OUCH! אוגוסט 2014

הניוזלטר החודשי למודעות אבטחת מידע למשתמשי המחשב

OUCH!

בגליון זה...

- הצפנה מהי?
- הצפנה באחסון
- הצפנה בתנועה

הצפנה

הצפנה מהי?

אתם עשויים לשמוע אנשים משתמשים במושג «הצפנה» ומסבירים כיצד אתם צריכים להשתמש בה כדי להגן על עצמכם ועל המידע שלכם. עם זאת, הרעיון של הצפנה עשוי להיות מבלבל. בנוסף, הצפנה לא יכולה להגן עליכם מכל דבר, יש לה את המגבלות שלה. בניוזלטר זה אנו מסבירים במושגים פשוטים ביותר מהי הצפנה, למה אתם צריכים להשתמש בה, ואיך ליישם אותה נכונה.

עורך אורח

כריסטופר קרוולי (Christopher Crowley, **+ChrisCrowley**; **@CCrowMontance**) הוא יועץ הממוקם באזור וושינגטון הבירה. הוא המרצה המוביל בקורס של SANS Mobile Device Security and Ethical Hacking (SEC575), והכותב של Incident Response Team Management (MGT535).

יש לכם כמות עצומה של מידע על המכשירים השונים שלכם כמו מידע פיננסי, תמונות, דואר אלקטרוני ומידע רפואי. אם אחד המכשירים שלכם ייגנב או יאבד, כל המידע המאוד רגיש הזה עלול להיות נגיש ע»י מי שיחזיק במכשיר שלכם. בנוסף, אתם עשויים לבצע פעילויות רגישות מקוונות כגון פעולות בנקאיות ורכישות אינטרנטיות. אם תוקף סייבר יינטר את הפעילויות המקוונות שלכם, הוא יוכל לגנוב את המידע שלכם, כמו פרטי חשבון הבנק או מספר כרטיס האשראי. הצפנה מגנה עליכם ממצבים כאלו על ידי מניעת גישת לא מורשים למידע שלכם.

כאשר מידע אינו מוצפן, הוא נקרא מידע גלוי. המשמעות היא שכל אחד יכול בקלות לקרוא או לגשת אליו. הצפנה ממירה את המידע למצב לא קריא הנקרא מידע מוצפן. הצפנה עובדת על ידי ביצוע פעולות מתמטיות מסובכות ועל ידי מפתח ייחודי שממיר את המידע שלכם למידע מוצפן. המפתח הוא מה שנועל או לא נועל את המידע שלכם, בדיוק כמו שמפתח נועל ופותח דלת. דוגמא נפוצה למפתח היא סיסמה, רק אנשים שיודעים את הסיסמה יכולים לפתוח ולגשת למידע מוצפן. כדי להגן על המידע המוצפן שלכם אתם צריכים להגן על המפתח שלכם. באופן כללי הצפנה עובדת בשתי דרכים, ניתן להצפין מידע מאוחסן (כמו המידע האגור במחשב הנייד שלכם) ומידע בשינוע (כמו שידור מידע בצורה מקוונת).

הצפנה באחסון

המטרה הראשית של הצפנה מידע מאוחסן הוא הגנה על המידע במקרה שהמחשב שלכם או המכשיר הנייד שלכם אובד או נגנב. לפני 15 שנים לא היה בכך עניין מאחר שמרבית המחשבים היו מחשבים שולחניים גדולים ומגושמים

הצפנה

הצפנה היא דרך רבת עוצמה לאבטח את המידע שלכם, אך היא חזקה כחוזק המפתח.

שהיה מאוד קשה להזיז אותם. היום מחשבים ניידים רבים שוקלים מעט יותר מקילוגרם אחד בעוד מכשירים ניידים שוקלים מספר עשרות גרמים בודדים. מכשירים אלו הם מאוד חזקים ומחזיקים כמות עצומה של מידע, אך גם קל מאוד לאבד אותם. בנוסף, מדיה ניידת נוספת יכולה להחזיק מידע רגיש כמו רכיבי זכרון על USB (דיסק און קי) או CD. טכניקה נפוצה להצפנת מדיות כאלו היא הצפנת דיסק מלאה (Full Disk Encryption) המשמעות היא שהכל מוצפן אוטומטית ואתם לא צריכים להחליט מה מוצפן ומה לא. מרבית מערכות ההפעלה של ימינו מכילות הצפנת דיסק מלאה, פשוט צריך להפעיל יכולת זו. לדוגמא, ב Mac OS X יש את FileVault וחלק מגרסאות חלונות מכילות את Bitlocker. אם המחשב שלכם תומך בהצפנת דיסק מלאה, אנו ממליצים בחום לאפשר זאת. בנוסף, מרבית הטלפונים הניידים תומכים בהצפנת דיסק מלאה לאמצעי אחסון המידע הפנימי שלהם. לדוגמא iOS, מערכת ההפעלה למכשירי iPhone ו iPad אוטומטית מפעילה הצפנת דיסק מלאה ברגע שקובעים סיסמת פתיחה. על מנת ללמוד אם המחשב או המכשיר הנייד שלכם במקום העבודה תומך בהצפנת דיסק מלאה, פנו למוקד התמיכה. למחשב האישי שלכם, פנו ליצרן המחשב שלכם או בדקו באינטרנט.

