منوعات, محطات

24 أبريل 2024 18:28 مساء

الهجمات الإلكترونية تهديد سائد للشركات.. وتدابير استباقية

إعداد: مصطفى الزعبي

في العصر الرقمي الحالي، أصبحت الهجمات الإلكترونية تهديداً سائداً للشركات من جميع الأحجام، في حين أن الكبيرة غالباً ما تتصدر عناوين الأخبار لوقوعها ضحية للجرائم الإلكترونية، أصبحت الصغيرة أهدافاً للقراصنة، ومن المهم لأصحاب الأعمال الصغيرة أن يفهموا المخاطر، وأن يتخذوا تدابير استباقية لحماية بياناتهم وعملياتهم الحساسة.

الشركات الصغيرة معرضة بشكل خاص للهجمات الإلكترونية بسبب محدودية الموارد والخبرة في مجال الأمن السيبراني، وغالباً ما ينظر المتسللون إلى الشركات الصغيرة على أنها أهداف سهلة، لأنه قد لا يكون لديهم إجراءات أمنية قوية، ونتيجة لذلك، تتعرض لخسائر مالية، والإضرار بسمعتها، واضطرابات تشغيلية في حالة وقوع هجوم إلكتروني.

ووفقاً للدراسات الحديثة، فإن الهجمات الإلكترونية على الشركات الصغيرة آخذة في الارتفاع، ويستخدم المتسللون

أساليب مختلفة مثل: رسائل البريد الإلكتروني التصيدية وبرامج الفدية والبرامج الضارة، للتسلل إلى شبكات الأعمال الصغيرة وسرقة المعلومات الحساسة، ويمكن أن يكون لهذه الهجمات عواقب مدمرة على الشركات الصغيرة، ما يؤدي إلى اختراق البيانات والاحتيال المالي وحتى إغلاق الأعمال في بعض الحالات.

وباعتبارك مالك شركة صغيرة، من الضروري إعطاء الأولوية للأمن السيبراني وتنفيذ أفضل الممارسات لحماية عملك من التهديدات السيبرانية.

المتخصصة بالأمن السيبراني، فإن «Verizon» ووفقاً لتقرير تحقيقات خرق البيانات لعام 2023 الذي أصدرته شركة الكلفة لكل هجوم ببرامج الفدية، الذي يتميز بنوع من البرامج الضارة المصممة لمنع الوصول إلى نظامٍمتوسط الكمبيوتر حتى يتم دفع مبلغ من المال، وزاد بأكثر من الضعف خلال العامين الماضيين.

وتقدم الشركة خطوات أساسية يمكن اتخاذها لحماية الأعمال الصغيرة، منها الاستثمار في حلول الأمن السيبراني، فكر في الاستثمار ببرامج مكافحة الفيروسات وجدران الحماية وأدوات التشفير لتأمين شبكة عملك وبياناتك.

ومن ضمن الخطوات، يأتي تدريب الموظفين حول أفضل ممارسات الأمن السيبراني، مثل: تجنب رسائل البريد الإلكتروني ومواقع الويب المشبوهة، وتنفيذ سياسات كلمات مرور قوية، وعمل نسخة احتياطية للبيانات ونقلها إلى موقع آمن لمنع فقدان البيانات في حالة وقوع هجوم إلكتروني، بالإضافة إلى تحديث البرامج والأنظمة بأحدث تصحيحات الأمان للحماية من الثغرات الأمنية المعروفة، وتنفيذ أدوات مراقبة الشبكة لاكتشاف الأنشطة المشبوهة على شبكة عملك والرد عليها.

وأكد التقرير، أن الهجمات الإلكترونية تمثل تهديداً متزايداً للشركات الصغيرة، ومن الضروري لأصحاب الأعمال أن يكونوا استباقيين في حماية أعمالهم من المخاطر المحتملة، عبر الاستثمار بحلول الأمن السيبراني، وتدريب الموظفين، والنسخ الاحتياطي للبيانات، وتحديث البرامج، ومراقبة أنشطة الشبكة، وعليه يمكن للشركات الصغيرة التخفيف من المخاطر المرتبطة بالهجمات السيبرانية وحماية عملياتها.