الخليج

اقتصاد, إدارة وأعمال, فقرة حرة

26 ديسمبر 2023 17:36 مساء

توصية للحد من مخاطر «التكنولوجيا المخالفة» على الشركات 11

وجدت دراسة حديثة أن الشركات معرضة بشكل متزايد لخطر الحوادث السيبرانية، بسبب لجوء بعض موظفيها إلى استخدام منتجات تكنولوجية غير مصرّح بها، دون علم أقسام تكنولوجيا المعلومات، وسط التوجه المتزايد نحو توزيع القوى العاملة جغرافياً. ووفقاً لبحث أجرته شركة «كاسبرسكي»، تعرضت 87% من الشركات في دولة الإمارات لحوادث سيبرانية في العامين الماضيين، وكان 13% منها، بسبب استخدام مثل هذه المنتجات.

وأظهرت دراسة حديثة لـ «كاسبرسكي» أنه خلال العامين الماضيين، عانت 11% من الشركات عالمياً حوادث سيبرانية، بسبب استخدام الموظفين لمنتجات تكنولوجية غير مصرح بها، ويمكن أن تتنوع عواقب استخدام هذه التكنولوجيا، من حيث مستوى الخطورة، ولكن هذه الخطورة موجودة دائماً، سواء كان ذلك تسرّباً لبيانات سرية أو ضرراً ملموساً على الشركات.

- تكنولوجيا غير المصرح بها

تعد تكنولوجيا المعلومات غير المصرح بها جزءاً من البنية التحتية التقنية للشركة، لكنها تقع خارج مجال سيطرة أقسام تكنولوجيا المعلومات وأمن المعلومات، ومنها التطبيقات، والأجهزة، والخدمات السحابية العامة، وما إلى ذلك، ولكن لا يتم استخدامها ضمن سياسات أمن المعلومات في الشركة.

ويمكن أن يؤدي نشر وتشغيل هذه التكنولوجيا إلى تبعات سلبية خطيرة على الشركات. وقد عثرت «كاسبرسكي» على العديد من الحالات التي كشفت أن صناعة تكنولوجيا المعلومات كانت الأكثر تضرراً، حيث تعرضت لنسبة 16% من جميع الحوادث السيبرانية الناتجة عن الاستخدام غير المصرح به للتكنولوجيا، عامي 2022 و2023، وكانت القطاعات الأخرى المتضررة من المشكلة هي البنية التحتية الحيوية ومؤسسات النقل والخدمات اللوجستية، التي شهدت 13% من جميع تلك الحوادث السيبرانية.

وتثبت عمليات اختراق شركة «أوكتا» الأخيرة بوضوح مخاطر استخدام هذه التكنولوجيا، فهذا العام، أعطى أحد موظفي الشركة (الذي كان يستخدم حسابه الشخصي على جوجل على جهاز مملوك للشركة) مصادر التهديد وصولاً غير مصرح به إلى نظام دعم العملاء التابع للشركة عن غير قصد. ما مكّنهم من اختراق ملفات تحتوي على معرّفات الجلسات، التي يمكن استخدامها لشنّ الهجمات. استمرت هذه الحادثة السيبرانية لمدة 20 يوماً، وأثرت في 134 من عملاء الشركة وفقاً لتقريرها.

• تحديد التكنولوجيا المخالفة

يمكن أن تكون هذه التكنولوجيا تطبيقات غير مصدّقة مثبتة على حواسيب الموظفين، أو وحدات تخزين، أو هواتف محمولة، أو حواسيب محمولة غير مسجلة، وما إلى ذلك. ولكن يوجد أيضاً بعض الخيارات الأقل وضوحاً مثل الأجهزة المهجورة المتبقية، بعد تحديث أو إعادة تنظيم البنية التحتية التقنية للشركات. إذ يمكن أن يستخدم الموظفون هذه الأجهزة «خفية»، ما يكوّن نقاط ضعف ستصبح جزءاً من بنية الشركة التحتية عاجلاً أم آجلاً.

كما يحدث غالباً، يمكن لمتخصصي تكنولوجيا المعلومات والمبرمجين أن يطوروا برامج مخصصة لتحسين العمل داخل فرق/أقسام شركاتهم، أو لحل المشكلات الداخلية، ما يجعل العمل أسرع وأكثر كفاءة. ومع ذلك، فهم لا يطلبون دائماً التصريح لاستخدام هذه البرامج من قسم أمن المعلومات، وقد ينتج عن ذلك عواقب وخيمة.

