الخليج

اقتصاد, أسواق الإمارات

27 نوفمبر 2022 22:06 مساء

العنصر البشري المسؤول الأول عن الهجمات الإلكترونية والسيبرانية

شدد مسؤولو شركات متخصصة في حماية البيانات على أن العنصر البشري يتحمل المسؤولية عن أغلبية الهجمات الإلكترونية والسيبرانية على المؤسسات والشركات؛ بسبب عدم إدراك العديد من الأساليب الاحتيالية للقراصنة أو القدرة على تحديد مكمن الخطر، ما يعزز من خطورة الهجمات وانتشارها.

وقالو ل «الخليج»: إن معظم قراصنة المعلومات يتّسمون بالكفاءة التقنية والسرعة العالية، كما يخططون للهجمات المعلوماتية بشكل جيد وعلى مدار الوقت، مستهدفين الأخطاء البشرية على وجه الخصوص للإيقاع بالضحايا.

وأشاروا إلى أن القراصنة وخبراء وشركات حماية المعلومات سيواصلون ممارسة أدوارهم لصد الهجمات، وسيعمل المهاجمون دائماً على تغير أساليبهم الاحتيالية في ذات الوقت وربما بصورة أسرع وبشكل مباغت وغير متوقع.

الصورة

قال مجد سنان، مدير عام شركة «تريند مايكرو» في الإمارات: إن سبب أغلبية الهجمات والتهديدات هو العنصر البشري غير المدرب أو الواعي للمخاطر المتعاظمة على البيانات في العالم كله، متوقعاً مواصلة مجموعات فيروسات الفدية وبشكل متزايد استهداف خوادم المعلومات.

وأوضح أن عمليات الكشف عن هجمات فيروسات الفدية كخدمة شهدت ارتفاعاً؛ حيث حقق نموذج فيروسات الفدية كخدمة أرباحاً كبيرة بالنسبة لمطوري فيروسات الفدية والشركات التابعة لهم.

وقال، إن الشركة حجبت واكتشف أكثر من 58 مليون تهديد سيبراني في دولة الإمارات، مع زيادة عالمية بنسبة 75% في هجمات فيروسات الفدية، قامت الشركة بحماية المؤسسات العالمية من 63 مليار تهديد خلال النصف الأول من 2022.

وتابع سنان: كشفت «تريند مايكرو» وحظرت على صعيد دولة الإمارات أكثر من 15 مليون تهديد عبر البريد الإلكتروني، وتصدت لأكثر من 11 مليون هجوم عبر الروابط الضارة، بالإضافة إلى ذلك، تم تحديد وإيقاف ما يقرب من 10 ملايين هجوم برمجيات خبيثة.

وشدد سنان على أن المخاطر المستمرة لبيئات العمل والتعلم عن بُعد والهجينة أيضاً كان لها دور كبير كذلك في زيادة التهديدات، ما يدعو لتبني أفضل الحلول السيبرانية والكوادر البشرية لتأمين وضع مؤسساتهم وشركاتهم المعلوماتية وحماية أصولهم الرقمية، كما أنه ومن الأهمية بمكان توفير بيئة معلوماتية آمنة للموظفين.

وقال: يجب أن تمتلك المؤسسات دراية كبيرة بسطح الهجمات ونهجاً استباقياً لتوقع المخاطر؛ لضمان قدرتها على مواجهة مشهد التهديدات السيبراني الحالي، كما نؤمن بأن منصات الأمن السيبراني المزودة بعدة طبقات أمنية قادرة على دعم البيئات الرقمية للمؤسسات وتأمينها من المخاطر المستقبلية.

وأكد سنان أن هناك مجموعات جديدة من فيروسات الفدية تظهر بشكل يومي، وعلى الرغم من أن الشركات الصغيرة والمتوسطة تعدّ هدفاً أكثر شيوعاً بالنسبة لمجرمي الإنترنت، إلا أن العديد من هذه الجهات الخبيثة عمدت على إطلاق حملاتها الإجرامية على الشركات الكبيرة، علماً أن الثغرات الأمنية التي لم يتم إصلاحها تزيد من مساحة الهجمات على الأجهزة التي دائماً ما تسعى المؤسسات للحفاظ عليها، خصوصاً في ظل نموذج العمل الهجين الذي وسّع من بيئة تكنولوجيا المعلومات؛ حيث أكد 43% من المؤسسات العالمية أن التوسع الكبير لبيئة تكنولوجيا المعلومات يجعل الأمور تخرج عن نطاق السيطرة.

• الأجهزة الأكثر استهدافاً

وقال إيهاب معوض، نائب الرئيس لمنطقة الشرق الأوسط وتركيا وإفريقيا لشركة «فورسكاوت تكنولوجيز»: إن الشركة تضع الكادر البشري القائم على حماية البيانات والمعلومات على رأس الأولويات للمؤسسات الشركات؛ لقدرته على التنبؤ وسرعة رد الفعل تجاه أي مخاطر متوقعة.

