

في مجال الأمن السيبراني الموجودة على الأرجح على الجانب الآخر من العالم

كاتب صحفي ومدير النشر للجريدة الإلكترونية حقيقة نيوز. نت



عبدالحق خرباش، 28/12/2022.

هل يأخذ مجرمو الانترنت إجازة خلال موسم الأعياد؟
يعتقد الكثير من الناس أن المتسللين، مثل أي شخص آخر، يأخذون
استراحة خلال موسم الأعياد. ولكن في الواقع، تجري الأمور بالعكس حيث
يقضي مجرمو الانترنت ساعات إضافية أونلاين خلال العطلات في محاولة
لتنفيذ هجماتهم لأنهم يعلمون أن الشركات والأفراد غالباً ما يتخلون
عن حذرهم الأمني الإلكتروني في هذا الوقت من السنة.
ومن المرجح أن تنجح الهجمات لأن معظم الموظفين يتركون العمل لقضاء
المزيد من الوقت مع أسرهم. في الولايات المتحدة الأميركية على سبيل
المثال، أصدر مكتب التحقيقات الفيدرالي تذكيراً إلى مؤسسات
البنية التحتية الحيوية يطلب منهم البقاء متيقظين لصد أي تهديدات
خلال موسم الأعياد وعطلات نهاية الأسبوع. ويعتبر هذا أيضاً تنبيهاً
للأفراد والشركات الصغيرة والمتوسطة لضرورة تحسين إجراءات الأمن
السيبراني الخاصة بهم.

وذكرت الأجهزة الحكومية الجميع بالهجمات المتعددة التي حدثت خلال
هذه السنة. واعتبرت أن الجهات الفاعلة في مجال الأمن السيبراني
الموجودة على الأرجح على الجانب الآخر من العالم، ستبحث بنشاط عن
طرق لتعطيل الشبكات والأنظمة الهامة المرتبطة بالبنية التحتية.
يعرف المتسللون أن العديد من الموظفين سيكونون بعيدين عن العمل
أو سيعودون إلى المنزل للاستمتاع مع العائلة وبأجواء الاحتفالات،

وهذا هو بالضبط الوقت الذي قد يهاجمون فيه .
يجب أن يكون كل من الأفراد والمؤسسات في حالة تأهب دائم للتمكن من
صد التهديدات المحتملة ، بكافة أنواعها ، أبرزها هجمات برامج
الفدية . ففي وقت سابق من هذا العام ، هاجم المتسللون بنجاح العديد
من المؤسسات في أيام العطل مثل 4 يوليو وعيد الأم . ولن يكون من
المستغرب أن يقوم المتسللون بتنفيذ الهجوم يوم عيد الميلاد أو رأس
السنة الميلادية على سبيل المثال .
لا يحب مجرمو الانترنت مهاجمة الأهداف الصعبة ، فينتظرون بصبر تخليكم
عن حذركم . وبالتالي ، وقت توقف الموظفين عن العمل خلال موسم العطلات
هو فرصة مثالية لمجرمي الإنترنت لتنفيذ هجماتهم باعتبار أنهم
سيواجهون مقاومة أقل .
في سياق متصل ، تُعتبر نهاية العام فترة مرهقة للعديد من
الموظفين . ومن المرجح أن يفتح الأشخاص المشتتون رسائل البريد
الإلكتروني المخادعة ، فيقومون عن غير قصد بالنقر على الروابط التي
ليس من المفترض أن يفتحوها .
لذلك ننصحكم بضمن حماية أجهزكم من الفيروسات وعمليات التصيد
الاحتيالي والمواقع المخادعة والعملات المشفرة وغيره ، من خلال تثبيت
برنامج خاص بمكافحة الفيروسات ذات السمعة الطيبة . ومن الأفضل شراء
النسخة المدفوعة منه للحصول على أكبر قدر من الحماية السيبرانية
المتوفرة .

