حلم مستقبل "إنترنت الأشياء" أصبح كابوسًا

ترجمة حفصة جودة

منذ ظهور الإنترنت، أكد مخترعوه أن زيادة الترابط سيسفر عن مستقبل أكثر إشراقًا، فشبكة الإنترنت – كما قالوا – سوف تقربنا من أشكال جديدة من وسائل الاتصال الجماهيري وتربطنا بقطاع الأعمال والحكومة، لتمنحنا المزيد من التحكم في حياتنا وتوفر لنا عالمًا جديدًا من السلع والخدمات.

لقد استفدنا جميعًا بطريقة أو بأخرى من ثمار التكنولوجيا، لكننا تعرضنا أيضًا لاضطرابات كثيرة وفقدان للوظائف، من الخدمات المصرفية وحتى وسائل الترفيه، وصعود ثقافة نقاط الضعف – مثلما حدث يوم 21 أكتوبر – والقابلية المرعبة للقرصنة والفيروسات وغيرهم من الهجمات.

كانت هجمات حجب الخدمة الموزعة – DdoS – التي حدثت يوم الجمعة الماضي قد استغلت موجة الابتكار الأخيرة التي وعدونا بأنها ستحسن حياتنا فقط، وهي: إنترنت الأشياء، فمن خلال ربط جميع الأجهزة مثل السيارات والمعدات والملابس، بالإنترنت، سنحصل على المزيد من الراحة والكفاءة، فمثلاً نصبح قادرين على ضبط الترموستات قبل العودة إلى المنزل وشراء الحليب عندما تخبرنا الثلاجة أنه قارب على النفاذ، وطبقًا لأحد التحليلات، فإن 6.4 مليار جهاز من هذا النوع سوف يكونون مرتبطين بالإنترنت بنهاية العام.

لكن الأجهزة المرتبطة بإنترنت الأشياء لم يتم تصميمها باستخدام مستويات أمن عالية مثل التي نستخدمها في هواتفنا وأجهزة الحاسب، ووفقًا لخبير الأمن التكنولوجي بريان كريبس، فإن هجمات الأمس كانت عن طريق برنامج يُسمى ميراي، والذي استغل نقاط الضعف في الكاميرات رخيصة السعر ومسجلات الفيديو الرقمية المتصلين بالإنترنت.

يقوم ميراي بمسح الشبكة والبحث عن الأجهزة المرتبطة بالإنترنت مثل الكاميرات وغيرها، والتي لا تمتلك أي حماية أكثر من إعدادات المصنع الافتراضية، ثم يقوم البرنامج بضم تلك الأجهزة واستخدامها

للهجوم وللدخول بأعداد كبيرة على الهدف الإلكتروني، وهو ما يسبب ضغطًا هائلاً على المواقع إلى حد لا تستطيع خوادم تلك المواقع استقبال المتصفحين أو المستخدمين الحقيقيين.

يعتقد كيربس أن هذه الكاميرات وأجهزة الفيديو قد تم تصنيعها في شركات صينية لتركيبها في منتجات مصانع أخرى، ولأن هذه الأجهزة مدمجة في التلفاز وغيره من الأجهزة، فلم يتم إعدادها بطريقة تمكننا من تحديثها ومن المستحيل ضبط كلمة سر جديدة بها، وكان هجوم مماثل قد حدث الشهر الماضي من خلال أكثر من مليون كاميرا صينية الصنع، وفقًا لما ذكرته صحيفة "وول ستريت جورنال".

ومع ازدياد عدد الأجهزة المرتبط بالإنترنت، فسوف تزداد احتمالات التعرض للاختراق، ولن يتوقف الاختراق على الأجهزة غير الضارة نسبيًا مثل الكاميرات، لكنه سينتقل إلى الأجهزة القاتلة مثل السيارات، ففي الشهر الماضي، قامت شركة التكنولوجيا الصينية تينسيت بتحذير تسلا من أنها تستطيع اختراق سياراتها وتفعيل أنظمة القيادة والكبح، وفقًا لموقع "ويرد"، وحينها قامت تسلا بتعزيز أنظمة الأمن في سياراتها.

ربما الحل المناسب هنا تحديد معايير جديدة على مستوى الصناعة المتعلقة بالأمن، ومؤسسات مستقلة تقوم بإصدار أختام الموافقة على العبوات والتي تشهد بسلامة المنتجات؛ كما يقول كيربس، تقوم المفوضية الأوروبية الآن بصياغة الاشتراطات بالفعل، لكنها لن تتمكن من إصلاح ملايين الجهزة الضعيفة الموجودة بالفعل.

في سباقهم لتوفير الأجهزة الجديدة والمعدلة، تتجاهل شركات التكنولوجيا المخاوف بشأن العواقب غير المقصودة لنمط الحياة الرقمية، فالثغرات الأمنية فرصة لتسويق منتجات جديدة.

يتبنى العديد من أباطرة شركة "سيليكون فالي" نظرة شبه ليبرالية ترفض القواعد، وترى أن التكنولوجيا تقوم بحل المشكلات التي لا تستطيع الحكومة حلها، لكن التعرض لهجمات خبيثة هي مشكلة أوجدتها التكنولوجيا، وإذا لم تتمكن التكنولوجيا من حلها فيجب على الحكومات أن تقوم بذلك.

المصدر: كوارتز

رابط المقال: https://www.noonpost.com/14709/