الخليج

اقتصاد, أسواق الإمارات

19 مارس 2022 21:48 مساء

قراصنة المعلومات يستهدفون نقاط ضعف الموظفين والبنية التحتية

دبي: حمدي سعد

توقع مسؤولو شركات متخصصة في تأمين البيانات ارتفاع وتيرة الهجمات الإلكترونية خلال 2022 على المؤسسات والشركات التي لا تمتلك قدرات تنبؤ أو استعدادات كافية لمواجهة الهجمات المبتكرة والخداعية من قبل قراصنة البيانات على مستوى العالم بغرض التخريب أو الحصول على الأموال.

وأكد المسؤولون أن الهجمات الإلكترونية دائماً ما تستهدف نقاط الضعف في شبكات المؤسسات والشركات والتي تمتلك بيانات مهمة أو تستهدف أجهزة الموظفين الذين ليست لديهم الخبرة الكافية للتعامل مع هذه الهجمات أو عن طريق مهاجمة أجهزتهم التي يتنقلون بها خارج نطاق العمل.

ونصح هؤلاء بضرورة تحديث برمجيات حماية البيانات بصورة مستمرة وبناء أنظمة تستخدم تقنيات الذكاء الاصطناعي وتعلم الآلة قادرة على توقع توقيت الهجمات الإلكترونية أو التنبؤ بها قبل وقوعها لاتخاذ الإجراءات الضرورية وبسرعة لمنعها أو على الأقل التقليل من خسائرها.

يقول أفرام تسفاي، مدير هندسة المبيعات في شركة «جينيتك»: ستبقى مخاوف الأمن السيبراني أولوية خلال 2022، حيث تحتاج الشركات إلى مناهج جديدة لمواجهة مخاطر الجرائم الإلكترونية المتزايدة وأن تكون سريعة الحركة وحساسة لتوسيع نطاق التهديدات كون المزيد من التهديدات تأتي عبر الإنترنت وتصبح معالجة البيانات أمراً حيوياً للعمليات، مما سيتطلب ذلك إنفاقاً إضافياً على أنظمة وحلول حماية البيانات.

وأضاف، حتى تحافظ المؤسسات والشركات على بياناتها آمنة، يجب عليها إعطاء الأولوية للأمن السيبراني، يجب استخدام منصات أمان موحدة تدمج وتستثمر في حماية البيانات عبر شبكات الإنترنت.

بنية تحتية أكثر تعقيداً

وأشار عماد فهمي، مدير هندسة النظم في الشرق الأوسط لدى «نتسكاوت»: «إلى أنه ونظراً لأن العمل الهجين أصبح على نحو متزايد «الوضع الطبيعي الجديد» للموظفين، فمن المهم التأكد من أن لديهم الأدوات المطلوبة لإكمال مهامهم اليومية. نتيجةً لذلك، يجب أن توفر الأدوات التعاونية وبرامج الأعمال إمكانية استخدام استثنائية، ويجب على شركات الأمن السيبراني أيضاً تقديم هذا التأمين.

وفي بيئة العمل الهجينة، أصبحت تقنيات الاتصال والتعاون الموحد شائعة بشكل متزايد، لذا تكافح العديد من فرق تقنية المعلومات لتحديد المشكلات وحلها، حيث تصبح البنية التحتية للأعمال أكثر تعقيداً، وتعتمد على موردي خدمات مختلفين لتوفير الخدمات الرئيسية لكل من مساحات العمل في المنزل والمكتب.وعلى هذا النحو، تتعرض شركات تكنولوجيا المعلومات لضغوط مستمرة من أجل تحسين تجربة المستخدم النهائي عبر عدد متزايد من التطبيقات، بما في ذلك التطبيقات كخدمة (SaaS) والاتصالات الموحدة كخدمة (UCaaS) والخدمات القائمة على مركز البيانات.

عائلة من برمجيات الفدية 120

يقول عماد الحفار، رئيس الخبراء التقنيين لمنطقة الشرق الأوسط وتركيا وإفريقيا في«كاسبرسكي»: إن الهجمات ببرمجيات طلب الفدية ليست جديدة، فهي موجودة منذ ما يزيد على عقدين من الزمن، لكنها تنمو وتتطور بطرق لا ندركها.

