خلال الأشهر الـ 12 السابقة

«بوز ألن هاملتون»: نسبة الشركات المتعرضة لهجوم سيبراني في الخليج 41 في المئة


زياد نصر الله


جاي تاونسند

أشارت مصادر بوز ألن هاملتون الى أنه مع استمرار تطور مشهد التهديدات السيبرانية، لا بد أن تنتبه الحكومات والقطاع الخاص لبعض المجالات الأكثر تعرّضا للمخاطر المتزايدة في الفضاء الالكتروني أو ما يعرف بالسيبراتي.وتشهد بيئة التهديدات السيبرانية في الشرق الأوسط توسّعا سريعا، حيث تتزايد الهجمات ضد بلدان المنطقة والمقيمين فيها من حيث الكم والفعالية والتعقيد. فاستنادا الى مسح كان قد أجري في مايو 2018، بلغت نسبة الشركات العاملة في منطقة الخليج والمتعرضة لهجوم سيبراني في الأشهر الـ 12 السابقة حوالي 41٪، اي بزيادة نسبتها 46٪ مقارنة بأرقام عام 2016.

أن الهجمات السيبرانية ذات الخطورة الشديدة تحصل ايضا بوتيرة متزايدة مع اكتشاف القراصنة لطرق جديدة يخترقون من خلالها الحواجز الأمنية (كجدران الحماية الالكترونية المعقدة) والأنظمة الأمنية، بالرغم من الجهود المستمرّة التي يقوم بها القطاع العام والتي ترمي الى تسريع عملية تطوير قدرات الأمن السيبراني. وعلى وجه الخصوص، فإن التهديدات السيبرانية لأنظمة التحكم الصناعية تولد المزيد من القلق في المنطقة بعد أن أشار العديد من التقارير في مارس إلى وقوف القراصنة وراء محاولة تفجير في مصنع للبتروكيماويات في المملكة العربية السعودية في العام الماضي.وأشار زياد انطوان نصر الله، مدير مشاريع في شركة بوز ألن هاملتون في منطقة الشرق الأوسط وشمال أفريقيا، الى أن «بيئة التهديدات السيبرانية المتطورة في منطقتنا وفي سائر أنحاء العالم تتطلب من الحكومات والأفراد إعطاء أولوية خاصة لاتخاذ الإجراءات والتدابير اللازمة لحماية أنفسهم من الهجمات. ويتطلب هذا الأمر تحديد الثغرات الأمنية التي يمكن للقراصنة استغلالها عبر كامل سلسلة التوريد، وفي الوقت عينه، ينبغي على الحكومات والمؤسسات أن تستثمر في إجراءات جدية للامن السيبراني أو للحماية من هجمات خطرة يمكن أن تعرض عملياتها كافة لمخاطر جمة».من جهته، أكد جاي تاونسند، مدير مشاريع في بوز ألن هاملتون في منطقة الشرق الأوسط وشمال أفريقيا، هذا الواقع مشيرا الى أن «دول الخليج تدرك التهديد السيبراني المتزايد للحكومات والشركات، وحيث أن التحول الرقمي الذي تشهده الاقتصادات في جميع انحاء المنطقة بتبنيها تقنيات رقمية وتطبيقها خدمات إلكترونية من شانه أن يزيد من التهديدات لأمن البيانات الشخصية، فإن مصلحة دول الخليج تقتضي اتخاذ كافة الإجراءات لتامين الشبكات كما البيانات السرية التي يمكن للقراصنة استغلالها».

وكانت بوز ألن هاملتون قد حدّدت سبعة تطاقات رئيسية من الفضاء السيبراني قد تواجه فيها بلدان الخليج هجمات كبيرة في المستقبل:

1. الهجوم على سلسلة التوريد عبر اختراق المورّدين

ان إدارة سلسلة التوريد هي جزء اساسي لنجاح اية مؤسسة، وبالتالي، يمكن ان تؤدي عمليات التسلل الناجحة الى منصات برامج الموردين في سلاسل التوريد الضخمة إلى مخاطر في عدد لا يحصى من الشركات بشكل متزامن. ويعتبر هجوم NotPetya والذي قام فيه القراصنة بتخريب برنامج الضرائب الأوكراني وإرسال تحديثات خاطئة انتشرت عبر الشبكات المخترقة وأصابت نقاط الاستخدام النهائية ببرمجيات خبيثة، المثال الأبرز حتى الآن. لقد تسبّب هذا الهجوم باضطرابات وأضرار عالمية بلغت تكاليفها حوالي 10 مليارات دولار أميركي. وبينما بقيت دول الخليج بمنأى إلى حد كبير، فإن العديد من المؤسسات ما زال يفتقر إلى وضوح الرؤية فيما يخص أمن موردييها، مما يجعلها عرضة لتهديدات ومخاطر غير معروفة.