وقال أليكسي فوفك، رئيس قسم أمن المعلومات لدى «كاسبرسكي»: «يعتقد الموظفون الذين يستخدمون التطبيقات، أو الأجهزة، أو الخدمات السحابية التي لم يصرّح لها قسم تكنولوجيا المعلومات، أنه إذا كانت منتجات تكنولوجيا المعلومات هذه تأتي من مزودين موثوقين، فبالتأكيد هي محمية وآمنة. ومع ذلك، يستخدم مزودو المنتجات الخارجيون ما يسمى «نموذج المسؤولية المشتركة» في «شروطهم وأحكامهم». وينص هذا النموذج على أنه بمجرد الموافقة على الشروط والأحكام، يؤكد المستخدمون أنهم سيقومون بإجراء تحديثات منتظمة لهذه المنتجات، وأنهم يتحملون المسؤولية عن الحوادث المتعلقة باستخدامها (بما في ذلك تسرّب بيانات الشركة). ولكن في نهاية المطاف، تحتاج الشركات إلى استخدام أدوات للتحكم في تكنولوجيا المعلومات غير المصرح بها عندما يستخدمها الموظفون. وسيظل قسم أمن المعلومات بحاجة إلى إجراء عمليات فحص منتظمة لشبكة شركتهم الداخلية لتجنب الاستخدام غير المصرح به للأجهزة، والخدمات، والتطبيقات غير الخاضعة للرقابة وغير الآمنة».

بشكل عام، يعد موضوع الاستخدام المنتشر لتكنولوجيا المعلومات غير المصرح بها موضوعاً معقداً، لأن العديد من

الشركات لا توثّق أي عقوبات سيتم تنفيذها على الموظفين نتيجة مخالفتهم سياسات تكنولوجيا المعلومات في هذا الشأن. علاوة على ذلك، من المفترض أن تصبح هذه التكنولوجيا واحدة من أكبر التهديدات لأمن الشركات السيبراني بحلول عام 2025.

عموماً، إن دوافع الموظفين لاستخدام هذه التكنولوجيا ليست خبيثة دائماً، بل تكون على العكس من ذلك في كثير من الأحيان. حيث يستخدمها الموظفون في كثير من الحالات خياراً لتوسيع وظائف المنتجات، التي يستخدمونها في العمل لأنهم يعتقدون أن مجموعة البرامج المسموح بها غير كافية، أو أنهم ببساطة يفضلون استخدام البرنامج المألوف من حواسيبهم.

توصيات الحماية •

توصي كاسبرسكي بما يلي للتقليل من مخاطر استخدام تكنولوجيا المعلومات غير المصرح بها في الشركات:

1. اضمن التعاون بين أقسام الأعمال وتكنولوجيا المعلومات لمناقشة احتياجات الشركة الجديدة بانتظام، وللحصول على تعليقات حول خدمات تكنولوجيا المعلومات المستخدمة من أجل إنشاء خدمات تكنولوجيا معلومات جديدة، وتحسين الخدمات القائمة التي تحتاج إليها الشركات.
2. قم بإجراء جرد منتظم لأصول تكنولوجيا المعلومات في الشركة، وبفحص شبكتك الداخلية، لتجنب ظهور الأجهزة والخدمات غير الخاضعة للتحكم.
3. من الأفضل أن تمنح الموظفين وصولاً محدوداً قدر الإمكان إلى الموارد التي يحتاجون إليها للقيام بعملهم فقط على أجهزتهم.
4. استخدم نظام تحكم في الوصول يسمح فقط للأجهزة المصرح لها بالوصول إلى شبكة الشركة.
5. احرص على تنفيذ برامج تدريبية لتحسين معرفة الموظفين بأمن المعلومات.
6. عند الموظفين، وذلك بتثقيفهم عبر السلوك الآمن على شبكة الإنترنتبادر إلى تعزيز الوعي الأمني.
7. استثمر في البرامج التدريبية الهامة للاختصاصيين في أمن تكنولوجيا المعلومات.
8. استخدم المنتجات والحلول التي تتيح لك التحكم باستخدام تكنولوجيا المعلومات غير المصرح بها داخل شركتك.
9. نفّذ جرداً منتظماً لأصول تكنولوجيا المعلومات للتخلص من ظهور الأجهزة والمعدات غير المستخدمة.
10. قم بتنظيم عملية مركزية لنشر الحلول المكتوبة داخلياً، بحيث يتعرف عليها متخصصو تكنولوجيا المعلومات وأمن المعلومات في الوقت المناسب.
11. احرص على الحد من عمل الموظفين مع خدمات خارجية لطرف ثالث، وإذا استطعتَ فاحظر الوصول إلى موارد تبادل المعلومات السحابية الأكثر شيوعاً.