الخليج

اقتصاد, تقنية وسيارات

17 يونيو 2022 17:20 مساء

من رؤساء أمن المعلومات يحذرون من الحساب السحابي % 30

دبي: «الخليج»

والتي تسمح Microsoft 365 أو Office 365 كشفت شركة بروف بوينت للأمن السيبراني عن أحدث خصائص بطريقة تجعلها غير قابلة للاسترداد بدون نسخ OneDriveو SharePoint لبرامج الفدية بتشفير الملفات المخزنة على احتياطية مخصصة أو مفتاح فك تشفير من الجهة التي تهاجم البرنامج وبمجرد اختراق البرنامج، يعمد قراصنة الإنترنت إلى تشفير الملفات في الحسابات التي تم اختراقها. تماماً كما هي الحال مع نشاط برامج الفدية عند اختراق أماكن تخزين الملفات، ولا يمكن استرداد هذه الملفات إلا باستخدام مفاتيح فك التشفير. يمكن أتمتة هذه الإجراءات باستخدام Microsoft APIs والبرامج النصية لواجهة سطر الأوامر (CLI) والبرامج النصية PowerShel.

وقال إميل أبو صالح، المدير الإقليمي لدى بروف بوينت في منطقة الشرق الأوسط وإفريقيا: «يؤكد 30% من رؤساء أمن المعلومات في دولة الإمارات أن الحساب السحابي يمثل التهديد الأكثر أهمية بين التهديدات التي تستهدف مؤسساتهم، ولذلك تعد مسألة حماية البيانات في السحابة أمر بالغ الأهمية ولحماية الحساب السحابي للشركات، يجب على المؤسسات التأكد من أنها تمتلك أنظمة أمنية قوية. ويجب أن تكون الأنظمة الأساسية الأمنية قادرة على التشفير الشامل ومراقبة البيانات باستمرار واكتشاف الحوادث بسرعة، لتمكين المسؤولين من الحد من الأضرار ومعالجتها».

هجمات الفدية

ومن بين الأمثلة على سلسلة هجمات برامج الفدية السحابية، يقوم قراصنة الإنترنت بتعديل إعدادات القائمة، ما يؤثر في جميع الملفات الموجودة في ملف المستندات. ويحتوي كل ملف مستندات على إعداد قابل للتعيين بواسطة المستخدم لعدد الإصدارات التي يتم حفظها، والتي يمكن لمالك الموقع تغييرها، بغض النظر عن أدوارها الأخرى وهناك طريقتان لإساءة استخدام آلية تعيين الإصدار لاختراق هذه الملفات- إما عن طريق تعيين عدد كبير جداً من إصدارات الملف وإما عن طريق تقليل حدود إصدار ملف المستندات. تتضمن عمليات التعديل والتي تزيد من إصدار أحد الملفات أو تغيير المحتويات واسم الملف والبيانات الأولية للملف وحالة تشفير الملف.

ستعمل الملفات المخزنة بأكثر من وضعية على كل مساحة تخزين وفي السحابة على سبيل المثال من خلال تخزين ملفات السحابية على تقليل تأثير هذه المخاطر الجديدة حيث لن يتمكن المهاجم من الوصول إلى الملفات المحلية / مكان تخزينها. لإتمام الإجراءات الكاملة لهجمات الفدية، سيتعين على قراصنة الإنترنت اختراق مكان التخزين والحساب السحابي للوصول إلى مكانها والملفات المخزنة على السحابة.

طرق للحماية

سيؤدي .CASB باستخدام Office 365 أولاً: قم بتشغيل برنامج الكشف عن تغييرات تعيين الملفات الحساسة لبرنامج ذلك إلى الحد من مخاطر من الهجمات على المستخدمين واستغلال حدود الإصدار المنخفضة لقوائم المستخدمين لهجمات الفدية على المؤسسة.

ثانيًا: تحسين المستويات الأمنية حول برامج الفدية.

* الأفراد المعرضون للهجوم بشدة:

حدد مستويات الحماية الأكبر أولوياتها للمستخدمين الذين يواجهون أكبر عدد من الهجمات على السحابة والبريد وقد يكون هؤلاء المستخدمون (TAP) .الإلكتروني والويب وأكثرها تهديداً باستخدام الحماية من الهجمات المستهدفة خارج قائمة لأشخاص المهمين جداً مثل المديرين التنفيذيين والمستخدمين المتميزين.

* إدارة الوصول:

وتطبيق سياسة مقننة في (MFA) حافظ على سياسة كلمة مرور قوية، وزد من استخدام المصادقة متعددة العوامل الامتيازات، وسياسة وصول قائمة على المبادئ عبر التطبيقات السحابية

* التعافي من الكوارث والنسخ الاحتياطي:

تحديث سياسات التعافي من الكوارث والاحتفاظ بنسخ احتياطية من البيانات لتقليل الخسائر في حالة التعرض لبرامج الفدية والوضع المثالي هو الاحتفاظ بنسخ احتياطية خارجية كاملة للملفات السحابية مع البيانات الحساسة بشكل لتوفير نسخ احتياطية من خلال تعيين إصدارات ملفات المستندات. Microsoft دوري منتظم. لا تعتمد فقط على

* الأمن السحابي:

كشف ومعالجة حالات الاختراق في الحساب وإساءة استخدام تطبيقات الطرف الثالث على سبيل المثال، يتكامل وذكاء التهديدات من طرف ثالث لإيقاف عمليات Proofpoint Nexus Threat Graph مع Proofpoint CASB الاستيلاء على الحساب وإساءة استخدام تطبيقات الطرف الثالث.

* حماية البيانات:

منع تنزيلات البيانات الحساسة وتنزيلات البيانات على نطاق واسع عبر الأجهزة غير المراقبة لتقليل احتمالية تعرضها .لتكتيكات الابتزاز المزدوجة في برامج الفدية