אאוץ! | אוקטובר 2019

עלון מודעות אבטחת מידע למשתמשי מחשב

ארבע דרכים פשוטות להישאר מאובטחים

סקירה כללית

להפיק את המקסימום מהטכנולוגיה בצורה בטוחה ומאובטחת יכול להיות מכריע ומבלבל. עם זאת, ללא קשר לאיזו טכנולוגיה אתה משתמש או כיצד אתה משתמש בה, הנה ארבע דרכים פשוטות שיעזרו לך לשמור על רמת אבטחה גבוהה.

1. אתה: בראש ובראשונה, טכנולוגיה בלבד לא יכולה להגן עליך, אתה ההגנה הטובה ביותר שלך. התוקפים למדו שה־דרך הקלה ביותר להשיג את מבוקשם היא לכוון אלייך, ולא למחשב או למכשירים אחרים. אם הם רוצים את הסיסמה, כרטיס האשראי או לשלוט במחשב שלך, הם ינסו להערים עלייך בכדי שתמסור להם את המידע. לעתים קרובות על ידי יצירת תחושת דחיפות. לדוגמה, הם יכולים להתקשר אליך ולהעמיד פנים שהנציג שמשוחח אתך הוא תומך של חברת מיקרוסופט וטוען שהמחשב שלך נגוע, כאשר במציאות הוא פשוט פושע סייבר שרוצה שתתן לו גישה למחשב שלך. או שאולי הוא ישלח לך אזהרה בדוא"ל שלא ניתן למסור את החבילה שלך ועליך ללחוץ על הקישור המצורף לאשר את הכתובת שלך, כאשר במציאות הוא מרמה אותך לבקר באתר זדוני שיפרוץ למחשב שלך. בסופו של דבר, ההגנה הטובה ביותר נגד התוקף היא אתה. באמצעות השכל הישר אתה יכול לאתר ולעצור התקפות רבות.

2. משפט סיסמה: מהירויות מחשוב מודרניות הפכו את הסיסמה הישנה, בת 8 התווים, למיושנת ופגיעה. כאשר אתר מבקש מכם ליצור סיסמא, צרו במקום זאת משפט סיסמה חזק וייחודי. משפט סיסמה הוא סוג של סיסמא המשתמשת בסדרת מילים שקל לזכור, למשל "ברד ירד בדרום ספרד". ככל שמשפט הסיסמה שלך ארוך יותר, הוא חזק יותר. משפט סיסמה ייחודי פירושו להשתמש במשפט אחר לכל מכשיר או חשבון מקוון. בדרך זו אם משפט סיסמה אחד נפגע, כל החשבונות והמכשירים האחרים שלך עדיין בטוחים. לא זוכר את כל משפטי הסיסמה שלך? השתמש במנהל סיסמאות, שהיא תוכנה מיוחדת המאחסנת בצורה מאובטחת את כל משפטי הסיסמה שלך בפורמט מוצפן (והרבה תכונות נהדרות אחרות גם כן).

לבסוף, אפשר אימות דו-שלבי (נקרא גם אימות דו-גורמי או ריבוי גורמים). משתמש בסיסמה שלך, אך גם מוסיף שלב שני, כמו קוד שנשלח לסמארטפון שלך או אפליקציה שמייצרת את הקוד עבורך. אימות דו-שלבי הוא ככל הנראה הצעד החשוב ביותר שאתה יכול לנקוט כדי להגן על חשבונותיך המקוונים וזה הרבה יותר קל משאתה חושב.

3. עדכון: ודא שכל אחד מהמחשבים, המכשירים הניידים, התוכניות והאפליקציות שלך מריצים את הגרסה האחרונה הקיימת לאותו מכשיר או אפליקציה. תוקפי סייבר מחפשים כל הזמן אחר פגיעויות חדשות בתוכנות שהמכשירים שלך משתמשים. כאשר הם מגלים פגיעויות, הם משתמשים בתוכנות מיוחדות כדי לנצל את הפרצות ולפרוץ למכשירים שבהם אתה משתמש. במקביל, החברות שיצרו את התוכנה עבור מכשירים אלה עובדות קשה לתקן את הפרצות שנתגלו על ידי שחרור עדכונים. על ידי עדכון המחשבים והמכשירים הניידים שלך בעדכוני גרסה האחרונים, אתה מקשה על התוקפים להצליח לפרוץ אלייך. כדי להישאר מעודכן, פשוט אפשר עדכון אוטומטי בכל הזדמנות אפשרית. כלל זה חל כמעט על כל טכנולוגיה המחוברת לרשת, כולל טלוויזיות אשר מחוברות לאינטרנט, מוניטור תינוקות, מצלמות אבטחה, נתבים ביתיים, קונסולות משחק או אפילו המכונית שלך.

4. גיבויים ושחזור: לפעמים, לא משנה כמה אתה מקפיד, מכשירך עלולים להיפרץ. אם זה המקרה, בדרך כלל הדרך היחידה לשחזר את כל המידע האישי שלך היא מגיבוי. הקפד לבצע גיבויים קבועים של כל מידע חשוב וודא שאתה יכול לשחזר את הנתונים מהגיבוי. מרבית מערכות ההפעלה והמכשירים הניידים תומכים בגיבויים אוטומטיים, או לכוננים חיצוניים או לענן.

עורך אורח

מאט ברומיילי הוא מומחה אבטחת סייבר ותגובה לאירועים, הוא עובד עם ארגונים מכל הגדלים. בנוסף, הוא מדריך SANS אשר מלמד את קורסי התגובה לאירועי סייבר, FOR508 ו FOR572. ניתן להגיע אליו בטוויטר @mbromileyDFIR.

מקורות

הנדסה חברתית: https://www.sans.org/u/W3G
הונאות בהתאמה אישית: https://www.sans.org/u/W3Q
הפיכת סיסמאות לפשוטות: https://www.sans.org/u/W3V
קיבלתם גיבויים: https://www.sans.org/u/W40