وأضاف معوض أن دراسة ل «فورسكاوت تكنولوجيز»، كشفت عن أكثر الأجهزة عرضة لخطر الهجمات الإلكترونية، والتي أظهرت أن أجهزة التخزين الشبكي تعدّ الأكثر عرضة للمخاطر الأمنية، نظراً لنقاط ضعفها سهلة الاستغلال من

جهة، والاتصال بشبكة الإنترنت من جهة أخرى، ما يشجع المجرمين السيبرانيين على استهدافها في إطار هجمات فيروسات الفدية والشبكات وتعدين العملات الرقمية، أو هجمات تدمير البيانات بشكل عام.

وأشار معوض إلى أنه من الضروري جداً تعزيز مستوى الوعي لدى الجهات الحكومية والاقتصادية، وتعريفها بمكامن الضعف في شبكاتها بدقة، وتحديد القطاعات النوعية التي يتم استهدافها باستمرار، والأجهزة المتصلة الأكثر عرضة للخطر.

وقال: وفقاً لدراسة الشركة، يضم قطاع التصنيع أعلى نسبة من الأجهزة الأكثر عرضة للخطر بنسبة 11% من عينة الدراسة، بينما تضم المؤسسات الحكومية والمالية أعلى نسبة مجتمعة من الأجهزة عالية ومتوسطة الخطورة ب43% لدى الجهات الحكومية و37% في المؤسسات المالية، فيما سجل قطاعا الرعاية الصحية والتجزئة الخطورة الأقل؛ حيث بلغت نسبة الأجهزة متوسطة أو عالية الخطورة 20% في قطاع الرعاية الصحية، و 18% في قطاع التجزئة.

وتابع: لم يشهد تصنيف أكثر الأجهزة عرضة للخطر بين القطاعات المختلفة تغيّراً ملحوظاً، ما يبيّن أن جميع المؤسسات تقريباً تعتمد في إنجاز أعمالها على مزيج من تكنولوجيا المعلومات وإنترنت الأشياء والتكنولوجيا التشغيلية (إضافة إلى إنترنت الأشياء الطبية بالنسبة لقطاع الرعاية الصحية)، وأن جميع المؤسسات تقريباً تعاني من ازدياد السطح المعرض لهجمات. ويبقى معدل أجهزة تكنولوجيا المعلومات والتكنولوجيا التشغيلية الأكثر عرضة للخطر، ثابتاً تقريباً في مختلف المناطق، بينما لوحظت فروقات طفيفة في هذه المعدلات بين المناطق في مجال إنترنت الأشياء وفروقات كبيرة في مجال إنترنت الأشياء الطبية.

وأشار معوض إلى سعي الشركة الدائم لمساعدة المؤسسات والشركات على فهم وتقليل المخاطر الناجمة عن التحول الرقمي، والزيادة السريعة في أجهزة إنترنت الأشياء في مختلف المؤسسات، واندماج شبكات تكنولوجيا المعلومات والتكنولوجيا التشغيلية، والذي يشجع على تصاعد نشاط عصابات برمجيات الفدية كخدمة.

وقال: نعمل كذلك على إطلاع المؤسسات والشركات على أفضل السُبل لحماية نفسها ضد الأشكال الجديدة من هجمات برمجيات الفدية القادرة على توظيف أجهزة إنترنت الأشياء، بما فيها كاميرات المراقبة، لنشر هذه البرمجيات.

وقال معوض: لا تزال أجهزة تكنولوجيا المعلومات الهدف الرئيسي للبرمجيات الخبيثة، بما فيها برمجيات الفدية، كما أنها نقطة الاختراق الأولية الرئيسية للمجرمين السيبرانيين، الذين يستغلون نقاط الضعف في الأجهزة المتصلة بالإنترنت، كالخدمات التي تعتمد على أنظمة تشغيل وتطبيقات تجارية تعاني من ثغرات لم يتم إصلاحها، أو يستخدمون تقنيات الهندسة الاجتماعية والتصيد الاحتيالي لخداع الموظفين وجعلهم يشغلون برمجيات خبيثة على حواسيبهم؛ لذا من الأهمية بمكان رفع قدرات الكوادر البشرية للتعامل الاستباقي مع المخاطر وليس بعد حدوثها.

