الخليج

اقتصاد, تقنية وسيارات

28 مارس 2023 23:21 مساء

الجرائم الإلكترونية والسيبرانية تنتقل إلى الاحترافية

دبي: حمدي سعد

شدد مسؤولو شركات على أن الجرائم الإلكترونية باتت أكثر تنظيماً واحترافية عن ذي قبل؛ إذ إنها تقوم بعمل دراسات وتوظيف خبرات بشرية ماهرة وتقنيات توازي قدرات شركات الأمن السيبراني والإلكتروني في الكفاءة والتخطيط الطويل، لارتكاب الهجمات، واستهداف المؤسسات والشركات والأفراد كذلك.

وقال المسؤولون ل «الخليج»: إن ازدياد الارتباط بشبكة الإنترنت حول العالم، والارتفاع المهول في أعداد الأجهزة المرتبطة بهذه الشبكات وأجهزة «إنترنت الأشياء» أسهم في اتساع مسرح الجرائم الإلكترونية والسيبرانية، ما يؤكد أن الصراع سيستمر بين القراصنة وشركات الحماية.

وأكدوا مواصلة التعاون بين كافة أطراف الحماية من الهجمات الإلكترونية والسيبرانية، والعمل وفق إجراءات استباقية ورفع كفاءة الكوادر البشرية والاستثمار في الحلول، لمواجهة موجات جديدة من الهجمات بصورة مستمرة، فضلاً عن

.الاستعانة بقدرات وخبرات المؤسسات الحكومية والشركات المتخصصة في هذا المجال

طارق حلواني

قال طارق حلواني، المدير التنفيذي لحلول الشركات في مايكروسوفت الإمارات: لا يزال تحدي الأمن الإلكتروني والسيبراني ماثلاً؛ لذا يتطلب الأمر سرعة كبيرة في الحركة للتطوير واستخدام أساليب جديدة للحماية من الهجمات التي باتت أكثر احترافية، مستخدمة الذكاء الاصطناعي وغيره من التقنيات الحديثة والتي كان آخرها تطبيقات «شات جيب .ي تي» وبرمجيات «التزييف العميق» وغيرها

وأضاف حلواني أن من الضروري مواصلة العمل على رفع جاهزية الكوادر البشرية وأنظمة الحماية والاستعانة بالبنى التحتية القوية، ممثلة في منصات الحوسبة السحابية وغيرها والتي توفر ملاذاً آمناً إلى حد كبير للمؤسسات والشركات .من الهجمات السيبرانية

.وتابع حلواني: أن التهديدات الإلكترونية أصبحت أولوية

رفع الجاهزية

أشرف كحيل

وأكد أشرف كحيل، مدير تطوير الأعمال الإقليمي في شركة «غروب-آي بي»: أصبحت قرصنة المعلومات نشاطاً اقتصادياً منظماً على مستوى العالم، يمارسها أشخاص لديهم خبرات وكفاءات بشرية وقدرات تقنية فائقة، كما يقومون .في بعض الأحيان بتبادل الخبرات فيما بينهم، لإنجاح أهدافهم وخططهم الإجرامية وجني الأموال

وأضاف كحيل: يقابل ذلك ضعف في العديد من المؤسسات والشركات من حيث الجاهزية وتوافر الكوادر البشرية المؤهلة للتعامل الاستباقي أو الآني مع الهجمات المستمرة التي لا تتوقف وتتغير أشكالها حسب كل مؤسسة أو شركة أو .غيرها من الجهات المستهدفة

وتابع كحيل: إن من أبرز التغيرات في قطاع الأمن الإلكتروني والسيبراني حالياً في الإمارات أنه يشهد وجود ثقافة ووعي كبيرين لدى العديد من العملاء؛ حيث يقومون بوضع متطلباتهم للأمن المعلوماتي والسيبراني حسب قطاعاتهم، لا سيما في القطاعات الحيوية مثل: المؤسسات الحكومية التي تمتلك معلومات حساسة أو في قطاعات أبرزها: النفط والغاز .والمالية

تضاعف الهجمات

رولان الدكاش

وقال رولان الدكاش، مدير الأنظمة السيبرانية في «كراودسترايك»: تطور منظومات الهجمات الإلكترونية والمعلوماتية حول العالم من نفسها بصورة متسارعة ومخيفة، فيما تشير الدلائل كافة إلى تضاعف هذه الهجمات السيبرانية والاختراقات المعلوماتية وسيتضاعف سوق الأنظمة والحلول من رقمين خلال 3 سنوات.