وتشير التقديرات إلى أن هناك الآن أكثر من 120 عائلة منفصلة من برمجيات الفدية، وأصبحت الجهات التخريبية التي تقف وراءها بارعة في إخفائها.

وقد أدّت رقمنة الشركات والعمل عن بُعد إلى إنشاء منافذ وأهداف جديدة لهذه الهجمات، فأصبح من السهل على

.عصابات طلب الفدية استهداف الأفراد، فاستخدامك جهاز حاسوب مزوّداً ببرمجيات قديمة، مثلًا، يجعلك هدفًا سهلًا

وكان هجوم طلب الفدية على شركة «كولونيال بايبلاين» المشغلة لخط أنابيب وقود الساحل الشرقي في الولايات المتحدة، أحد أكبر حوادث الأمن الرقمي التي هزّت العالم في العام 2021، بعد أن نجح الهجوم في قطع إمدادات الغاز .وإحداث شلل كامل في الساحل الشرقي للبلاد لمدة ستة أيام

ومثل هذه الحوادث تعلمنا أن الأمر لا يتطلب هجوماً متطوراً لتعطيل العمليات وشلّ البنى التحتية الحرجة، كما سلّط هذا الحادث الضوء على أهمية الأمن الرقمي في كل جانب من جوانب الأعمال والاقتصاد. كذلك، فنحن نواجه أصلاً نقصاً في التوريدات بسبب الجائحة، التي دفعت إلى مزيد من الأتمتة في قطاع سلاسل التوريد، الأمر الذي يترافق مع .مجموعة من التهديدات

ويتزايد اعتماد قطاعات الخدمات اللوجستيات والصناعة على الرقمنة، ما يجعلها أكثر عرضة للهجمات. وقد شهدنا .عدداً كبيراً من الهجمات، لذا يصبح تعطّل سلاسل التوريد مصدر قلق كبير

وإن الاعتماد الواسع النطاق للتقنية، والزخم المتسارع للتحول الرقمي، وانخفاض مستويات الوعي، والافتقار إلى المساواة في تطبيق الأمن الرقمي في البيئة المؤسسية، أمور تساعد مجرمي الإنترنت على النجاح في مهام التجسس الرقمي والنفاذ بها من دون أخطاء. فعصابات الجريمة الرقمية تستخدم أساليب متطورة لحماية الشيفرات البرمجية .الخبيثة وإخفائها عن أعين التحليل الأمني بعد الهجوم

ويؤكد الحفار أنه من المهم حماية الموظفين العاملين عن بُعد لكونهم بعيدين عن أنظار الشركة، وذلك مما يُساعد في .زيادة الإنتاجية

ويقول: إن العمل عن بُعد قد يعني أيضاً أن الموظفين ليسوا صارمين في اتباع أفضل ممارسات الأمن الرقمي، ففريق تقنية المعلومات ليس متاحاً لتقديم الإرشاد والمشورة، الموظفون سينجزون أعمالهم باستخدام أجهزة الشركة، ولكنهم قد يستخدمونها أيضاً لأغراض شخصية كالتسوّق. ويتوقع مجرمو الإنترنت هذه التغيّرات ويبحثون دائماً عن سبل .جديدة لاستغلالها

تكتيكات الضغط

بدوره يؤكد جوني كرم، المدير العام ونائب الرئيس الإقليمي للأسواق الناشئة الدولية في شركة «فيريتاس تكنولوجيز»، أن سعي المجرمين الإلكترونيين في ازدياد لرفع عائداتهم المالية بأقل جهد ممكن، لذا بدؤوا باللجوء إلى اختيار برمجيات الفدية كوسيلة رئيسية للهجوم وتركيز جُلّ اهتمامهم على المؤسسات عالية القيمة. وبالنظر إلى أعداد الشركات الناجحة في المنطقة، والتي تتبوأ مكانةً عالميةً رائدةً في قطاعات النفط والغاز والخدمات المالية والرعاية .الصحية، أصبحت الإمارات هدفاً رئيسياً لهجمات برمجيات الفدية

