معهـــد قطر
لبحـوث الحوسبة

تقرير التهديدات الإلكترونية الجديدة

في قطـر والشرق الأوسط

معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute
عـضـو فـي مـؤسـسـة قـطـر
Member of Qatar Foundation

معهـــد قطر
لبحـوث الحوسبة

تقرير التهديدات الإلكترونية الجديدة

في قطر والشرق الأوسط

معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute

عـضـو في مـؤسـسـة قـطـر
Member of Qatar Foundation

معهـــد قطر
لبحـوث الحوسبة

تقرير التهديدات الإلكترونية الجديدة

في قطـر والشرق الأوسط

أعد التقرير

روبرت ليموس
شركة ليموس وشركاه، ذ م م
ص. ب ٥٥٢
NH ٠٣٨٢٥ بارينجتون

مستاق أحمد
مركز جورجيا تيك لأمن المعلومات
مبنى كلاوس للحوسبة المتقدمة
٢٦٦ فيرست درايف
GA ٣٠٣٣٢-٠٧٦٥ ،أتلانتا

المحتويات

٤	الرسالة
٦	نظرة عامة
٨	الخطر الأول: إعاقة وضع الخطط لمواجهة المخاطر الأمنية الإلكترونية بسبب عدم وضوح الرؤية حول التهديدات و الهجمات
١٢	الخطر الثاني: استهداف المهاجمون المتزايد للبنية التحتية المعلوماتية و مزوّدي الخدمات
١٦	[الخطر الثالث: البرامج الضارة والجهات الفاعلة تنمو أكثر تطوراً مع زيادة تنوع الأهداف]
٢٠	الخطر الرابع: تبنّي التكنولوجيا المتصلة يزيد من الفرص الاقتصادية لكنه يشكل خطراً على الخصوصية
٢٤	الجهود الحالية في الأمن المعلوماتي
٢٨	المساهمون في التقرير
٣٠	Endnotes

الرسالة

حازت قضية الأمن الملعوماتي (السيبراني) على المزيد من الإهتمام خلال العام الماضي، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية على الصعيدين الإقليمي والعالمي سواء من جهة ارتفاع عدد الهجمات أو الأضرار الناجمة عنها. وقد شهدت بلدان المنطقة في الآونة الأخيرة اختراقات أمنية مقلقة استهدفت مؤسسات وشركات وأدت إلى سرقة بيانات حساسة وسرية. أما في دولة قطر، فقد أصبحت هجمات حجب الخدمة أكثر شيوعاً، كما أصبحت هجمات القرصنة المنظمة على وسائل التواصل الاجتماعي هي الوسيلة المفضلة لنشطاء القرصنة السياسية.

وللأسف، لم يتم حتى الآن تطبيق إجراءات واستراتيجيات دفاع فعّالة لمواجهة تحديات الأمن المعلوماتي، وعند تطبيقها، لم يتم الإستفادة منها إلى أقصى إمكاناتها. وعلى الرغم من زيادة معدلات الإنفاق على الأمن المعلوماتي والجهود المبذولة، إلا أن الشركات والمؤسسات الحكومية لا زالت تواجه مشاكل كبيرة في حماية مستخدميها والبيانات الخاصة بها. ولا يكاد يمر شهر دون الكشف عن اختراقات كبيرة على بيانات المستهلكين في مكان ما من العالم أو اكتشاف عملية تجسس واسعة النطاق هدفها اختراق بيانات حكومية أو عائدة للقطاع الخاص. على سبيل المثال، في شهر ديسمبر من العام ٢٠١٤، أصدرت شركة أمنية تقريراً عن شبكة تجسس استهدفت شركات ودوائر حكومية قطرية وغير قطرية.

وعلى ضوء ذلك تبرز الحاجة إلى تحليل مكثف لاتجاهات الأمن المعلوماتي والبحث عن استراتيجيات دفاع وسياسات فعّالة لمواجهة هذه التهديدات. وقد تسهم دراسة الأساليب التي يستخدمها المهاجمون في وضع التدابير الأمنية والسياسات التي من شأنها أن تحمي البنية التحتية الحيوية والبيانات الخاصة بالمواطنين. وعلى سبيل المثال، قد تساعد نظم المعالجة الذاتية في الحد من الاختراقات، كما قد تساعد الطبقات الإضافية من الدفاعات والحاسوبية الافتراضية في حماية البيانات الحساسة والحيوية من التهديدات المحتملة. أما على مستوى سياسة أمن المعلومات، فقد يساعد تبادل المعلومات بشكل أفضل، مثل تبادل المعلومات والبيانات على الصعيد العالمي، إلى حماية الأنظمة الإلكترونية.

وقد شَرَعت دولة قطر في إطلاق العديد من المبادرات الحكومية لحماية أمنها المعلوماتي. ففي عام ٢٠١٣، أسست دولة قطر اللجنة الوطنية لأمن المعلومات التي أخذت على عاتقها مهمة وضع الاستراتيجية الوطنية للأمن السيبراني لحماية البيانات والأنظمة من أشد الهجمات خطورة. وفي شهر مارس من العام ٢٠١٤، نشرت وزارة الاتصالات وتكنولوجيا المعلومات التقرير الثاني للاستراتيجية الوطنية للأمن السيبراني الذي يحدد المسؤوليات والواجبات التي يتوجب على الشركات العاملة في قطاعات البنية التحتية الحيوية اتخاذها من أجل حماية شبكاتها.[1] وتُعَد دولة قطر أول بلد يشترك مع المنظمة الدولية للشرطة الجنائية (الإنتربول) في إعداد تقييم للعناصر الأساسية لخطة أمن وطنية معلوماتية، الذي سيكون له دور كبير في تعزيز تبادل المعلومات وقدرة الجهات التي تطبّق القانون على التحقيق في جرائم الأمن المعلوماتي.

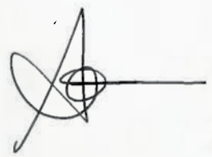
> وهناك مشاريع ومبادرات جديدة تزيد من أهمية هذه الجهود، مثل الرعاية الصحية الوطنية والاستعدادات لنهائيات كأس العالم لكرة القدم في العام ٢٠٢٢ والتزام دولة قطر بإنشاء المدن الذكية.

ودعماً لهذه الجهود، يواصل معهد قطر لبحوث الحوسبة (QCRI) أبحاثه حول التهديدات والمخاطر التي تجابه الأمن المعلوماتي بهدف إيجاد حلول للقضايا التقنية التي تشكلها مثل هذه التهديدات. منذ إنشاء معهد قطر لبحوث الحوسبة في العام ٢٠١٠ كعضو تابع لمؤسسة قطر للتربية والعلوم وتنمية المجتمع كانت مهمة المعهد معالجة هذه التحدّيات، ويهدف المعهد إلى أن يصبح الرائد عالمياً في بحوث الحوسبة ضمن مجالات محددة تحقق أثراً إيجابياً في حياة المواطنين وفي المجتمع عموماً. وتتمثل رسالة المعهد في إجراء أبحاث حاسوبية تطبيقية مبتكرة ومتعددة التخصصات تتماشى مع الأولويات الوطنية وذلك عبر رفع مستوى حياة المواطنين، وفتح المجال أمام اكتشافات علمية جديدة وتمكين الأعمال والتجارات المحلية على المنافسة على مستوى العالم.

وعلى اعتبار أن الأمن المعلوماتي يُعتبر من التحديات الكبرى التي تواجهها دولة قطر، فقد أطلقت الحكومة القطرية العديد من المبادرات البحثية، كما بادرت بالتعاون مع العديد من الجامعات والمراكز البحثية في جميع أنحاء العالم بهدف وضع سياسة وطنية، وبناء بنية تحتية معلوماتية أكثر قدرة على مجابهة الأخطار والتهديدات. ويوفّر هذا التقرير رؤية موسّعة لمشهد التهديدات الأمنية الإلكترونية ويهدف إلى إيجاد أساس للنقاش الوطني حول الطريقة التي يمكن للمؤسسات حماية نفسها ضد الهجمات الإلكترونية.

ويُعَدُّ إجراء البحوث في مجال الأمن المعلوماتي من الأهداف الرئيسية لمعهد قطر لبحوث الحوسبة. ففي العام ٢٠١٣، قام المعهد باستضافة مجموعة من الخبراء من داخل قطر ومن حول العالم بالتعاون مع المؤسسات القطرية المعنية مثل الجامعات والمؤسسات الإعلامية وشركات النفط والغاز ووزارة الداخلية القطرية لمناقشة تحديات الأمن المعلوماتي التي تواجه دولة قطر، بهدف صياغة إطار عام لإنشاء مركز لبحوث الأمن المعلوماتي. وفي العام التالي، أصدر معهد قطر لبحوث الحوسبة تقريره السنوي الأول للتهديدات الإلكترونية في قطر والمنطقة.[2]

يناقش هذا التقرير ظهور أوجه جديدة وفريدة من نوعها للتهديدات الإلكترونية الحالية، فضلاً عن التحدّيات المستمرة من التهديدات التي أوردناها في تقرير العام الماضي. وفي حين لا يزال مشهد التهديدات الإلكترونية على حاله، يأمل معهد قطر لبحوث الحوسبة أن يوفر هذا التقرير أساساً يتيح لدولة قطر من خلاله تعزيز النقاش حول التهديدات والمخاطر، والتأثير المحتمل لهذه التهديدات على قطر والمنطقة برمتها، فضلاً عن تطوير استراتيجيات وأساليب دفاع فعّالة لاحتوائها.



الدكتور أحمد المقرمد
المدير التنفيذي
معهد قطر لبحوث الحوسبة

نظرة عامة

وضعت دولة قطر في العام ٢٠٠٨ رؤيتها الوطنية الملتزمة بتحقيق التنمية البشرية والاقتصادية والاجتماعية والبيئية المستدامة لمواطنيها. وتستند رؤية قطر الوطنية بشكل رئيسي على بناء اقتصاد مستدام ومتنوع بحلول العام ٢٠٣٠ وتوفير بيئة أعمال مبدعة قائمة على المعرفة وتكنولوجيا المعلومات.[٣]

وقد حققت قطر تقدماً كبيراً في تحقيق أهدافها التقنية، ولكن التهديد الأمني يمثل العقبات المحتملة لجهودها. خلال العام التالي لإصدار التقرير السابق، تغيّر وضع الأمن المعلوماتي بشكل كبير حيث تداخل العالم الرقمي مع العالم الحقيقي أكثر من أي وقت مضى. المبادرات العديدة مثل مشيرب ومدينة لوسيل الذكية والرقمنة المتزايدة للسجلات الطبية ورصد ومراقبة العديد من الأجهزة ، من خلال ما يُدعى بـ»إنترنت الأشياء»، تَعِد بأرباح كبيرة.

> ويُعتبر التطور الذي شهده قطاع الاتصالات وتكنولوجيا المعلومات من أهم المؤشرات الدالة على مدى التطور الذي حققته دولة قطر في هذا المجال، حيث حقق هذا القطاع معدلات نمو قدرها ١٧٪ سنوياً. وبحلول العام ٢٠١٦، تسعى قطر إلى تطبيق خطة وطنية لتوفير الإنترنت السريعة (broadband) بسرعة تنزيل تعادل ١٠٠ ميغابايت في الثانية إلى ٩٥٪ من المنازل، وأن يكون لجميع الشركات والمؤسسات والمستشفيات إمكانية النفاذ إلى سرعة لا تقل عن ١ جيجابايت في الثانية للتنزيل.

وقد حلّت قطر على مدى عامي ٢٠١٣ و ٢٠١٤ على التوالي في المرتبة ٢٣ عالمياً [٤] من أصل ١٤٨ دولة في مؤشر الجاهزية الشبكية العالمية الذي يقيس استعداد شركات ومواطني هذه الدول لاستخدام تكنولوجيا المعلومات والاتصالات بفاعلية. وكانت قطر قد حلّت في المرتبة ٣٦ في العام ٢٠٠٧.[٥]

ويُسلّط هذا التطور السريع الضوء على المزايا التي تتمتع بها دولة قطر. وفي هذا الصدد قال الدكتور سوميترا دوتا، البروفيسور في كلية جونسون للدراسات العليا في الإدارة بجامعة كورنيل أن:

«الثروات الطبيعية التي تتمتع بها دولة قطر، إلى جانب عدد سكانها المحدود نسبياً، واقتصادها النشط يتيح لها نمواً اقتصادياً سريعاً ويمكّنها من مجابهة التحديات الجديدة بقدر أكبر من المرونة.»

وأضاف قائلاً: «إن دولة قطر قادرة على تبنّي تقنيات متطورة بوتيرة أسرع من معظم الدول الأخرى. ولكن هذا التطور التقني السريع قد يترتّب عليه مخاطر عدة.»

وعلى الرغم من الانعكاسات الاقتصادية الإيجابية لتطور تكنولوجيا المعلومات والاتصالات، إلا أن تزايد استخدام هذه التكنولوجيا يترتّب عليه تنامي التهديدات والجرائم الإلكترونية. وفيما تتيح الخدمات التي تقدمها الشركات والحكومات عبر الإنترنت مستوى أفضل من الخدمة للعملاء والمواطنين، إلا أنها تفتح المجال واسعاً أمام مختلف أنواع الجرائم الإلكترونية سواء تلك التي تشنها الحكومات المعادية أو القراصنة الإلكترونيين بهدف تعطيل الخدمات الحيوية. وبما أن العالم الرقمي يتقاطع بشكل متزايد مع حياة المواطنين، فبإمكان القراصنة الوصول إلى المزيد من البيانات عن المواطنين ومع الاعتماد المتزايد على الأجهزة المتصلة، فهذا يتيح أيضاً الوصول إلى الأشياء الأخرى في حياتهم.

ويُركّز هذا التقرير على القضايا والتهديدات التي تُمَكّن المهاجمون من اختراق وتعطيل الأنظمة الرقمية. إن عدم تبادل المعلومات بين الجهات المعنية ونقص العمالة ذات مهارات

الأمن المعلوماتي تضع الشركات والوكالات الحكومية في وضع غير مواتٍ أثناء الدفاع ضد الهجمات الأكثر تقدماً. الصعوبة في ضمان أمن البنية التحتية المكتسبة والحماية اللاحقة لها، تضع النُظم الحيوية في خطر. ومع التطور المتزايد للمهاجمين والأساليب المستخدمة، على المدافعين العمل بجد أكثر لحماية مجموعة متزايدة من الأجهزة الرقمية والشبكات والأنظمة.

وفيما تركّز دولة قطر جهودها على بناء اقتصاد مبني على المعرفة، لا بد من اتخاذ كافة التدابير والإجراءات اللازمة التي تضمن حماية بنيتها التحتية الحيوية من التهديدات والأخطار الإلكترونية. ومع ازدياد اعتماد الشركات والمستهلكين على وسائل الاتصالات والتكنولوجيا المتصلة بالإنترنت لا بد أيضاً من بذل كافة الجهود التي تضمن حماية هذه التكنولوجيا.

ومن أجل مجابهة هذه التهديدات لا بد من نشر الوعي بالأمن المعلوماتي وبناء قوة عاملة مدرّبة على استخدام تكنولوجيا المعلومات والاتصالات والإستفادة منها بطريقة فعّالة وآمنة. الإنفاق على التكنولوجيا الحالية لن يوفّر للدولة الدفاعات التي تحتاجها، حيث يستمر المهاجمون في تطوير هجماتهم وترقية وسائلهم المختلفة على الرغم من الإنفاق الهائل على التكنولوجيا والخدمات الخاصة بالحماية من التهديدات. ولا بد للدول من تبنّى أجندة بحثية بهدف ابتكار أساليب وتدابير جديدة لحماية البنية التحتية الحيوية، وتأمين بيانات المواطنين ورصد واحتواء التهديدات والمخاطر.

وفي هذا الصدد قال الدكتور أحمد المقرمد، المدير التنفيذي لمعهد قطر لبحوث الحوسبة: «في ظل عالم متغيّر وسريع، نحن بحاجة لأن نكون على أهبة الاستعداد لكل طارئ. يجب أن نبحث عن الحلول غير التقليدية لمشاكل الأمن المعلوماتي، وأن نفكر بطرق ابتكارية.»

وقد احتضنت دولة قطر هذا التحدي حيث أنشأت الحكومة الوطنية بالفعل اللجنة الوطنية للأمن السيبراني لتحديد أولويات الأمن المعلوماتي، ووضع سياسة ضمان المعلومات الوطنية، وهي أول دولة تشترك مع الإنتربول على تقييم الأمن السيبراني الوطني.

ومن جانبه قال ستيف هونيس، مدير المشاريع في مجمع الإنتربول العالمي للابتكار والتواصل (IGCI): «لو أننا سنناقش هذا الموضوع في ذات الوقت من العام المقبل، أتوقع أن يكون المشهد مختلفاً تماماً عما هو عليه الآن. وتنفرد دولة قطر عن غيرها من الدول بفضل خططها الطموحة وتطلعاتها نحو بناء اقتصاد رقمي حقيقي.»

> سينمو سوق الأمن المعلوماتي العالمي من ما يقدر بنحو ٧١ مليار دولار في العام ٢٠١٣ إلى ١٥٥ مليار دولار في العام ٢٠٢٠، وهو ما يمثّل معدّل نمو سنوي مركّب بنسبة ١١,٨ في المئة، وفقاً لفروست أند سوليفان.[٦]

الخطر الأول

إعاقة وضع الخطط لمواجهة المخاطر الأمنية الإلكترونية بسبب عدم وضوح الرؤية حول التهديدات و الهجمات

في حين قامت دولة قطر بالعديد من المبادرات لتبادل المعلومات، فإن على الشركات والمؤسسات الحكومية أن تتعاون بشكل أكبر من أجل تقييم وفهم المخاطر والتهديدات.

أبرز الحقائق

- افتقار الشركات إلى الرؤية المناسبة في استخدام شبكاتها وبياناتها يسمح للمهاجمين بالعمل في الخفاء.
- افتقار معظم الشركات إلى المعلومات الاستخباراتية حول الوضع الراهن لحجم المخاطر والتهديدات بالرغم من تبادل بعض القطاعات الحيوية المعلومات حول التهديدات والمخاطر.
- افتقار المواطنون المستمر إلى فهم التأثير الذي تشكّله الهجمات الإلكترونية على حياتهم.
- الحاجة لتدريب المزيد من العاملين في مجال تكنولوجيا المعلومات على قضايا الأمن المعلوماتي وعمليات التحكم من أجل حماية الشبكات والبيانات الخاصة بدولة قطر.

يواجه العاملون والمسؤولون الحكوميون في دولة قطر نقصاً في المعلومات حول المخاطر التي تهدد البنية التحتية لدولة قطر والشركات العاملة بها. ولا تمتلك العديد من المجموعات من مشغلي الشبكات إلى العاملين في أقسام أمن المعلومات في الشركات إلى المؤسسات الحكومية سوى نبذة بسيطة فقط من الصورة الكاملة. كما أن المعلومات حول المخاطر لا تصل إلا إلى عدد قليل من المجموعات.

ويقول الدكتور أحمد المقرمد:

«من الواضح أننا لا نقوم بتبادل المعلومات حتى على المستوى الوطني، ولا يوجد لدينا آلية شاملة لتبادلها.»

ولا تقتصر مشاكل تبادل المعلومات على دولة قطر فقط، حيث تتحفظ غالبية القطاعات الخاصة والحكومية في معظم البلدان على نشر المعلومات عن المخاطر التي تتعرض لها. وعلى سبيل المثال، واجهت الولايات المتحدة صعوبات في تمرير قانون يمنح الشركات التي تتبادل معلومات عن الهجمات التي تتعرض لها الحماية القانونية من الملاحقة القضائية.[٧]

وقد اتخذت دولة قطر العديد من الخطوات لتشجيع وتبادل المعلومات بين الأطراف المخوّلة بذلك. واعتبرت «الاستراتيجية الوطنية للأمن السيبراني» أن جمع وتبادل المعلومات حول المخاطر والتهديدات الأمنية الإلكترونية هو هدف رئيسي لها.[٨] بالإضافة إلى ذلك ، أنشأت دولة قطر ثلاث لجان متخصصة لأمن المعلومات (IRECs) تقوم بتبادل المعلومات بين الشركات والمؤسسات الحكومية في قطاعات الطاقة والمال والحوكمة. وفي شهر ديسمبر من العام ٢٠١٤، أجرت دولة قطر تدريبها الثاني حول الأمن المعلوماتي بمشاركة أكثر من ٣٠٠ مشارك من قطاعات البنوك والطاقة والحكومة والنقل.

ومع ذلك، هنالك الكثير مما يتعيّن القيام به. وفي حين يقوم المهاجمون في كثير من الأحيان بنشر تقنياتهم الهجومية على شبكة الإنترنت، تُفَضّل الجهات التي تتعرض للهجمات عدم الإفصاح عن خبرتها في الدفاع عن الأنظمة ورد الهجمات.

افتقار الشركات إلى رؤية واضحة للنشاطات الشاذة على الشبكات واستخدام البيانات

تهدد الأنظمة في دولة قطر مجموعة من المخاطر، إلا أنه لا يوجد الكثير من الدراسات التي تحدد حجم ونطاق المشكلة. وقد أظهرت دراسة بحثية مبدئية أجراها معهد قطر لبحوث الحوسبة أن «البوت نت» ZeroAccess قد أصاب أكثر من ١٠٠ جهاز حاسوب شخصي داخل البلاد. وفي دراسة ثانية أُجريت من قبل طلبة جامعيين، تم اكتشاف آلاف الفيروسات الأخرى داخل أنظمة المعلومات والاتصالات في دولة قطر.

وفي غياب المعلومات عن نوع المخاطر وتأثيرها، لا تستطيع المؤسسات الحكومية والشركات أن تصل إلى قرارات تستند إلى المعلومات اللازمة حول أفضل الطرق لحماية شبكات دولة قطر وبياناتها. وقد أكدت هجمات فيروس شامون (Shamoon) ضد كل من شركتي الغاز والنفط أرامكو السعودية وراس غاز القطرية في العام ٢٠١٢ ضعف تلك الشركات وإمكانية تعرّضها للهجمات.[٩] بالرغم من ذلك، حصلت هجمة مماثلة في العام ٢٠١٤ تحت اسم عملية الساطور[١٠] (Operation Cleaver) والتي استهدفت شركات ومؤسسات حكومية في ١٦ دولة من ضمنها ٤ مؤسسات داخل دولة قطر دون أن يتم كشفها.[١١]

وقال علي ماجد الهاشمي، مدير التحكم والمعايير بإدارة تكنولوجيا المعلومات بمؤسسة قطر: «إن التهديد الرئيسي الذي نواجهه لا يتمثل في الهجمات المتزايدة لتشويه سمعة الشركات أو إمكانياتها المالية وإنما في عدم وجود الوعي والاستعداد الكافي لدى المؤسسات للتصدي لهذه التهديدات.»

