الخليج

اقتصاد, تقنية وسيارات

12 ديسمبر 2023 17:10 مساء

كاسبرسكي»: انتهاكات الموظفين لأمن شركاتهم تعادل ضرر الاختراق»

دبي: «الخليج»

تعادل انتهاكات الموظفين لسياسات أمن المعلومات في شركاتهم، وفقاً لدراسة حديثة أجرتها «كاسبرسكي»، خطورة هجمات المخترقين الخارجيين. ففي العامين الماضيين، كان سبب 33% في الإمارات من الحوادث السيبرانية في الشركات، انتهاك الموظفين المتعمد للبروتوكول الأمني. ويكاد هذا الرقم يساوي أضرار الشركات الناجمة عن انتهاكات الأمن السيبراني، التي كان الاختراق سبب 36% منها.

ويسود اعتقاد بأن الخطأ البشري هو أحد الأسباب الرئيسية للحوادث السيبرانية في الشركات، غير أن المسألة ليست واضحة، على طريقة الأبيض والأسود. حيث تعتبر حالة الأمن السيبراني في أي شركة أكثر تعقيداً، وتدخل في معادلتها عوامل أكثر من ذلك.

ومع أخذ هذا في الاعتبار، أجرت «كاسبرسكي» دراسة لمعرفة آراء متخصصي أمن تكنولوجيا المعلومات في الشركات الصغيرة والمتوسطة والمنظمات الكبيرة في جميع أنحاء العالم، حول التأثير البشري على أمن الشركات السيبراني، وتهدف الدراسة إلى جمع معلومات حول تأثير مجموعات مختلفة من الأشخاص على الأمن السيبراني، سواء كانوا موظفين داخليين أو أشخاص خارج الشركة.

وكشفت «كاسبرسكي» أنه بالإضافة إلى الأخطاء الحقيقية، كانت انتهاكات الموظفين لسياسة أمن المعلومات من أكبر المشاكل التي تواجه الشركات، حيث ادعى مشاركون من شركات حول العالم أن الإجراءات المتعمدة لخرق قواعد الأمن السيبراني، قام بها كل من الموظفين غير المتخصصين في مجال تكنولوجيا المعلومات وأيضاً المتخصصين في المجال خلال العامين الماضيين.

• انتهاكات

وقال المشاركون إن ارتكاب موظفي أمن تكنولوجيا المعلومات مثل هذه الانتهاكات للسياسة تسبب في 13% من الحوادث السيبرانية في العامين الماضيين. كما تسبب انتهاك متخصصو تكنولوجيا المعلومات الآخرون للبروتوكولات الأمنية بحوالي 23% من هذه الحوادث، أما زملاؤهم من غير المتخصصين في المجال، فتسببوا بحوالي 5% منها.
أما بالنسبة إلى سلوك الموظفين الفردي، فإن المشكلة الأكثر شيوعاً هي أنهم يتعمدون فعل الممنوع، وبالمقابل يفشلون في أداء المطلوب. بالتالي، يرى المشاركون أن 17% من هذه الحوادث في العامين الماضيين، حدثت بسبب استخدام كلمات مرور ضعيفة أو الفشل في تغييرها في الوقت المناسب، وكان سبب انتهاكات الأمن السيبراني الآخر هو زيارة الموظفين لمواقع إلكترونية غير آمنة، والذي تسبب في 29% من الانتهاكات، وأفاد 29% آخرون أنهم واجهوا حوادث، لأن الموظفين لم يقوموا بتحديث برامج نظامهم أو تطبيقاته عندما لزم ذلك.
ومن المقلق أن المشاركين يعترفون أنه إلى جانب هذا السلوك غير المسؤول، فإن 25% من الإجراءات الخبيثة ارتكبها موظفون لتحقيق مصالح شخصية، ومن النتائج الأخرى المثيرة للاهتمام هي أن انتهاكات الموظفين الخبيثة عمداً منلسياسة أمن المعلومات، كانت مشكلة كبيرة نسبياً في شركات الخدمات المالية، وذلك حسب ما أفاد 34% المشاركين في هذا القطاع.

• تهديدات

وقال «أليكسي فوفك»، رئيس قسم أمن المعلومات لدى كاسبرسكي: «إلى جانب تهديدات الأمن السيبراني الخارجية، هناك العديد من العوامل الداخلية، التي يمكن أن تؤدي إلى وقوع حوادث في أي شركة. كما تظهر الإحصائيات، يمكن أن يؤثر الموظفون من أي قسم ـ سواء كانوا متخصصين في تكنولوجيا المعلومات أو غير متخصصين ـ سلباً على أمن الشركات السيبراني عن قصد أو عن غير قصد. ولهذا، من المهم اعتبار طرق تمنع انتهاكات أمن المعلومات عند ضمان الأمان، أي تنفيذ نهج متكامل للأمن السيبراني. وفقاً لأبحاثنا، بالإضافة إلى كون 26% من الحوادث ناجمة عن انتهاك سياسات أمن المعلومات، فإن 38% من الانتهاكات تحدث بسبب أخطاء بشرية. هذه الأرقام مثيرة للقلق، لذا من الضروري ترسيخ ثقافة الأمن السيبراني في الشركة، منذ البداية من خلال تطوير السياسات الأمنية وإنفاذها، فضلاً عن رفع مستوى وعي الموظفين به وبالتالي، سيتعامل الموظفون مع القواعد الأمنية بمسؤولية أكبر وسيفهمون العواقب المحتملة لانتهاكاتهم بوضوح».
وتوصي «كاسبرسكي» للحفاظ على البنية التحتية لشركة آمنة من عواقب انتهاكات الموظفين لسياسات أمن المعلومات، استخدم منتجات الأمن السيبراني بميزات تحكم في التطبيقات والمواقع الإلكترونية والأجهزة، إذ يمكن لهذه الميزة أن تحد من استخدام التطبيقات والمواقع الإلكترونية والأجهزة الطرفية غير المرغوب فيها، ما يقلل من مخاطر الانتهاكات الأمنية، تساعد ميزة التحكم المتقدم في الحالات الشاذة في على منع حدوث الأنشطة الخطيرة المحتملة و«الخارجة عن المألوف»، سواء قام بها المستخدم أو بدأها المهاجم الذي تولى السيطرة على النظام، هناك مخاطر محتملة لنقل بيانات التحكم في كلا الاتجاهين؛ إلى النظام وخارجه.