النشرة الشهرية حول الوعي الأمني لمستخدمي الحاسب الآلي

OUCH!

في هذا العدد..

تم اختراق أحد أجهزتي، ماذا افعل؟

لمحة عامة

نحن نعلم بأنك تهتم بحماية أجهزتك وهواتفك المحمولة وتتخذ الخطوات اللازمة لضمان ذلك. ولكن، مهما كان استخدامك الآمن للتقنية، عاجلاً أم آجلاً قد تتعرض أحد أجهزتك للاختراق. سنعرض في هذا العدد كيف تعرف إذا كان جهازك أو هاتفك المحمول قد تعرض للاختراق، وكيف تتعامل مع ذلك. وبالتأكيد، بقدر سرعتك في ملاحظة هذا الاختراق والتعامل معه بشكل سريع، بقدر ما تقلل حجم الضرر الذي قد يسببه.

المحرر الضيف

سامانثا دافيسون (@sam_e_davison) هي مديرة برنامج التعليم والتوعية الأمنية بشركة أوبر، تشرف على توعية موظفي الشركة في أكثر من ٣٥٠ مدينة حول العالم.

دلائل على حدوث الاختراق

ربما يكون من الصعب أن تعرف إذا ما كان جهازك أو هاتفك المحمول قد تعرض للاختراق، لعدم وجود طريقة واحدة لمعرفة ذلك. عند حدوث اختراق عادة ماتكون هناك عدد من الدلائل أو المؤشرات. وبحسب ظهور هذه المؤشرات تزيداحتمالية أن جهازك قد تم اختراقه.

- برنامج مكافحة الفيروسات لديك يُظهر بشكل متكرر العديد من التنبيهات بأن نظامك مصاب بفايروس، وأنه غير قادر على حذف الفايروس أو عزل الملفات المصابة.
- الصفحة الرئيسية للمتصفح تغيرت بشكل مفاجئ، أو أن المتصفح ينقلك لمواقع لم تطلبها.
- وجود مستخدمين جدد على جهازك لم تضفهم مسبقًا، أو برامج جديدة على جهازك لم تقم بتثبيتها.
- جهازك أو بعض التطبيقات المثبتة عليه تتوقف عن العمل بشكل متكرر، وكذلك وجود أيقونات لتطبيقات مجهولة أو ظهور نوافذ منبثقة بشكل غريب.
- تطبيق يطلب إذنك في إجراء تعديلات في النظام، على الرغم من عدم تحديث أو تثبيت أي تطبيقات.
- كلمة المرور لا تعمل لديك عندما تحاول الدخول على نظامك أو أحد حساباتك عبر الانترنت، على الرغم من تأكدك من صحة كلمة المرور.
- يسألك أصدقاءك عن سبب إرسالك رسائل بريد إلكترونية مزعجة لم ترسلها مطلقًا.
- هاتفك المحمول يرسل رسائل قصيرة SMS لخدمات مدفوعة بدون إذنك.

تم اختراق أحد أجهزتي، ماذا افعل؟

- هاتفك المحمول يستهلك كمية كبيرة من البيانات أو البطارية بشكل مفاجئ.

كيف تتصرف عند حدوث اختراق

إذا إكتشفت أن جهازك أو هاتفك المحمول قد تعرض للاختراق، فعليك التصرف بسرعة، فبقدر سرعتك في التعامل معه، بقدر ما تقلل حجم الضرر الذي قد يسببه. إذا كان الجهاز الذي تم اختراقه يخص جهة عملك، لا تحاول حل المشكلة بنفسك. فقد يسبب ذلك أضرارا أكثر من النفع، كما يمكن أن تفقد بعض الأدلة القيمة التي يمكن استخدامها للتحقيق في ما حدث. عوضاً عن ذلك، تواصل مباشرة بمكتب الدعم الفني في جهة عملك وأبلغهم بما حدث. إذا لم تتمكن من الاتصال بمكتب الدعم الفني، أو كنت تشعر بالقلق إزاء أي تأخير في التصرف، عليك بفصل الجهاز عن الشبكة ومن ثم وضعه في حالة نوم أو تعليق أو وضع الطائرة. حتى إذا لم تكن متأكداً من حدوث الاختراق، فمن الأفضل أن تقوم بإبلاغ مكتب الدعم الفني للتحقق من ذلك. إذا كان الجهاز الذي تم اختراقه يخصك، أدناه بعض الخطوات التي يمكن القيام بها.

عاجلا أم آجلا هناك احتمال لحصول اختراق لاحد أجهزتك. إذا إكتشفت حدوث الاختراق، فعليك التصرف بسرعة، فبقدر سرعتك في التعامل معه، بقدر ما تقلل حجم الضرر الذي قد يسببه.

