מרכז סליקה בנקאי בע"מ
שירותי בנק אוטומטיים בע"מ
SANS SECURING THE HUMAN

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- **גיבויים: מה, מתי וכיצד**
- **שחזור**
- **נקודות עיקריות**

גיבוי ושחזור

סקירה כללית

אם אתה משתמש במחשב או בהתקן נייד לאורך זמן, במו־קדם או במאוחר משהו ישתבש וכתוצאה מכך אתה עלול לאבד את הקבצים האישיים שלך, מסמכים או תמונות. לדו־גמה: ייתכן שבטעות תמחק קבצים, תחווה כשל חומרתי, איבוד ההתקן או שתידבק בתוכנות זדוניות כגון כופרה. במו־קרים כאלו, גיבויים הם בדרך כלל הדרך היחידה שבה אתה יכול לבנות מחדש את החיים הדיגיטליים שלך. בעלון זה, אנו נסביר מה הם גיבויים, כיצד לבצע גיבוי של נתוניך ולפתח אסטרטגית גיבוי המתאימה לך.

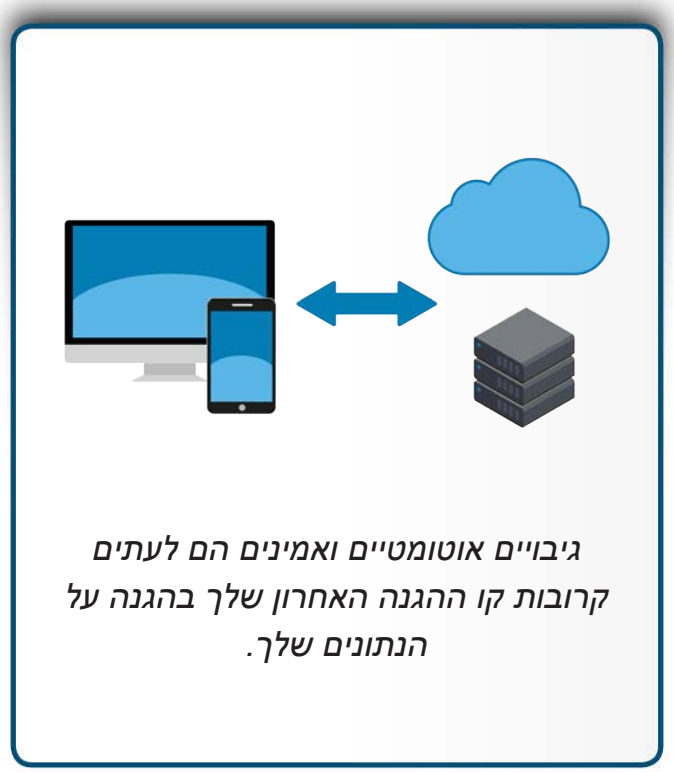
עורך אורח
קית' פלמגרין הוא מומחה בתחום אבטחת המידע בעל ניסיון של מעל 30 שנים בתחום אבטחת תשתיות. הוא מרצה בכיר של SANS ומחבר קורס SANS SEC301 "מבוא לאבטחת מידע". קית' פועל בהצלחה בייעוץ אבטחת מידע. טוויטר: **@kpalmgren**

גיבויים: מה, מתי וכיצד

גיבוי הוא עותק של המידע הדיגיטלי שלך אשר מאוחסן במקום אחר מאשר במחשב או בהתקן נייד. כאשר אתה מאבד נתונים בעלי ערך, תוכל לשחזר את הנתונים מגיבויי. למרבה הצער, יותר מדי אנשים כושלים בביצוע גיבויי באופן סדיר, למרות שהתהליך פשוט ולא יקר. הצעד הראשון הוא להחליט מה אתה רוצה לגבות. ישנן שתי גישות; לגבות רק נתונים שחשובים לך או את לגבות הכל, כולל את מערכת ההפעלה. ברירת מחדל בפתרונות גיבוי רבים היא הגישה הראשונה, גיבוי נתונים מהתיקיות הנפוצות ביותר, במקרים רבים, זה כל מה שאתה צריך. עם זאת, אם אתה לא בטוח באיזה גיבוי לבחור או שברצונך להיות זהיר במיוחד, מומלץ לגבות את הכל.

שנית, עליך להחליט באיזו תדירות יתבצע הגיבוי. תוכניות גיבוי מובנות כגון "מכונת הזמן של אפל" או "גיבוי ושחזור של Microsoft Windows" מאפשרות לך ליצור לוח זמנים אוטומטי, "שגר ושכח". האפשרויות הנפוצות כוללות גיבוי שעתי, יומי, שבועי וכו'. פתרונות אחרים מציעים "הגנה מתמשכת" שבו קבצים חדשים או קבצים ששונו מגובים באופן מיידי בכל פעם שאתה שומר מסמך. אנו ממליצים על גיבוי אוטומטי יומי לכל הפחות.

גיבוי ושחזור



גיבויים אוטומטיים ואמינים הם לעתים קרובות קו ההגנה האחרון שלך בהגנה על הנתונים שלך.