> لا زالت الشركات والمؤسسات الحكومية تتعامل مع المشكلة بطريقة رد الفعل، بينما هناك حاجة ماسة لإتباع نُهج أكثر استباقية، بما في ذلك إنشاء قاعدة بيانات وطنية للحوادث الأمنية وتبادل المعلومات الاستخباراتية بين الشركات والهيئات الحكومية وإيجاد الموارد للمساعدة في تحليل الهجمات.

وقال فيصل الكوّاري الرئيس التنفيذي للتكنولوجيا في شركة ميزة: «يحتاج الأمر للكثير من العمل. إنه ليس بالأمر السهل. عندما تعمل في مجال الأمن فنسبة الأمان المتوفر هي بمقدار ما تكون عليه التكنولوجيا والكادر البشري والعمليات المطبّقة. هناك حاجة للاستثمار الكافي والدعم من الإدارة العليا من أجل الحصول على النتائج المرجوة.»

إعاقة جهود الدفاع بسبب الفشل في تبادل المعلومات حول التهديدات

أحرزت دولة قطر تقدما ملحوظاً في مجال تبادل المعلومات حول المخاطر والتهديدات الإلكترونية التي تواجهها أهم القطاعات الخاصة والحكومية في الدولة، وذلك من خلال تأسيس لجان خبراء الأمن السيبراني السابق ذكرها وإجراء تمرينين للأمن المعلوماتي، بمشاركة ٣٠ مؤسسة تعمل في القطاعات الحيوية للدولة في التمرين الأخير.[١٢]

إلا أن الشركات الكبرى فقط هي المستفيد الأكبر من نُظم تبادل المعلومات. ففي الولايات المتحدة على سبيل المثال، تستفيد البنوك الكبرى بشكل رئيسي من الخدمات التي يقدمها مركز تحليل وتبادل المعلومات للخدمات المالية (FS-ISAC) فيما أنشأت المؤسسات المالية الصغيرة والصناعات ذات الصلة، مثل الشركات المزودة للبطاقات الإئتمانية،-مجموعاتها الخاصة لتبادل المعلومات بما يلبي احتياجاتها الخاصة.[١٣]

يتعيّن على الشركات أن تجد طرق لتبادل المعلومات حول التهديدات بصورة أوسع. وفي حال انعدام تبادل المعلومات سوف تميل الدفة لصالح المهاجمين.

وقال مصطفى هَنيد بنغالي المسؤول عن أمن المعلومات في مكتب المدير التنفيذي بشركة أوريدوو:

«ينبغي أن تمتلك كافة المؤسسات نظام للاستجابة الفورية للتهديدات والاختراقات وأن تعمل لهذا الهدف، وإلا سيتمكن المهاجمون، إذا توفر لهم المال والوقت، من تنفيذ اختراقاتهم.»

من الممكن للتبادل الخاص للمعلومات أن يساعد كثيرا، وقد تم إنشاء العديد من المنتديات في جميع أنحاء العالم لمشاركة استخبارات التهديدات الأمنية. على سبيل المثال، قامت شركة IBM بإطلاق منتدى X-Force Exchange الذي يتيح لأكثر من ١٠٠٠ منظمة في ١٦ مجال صناعي مختلف الفرصة لتبادل المعلومات حول التهديدات ولمساعدة بعضهم البعض لمواجهتها.

وصرّح الدكتور تامر أبو علي، الرئيس التنفيذي للتكنولوجيا في قسم الشرق الأوسط وأفريقيا لشركة IBM «بإمكان المشاركون في المنتدى أن يتحققوا من صحة نتائج البحوث ومشاركة مجموعة من مؤشرات التسوية (IOC) للمساعدة في التحقيق في الهجمات والتهديدات وإضافة السياق إلى التهديدات من خلال التعاون مع الآخرين.»

إعاقة عمليات الدفاع عن الشركات والأفراد على حد سواء بسبب نقص المعلومات الأمنية

وتبرز الحاجة للحصول على المعلومات والبيانات عن المهاجمين ووسائلهم بغية الاستفادة منها للتمكّن من التصدّي للهجمات المختلفة. إلا أن نقص الكوادر والخبرات المتخصصة في مجال أمن المعلومات لن يؤدي إلى حماية أفضل حتى في حال توفّر التصوّر الواضح للأخطار. يتوجب بحلول عام ٢٠١٧ ملئ أكثر من ٢ مليون وظيفة شاغرة في مجال الأمن المعلوماتي، حيث تعاني المؤسسات في منطقة الشرق الأوسط من نقص حاد في المهارات وبالأخص في المناصب القيادية بأمن المعلومات وكذلك في مجالات التدقيق والاختبار والتحليل والتعامل مع الحوادث.[١٤]

ويُعتبر نقص الأخصائيين في مجال أمن وحماية المعلومات الإلكترونية مشكلة عالمية، إلا أنها تؤثر على دولة قطر بشكل خاص. ويقول أسامة كمال فريد محمد، مدير قسم استخبارات تهديدات الأمن المعلوماتي في وزارة الاتصالات وتكنولوجيا المعلومات القطرية أن: «نقص الكوادر المتخصصة يجعل دولة قطر عرضة للعديد من التهديدات.»

لا تقتصر الحاجة للمعرفة والخبرة في مجال أمن المعلومات على الأخصائيين في أمن المعلومات، وإنما لا بد أن يمتلك الأفراد والمستهلكين وعي أكبر بالتهديدات الإلكترونية التي يمكن أن تؤثر على حياتهم.

وتُشير إحدى الدراسات [١٥] إلى أن مستخدمو الإنترنت في الشرق الأوسط وشمال أفريقيا هم من بين المستخدمين الأكثر حذراً على الإنترنت، حيث اتفق ٤٥٪ منهم «اتفاق تام» مع العبارة «أنا حريص جداً حول ما أفعله أو أقوله على الإنترنت». ومع ذلك، يُعتبر مستخدمو الحواسب والشبكات الإلكترونية في منطقة الشرق الأوسط عموماً وحسب الدراسة ذاتها، أكثر عرضة من غيرهم لممارسة الاستخدام الغير آمن على الإنترنت، كفتح الملفات والوثائق المرفقة من أشخاص مجهولين. كما أنهم أقل لجوءاً من المستخدم العادي لاستخدام برامج مضادة للفيروسات وغيرها من برامج الحماية التي تهدف إلى حماية المعلومات والتأكد من بقاء أنظمتهم سليمة. بعبارة أُخرى، يَعتقد هؤلاء المستخدمون أنهم حريصون لكن تصرفاتهم تشير إلى واقع مغاير، ولكن بإمكان التعليم والتدريب أن يحل هذه القضايا.

التنقيب في البيانات الكبيرة لاكتشاف التهديدات

فيما يُعتبر إقناع الشركات بنشر البيانات المتعلقة بالهجمات أمراً صعباً، إلا أن مردود ذلك يمكن أن يكون كبيراً جداً. ويعمل معهد قطر لبحوث الحوسبة على إيجاد الطرق الأمثل للتنقيب في مجموعات كبيرة من بيانات الشبكة باستخدام مجموعة متنوعة من تقنيات تحليل البيانات بهدف اكتشاف مؤشرات تدل على الهجمات المحتملة.

على سبيل المثال، أشار الدكتور تينغ يو، وهو باحث رئيسي في معهد قطر لبحوث الحوسبة، إلى أن: «من خلال استخدام تقنيات تصنيف البيانات والبيانات المنبثقة عن هجمات سابقة، يأمل الباحثون في المعهد اكتشاف أنماط مثيرة للإهتمام قد تساعد في التحذير من الهجمات التي يصعب الكشف عنها في الوقت الحاضر. نريد استخراج خصائص تساعد على الوصول إلى تصنيف أفضل يمكن أن يقود إلى اكتشاف الهجمات الغير معروفة سابقاً أو القدرة على التنبؤ بالهجمات المستقبلية.»

الخطر الثاني

استهداف المهاجمون المتزايد للبنية التحتية المعلوماتية ومزوّدي الخدمات

اتخذت قطر خطوات لحماية الشبكات الأكثر أهمية لاقتصادها، ولكن المهاجمون سيستمرون في استهداف أنظمة البنية التحتية والشركات التي تقدم التكنولوجيا والخدمات.

أبرز الحقائق

- قد يؤدي التحديث السريع للبنية التحتية المعلوماتية والاتصالات بدولة قطر إلى عدم اكتشاف الثغرات الأمنية.
- فيما يتم العمل على تحصين الشبكات ضد الهجمات، سيحاول المهاجمون العثور على نقاط ضعف أخرى أو استخدام برامج متخفّية في أحصنة طروادة في منظومة المورّدين.
- يزداد ظهور المهاجمين المحليين وتُصبح هجماتهم أكثر حدة وتستهدف البنية التحتية الحيوية.
- لا تزال عملية تحديث أمن البنية التحتية الحيوية تشوبها معوقات بسبب وجود مكوّنات قديمة لا تحتوي على الحماية أو التصميم الآمن للعمل بشكل آمن في عالم متصل بشكل متزايد.

في حين أن التهديدات التي تواجه قطاع البنية التحتية الحيوية بدولة قطر هي مماثلة لما تتعرض له الدول الأخرى، إلا أن الاستثمار في البنية التحتية في دولة قطر أسرع من الدول الآخرى. ففي قطاع النقل على سبيل المثال استثمرت دولة قطر المليارات من الريالات لإنشاء ميناء بحري جديد وتحسين البنية التحتية للطرق وتحديث مطار الدوحة الدولي وبناء نظام نقل جماعي بالخطوط الحديدية ذو سرعة عالية.

يُشكّل هذا التطور السريع للبنية التحتية تحدياً في المحافظة على أمن الشبكات والأنظمة الحيوية للدولة. وقد تم بالفعل استهداف هذه الشبكات والأنظمة من قبل القراصنة، حيث تم استهداف شركة راس غاز في العام ٢٠١٢ بواسطة البرنامج الضار شامون الذي قام بحذف بيانات وتعطيل الأنظمة. وكان للهجوم تأثير أكبر على شركة أرامكو السعودية للنفط والغاز ما اضطرها إلى تغيير الأقراص الصلبة على عشرات الألوف من الأنظمة.[١٦] وفي العام ٢٠١٤، قامت مجموعة من القراصنة، برعاية دولة شرق أوسطية كما يُعتقد، بشن هجوم ناجح على مجموعة من شركات البنية التحتية الحيوية المرتبطة بإنتاج الغاز والنفط، من ضمنها ٤ شركات كبرى داخل دولة قطر.[١٧]

ويقول الدكتور ديميتريوس سيربانوس، وهو باحث رئيسي في معهد قطر لبحوث الحوسبة:

«قد تحتوي البنية التحتية لتكنولوجيا المعلومات والاتصالات على مكوّنات وبرامج تعود إلى عشرات السنين ولذلك في الحملات المكثّفة والمستمرة، تحتاج إلى دفاعات يمكن تحديثها باستمرار.»

وتعْتَبِر حكومة دولة قطر حماية البنية التحتية لتكنولوجيا المعلومات والاتصالات من الأولويات المشار إليها كهدف رئيس في الاستراتيجية الوطنية للأمن السيبراني.[١٨] وفي شهر مارس من العام ٢٠١٤، أصدرت وزارة المعلومات والاتصالات القطرية تحديث لسياسة تأمين المعلومات الوطنية[١٩] يُعطي مدراء تكنولوجيا المعلومات طريقة يستطيعون من خلالها تصنيف الأصول وقواعد تكنولوجيا المعلومات التي تتعلق بحماية هذه الأصول.

ويقول جيوم صالحة، رئيس مهندسي الأنظمة في شركة قطر للبترول، «نحن بصدد إنشاء هيكلية مناسبة للتعامل مع كل هذه القضايا الأمنية، لدينا أسلوب للتعامل مع المخاطر، لذا سنقوم بإعادة النظر بالسياسات والإجراءات المُتَّبعة».

النمو السريع للبنية التحتية لتكنولوجيا المعلومات والاتصالات يمكن أن يُعَرِّض دولة قطر للهجمات

في إطار جهودها الرامية إلى إنشاء اقتصاد ومجتمع مبني على المعرفة بحلول العام ٢٠٣٠، أخذت القيادة القطرية على عاتقها مهمة تحديث وتوسيع البنية التحتية. مِن بناء المدن الذكية إلى توفير نطاق عريض فائق السرعة، تسعى الحكومة القطرية إلى بناء مجتمع متقدّم يعتمد بشكل كبير على تكنولوجيا المعلومات.

وباعتماد العديد من التكنولوجيات الحديثة تظهر المخاطر، حيث يستهدف المهاجمون والقراصنة مزوّدي الخدمات. وفي بلدان أخرى أصبحت المشكلة واضحة بالفعل، وتُظهِر المُذَكِّرات المُسَرَّبة بأن وكالات الإستخبارات قد ركّزت اهتمامها على اختراق وزرع برمجيات ضارة في أجهزة وحواسب قبل تسليمها إلى وجهاتها.[٢٠] وفي العام ٢٠١٣، نجح قراصنة الإنترنت في اختراق شركة تارغت (Target) الأمريكية من خلال اختراق الشركة المتعاقدة على تزويد أنظمة التدفئة والتهوية وتكييف الهواء في الشركة.[٢١]

وقال عمر شيرين، مدير إدارة حماية المعلومات الحساسة (CIIP) في وزارة الاتصالات وتكنولوجيا المعلومات: «النمو السريع في البنية التحتية لتكنولوجيا المعلومات والاتصالات بدولة قطر يجعل المخاطر أكثر حدة.»

وأضاف قائلاً: «نحن نشتري ونعتمد التكنولوجيا الجديدة بصورة أسرع من أي بلد آخر، ولكن علينا أن نعير إنتباه أكثر إلى طرق حماية هذه التكنولوجيا.»

ومن المؤسف أن حماية المعلومات من مهاجم جاد هي مسألة بحثية صعبة، فبينما من الممكن العثور على العيوب التصميمية من خلال مراجعة شيفرة البرامج والتحاليل التقنية، إلا أن اكتشاف المنتجات المحتمل أن تكون غير سليمة هو أمر صعب للغاية. ومع ذلك، شرعت قطر في إنشاء مختبر للتحقق من إلتزام المنتجات بمعايير أمنية محددة.

وأضاف شيرين: «لا نرغب في نهاية المطاف أن يقوم بعض مزوّدي الخدمات والشركات المتعاقدة معنا باستخدام أجهزة رخيصة. سوف يساعدنا هذا المختبر على تقييم المعدّات والأجهزة وإنشاء مقياس للحد الأدنى من المعايير.»

ازدياد عدد المهاجمون المحليون وقيامهم بالمزيد من الهجمات الشرسة والتي تستهدف البنية التحتية الحيوية

لقد ركّزت جماعات التجسس، ولفترة من الزمن، على التسلل إلى الوكالات الحكومية والشركات في منطقة الشرق الأوسط ولكن الهجمات العلنية تمّت بشكل عام من قِبل المعارضين لاستهداف الشبكات الاجتماعية ومواقع الإنترنت. ولم يتم الإبلاغ عن الهجمات التخريبية، مثل استهداف شركة أرامكو السعودية وشركة راس غاز، إلا نادراً.

ولكن يتوقع الخبراء أن يتغير ذلك حيث سيزداد عدد الهجمات التي تستهدف تعطيل العمليات وحذف البيانات الحيوية للشركات وسرقة المعلومات الاستخباراتية. وقد استهدفت مجموعة محلّية معيّنة، صقور الصحراء، عدة وكالات حكومية وشركات، بما في ذلك شركات البنية التحتية الحيوية، في كل من فلسطين وإسرائيل ومصر وقاموا بسرقة أكثر من مليون ملف بحثاً عن وثائق استخباراتية حساسة. [٢٢]

وتم تسليط الضوء في التقرير الصادر في ديسمبر من العام ٢٠١٤ على مجموعة أخرى،[٢٣] كانت قد تمكنت من اختراق خلسةً أكثر من ٥٠ شركة ووكالة حكومية في ١٦ دولة، حيث استهدفت شركات البنية التحتية الحيوية والمطارات وشركات الطيران وقطاع الصناعة والشبكات العسكرية بالإضافة إلى مجال النفط والغاز. ووفقاً للشركة الأمنية سيلانس (Cylance) التي أعدّت التقرير، فإن أكثر من ٧٥ في المئة من هذه الشركات كانت في منطقة الخليج.

وقال جون ميلر، نائب رئيس الاستراتيجية في شركة سيلانس التي أجرت البحث ونشرت التقرير:

«كان الهدف الرئيسي من المجموعة التي قامت بعملية الساطور هو فقط اختراق وإضعاف شركات البنية التحتية الحيوية.»

وقد أخطرت شركة سيلانس هذه الشركات المستهدَفة اعتقاداً بأن الهدف النهائي من الهجوم كان يهدف لعرقلة إمدادات النفط. وأضاف: «كان كل ما يريدون القيام به هو الحفاظ على استمرار الهجوم وليس هناك الكثير من القيمة في الحفاظ على استمرار الهجوم على شركة نفط سوى لتعطيل إمداد النفط.»

استمرار معاناة أنظمة التحكم الصناعية بسبب عدم التحديث في المجال الأمني

تم تصميم أنظمة التحكم الصناعية عبر السنين لتوفير الثقة باستمرارية العمل وليس لمقاومة الهجمات المحتدة. ولكن مع ازدياد ربط هذه التقنيات التشغيلية على نحو متزايد بشبكات المعلومات، ومن خلالهم إلى الإنترنت، أصبحت النُظم الصناعية أكثر عرضة للهجمات الخبيثة. وقد ركّز العديد من الباحثين في مجال الأمن على إيجاد نقاط الضعف في نُظم التحكم والرقابة الصناعية، حيث تم إيجاد أكثر من ٨٠٠ قضية أمنية في المنتجات المستخدمة حول العالم منذ بداية العام ٢٠١١. [٢٤] وفي هذه الأثناء من العام ٢٠١٢ إلى العام ٢٠١٣، تضاعف عدد الهجمات التي استهدفت الأنظمة الإشرافية للتحكم وتحليل البيانات (SCADA)، ومن ثم مرة أخرى في العام الماضي. [٢٥]

ومع ذلك، كانت استجابة الشركات الموّردة لهذه الأنظمة بطيئة جداً. في حين أن صانعي هذه الأنظمة قد بدأوا بالفعل في إصدار تحديثات للبرامج إلا أن تطوير هذه التحديثات كان أيضاً بطيئاً جداً. وعلاوة على ذلك، فإن تحديث أنظمة التحكم الصناعية، المصممة ليتم توزيعها في مناطق جغرافية واسعة ولمقاومة العبث، ليست بالعملية السهلة.

لحين تمكن الموّردون ومهندسو الأمن من إيجاد حلول لهذه القضايا، يبقى أفضل مسار لموفري البنية التحتية الحيوية هو التأكد من انفصال التكنولوجيا التشغيلية المستخدَمة عن تكنولوجيا المعلومات. وقال محمد أبو نجم، رئيس قسم الأنظمة وعمليات الشبكة في شركة قطر غاز، أنه: «ليس هناك الكثير من الخيارات. نحن بحاجة إلى إعادة هيكلة الخدمات في جميع أنحاء نظام SCADA باستخدام تقنيات مختلفة ولكن دون المساس بجوهر أنظمة SCADA.»

من الممكن للتكنولوجيا الأمنية الجديدة أن تساعد، على سبيل المثال، باستطاعة الأنظمة المبرمجة والموصولة للسماح فقط لمنتجات SCADA بالتواصل إلى أنظمة الرقابة ولكن دون السماح بالوصول إلى الأجهزة، بأن تُقيم جدار حماية فعلي لشبكة تشغيلية ضد أي هجوم محتمل.

التأكد من العمل الصحيح للبنية التحتية الحيوية

عندما يستغل المهاجمون الأنظمة، فإنهم عادة ما يتتسببون في تصرّف أجهزة الكمبيوتر بطرق غير متوقعة. وقد تعاون الباحثون في معهد قطر لبحوث الحوسبة مع مختبر علوم الحاسوب والذكاء الاصطناعي (CSAIL) في معهد ماساتشوستس للتكنولوجيا لبناء النُظم التي تشمل نماذج من السلوك الصحيح ومن ثم التحذير عندما تحيد عن هذا السلوك. وتشمل هذه الأجهزة نظام الوسيط المعرفي، يُطلق عليه اسم ARMET، والذي يكتشف الأحداث التي تشير إلى هجوم ويقوم بتشخيص المشكلة وتقرير الإجراءات الأنسب لاحتواء آثارها واستعادة الوضع العادي.

وقال الدكتور ديميتريوس سيربانوس، وهو عالم رئيسي في معهد قطر لبحوث الحوسبة: «سيقوم النظام بمراقبة التطبيقات المدمجة وأنظمة التحكم الصناعية ويقارن سلوكهم مع المواصفات القصوى لتحديد ما إذا كان هناك شيء ما غير طبيعي يحدث وليتمكن من استعادة الوضع الصحيح من الهجمات والفشل العشوائي في إطار العمل المستمر.»

الخطر الثالث

البرامج الضارة والجهات الفاعلة تنمو أكثر تطوراً مع زيادة تنوع الأهداف

تزداد هجمات مجرمو الإنترنت على الأهداف في دولة قطر في حين تكشف البيانات عن التركيز القائم من قبل جماعات تجسس.

أبرز الحقائق

- أصبحت الإنترنت المصدر الأكثر شيوعاً للعدوى عوضاً عن أقراص الفلاش أو الوسائط المحلية الأخرى.
- ارتفاع عدد المجموعات المتطورة التي تهاجم الأهداف في منطقة الشرق الأوسط باستخدام البرمجيات الضارة (malware) وهجمات الحرمان من الخدمة والبوت نِت.
- نظراً لشعبية وانتشار الهواتف الذكية في المنطقة، فمن المتوقع أن تزيد الهجمات عليها إذا تمكن المهاجمون من جني المال بنجاح من تلقاء هذه الهجمات.
- الموارد الموجودة في منطقة الخليج جعلت من دولة قطر وغيرها هدف جذّاب لجرائم الإنترنت والتي هي مشكلة متنامية في منطقة الشرق الأوسط.

خلال العامين الماضيين، حصل ارتفاع سريع بعدد الهجمات التي استهدفت المؤسسات التجارية والبنية التحتية والحكومة المحلية. فقد واجهت أجهزة الكمبيوتر في الشرق الأوسط في العام ٢٠١٤ المزيد من البرمجيات الضارة بنسبة تصل إلى ٤٠ في المئة مقارنة بالعام السابق، وذلك وفقاً لشركة كاسبرسكي لاب الأمنية.[٢٦] في دولة قطر على وجه التحديد، إزداد عدد هجمات الحرمان من الخدمة على مزوّدي الشبكة المحلية بنسبة ٢٠ في المئة في العام ٢٠١٤، وفقاً لمزود خدمة الإنترنت أوريدوو.[٢٧]

في حين أن انتشار البرمجيات الضارة والهجمات على مواقع الإنترنت لديها العديد من الجذور، إلا أن تزايد الهجمات الأكثر تطوراً وتدميراً المنسوبة لدول ولمجرمي الإنترنت هو أمر مقلق. في نوفمبر من العام ٢٠١٤، اكتشفت شركة سوني بيكتشرز إنترتينمنت بأنه تم اختراق أنظمتها اختراقاً تاماً وذلك عندما ظهرت صورة على شاشات الشركة تُعلن أن قراصنة كمبيوتر يطلقون على أنفسهم اسم حَرّاس السلام (GOP) قد قاموا بسرقة بيانات الشركة.[٢٨] قام القراصنة بحذف الكثير من المعلومات الموجودة على الأنظمة المصابة، واصفين ما قاموا به على أنه رد على الفيلم الذي أنتجته شركة سوني والذي يعتبره القراصنة أنه مسيئاً.

