الخليج

اقتصاد, آراء وتحليلات, مقالات

4 ديسمبر 2022 21:34 مساء

التأمين السيبراني.. هل يُجدي نفعاً؟

الكاتب

أندرياس بيك

*** أندرياس بيك**

دولة الإمارات في طليعة الابتكار التكنولوجي وذلك بفضل قيادة الدولة التي تضع التحول الرقمي في صميم استراتيجيتها الوطنية وتعزيز دور التكنولوجيا في تنمية المجتمع، وتمكين التقدم البشري، والتحول إلى اقتصاد قائم على المعرفة.

وقد احتلت الدولة المرتبة العاشرة عالمياً في الترتيب العام كأفضل دول العالم في «تقرير التنافسية الرقمية العالمية 2021»، الصادر عن «مركز التنافسية العالمي» التابع ل«المعهد الدولي للتنمية الإدارية» بمدينة لوزان السويسرية. يقيس التصنيف قدرة 64 اقتصاداً واستعداده لتبني التقنيات الرقمية واستكشافها كعامل رئيسي للتحول الاقتصادي في الأعمال والحكومة والمجتمع الأوسع.

ولعلّنا إذا ما نظرنا إلى الأمن السيبراني، سنجد أنه أصبح جزءاً لا يتجزأ من التحوّل الرقمي للتكنولوجيا المعلوماتية الذي سرعان ما أصبح هدفاً لمجرمي الإنترنت. أصبحت الهجمات الإلكترونية التي يتمكن من خلالها المحتالون من الإغلاق الرقمي لأنظمة تكنولوجيا المعلومات الحساسة للشركات والحكومة من أجل الضغط عليهم لتقديم فدية تحدث بصورة يومية. ووفقاً لرئيس الأمن السيبراني لحكومة الإمارات، زادت الهجمات السيبرانية في الدولة بنسبة 400 %بعد تفشي جائحة فيروس كورونا، ما أدى إلى خسائر بلغت ما يقارب 700 مليون دولار في غضون ستة أشهر.

إذاً، هل الحل هو شراء التغطية التأمينية ضد القرصنة الإلكترونية؟ أو القدرة على دفع الفدية لاستعادة الوصول إلى أنظمة تكنولوجيا المعلومات وفك تشفير الملفات المسروقة؟ لسوء الحظ، يعتبر دفع الفدية مشكلة خطرة للغاية ونادراً ما تكلل بالنجاح. ليس هناك ما يضمن أن منفذي هذه الهجمات سيوفون بوعودهم، على الرغم من أن دفع الفدية قد يبدو

الطريقة الوحيدة والأمثل لاسترداد المعلومات، فللأسف لا يوجد ما يضمن أن الشركات ستستعيد إمكانية الوصول إلى أنظمتها أو قدرتها على فك تشفير الملفات. تضطر الشركات في بعض الحالات إلى الاكتفاء باسترداد جزء صغير من الملفات المسروقة.

ووفقاً لاستطلاع الرأي العالمي حول مرونة المؤسسات والإنفاق في المستقبل الذي أجرته مؤسسة البيانات الدولية (IDC)، فإن أقل من نسبة 28 % من المشاركين في الاستطلاع تمكنوا من استعادة بياناتهم بعد دفع الفدية.

وهي شركة لتكنولوجيا الأمن «Cybereason» لا ينبغي الوثوق بالأنظمة غير الموثوقة، وفقاً لبحث أجرته شركة السيبراني، فإن 80 % من ضحايا هجمات الفدية الذين دفعوا فدية مسبقاً تعرضوا للهجوم مرة أخرى، ومن بين أولئك الذين تعرضوا لهجمات متكررة، اعتبر نصفهم تقريباً أن الهجوم المتكرر كان على يد نفس المهاجمين ما يشير إلى أن البرمجيات الخبيثة ظلت في الأنظمة والملفات التي تم الاستيلاء عليها.

نادراً ما يغطي التأمين التكلفة الكاملة ضد القرصنة السيبرانية في حين أن التغطية التأمينية ضد القرصنة السيبرانية تعوض الشركات عن تكلفة الهجمات التي تؤثر في أعمالها، فإن القليل فقط من السياسات تغطي استعادة البيانات واستعادة سمعة المؤسسات التجارية. وفي بعض الحالات يستعان بالخبراء لتسهيل مفاوضات الفدية. دعونا أيضاً لا ننسى أن أنظمة التكنولوجيا المعلوماتية يمكن اعتبارها كمسرح جريمة وبالتالي يمكن أن تستغرق التحقيقات وقتاً طويلاً.

الاستثمار في المرونة الإلكترونية هو أفضل «بوليصة تأمين».التأمين ضد القرصنة السيبرانية غير كاف لحماية المؤسسات، ولا يعتبر الهدف منه تغطية الإهمال لتجاهل المخاطر السيبرانية. يجب على المؤسسات في العالم الرقمي أن تفهم أنه لم يعد السؤال عما إذا كان المهاجمون السيبرانيون سيخترقون دفاعاتنا، ولكن متى سيخترقونها وما مقدار الضرر الذي سيحدثونه؟. كل ما يحتاجه المهاجمون هو أن يكونوا ماهرين (أو محظوظين) بما يكفي للاختراق مرة واحدة فقط، وبالتالي فإن الاستثمار في المرونة الإلكترونية أمر بالغ الأهمية.

المرونة الإلكترونية يُقصد بها توقع الهجمات على الخدمات التي يجري تمكينها عبر الإنترنت والحماية منها والتصدي لها والتخلص منها كلياً. فالمرونة الإلكترونية تتجاوز الأمن السيبراني التقليدي وتؤكد الاستمرارية والتعافي من الهجمات لأنه في النهاية سيخترق المهاجمون الدفاعات.

تؤثر الحوادث السيبرانية في المجتمع بأسره، وتنشر حالة عدم اليقين بين المجتمع والحكومات والأسواق على حد سواء. لذلك يجب على القطاعين العام والخاص تبني نهج شامل للدفاع ضد الهجمات السيبرانية وإبقاء المهاجمين السيبرانيين في قيد محكم لتخفيف الضرر الذي يتسببون فيه.

المدير التنفيذي لشركة «كيندريل» في الشرق الأوسط وإفريقيا *