לבסוף, אתה צריך להחליט איך תגבה. קיימות שתי דרכים לגיבוי הנתונים: מדיה פיזית או אחסון מבוסס ענן. לכל גישה יש יתרונות וחסרונות. אם אינך בטוח באיזו שיטה להשתמש אתה יכול להשתמש בשתיהם בו זמנית. מדיה פיזית הם התקנים שברשותך, כגון כונני USB חיצוניים או כונני רשת. היתרון בשימוש במדיה הפיזית הוא שמדיה זו מאפשרת לך לגבות ולשחזר כמויות גדולות של נתונים במהירות רבה. החיסרון של גישה זו הוא שבמידה ונדבקת בתוכנה זדונית, כגון תוכנת כופר, יש סיכוי שההדבקה תדביק גם את הגיבויים שלך.

חס וחלילה אם התרחש אסון, כגון שריפה או גניבה, אתה עלול לאבד לא רק את המחשב, אלא גם את הגיבויים. במידה ואתה משתמש בהתקנים חיצוניים לגיבויים, עליך לאחסן עותק של מדיית הגיבוי במקום בטוח ומרוחק. ודא שהגיבוי שאתה מאחסן באתר מרוחק מסומן כהלכה.

פתרונות מבוססי-ענן הם שירותים מקוונים שמאחסנים את הקבצים שלך באינטרנט. בדרך כלל, אתה מתקין יישום במחשב שלך. היישום מגבה באופן אוטומטי את הקבצים בזמן אמת או לפי תזמון שהגדרת מראש. היתרונות של פתרונות ענן הם הפשטות שלהם, הגיבויים מתבצעים בדרך כלל אוטומטית ואתה יכול לגשת לקבצים שלך מכל מקום. כמו כן, בגלל שהנתונים שלך נמצאים בענן, אסונות בבית כגון אש או גניבה לא ישפיעו על הגיבוי והמידע שלך. לבסוף, גיבויים מבוססי ענן יכולים לסייע לך להתאושש מהדבקות של תוכנות זדוניות כגון תוכנות כופר, מכיוון שרוב פתרונות מבוססי הענן מאפשרים לך לשחזר מגרסאות ישנות של הקבצים שלך. החיסרונות של גיבוי בענן הן שיכול לקחת זמן רב כדי לגבות או לשחזר כמויות גדולות מאוד של נתונים. כמו כן, הפרטיות והאבטחה חשובים. האם שירות הגיבוי מספק אמצעי אבטחה חזקים כגון הצפנת הנתונים ואימות דו-שלבי?

לבסוף, אל תשכח את המכשירים הניידים שלך. במכשירים ניידים, רוב הנתונים שלך, כגון דוא"ל, אירועי יומן ואנשי קשר, כבר מאוחסנים בענן. עם זאת, ייתכן שהגדרות שונות של הנייד, תמונות אחרונות והעדפות המערכת לא יאוחסנו בענן. בעת גיבוי של המכשיר הנייד, אתה שומר על כל המידע, ובנוסף קל יותר להעביר את הנתונים שלך בעת שדרוג למכשיר חדש. אייפון או אייפד יכולים לבצע גיבוי אוטומטי בענן של אפל. מכשירי אנדרואיד או מכשירים ניידים אחרים תלויים ביצרן או בשירות המפעיל. במקרים מסוימים, ייתכן שיהיה עליך לרכוש אפליקציה לנייד שתוכננה במיוחד עבור גיבויים.

גיבוי ושחזור

שחזור

גיבוי נתונים זו רק חצי הדרך, אתה חייב להיות בטוח שאתה מסוגל לשחזר את המידע. בדוק מעת לעת שהגיבויים שלך פועלים על-ידי אחזור קובץ ווידוא שהוא זהה למקור. כמו כן, הקפד לבצע גיבוי מערכת מלא לפני שדרוג גדול (כגון מעבר למחשב חדש או התקנה חדשה) או תיקון גדול (כגון החלפת כונן קשיח) וודא שהגיבוי ניתן לשחזור.

נקודות עיקריות

- ללא קשר לפתרון שבו אתה משתמש לגיבוי הנתונים, ודא שהגיבוי מתבצע באופן אוטומטי, כמו כן יש לבדוק אותם מעת לעת.
- בעת שחזור מערכת מגיבוי, הקפד, לפני המשך שימוש, להתקין מחדש את עדכוני מערכת ההפעלה ואת עדכוני האבטחה.
- גיבויים מיושנים שאינם נחוצים עוד הם נטל ויש להשמיד אותם כדי למנוע גישה של אנשים לא מורשים.
- אם אתה משתמש בפתרון ענן, בדוק את המדיניות ואת המוניטין של הספק וודא שהם עומדים בדרישות שלך. לדוגמה, האם הם מצפינים את הנתונים שלך? האם הם תומכים באימות חזק כגון אימות דו-שלבי?

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

משפטי סיסמה:	https://securingthehuman.sans.org/ouch/2017#april2017
אימות דו-שלבי:	https://securingthehuman.sans.org/ouch asked#september2015
אבטחת ענן:	https://securingthehuman.sans.org/ouch/2016#november2016
הצפנה:	https://securingthehuman.sans.org/ouch/2016#june2016
תוכנות כופר:	https://securingthehuman.sans.org/ouch/2016#august2016

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


securingthehuman.sans.org/blog


/securethehuman


@securethehuman


securingthehuman.sans.org/gplus