بغض النظر عمّا إذا كان الهجوم من طرف دولة أو تصرف فردي من أحد العاملين في الشركة أو حملة قرصنة، فإن الضرر الهائل الناتج يشير إلى إمكانية وصول المهاجمين عبر الفضاء الإلكتروني والتأثير على من يختلفون معهم بالرأي إن كانت شركة أو منظمة أو دولة. إلى حين الوصول إلى معايير دولية بخصوص عمليات الإنترنت ستستمر الدول وكذلك المتظاهرون والمجرمون في شن الهجمات عبر الإنترنت كالوسيلة المفضلة والممكن إنكارها.

وقال توم كيللرمان، الرئيس التنفيذي للأمن المعلوماتي في شركة تريند مايكرو ومحلل المخاطر السابق للبنك الدولي أن: «الإنترنت هي مظهر من مظاهر الجغرافيا السياسية، ولكن في نواح كثيرة ستكون النذير الأول.»

يؤكد الهجوم على شركة سوني، مثل الهجمات على راس غاز وشركة أرامكو السعودية، الأخطار المتمثلة في العناصر الخارجة على الشرعية في البيئة الإلكترونية. بينما أن الدول والشعوب المسؤولة عن أفعالها سوف تتخذ قرارات منطقية تستند إلى الأهداف الاستراتيجية، إلا أن التنبؤ بأفعال الجماعات المارقة، سواء كانت حكومات أو أفراد، هي أصعب بكثير.

وقال جن ويدون، مدير في شركة فاير آي للخدمات الأمنية، أنه: «إذا كانت هذه الجهات قد تصوّرت بأن فيلم مسيء يُمثّل تهديداً وجودياً، إذاً علينا أن نتوقع منهم أن يتصرفوا بطرق لم نتوقعها بعد.»

الهندسة الاجتماعية أصبحت الناقل الرئيسي للتسوية

خلال عقد كامل من الزمن، مثّلت الوسائط المحلية، مثل شرائح ذاكرة USB والأقراص والأقراص المدمجة، أكبر وسيلة عدوى للأنظمة في الشرق الأوسط.[٢٩] لكن خلال العام الماضي، أدى الاستخدام المتزايد لشبكة الإنترنت وتطوّر المهاجمين إلى ظهور طرق مختلفة لانتشار البرامج الضارة عن طريق الهندسة الاجتماعية، ذلك وفقاً لبحث دراسي من شركة كاسبرسكي لاب الأمنية.

وقال غريب سعد محمد، كبير الباحثين في مجال الأمن مع فريق البحث والتحليل العالمي في شركة كاسبرسكي لاب، أن:

«العدوى من خلال الإنترنت قد تزايدت بشكل كبير خلال العام الماضي، وقد نتج عن هذا التحوّل أنواع جديدة وأكثر استهدافاً من البرمجيات الضارة والتي أصبحت أكثر شيوعاً، مثل أحصنة طروادة المصرفية وبرامج التجسس وبرامج رصد لوحات المفاتيح (keyloggers) وبرامج الإعلانات (adware).»

بما أن الإنترنت أصبحت الناقل الرئيسي للهجوم، كذلك أصبحت الهندسة الاجتماعية الطريقة التي يستخدمها المهاجمون لاختراق الأجهزة المستهدفة. وتشمل الهندسة الاجتماعية تقنيات بسيطة مثل رسائل البريد الإلكتروني الوهمية وأُخرى أكثر تطوراً، مثل اختراق مواقع إنترنت شرعية وإصابة بعض المتصفّحين لها ببرمجيات ضارة. وتقدّر شركة تريند مايكرو الأمنية بأن مثل هذه الهجمات قد إزدادت ستة أضعاف.[٣٠]

قد تُصبح الهجمات المعتمدة على التجسس والتعطيل أكثر شيوعاً

تتبع العديد من الهجمات على الشبكات والأنظمة في الشرق الأوسط من خارج المنطقة وحوالي ٥ في المئة من جميع البرمجيات الضارة المتطورة التي أصابت منطقة أوروبا والشرق الأوسط وأفريقيا (EMEA) في النصف الأول من العام ٢٠١٤، كانت بالفعل قد استهدفت دولة قطر، وفقاً لشركة فاير آي الأمنية. [٣١]

ومع ذلك، فإن هناك عدد متزايد من المجموعات الإقليمية المسؤولة عن هجمات ضد دول في الشرق الأوسط. على سبيل المثال، مجموعة صقور الصحراء التي تم اكتشافها مؤخراً، تبدو وكأنها من المتحدثين باللغة العربية وقامت بسرقة أكثر من مليون وثيقة من الجهات المستهدفة وإحداها على الأقل كانت في دولة قطر. [٣٢] وقامت مجموعة الجيش السوري الإلكتروني في أكتوبر من العام ٢٠١٣ بإعادة توجيه طلبات لمواقع إنترنت قطرية إلى مواقع تنشر الأفكار المؤيدة لنظام الأسد. [٣٣]

وقال شريف علي السيد، مستشار أمن المعلومات مع وزارة الداخلية: «إن المشهد قد تغيّر فعلاً، نحن نشهد الآن مجموعة أكثر تعقيداً من قبل.»

بالإضافة إلى التطوّر المتزايد للمهاجمين في المنطقة، هناك تقنيتان مثيرتان للقلق أصبحتا أكثر شيوعاً. إحدى التوجهات الخطيرة هي البرمجيات الضارة (malware)، مثل هجوم فيروس شامون في العام ٢٠١٢ ضد شركة أرامكو السعودية وشركة راس غاز، والتي دُمّرت البيانات على الأنظمة المستهدفة. مثل هذه التقنيات التدميرية قامت أيضاً بحذف بيانات أثناء الهجوم على شركات وسائل الإعلام الكورية الجنوبية في العام ٢٠١٣ والهجوم على شركة سوني بيكتشرز إنترتينمنت في العام ٢٠١٤. فقدان البيانات من شركة سوني بيكتشرز أدى إلى تعطيل الأعمال الهامة وألحق أضرار بقيمة ٣٥ مليون دولار على الأقل واستقالة الرئيس التنفيذي. [٣٤]

وقال ديمتري ألبيروفيتش، الرئيس التنفيذي للتكنولوجيا والمؤسس المشارك لشركة كراودسترايك، أن:

«في حين يمكن للشركات المجهّزة جيداً أن تتغلب على تأثير مثل هذه الهجمات، إلا أن فقدان البيانات قد يؤدي إلى تعطيل كبير في الأعمال بسبب تباطؤ الجهود للرد على الحدث.»

وأضاف أن: «الوضع بالنسبة لشركة سوني كان بمثابة العاصفة المتكاملة من سرقة البيانات السرّية وتسريبها للعموم وحذف بيانات من قِبل البرامج الضارة. سيكون لمثل هذا الهجوم تداعيات على الأعمال لسنوات قادمة، وهذا بالتأكيد تطور مقلق».

أسلوب آخر يجعل من الصعب الكشف عن الهجمات أو التخفيف من تأثيرها يستبدل استخدام البرمجيات الضارة بسرقة بيانات اعتماد مسؤول في الشركة واختراق الشركة والتظاهر كأحد الموظفين. هذا الأسلوب يجعل من الصعب نسب الهجمات لطرفٍ ما بسبب عدم وجود البنية التحتية أو البرمجيات الضارة التي يمكن أن تربط الهجوم إلى مجموعة معينة.

وأضاف ألبيروفيتش: «نرى الخصوم يستخدمون هذه الأساليب الخالية من البرمجيات الضارة حيث يتم الاختراق وسرقة بيانات الاعتماد واستخدام أدوات المسؤول وليس البرمجيات الضارة، والتنقّل في جميع أنحاء الشبكة وسرقة المعلومات. وهذا يخلق تحدياً حقيقياً للمدافعين، الذين لا زالوا في عقلية 'العثور على البرمجيات الضارة'.»

أصبحت جرائم الإنترنت، والتي شكّلت تاريخياً مشكلة للدول الغربية، أكثر انتشاراً

أصبحت جرائم الإنترنت تُشكّل تهديداً أكبر لدولة قطر ودول الخليج الأخرى. فقد واجه المستخدمون بشكل عام في منطقة الشرق الأوسط في العام ٢٠١٤ ثلاث أضعاف حالات الهجوم بأحصنة طروادة المصرفية مقارنة بالعام السابق. [٣٥] بالإضافة إلى ذلك، تم الآن ترجمة أحصنة طروادة المصرفية، فهي الآن مكتوبة باللغة العربية لتظهر وكأنها رسائل رسمية من المؤسسات المالية المحلية.

وقال محمد سعيد من شركة كاسبرسكي لاب: «في الماضي، كان ممكن للمستخدم في الشرق الأوسط أن يحصل على هجوم بحصان طروادة مصرفي، ولكن ذلك لم يسبب الضرر لأن هذه البرمجيات الضارة لم تكن مصممة لمنطقة الشرق الاوسط.»

ووفقاً لبيانات وزارة الداخلية، فإن تقريباً نصف إجمالي الجرائم السيبرانية يكون الدافع فيها مالي. [٣٦]

هناك أسلوب إجرامي آخر والمعروف باسم انتزاع الفدية (ransomware)، حيث يتم تشفير الأقراص الصلبة للجهة المستهدفة ويقوم المجرم ببيع المفتاح الرقمي. يُمَثّل هذا النوع من الجريمة نحو ٦ في المئة من جرائم الإنترنت المُبَلّغ عنها. في حين أن هذا الأسلوب معروف جداً في أوروبا وأمريكا الشمالية، إلا أن عدد قليل واجهه من المستهلكين والعاملين في مجال تكنولوجيا المعلومات في الشرق الأوسط.

والخطر الأكثر شيوعاً هو الإبتزاز عبر الإنترنت، حيث يقوم المجرم بسرقة الصور من جهاز الكمبيوتر الخاص بالضحية أو من حساب على الإنترنت، أو يقوم بالبحث عن صور محرجة، ومن ثم ابتزاز الشخص كي يدفع مبالغ شهرية. وقال شريف علي السيد من وزارة الداخلية: «لأن العديد من المستخدمين لا يعلمون كيفية الحفاظ على البيانات الخاصة بهم بطريقة آمنة، أصبحت هذه الجريمة شائعة الى حد كبير بحيث تُمَثّل حوالي ٢٠ في المئة من إجمالي الجرائم على الإنترنت.»

وأضاف أيضاً، «سيكون أمامنا أيام صعبة جدا إذ أن الأمور تزداد سوءاً والناس لا تتخذ حذرها. الناس تتبنّى التكنولوجيا وأحدث البرامج بسرع كبيرة تفوق قدرتهم على فهم المخاطر ووضع الضوابط اللازمة.»

بناء المختبر الافتراضي للبرمجيات الضارة (Malware)

يحتاج المتخصصون في مجال الأمن إلى مختبر افتراضي لاختبار الملفات المشبوهة والبرمجيات الضارة كي يتمكنوا من معرفة من يهاجم الشركات والشبكات الحكومية في دولة قطر. يقوم معهد قطر لبحوث الحوسبة ببناء نظام تبادل مفتوح ومنصة تحليل.