2. استهداف انظمة التحكم الصناعية

تمثل انظمة التحكم الصناعية مجموعة متنوعة من التقنيات التي تقوم بإدارة وأتمتة أجزاء كبيرة من المجتمع، بما في ذلك شبكات الكهرباء وعمليات النفط والغاز والتصنيع وغيرها. ومن الممكن أن تكون الهجمات على أنظمة التحكم الصناعية مدمّرة كونها قد تؤدي إلى توقف العمليات وحتى التسبب باضرار مادية. وبالفعل، فإن مصنع البتروكيماويات المذكور سالفا في المملكة العربية السعودية كان قد نجا من أضرار مادية ضخمة ناجمة عن الهجوم السيبراني فقط بسبب خطا في رمز القراصنة.

3. مهاجمة أدوات ومنصات برمجيات تابعة لجهات خارجية ((Third-party مع تضوج عمليات تطوير النظم، تهدف منصات البرمجيات إلى توفير أفضل فائدة للمستهلكين والمطورين. العديد من هذه المنصات سهل الاستخدام ويمكن تعديله وفق الطلب ببساطة، مما يزيد من سهولة تعرّض هذه المنصات للاختراق من قبل القراصنة الذين يسعون لنشر الشيفرات الخبيثة عبر التطبيقات التي يقومون بإنشائها. وبالفعل، فقد حصلت حوادث مشابهة، حيث قامت حملتان على الأقل بتوزيع شيفرات خبيثة في مكتبات تطوير iOS و Android والتطبيقات التي تتضمنها. ومع تطور عملية تطوير النظم في الشرق الأوسط، ينبغي أن تكون المؤسسات حذرة من مخاطر قيام القراصنة بتعريض مكتبات البرمجيات وأدوات تطوير النظم التابعة لجهات خارجية لاختراقات من هذا النوع.

4. استغلال بيئة العملة المشفرة حديثة العهد

في وقت سابق من هذا العام، سرق القراصنة حوالي 532.6 مليون دولار أميركي من مؤسسة لتحويل العملة المشفرة في طوكيو، مما أدى إلى إعادة إطلاق النقاشات حول الأمن والحماية التنظيمية في السوق الناشئة بالنسبة للعملات المشفرة مثل بيتكوينBitcoin . وفيما يفكر المشرّعون الماليون في دولة الإمارات بوضع قوانين خاصة بالعملة المشفّرة وتطوير إطار عمل مع شركات القطاع والهيئات المرتبطة بنشاطها، فإن البيئة التي تفتقر إلى معايير حماية أمنية عالمية صارمة تظل هدفا مربحا للقراصنة، خصوصا مع استمرار توسّع عدد فئات العملة المشفرة وتبادلها.

5. خرق القواعد الضخمة

للبيانات التابعة للحكومات والقطاعات في عالم يزداد فيه الاعتماد على التقنية الرقمية، غالبا ما تكون البيانات الشخصية الحساسة أهدافا مهمة من قبل المجرمين في البيئة السيبرانية ومجموعات القراصنة المنظمة المدعومة من الدول. لقد أدت الخروقات التي تم اكتشافها في مكتب إدارة شؤون الموظفين في الولايات المتحدة في عام 2015، ومكتب الائتمان Equifax في عام 2017 الى فقدان معلومات حساسة عن مئات الملايين من الأشخاص، وهي معلومات يمكن أن يبيعها أو يستغلها المجرمون السيبرانيون كما يمكن للقراصنة المدعومين من الدول استخدامها لبناء قواعد مهمة لبيانات الاستخبارات. وقد يكون الخرق الامني الأخير لـ SingHealth، أكبر مجموعة من مؤسسات الرعاية الصحية في سنغافورة، هو تذكير آخر بأن جميع البيانات تظل عرضة للسرقة والاستغلال. وفيما تسعى دول الخليج مثل المملكة العربية السعودية والإمارات العربية المتحدة إلى رقمنة اقتصاداتها وقطاعاتها الصناعية بأكملها، كالسجلات الصحية الإلكترونية على سبيل المثال، تشكل قواعد البيانات المتزايدة بفعل التحول الرقمي أهدافا جديدة للقراصنة.

