آوتش! | نوفمبر ٢٠١٦

النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

- نظرة عامة
- اختيار مزود الخدمة
- تأمين بياناتك

استخدم الحوسبة السحابية بأمان

لمحة عامة

المحرر الضيف

ديف شاكيلفورد (@daveshackleford) مستشار محترف يملك شركة Voodoo Security وهو مؤلف للعديد من دورات سانس التعليمية من ضمنها SANS Security 579: Virtualization and Private Cloud Security and Security 524: Cloud Security Fundamentals.

الحوسبة السحابية، يمكن أن تعني أشياء مختلفة لأناس مختلفين، ولكن عادة ما تعني استخدام مزود خدمة على شبكة الإنترنت لتخزين وإدارة البيانات. أهم ما يميز الحوسبة السحابية هو امكانية مزامنة البيانات والوصول إليها بسهولة من أجهزة متعددة من أي مكان في العالم، ويمكنك أيضا مشاركة المعلومات الخاصة بك مع أي شخص تريد. ونحن نطلق على هذه الخدمات «السحابية» لأنك في كثير من الأحيان لا تعرف أين يتم تخزين البيانات الخاصة بك بشكل حقيقي. وتشمل الأمثلة على الحوسبة السحابية إنشاء وثائق على مستندات جوجل، وتبادل الملفات عبر دروب بوكسDropbox ، تجهيز الخادم الخاص بك على سحابة أمازون Amazon Cloud، تخزين بيانات العملاء في Salesforce أو أرشفة الملفات الصوتية أو ملفات الصور على iCloud. ويمكن لهذه الخدمات عبر الإنترنت أن تجعلك أكثر إنتاجية، ولكنها تأتي أيضا مع مخاطر عديدة. في هذه النشرة سوف نعرض كيف نستخدم الحوسبة السحابية بشكل أمن.

اختيار مزود الخدمة

الحوسبة السحابية ليست شيء سيئ أو جيد، بل هي أداة لإنجاز الأعمال، سواء في العمل أوالمنزل. ومع ذلك، عند استخدام هذه الخدمات أنت تسلم بيانات خاصة للآخرين، وتتوقع منهم تخزينها بشكل أمن وتوفيرها كلما احتجت إليها. يجب أن نقوم باختيار مزود الحوسبة السحابة بحكمة. بالنسبة لأجهزة الكمبيوتر في عملك أو المعلومات ذات الصلة بالعمل، تحقق من الإدارة المعنية في مكان عملك لمعرفة ما إذا كان يمكنك استخدام الخدمات السحابية للملفات الخاصة بالعمل، وما هي سياسات الاستخدام والقواعد الواجب اتباعها. أما إذا كنت تفكر في الخدمة السحابية للاستخدام الشخصي تأكد مما يلي:

١. **الدعم الفني**: هل من السهل الحصول على مساعدة اذا كان لديك استفسار عن الخدمة؟ هل هناك عنوان بريد إلكتروني يمكنك الاتصال به؟ أومنتديات عامة يمكنك نشر الأسئلة بها، أو أسئلة وأجوبة على موقع الخدمة على الانترنت؟.
٢. **سهولة الاستخدام**: ما مدى سهولة استخدام الخدمة؟ كلما كانت الخدمة أكثر تعقيدا، كلما زادت احتمالية حدوث اخطاء واحتمال

استخدم الحوسبة السحابية بأمان

فقدان البيانات أو كشفها. اختر خدمة سحابية سهلة في الفهم والاعداد والاستخدام.

٣. **الأمان**: ما هي البيانات التي يتم جمعها عنك، إن وجدت؟ كيفية الحصول على البيانات من جهاز الكمبيوتر الخاص بك إلى السحابة وكيف يتم تخزينها في السحابة – هل هي مشفرة؟ وإذا كان الأمر كذلك من يمكنه فك تشفير البيانات الخاصة بك؟

٤. **شروط الاستخدام**: توقف لحظة لمراجعة شروط الخدمة(من السهل قراءتها). تأكد من يمكنه الوصول إلى البيانات الخاصة بك وما هي الحقوق القانونية الخاصة بك. أخيرا، تأكد من المسؤوليات الأمنية التي يتحملها مقدم الخدمة تجاهك.

الحوسبة السحابية تمكنك من مشاركة البيانات بسهولة و تجعلك أكثر إنتاجية، ولكن كن حذراً عند مشاركة المعلومات الخاصة بك.