قال الدكتور مارك داسيير، وهو عالم رئيسي في معهد قطر لبحوث الحوسبة، أنه: «من المهم امتلاك هذه القدرة، وهذه الخبرة محلياً. نحاول أن نفهم من هو الذي يهاجمنا، ولذلك بناء منصة تستخدمها الشركات ستتيح الفرصة لتبادل المعلومات الإستخبارية مع الآخرين.»

وبسبب وجود الكثير من البيانات في أيدي القطاع الخاص، يحتاج معهد قطر لبحوث الحوسبة لشركاء لتوضيح الرؤية بالنسبة للهجمات على الشبكات.

وقال عمر الراوي، مهندس البرمجيات في معهد قطر لبحوث الحوسبة: «إن الشراكة مع مزوّدي خدمة الإنترنت المحليين ستعطينا رؤية أفضل عمّا يحدث في قطر.»

الخطر الرابع

تبنّي التكنولوجيا المتصلة يزيد من الفرص الاقتصادية لكنه يشكل خطراً على الخصوصية

التكنولوجيا المتنقّلة المتصلة والأجهزة الذكية والاستخدام المتزايد للإنترنت ستضع حياة المواطنين على الإنترنت ما لم تأخذ التربية وحماية الخصوصية دورها.

أبرز الحقائق

- تبنّي قطر السريع للأجهزة والتكنولوجيا المتّصلة بالإنترنت يجعل الخصوصية قضية متزايدة الأهمية.
- إنترنت الأشياء ستضع حياة المواطنين على الإنترنت مما يجعل تعزيز الأمن والحماية الأشمل للخصوصية ضروريا.
- مراقبة وتحليل البيانات حول المواطنين قد تساعد على حماية المجتمع إلا أنها أيضاً تُشكّل مخاطر بالنسبة للخصوصية.
- سيستمر التوجه نحو تصنيف وتنميط المواطنين لينتقل من فهم سلوك المستهلك الى التأثير عليه.

مع ازدياد عدد الذين يستخدمون أجهزة الهاتف الذكية والتواصل عبر الإنترنت واستخدام أجهزة متصلة بالإنترنت، سيتم تسجيل وتجميع جزءاً أكبر من حياتنا على الإنترنت من قبل الغير، وتعمل شركات عديدة على جمع هذه البيانات. ففي حين أن منطقة الشرق الأوسط وشمال أفريقيا أقل اهتماماً بالخصوصية على الإنترنت، فإن مواطني دولة قطر وغيرها من الدول الأعضاء في مجلس التعاون الخليجي هم على الأرجح أكثر إدراكاً لأخطار وضع بياناتهم على الإنترنت. [٣٧]

وتقول الدكتورة مشاعل الصباح، الباحثة في معهد قطر لبحوث الحوسبة والتي تجري في الوقت الحالي بحثاً في معهد ماساتشوستس للتكنولوجيا:

«في العالم الحقيقي، القطريون على قدر كبير من الوعي بالخصوصية ولكن في العالم الرقمي، لا يزال هناك حس غير متطور بالنسبة لموضوع الخصوصية حيث لا يزالون يظهرون معلوماتهم على الإنترنت.»

الناس في قطر أقل اهتماماً بالمراقبة الحكومية لكنهم قلقون على خصوصيتهم. فعدد المواطنين غير المهتمين بمراقبة الاتصالات عبر الإنترنت في الشرق الأوسط يصل الى الضعفين مقارنة مع المعدل العالمي (١٧٪ مقارنة مع ٨٪). [٣٨]

ويقول الدكتور رايان رايلي، الأستاذ المساعد في قسم علوم وهندسة الكومبيوتر في جامعة قطر: «يرى العديد من طلبتي أن المراقبة ضرورية من أجل الأمن وهو أمر يتوجب على الحكومة القيام به، إلا أن إبقاء التوازن ما بين تلك الرغبة مع رغبتهم بالحفاظ على الخصوصية يبدو أكثر تعقيداً.»

ستوفّر إنترنت الأشياء كمية كبيرة من البيانات حول المستهلك وستجعل قضايا الخصوصية أكثر جدية

تمضي قطر قدماً كواحدة من الأمم الرائدة في مجال المدن الذكية. فاستعداداً لكأس العالم «فيفا ٢٠٢٢» تقوم قطر بإنشاء مدينة «لوسيل» حيث يتم دمج التكنولوجيا ضمن التصميم. فمن إشارات المرور إلى أنظمة الطاقة إلى إدارة النفايات، تُركّز مثل هذه المدن على استخدام تكنولوجيا المعلومات لجعل الإدارة المدنية أكثر كفاءة وفعالية.

الحواسب وأجهزة الاستشعار القابلة للارتداء و التشغيل الالي للمنازل والحواسب المضمّنة داخل أجهزة أخرى كالسيارات، ستخلق مستقبلاً يزداد فيه اعتماد المواطنين على الحاسوب ويترك فيه الشخص أثراً رقمياً في حياته اليومية، وحسب التقديرات، سيكون هناك حوالي ٥٠ إلى ٢٠٠ مليار جهاز قيد الاستخدام بحلول عام ٢٠٢٠. [٣٩]

يقول الدكتور جايديب سريفاستافا، مدير أبحاث الحوسبة الاجتماعية في معهد قطر لبحوث الحوسبة: «علينا أن نتساءل عن الآثار الجيدة والسلبية لهذه الأجهزة على طريقة الحياة التقليدية. والكيفية التي ستؤثر فيها أصبحت مكشوفة على الملأ، فهي تحدث بسرعة كبيرة جداً.»

في معرض التنبؤ بمدى تأثير هذه الأجهزة على المجتمع فإن التبنّي السريع لهذه التكنولوجيا سيُسلّط الضوء على التعامل مع البيانات الشخصية ويجعل السياسات الوطنية أكثر أهمية.

الخطر الرابع

تركيز الشركات على تحليل البيانات الكبرى قد يُعرّض الخصوصية الشخصية إلى الخطر

إن إمكانية وصل الأجهزة والسماح للناس بالوصول إلى المعلومات في كل مكان تحمل في طياتها وعوداً كبيرة. إلا أن هذا التحليل قد يُسرّب معلومات هامة إلى العلن حتى لو كانت البيانات مجهلة المصدر. لقد بيّنت دراسات عن استخدام الفيديو واستخدام محركات البحث وغيرها من الأنشطة على الإنترنت بأن بيانات البحوث، حتى المجهلة المصدر منها في حال توفر ما يكفي منها، باتت تُشكّل خطراً على الخصوصية.

> يقول الدكتور تينغ يو، وهو باحث رئيسي في معهد قطر لبحوث الحوسبة: «هناك حالات عديدة تُظهر بأن منع الاستنتاج بين البيانات الشخصية ليس بالأمر السهل عند نشر بيانات حول مجموعة من المستخدمين. سيحاول المهاجمون الربط بين أية بيانات، حتى لو كانت غير شخصية، وبيانات أخرى في محاولة للكشف عن معلومات شخصية».

ففي حين تعمل الحكومة على خلق إطار قانوني لتطبيق أنظمة الخصوصية، فإن قدرة الشركات على إجراء تحليلات لكتل كبيرة من البيانات، بما فيها عادات التصفّح أو خيارات شراء الملابس عند مواطني قطر، ستُسَلّط الضوء على مخاطر جديدة فيما يتعلق بالخصوصية.

تحليلات الإنترنت ستنتقل من فهم سلوك المستهلك إلى التأثير عليه

بما أن البيانات حول المستهلك تُشكّل سلعة قيّمة في عالم الأعمال، فإن تجميع البيانات وتحليل عادات المستخدم سيستمر في غياب سياسات أكثر صرامة. هناك مجموعة من خدمات شبكة الإنترنت، بدءً بمحركات البحث وحتى وسائط التواصل الاجتماعي، تعمل على تجميع المعلومات حول مستخدميها منشئة في نفس الوقت ملفات شخصية لزبائنها تقوم ببيعها لاحقاً كمصدر إضافي للإيرادات.

لقد بدأت الشركات بالانتقال لما بعد تنميط المستخدمين فقط. ففي العام ٢٠١٤ تبيّن لباحثين من فيسبوك وجامعة كورنيل بأن تصفية وإزالة العبارات السلبية نتج عنها مشاركات أكثر إيجابية وبالعكس.[٤٠] أي بعبارة أخرى، أظهر الكاتب كيف يمكن للمستخدمين نقل حالتهم العاطفية للآخرين، إلكترونياً عن طريق العدوى العاطفية مما يجعلهم يشعرون بنفس المشاعر دون علمهم. تُبرز هذه النتيجة إمكانية التأثير من خلال الإنترنت على عقول الناس عن طريق عدوى واسعة النطاق عبر شبكات التواصل الاجتماعية. وفي مقالة لاحقة، ذكر فيسبوك بأنه قد تم وضع المزيد من الإرشادات لمثل هذه الأبحاث مستقبلاً ولكن دون تقديم أي اعتذار أو وعد بالامتناع عن مثل هذا الاستغلال مستقبلاً.[٤١]

وقال الدكتور أحمد المقرمد، المدير التنفيذي لمعهد قطر لبحوث الحوسبة: «لقد بدأت الموجة التالية من الهجوم على الخصوصية في الظهور مع تقدّم الذكاء الإصطناعي، ومن المحتمل لشركة أن تستغل مواقف وردود أفعال المستخدمين لتغيير إعجابهم وعدم إعجابهم وعدم الاكتفاء بتوثيق وتتبّع سلوكهم.»

هناك بالفعل بعض المؤشرات على حدوث مثل هذا الاستغلال على الرغم من أنه بغرض الرقابة وليس الربح. بحثت الشركة الأمنية «Thinkst»، والتي تُقدّم المشورة الى شبكة «الجزيرة» عن استغلال وسائط التواصل باستخدام «حسابات وهمية» لتجد منتديات على الإنترنت تسيطر عليها مثل هذه الحسابات.[٤٢]

وقال هارون مير، المستشار لدى الجزيرة وكبير المستشارين لدى «Thinkst»:

> **«باستطاعتك بسهولة اكتشاف جيوش من البرمجيات الضارة قيد الاستخدام والتأكد من أن أي تعليق لطرف ما سيحظى بحصة الأسد من الاهتمام».**

الجهود الحالية في الأمن المعلوماتي

حددت قطر موضوع الأمن المعلوماتي كواحد من أهم التحديات الكبرى في البلد. في العام ٢٠١٤، وجهت الدولة جهود البحث والتطوير لتخفيف تهديدات الهجمات الحالية وإيجاد سبل لحماية البيانات والبنية التحتية الرقمية المستقبلية. وتشمل التحديات الأخرى ذات الأولوية العالية الأمن المائي وأمن الطاقة والرعاية الصحية. [٤٣]

كما أظهرت المقاطع السابقة، التهديدات القادمة من المجرمين على الإنترنت والقراصنة والجهات التجسسية على شبكة الإنترنت مستمرة ولا تتلاشى، بل أصبحت أكثر حدة. إن الأمن المعلوماتي هو تحدي يؤثر في العديد من المجالات ويعتمد عليه جزءاً كبيراً من البنية التحتية للدولة الآن أو سوف يعتمد عليها في المستقبل. وقد أنشأت دولة قطر أساساً متيناً لسياستها بما في ذلك إنشاء الاستراتيجية الوطنية للأمن السيبراني وسياسة تأمين المعلومات الوطنية وصياغة قوانين لحماية البيانات والتواصل مع الإنتربول لإجراء مراجعة وتقييم من جهة مستقلة.

