نشرتك الشهريه للتوعية بأمن المعومات

هل أنا مُخترق؟

نظره عامه

مهما كنت تعتبر نفسك آمنا، فإنك وكما الحال في سواقة السيارة معرض عاجلا أم آجلا للحوادث. نسرد فيما يلي دلائلاً ومؤشرات تساعدك لتعرف ما إذا تم تعرضك لاختراق وما الذي يتعين عليك فعله لو حصل. فكلما أسرعت في تحديد وتشخيص حالة الاختراق، زادت حظوظك في إصلاح المشكلة وتقليل الأضرار.

دلائل ومؤشرات الاختراق

- قيام برنامج فحص الفيروسات لديك بإعطاء تنبيهات بإصابة الجهاز. عليك ان تنتبه من أن هذا التنبيه تم إصداره من برنامج الحماية لديك وليس عبر صفحة او نافذة منبثقة خداعة في صفحات الويب عبر المتصفح والتي تهدف لاستدراجك وتخويفك لتقوم بتحميل برامج ضارة يقترحونها عليك. وان لم تكن متأكدًا اذهب الى سجلات برنامج الحماية لديك وراجع منها التنويهات الأمنية.
- انبثاق نوافذ تخبرك بأن الملفات على حاسوبك ستشفر او تم تشفيرها ولمنع ذلك يتعين عليك دفع الفدية لاسترجاعها.
- يأخذك المتصفح للكثير من المواقع التي لا ترغب بالوصول اليها.
- انهيار لنظام التشغيل او التطبيقات بشكل متكرر إضافة لظهور أيقونات لتطبيقات غريبة ونوافذ غريبة تنبثق بلا سبب.
- كلمات المرور لحساباتك لم تعد تعمل بالرغم من تأكدك من صحتها.
- يتصل بك اصدقاؤك متعجبين من رسائل الكترونية غير مرغوبه تصلهم من بريدك الخاص لم تكن فعلا قد قمت بإرسالها.
- حصول سحوبات نقدية من حساباتك البنكية من خلال بطاقات الائتمان البنكية لم تقم بها ابداً.

كيف ستتصرف؟

عندما تشك بحصول الاختراق فإنك كلما اسرعت بالتصرف كلما كان أفضل. وان كان هذا الاختراق لأجهزة او حسابات متعلقة بالعمل فمن الأفضل ألا تقوم بالإصلاح بنفسك بل قم بتبليغ الجهات المسؤولة في العمل. أما إن كان الاختراق حاصلا لحساباتك أو أجهزتك الشخصية فإليك بعض الخطوات التي يمكنك القيام بها:

قم بتغيير كلمات المرور: وهذا لا يقتصر على حسابات الدخول الى الجهاز أو الموبايل فقط بل على كل الحسابات المستخدمة في تطبيقات الويب المختلفة. ولا تقم بتغيير كلمات المرور من نفس الجهاز المخترق بل قم بذلك من جهاز مختلف تكون متأكدا من سلامته وأمانه. وان كان لديك الكثير من الحسابات فابدأ بالأهم أولاً. ولا ننصح باستخدام نفس كلمه المرور لكل الحسابات وإن لم تستطع تعقب كلمات المرور المختلفة يمكنك استخدام برامج إدارة لكلمات المرور.

الحسابات المالية: للأمور المتعلقة ببطاقات الائتمان قم فورا بالاتصال بالبنك والابلاغ. اتصل بأرقام البنك الموثوقة للتبليغ أو قم بزيارة موقع البنك على الانترنت من جهاز موثوق، مع الاخذ بعين الاعتبار طلب توقيف او تجميد البطاقة.

برنامج الحماية من الفيروسات: في حال إبلاغك عن وجود فيروسات من خلال برنامج الحماية لديك فإنه يتعين عليك اتباع تعليمات وتوجيهات برنامج الحماية، أغلب برمجيات الحماية ستعطيك روابط وأدوات تساعدك في معالجة الفيروسات.

إعادة التنصيب أو التهيئة: ان لم يكن هناك وسيله لتنظيف العدوي أو الفايروس فقد يلزمك حينها إعادة التهيئة والتنصيب لنظام التشغيل. ولا نقم باسترجاع نظام التشغيل من النسخ الاحتياطية، استخدمها لاسترجاع ملفاتك الشخصية فقط. وان كنت غير مرتاحاً لإعادة التهيئة لخشيتك فقد تطبيقات حساسة أو نادرة مثلاً يمكن مراجعه الخبراء للمساعدة. أيضا ان كان جهازك قديماً فقد يكون أجدى لك شراء جهاز جديد. أخيراً، بمجرد إعادة التهيئة أو حتى شراء جهاز جديد فانت مطالب بالتأكد من حصول نظام التشغيل على آخر التحديثات الأمنية مع تفعيل التحديث الاوتوماتيكي ما أمكن.

النسخ الاحتياطي: أحد الامور الهامة لحماية نفسك وعالمك الرقمي هو استباق الأحداث بأخذ نسخ احتياطية من البيانات بشكل دوري ومنتظم. هناك الكثير من الحلول البرمجية والتي يمكنها تأمين نسخ احتياطيه من البيانات وبشكل اوتوماتيكي بصوره يوميه او حتى كل ساعة. وبغض النظر عن البرنامج المستخدم عليك التأكد وبصورة منتظمة إمكانية استرجاع الملفات بشكل سليم. غالباً النسخ الاحتياطية للبيانات هي ملاذك الوحيد لاستعاده الملفات الضائعة سواء بالاختراق او التشفير.

التدخل القضائي: إذا شعرت بأي شكل من التهديدات، فأبلغ الشرطة المحلية عن الحادث. إذا كنت ضحية «سرقة الهوية» راجع اقرب مركز للشرطة الخاص ببلدك.

الضيف المحرر

الدكتور جوهانس اولرتش(@johullrich)كبير الباحثين في معهد SANS للتقنية، ومدير برنامج Internet Storm SANS Center و SANS Fellow. هو من انشأ منظومهsensor DShield collaborative التعاونية لتحليل سجلات الجدار الناري Firewall لدراسة وتحليل وسلوك الهجمات. كما أنه يستضيف البث اليومي لنشرة أخبار أمن الشبكات في مركز Internet Storm.

مصادر إضافية

النسخ الاحتياطي(اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_aa.pdf

عبارات المرور(اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_aa.pdf

تطبيقات إدارة كلمات المرور(اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_aa.pdf

ما هي البرمجيات الخبيثة (اللغة العربية): https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201603_aa.pdf