الخليج

اقتصاد, آراء وتحليلات, مقالات

22 سبتمبر 2022 21:44 مساء

كيف يمكن التصدّي لهجمات برامج الفدية؟

الكاتب

نيكولاي سولينغ

***نيكولاي سولينغ**

في خضم عام حافل بانتهاكات الأمن السيبراني حول العالم، تزايدت حدّة هجمات برامج الفدية لتتحول إلى تجارة مربحة في المنطقة، حيث تزايدت احترافيّة منفذيها مع وجود موارد هائلة تحت تصرفهم. فقد وجدت دراسة أجراها زي «Zscaler» سكيلر في عام 2022 أن هجمات برامج الفدية حقّقت نموّاً سنويّاً بنسبة 80% نتيجة ازدياد الاحترافية في هذا المجال وانتشار برامج الفدية كخدمة ransomware-as-a-service.

ويمكن ملاحظة اتجاهات مماثلة في دولة الإمارات العربية المتحدة، حيث تعرّضت 59% من المؤسسات التي شملتها إحدى الدراسات إلى هجمات متعلّقة ببرامج الفدية عام 2021، بعد أن بلغت هذه النسبة 38% عام 2020.

ومع نمو تهديدات برامج الفدية من حيث عددها وتعقيدها، تزداد الحاجة إلى اعتماد استراتيجية أمن سيبراني أكثر استباقية للمؤسسات، حيث لم يعد الاعتماد على منع برامج الفدية كافياً بعد الآن. ويجب أن تركز الشركات على نهج شامل يتضمن الاستثمار في الاستجابة للحوادث والتعافي منها وكذلك في تنفيذ تدابير دفاعية متقدمة.

ويُعتبَر توجّه المؤسسات إلى دفع الفدية أحد أبرز العوامل التي أدت إلى تنامي هجمات برامج الفدية بشكل متزايد يشكل تحدياً شاقاً يتعين على الشركات مجابهته. وفي الواقع، وجدت دراسة حديثة أن 90% من المؤسسات الإماراتية التي دفعت الفدية بعد الهجمة الأولى تم استهدافها مرّةً أخرى. ولعلّ من ضمن الأسباب الأخرى وراء نجاح حملات برامج الفدية هو بساطة تنفيذ هذا النوع من الهجمات والقدرة على تفخيخ الأدوات والأصول الخاصة بالمؤسسة بالبرمجيات الخبيثة.

ويمكن أن تنجم عن برامج الفدية آثار كارثية على الشركات إذا تمّ تركها دون رادع، وهي تشكّل أحد أبرز مصادر القلق للمسؤولين عن الأمن السيبراني في الإمارات العربية المتحدة وحول العالم. فبحسب إحصائيّة لوزارة الخزانة الأمريكية، تبيّن أنّ ما قيمته 5.2 مليار دولار من معاملات البيتكوين كانت مرتبطة بأهمّ 10 أنواع من برامج الفدية عام 2021.

ويتفاقم الخطر مع استمرار تنامي هجمات برامج الفدية من حيث التكتيكات والتنفيذ، وهو ما يجعل الاكتفاء بمنعها بغرض الإلهاء إلى استخدام (DDoS) استراتيجية غير فعّالة بعد الآن. ومع استخدام هجمات حجب الخدمة الموزعة التصيد الاحتيالي والهندسة الاجتماعية لخداع المستخدمين، تترتّب على زيادة احترافيّة برامج الفدية عواقب وخيمة على المؤسسات وعملياتها. ويزداد المشهد تعقيداً بسبب انتشار برامج الفدية كخدمة وتحوّلها إلى نموذج عمل مربح، حيث يتمّ بيع التعليمات البرمجية الخبيثة الجاهزة للمهاجمين السيبرانيين. وتأكيداً على هذا، وجد تقرير أعدّته زي سكيلر أن برامج الفدية كخدمة يتم الآن اعتمادها من قبل 8 أكبر 11 مجموعة من برامج الفدية.

ولعلّ المثير للقلق هو أن تدابير الأمن المؤسسية لا تتطور بالسرعة الكافية لمواكبة مشهد التهديد. فقد كشف تقرير Voice of the CISO الصادر عام 2022 عن شريكنا Proofpoint في أن 53% من كبار مسؤولي أمن المعلومات في الإمارات العربية المتحدة يعطون الأولوية لمنع هجمات برامج الفدية على حساب كشفها والاستجابة لها، وأن 53% منهم ما زالوا لا يتّبعون سياسة لدفع الفدية.

قد لا تنطبق عمليات استرداد المعلومات واستمرارية الأعمال العادية على هجوم نموذجي من برامج الفدية. فقد أصبحت الأنظمة الآن أكثر ترابطاً من السابق، وقد أدى استخراج البيانات من قبل المهاجمين بالفعل إلى تغيير المعادلة من كونها مجرد عملية نسخ احتياطي واسترداد للمعلومات إلى حماية للبيانات.

ولا شكّ في أنّه من الضروري للمؤسسات التركيز بشكل أكبر على استراتيجيات الاستجابة للحوادث واسترداد المعلومات لتقليل تأثير هجمات برامج الفدية. كما يتحتّم عليها إجراء إعادة تقييم كلّي لأساليب استرداد المعلومات المعمول بها، وذلك نظراً إلى أن أنظمة الاسترداد القديمة ليست كافية في مواجهة مشهد التهديد الحديث.

ويمكن أن تفرض حالات برامج الفدية تحدّياً على فرق الأمن الداخلي، وبات بالتالي العمل مع خبير موثوق به وشريك في الأمن السيبراني أمراً شديد الأهمية.

ومع حصد منفّذي الهجمات السيبرانيّة المليارات من جرائمهم، بات من الواضح أن منع الهجمات لم يعد كافياً. وقد حان الوقت لتغيير قواعد اللعبة وبناء المرونة السيبرانيّة من خلال إعادة تشكيل تخطيط الأمن السيبراني الخاص بكل مؤسسة. ويجب على المؤسسات في دولة الإمارات العربية المتحدة تمكين نفسها من خلال الجمع بين الاستجابة والتعافي والوقاية من برامج الفدية، محوّلةً موظفيها إلى خط الدفاع الأول مع تعزيز قوّة مركز عمليات الأمن الخاصّ بها من خلال الذكاء الاصطناعي، إلى جانب التعاون مع شركاء موثوقين لتقليل مخاطر الهجمات الناجحة والتخفيف السريع من ضررها في حال حدوثها. ومع وجود عقلية استباقية واستراتيجيات شاملة، يمكن للشركات إحباط المتسلّلين.

الأمن السيبراني لعبة ثنائية يكفي فيها للمهاجمين أن ينجحوا مرّة واحدة.

*** رئيس قسم التكنولوجيا في «هلب أي جي»**