אאוץ! | נובמבר 2018

SANS SECURITY AWARENESS

עלון מודעות אבטחת מידע למשתמשי מחשב

האם נפרצתי?

סקירה כללית

לא משנה כמה אתה בטוח, בדיוק כמו נהיגה במכונית במוקדם או במאוחר אתה עלול להיות מעורב בתאונה. להלן מספר רמזים שיעזרו לך להבין אם נפרצת אם כן, מה ניתן לעשות. ככל שתקדים לזהות שמשהו רע התרחש, כך סביר יותר שתוכל לתקן את הבעיה.

רמזים על כך שכבר נפרצת

- תוכנית האנטי וירוס שלך יוצרת התראה שהמערכת נגועה. ודא שזה האנטי וירוס שלך שמייצר את התראה, ולא חלון קופץ מאתר אינטרנט המנסה לשטות בך להתקשר או להתקין משהו אחר. אם אתה לא בטוח, פתח את תוכנית האנטי וירוס שלך ישירות.
- מופיע לך חלון קופץ שאומר שהמחשב שלך מוצפן ואתה צריך לשלם כופר כדי לקבל את הקבצים בחזרה.
- הדפדפן שלך מוביל אותך לכל מיני אתרים שלא רצית להגיע אליהם.
- המחשב או היישומים שלך מתרסקים ללא הרף, קיימים צלמיות עבור אפליקציות לא ידועות או חלונות מוזרים שצצים.
- הסיסמה שלך אינה פועלת עוד, למרות שאתה יודע שהסיסמה שלך נכונה.
- חברים שואלים אותך מדוע אתה שולח להם ספאם בדוא"ל שאתה יודע שמעולם לא שלחת.
- יש חיובים בכרטיס האשראי או משיכות מחשבון הבנק שלך שמעולם לא ביצעת.

כיצד להגיב

אם אתה חושד שנפרצת ככל שתפעל מהר יותר עדיף. אם הפריצה קשורה לעבודה, אל תנסה לתקן את הבעיה בעצמך, יש לדווח על כך מיד. אם זוהי מערכת אישית או חשבון שנפרץ, הנה כמה צעדים שתוכל לנקוט:

שנה את הסיסמאות שלך: זה כולל לשנות לא רק את הסיסמאות במחשבים ובניידים, אלא גם עבור החשבונות המקוונים שלך. אל תשתמש במחשב הפרוץ כדי לשנות את הסיסמאות שלך, השתמש במערכת אחרת שידוע לך כי היא מאובטחת. אם יש לך הרבה חשבונות להתחיל עם החשובים ביותר קודם. לא יכול לעקוב אחר כל הסיסמאות שלך? השתמש במנהל סיסמאות.

פיננסי: עבור בעיות עם כרטיס האשראי שלך או חשבונות פיננסיים, התקשר לבנק או לחברת האשראי שלך מיד. התקשר למספר טלפון מהימן, כגון מהחלק האחורי של הכרטיס הבנקאי שלך, הדוחות הכספיים שלך או בקר באתר שלהם ממחשב מהימן. בנוסף, שקול להקפיא את כרטיס האשראי שלך.

אנטי וירוס. אם תוכנת האנטי וירוס שלך מודיעה לך על קובץ נגוע, בצע את הפעולות שהוא ממליץ. לרוב תוכנות אנטי וירוס יהיו קישורים אשר תוכל לגשת כדי ללמוד עוד על הזיהום הספציפי.

התקנה מחדש. אם אין באפשרותך לתקן מחשב נגוע או שברצונך להיות יותר בטוח שהמערכת שלך בטוחה, התקן מחדש את מערכת ההפעלה. אין להתקין מחדש מתוך גיבויים, בגיבויים צריך להשתמש רק עבור שחזור הקבצים האישיים שלך. אם אתה מרגיש לא נוח לבנות מחדש, שקול להשתמש בשירות מקצועי כדי לעזור לך. לחלופין, אם המחשב או המכשיר שלך ישנים, ייתכן שיהיה קל יותר לרכוש מחשב חדש. לבסוף, ברגע שיש לך מחשב חדש או משוחזר, וודא שהוא מעודכן ואפשר עדכונים אוטומטיים בכל הזדמנות אפשרית.

גיבויים. צעד חשוב בהגנה על עצמך הוא להכין מראש גיבויים מסודרים. פתרונות רבים יגבו באופן אוטומטי את הקבצים שלך מדי יום או אפילו מדי שעה. לא משנה איזה פתרון גיבוי אתה משתמש, יש לבדוק מעת לעת כי אתה מסוגל לשחזר את הקבצים האלה. לעתים קרובות שחזור נתונים שלך מגיבויים היא הדרך היחידה שאתה יכול להתאושש מאירוע פריצה.

אכיפת החוק: אם אתה מרגיש באיום כלשהו, דווח על האירוע לאכיפת החוק המקומית. אם אתה קורבן של גניבת זהות ומתגורר בארצות הברית, בקר https://www.identitytheft.gov.

עורך אורח

ד"ר יוהנס אולריך (@johullrich)הוא דיקן המחקר של המכון SANS לטכנולוגיית, מנהל SANS Internet Storm Center ועמית SANS. הוא יצר את רשת החיישנים שיתופית DShield ומארח את פודקסט אבטחת מידע היומי ("StormCast") Daily Information Security Podcast.

מקורות

גיבויים: https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_he.pdf
משפטי סיסמה: https://www.sans.org/u/JGU
מנהלי סיסמאות: https://www.sans.org/u/JGZ
מהי תוכנה זדונית: https://www.sans.org/u/JH4
הקפאת אשראי: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Security Awareness, 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 www.sans.org/security-awareness/ouch-newsletter. עורכי המערכת: וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי | תורגם על ידי: גדי מרגלית ודרור ענבר