الخليج

اقتصاد, تقنية وسيارات

6 نوفمبر 2022 21:42 مساء

جارتنر»: 6 طرق للتصدي لهجمات برامج الفدية المعلوماتية«

دبي: حمدي سعد

تصل كلفة هجمات برامج الفدية على الشركات إلى ملايين الدولارات، وربما تكون السبب في خسائر أكبر على المدى الطويل، لا سيما عندما تنعكس تأثيراتها على سمعة الشركة وموثوقيتها. وسواء كانت شركات كبرى في مجال الرعاية الصحية أو البيع بالتجزئة أو شركات تأمين، فقد أثبتت هجمات برامج الفدية أنها باتت تمثل تهديداً مستمراً للأمن السيبراني.

وتعرف هجمات برامج الفدية بكونها ابتزازاً سيبرانياً يحدث عندما تتسلل هذه البرمجيات الضارة إلى أنظمة الكمبيوتر وتعمل على تشفير البيانات، واحتجازها رهينة إلى حين سداد الضحية لمبلغ الفدية – ويمكن أن تمتد لأكثر من مجرد اختراق للبيانات بالنسبة للمؤسسات.

بول ويبر

قال بول ويبر، كبير المحلّلين لدى شركة «جارتنر» ل«الخليج»:«اضطرت المنظمات التي وقعت ضحية لهجمات برامج الفدية في بعض الحالات الأخيرة لدفع مبالغ ضخمة لمنفذي هذه الهجمات، الأمر الذي قد يتسبب بمزيد من الانتشار لهذه الممارسات.

وأضاف ويبر، يتوجب على الشركات أن تصبّ تركيزها على إتمام جاهزيتها والعمل على الوقاية في مراحل مبكرة إن كانت ترغب في وضع حد لهذه الخسائر الناجمة عن هجمات برامج الفدية».

وينصح ويبر باتخاذ عدة خطوات كإجراءات استباقية أو احترازية وبعض التوجيهات التي يمكن أن تخفف من آثار هجمات طلب الفدية على المؤسسات والشركات بشكل عام وذلك عبر التوجيهات التالية:

1- إجراء تقييمات أولية لبرامج الفدية

يجب إجراء تقييم المخاطر واختبارات الاختراق للتعرف على احتمالات الاختراقات الوضع الحالي للفعالية الأمنية وجاهزيتها فيما يتعلق بالأدوات، والإجراءات، والمهارات المطلوبة للتصدّي لهذه الهجمات.

ويقول ويبر:«قبل أن تقرّر أن تسديد الفدية هو الخيار الوحيد أمامك، تحقق من الأمر بواسطة البرامج المجانية المتاحة لفك تشفير برامج الفدية».

2- فرض إجراءات لحوكمة هجمات برامج الفدية

يجب فرض عمليات وإجراءات الامتثال التي تشمل صنّاع القرار الرئيسيين في المؤسسة، حتى في مرحلة تسبق الإعداد للاستجابة التقنية لهجمات برامج الفدية. إذ يمكن لهذه الهجمات أن تتفاقم من كونها قضية عابرة إلى أن تشكل أزمة حقيقية خلال فترة قصيرة، مما قد ينتج عنه خسائر في عائدات الشركة وأضرار تلحق بسمعتها التجارية.

ويجب أن تكون الأطراف الرئيسية مثل الرئيس التنفيذي ومجلس الإدارة وغيرهم من الجهات المعنية مشاركة في عملية الإعداد هذه. وفي حال وقوع هجمة لبرامج الفدية، فإن عدداً من الصحفيين أو الأطراف الخارجية المعنية سوف تخاطب مجلس الإدارة للاستفسار عن طريقة التعامل مع هذه الهجمات، بدلاً من التواصل مع المسؤولين عن أمن المؤسسة أو الرئيس التنفيذي لأمن المعلومات لديها.

