الخليج

اقتصاد, تقنية وسيارات

1 أبريل 2022 21:46 مساء

الأمن السيبراني.. تدابير لحماية الأجهزة والشبكات والبيانات

دبي: أحمد البشير

يشير الأمن السيبراني إلى التدابير المتخذة لحماية الأجهزة والشبكات والبيانات المتصلة بالإنترنت، من الوصول غير المصرح به والاستخدام الإجرامي. وإضافة إلى ذلك، يضمن الأمن السيبراني سرية البيانات وسلامتها وتوافرها على مدار دورة حياتها بالكامل.

وينطبق الأمن السيبراني على البرامج والأجهزة، إضافة إلى المعلومات الموجودة على الإنترنت. ويمكن استخدامه لحماية كل شيء من المعلومات الشخصية إلى الأنظمة الحكومية المعقدة.

وتشمل تدابير الأمن السيبراني منع الهجمات الإلكترونية واكتشافها والاستجابة لها. ويمكن اختراق أي معلومات مخزنة على جهاز متصل بالإنترنت أو نظام كمبيوتر أو شبكة، ومع وجود التدابير المناسبة في مكانها الصحيح، يمكن منع ذلك. ونظراً لأن العالم يعتمد على أجهزة الكمبيوتر أكثر من أي وقت مضى، فقد أصبح الأمن السيبراني ضرورياً.

ويراوح الأمن السيبراني من البسيط إلى المعقد. وكإجراء وقائي أساسي، تأتي معظم الأجهزة مزودة بنظام حماية لمنع القرصنة، ويعد تحديث البرامج طريقة مباشرة أخرى لمنع الهجمات الإلكترونية.

وإذا تعرض نظام للهجوم أو كان معرضاً لخطر الهجوم، فقد يتم اتخاذ تدابير محددة اعتماداً على نوع الهجوم. وتشفير البيانات على سبيل المثال، هو إحدى طرق منع الهجمات، ويمكن لبعض برامج مكافحة الفيروسات اكتشاف نشاط مشبوه عبر الإنترنت، وحظر معظم هجمات البرامج.

وللتأكد من أن النظام آمن، من الضروري فهم المخاطر ونقاط الضعف الكامنة في ذلك الجهاز أو الشبكة المحددة، وما إذا كان بإمكان المتسللين استغلال هذه الثغرات الأمنية أم لا.

ويمكن أن تكون للهجمات الإلكترونية تأثيرات واسعة النطاق في الأفراد والشركات والمؤسسات الحكومية، بما في ذلك الخسائر المالية وسرقة الهوية والإضرار بالسمعة، ويتم تصنيفها حسب الطريقة المستخدمة للهجوم، نذكر منها:

برامج الفدية «رانسوم وير»

وهي برامج خبيثة تقيّد الوصول إلى نظام الحاسوب الذي تصيبه، وتطالب المستخدم بدفع فدية لصانع البرنامج من أجل إمكانية الوصول إلى الملفات، وبعض أنواع هذه البرامج تقوم بتشفير الملفات على القرص الصلب وتعرض

رسائل تطلب من المستخدم الدفع. ولاتزال هذه البرامج من أكبر التهديدات الخبيثة، ومن غير المتوقع أن يتغير هذا الاتجاه في المستقبل المنظور.

لاحتيال المالي

أسهم استبدال أجهزة الصراف الآلي القديمة بنماذج حديثة، واعتماد رقائق إلكترونية في البطاقات المصرفية بدلاً من الشريط المغناطيسي في انخفاض معدل السرقات بنحو طفيف ولفترة وجيزة، إلا أن الهجمات الخبيثة ضد أجهزة الصراف الآلي أصبحت أكثر تطوراً. وهناك عدة طرق لسرقة بيانات البطاقات المصرفية من ضمنها الـ«سكيمينغ»، حيث يتلاعب المجرمون بأجهزة الصراف الآلي لسرقة البيانات من الشرائط الممغنطة للبطاقات، لكن هذه الطريقة أصبحت غير رائجة مؤخراً نتيجة ظهور بطاقات مصرفية تحتوي على رقائق إلكترونية.

إساءة استخدام الشبكة المظلمة (دارك نت)

تستمر الشبكة المظلمة في تمكين المجرمين المتورطين بمجموعة من الأنشطة غير المشروعة مثل بيع البيانات المتعلقة بالحسابات البنكية. وفي الوقت الحالي لا يتوافر سوى دليل ضعيف على أن قدراتهم على تنفيذ هجوم بواسطة الإنترنت تتجاوز التشويه المعتاد للمواقع الإلكترونية، إلا أن إتاحة أدوات وخدمات الجريمة الإلكترونية وشراء السلع المحظورة ومنها الأسلحة على «الدارك نت» يتيح فرصاً كبيرة لتغيير ذلك.

التصيّد

يحدث التصيد الاحتيالي عندما يبدو أن بريداً إلكترونياً أو نصاً قد تم إرساله من مصدر حسن السمعة. والهدف من التصيد الاحتيالي هو خداع المستلم لمشاركة معلومات حساسة مثل تفاصيل بطاقة الائتمان، وبيانات اعتماد تسجيل .الدخول أو لتثبيت برامج ضارة. ويعد التصيّد الاحتيالي أحد أكثر الهجمات شيوعاً على المستهلكين