اختراق بيانات يكشف الأسرار التجارية لكبار صانعي السيارات

الأحد 22 يوليو 2018 11:07 م

كشف باحث أمني من شركة UpGuard للخدمات الأمنية عن اختراق أمني مكّنه من العثور على عشرات الآلاف من الوثائق الحساسة لكبرى الشركات الصناعية – بما فيها معظم شركات تصنيع السيارات الكبرى – على جهاز خادم احتياطي غير محمي. وقد تضمنت هذه الوثائق موادًا لأكثر من 100 شركة تعاملت مع الشركة الكندية Level One Robotics، التي تُقدم خدمات الأتمتة الصناعية للشركات، وذلك وفقًا لما جاء في تقرير جديد لصحيفة نيويورك تايمز.

وقال الباحث الأمني إنه عثر على هذه الوثائق على خادم احتياطي خاص بالشركة الكندية غير المحمي، فهو لا يتطلب أي كلمات مرور أو أذونات وصول خاصة، ويمكن لأي شخص متصل أن يقوم بتنزيل المواد التي بلغ حجمها 157 جيجابايت على الأقل، وتحتوي على ما يقرب من 47 ألف ملف يشتمل على الأسرار التجارية لعدد من الشركات مثل فيات كرايسلر وفورد وجنرال موتورز وتيسلا وتويوتا وفولكس واجن.

ولا شك بأن شركات تصنيع السيارات مثل جنرال موتورز وفورد وتيسلا وتويوتا وفولكس واجن تبذل قصارى جهدها للحفاظ على سرية معلوماتها الفنية. وتعد التفاصيل المتعلقة بآلات خط التجميع وعمليات الأتمتة من بين الأسرار التجارية الأكثر حساسية في هذه الصناعة.

ويبلغ حجم البيانات التي تم الكشف عنها 157 جيجابايت تقريبًا، وتتضمن مخططات خاصة بخطوط التجميع خلال 10 سنوات، و المخططات التفصيلية الأصلية للمصانع Blueprint، ووثائق وإعدادات الآلات الروبوتية، ونماذج طلب شارة الهوية، ونماذج طلب الوصول إلى الشبكة الخاصة الافتراضية VPN، واتفاقيات عدم الإفصاح عن سرية المعلومات NDAs -التي توضح بالتفصيل مدى حساسية المعلومات المكشوف عنها.

وتشتمل البيانات أيضًا على التفاصيل الشخصية لبعض موظفي شركة Level One الكندية، بما فيها صورًا ضوئية لتراخيص القيادة وجوازات السفر، وبيانات عملاء شركة Level One بما فيها من خطط العمل والفواتير والعقود وتفاصيل الحسابات المصرفية.

وقد تم اكتشاف هذا الاختراق أول الشهر الجاري من قبل كريس فيكيري Chris Vickery الباحث الأمني بشركة UpGuard، والذي قال: "يعتبر هذا الاختراق من أسوأ عمليات الكشف عن بيانات حساسة في مجال الأمن الإلكتروني حتى الآن، حيث أنه يكشف عن الكثير من الأسرار التجارية لكبرى الشركات الصناعية، وبطبيعة الحال إذا ما عثرت على مصطلح NDAs على وثيقة ما، فاعلم على الفور أنك عثرت على شيء لا يُفترض أن يكون متاحًا للجميع".

تجدر الإشارة إلى أن مصطلح NDA هو اختصار للعبارة الإنجليزية التالية: non-disclosure agreement، أي: اتفاقية عدم الإفصاح، وهي اتفاقية توقع ما بين طرفين على الأقل وتنص على أن هناك بعض المعلومات السرية التي سيتم مشاركتها بين أطراف العقد فقط ويمنع الإفشاء عنها للعلن.

لم يكن من الواضح ما إذا كان أي شخص آخر قد شاهد أو قام بتنزيل هذه البيانات غير المحمية، والتي تضمنت بعض المعلومات الشخصية لموظفي شركة Level One والأسرار التجارية للشركات التي تتعامل معها. وقد أبلغ الباحث فيكيري الشركة الكندية خلال الأسبوع الماضي، وبالفعل تم حجب هذه المعلومات غير المحمية في غضون يوم واحد. إلا أن الكشف غير المقصود لبيانات العملاء يوضح مشكلة كبيرة تواجها الشركات الكبري وهي تعرضها لمخاطر أمنية كبيرة عن طريق مورديها والشركات الخارجية التي تتعامل معها.

وقد تم الكشف عن البيانات عن طريق اختراق موقع شركة Level One Robotics الكندية من خلال الوصول إلى بروتوكول rsync، وهو بروتوكول نقل ملفات شائع يُستخدم في النسخ الاحتياطي لمجموعات البيانات الكبيرة.

وفقًا لباحثين أمنيين فإنه لم يتم وضع قيود على خادم rsync بواسطة عنوان IP أو اسم مستخدم User Name، وهذا يعني أن أي عميل rsync متصل بمنفذ rsync كان لديه حق الوصول إلى تنزيل هذه البيانات، ويوضح هذا الكم الهائل من البيانات الحساسة وعدد الأعمال المتأثرة كيف يمكن أن تؤثر المخاطر الإلكترونية لسلسلة الإمداد من طرف ثالث ورابع على أكبر الشركات.