١. المدن الذكية تسلط الضو علي اهمية الامن السيبراني

وقال محمد سميع الله، مدير أمن تكنولوجيا المعلومات وإدارة المجال لمشروع مشيرب، أن: «المستقبل سيجعل هذه الجهود أكثر أهمية. على سبيل المثال، تتّوعّد المدن الذكية برفع مستوى المعيشة للسكان وأصحاب الأعمال من خلال الاستخدام الفعّال لتكنولوجيا المعلومات والاتصالات. ومع ذلك، يجب تضمين الأمن داخل البنية التحتية لأن زيادة الاتصال يمكن أن تزيد من الخطر.»

وقال: «كلما زادت نسبة الربط والاتصال، كلما أصبح الهدف أكثر عرضة للهجوم، ونقطة ضعف واحدة قد تؤدي إلى كارثة، وهذا ما يجعل من الأمن عنصراً أساسياً للبحث فيه.»

وقد حددت دولة قطر تطوير المدن الذكية كمبادرة رئيسية للمستقبل وكذلك بناء المدن الجديدة مثل لوسيل والمشاريع الأخرى مثل مشيرب، لتتضمن مجموعة متنوعة من التقنيات التي تُسَهّل عملية الإدارة على مستوى المدينة. وجعلت QCERT وضع معايير الأمن السيبراني للمدن الذكية من الأولويات للعام ٢٠١٥. [٤٤]

وقال الدكتور حسين بحران، مدير المشاريع الخاصة في معهد قطر لبحوث الحوسبة، أن:

«معظم مشاريع المدن الذكية في دولة قطر تعتزم استخدام، وفي بعض الحالات بناء، مراكز البيانات المحلية الخاصة بها لتخزين الكم الهائل من بيانات المستخدمين التي سيتم جمعها بواسطة أجهزة الاستشعار والخدمات الذكية الأخرى المقدمة للمقيمين والزوار. وسيتم الحفاظ على هذه البيانات بدقة لضمان خصوصية المستخدم وللامتثال كحد أدنى لقانون خصوصية البيانات المتوقع، والذي ينتظر حالياً موافقة الحكومة النهائية.»

يتم بناء الأمن السيبراني في تصميم لوسيل حيث أنظمة التحكم والسيطرة المركزية تستخدم شبكة خاصة ومراجعات مستمرة للتصميم والمشاركة في تقييم الهجوم. وقال ابراهيم كوتشاغوز، مدير مشروع المدن الذكية لمشروع تطوير مدينة لوسيل: «نحن نركز على حماية بنيتنا التحتية وشبكتنا من الهجمات السيبرانية وندرس كافة الجوانب الأمنية التي تقع تحت مسؤوليتنا.»

بشكل عام، أخذت دولة قطر نهجاً مماثلاً، ويصف القسم التالي بعض الجهود الجارية حالياً في قطر.

٢. السياسات الوطنية

تواصل حكومة قطر تطوير عدد من السياسات لتعزيز الأمن السيبراني مع التركيز على الخصوصية والبنية التحتية الحيوية وتحسين تدريب الأمن السيبراني والتعليم.

قانون حماية المعلومات الشخصية

قامت حكومة قطر في عام ٢٠١١ بنشر الصيغة الأولى لقانون حماية خصوصية المعلومات الشخصية والذي يجعل الشركات والمشغّلين مسؤولين عن المعلومات الشخصية التي يجمعونها عن المواطنين. تمت الموافقة على القانون من قِبل مجلس الوزراء في دولة قطر، وهو الآن قيد المراجعة من قِبل اللجنة التشريعية.[٤٥] ويحدد القانون المبادئ التوجيهية للشركات في مجال حماية بيانات المواطن، وبالأخص الأطفال. تتضمّن المعلومات التي يعتبرها القانون أنها معلومات حساسة بيانات تحديد الموقع الجغرافي والمعلومات حول المواضيع الحساسة، مثل الإنتماءات الدينية والحالات الطبية.

سياسات وتشريعات حماية البنية التحتية الحيوية

أصدرت وزارة الاتصالات وتكنولوجيا المعلومات (ICTQatar) في فبراير من العام ٢٠١٤ الإصدار الثاني من سياسة قطر لتأمين المعلومات الوطنية والذي يُعطي الشركات مخططاً لإنشاء برامج أمنية فعّالة للصناعات الحيوية. [٤٦] في حين أنه لم يتم بعد تطبيق قانون حماية البنية التحتية للمعلومات الحيوية إلا أنه سيُطلب من الشركات في قطاعات الطاقة والتمويل والحكومة والرعاية الصحية والاتصالات الالتزام بالقواعد التي تحددها وزارة الاتصالات وتكنولوجيا المعلومات.

وقال شيرين من MICT: «يتم الآن تطوير مختبر لاختبار مكوّنات البنية التحتية الحيوية وسوف تبدأ دولة قطر باستخدام المعايير الشائعة، وهي مجموعة من المعايير للشركات لتشهد على مستوى معيّن من الأمن. وبحلول العام ٢٠١٨، ستكون هذه المعايير إلزامية وليست فقط مشروطة.»

الاستراتيجية الوطنية للأمن السيبراني

أصدرت لجنة الأمن السيبراني الوطني لدولة قطر في مايو من العام ٢٠١٤ الاستراتيجية الوطنية للأمن السيبراني، وهي الوثيقة التي حددت خمسة أهداف حاسمة للدولة لتحسين الحماية على الإنترنت والحماية الرقمية. وتطالب هذه الاستراتيجية بذل الجهود لحماية البنية التحتية الحيوية وسرعة الاستجابة للحوادث ومشاركة المعلومات حول التهديدات ووضع إطار قانوني ملائم وتوعية المواطنين والمهنيين في مجال الاستخدام الآمن لشبكة الإنترنت وتأسيس قدرة وطنية للأمن السيبراني. إن تحسين الأمن السيبراني هو جزء من جهود قطر لإنشاء إمكانيات قوية ومتطورة لتكنولوجيا المعلومات والاتصالات (ICT) بحلول العام ٢٠١٥. [٤٧]

الجهود الحالية في الأمن المعلوماتي

تقييم الإنتربول للأمن السيبراني الوطني

تعمل دولة قطر مع مجمع الإنتربول العالمي للابتكار (IGCI) [٤٨] المنشأ حديثاً لتقييم أوضاع الأمن السيبراني في الدولة والقدرة على التحقيق في الجرائم السيبرانية ومقاضاتها. يقوم التقييم للأمن السيبراني الوطني بجمع وتحليل البيانات على قدرات قطر وتسليط الضوء على نقاط القوة والضعف في قوانين الجرائم الإلكترونية وتطبيقها.

وقال هونيس:

«في الوقت الراهن، إن المخاطر التي تواجه الأمن السيبراني في جميع البلدان مرتفعة. ولكن سعي قطر لهذا التقييم يُسلّط الضوء على الموارد الكبيرة والجهود المستثمرة في الأمن السيبراني.»

٣. الجهود المبذولة للأمن السيبراني وشراكات القطاعين العام والخاص

بالإضافة إلى جهود الحكومة لإنشاء السياسات والتشريعات والقوانين لتحسين الأمن السيبراني، هناك عدداً من المبادرات لجمع الخبراء جنباً إلى جنب مع مجموعات عامة لتوفير حماية أفضل للبنية التحتية للمعلومات.

لجان خبراء مخاطر المعلومات (IRECs)

قال شيرين من MICT: «أسست دولة قطر ثلاث مجموعات شراكة بين القطاعين العام والخاص لتبادل المعلومات حول التهديدات وأفضل الممارسات في مجال الطاقة والتمويل والحكومة. تُدعى هذه المجموعة بلجان خبراء مخاطر المعلومات (IRECs) وتجتمع مرة شهرياً لمشاركة المعلومات حول الأحداث بعد إزالة معلومات الخصوصية منها والتعاون على وضع توصيات للأمن السيبراني. وفي حين أن بعض البلدان، مثل الولايات المتحدة، لديها العشرات من مثل هذه المجموعة، إلى أن دولة قطر تتطلّب أقل بكثير.»

وأضاف: «في بعض القطاعات، ليس لدينا سوى لاعب واحد في هذا المجال، ولسنوات عديدة، على سبيل المثال، كان لدينا فقط موفّر خدمات واحد في مجال الاتصالات السلكية واللاسلكية. الآن لدينا إثنان.»

تمارين STAR للأمن السيبراني

في ديسمبر من العام ٢٠١٤، قامت QCERT بتنظيم التمرين الثاني للأمن السيبراني، STAR-٢، لزيادة مستويات استعداد كل من الحكومة والشركات. وقد اشتمل هذا التمرين على سيناريوهات خاصة بتسعة قطاعات لاختبار الاستجابة وتحسين العمل الجماعي وزيادة الوعي بقضايا الأمن السيبراني ضمن مجتمع المدافعين في البلد. وقد ضم التمرين أكثر من ٣٢٠ مشاركاً من ٣٠ منظمة كبيرة من مجموعة متنوعة من الصناعات الهامة، بما في ذلك الطيران والطاقة والمال والصحة والحكومة والاتصالات.

أمن الرعاية الصحية وحماية البيانات

قال الدكتور خوليو سي. سيلفا، المدير التنفيذي للمعلوماتية الطبية في مركز أبحاث السدرة للطب، أنه: «بحلول العام ٢٠١٦، ستستخدم غالبية المستشفيات وبعض العيادات في قطر نُظم السجلات الطبية الإلكترونية بالرغم من أن المواطنين والمقيمين في قطر قد لا يزال لديهم الشكوك بشأن حماية البيانات الحساسة وكيف سيتم استخدامها. بما أن أصحاب المصلحة الأهم في مجال الرعاية الصحية هم المرضى، فهم بحاجة إلى معرفة أنه سيتم حماية خصوصية بياناتهم الطبية.»

وأضاف: «بعض المطلوب هو شعورهم بالراحة والثقة لوجود بياناتهم في هذه الأنظمة. نعلم أن هذه بياناتهم ونعلم أيضاً أنها هامة.»

وقال مصطفى إسّمّار، مدير تقنية المعلومات وأمن المعلومات في مركز السدرة للطب والبحوث، أنه: «بينما الخدمات المصرفية والمالية لديها متطلبات أمنية صارمة إلى حد ما، إلا أن بالإمكان جعل القوانين في مجال الرعاية الصحية والطاقة وقطاعات أخرى أكثر شمولاً.»

وأضاف: «من الممكن أن يتم ضبط قطاع الرعاية الصحية والقطاعات الأخرى بطريقة أكثر فعالية والاستفادة من ضوابط أمنية موحدة ومحددة بما أن نوع المعلومات والعمليات تختلف كثيراً من قطّاع إلى آخر.»