- تغيير كلمات المرور: وهذا يشمل ليس فقط تغيير كلمات المرور على أجهزة الكمبيوتر والأجهزة النقالة، ولكن لجميع حساباتك على الانترنت. تأكد من أنك لا تستخدم الجهاز المخترق لتغيير كلمات المرور. أستخدم جهاز آمن للقيام بذلك
- برنامج مكافحة الفيروسات. إذا كان برنامج مكافحة الفيروسات قد وجد ملفا مصابا، فيمكنك اتباع الإجراءات التي يوصي بها هذا البرنامج. هذه الوصايا عادة ما تتضمن عزل الملف، أو إزالة الفيروس منه أو حذف الملف. معظم برامج مكافحة الفيروسات توفر معلومات إضافية حول الفيروسات التي يتم اكتشافها، ننصحك بقرائة هذه المعلومات لمعرفة المزيد عن الاختراق الذي حصل. إذا لم يتمكن برنامج مكافحة الفيروسات من إزالة الفيروس أو عزل الملف فننصحك بحذف الملف المصاب.
- إعادة بناء النظام. إذا كنت غير قادر على اصلاح جهازك او اردت التأكد من ان النظام امن تماما. الخيار الاكثر امانا هو اعادة بناء النظام. بالنسبة لأجهزة الكمبيوتر اتبع تعليمات الشركة المصنعة الخاصة بك. في معظم الحالات هذا يعني استخدام الادوات المساعدة المدمجة في اعادة تثبيت نظام التشغيل. إذا كانت هذه الادوات مفقودة او تالفة او مصابة قم بالاتصال بالشركة المنتجة لجهازك او قم بزيارة موقعها على الانترنت. لا تقم بإعادة تثبيت نظام التشغيل من النسخة الاحتياطية قد يكون بها نفس نقاط الضعف التي من خلالها تم اختراق جهازك. النسخة الاحتياطية تستخدم فقط لاستعادة البيانات الخاصة بك. بالنسبة للهاتف المحمول اتبع تعليمات الشركة المصنعة للجهاز. معظم منتجي الأجهزة يقومون

تم اختراق أحد أجهزتي، ماذا افعل؟

بتوفير هذه المعلومات على موقع الانترنت الخاص بهم. في كثير من الأحيان يمكن استخدام خيار «اعادة ضبط المصنع» من بين خيارات الضبط لهاتفك المحمول. إذا لم تكن لديك الخبرة الكافية لاعادة بناء النظام، نوصي بالاستعانة بشخص متخصص. إذا كان جهازك او هاتفك قديم، قد يكون من الأفضل (وأحياناً أقل كلفة) أن تقوم بشراء جهاز جديد. اخيرا، إذا عملت على اعادة بناء النظام على الجهاز المخترق او قمت بشراء جهاز جديد تأكد من تحديث نظام التشغيل وجميع التطبيقات التي قمت بتثبيتها واجعل التحديث يعمل بشكل تلقائي كلما كان ذلك ممكناً.

- النسخ الاحتياطي. من اهم الخطوات التي يمكنك اتخاذها لحماية بياناتك في حال حدوث اختراق هو القيام بالنسخ الاحتياطي المنتظم. كلما قمت بذلك بشكل أكبر كلما كان ذلك أفضل. بعض تطبيقات النسخ الاحتياطي تتيح لك القيام بعملية النسخ الاحتياطي بشكل تلقائي للملفات كل ساعة. بغض النظر عن أي من تطبيقات النسخ الاحتياطي تقوم باستخدامه عليك التأكد بشكل دوري من إنك قادر على استعادة هذه الملفات. عليك تجربة استعادة البيانات من النسخة الاحتياطية من حين لآخر.
- إبلاغ الجهات المختصة. إذا تعرضت لأي تهديد باي شكل من الاشكال. عليك إبلاغ الجهات المختصة في بلدك.

إعرف أكثر

أوتش الشهرية! نشرة توعوية بالأمن المعلوماتي. للاشتراك والوصول إلى الأعداد السابقة ولمعرفة المزيد حول "سانس" نأمل زيارة

http://www.securingthehuman.org.

النسخة العربية

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

مصادر إضافية

عدد أوتش حول النسخ الاحتياطي واستعادة البيانات:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_aa.pdf
عدد أوتش حول عبارات المرور:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_aa.pdf
عدد أوتش حول ما هي البرمجيات الخبيثة:	http://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_aa.pdf
عدد أوتش حول تأمين الجهاز اللوحي الجديد (باللغة الانجليزية):	https://securingthehuman.sans.org/ouch/2016#january2016

مجلس التحرير: بيل وايمان، والت سكريفن، فيل هوفمان، لانس سبيتسر، كارمن رويل هاردي
ترجمها إلى العربية: طلال موسى الخروبي، فرج أحمد عز الدين, محمد سرور، زياد الشهري.