وتلجأ الجهات التي تعمد إلى اتباع هذا النوع من الهجمات ضد الشركات في الإمارات إلى استخدام تكتيكات قائمة على الضغط، مثل تشفير البيانات وسحب البيانات التجارية والشخصية الحسّاسة، بهدف ابتزاز ضحاياها لدفع الفدية مقابل .فك تشفير هذه البيانات واستعادة إمكانية الوصول إلى الأنظمة والبيانات الخاصة بها

وحتى إن تمكّنت الشركة من استعادة بياناتها المشفرة أو استنساخها، ستواجه مخاطر كشف البيانات المستخلصة وإتاحتها للعامة كوسيلة ضغط يستخدمها المهاجمون لإجبار الشركات على دفع الفدية المطلوبة. ومن المتوقع أن يستمر هذا التوجه في الإمارات، لا سيما في القطاعات التي يُعرف عنها تخزينها لبيانات العملاء الحسّاسة، مثل قطاعات الخدمات المالية والرعاية الصحية.

جهود التصدي

ويضيف كرم، تبدأ جهود التصدي لأي نوع من هجمات الفدية الخبيثة دائماً بأن تكوّن الشركة فهماً واضحاً لبياناتها، أي بتحديد طبيعتها ومواقع حفظها وقيمتها. إذ يوفر ذلك حماية للبيانات الاستراتيجية، كما يوفر للشركات المعلومات اللازمة للاستجابة بشكل فعال لتلك الهجمات.

وتتطلب القدرة على رفض دفع الفدية مستويات عالية من الثقة بقدرة الشركات على احتواء المخاطر من خلال استعادة البيانات دون الحاجة لدفع الفدية وعدم وجود بيانات مسروقة أياً كانت أهميتها، ما يعني امتلاك نسخ احتياطية موثوقة عن البيانات، والقدرة على عزل جميع البيانات المهمة.

ويقول كرم: تعد معرفة موعد حدوث هجمات الفدية الخبيثة أكثر أهمية من معرفة إمكانية حدوثها، إذ يمكن للكشف السريع عن العيوب والأخطاء أن يتيح إمكانية تحديد نقطة استرداد دقيقة، والحماية من عمليات تسريب البيانات، وبالتالي تقليص التأثيرات السلبية للهجمات الناجحة إلى الحد الأدنى.

بيل سكودر: نضج في استخدامات الذكاء الاصطناعي

يقول بيل سكودر، نائب أول الرئيس والمدير العام لحلول الذكاء الاصطناعي المرتبطة بإنترنت الأشياء في شركة «آسبن تكنولوجي»: يشهد عام 2022 نضجاً في استخدامات الذكاء الاصطناعي وسنرى المزيد من المؤسسات تعمل على تحويل العديد من الاستثمارات لتوظيف التطبيقات الأكثر دقة والتي تناسب الغرض وتساعدها على تحقيق أهدافها الربحية والمستدامة.

وأضاف ينبغي مواصلة اعتماد نماذج الذكاء الاصطناعي وبشكل أكبر للاستفادة من الخبرات التي تساعدها على التفسير والتنبؤ بالتحليلات العميقة والتعلم الآلي، كما سيتم تحويل البيانات الصناعية إلى نتائج أعمال حقيقية عبر دورة حياة الأصول الكاملة.

وأشار سكودر إلى أن لهذا التحول فائدة مزدوجة تتمثل في تسهيل التحالفات الجديدة الأفضل من نوعها التي تتمحور حول الذكاء الاصطناعي. ففي سابق الأمر، كانت مجمل الشراكات تتمحور حول التكنولوجيا بشكل رئيسي، مدفوعة بالخدمات أو مورد وحيد كبير. في حين يتطلب التركيز الأكثر تخصصاً للذكاء الاصطناعي وجود مجموعة أكبر من موردي الحلول، والذين يجمعون معاً خبراتهم المستقلة والمتخصصة.

وهذا لا يساعد فقط في تطوير الشراكات بعيداً عن مشاريع الذكاء الاصطناعي الأكثر عمومية، بل سيضع تركيزاً أكبر على الشراكات التي تعتمد القيمة والوقت مما يساعد على تقليل العائق أمام تبني الذكاء الاصطناعي أكثر من أي وقتٍ مضى.

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©