6. استخدام القرصنة بنظام الفدية لتخريب الاقتصادات

ان التهديدات الامنية الخاصة بنظام الفدية، وهي اداة إجرامية انتشرت عبر الإنترنت لعدة سنوات، مستمرّة في التطور وتشمل كلا من الأفراد والاقتصادات، على المستوى الفردي، لا تزال حملات القرصنة بنظام الفدية تحقق عائدات كبيرة للقراصنة – ففي الإمارات وحدها، تم خسارة حوالي 1.1 مليار دولار أميركي من افراد المجتمع لأنشطة الجريمة السيبرانية في عام 2017، وشكلت هجمات الفدية جزءا كبيرا من هذه الخسائر. لكن ما هو أكثر خطورة يتمثل في سيناريوهات يهاجم فيها القراصنة شبكات حكومية أو قطاعية يحتمل أن تؤدي إلى تعطيل العمليات. على سبيل المثال، في الولايات المتحدة هذا العام، تم ضرب مدينة أتلانتا بجرتومة SamSam مقابل فدية، مما اضطر العديد من الشركات في المدينة للعودة الى الورق لإدارة عملياتها التجارية. وبالفعل، تشير بعض التقديرات الى أن قطاع الأعمال في المنطقة يمكن أن يواجه خسارات تصل الى 1 مليون دولار أميركي لكل حادثة من الهجمات بنظام الفدية تستهدف شبكاتها. وفي جميع أنحاء منطقة الخليج، يؤدي إطلاق برامج الحكومة الذكية وأنظمة التشغيل الآلي، مثل البوابات الإلكترونية في مطارات أبوظبي ودبي، إلى استحداث نقاط ضعف محتملة تمكّن الهجمات من استغلالها لاحداث اضطرابات كبيرة.

7. استهداف الاحداث والمناسبات البارزة

وختاما، ان المناسبات والأحداث الكبيرة لا تؤدي فقط الى جذب الحشود الضخمة بل ايضا الى لفت اهتمام القراصنة. وقد شهد أكبر حدثين أقيما في عام 2018 حتى الآن، وهما الأولمبياد الشتوي في كوريا الجنوبية وكأس العالم في روسيا، كما هائلا من الهجمات السيبرانية: فقد تسبب الهجوم الالكتروني في الأولمبياد في إحداث اضطرابات في حفل الافتتاح بينما زعمت روسيا أنها واجهت 25 مليون هجمة سيبرانية خلال احداث كأس العالم. وكذلك، فإن معرض إكسبو 2020 في دبي قد يجذب اهتماما مماثلا بالحدث وبدولة الإمارات على نطاق واسع، من قبل القراصنة.

خلال الاجتماع الوزاري للمجلس الاقتصادي والاجتماعي بجامعة الدول العربية

نصار: اتفاقية استثمار عربية جديدة تلائم التطورات الدولية...قريباً


عمرو نصار

ذكر وزير التجارة والصناعة المصري أن الاجتماع الوزاري للمجلس الاقتصادي والاجتماعي بجامعة الدول العربية أقر إعداد اتفاقية استثمار عربية جديدة تلائم التطورات الدولية وتوفر بيئة مناسبة لجذب الاستثمارات إلى المنطقة العربية.

وقال عمرو نصار، في بيان صادر، أمس الخميس، إن الاتفاقية الجديدة تأتي في إطار قيام عدد من الدول ومنها مصر بتطوير قوانين الاستثمار بها، مؤكداً أن الاتفاقية ستسهم في تطوير مناخ الاستثمار في الدول العربية من خلال الترويج للفرص الاستثمارية بدول المنطقة.

جاءت تصريحات نصار خلال رئاسته وفد مصر المشارك باجتماعات الدورة الـ102 للمجلس الاقتصادي والاجتماعي بجامعة الدول العربية.

وشوه الوزير بأن جدول أعمال الاجتماعات ناقش عدداً من الموضوعات المتعلقة بالعمل الاقتصادي والاجتماعي العربي المشترك، منها متابعة منطقة التجارة الحرة العربية الكبرى التي تضم في عضويتها 18 دولة عربية.وتناول الاجتماع ضرورة اعتماد آلية لتحقيق الشفافية في إطار الاتفاقية، وكذا آلية لالتزام الدول بقرارات المجلس، وذلك بهدف الحد من معوقات التجارة العربية بين الدول الأعضاء.

وتابعت الاجتماعات تطورات الاتحاد الجمركي العربي، المقرر إقامته في دولة الكويت.

وأوضح نصار أن الاجتماعات أقرت الميثاق العربي الاسترشادي لتطوير قطاع المشروعات المتوسطة والصغيرة ومتناهية الصغر للدول العربية، كما تابعت تنفيذ القرارات الصادرة عن القمة العربية الافريقية وخطة التعاون المشترك والتي تشمل مشروعات عربية أفريقية مشتركة ذات أولوية من الجانبين.

وأشار إلى أنه تم إصدار قرار بشأن إعداد الملف الاقتصادي والاجتماعي للقمة العربية القادمة المقرر عقدها بدولة تونس خلال شهر مارس المقبل، فضلاً عن الإعداد للموضوعات الاقتصادية والاجتماعية والمشروعات الاقتصادية المقترح عرضها على القمة العربية التنموية الاقتصادية والاجتماعية المقرر عقدها بلبنان خلال شهر يناير المقبل.