3- الحفاظ على نسق الجاهزية التشغيلية

يجب إجراء تدريبات واختبارات متكررة لضمان جاهزية الأنظمة الدفاعية وقدرتها على اكتشاف هجمات برامج الفدية. ويمكن القيام باختبارات منتظمة لسيناريوهات الاستجابة لهذه الحوادث ضمن خطة الاستجابة لهجمات برامج الفدية.

ويجب إعادة الاختبار على فترات منتظمة للتحقق من وجود أية ثغرات أمنية، أو عدم امتثال للإجراءات أو ضبط خاطئ الإعدادات. كما يفترض التأكد بصورة مستمرة من أن إجراءات الاستجابة لهذه الحوادث لا تعتمد بنفسها على أنظمة تقنية المعلومات التي يمكن أن تكون عرضة لتأثيرات هجمات برامج الفدية هذه أو في حال توقفها عن العمل في حال وقوع حادث خطير.

4- الاحتفاظ بنسخ احتياطية

لا يجب أن تقتصر النسخ الاحتياطية على البيانات فحسب، بل يجب أن تشمل كذلك التطبيقات غير القياسية وأية بنية تحتية مساندة لتقنية المعلومات. وعلى المؤسسات والشركات الاحتفاظ بنسخ احتياطية دورية ذات موثوقية عالية، والحرص على توفير قدرات استردادها.

وفي حال الاعتماد على النسخ الاحتياطي عبر الإنترنت، يجب التأكد من عدم إمكانية تشفيرها بواسطة هجمات برامج الفدية. ومن الضروري جداً تعزيز مكونات منظومة النسخ الاحتياطي للمؤسسة والبنية التحتية لعملية الاسترداد وتأمينها من هجمات برامج الفدية من خلال الاختبارات الدورية لتطبيق النسخ الاحتياطي، والتخزين، والنفاذ عبر الشبكة، ومقارنة ذلك مع النشاط المتوقع أو الأساسي.

5- تطبيق مبدأ صلاحية الحد الأدنى

يجب ضبط وتقييد صلاحيات الوصول للأجهزة أمام الأطراف غير المصرّح لها. يجب إزالة صلاحيات المشرف المحلي من جميع المستخدمين النهائيين وحجب إعدادات تثبيت التطبيقات للمستخدم العادي، واستبدال ذلك بخيار أدوات توزيع البرامج المُدارة مركزياً.

ويتوجب على الرؤساء التنفيذيين لأمن المعلومات والمسؤولين الأمنيين اعتماد ميزة التحقق من الهوية متعدد العوامل حيثما كان ذلك ممكناً، لا سيما بالنسبة للحسابات ذات الصلاحيات الأعلى.

ويجب زيادة سجلات المصادقة على هوية استخدام جميع أنظمة الخادم الحساسة، وتطبيقات الشبكة، وخدمات الدليل، والتأكد من عدم حذف هذه السجلات، كما يجب إخطار فريق العمليات الأمنية بأية عمليات مشبوهة والحرص على قيامهم استباقياً بالتحقق من أية محاولات تسجيل دخول فاشلة أو غير اعتيادية.

6- التدريب على إجراءات الاستجابة للهجمات

يمكن البحث عن الجهات الحكومية والسلطات الإقليمية التي توفّر إرشادات حول كيفية تعزيز البنية التحتية للشبكات وتحصينها ضد هجمات برامج الفدية.

وبإمكان رؤساء أمن تقنية المعلومات والمسؤولين الأمنيين اتّباع إرشادات كهذه من أجل إعداد برامج تدريب أساسية لجميع العاملين في المؤسسة أو الشركة. ومع ذلك، يجب تطوير برامج تدريب لجاهزية التعامل مع هجمات برامج الفدية بما يتناسب مع المؤسسة، ويمكنها من تحقيق أفضل النتائج.

ويضيف ويبر: «يمكن استخدام أدوات محاكاة الأزمات السيبرانية لغايات التدريبات الوهمية التي تتيح ظروفاً تحاكي إلى حد بعيد الظروف الحقيقية، وذلك لتجهيز المستخدم النهائي على التعامل مع هجمات برامج الفدية».