אאוץ! | אוגוסט 2019

עלון מודעות אבטחת מידע למשתמשי מחשב

יש גיבויים?

סקירה כללית

אם אתה משתמש במחשב או בהתקן נייד לאורך מספיק זמן, במוקדם או במאוחר משהו ישתבש. ייתכן שתמחק בטעות את הקבצים הלא נכונים, תקלה בחומרה או איבוד המכשיר. גרוע מכך, תוכנות זדוניות כגון תוכנת כופר עשויה למחוק את הקבצים שלך ו / או להחזיק אותם בשבי. בזמנים כאלה, גיבויים הם בדרך כלל הדרך היחידה שבה אתה יכול לבנות מחדש את החיים הדיגיטליים שלך.

מה, מתי וכיצד

גיבויים הם עותקים של המידע המאוחסן במקום אחר מאשר במחשב או בהתקן הנייד. כאשר אתה מאבד נתונים בעלי ערך, תוכל לשחזר את הנתונים שלך מגיבויים. הצעד הראשון הוא להחליט מה אתה רוצה לגבות, אילו נתונים ספציפיים שחשובים לך או לגבות הכל, כולל מערכת ההפעלה. פתרונות גיבוי רבים מוגדרים בברירת מחדל לגבות, תיקיות נפוצות וחשובות. אם אתה לא בטוח איזה גיבוי לבצע או שאתה רוצה להיות זהיר במיוחד, תגבה את הכל.

צעד שני, להחליט באיזו תדירות לגבות. תוכניות גיבוי מובנות כגון "מכונת הזמן של אפל" או "גיבוי ושחזור של חלונות" מאפשרות לך ליצור לוח זמנים אוטומטי "הגדר ושכח". האפשרויות הנפוצות כוללות שעתי, יומי, שבועי וכו' פתרונות אחרים מציעים "הגנה מתמשכת" שבו קבצים חדשים או שינוי בקבצים קיימים מגובים באופן מיידי בכל פעם שאתה שומר מסמך. לכל הפחות, אנו ממליצים על גיבוי יומי אוטומטי של קבצים קריטיים.

לבסוף, עלייך להחליט איך אתה הולך לגבות. ישנן שתי דרכים: אחסון מקומי או אחסון בענן. גיבויים מקומיים מסתמכים על מכשירים שאתה שולט בהם, כגון כונני USB חיצוניים או התקני רשת. היתרון של כוננים מקומיים הוא שהם מאפשרים לך לגבות ולשחזר כמויות גדולות של נתונים במהירות ובזמן קצר. החיסרון הוא שאם אתה נגוע בתוכנות זדוניות, כגון תוכנת כופר, אפשרי שהזיהום יתפשט לגיבויים שלך. בנוסף, אם יש לך אסון, כגון אש או גניבה, זה יכול לגרום לך לאבד לא רק את המחשב, אלא גם את הגיבויים. אם אתה משתמש בהתקנים חיצוניים לגיבויים, אחסן עותק מחוץ לאתר במיקום מאובטח וודא שהגיבויים שלך מסומנים כהלכה.

פתרונות מבוססי ענן הם שירותים מקוונים שמאחסנים את הקבצים שלך באינטרנט. בדרך כלל, אתה מתקין יישום במחשב שלך, היישום באופן אוטומטי מגבה את הקבצים שלך לפי לוח זמנים או לפי איך שאתה תקבע. היתרון של פתרונות ענן היא הפשטות שלהם, הגיבויים הם לעתים קרובות אוטומטיים ואתה יכול בדרך כלל לגשת לקבצים שלך מכל מקום. כמו כן, משום שהנתונים שלך נמצאים בענן, אסונות בבית כגון אש או גניבה לא ישפיע על הגיבויים. לבסוף, גיבויים של ענן יכולים לסייע לך להתאושש מזיהומים של תוכנות זדוניות כגון תוכנות כופר. החסרונות הם היכולת לשחזר מהגיבוי כמות נתונים גדולה אשר תלויה במהירות הרשת שלך. לא בטוח אם אתה רוצה להשתמש בגיבוי מקומי או גיבוי מבוסס ענן? עדיף להיות בטוח ולהשתמש בשניהם.

במכשירים ניידים, רוב הנתונים שלך מאוחסנים כבר בענן. עם זאת, ייתכן שהגדרות מסוימות, תמונות אחרונות והעדפות המ־ערכת שלך לא יהיו מגובים. בגיבוי של המכשיר הנייד שלך, אתה שומר על מידע זה ובנוסף יהיה לך קל יותר להעביר את כל הנתונים בעת שדרוג למכשיר חדש.

נקודות מפתח

- **גיבוי הנתונים שלך הוא רק חצי מהדרך. אתה חייב להיות בטוח שאתה יכול גם לשחזר אותו. בדוק מעת לעת שהגיבויים שלך פועלים על-ידי שחזור ופתיחה של קבצים.**
- **במידה ותשחזר מחדש מערכת הפעלה מגיבוי, הקפד להתקין את העדכונים האחרונים ואת עדכוני האבטחה לפני שתשתמש במערכת.**
- **אם אתה משתמש בפתרון ענן, בחר פתרון שקל לך להשתמש בו, תבדוק את אפשרויות האבטחה. לדוגמה, האם הם תומכים באימות דו-שלבי כדי לאבטח את החשבון המקוון שלך.**

גיבויים הם דרך פשוטה וזולה כדי להגן על החיים הדיגיטליים שלך.

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

הפיכת סיסמאות לדבר פשוט: https://www.sans.org/u/TqR
עצור את התוכנה הזדונית: https://www.sans.org/u/TqW
יצירת בית מאובטח: https://www.sans.org/u/Tr1

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

© SANS Institute 2019