لهذه الأسباب يمكن اختراق البلوكشين

كتبه موقع بروفيسور | 22 يونيو ,2019

ترجمة وتحرير: نون بوست

على الرغم من أن قيود البلوكشين ثابتة وغير قابلة للتغيير، إلا أنه من الممكن اختراقها خاصة وأن كتابة الشيفرات يعدّ من صنع البشر. وفي حين يمكن أن تبلغ هذه الشيفرات المستوى المطلوب من الثقة، إلا أنه لا يمكن نتوقع ذلك من جميع البشر، لأنه في النهاية، كما كتب الكاتب المسرحي الروسي، أنطون تشيخوف: "ينبغي عليك أن تثق في الناس وتؤمن بهم، وإلا سيُصبح من الصعب العيش في الحياة".

تُعتبر الثقة أمرا لا غنى عنه في العلاقات الشخصية، غير أن إمكانية إساءة استخدامها لطالما كان مطروحا. وفي هذا الصدد، قال الرئيس السابق، رونالد ريغان، إنه ينبغي علينا اتباع قاعدة "ثق ولكن تحقق". وعند البحث في عالم مخترقي الإنترنت وأولئك الذين كانوا من ضحاياهك، أعتقد أن مجال "الثقة" هو نقطة بداية عالم الاختراق. لذلك، يعدّ منح الثقة فيمايتعلق بثبات ومعايير الأمان في البلوكشين أمرين مختلفين. وفي اعتقادي، لا يختلف هذا النظام عن بقية الكيانات القابلة للاختراق.

وفقًا لشركة كاسبرسكي لاب المختصة في أمن الحواسيب في الربع الأول من سنة 2018؛

- قامت كاسبرسكي لاب بالتصدي لحوالي 796،806،112 هجوم أطلقته الموارد المتاحة عبر الإنترنت في 194 دولة حول العالم.
- وقع تحديد 282،807،433 محدد خاص لموقع الموارد المُوحّد على أنها برمجيات خبيثة بواسطة برنامج "ويب أنتي فيروس".
- وقع تسجيل محاولات اختراق بواسطة استخدام برمجيات خبيثة مصممة خصيصا للاستيلاء على الأموال من خلال الولوج إلى الحسابات المصرفية على أجهزة الكمبيوتر التي يبلغ عدد مستخدميها 204،448 مستخدما.

> وفقًا لموقع "ستاتيستا"، وقع شحن 262.68 مليون جهاز كمبيوتر سنة 2017 بالإضافة إلى 259.39 جهاز آخر في سنة 2018

- وقع تسجيل هجمات "رانسوم وير" على أجهزة الكمبيوتر الخاصة بقرابة 179،934 مستخدمًا فريدًا.
- سجّل ملف مكافحة الفيروسات الخاص بنا 187،597،494 برنامجا خبيثًا فريدًا وربما غير مرغوب فيه.

منتجات كاسبرسكي للأجهزة المحمولة التي تم اكتشافها:

- 1،322،578 برنامج تثبيت خبيث.
- 18،912 برنامج تثبيت لشفرة حصان طروادة المصرفية عبر الهاتف المحمول.
- 8،787 برنامج تثبيت شفرة رانسوم وير حصان للأجهزة المحمولة.

في هذا المقال، سأدرس السيكولوجيا المبنيّة على "الثقة"، عوضا عن "التحقق" من وجهة نظر الشخص الذي تعرّض للاختراق. وأنا أؤكد أن هناك أربعة أسباب رئيسية تجعل الشخص عرضة للاختراق.

أسباب تعرّض الناس اختراق:

1. الإفراط في منح الثقة

وفقًا لموقع "ستاتيستا"، وقع شحن 262.68 مليون جهاز كمبيوتر سنة 2017 بالإضافة إلى 259.39 جهاز آخر في سنة 2018. علاوة على ذلك، هناك ما يقارب المليار جهاز كمبيوتر قيد

الاستخدام في جميع أنحاء العالم، حيث يشتري ملايين الأشخاص هذه الأجهزة، بنيّة توصيلها بالإنترنت وبدء العمل عليها. وبناء على تجربتي الخاصة، لاحظت أن معظم الناس يقصدون بعض المتاجر مثل "بيست باي"، دون أن تكون لديهم أي فكرة عما يبحثون عنه أو حتى ما يستطيع الكمبيوتر فعله.

