מכשירי ה-IOT לא פותחו עם תודעת אבטחת סייבר, הרבה יצרנים אינם מספקים מידע על אבטחת המכשירים. אבל ככל שהמודעות לאבטחת סייבר גדלה, אנחנו מקווים לראות יותר ויותר ספקי IOT אשר מכניסים הגדרות אבטחה לתוך המכשירים שלהם ולספק לנו מידע נוסף על איך להגן ולעדכן אותם.

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 http://www.securingthehuman.org.

מקורות

סיסמאות:	https://securingthehuman.sans.org/ouch/2015#april2015
ניהול סיסמאות:	https://securingthehuman.sans.org/ouch/2015#october2015
אבטחת הטאבלט החדש שלך:	https://securingthehuman.sans.org/ouch/2016#january2016
אבטחת הרשת הביתית שלך:	https://securingthehuman.sans.org/ouch/2016#february2016

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

securingthehuman.org/blog

/securethehuman

@securethehuman

securingthehuman.org/gplus