وكان المجلس الاقتصادي والاجتماعي العربي قد عقد اجتماعاً على مستوى كبار المسؤولين برئاسة رئيس دائرة العلاقات الاقتصادية بوزارة التجارة العراقية، عادل خضير المسعودي، للإعداد لمشاريع القرارات في المجالات الاقتصادية والاجتماعية التي ستعرض على المجلس في دورته الوزارية.

هبوط حاد للعملات الإلكترونية مع تراجع الدعم العالمي لتداولاتها


العملات الإلكترونية تعاني عالمياً

انخفض أداء العملات الإلكترونية خلال تعاملات أمس الخميس، مع مخاوف متعلقة بأن تبني تداولاتها بشكل أوسع سيستغرق وقتاً أطول.

وأفادت صحيفة «بيزنس إنسايدر» أمس، بأن بنك «جولدمان ساكس» تراجع في الوقت الحالي عن خطته لإنشاء منصة تداول للعملات الإلكترونية.

وبحلول الساعة 8:55 صباحاً بتوقيت جرينتش، هبطت «البيتكوين» بنحو 12.2% إلى 6455.2 دولار، ومنذ بداية الشهر الجاري هبطت «البيتكوين» بمقدار 600 دولار.

كما تراجعت عملة «الإيثريوم» عند 229.2 دولار بنسبة انخفاض 18.5%، فيما هبطت «الريبل» بنحو 11.8% مسجلة 0.28881 دولار.

كما أعلنت منصة «شيب شيفت إيه جي» الأسبوع الجاري أنها ستبدأ في مطالبة المستخدمين بمعلومات شخصية وهي خطة قد تدفع بعض العملاء الذين يفضلوا عدم الكشف عن هويتهم إلى عدم التداول في العملة الإلكترونية.

وبالنسبة لرابع أكبر عملة إلكترونية من حيث القيمة السوقية «بيتكوين كاش» فهبطت بنسبة 19.6% إلى 500.9 دولار، بينما انخفضت «أي. أو.إس» بنحو 21.1% عند 5.08 دولار.

وفي الأسبوع الماضي أعلنت حكومة بولندا مسودة مشروع قانون جديد يهدف إلى تبسيط النظام الضريبي لمعاملات العملات الإلكترونية وسيتم مناقشتها في الربع الجاري.

وعلى مستوى القيمة السوقية الإجمالية للعملات الإلكترونية فوصلت في الوقت الحالي عند مستوى 203 مليارات دولار.

وفي أغسطس الماضي، تعرضت العملات الإلكترونية إلى تراجع حاد خسرت معه 49.54 مليار دولار.

«مبكو» تعدل اتفاقيتي تسهيلات بنكية مع «الكويت الوطني» و«ساب»

أعلنت شركة الشرق الأوسط للورق (مبكو) عن الانتهاء من تجديد وتعديل اتفاقيتي التسهيلات البنكية (المتوافقة مع الشريعة الإسلامية)، مع بنك الكويت الوطني والبنك السعودي البريطاني- ساب، بقيمة 421 مليون ريال بدلا من 260 مليون ريال.

وقالت شركة «مبكو» في بيان على «تداول»، إنها وقعت أمس الخميس، إنها تم الانتهاء من تجديد وتعديل اتفاقية التسهيلات البنكية (المتوافقة مع الشريعة الإسلامية) مع بنك الكويت الوطني بزيادة قيمة التسهيلات من 110 مليون ريال إلى 213 مليون ريال.

واضافت أن اتفاقية التسهيلات الائتمانية قابلة للتجديد في نهاية الاتفاقية بتاريخ 30 يونيو 2019م.

وأشارت إلى أن اتفاقية التسهيلات مضمونة بسند لأمر بقيمة التسهيلات لصالح البنك.

وقالت إن الغرض من التسهيلات هو تمويل رأس المال العامل للشركة وتلبية متطلبات الأعمال الأخرى.

وتابعت: لا يوجد أطراف ذات علاقة في الاتفاقية.وفي سياق متصل وقعت «مبكو» تجديد وتعديل اتفاقية التسهيلات البنكية (المتوافقة مع الشريعة الإسلامية) مع البنك السعودي البريطاني بزيادة قيمة التسهيلات من 150 مليون ريال إلى 208 مليون ريال.

وأوضحت أن اتفاقية التسهيلات الائتمانية قابلة للتجديد في نهاية الاتفاقية بتاريخ 28 فبراير 2019.

وأشارت إلى أن اتفاقية التسهيلات مضمونة بسند لأمر بقيمة التسهيلات لصالح البنك.وأوضحت أن الغرض من التسهيلات هو تمويل رأس المال العامل للشركة وتلبية متطلبات الأعمال الأخرى.

وقالت إنه لا يوجد أطراف ذات علاقة في الاتفاقية.