> تخلّف ثقة الناس فيما يخبرهم به الباعة بالإضافة إلى ثقتهم المفرطة في قدراتهم المعرفية الخاصة لتحليل الأخبار التي يتلقّونها، كارثة تقنية حتميّة

عموما، ينطبق هذا الأمر على الناس الذين ينقادون وراء عاطفتهم بينما يتبضّعون دون تحديد ما يريدونه أو ما يحتاجون إليه أولاً. وبمجرد توصيل الجهاز بالإنترنت، يكون هؤلاء الأفراد على ثقة تامة بأن كل ما اشتروه محدّث وبالتالي هم لا يدركون خطر التعرّض للقرصنة المحيطة بهم، سواء كان ذلك من خلال البرامج التي ينزّلونها أو عبر الإنترنت كما هو موضح أعلاه.

في الواقع، تخلّف ثقة الناس فيما يخبرهم به الباعة بالإضافة إلى ثقتهم المفرطة في قدراتهم المعرفية الخاصة لتحليل الأخبار التي يتلقّونها، كارثة تقنية حتميّة. في هذا السياق، كتب عالم النفس إريك إريكسون في دوراته التدريبية الثمانية عن التنمية، أن الثقة تكون جزءا من نفسياتنا منذ الطفولة وتظل معنا حتى الكبر. لذلك، نميل إلى أن نثق بما يقال لنا، مما يتسبب في إمكانية تعرّضنا للخداع. ومما لا شك فيه، تُعتبر طبيعتنا، التي تميل إلى الإفراط في الثقة، هي السبب الأساسي وراء نجاح المخترقين في مهاجمة بياناتنا الشخصية ووجودنا الرقمي.

2. عدم التثبّت

على الرغم من سهولة التحقق من المعلومات التي يتلقاها المرء، إلا أن الكثير من الناس لا يفعلون ذلك. وعادة ما نتلقى رسائل البريد الإلكتروني التي قد تبدو موثوقة فنفتحها، كما نستقبل مكالمات هاتفية من دائرة الإيرادات الداخلية ونعتقد أنها حقيقية. كنتيجة لذلك، تتسبّب هذه العمليات والعديد غيرها في سرقة العديد من الهويات، ما ينجر عنه الكثير من الخسائر المالية.

وتجدر الإشارة مرة أخرى إلى أن ثقتنا هي التي تعترض طريق سلامتنا، إذ تكثر الوسائل الرقميّة التي يمكن أن تساعدك على معرفة مدى صحّة وشرعيّة المعلومات التي تتلقاها. في المقابل، نحن نثق في أجهزة الكمبيوتر الخاصة بنا للقيام بهذه المهمة، على الرغم من عدم معرفتنا ما إذا كان بحوزتنا برنامج إلكتروني يمكنه تقديم المساعدة.

> لا يسعني فهم كيف يقضي بعض الأشخاص الوقت في التأكد من أن صلاحيّة قسيمة السوبر ماركت لم تنقض بعد، في حين أنهم لا يستطيعون التحقق من تحديث أمن معلوماتهم الشخصية

في هذه الحالة على وجه التحديد، أعتقد أن تكنولوجيا البلوكشين يمكن أن تقدم بعض الحلول نظرا لأنها ستسمح للأفراد ببناء ملفات تعريف هوية مؤكّدة وغير قابلة للتغيير. وفي الوقت الراهن، هناك شركات على غرار "أفرنيم" غير تابعة لمبادرة البلوكشين لمدينة يوتا وإلينوي التي تعمل بالفعل في مجال تحديد البلوكشين. ومما لا شك فيه، سيستمر هذا الوضع على حاله، ولن تؤتي نتائج هذه المشاريع أكلها أو تساعد في منع القرصنة حتى يبدأ المستخدم في التحقق من المعلومات التي يتلقاها. ولا يسعني فهم كيف يقضي بعض الأشخاص الوقت في التأكد من أن صلاحيّة قسيمة السوبر ماركت لم تنقض بعد، في حين أنهم لا يستطيعون التحقق من تحديث أمن معلوماتهم الشخصية.

3. المعرفة المحدودة

وفقًا لماكافي ومركز الدراسات الاستراتيجية والدولية، تبلغ التكلفة السنوية المحتملة التي يواجهها الاقتصاد العالمي من جرائم الإنترنت 445 مليار دولار سنويًا. ويرجع جزء كبير من ذلك إلى غياب التعليم الضروري فيما يتعلق بالقرصنة والجرائم الإلكترونية وسرقة الهوية. وهناك اقتباس في هذا الشأن من جون ديوي يشير إلى أن: "التعليم ليس تحضيرا للحياة، التعليم هو الحياة بعينها". وفي حال كان هذا الأمر صحيحًا، وأعتقد أنه كذلك، فإن مستخدم الكمبيوتر العادي "لا يعيش" حياة طبيعية، وإنما "يعيشون على حافة الخطر" من التعرض للاختراق.