• تسارع التحول الرقمي

فرض (GBM): بدوره أكد هاني نوفل، نائب الرئيس لحلول البنية التحتية الرقمية في شركة الخليج للحاسبات الآلية تسارع وتطور الأعمال بين عشية وضحاها للتوافق مع ديناميكيات السوق الجديدة، وتسريع المبادرات الرقمية وتبني السحابة الهجينة، ضرورة تعزيز استراتيجيات الأمن الإلكتروني، ويتمثل دور المؤسسات والشركات الحتمي في مواكبة تغير أولويات وخريطة المخاطر ومعرفة استراتيجيات الأمان المتبعة خلال سعيهم للتحول الرقمي.

وأوضح نوفل أن استطلاعاً أجرته الشركة مؤخراً أكد أن مخاطر الأمن الإلكتروني حصلت بسبب توسع القوى العاملة الموزعة خلال «كوفيد-19»، حيث واجهت نحو نصف المؤسسات في منطقة الخليج العربي زيادة في عدد الهجمات على بنيتها التحتية الرقمية.

وقد ركزت المؤسسات التي شملها الاستطلاع على ضرورة حماية بياناتها في بناء الثقة مع العملاء، وأن 84% من تلك المؤسسات وضعت خططها للاستثمار في أمن البيانات خلال العام التالي.

وكشفت نسبة 34% من المؤسسات التي شملها الاستطلاع، عن أنها اشتكت من عدم فاعلية إجراءات أمن السحابة الخاصة، فقد واجه 66% منهم صعوبات في تقنيات إدارة هويات ووصول المستخدمين ضمن بيئات سحابية هجينة.

وأضاف نوفل، إلى جانب ارتفاع الطلب على خدمات ونظم الحوسبة السحابية، أنه قد حظيت حلول الأمن الإلكتروني واتباع أفضل الممارسات للتخفيف من الهجمات المحتملة على الأولوية الكبرى، لا سيما مع عمل الموظفين عن بُعد ليصبحوا أكثر عرضة لبرامج الابتزاز والفدية، والروابط الضارة، وهجمات التصيد الاحتيالي.

وقد تعرّضت الشركات التي خاضت رحلات التحول الرقمي إلى مخاطر أمنية كبيرة، وسرقات، وعمليات احتيال، وبرامج الفدية، والعديد من أنواع الهجمات الإلكترونية الأخرى.

وشدد نوفل على أن معالم المستقبل الرقمي قد باتت واضحةً تماماً في دولة الإمارات؛ حيث تسعى المؤسسات والشركات الإماراتية نحو التحول الرقمي لبلوغ أهدافها، وقد سارعت في دمج تقنيات جديدة مثل الذكاء الاصطناعي وتعلّم الآلة، وتقنية «بلوك تشين»، والحوسبة الطرفية لدعم الأمان والامتثال والتشغيل الآلي.

وشهدت المنطقة على مدى العقد الماضي إصدار عدد من القوانين الجديدة حول تنظيم إدارة البيانات، ورغم كل ذلك، فإن الحكومات لا تستطيع بمفردها الحفاظ على الأمن الإلكتروني العام، ولذلك يتوجب على القطاعين العام والخاص أن يتعاونا لمواجهة الهجمات الإلكترونية والحد من الخسائر، ويتطلب تحقيق هذا الهدف الشراكة بين الكيانات التجارية والحكومات والأفراد.

• أمير كنعان : تغير أساليب العمل

أمير كنعان

قال أمير كنعان، المدير التنفيذي لمنطقة الشرق الأوسط وتركيا وإفريقيا في «كاسبرسكي»: نعتقد بأن الوقت قد حان لإلقاء نظرة متجدّدة على طريقة تصوّر الأمن السيبراني وتطبيقه، وإن فترة تفشي جائحة «كوفيد-19» قد غيرت طريقة العمل في العالم وقدمت أساليب مثل العمل عن بعد والعمل الهجين، وهي الآن أساليب عمل مفضلة للغاية بين الموظفين لأسباب مختلفة؛ لذا من الضروري العمل على الاحتفاظ بالمواهب والكوادر البشرية الجديدة أو جذبها للعمل لتعزيز منظومة حماية المعلومات.

وأضاف كنعان، خلال وبعد الجائحة، كانت أيضاً فترة تعلم لمجرمي الإنترنت، وتم استغلال هذه الخيارات عند تغيير سلوك لدى الأشخاص. وعلى سبيل المثال، سمحت الشركات للموظفين بالاتصال بالبنية التحتية لتكنولوجيا

المعلومات للمكتب من الأجهزة المنزلية دون الحماية المناسبة، وأدى ذلك إلى زيادة الهجمات ضد بروتوكولات سطح المكتب البعيد؛ لأنها تم تكوينها بشكل غير صحيح وكان على الموظفين الذين يعملون عن بُعد استخدام هذه البروتوكولات للاتصال بشبكات وخوادم الشركة.

