فريق التحرير | نشر في ١٠ أكتوبر ٢٠١٦,

لماذا لا يستعمل أحد أهم خبراء أمن المعلومات الهواتف الذكية؟

”لن أستخدم هاتفًا ذكيًا، وقبل هذا، أنا استخدام هاتفًا محمولًا أساسيًا من طراز ما قبل الهاتف الذكي بوظائفه التي تقتصر على إجراء واستقبال المكالمات والرسائل القصيرة. لا يتعلق الأمر بالمسائل الأمنية، إنني أفضل فقط الطريقة القديمة في استخدام الهواتف“.

كان هذا رد يوجين كاسبيرسكي، الرئيس التنفيذي ومؤسس شركة كاسبرسكي لاب، على سؤال في حواره مع شبكة أريبيان بزنس، والمتعلق بتفضيله إجراء معاملة تجارية بمبلغ يفوق مليون دولار من خلال حسابه المصرفي عبر الهاتف المحمول، وإذا ما كان هل سيشعر بالأمان حيال القيام بذلك أم لا؟

يرى يوجين أنه يشعر بالأمان بشكل كبير، وليس خائفًا من حدوث اختراق لجهاز الكمبيوتر الخاص بي. فهو محمي بشكل جيد (يمكنكم تخمين البرمجية الأمنية التي استخدمها هكذا قال)، كما أنه يعي تمامًا بعدم وجود حماية أمنية تصل لـ100 % سواء كنت متصلًا بشبكة الإنترنت أو غير متصل بها.

من وجهة نظر مؤسس أهم شركة أمن معلومات، بأنه يمكن أن يكون أي حساب مصرفي ضحية لإختراق ناجح، إذ يعتمد الأمر فقط على مدى الجهد والمخاطرة التي يتطلبها منفذو التهديد.

يمكن أن يكون أي حساب مصرفي ضحية لإختراق ناجح، إذ يعتمد الأمر فقط على مدى الجهد والمخاطرة التي يتطلبها منفذو التهديد

ويرى أن استخدام عدد كبير من التدابير الأمنية المختلفة، يجعل عملية التسلل معقدة جدًا ومكلفة وتستغرق وقتًا أطول، الأمر الذي يجعل المخترقين يأخذون بالحسبان السلبيات التي تفوق الإيجابيات للقيام بذلك.

"أنا شخصيا مقتنع بعدم وجود الخصوصية"

يقول يوجين كاسبيرسكي في حواره "أنا شخصيًا مقتنع بعدم وجود الخصوصية، حتى مع وجود التشفير. وإذا نظرنا إلى الوضع بشكل أكثر تفاؤلًا، فإن الخصوصية محدودة في وقتنا هذا. نحن نعيش في عصر الفضاء الإلكتروني، ومعظم بياناتنا رقمية على أجهزة الكمبيوتر والهواتف الذكية والخدمات السحابية، وتلوح دائمًا في الأفق احتمالية الكشف عن هذه البيانات أو تسريبها. فكلما زاد استخدامنا للتكنولوجيا، قلت فرص الخصوصية لدينا، إذ يتم جمع المزيد من البيانات وإطلاقها. هذا هو الواقع المرير.

أي نظام حاسوبي تقريبًا يمكن أن يعاني من نقاط ضعف من شأنها أن تعرضه لخطر الإختراق

وعن مدى فعالية النواحي الأمنية عندما يتعلق الأمر بهجمات أكثر تطورًا تستهدف محركات الأقراص الصلبة أو أنظمة التشغيل أو حتى تتنصت على شبكات الألياف البصرية يقول الرجل الذي يمتلك أقوى أحد الشركات في الأمن السيبراني: "من الصعب كشف وتحديد الهجمات المستهدفة الأكثر تطورًا من خلال التقنيات التقليدية".

وأضاف: "تتطلب الاستراتيجية المتينة للحماية الأمنية المرنة فحص النظم الأمنية القائمة، وتتطلب تحليلًا واسع النطاق للمخاطر وناقلات الهجوم المحتملة، كما ينبغي أن نصل إلى نقطة يكون فيها تطوير هدف تم الهجوم عليه أكثر تكلفة من الضرر الذي قد تسببه".

وحول سؤاله عما إذا كانت أنظمة التشغيل الحالية مثل ويندوز وأندرويد هي الأكثر عرضة للتهديدات السيبرانية، أجاب بقوله: " تظهر البرمجيات الخبيثة عندما يكون النظام مشهورًا وموثقًا ومفتوحًا بما فيه الكفاية، والعامل الرئيسي في النهاية هو المرونة، ونعني بذلك سهولة التطوير؛ والمرونة أيضًا بالنسبة للمستخدمين، كبساطة تحميل التطبيقات من أي مكان يختارونه على سبيل المثال".

معظم بياناتنا رقمية على أجهزة الكمبيوتر والهواتف الذكية والخدمات السحابية، وتلوح دائمًا في الأفق احتمالية الكشف عن هذه البيانات أو تسريبها

وأضاف: "يعد هذا أحد الأسباب التي جعلت أنظمة ويندوز وأندرويد أكثر أنظمة التشغيل عرضة للهجوم في وقتنا الحالي باعتبارهما الأكثر استخدامًا على نطاق واسع. ولكن بصفة عامة، فإنه من الجدير بالذكر أن أي نظام حاسوبي تقريبًا يمكن أن يعاني من نقاط ضعف من شأنها أن تعرضه لخطر الاختراق".

رابط المقال: https://www.noonpost.com/14427/