> غالبًا ما يثق الأشخاص الكسالى بالكمبيوتر من أول يوم يبدؤون في استخدامه ولا يفكرون فيه بعد ذلك، مما يجعلهم أكثر عرضة ليكونوا ضحايا للمخترقين\

علاوة على ذلك، تكون دروس تعليم استخدام الكمبيوتر متاحة للجميع عبر الإنترنت، ومع ذلك لا يستفيد الكثير من الأشخاص منها. لذلك، بدلاً من استخدام هذه المعلومات لحماية أنفسهم، يجعلون أنفسهم أكثر عرضة للقرصنة. ومرة أخرى، يتلخص الأمر في الأهميّة التي تحتلّها الثقة في بيئتهم بدلاً من تثقيف أنفسهم.

4. التكاسل

يعود السبب الرابع وراء تسبّب الناس في تعرّضهم للاختراق إلى الكسل، إذ أنه من الممتع للغاية أن تلعب لعبة على الكمبيوتر، أو تشاهد فيلما على نتفليكس أو تتصفح الإنترنت فقط، مقارنة بتخصيص بعض الوقت لتعلم مهارة جديدة. لقد أصبح المجتمع ا ينجذب أكثر لعيش الحياة الزائفة التي يراها في تلفزيون الواقع، بالتالي، تكمن مشاكل العالم وإجاباته بين حدود شاشاتنا.

في الواقع، هناك قول فرنسي يشير إلى الآتي: "الناس الكسالى دائمو الحرص على القيام بشيء ما"، لكن المشكلة الوحيدة تكمن في أن هذا "الشيء" هو اللاشيء الذي يسمح للمخترقين بالتسلّل إلى المساحة الالكترونيّة الخاصة بالفرد دون أن يدرك ذلك. لماذا؟ لأنهم كسولون للغاية ليبدو أي اهتمام، ولأنهم يعتقدون أن شخصًا آخر سيعتني بالمشكلة نيابة عنهم. وغالبًا ما يثق الأشخاص الكسالى بالكمبيوتر من أول يوم يبدؤون في استخدامه ولا يفكرون فيه بعد ذلك، مما يجعلهم أكثر

عرضة ليكونوا ضحايا للمخترقين.

العشوائية

في المقابل، أعتقد أن السلوك البشري يلعب دورًا كبيرًا في عمليّة القرصنة، حيث يجب أن نعترف بأن عمليات القرصنة تحدث بطريقة عشوائيّة. وقد يتخذ الشخص كل الخطوات اللازمة لحماية نفسه، ليجد نفسه في مواجهة اختراق كبير. وعلى سبيل المثال، قد تتعرّض كلمات المرور الخاصة بهؤلاء الأشخاص للسرقة على موقع بيع إلكتروني أو يتعرّض البائع الذي يتعاملون معه للقرصنة، مما يعرّضهم بدورهم للاختراق.

> قد يكون هؤلاء الأشخاص الذين يعملون في الشركات والمجالات الصناعيّة، متكاسلين عندما يتعلّق الأمر بأمنهم الخاص، كما أنهم يكونون أكثر كسلا من غيرهم عندما يعملون لحساب شخص آخر

ومن الوارد أيضا أن يواجه المستخدم هجوما دون انتظار أو بسبب عيوب لم تكتشف من قبل. في المقابل، لا تعد هذه الأنواع من الاختراقات محور اهتمام هذا المقال، نظرا لأن مثل هذه القضايا تتجاوز سيطرة الفرد، بينما يمكن إصلاح العيوب الأربعة المذكورة أعلاه من خلال التعليم. وبمجرد تلقينهم مثل هذه الأمور، سيختفي قدر كبير من الأسباب والتأثيرات البشرية داخل عالم الاختراق.

الخلاصة

تكشف التفسيرات المذكورة أعلاه حول سبب تعرّض الناس للاختراق، عن صحة هذا الأمر، ولكن ليس فقط في المجال الخاص. فقد يكون هؤلاء الأشخاص الذين يعملون في الشركات والمجالات الصناعيّة، متكاسلين عندما يتعلّق الأمر بأمنهم الخاص، كما أنهم يكونون أكثر كسلا من غيرهم عندما يعملون لحساب شخص آخر. وفي النهاية، يجب أن تدرك شركات الأمن السيبراني نفسيّة البشر، في حال أرادت هزيمة المخترقين حول العالم. وفي غياب فهم النفسيّة البشرية، فإن أي برنامج أمني أو أي كتلة تسلسلية "غير قابلة للتغيير" ستفتقد دائما أحد العناصر الرئيسية التي ستدافع منم خلالها عن نفسها.

المصدر: هاكر نون

رابط المقال : https://www.noonpost.com/28191/