الخليج

اقتصاد, آراء وتحليلات, مقالات

16 نوفمبر 2023 21:55 مساء

ممارسات الأمن السيبراني الفعّالة للشركات

الكاتب

كانديد فيست

*** كانديد فيست**

في عصرنا الرقمي الحالي، يعمل مصطلح «الهجوم السيبراني» كتذكير بالضعف الذي ينتشر في عالمنا المترابط. يشمل هذا المصطلح مجموعة واسعة من الحوادث عبر الإنترنت التي يقوم بها خبراء الجرائم السيبرانية بهدف استغلال الضعاف بطرق متعددة. يمكن أن تشمل هذه الهجمات سرقة البيانات الحساسة، والسعي لتحقيق مكاسب مالية، وشن هجمات إضافية على أجهزة الكمبيوتر الشخصية أو بنية تكنولوجيا المعلومات في الشركات.

يمكن أن تأخذ هذه الهجمات أشكالاً مختلفة، مثل البريد الضار العشوائي، واختراق البرمجيات الضارة، وهجمات الفدية، ومحاولات التصيد الاحتيالي، ومخططات اختراق بريد الشركات، ومحاولة تعطيل خدمة عبر الإنترنت، واستغلال ثغرات البرمجيات التي لم يتم اكتشافها بعد. ويتم تصميم هذه الاستراتيجيات بشكل استراتيجي لاستغلال تعقيدات العالم الرقمي.

تتنوع دوافع الجرائم السيبرانية لاستهداف مؤسسات الحكومة والشركات على حد سواء. الربح المالي هو عامل مهم يدفع المجرمين السيبرانيين إلى التخطيط والتنفيذ الدقيق لسرقة بيانات الأعمال السرية، والمعلومات الشخصية المحددة، وغيرها من البيانات الحساسة مثل بيانات بطاقات الائتمان. غالباً ما يتم استخدام هذه المعلومات المسروقة لطلب فدية، أو سرقة الهوية، أو السرقة المالية المباشرة من الحسابات المالية المخترقة. إضافة إلى ذلك، هناك حالات يسعى فيها الأفراد الذين يدفعهم الانتقام، مثل الموظفين الغاضبين، إلى تعطيل عمليات الشركات كوسيلة للانتقام. يمكن أن تنشأ هذه الهجمات الداخلية من الأفراد الذين يمتلكون معرفة داخلية بأنظمة وإجراءات المؤسسة. وفي حين أن بعض هذه الهجمات الداخلية قد تحدث عن طريق الخطأ، مثل حذف البيانات المهمة عن طريق الخطأ أو استخدام

.برمجيات غير رسمية تحتوي على برامج ضارة لتشويه سمعة وعلامة المؤسسة

وفقاً لتقرير التهديدات السيبرانية لعام 2023 من أكرونيس، فإن الاصطياد الاحتيالي هو الأسلوب الرئيسي الذي يستخدمه المتصيدون لاكتشاف بيانات تسجيل الدخول. خلال النصف الأول من عام 2023 وحده، زاد عدد هجمات الاصطياد الاحتيالي عبر البريد الإلكتروني بنسبة 464% مقارنةً بعام 2022. وخلال نفس الفترة، شهدنا زيادة بنسبة 24% في عدد الهجمات لكل منظمة.

لماذا تُعتبر الشركات الصغيرة والمتوسطة الحجم أهدافاً ضعيفة؟

على العكس من المعتقدات الشائعة، يمكن توجيه الهجمات السيبرانية نحو الشركات الصغيرة والمتوسطة الحجم بشكل واسع. تُعتبر هذه الشركات بالفعل أهدافاً جذابة بسبب ميلها إلى تقدير خطورة التهديدات السيبرانية بشكل غير كافٍ وتجاهل التدابير الأمنية الأساسية. ويضع نقص الإطار الأمني القوي الشركات الصغيرة والمتوسطة الحجم في وضع ضعيف، خاصة أنها تعتمد بشكل كبير على برمجيات موروثة قديمة تفتقر إلى مزايا الأمان الحديثة. وبالتالي، فإنها غير محمية بشكل كافٍ ضد الهجمات المعاصرة، وتواجه تحديات في تثبيت التصحيحات بسرعة. علاوة على ذلك، مع القيود المالية التي تواجهها الشركات الصغيرة والمتوسطة الحجم، من الصعب توظيف خبراء تقنية معلومات ماهرين أو إنشاء أقسام تكنولوجيا معلومات مخصصة. غالباً ما يجد موظفو تقنية المعلومات الداخليون أنفسهم يتعاملون مع مسؤوليات تقنية متعددة ويكافحون من أجل مواكبة التطور المستمر في مجال التهديدات السيبرانية. وتزيد تكاليف التحليل الأمني الباهظة، إضافة إلى ندرة المواهب المتاحة، من تعقيد هذه المشكلة.

وتمتد ندرة الموارد أيضاً إلى تدريب المستخدمين، ما يؤدي إلى عدم تجهيز الموظفين بشكل كاف لاكتشاف الهجمات السيبرانية والوقوع عن غير قصد ضحية لاستراتيجيات خادعة. والمثير للقلق أن 95% من اختراقات الأمن السيبراني يمكن أن يُعزى إلى الخطأ البشري.

لماذا يعد الأمن السيبراني ضرورياً للشركات؟

يواصل المجرمون في القطاع الإلكتروني جهودهم، حيث يزيدون من هجماتهم ويعدلون استراتيجياتهم باستمرار باستخدام أحدث التقنيات. كما أنهم لا يميزون بين المؤسسات بناءً على الحجم أو الموقع أو القطاع، بل بدلاً من ذلك، يسعون إلى العثور على الفرص المثلى لسرقة البيانات والأموال. وقد تكون شركتك عرضة للاختراق في حال عدم توفر تدابير أمن البيانات القوية، ما يترتب عليه تكاليف كبيرة. وتشمل هذه التكاليف نفقات إعادة تأهيل الأنظمة (على سبيل المثال، ترقية الأنظمة، والاستعداد للهجوم التالي، وتنفيذ الدروس المستفادة، وتكاليف الاستجابة للهجوم من خلال الشبكات الداخلية وتصحيح الأضرار، ورسوم الاستشارات للتعافي من الحادث الحالي)، وانخفاض قيمة الشركة في السوق.

علاوة على ذلك، تسبب هذه الحوادث فقدان ثقة العملاء والتغطية الإعلامية السلبية، والضرر لسمعة العلامة التجارية. هناك أيضاً عواقب قانونية وعقوبات لعدم الامتثال لقوانين حماية البيانات مثل لائحة الحماية العامة للبيانات وقانون الخصوصية لعموم المستهلكين. إضافة إلى ذلك، هناك خطر من هجمات تابعة تستغل البيانات المسروقة، بما في ذلك سوء استخدام كلمات المرور، فضلاً عن إمكانية التعرض لابتزاز من قبل المجرمين السيبرانيين الذين يهددون بنشر البيانات.

نائب رئيس البحوث في أكرونيس *