

العمل عن بعد يفاقم المخاطر السيبرانية

التأقلم مع متطلبات بيئة أمنة شرط أساسي لتأمين المعلومات والتحويلات المصرفية



أشباح الإنترنت لا أحد يراها

أفضل الطرق التي يجب اتخاذها، عليها أن تحدد بعض المواعيد مع خبراء الأمن السيبراني لتطوير إستراتيجية تسلط الضوء على جميع المستويات التي يمكن أن تهمشها.

هجمة سيبرانية على البنوك

ينظر الكثيرون إلى إمكانية سحب الأموال من حسابنا المصرفي وتحويلها إلكترونياً إلى أحد أفراد الأسرة في بلد آخر وسداد الفواتير عبر شبكة الإنترنت باعتبارها أمورا مسلما بها. وفي خضم الجائحة العالمية رأينا مدى أهمية الاتصال الرقمي في حياتنا اليومية. ولكن ماذا لو أدت هجمة سيبرانية إلى تعطيل العمل المصرفي ولم يصل التحويل المطلوب؟

لقد تضاعف عدد الهجمات السيبرانية ثلاث مرات على مدار العقد الماضي مع تزايد اعتمادنا على الخدمات المالية الرقمية. ولا تزال الخدمات المالية هي الأكثر استهدافا. ومن الواضح أن المخاطر السيبرانية أصبحت مصدر تهديد لاستقرار المالي. ونظرا لقوة الروابط المالية والتكنولوجية المتبادلة فإن أي هجمة ناجحة على مؤسسة مالية كبرى أو نظام أساسي أو خدمة يستخدمها الكثيرون يمكن أن تنتشر تداعياتها سريعا في النظام المالي بأسره، مما يؤدي إلى اضطراب واسع الانتشار ويتسبب في فقدان الثقة. ومن الممكن أن تفشل المعاملات نظرا لحبس السيولة، وأن تفقد الأسر والشركات قدرتها على النفاذ إلى الودائع والمدفوعات. وفي مثل هذا السيناريو الحاد قد يطالب المستثمرون والمودعون باموالهم أو يحاولون إلغاء حساباتهم أو غير ذلك من الخدمات والمنتجات التي يستخدمونها في العادة. وقد أصبحت أدوات القرصنة الآن أقل تكلفة وأكثر سهولة وأشد قوة، مما يتيح للقرصنة ذوي المهارات المحدودة إلحاق ضرر أكبر مقابل نسبة ضئيلة من التكلفة السابقة. ويؤدي التوسع في الخدمات القائمة على الأجهزة المحمولة (وهي المنصة التكنولوجية الوحيدة المتاحة للكثيرين) إلى زيادة فرص القرصنة ويستهدف المهاجمون المؤسسات الكبرى والصغرى على حد سواء والبلدان الغنية والفقيرة، ويعملون عبر الحدود. ولذلك يجب أن تكون محاربة الجريمة السيبرانية والحسد من مخاطرها مسؤولية مشتركة بين مختلف البلدان وداخل كل بلد.

وبينما لا تزال المؤسسات المالية تضطلع بالعمل اليومي الأساسي في مجال إدارة المخاطر -صيانة الشبكات وتحديث البرمجيات وإنفاذ عملية "نظافة سيبرانية" قوية- فإن هناك حاجة أيضا إلى معالجة التحديات المشتركة السيبرانية والروابط المتبادلة عبر مختلف أجزاء النظام المالي. فحواجز الاستفهام في الحماية غير كافية بالنسبة إلى الشركات التي تعمل بشكل منفرد، والتنظيم والتدخل من جانب السياسة العامة ضروريان للوقاية من نقص الاستثمار وحماية النظام المالي الأوسع نطاقا من عواقب الهجمات المحتملة. ويبدو أن الكثير من النظم المالية الوطنية ليست مستعدة بعد للتعامل مع الهجمات، كما أن التنسيق الدولي لا يزال ضعيفا.

بروتوكول الإنترنت، والجدار الناري للتطبيقات ومواقع الويب، وتحليل حركة مرور الشبكة، ووساطة الوصول إلى الشبكة.

ويكمن جزء من تقييم التهديدات السيبرانية وتخفيفها في فهم الخطر. ولهذا السبب ينبغي أن تبدأ السياسة على مستوى المؤسسة بأضعف حلقة لتقييم المخاطر. كما أن السحابة أصبحت الآن مركزية لضمان بنية تحتية آمنة. ومع ظهور الوباء أجبرت الشركات على تحويل خيارات التخزين والتركيز على أفضل الممارسات والعمليات للوصول إلى الموظفين. هنا يأتي التشغيل الآلي المفرد. وتتعامل الشركات مع تطبيق التقنيات مع ظهور الوباء أجبرت الشركات على إعادة صياغة هذا الحل من أجل مساعدة الموظفين على العمل بشكل أكثر أمانا بدلا من التجسس عليهم.