كأس العالم لكرة القدم ٢٠٢٢

تتطلب التحضيرات لكأس العالم (فيفا) في العام ٢٠٢٢ بأن تقوم الجهات المعنية في قطر بالتركيز على الأمن السيبراني. في العام ٢٠١٤، أصبح كأس العالم لكرة القدم في البرازيل هدفاً لهجمات سيبرانية كبيرة حيث قام القراصنة التابعين لحركة مجهولة بهجمات حرمان من الخدمة قبل الحدث في يونيو ضد البنوك والوكالات الحكومية ومنظمة فيفا. استهداف المهاجمين للبرازيل جعلها في أعلى قائمة الدول المستهدفة من قبل البرمجيات الضارة بمعدّل أربعة أضعاف الهجمات التي استهدفت روسيا ، والتي تقع في المركز الثاني على القائمة. [٤٩]

بالفعل، بدأت قطر التحدث مع دول أخرى حول تجاربهم في توفير الأمن لمباريات كأس العالم، في العالم الحقيقي وعلى الإنترنت على حد سواء. بالتعاون مع الإنتربول، التقى مسؤولون قطريون مع السلطات البرازيلية في نوفمبر لمناقشة الدروس المستفادة من هجمات الإنترنت التي استهدفت المؤسسات البرازيلية. [٥٠] وفي فبراير، التقى خبراء قطريون مع المنظمين من المملكة المتحدة التي استضافت دورة الألعاب الأولمبية الصيفية لعام ٢٠١٢. [٥١] وقال عمر شيرين من وزارة الاتصالات وتكنولوجيا المعلومات: «باقترابنا من كأس العالم، تقوم الدولة ببناء بنية تحتية جديدة صُمّمت لأحدث التكنولوجيا. هذا هو التحدي الذي نواجهه: نحاول أن نتعلم من كل التجارب السابقة والدروس المستفادة.»

المساهمون في التقرير

الدكتور تامر أبو علي
الرئيس التنفيذي للتكنولوجيا في الشرق الأوسط وأفريقيا، قسم الأمن في شركة آي بي إم

محمد أبو نجم
رئيس النّظم وعمليات الشبكة لقطر غاز

ديمتري آليبروفيتش
الرئيس التنفيذي للتكنولوجيا والمؤسس المشارك لشركة كراودسترايك

عمر الراوي
مهندس أول برمجيات - الأمن المعلوماتي، معهد قطر لبحوث الحوسبة

شريف علي السيد
مستشار أمن المعلومات، وزارة الداخلية

علي ماجد الهاشمي
حوكمة تكنولوجيا المعلومات والمعايير، مدير في مديرية تكنولوجيا المعلومات، مؤسسة قطر

فيصل الكواري
الرئيس التنفيذي للتكنولوجيا، Meeza.net

الدكتور مشاعل آل الصباح
عالم، الأمن المعلوماتي، معهد قطر لبحوث الحوسبة

الدكتور حسين بدران
مدير المشاريع الخاصة في معهد قطر لبحوث الحوسبة

مصطفى هنيد بنغالي
أمن معلومات الشركات في مكتب الرئيس التنفيذي، أوريدوو

سيزار سيرّودو
الرئيس التنفيذي للتكنولوجيا، IOActive

الدكتور مارك داسيير
عالم رئيسي، معهد قطر لبحوث الحوسبة

الدكتور سوميترا دوتا
عميد وأستاذ الإدارة والمنظمات، كلية جونسون للدراسات العليا للإدارة، جامعة كورنيل

الدكتور أحمد خليفة المقرمد
المدير التنفيذي لمعهد قطر لبحوث الحوسبة

مصطفى إسّمّار
مدير تقنية المعلومات وأمن المعلومات في مركز السدرة للطب والبحوث

ستيف هونيس
مدير سايبر ناشيونال ريفيو، مُجمّع الإنتربول العالمي للابتكار

توم كيلليرمان
الرئيس التنفيذي للأمن السيبراني، تريند مايكرو

الدكتور عيسى خليل
عالم أول، أمن الشبكات وتحليلات البيانات الآمنة، معهد قطر لبحوث الحوسبة

إبراهيم كوتشاغوز
مدير مشروع المدن الذكية، مشروع تطوير مدينة لوسيل

هارون مير
مستشار لقناة الجزيرة / مؤسس ومستشار رئيسي لشركة Thinkst

جون ميلر
نائب الرئيس للاستراتيجية في شركة Cylance

أسامة كمال
مدير قسم استخبارات التهديدات السيبرانية،وزارة الاتصالات وتكنولوجيا المعلومات في قطر

غريب سعد محمد
باحث أمني أول، كاسبرسكي لاب - القاهرة

الدكتور رايان رايلي
أستاذ مساعد، قسم علوم الحاسوب والهندسة، جامعة قطر

الدكتور غييوم صالحة
رئيس هندسة الأنظمة، هندسة أمنية، قطر للبترول

محمد سميع الله
مدير أمن تكنولوجيا المعلومات وإدارة المجال لمشروع مشيرب

الدكتور ديميتريوس سيربانوس
عالم رئيسي، الأمن المعلوماتي، معهد قطر لبحوث الحوسبة

عمر شيرين
مدير قسم حماية معلومات البنية التحتية الحيوية، وزارة الاتصالات وتكنولوجيا المعلومات

البروفيسور هاورد شروب
عالم أبحاث رئيسي، علم الحاسوب ومختبر الذكاء الاصطناعي في معهد ماساتشوستس للتكنولوجيا

الدكتور خوليو سي. سيلفا، MD، MPH
الرئيس التنفيذي للمعلوماتية الطبية، مركز السدرة للطب والأبحاث

جايديب سريفاستافا
مدير أبحاث الحوسبة الاجتماعية، معهد قطر لبحوث الحوسبة

جين ويدون
مدير في شركة FireEye

الدكتور تينغ يو
عالم أول - الأمن المعلوماتي، معهد قطر لبحوث الحوسبة

ENDNOTES

[1] ictQatar. National Information Assurance Policy v 2.0. Ministry of Information and Communications Technology. March 2014. PDF file.

[2] Qatar Computing Research Institute. QCRI Emerging Cyber Threats 2014 Report. 26 Mar. 2014. PDF file.

[3] General Secretariat for Development Planning. Qatar National Vision 2030. July 2008. PDF file.

[4] INSEAD and Cornell University Johnson School of Business. The Global Information Technology Report 2014. World Economic Forum. 2014. PDF file.

[5] Mia, Irene and Dutta, Soumitra. The Global Information Technology Report 2007-2008. World Economic Forum. PDF file.

[6] Frost & Sullivan. Global Cyber Security Assessment 2014 - Executive Summary. 2014. PDF file.

[7] Musil, Steven. Senate panel approves controversial cybersecurity bill. CNET News.com. 12 Mar. 2015. Web. 14 Mar. 2015.

[8] Ministry of Information and Communications Technology (ictQatar). Qatar National Cyber Security Strategy. May 2014. 10-11, 14. PDF file.

[9] Mackenzie, Heather. Shamoon Malware and SCADA Security – What are the Impacts? Tofino Security blog. 25 Oct. 2012. Web. 23 Feb 2015.

[10] Cylance. Operation Cleaver Report. Dec. 2014. PDF file.

[11] Cylance. Communication with author. Data not published in the Operation Cleaver Report.

[12] Q-CERT. Fact Sheet: National Cyber Drill (STAR-2). ictQatar. 16 Dec. 2014. PDF file.

[13] Lemos, Robert. "Cybersecurity information sharing initiatives on the rise." TechTarget. May 2012. Web.

[14] Frost & Sullivan. Critical Times Demand Critical Skills: An analysis of the skills gap in information security. ISC2. 2013. PDF file.

[15] Rassed Group and the Ministry of Information and Communications Technology (ictQatar). The attitudes of online users in the MENA region to Cybersafety, Security and Data Privacy. 2014. 42 - 43. PDF file.

[16] Perlroth, Nicole. "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back." The New York Times. 23 Oct 2012. Web.

[17] See Cylance, Operation Cleaver.

[18] See ictQatar, Qatar National Cyber Security Strategy, especially pages 10 and 13.

[19] Ministry of Information and Communications Technology (ictQatar). Qatar National Information Assurance Policy (v2.0). March 2014. PDF file.

[20] Greenwald, Glenn. How the NSA tampers with US-made internet routers. The Guardian: London. 12 May 2014. Web. 23 Feb. 2015.

[21] Krebs, Brian. Target Hackers Broke in Via HVAC Company. KrebsOnSecurity.com. 5 Feb. 2014. Web. 23 Feb. 2015.

[22] See Kaspersky Labs' Global Research & Analysis Team, The Desert Falcons.

[23] See Cylance, Operation Cleaver.

[24] SCADAHacker.com. n.d. Web. 14 Mar. 2015.

[25] Dell Secureworks. 2015 Dell Security Annual Threat Report. April 2015. PDF. See pages 7 to 9.

[26] Muhammad, Ghareeb Saad, Senior Security Researcher with the Global Research & Analysis Team at Kaspersky Lab. 22 Jan. 2015. Interview.

[27] Bengali, Mustapha Huneyd. Personal interview. 28 Jan. 2015.

[28] Spangler, Todd. Sony Pictures Targeted by Apparent Hack Attack to Corporate Systems. Variety. 24 Nov. 2014. Web. 10 Mar. 2015.

[29] Muhammad, Ghareeb Saad, Global Research & Analysis Team at Kaspersky Lab. interview.

[30] Kellermann, Tom. Personal interview. 19 Feb. 2015.

[31] FireEye. Regional Advanced Threat Report - Europe, Middle East and Africa, 1H2014. Oct 2014. PDF.

[32] See discussion in Kaspersky's The Desert Falcons targeted attacks.

[33] Paganini, Pierluigi. "Syrian Electronic Army attacked most major Qatar websites." Security Affairs. 20 Oct 2013. Web.

[34] Lemos, Robert. "Sony Pegs Initial Cyber-Attack Losses at $35 Million." eWEEK. 4 Feb 2015. Web.

[35] Muhammed interview.

[36] Correspondence with Shareef Ali Alsayed, Qatar Ministry of Interior.

[37] Rassed Group and the Ministry of Information and Communications Technology. The attitudes of online users in the MENA region to Cybersafety, Security and Data Privacy. 2014. PDF file.

[38] Rassed Group 28. Note: Survey is prior to revelations about mass surveillance by intelligence agencies via Snowden.

[39] The Internet of Things. Cisco. n.d. Infographic.

[40] Kramer, Adam et al. Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences of the United States. 17 June 2014. PDF file.

[41] Schroepfer, Mike. Research at Facebook. Facebook newsroom. 2 Oct. 2014. Web. 15 March 2015.

[42] Meer, Haroon et al. Weapons of Mass Distraction: Sock Puppetry for Fun & Profit." Oct 2014. PDF.

[43] Qatar Foundation. Meeting Qatar's Grand Challenges. 21 Aug 2014. Web. 10 May 2015.

[44] Interview with Omar Sherin, Ministry of Information and Communications Technology.

[45] ictQatar. Ministry of Information and Communications Technology - Annual Report 2013/2014. 28 Jan 2015. PDF. Pg. 10.

[46] ictQatar. National Information Assurance Policy v. 2.0. Feb 2014. PDF.

[47] ictQatar. Qatar's National ICT Plan 2015: Advancing the Digital Agenda. July 2011. PDF.

[48] INTERPOL. The INTERPOL Global Complex for Innovation. Web. 12 May 2015.

[49] Kaspersky Lab. 2014 Cybercrime World Cup Brazil. 29 Jul 2014. Web. 5 May 2015.

[50] Interpol. INTERPOL brings together sporting event security experts to exchange best practice. 24 Nov 2014. Web. 3 May 2015.

[51] Aguilar, Joey. "Top Qatari official to meet UK cyber security experts." Gulf Times. 19 Feb 2015. Web. 12 May 2015.

معهد قطر لبحوث الحوسبة
الطابق ١٨ ، برج تورنيدو، الدوحة، قطر
هاتف: ٠٦٢٩ ٤٤٥٤ ٩٧٤ + فاكس: ٠٦٣٠ ٤٤٥٤ ٩٧٤ +
www.qcri.qa

معهد قطر لبحوث الحوسبة

الطابق ١٨ ، برج تورنيدو، الدوحة، قطر

هاتف: ٠٦٢٩ ٤٤٥٤ ٩٧٤ + فاكس: ٠٦٣٠ ٤٤٥٤ ٩٧٤ +

www.qcri.qa