وأكد كنعان أن التهديدات المتقدمة والموجّهة ستبقى مصدر تهديد للمؤسسات والشركات، ليس فقط في دولة الإمارات وحدها، بل على مستوى العالم.

• إميل أبو صالح: إهمال المهنيين

إميل أبو صالح

قال إميل أبو صالح، المدير الإقليمي لشركة «بروف بوينت»: «تشكل الهجمات الإلكترونية التي تتمحور حول الأفراد أكبر خطر على الشركات والعاملين في الإمارات والسعودية، لكن الشركات تتخذ الخطوات الصحيحة حالياً لتعزيز وعي الموظفين بالأمن السيبراني.

ومع ذلك، فإن البرنامج التدريبي الفعال والشامل للتوعية بالأمن السيبراني الذي يتكيف مع مشهد التهديدات المتطور باستمرار يعد أمراً أساسياً؛ لأن الموظفين يصلون بشكل متزايد إلى البيانات التنظيمية من منصات وأجهزة ومواقع متعددة، لذلك لم تكن حماية البيانات أكثر أهمية من أي وقت مضى.

وأضاف أبو صالح، كشفت دراسة إحصائية، أجرتها «بروف بوينت»، عن أن المهنيين العاملين في المنطقة يعرضون الشركات وأصحاب عملهم للخطر، وذلك بسبب إهمالهم في مجال الأمن السيبراني، والذي يغذيه اعتماد نماذج العمل الهجينة بعد الجائحة؛ حيث كان العديد من الموظفين مسؤولين عن فقدان البيانات لمؤسستهم، ويشعر 17٪ فقط من الموظفين في دولة الإمارات و 14٪ في المملكة العربية السعودية بأنهم يتحملون مسؤولية الأمن السيبراني في مؤسساتهم، ونوهت الدراسة بأن العديد من الموظفين في المنطقة أظهروا سلوكيات محفوفة بالمخاطر يمكن أن تساعد في شن هجمات إلكترونية.

وقال أبوصالح: يجب أن يدرك الموظفون أنهم يلعبون دوراً مهماً في التصدي إلى انتهاك وفقدان البيانات، ومع تطور نماذج العمل التقليدية لم تعد الطرق القديمة لحماية البيانات سداً منيعاً أمام الهجمات السيبرانية. سوف تحتاج المؤسسات إلى العمل جنباً إلى جنب مع موظفيها للارتقاء بمستوى أنظمة الأمن السيبراني.

• حيدر نظام: سلوك العاملين حاسم للحماية

حيدر نظام

أكد حيدر نظام، رئيس زوهو في منطقة الشرق الأوسط وإفريقيا، أن سلوك العاملين بإدارات المعلومات يظل أحد العوامل الحاسمة لحماية البيانات، ولتجنب الأخطاء البشرية، التي عادة ما تقود إلى فقدان أو تعريض البيانات للخطر،

سواء عمداً أو عن غير قصد، يجب تطبيق سياسات وإجراءات أكثر صرامة، والتي من شأنها أن تكمّل العمليات الفعالة والآمنة المحددة للتعامل مع البيانات.

وأضاف، تستهدفت المنطقة بشكل مكثف من قبل قراصنة المعلومات، عبر برامج التصيد الاحتيالي والفدية، وكمنطقة تهيمن عليها في الأغلب قطاعات: الطاقة والرعاية الصحية والصناعات المالية، تصبح البيانات أكثر حساسية وأهمية، وتتطلب أعلى مستويات الأمان والموثوقية لحمايتها.

وتابع نظام: توجد العديد من بروتوكولات الأمان التي يجب على الشركات الالتزام بها، بما في ذلك تبني «نموذج الثقة الصفرية»، وتفعيل خاصية «المصادقة متعددة العوامل»، و«أمن نقاط النهاية»، والمحافظة على رفع درجة الوعي بأهمية الأمان بين موظفي المؤسسة، وتثقيفهم بشأن الممارسات الإلكترونية غير الآمنة.

وأكد نظام أن التهديدات السيبرانية تتطور بشكل مستمر، وتجد ثغرات كثيرة جديدة، مما يضع ضغطاً إضافياً على فرق تكنولوجيا المعلومات، لإجراء التحسينات بشكل متواصل، وتهيئة البنية التحتية، وإجراء الاختبارات والتقييمات بصورة متكررة.

تعد الاختبارات الأمنية في غاية الأهمية لضمان بقاء البيانات والشبكات آمنة جيداً، ليصبح بالإمكان اكتشاف أية برامج ضارة أو عمليات إدخال غير متوقعة وغير مصرّح لها بشكل مبكر والتعامل معها فورياً. بالإضافة إلى ذلك، يجب بذل جهود حثيثة لرفع مستوى الوعي بين المستخدمين، للمساعدة على إنشاء إطار أمني شامل وأكثر صرامة.