وأضاف: مع استمرار مجرمي الإنترنت ومجموعات القرصنة في مختلف أنحاء العالم في التطور والتعامل مع أنظمة الحماية، فمن الأهمية بمكان أن تعمل المؤسسات والشركات على وجه أسرع عبر تطوير قدراتها في مواجهة هذه التهديدات، عبر دمج تقنيات وحلول واستراتيجيات جديدة.

وأشار الدكاش، إلى أن القطاعات الأكثر استهدافاً مثل: «الطاقة والمالية والتجزئة» لا تزال ضمن أولويات القراصنة، مشيراً إلى توافر مجموعة من الأدوات القادرة على اكتشاف التهديدات بدقة، وتوفير حماية آلية عبر أجهزة استشعار تعمل على الأنظمة والشبكات، ما يعزز الحماية السيبرانية.

نقاط الضعف

أسامة رضوان

بدوره، قال أسامة رضوان، مدير المبيعات في الشرق الأوسط لدى نوزومي نتووركس: تمثل أجهزة «إنترنت الأشياء» أرضية خصبة لقراصنة المعلومات حالياً، كونها ترتبط بالبنية التحتية والشبكات الصناعية للمؤسسات الحكومية والخاصة، ما يرفع من التهديدات السيبرانية، وقد شهد عام 2022 هجمات غير مسبوقة، استهدفت قطاع التقنيات التشغيلية وأمن إنترنت الأشياء وأمن أنظمة التحكم الصناعي.

وأضاف: إن هجمات طلب الفدية والتهديدات التي واجهت التقنيات التشغيلية وأنظمة التحكم الصناعي، والإعلانات عن نقاط الضعف وغيرها ما زالت منتشرة بشكل كبير؛ حيث يكشف أحدث تقارير الشركة حول أمن التقنيات التشغيلية وإنترنت الأشياء أن قطاعات النفط والغاز، والرعاية الصحية، والمواصلات، والتجزئة هي مجرد أمثلة على القطاعات الصناعية التي ازدادت فيها الهجمات خلال 2022.

العالم أكثر تشابكاً

يانيف فاردي

وأشار يانيف فاردي، الرئيس التنفيذي في شركة «كلاروتي» إلى أن العالم أصبح أكثر تشابكاً، ونتيجة لذلك، يوجد طلب متزايد على الحلول المصممة لحماية الأنظمة الفيزيائية الإلكترونية، وعاماً بعد عام، نشهد زيادة في نقاط الضعف التي تؤثر في البيئات الصناعية والرعاية الصحية والتجارية، وفي كل عام، يصبح مجرمو الإنترنت أكثر ذكاءً واستراتيجية في جهودهم؛ وذلك لاستغلالها من خلال برامج الفدية وأنواع أخرى من الهجمات الإلكترونية. نتيجة للهجوم المستهدف، قد تواجه المنظمات أوقات توقف مكلفة، فضلاً عن التأثير السلبي على النتائج الحرجة مثل رعاية المرضى وسلامة عملية التصنيع.

وقال فاردي: بالتأكيد توجد فجوة في المهارات الخاصة بالأمن السيبراني، لكن لا يزال هناك عدد من الخطوات التي يمكن للمنظمات اتخاذها مثل التدريب المتبادل لموظفي أمن تكنولوجيا المعلومات.

هاني نوفل: 10% ارتفاع الإنفاق على أمن المعلومات

قال هاني نوفل، نائب الرئيس لحلول البنية التحتية الرقمية في شركة الخليج للحاسبات الآلية: نتوقع أن يرتفع الإنفاق على حلول وأنظمة أمن البيانات في الإمارات خلال عام 2023 بنحو 11% لعدة عوامل؛ أهمها التحول الرقمي، بسبب الجائحة وتوجه الأعمال للاعتماد على الحوسبة وغيرها.

وعن أبرز توجهات قطاع الأمن الإلكتروني والسيبراني 2023 أوضح نوفل أن القطاع في السنوات المقبلة سيوجه تركيزه على خدمات الأمن المدارة والتحول لبرامج الحماية المتكاملة.