OUCH!

בגיליון זה...

- מהי הצפנה?
- מה ניתן להצפין?
- הדרך הנכונה להצפין

הצפנה

מהי הצפנה?

שמעת בוודאי שמשתמשים במונח "הצפנה" ושעלייך להשתמש בה על מנת להגן על עצמך ועל המידע שלך. עם זאת, הצפנה יכולה להיות מבלבלת ועלייך להבין את המגבלות שלה. בעלון זה נסביר במונחים פשוטים מה היא הצפנה, איך היא מגנה עלינו וכיצד ליישם אותה כמו שצריך.

עורך אורח

פרנצ'סקה בוסקו (@francibosco) היא חוקרת ומנהלת פרויקטים, פרויקטים הקשורים לפשעי סייבר, אבטחת סייבר ושימוש לרעה בטכנולוגיה. היא עובדת באו"ם במכון הבינלאומי לחקר משפט וצדק. וממייסדי המרכז לטכנולוגיה משפט (Tech and Law Center).

יש לך כמות עצומה של מידע רגיש על המכשירים שלך, כגון מסמכים אישיים, תמונות, ודואר אלקטרוני. אם אחד המכשירים שלך נאבד או נגנב, כל המידע הרגיש שלך יכול להגיע לידיים הלא נכונות. בנוסף, יכול להיות שאתה מנהל עסקות רגישות באינטרנט, כגון בנקאות או רכישה. אם מישהו היה מנטר פעילויות אלו, הוא עלול לגנוב את המידע שלך, כגון מספרי חשבון או כרטיס אשראי. הצפנה מגנה עליך במצבים אלה בכך שהיא מסייעת להבטיח שלאנשים לא מורשים אין אפשרות לגשת או לשנות את המידע שלך.

ההצפנה קיימת כבר אלפי שנים. כיום, הצפנה הרבה יותר מתוחכמת, אבל משרתת את אותה מטרה - להעביר מסר סודי ממקום אחד למשנהו על ידי הבטחה שרק המורשים לקרוא את ההודעה יוכלו לגשת אליה. כאשר המידע אינו מוצפן, זה נקרא טקסט רגיל (Plain-Text). זה אומר שמישהו יכול לקרוא או לגשת אל המידע בקלות. הצפנה ממירה את המידע הזה לטקסט מוצפן (cipher-text), פורמט זה אינו קריא. ההצפנה של היום פועלת באמצעות פעולות מתמטיות מורכבות ומפתח ייחודי להמרת המידע לתוך טקסט מוצפן. המפתח הוא מה שנועל או פותח את המידע שלך. ברוב המקרים, המפתח הוא סיסמה או קוד גישה.

מה אתה יכול להצפין?

באופן כללי יש שני סוגים של נתונים אשר ניתנים להצפנה, נתונים במנוחה (כגון נתונים המאוחסנים במכשיר הנייד שלך) ונתונים בתנועה (כגון שליחה וקבלה של דוא"ל או שליחת הודעה לחבר).

הצפנה

הצפנת נתונים במנוחה חיונית על מנת להגן על המידע במקרה שהמחשב או המכשיר הנייד שלך אבד או נגנב. המכשירים של ימינו חזקים מאוד ומחזיקים כמות עצומה של מידע, אבל גם נאבדים בקלות רבה. בנוסף, ישנם סוגים נוספים של מדיות ניידות אשר יכולים להחזיק מידע רגיש, כגון כוננים ניידים מסוג USB או כוננים קשיחים חיצוניים. הצפנת דיסק מלאה (FDE) היא טכניקת הצפנה בשימוש נרחב אשר מצפינה את הכונן כולו במערכת שלך. משמעות הדבר היא כי כל המידע הקיים במערכת מוצפן באופן אוטומטי, אתה לא צריך להחליט מה להצפין ומה לא. כיום, רוב המחשבים מגיעים עם FDE, אבל ייתכן שיהיה צורך להפעיל אותו באופן ידני. במחשבי Mac אופציית ההצפנה נקראת FileVault ובמחשבי Windows, בהתאם לגרסה, ניתן להצפין בעזרת Bitlocker. רוב המכשירים הניידים תומכים גם בהצפנת דיסק מלאה (FDE), במכשירי iPhone ו-iPad ההצפנה נעשית באופן אוטומטי כאשר הוגדרה סיסמא למכשיר. החל מאנדרואיד 6.0 (מרשמלו), גוגל מפעילה הצפנת דיסק מלאה כברירת מחדל, בתנאי שחומרת המכשיר עומדת בסטנדרטים מינימאליים מסוימים.

