نشرتك الشهريه للتوعية بأمن المعومات

هل لديك نسخه احتياطية لبياناتك؟

نظرة عامة

إذا كنت تستخدم جهاز كمبيوتر أو جهاز محمول لفترة، عاجلاً أم آجلاً سيحدث خطأ ما. فمن الممكن أن تحذف ملفاتك بالخطأ أو يحدث خلل بالجهاز يسبب فقد البيانات. وفي أسوء الاحتمالات البرمجيات الخبيثة مثل برمجية الفدية ransom ware قد تحذف ملفاتك أو تقوم بتشفيرهم. ومن هنا تكون النسخ الاحتياطية للبيانات هي الطريقة الوحيدة لاستعادة حياتك الرقمية.

لماذا ومتي وكيف؟

النسخ الاحتياطية هي نُسخ من معلوماتك المخزنة في مكان آخر بخلاف الكمبيوتر أو الجهاز المحمول. عندما تفقد بيانات ذات قيمة، يمكنك استرداد بياناتك من النسخ الاحتياطية. الخطوة الأولى: هي تحديد ما تريد نسخه احتياطيًا.1.بيانات محددة مهمة بالنسبة لك2.كل شيء، بما في ذلك نظام التشغيل بأكمله. يتم تكوين العديد من حلول النسخ الاحتياطي بشكل افتراضي لاستخدام الطريقة الأولى، فهي تقوم بعمل نسخ احتياطي للمجلدات الأكثر استخدامًا. إذا لم تكن متأكدًا مما تريد نسخه احتياطيًا أو تريد أن تكون دقيقًا، فقم بنسخ كل شيء احتياطيًا. الخطوة الثانية: قرر عدد مرات النسخ الاحتياطي.

تتيح لك برامج النسخ الاحتياطي المضمنة مثل Apple Time Machine أو Windows Backup and Restore إعدادات افتراضية للخيارات الأكثر شيوعاً وتشمل خيارات للنسخ كل ساعة أو يوميًا أو أسبوعيًا، إلخ. كما توجد حلول لعمليات النسخ الاحتياطي تضمن نسخ الملفات الجديدة أو المعدلة بشكل فوري، وهنا فإننا نوصي على الأقل بعملية النسخ الاحتياطي التلقائي يوميا للملفات المهمة.

هناك طريقتان: التخزين المحلي والتخزين السحابي (علي الانترنت). ففي طريقة التخزين المحلية للنسخ الاحتياطية تعتمد على الأجهزة التي تتحكم فيها مثل محركات أقراص USB الخارجية أو أجهزة شبكة Wi-Fi التي يمكن الوصول إليها. مميزات التخزين المحلي للنسخ الاحتياطية هي أنها تمكنك من النسخ الاحتياطي واستعادة كميات كبيرة من البيانات بسرعة. المشاكل التي قد تواجهك في استخدام التخزين المحلي هو إذا أصبحت مصابًا ببرامج ضارة، مثل برمجية الفدية» ransom ware "، فمن الممكن أن تنتشر العدوى إلى نُسخك الاحتياطية. أيضًا إذا كنت تعاني من كارثة، مثل الحريق أو السرقة، فقد يؤدي ذلك إلى فقدان الكمبيوتر وأيضًا النسخ الاحتياطية. إذا كنت تستخدم أجهزة خارجية للنسخ الاحتياطية، فقم بتخزين نسخة خارج الموقع في مكان آمن وتأكد من تسمية النسخ الاحتياطية بشكل صحيح.

أما طريقة التخزين السحابي للنسخ الاحتياطية فهي تقوم بتخزين ملفاتك على الإنترنت. عادةً ما تقوم بتثبيت تطبيق على جهاز الكمبيوتر الخاص بك، ثم يقوم التطبيق تلقائيًا بأخذ نسخة احتياطية من ملفاتك إما وفق جدول زمني محدد أو عند تعديلها. تتمثل ميزة الحلول السحابية في بساطتها، وغالبًا ما تكون النسخ الاحتياطية تلقائية ويمكنك عادة الوصول إلى ملفاتك من أي مكان. أيضًا، نظرًا لأن بياناتك موجودة في السحابة، فلن تؤثر الكوارث المنزلية، مثل الحريق أو السرقة، على النسخ الاحتياطي. أخيرًا، يمكن أن تساعدك النُسخ الاحتياطية السحابية على التعافي من إصابات البرامج الضارة مثل Ransomware. العيوب التي تواجهك في التخزين السحابي للنُسخ الاحتياطية هي قدرتك على النسخ الاحتياطي والاعتماد على مقدار البيانات التي قمت بنسخها احتياطيًا وسرعة شبكتك. قد تكون متردد لاستخدام أي من الطرق السابقة لعملية النسخ الاحتياطي، يمكن استخدام الطريقتين معًا لزيادة الأمان لملفاتك.

في الأجهزة المحمولة، يتم تخزين معظم بياناتك بالفعل في السحابة. ومع ذلك، فقد لا تكون إعدادات تطبيقات المحمول والصور الحديثة وتفضيلات النظام مُدرجة بشكل سليم لذلك عليك ضبطها. من خلال عمل نسخة احتياطية لجهازك المحمول، وهذه الطريقة لا تحافظ على هذه المعلومات فحسب، بل إنه من الأسهل نقل بياناتك عند الترقية إلى جهاز جديد.

النقاط الرئيسية

- **النسخ الاحتياطي للبيانات الخاصة بك هو نصف المعركة؛ يجب أن تكون متأكدًا من أنه يمكنك استعادة نسختك الاحتياطية من خلال اختبار دوري للنُسخ الاحتياطية الخاصة بك.**
- **إذا قمت بإعادة إنشاء نظام من النسخة الاحتياطية، فتأكد من إعادة تطبيق أحدث تصحيحات الأمان والتحديثات قبل استخدامه مرة أخرى.**
- **إذا كنت تستخدم حلًا سحابيًا عبر الإنترنت، فحدد أحد الحلول التي يسهل عليك استخدامها والبحث في خيارات الأمان. على سبيل المثال، هل يدعم التحقق بخطوتين لتأمين حسابك عبر الإنترنت؟**

النسخ الاحتياطية هي طريقة بسيطة ومنخفضة التكلفة لحماية حياتك الرقمية.

الضيف المحرر

مات برومیلي Matt Bromiley يعمل في الاستجابة لحالا الطوارئ الناتجة عن الهجمات الالكترونية، حيث يتعامل مع جميع أنواع الاختراقات وتسريب البيانات. يعمل أيضا مدرس لدي SANS لدورة التحقيقات الجنائية الالكترونية المتقدمة والتصرف في حالات الطوارئ FOR508 تابع مات عبر تويتر @mbromileyDFIR.

مصادر إضافية

Making Passwords Simple: https://www.sans.org/u/TqR

Stop That Malware: https://www.sans.org/u/TqW

Creating a Cybersecure Home: https://www.sans.org/u/Tr1