تأمين بياناتك

بمجرد الانتهاء من اختيار مزود خدمة جيد، فإن الخطوة التالية هي التأكد من أنك تستخدم الخدمات السحابية بشكل صحيح. ان كيفية الوصول إلى بياناتك وكيفية تبادلها، له تأثير كبير على أمن بياناتك. في ما يلي الخطوات الرئيسية التي يمكنك اتخاذها:

١. **المصادقة** : استخدم كلمة مرور قوية و فريدة من نوعها للمصادقة على حساب الخدمة السحابية الخاص بك. إذا كان خيار التحقق من خطوتين متاحا فنحن نوصي بشدة أن تقوم بتفعيله. هذه الخطوة من أهم الخطوات التي يمكنك اتخاذها لحماية حسابك.

٢. **مشاركة الملفات / المجلدات**: الحوسبة السحابية تجعل المشاركة سهلة لدرجة خطيرة. فربما وأنت تحاول مشاركة بعض الملفات الخاصة مع شخص معين، تقوم بمشاركتها مع جميع مستخدمي شبكة الإنترنت. أفضل طريقة لحماية نفسك هي عدم مشاركة أي من الملفات الخاصة بك مع أي شخص بشكل افتراضي. ثم السماح فقط لأشخاص معينين (أو مجموعة من المستخدمين) الوصول إلى ملفات أو مجلدات معينة على حسب الحاجة. قم بازالة الصلاحيات الغير ضرورية بشكل دوري. ينبغي أن يوفر مزود السحابة الخاص بك طريقة سهلة لمعرفة من يمكنه الوصول إلى الملفات والمجلدات الخاصة بك.

٣. **مشاركة الملفات / المجلدات باستخدام الروابط**: ميزة مشتركة في الخدمات السحابية هي القدرة على إنشاء رابط يشير إلى الملفات أو المجلدات الخاصة بك. هذه الميزة تسمح لك بتبادل الملفات مع أي شخص تريد ببساطة عن طريق توفير رابط. ولكن هذه الطريقة غير أمنة اطلاقا، أي شخص يعرف هذا الرابط يمكنه الوصول إلى الملفات أو المجلدات الشخصية الخاصة بك. إذا قمت بإرسال الرابط لشخص واحد فقط، يمكنه أن يشارك هذا الرابط مع الآخرين أو أنها يمكن أن تظهر على محركات البحث. إذا كنت مضطراً

استخدم الحوسبة السحابية بأمان

لتبادل البيانات باستخدام الروابط، تأكد من تعطيل الرابط اذا لم تعد هناك حاجة إليها من خلال وضع تاريخ انتهاء الصلاحية أو إذا أمكن، حماية الرابط بكلمة مرور.

٤. **الاعدادات**: فهم إعدادات الأمان التي يوفرها مزود خدمة السحابة الخاص بك. على سبيل المثال، إذا كنت تشارك مجلد مع شخص آخر، فهل يستطيع مشاركة البيانات الخاصة بك مع الآخرين دون علمك؟. انظر أيضا إذا كانت هناك طرق لمعرفة من الذي شاهد مجلدات المشاركة الخاصة بك، وهل يمكنك تقييد المشاركة»للقراءة فقط» مقابل منح «قراءة + كتابة» وهو ما يعني إمكانية تعديل الملفات؟

٥. **مضاد الفيروسات**: تأكد من تثبيت أحدث إصدار من برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك وعلى أي كمبيوتر آخر يستخدم لتبادل البيانات الخاصة بك. في حالة إصابة ملف وهو في جهاز معين' فعند نقله للسحابة، يمكن بسببه أن يصاب أي جهاز آخر عند محاولة الوصول إليه.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة securingthehuman.sans.org/ouch/archives.

النسخة العربية

تتم ترجمة هذه النشرة شهريا من قبل مجموعة من الأساتذة و المتخصصين في أمن المعلومات.

مصادر إضافية

عدد أوتش حول التحقق باستخدام خطوتين:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_aa.pdf
عدد أوتش حول عبارات المرور:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_aa.pdf
عدد أوتش حول مدير كلمات المرور (باللغة الإنجليزية):	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_en.pdf
عدد أوتش حول ما هي البرمجيات الخبيثة:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf
دورة من سانس عن اساسيات أمن الحوسبة السحابية(باللغة الإنجليزية):	https://sans.org/sec524

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي، شيريل كونلي
ترجمها إلى العربية: طلال موسى الخروبي، محمد سرور