وتخطى العديد من المنظمات في محاولة حل المشاكل الأمنية إما بالحكومة أو بالهيكل الأساسية وحدها. ولكن النهج المتوازن الثلاثي هو المفتاح، حيث يخصص الميزانيات على قدم المساواة. ولا يقل الاستثمار في تدريب الموظفين وتوعيتهم أهمية عن الاستثمار في البنية التحتية والحوكمة. وبالنسبة إلى الشركات التي لا تزال غير متأكدة من

وتبقى برامج التدريب ضرورية لضمان بقاء الموظفين على معرفة بكيفية التعامل مع الأصول الرقمية والمادية مثل الهواتف وأجهزة الكمبيوتر المحمولة الأجهزة المحمولة التي توفر للموظفين المزيد من حرية التنقل، وتزيد من فرص تركها في مكان ما أو سرقتها. لكن يمكن لبرامج التشفير الجيدة أن تمنع بيانات الشركة من الوقوع في أيدي الغريباء من خلال رفض الوصول إلى المستخدمين غير المعتمد.

ليست معظم الشركات معتمدة على هذا. وفي الواقع افترضت أغلبية الشركات أنها يمكن أن تنفق في أنه من الأمن للموظفين العمل خارج بيئة الشركة. ولأن العديد من الموظفين أصبحوا خارج سيجار شركاتهم صار من الواضح أن السيطرة قد ضعفت. وهذا ما جعل الحلول أكثر أهمية بكثير خاصة للوصول إلى الشبكة الافتراضية الموثوق بها والتي تعتمد على تحديد ثنائي الاتجاه لكل من الخادم وأجهزة الكمبيوتر المحمولة والهواتف، وما إلى ذلك. ويوصى باتباع نهج متعدد الطبقات يوفر تشفيراً متكاملاً لبناء بيئة ثقة صفرية قابلة للتطوير. وهذا يشمل بروتوكول الأنفاق في الطبقة الثانية، وحزمة أمن

وفي حين أن ذلك يشمل مجموعة من الأدوات التي يمكن أن تكون آية فإنه بشير أيضا إلى تطور التشغيل الآلي للاكتشاف والتحليل والتصميم والأتمتة والقياس والمراقبة وإعادة التقييم. وهذا أمر بالغ الأهمية، لأنه يحول التركيز بعيدا عن التكنولوجيا الفردية التي نادرا ما تنتج في الممارسة العملية. ويعتبر اعتماد الذكاء الاصطناعي والتعلم الآلي استثمارا طويل الأجل

سواء كان الموظف في المنزل أو في مقهى، فالعايير والحوكمة غالبا ما تكونان في المقدمة وفي المركز. ولكن دون الاعتراف بأهمية تدريب الموظفين وبناء البنية التحتية المناسبة تبقى الإستراتيجية غير مكتملة وتظل نقاط الضعف مخفية. ليس العمل عن بعد شيئا جديدا، لكنه يختلف كثيرا عن الحالة التي كان عليها. وأصبحت الأشياء التي كان يتوقعها الموظفون ويعتمدون عليها في المكتب بعيدة أيضا مما جعل الأوضاع أكثر تعقيدا.

برامج التشفير

يتفق الكثيرون على أن دراسة محيط المرء كانت دائما مهمة عند العمل خارج المكتب. على سبيل المثال يفهم الكثيرون وجوب توخي الحذر إزاء الشاشة. وهذه قاعدة غير معلنة للتأكد من أن محتويات الشاشة مخفية عن الغريباء. ومع التحول إلى العمل من المنزل من المرجح أن يتهاون الموظفون، مما يسمح للمتواجدين في نفس المنزل، سواء الأسرة أو الزوار، بالوصول إلى المحتوى المرتبط بالعمل. ولهذا السبب تبدأ إستراتيجية الأمن السيبراني الجيدة بالأشخاص وبمسألة الثقة.

القانوني السعودي أصيل الجعيد لـ«العرب»: محاربة أخطار الفضاء السيبراني تبدأ ببنية تشريعية قوية