ونشرت شركة UpGuard تفاصيل الحدث في منشور عبر مدونتها يحمل عنوان كيف أظهر مورد الروبوتات بيانات سرية لشركات التصنيع الرئيسية؟ موضحةً أنه إذا كان هناك شخص يعرف مكان البحث سيمكنه الوصول إلى الأسرار التجارية المحمية من قبل شركات صناعة السيارات وذلك بسبب خطأ من الشركة الموردة.

والجدير بالذكر أنه في عام 2013 حدث أسوأ اختراق بيانات بسبب خطأ الشركة الموردة، حينما أكدت شركة Target Stores العملاقة أنّ هناك قراصنة قد استولوا على حوالي 40 مليون رقم بطاقة ائتمان، وبطاقة خصم تم استخدامها في متاجرها وقد توصل المهاجمون لهذه البيانات عن طريق اختراق أحد مقاولي أنظمة التدفئة والتهوية التابعين لشركة تارجت ثم استخدام المعلومات المسروقة من هذا النشاط التجاري للوصول إلى أنظمة تارجت واختراقها.

وخلال الشهر الماضي كشفت شركة تيكت ماستر Ticketmaster لبيع التذاكر أن معلومات الدفع الخاصة بآلاف العملاء قد سُرقت في الآونة الأخيرة في اختراق حدث بسبب برنامج غير آمن من شركة Inbenta، وهي شركة تدير منتديات دردشة دعم العملاء على موقع TicketMaster.

وأكدت 56 في المائة من الشركات -التي شاركت في استطلاع العام الماضي الذي أجراه معهد بونيمون Ponemon Institute للأبحاث الأمنية- إنهم تعرضوا في وقت ما لاختراق أمني بسبب الموردين، وتزاد احتمالية الاختراق مع زيادة عدد الجهات الخارجية التي تتعامل معها الشركات: قال المشاركون في الاستطلاع إن ما متوسطه 470 شركة خارجية قد تمكنت من الوصول إلى معلومات الشركة الحساسة مقارنةً بـ 380 شركة قبل عام واحد.

وقال لاري بونمون مؤسس شركة الأبحاث: "لقد بدأ المديرون التنفيذيون في الإقرار بأن بعض علاقاتهم مع الأطراف الثالثة تخلق مخاطر أمنية غير معقولة".

وقالت فاي فرانسي Faye Francy المديرة التنفيذية لمركز تقاسم وتحليل المعلومات المتعلقة بالسيارات وهي مجموعة تجارية تركز على الأمن السيبراني: "إن صناعة السيارات لديها سلسلة إمدادات عميقة ومعقدة كما أن المخاطر الأمنية التي يواجهها الطرف الثالث تشكل مصدر قلق متنامٍ".

ورفض ميلان جاسكو Milan Gasko الرئيس التنفيذي للشركة الكندية Level One مناقشة أي تفاصيل حول الحادثة حيث أن هذه الوثائق السرية قد تم الكشف عنها من خلالها، حيث قال الشركة تأخذ هذه المزاعم على محمل الجد، وتعمل على إجراء تحقيق كامل في طبيعة ومدى وتشعبات هذا الكشف عن البيانات، وأضاف: "من أجل الحفاظ على سلامة هذا التحقيق لن نقدم أي تعليق في هذا الوقت".

الجدير بالذكر أن شركة Level One تأسست في عام 2000 بمدينة وندسور في كندا، وافتتحت مكتبًا أمريكيًا بعد ست سنوات في مدينة ديترويت، وتقدم الشركة خدمات هندسية مع التركيز على الروبوتات والأتمتة لشركات التصنيع.

وامتنع مسؤولون من جنرال موتورز وتويوتا وفولكس واجن عن التعليق على البيانات التي تم الكشف عنها، في حين لم تستجب فيات كرايسلر وفورد وتيسلا لطلبات التعليق.

الاستنتاج النهائي:

أصبحت سلسلة التوريد أضعف جزء في مجال خصوصية بيانات الشركات الكبرى، ولا تزال الشركات التي تنفق ملايين الدولارات سنويًا في مجال الأمن السيبراني معرضة للخطر من قِبل مورد يتعامل مع بياناتها، حيث تنطوي خطورة سلسلة التوريد على توسعة الأطراف الثالثة والرابعة الذين يتعاملون مع مجموعات بيانات الشركات.

جميع هؤلاء الموردين لديهم عمليات وأنظمة خاصة بهم تحدد مدى حماية البيانات، لذلك يجب أن يكون لدى المؤسسات وموردها عمليات نشر موحدة تعمل على إنشاء أصول والحفاظ عليها بشكل آمن، مما يقلل من احتمال وقوع حادث اختراق للبيانات. إذا لم يتم تضمين هذا الأمان في العمليات نفسها فستكون هناك دائمًا أخطاء في التهيئة تؤدي إلى اختراق للبيانات.

كما يجب أن يكون لديهم أيضًا خطة استجابة في حالة اختراق البيانات، بحيث يمكنهم التصرف بسرعة لمعالجة الأمر عندما يتعرضون لحادث ما، كما فعلت شركة Level One في هذه الحالة.

تعمل شركة Level One Robotics مع العملاء والموردين الآخرين كما تقتضيه عملية تصنيع وبيع الروبوتات. وهذه المنظومة من السهل جدًا أن تُعرض السلسلة بأكملها للخطر في حالة وجود رابط واحد غير مؤمن ومحمي جيدًا.