הצפנה בתנועה

מידע הוא פגיע גם כשהוא בתנועה. אם המידע אינו מוצפן, הוא עשוי להיות מנוטר ונגיש באופן מקוון. לכן אתם מעוניינים לוודא כי כל פעילות מקוונת רגישה, כמו בנקאות מקוונת, שליחת דואר אלקטרוני ואולי אפילו גישה לרשתות חברתיות היא מוצפנת. הצורה הנפוצה ביותר של הצפנה מקוונת היא HTTPS. המשמעות של זה היא שכל תעבורה בין הדפדפן שלכם לבין אתר אינטרנט היא מוצפנת. חפשו את הכיתוב https:// בכתובת האתר, מנעול בדפדפן או ששורת הכתובת נצבעת בירוק. כל אלו הם סימנים לכך שהתקשורת מוצפנת. אופן הצגת ההצפנה תלוי בדפדפן שלכם והאתר שאתם ניגשים אליו. כמו כן אתם עשויים לראות את כל שלושת הסימנים בעת ובעונה אחת. בנוסף, בכל פעם שאתם מתחברים לרשת אלחוטית ציבורית, וודאו שאתם משתמשים בהצפנה כשזה אפשרי. לבסוף, כאשר שולחים ומקבלים דואר אלקטרוני וודאו שתוכנת הדואר אלקטרוני מוגדרת לעבוד בצורה מוצפנת. מרבית תוכנות הדואר האלקטרוני תומכות בהצפנה ובנוסף ספק האינטרנט שלכם יוכל לסייע לכם בהגדרת תוכנת הדואר לעבודה מוצפנת.

הצפנה

יישום נכון של הצפנה

ללא קשר באיזו הצפנה אתם משתמשים וכיצד אתם משתמשים בה, כמעט לכל צורות ההצפנה יש מאפיינים משותפים:

- ההצפנה חזקה כחוזק המפתח. אם מישהו מנחש או משיג את המפתח שלכם, תהיה לו גישה למידע שלכם. אתם צריכים להגן על המפתח שלכם.
- אם אתם משתמשים בקוד או בסיסמה למפתח שלכם, וודאו שזוהי סיסמה ארוכה ומאובטחת ואל תשכחו או תאבדו אותה. אם אתם שוכחים אותה, תמנע מכם הגישה למידע שלכם.
- ההצפנה שלכם חזקה כמו רמת האבטחה של המחשב שלכם. אם פרצו למחשב שלכם או שהוא נפגע מפוגען, תוקפי סייבר יכולים לעקוף את ההצפנה שלכם. לכן, אנא הקפידו לשמור את המחשב או המכשיר הנייד שלכם מאובטחים.
- אם אתם יכולים לבחור בין צורות הצפנה שונות, תמיד בחרו בצורה החזקה ביותר.

למדו עוד

הרשמו ל OUCH! הניוזלטר החודשי למודעות אבטחת מידע, גשו לארכיון OUCH!, בקרו אותנו ב http://www.securingthehuman.org ולמדו עוד על פתרונות מודעות אבטחת מידע של SANS.

מקורות

Mac OS X FileVault: http://support.apple.com/kb/ht4790

iOS encryption: http://support.apple.com/kb/ht4175

Android encryption: http://www.androidauthority.com/how-to-encrypt-android-device-326700/

Windows Encryption: http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

Securing Your Computer: http://www.securingthehuman.org/ouch/2012#december2012

Password Managers: http://www.securingthehuman.org/ouch/2013#october2013

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
צוות העורכים: ביל ווימן, וולט סקריבנס, פיל הופמן, בוב רודיס.