كتاب «السيبرانية والقانون» يقترح إنشاء منظمة عالمية للتخصص بالأمن السيبراني

البيانات والذكاء الاصطناعي أن تقترح للجهات المختصة في السعودية تشريعات سيبرانية تواكب العصر وتحد من استغلال بعض شركات التقنية الكبرى لما يسمى بالبيانات الخام وتقدير مفهوم الخصوصية للأفراد. إن الرقابة الحكومية على الفضاء السيبراني أمر لا بد منه حتى لو أن الرقابة من ناحية اقتصادية تعتبر صعبة ومكلفة إلا أن التشريعات السيبرانية تظل ضرورة ملحة. ويشدد على أن القوانين في العالم العربي تحتاج إلى إيجاد وسيلة لتسريع تمرير التشريعات السيبرانية بحيث لا تعوقها معوقات بيروقراطية، بالإضافة إلى ضرورة أن يكون في النيابة العامة محققون جنائيون سيبرانيون وقسم طب شرعي سيبراني. وربما كانت للغياب أسباب أحدها قلة المختصين، وجدة التشريعات السيبرانية والجامعات لا تساعده، فلا توجد جامعة سعودية أو عربية لحد علمي تدرس القانون السيبراني كتخصص دقيق. ويشير إلى أن التعاون موجود بين الجهات المعنية بحماية الأمن القومي داخل الدولة السعودية وبين الدول

والتي بكل جديد، بطريقة تشريع القوانين والبيروقراطية حولها لا تجدي نفعا. ويلفت على الهيئة الوطنية للأمن السيبراني وضع برامج استقطاب لهؤلاء العباقرة الهائزين ونحوهم الذين يخطون ولا بد لنا من إعادة تأهيلهم بشكل خاص بحيث نجد طريقة لإحتوائهم واستخدام مواهبهم لتعزيز الكفاءات في الدولة. ويرى الجعيد أن التحرك العربي للسيبرانية كمجال جديد في العمليات العدائية بين الدول وحتى بين الأفراد مع غير مرض وليس على قدم وساق مع ما يحدث في الفضاء السيبراني العالمي، لكن في ظل ذلك يظل التحرك السعودي على الجانب الآخر ملقفا، فإشياء الهيئة الوطنية للأمن السيبراني وهيئة البيانات والذكاء الاصطناعي دليل على أن المملكة عازمة على الاستثمار في المستقبل السيبراني الذي نعيشه حاليا ومع الأجيال القادمة. الحروب الإلكترونية الإعلامية والتشويه والتضليل وما يسمى بالحسابات السوداء والذباب الإلكتروني كلها حروب سيبرانية بامتياز، فلا يحتاج الأمر إلى تحرك مادي بالجيش بل مجرد جيش صغير إلكتروني يعرف ماذا يفعل وكيف يحرك الرأي العام ويجيشه لتشويه سمعة أو لإثارة البلبله والمساس بالنظام العام. ويعتقد الجعيد أنه على الهيئة الوطنية للأمن السيبراني وهيئة

الجنائي تخصص الجرائم المعلوماتية من كلية القانون بجامعة واك فورست بولاية نورث كارولينا بالولايات المتحدة، في حوار له «العرب» إن الفضاء السيبراني بدل كل شيء في حياتنا فتأثر كل شيء بدءا من الاقتصاد إلى الحياة الاجتماعية إلى السياسة. ويستشهد المتحدث بقوله «تذكر عندما ضاع مكان هاتفك النقال وكيف كان شعورك سلبيا وكأنك أضعت ابنا من أبنائك؛ محاربة أخطار الفضاء السيبراني تبدأ ببنية تشريعية سريعة

الرياض - يقترح القانوني السعودي أصيل الجعيد الأستاذ المساعد في القانون الجنائي بمعهد الإدارة العامة بالرياض إنشاء منظمة عالمية موازية لمنظمة الأمم المتحدة للتخصص فقط بالأمن السيبراني وفضائه، ويحدد لو تكون المملكة راعية لمثل هذا الاقتراح. وتجتمع كل دول العالم بالرياض يوما ما، حيث أن السعودية تقود مشروعا إقليميا تنويريا مستقبليا مضادا للأصوليات البائسة المتطرفة، وهذه الأصوليات جربت كل ما لديها من أفكار ولم تفرض أي شيء غير التوقع حول نفسها منتجة ظلاما دامسا.



محمد الحماصمي كاتب مصري

ويؤكد القانوني السعودي في حوار خاص مع «العرب» أن «السعودية اليوم تصنع سمعا خاصة بها تختلف عن سموات الآخرين، ومنظمة الأمم المتحدة على الصعيد الآخر مترهلة قانونيا على المستوى التنظيمي، ولا أعتقد أنها تضطلع بمثل هذه الجهود، بل إن الاتحاد الأوروبي سبقتها كثيرا بخطواته الجادة جدا من خلال توجه أعضائه نحو الأمن السيبراني واتفاقية بودابست أحد هذه الشواهد».

ويقول الجعيد الحاصل على درجتي الماجستير والدكتوراه في القانون



د. أصيل الجعيد

أصيل الجعيد: الحروب الإلكترونية والتشويه والتضليل وما يسمى بالحسابات السوداء والذباب الإلكتروني كلها حروب سيبرانية بامتياز

أصيل الجعيد: الحروب الإلكترونية والتشويه والتضليل وما يسمى بالحسابات السوداء والذباب الإلكتروني كلها حروب سيبرانية بامتياز