הצפנה היא דרך רבת עוצמה המסייעת באבטחת המידע שלך, אבל היא חזקה רק עם מפתח חזק.

מידע גם פגיע בזמן תנועה. אם הנתונים אינם מוצפנים, ניתן לנטר ולהאזין למידע ברשת. זו הסיבה שאתה רוצה להבטיח כי כל העסקות המקוונות והרגישות יהיו מוצפנות. סוג נפוץ של הצפנה באינטרנט הוא HTTPS. משמעות דבר היא כל המידע בין הדפדפן שלך לבין אתר האינטרנט מוצפן. חפש https בשורת הכתובת בדפדפן או את סמל המנעול ליד שורת הכתובת, כמו כן ניתן לראות כי ההתחלה של שורת כתובת האתר מופיעה בצבע ירוק. דוגמא נוספת היא כאשר אתה שולח או מקבל דוא"ל, רוב שירותי הדוא"ל מספקים יכולות הצפנה, ייתכן כי עליך להפעילם באופן ידני. דוגמה שלישית של הצפנת נתונים בתנועה היא בין שני משתמשים אשר מתכתבים אחד עם השני, לדוגמא WhatsApp, Wickr , iMessage או Telegram. אפליקציות מסוג זה משתמשות בהצפנה מקצה לקצה אשר מונעות שימוש במידע על ידי גורם צד שלישי. משמעות הדבר היא שרק אתה והאדם שאתה מתקשר עימו יכולים לקרוא מה שנשלח.

הצפנה

הדרך הנכונה להצפין

בכדי להיות בטוח שאתה מוגן בעת השימוש בהצפנה, יש חשיבות עליונה לשימוש נכון בהצפנה.

- ההצפנה שלך תהיה חזקה רק אם המפתח שלך יהיה חזק. אם מישהו ינחש או יקבל גישה למפתח שלך, תהיה לו גישה לנתונים שלך. יש להגן על המפתח שלך. אם אתה משתמש בקוד סודי או בסיסמה עבור המפתח שלך, יש לוודא שזו סיסמה חזקה וייחודית. ככל שהסיסמה ארוכה יותר, כך יהיה קשה יותר לתוקף לנחש או לנסות לפצח אותה. אל תשכח את הסיסמה שלך, ללא המפתח שלך אתה לא תוכל לפענח את המידע שלך. אם אתה לא יכול לזכור את כל הסיסמאות שלך אנו ממליצים על שימוש במנהל סיסמאות.
- ההצפנה שלך חזקה כמו האבטחה של המכשיר שלך. אם המכשיר שלך נפרץ או נגוע על ידי תוכנות זדוניים, האקרים יכולים לעקוף את ההצפנה שלך. זו הסיבה מדוע זה כל כך חשוב לנקוט בצעדים אחרים בכדי להגן על המכשיר שלך, כולל שימוש באנטי וירוס, סיסמאות חזקות ושמירה על מערכת הפעלה מעודכנת.
- כיום אפליקציות ותוכנות מחשב מציעות הצפנה חזקה בכדי להגן על הנתונים ועל התקשורת שלך. אם האפליקציה או תוכנת המחשב שאתה שוקל להשתמש אינה תומכת בהצפנה, יש לשקול חלופה.

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 securingthehuman.sans.org/ouch/archives.

מקורות

הצפנה סבירה:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
סיסמאות:	https://securingthehuman.sans.org/ouch/2015#april2015
ניהול סיסמאות:	https://securingthehuman.sans.org/ouch/2015#october2015
מהי תוכנה זדונית:	https://securingthehuman.sans.org/ouch/2016#march2016
אבטחת מחשב הלוח החדש שלך:	https://securingthehuman.sans.org/ouch/2016#january2016

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Securing The Human, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה ouch@securingthehuman.org.

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

securingthehuman.sans.org/gplus @securethehuman /securethehuman securingthehuman.sans.org/blog