OUCH! ספטמבר 2021

צעד אחד פשוט לאבטחת החשבונות שלך

לפעמים נדמה שלפושעי סייבר יש שרביט קסמים שבעזרתו הם יכולים להיכנס לדוא"ל שלך או חשבונות הבנק ואין שום דבר שאתה יכול לעשות כדי לעצור אותם? האם זה לא יהיה נהדר, אם היה צעד אחד שאתה יכול לנקוט והוא יעזור לך להתגונן מול הפושעים הקיברנטיים ולתת לך להשתמש בבטחה ברוב הטכנולוגיה? בעוד שאין צעד אחד שיגן מפני פושעים הסייבר, אחד השלבים החשובים ביותר שאתה יכול לעשות הוא להפעיל מנגנון שנקרא אימות שני גורמים (המכונה לפעמים 2FA, אימות דו-שלבי, או אימות רב-גורמים) על החשבונות החשובים ביותר שלך.

הבעיה עם סיסמאות

כשמדובר בהגנה על החשבונות שלך, סביר להניח שאתה כבר משתמש בסוג מסוים של סיסמה. ישנן מספר דרכים לאמת את עצמך ולהיכנס לחשבון: משהו שיש לך, משהו שאתה יודע, משהו שאתה, איפה שאתה. כאשר אתה משתמש ביותר משיטה אחת של אימות, אתה מוסיף שכבה נוספת של הגנה מפני פושעי הסייבר, גם אם הם יצליחו לפצח שיטה אחת, הם עדיין צריכים לעקוף את הגורמים הנוספים שהפעלת כדי לגשת לחשבון שלך. סיסמאות מוכיחות מי אתה על בסיס משהו שאתה יודע. הסכנה עם סיסמאות היא שהם נקודת כשל בודדת. אם פושע הסייבר יכול לנחש או לגלות את הסיסמה שלך, הוא יכול לקבל גישה לחשבונות החשובים ביותר שלך. בנוסף, פושעי סייבר מפתחים טכניקות מהירות וטובות במטרה לגלות מה הסיסמה שלך או למצוא דרך לעקוף את הסיסמה. למרבה המזל, אתה יכול להילחם בחזרה בעזרת אימות שני גורמים.

אימות שני גורמים

הוספת אימות שני גורמים הוא פתרון הרבה יותר מאשר להסתמך רק על סיסמאות. זה עובד על ידי דרישה של שתי שיטות שונות על מנת לאמת את עצמך. בדרך זו אם הסיסמה שלך נפגעת, החשבון שלך עדיין מוגן. דוגמה אחת היא כרטיס הכספומט שלך, כאשר אתה מושך כסף מהכספומט, אתה משתמש בצורה של אימות על ידי שני גורמים. כדי למשוך את הכסף שלך, תצטרך שני דברים: כרטיס כספומט שלך (משהו שיש לך) ואת מספר PIN - קוד סודי שלך (משהו שאתה מכיר). אם אתה מאבד את כרטיס כספומט שלך, מי שמוצא את הכרטיס שלך לא יכול למשוך את הכסף שלך מכיוון שהם לא יודעים את הקוד שלך. כך גם אם יש להם רק את הקוד שלך ולא את הכרטיס. תוקף חייב להחזיק גם את הכרטיס וגם לדעת את הקוד על מנת למשוך כסף בעזרת הכספומט שלך. הרעיון דומה לאימות שני גורמים; יש לך שתי שכבות של אבטחה.

שימוש באימות מקוון של שני גורמים

אימות שני גורמים הוא משהו שהגדרת בנפרד עבור כל אחד מהחשבונות שלך.
זה בעצם די פשוט: מה שצריך לעשות הוא פשוט לקשר את הטלפון הנייד שלך עם החשבון שלך. בדרך זו כאשר אתה צריך להיכנס לחשבון שלך, אתה מתחבר עם שם משתמש וסיסמה, אבל אתה גם צריך להשתמש בקוד חד פעמי ייחודי שאתה מקבל לטלפון שלך. הרעיון הוא השילוב של הסיסמה שלך בנוסף לקוד הייחודי על מנת להיכנס. בדרך כלל, קוד ייחודי זה יישלח באמצעות הודעת טקסט למכשיר הנייד או לדוא"ל שלך. ייתכן כי לטלפון שלך יש אפליקציית אימות (כגון Google Authenticator או Microsoft Authenticator) שתיצור לך את הקוד הייחודי. במידת האפשר, אפליקציות אימות למכשיר הנייד נחשבות לאפשרות המאובטחת ביותר לקבלת הקוד הייחודי שלך.

מה מקל על התהליך שאתה בדרך כלל רק צריך לעשות את זה פעם אחת מכל מחשב או מכשיר שאתה משתמש בכדי להיכנס. עיתים קרובות, לאחר שהאתר או החשבון שלך מזהה את ההתקן שלך, לצריך רק את הסיסמה שלך כדי להתחבר. בכל פעם שאתה מנסה (או מישהו אחר מנסה) להיכנס עם החשבון שלך, ממחשב או ממכשיר אחר, הם יצטרכו להשתמש שוב באימות של שני גורמים. משמעות הדבר היא שבמידה ופושעי סייבר משיגים את הסיסמה שלך, הם עדיין לא יכולים לגשת לחשבון שלך בגלל שהם לא יכולים לגשת לקוד הייחודי.

זכור, אימות שני גורמים אינו מופעל בדרך כלל כברירת מחדל, אז תצטרך לאפשר זאת בעצמך עבור כל אחד מהחשבונות החשובים ביותר שלך, כגון בנקאות, השקעות, פרישה או דוא"ל אישי. אמנם זה אולי נראה כמו עבודה נוספת בהתחלה, לאחר שזה מוגדר זה מאוד קל לשימוש.

עורכת אורחת

לייסנדרה קאפלה יש מעל 15 שנות ניסיון בעבודה אבטחת מידע וטכנולוגיה. היא מדריכה של ארגון SANS, קורס SANS AUD507 המתמקד במדידה וניהול סיכונים. כאשר היא לא מלמדת, ליזנדרה תומכת בצוותי ניהול מנהלים בתחום אסטרטגיה,אבטחה וממשל. https://www.linkedin.com/in/lysandracapella/.

משאבים
סיסמאות: https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf
מנהלי סיסמאות: https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Hebrew.pdf

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר