الأمن السيبراني وزيادة استخدام التجارة الإلكترونية في ظلّ أزمة فيروس كورونا (كوفيد-19)

15.04.2020

شرق للمحاماة
Sharq Law Firm

ما هو الأمن السيبراني وكيف تتزايد قضايا الأمن السيبراني في ضوء فيروس كورونا (كوفيد-19)؟

مقدمة

في أغلب الأحيان لا يمكن تجنب الهجمات السيبرانية ، [1]تكشف الإحصاءات عن وجود حوالي 80 إلى 90 مليون هجوم إلكتروني سنويًا في جميع أنحاء العالم، فمع تطور الانترنت وزيادة استعماله بجميع النواحي الحياتية ، خطر الهجمات السيبرانية ازداد وسيزداد في المستقبل. ([2]يتم إصدار حوالي 400 تهديد جديد في الدقيقة في جميع أنحاء العالم).
الدخول غير المشروع هو النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح.

ان الجريمة الالكترونية تتمثّل في الأفعال الضارة التي يقوم بها المخترقون من خلال استعمال الأجهزة الالكترونية (الحاسب الالي ، الهواتف الذكية ، اللوحات الذكية، وغيرها..). لهذا الفعل الجرمي اثار ضارة على الشركات و على الأفراد وحتى على المواقع الحكومية. للجريمة الالكترونية تسميات عدّة وأبرزها جرائم الحاسب والانترنت. يهدف المخترقون عند قيامهم بهذا النوع من الجرائم الوصول غير الشرعي الى المعلومات والبيانات والقيام بحذفها او تعطيلها او التعديل عليها، الامر الذي يحقق هدفهم الجرمي. كما قد يكون احد أهدافهم الولوج والوصول الى المعلومات التي تتمتع بسرية تامة والموجودة لدى المصارف والمؤسسات الحكومية والأفراد والعمل على ابتزازهم بواسطتها. اما احد الأهداف الشائعة للمخترقين من خلال القيام بالوصول غير المشروع الى البيانات والمعلومات تتمثّل بتزوير البطاقات المصرفية وسرقة الحسابات المصرفية.
مع ذلك ، إنّ ظهور فيروس كورونا المستجد COVID-19 ، أدى الى تسارع وتفاقم ارقام الهجومات السيبرانية والإختراقات الالكترونية بشكل كبير.

يثير فيروس كورونا المستجد الكثير من المخاوف كما ويجعل جميع المنظمات والشركات تشعر بالقلق تجاه حماية بياناتها الشخصية. بالإضافة الى ذلك، تقوم الشركات بمعالجة البيانات الضخمة الموجودة لديها والتي ازداد عددها من جراء الإقبال على استعمال الانترنت بشكل أكبر في ظلّ فيروس كورونا. بحسب قانون مكافحة الجرائم الإلكترونية القطري رقم 14 لسنة 2014 البيانات والمعلومات الإلكترونية هي كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام وسيلة تقنية المعلومات، وبوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات وغيرها.[3]

1 Cyber Security, Source:
https://www.allenovery.com/en-gb/germany/expertise/practices/data-and-data-protection/cybersecurity

2 Cyber Security, Source:
https://www.allenovery.com/en-gb/germany/expertise/practices/data-and-data-protection/cybersecurity

3 Covid-19 coronavirus: emerging data protection and cybersecurity guidance, Allen and Overy, Source:
https://www.jdsupra.com/legalnews/covid-19-coronavirus-emerging-data-12208/

بالإضافة إلى تهديدات الأمن السيبراني ، لا بد من الإشارة الى المخاطر التي ستواجه التجارة الالكترونية في ظلّ فيروس كورونا المستجد.

من أجل تجنب الذهاب إلى المتاجر حيث يوجد خطر أعلى للإصابة ونقص محتمل في المخزون على الرفوف، ينتقل العملاء إلى متاجر التجزئة عبر الإنترنت.[4] في هذا السياق،[5]ينتقل الأشخاص تدريجيًا من التسوق في مفهومه العادي والتقليدي إلى التسوق عبر شبكة الإنترنت ، مع العلم ان هذه العادة ستستمر الى ما بعد انتهاء الوباء. بالتالي، سيكون لها تأثيراً إيجابياً للغاية على سوق التجارة الإلكترونية بأكمله.

مع استمرار أزمة فيروس كورونا في التأثير على سكان العالم ، ومع تكيف سلوكهم ، يمكن للشركات التي تقوم على التجارة الالكترونية ضمان وجودها عندما يحتاجها المستهلكون. بما انّ سلوك المستهلك يتغير وينتج عنه المزيد والمزيد من العملاء الذين يتسوقون عبر الإنترنت ، هذا الأمر سيؤدي الى تغيّر السوق ليصبح أكثر تنافسيا من أي وقت مضى حيث ستسعى الشركات للاستفادة من هذا الاتجاه، كما انّ ممارسة كل هذه النشاطات اليومية على شبكة الانترنت سيضاعف حجم الهجمات الالكترونية.

لذلك ، سنعرض فيما يلي ثلاثة أسباب لأهمية تدابير الأمن السيبراني أكثر من أي وقت مضى. إنّ الإعتماد على البنية التحتية الرقمية يتكاثر في ظلّ جائحة فيروس كورونا المستجد بحيث ازداد استعمال واستخدام المنصّات الرقمية. أصبحت شبكة الإنترنت على الفور قناة للتفاعل البشري الفعال والطريقة الأساسية للعمل والاتصال. فالشركات ومنظمات القطاع العام تفرض بشكل متزايد سياسات «العمل عن بعد»، اما التفاعلات الاجتماعية فاقتصرت على مكالمات الفيديو ومشاركات وسائل التواصل الاجتماعي. كما وأنّه تقوم العديد من الحكومات بنشر المعلومات عبر الوسائل الرقمية. في ظلّ الوضع الراهن، يمكن أن يكون الهجوم السيبراني الذي يمنع المنظمات أو العائلات من الوصول إلى أجهزتهم أو بياناتهم أو الإنترنت

4 What eCommerce Managers and Directors should know in the time of Coronavirus, TOM KARWATKA, Source https://divante.com/blog/what-ecommerce-managers-and-directors-should-know-in-the-time-of-coronavirus/

5 Zhong Zhenshan, Vice-president of emerging technology research, IDC. Source: https://divante.com/blog/what-ecommerce-managers-and-directors-should-know-in-the-time-of-coronavirus/

مدمرًا:و في أسوأ السيناريوهات ، يمكن أن تتسبب الهجمات السيبرانية في فشل البنية التحتية الرقمية على نطاق واسع مما يعيق عمل الأنظمة والشبكات العامة. ثانيا، يستغل المخترقون الضعف البشري لاختراق الدفاعات النظامية. ثالثا، قد تكون هناك مخاطر خفية في طلبات الحصول على معلومات بطاقة الائتمان أو تثبيت تطبيقات عرض متخصصة. دائمًا ، وخاصة أثناء الوباء ، يمكن أن يكون النقر على الرابط الخاطئ أو توسيع عادات تصفح الإنترنت أمرًا خطيرًا ومكلفًا للغاية.

استعداد دولة قطر في التصدي للهجومات الالكترونية

في هذا الصدد، فإن دولة قطر تعتبر حالة فريدة وخاصة، حيث أن دولة قطر ومنذ ٢٠١٧ قد ضاعفت من قوتها الدفاعية ضد الهجمات السبرانية.

في حزيران (يونيو) 2017 قام المخترقون بتحميل معلومات ملفقة على موقع وكالة الأنباء القطرية ، ثم قاموا بمجموعة كبيرة من الهجمات الالكترونية على وسائل التواصل الاجتماعي ، ولكن تمكنت دولة قطر من التصدي لهذه الأختراق، الامر الذي وضعها مركز نقاش عالمي حول الأمن السيبراني الذي يضم خبراء التكنولوجيا بالإضافة إلى المحللين السياسيين والأمنيين والسياسيين، اذ تمكنت من الاستجابة بشكل مناسب وسريع لمثل هذا الإختراق[6].

منذ ذلك الوقت عملت دولة قطر على تكثيف الجهود الدبلوماسية السيبرانية. وبشكل خاص، من خلال التركيز على الأمن السيبراني والحرب السيبرانية، كما قدمت دولة قطر منبراً للحوار المتعدد الأطراف حول الكيفية التي لا بد أن يتم بها تشكيل أخلاقيات الفضاء السيبراني والسلام السيبراني في المستقبل[7].

هكذا خروقات ليست جديدة على دولة قطر التي منذ البداية قامت باستثمارات مستمرة وكبيرة في تصميم نظام بيئي يهدف الى حماية الفضاء الإلكتروني. لقد كان ولا يزال رفع مستوى البيئة الرقمية والمعرفة التكنولوجية في دولة قطر بالإضافة الى تعزيز قدراتها ، وتطوير العلاقات مع الشراكات عبر الوطنية الرائدة في مجال الأمن السيبراني معها من المكونات الرئيسية لتقوية وتعزيز الأمن السيبراني للبلاد منذ البداية.

أما فيما يتعلق بالتجارة الإلكترونية ، فكان من المتوقع أن ينمو سوق التجارة الإلكترونية في دولة قطر إلى 2.2 مليار دولار أمريكي بحلول عام 2019 الذي مضى، ارتفاعًا من 1.2 مليار دولار أمريكي في العام 2018[8] ، مما يعني أنه مع ظهور فيروس كورونا المستجد ، تكون قطر في مقدمة هذه الأرقام، اذ أصبحت التجارة الالكترونية لها الأولوية مقارنة مع سوق التجارة التقليدية.

6 Cyber Diplomacy in Qatar – A Virtue of Necessity?, Khristo Ayad and Abed Shirzai, Source: https://intpolicydigest.org/2019/12/30/cyber-diplomacy-in-qatar-a-virtue-of-necessity/

7 Cyber Diplomacy in Qatar – A Virtue of Necessity?, Khristo Ayad and Abed Shirzai, Source: https://intpolicydigest.org/2019/12/30/cyber-diplomacy-in-qatar-a-virtue-of-necessity/

8 E-Commerce in Qatar – Statistics and Trends, Source: https://www.go-gulf.qa/ecommerce-qatar/

الإطار القانوني المتّبع في دولة قطر فيما يخصّ الأمن السيبراني

أهداف الاستراتيجية الوطنية للأمن السبراني[9]

الهدف 1:	الهدف 2:	الهدف 3:	الهدف 4:	الهدف 5:
حماية البنية التحتية الوطنية للمعلومات الحيوية الوطنية.	الاستجابة للحوادث والهجمات الالكترونية وحلها والتعافي منها من خلال تداول المعلومات في الوقت المناسب والتعاون واتخاذ الإجراءات اللازمة.	وضع الإطار القانوني والتنظيمي لتعزيز سلامة وحيوية الفضاء الالكتروني.	تعزيز ثقافة الأمن السيبراني التي من شأنها دعم الاستخدام الآمن والمناسب للفضاء الالكتروني.	تطوير وصقل الإمكانيات الوطنية للأمن السيبراني.

أطلقت الدولة عددًا من المبادرات والسياسات ، بما في ذلك استراتيجيتها الوطنية للأمن السيبراني التي تم إطلاقها في العام 2014. لا بد من الإشارة الى انه تمّ توفير خطط وادوات طويلة المدى لوضع استراتيجيات الأمن السيبراني الوطنية موضع التنفيذ من قبل مركز التحقيق في الجرائم السيبرانية ، ومكتب تنسيق الأمن السيبراني ، بالإضافة إلى فريق الاستجابة للطوارئ الحاسوبية في قطر كيوسرت (Q-CERT)[10]، هناك أيضا هيئة رسمية مفوضة بتحديد ومنع الهجمات السيبرانية ضد الحكومة والقطاعات الحيوية الأخرى، من هنا تم وضع قواعد الإشراف المصرفي التي بدأها مصرف قطر المركزي بالتنسيق مع Q-CERT لحماية المؤسسات المالية في الدولة. لا بد من الإشادة في هذا المجال بالعمل الجبار التي تقوم به وزارة المواصلات والاتصالات القطرية، حيث تقيم تدريبات سنوية فريدة من نوعها في الدولة ، وتشرك المؤسسات العامة والخاصة في مجموعة من الأنشطة التقنية والتعليمية ، وتزيد من الاستعداد والوعي حول كيفية إدارة الهجمات الإلكترونية.

القدرات الحالية لمواجهة التهديدات والتحديات

تدرك قطر أهمية الأمن السيبراني وقد عملت بجد على مدى السنوات العديدة الماضية لتطوير وتنفيذ تدابير حماية الأمن السيبراني في جميع أنحاء البلاد. هذه الإجراءات جعلت من الممكن للحكومة والشركات والمؤسسات والأفراد الاستجابة للتهديدات والتحديات في الفضاء السيبراني ، وبالتالي توفير أساس قوي لتحقيق أهداف الأمن السيبراني.[11] من بين هذه الجهود: وضعت قطر استراتيجيات ونفذت مجموعة من السياسات لحماية البنية التحتية لنظم المعلومات الحيوية التي تعتبر مهمة للأمن القومي والازدهار الاقتصادي ، مثل تلك المستخدمة لتوليد الطاقة وإنتاج النفط والغاز والمعاملات المالية والرعاية الصحية والعمليات الحكومية. بالإضافة إلى ذلك ، كجزء من سياسة تأمين المعلومات الوطنية ، أصدرت دولة قطر

9 الاستراتيجية الوطنية للأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات،
https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

10 شؤون الأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات،
https://www.motc.gov.qa/ar/cyber-security

11 Qatar National Cyber Security Strategy, Source:
https://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf

فـي العام 2013 إرشـادات لمكافحة الرسـائل غير المرغوب فيها من المؤسسـات والأفراد. كما وأنشـأت قطر لجـان خبراء مخاطر أمـن المعلومـات (IREC) فـي قطاعات التمويل والطاقة والقطـاع الحكومي. تتعامل هذه اللجان مـع مجموعة متنوعة من قضايا الأمـن السـيبراني ، بمـا فـي ذلك التهديـدات والهجمـات ونقاط الضعف الناشـئة وأنشـطة الجاهزيـة والاسـتراتيجية المعنية الأخـرى، وذلـك بهدف تحسـين مرونة البنيـة التحتية الحيوية[12]. شـكلت قطـر تحالفات دولية قوية وتشـارك بنشـاط في الجهود العالميـة لصياغـة المعاييـر والقواعـد الدوليـة المعنية بالأمن السـيبراني ، بمـا في ذلك الجهـود المبذولة في الاتحـاد الدولي للاتصـالات (ITU) ، ومنتـدى الاسـتجابة للحوادث وفرق الأمن (FIRST). تعمل الحكومة بشـكل اسـتباقي وفعّال على الاسـتثمار فـي المـوارد البشـرية ووضـع السياسـات والاجـراءات وتطبيـق التكنولوجيا، وذلك لتحسـين وتعزيـز الأمن السـيبراني للجهات الحكوميـة والشـركات والمؤسسـات والأفـراد[13]. ومع ذلك ، هنـاك حاجة إلى بذل جهـود إضافية لتلبية متطلبات المسـتقبل مع ظهـور تهديـدات جديـدة وازدياد الاعتمـاد على تكنولوجيـا المعلومات والاتصـالات. إنّ الجهود حتى الآن موزعة بشـكل موسّـع وتنطلـق مـن أدنى المسـتويات الى المسـتويات الأعلـى. توفر الجهود التي ذكرت أعلاه أساسًـا قويًا للمسـتقبل ؛ ومع ذلك ، يجـب أن تعمـل الهيئات الحكومية والشـركات والمؤسسـات والأفراد معًـا لتعزيز الأمـن الإلكتروني في قطر.

لا بـد مـن الإشـارة أيضا الـى انّ دولة قطر أحـرزت تقدماً في وضع إطـار قانوني محلي يوفـر حوكمة وطنية للأمن السـيبراني ، ويكافـح الجرائـم الالكترونيـة ، ويحمـي خصوصيـة الأفـراد14. إن المرسـوم بقانـون رقـم 16 لسـنة 2010 بشـأن المعاملات والتجـارة الإلكترونيـة يفـرض عقوبـات علـى كل مـن يقـوم بالوصـول غير المشـروع إلى نظـم المعلومـات ، وسـرقة الهوية ، واعتـراض المعلومـات أو التدخل بشـكل غير قانوني في نظام المعلومات. في عام 2013 ، أنشـأت قطـر اللجنة الوطنية للأمن السـيبراني الأمـر الـذي وفّـر هيكل حوكمـة على اعلى المسـتويات الحكوميـة وذلك من أجـل التعامل مع الأمن السـيبراني15.

العقوبـات وفقـا لقانون مكافحة الجرائـم الإلكترونية 14 لسنة 2014

إنّ قانـون مكافحـة الجرائـم الإلكترونيـة القطري رقم 14 لسـنة 2014 فـرض عقوبات جمّة وقاسـية على كل مـن يخالف أحكامه، فمثـلا نصّـت المادة الثانيـة في الفصل الأول «جرائـم التعدي على أنظمة وبرامج وشـبكات المعلومات والمواقـع الإلكترونية» علـى عقوبـة الحبـس مـدة لا تجاوز ثلاث سـنوات، وبالغرامة التـي لا تزيد على (500,000) خمسـمائة ألف ريال، لـكل من تمكن عـن طريـق الشـبكة المعلوماتية أو بإحدى وسـائل تقنيـة المعلومات، بغيـر وجه حق، من الدخـول إلى موقـع إلكتروني أو نظام معلوماتـي لأحـد أجهـزة الدولـة أو مؤسسـاتها أو هيئاتهـا أو الجهـات أو الشـركات التابعة لهـا. وتُضاعف العقوبـة المنصوص عليهـا فـي الفقـرة السـابقة، إذا ترتـب على الدخـول الحصول علـى بيانات أو معلومـات إلكترونيـة، أو الحصول علـى بيانات أو معلومـات تمـس الأمـن الداخلـي أو الخارجـي للدولـة أو اقتصادها الوطني أو أيـة بيانات حكومية سـرية بطبيعتهـا. ولا بد من الإشـارة الـى المـادة 3 مـن القانـون نفسـه التي تتطـرق الـى الاختراق الـذي يقع على الأشـخاص والتـي نصّت علـى عقوبة الحبـس مـدة لا تجـاوز ثلاث سـنوات، وبالغرامة التي لا تزيـد على (500,000) خمسـمائة ألف ريال، أو بإحـدى هاتين العقوبتين،

12 الاستراتيجية الوطنية للأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات، https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

13 الاستراتيجية الوطنية للأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات، https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

14 الاستراتيجية الوطنية للأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات، https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

15 الاستراتيجية الوطنية للأمن السيبراني، المصدر: الموقع الاكتروني لوزارة المواصلات والاتصالات، https://www.motc.gov.qa/sites/default/files/lstrtyjy_lwtny_llmn_lsybrny.pdf

لكل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، كما نصّت المادة نفسها على مضاعفة العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين. كما نصّت المادة 12 في الفصل الرابع « جرائم بطاقة التعامل الإلكتروني» من القانون نفسه على عقوبة الحبس لمدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (200,000) مائتي ألف ريال، أو بإحدى هاتين العقوبتين، لكل من قام بإستخدام أو حصل أو سهل الحصول دون وجه حق على أرقام أو بيانات بطاقة تعامل إلكتروني عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات. وكل من زور بطاقة تعامل إلكتروني بأي وسيلة كانت او صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقات التعامل الإلكتروني.

مقارنة بين قطر و الكويت[16]

قطر

صدر قانون مكافحة الجرائم الالكترونية عام 2014 ، يتضمن القانون 54 مادة ، انّ العقوبة تطال كل من تمكّن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها كما وللأفراد المستخدمين او المستفيدين والدخول والحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة. وكل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور، وكل من كل من أنشأ أو أدار موقعاً إلكترونياً عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، لنشر أخبار غير صحيحة، بقصد تعريض سلامة الدولة أو نظامها العام أو أمنها الداخلي أو الخارجي للخطر. شملت العقوبات: الحبس وغرامات مالية. عقوبة السجن تتراوح من سنة إلى 3 سنوات. في حين تراوحت الغرامات النقدية بين 100,000 ريال قطري إلى 500,000 ريال قطري.

الكويت

صدر قانون مكافحة جرائم تقنية المعلومات عام 2015. يتضمن القانون 21 مادة ، ان العقوبة تطال كل من أرتكب دخولا غير مشروع الى جهاز حاسب آلي أو الى نظامه أو الى نظام معالجة إلكترونية للبيانات أو الى نظام إلكتروني مؤتمت أو الى شبكة معلوماتية، وكل من ارتكب دخولا غير مشروع الى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون، وكل من زور أو أتلف مستندا أو سجلا أو توقيعا إلكترونيا أو نظام معالجة إلكترونية للبيانات أو نظام إلكتروني مؤتمت أو موقعا أو نظام حاسب آلي أو نظام إلكتروني بطريق الاصطناع أو التغيير أو التحوي أو بأي طريقة أخرى، وذلك باستخدام وسيلة من وسائل تقنية المعلومات، وكل من أعاق أو عطل عمدا الوصول الى موقع خدمة إلكترونية أو الدخول الى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات الإلكترونية بأي وسيلة كانت، وكل من تنصت أو التقط أو اعترض عمدا، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات. شملت العقوبات: الحبس وغرامات مالية. وتراوحت عقوبة السجن لمدة تتراوح بين 6 أشهر و 7 سنوات. بينما تراوحت الغرامات النقدية من 100 دينار كويتي إلى 300،000 دينار كويتي.

16 Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia, Source: https://www.researchgate.net/publication/326335840_Cyber_Security_Crime_and_Punishment_Comparative_Study_of_the_Laws_of_Jordan_Kuwait_Qatar_Oman_and_Saudi_Arabia

توصيات للدولة والأفراد للوقاية من القرصنة:

❖ بالنسبة للأفراد

-أولاً، لا بد من اخذ الحيطة والانتباه وعدم النقر على الإعلانات التي تصل على الأجهزة الالكترونية والتأكد من مصداقيتها اذ قد يكون الهدف من وراء بعض الإعلانات تعطيل الجهاز او سرقة البيانات والمعلومات الموجودة فيه.

-ثانياً،يجب اخذ الحذر من الرسائل الالكترونية التي تكون في الغالب مجهولة والمصدر والقيام فورا بحذفها.

-ثالثاً، التأكد من انّ الرقم السري او كلمات المرور السرية المستخدمة من الأفراد او حتى من الشركات صعبة وليس من السهل معرفتها او فكّها من المقرصنين، فيجب ان تكون كلمات المرور السرية طويلة ومؤلفة من احرف الأبجدية والأرقام والرموز.

-رابعاً، يجب وضع برامج حماية مناسبة والتي هدفها الاساسي حماية جميع البيانات والمعلومات الموجودة على الحاسب الالي من الاختراق والقرصنة وأبرزها (Total AV Free Antivirus-Kaspersky Free-Internet Security-Firewall).

لا بد من الإشارة في هذا المجال الى انّ القانون الكويتي وحده في دول الخليج الذي طلب أن يكون الجهاز أو الموقع محمي من أجل أعتبار الدخول مجرّم، امّا على الصعيد الدولي فإنّ التشريع السويدي والإيطالي والإلماني هو الذي تطرّق الى حماية الجهاز او الموقع لتجريم الفعل الذي قام به المخترق.

❖ بالنسبة للدول

يجب على الدول القيام ببعض الخطوات للتأكد من انّ لديها الاستعداد الكامل لمواجهة الأوبئة التي قد تطرأ في المستقبل وذلك عن طريق إعادة تقييم قدرات اللأمن السيبراني لديها.

-أولاً، يجب القيام بمعاينة البيانات والمعلومات للأصول الأساسية للدولة بالإضافة الى البنية التحتية الرقمية الحيوية لها وحمايتها[17].

-ثانياً، يجب العمل على تقدير التهديدات وفداحة المخاطر والقدرات الاستراتيجية للأمن السيبراني للدولة وذلك عن طريق تحديد الثغرات والعمل على تحديث خطة العمل الموضوعة من قبل الدولة.

-ثالثاً، وضع خطط من شأنها تعزيز القدرات والاستراتيجيات المتعلقة بالأمن السيبراني للدولة.

- رابعاً، الحرص على تعزيز الاقتصاد المرن مع الأخذ بالاعتبار ما ترتب من تأثيرات في هذا المجال من جراء فيروس كورونا المستجد.

-خامساً،عند وضع الخطط يجب ان تكون جميع القطاعات التابعة للدولة مشمولة فيها.

17 التهديدات والمخاطر السيبرانية الناجمة عن تفشي فيروس كورونا وسبل الوقاية منها، محمد لاوند، https://hbrarabic.com/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%88%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7

الخلاصة

في أعقاب الهجوم الإلكتروني عام 2017 على دولة قطر الذي أثار أزمة إقليمية غير مسبوقة ، تمكنت دولة قطر من تقديم نفسها كمثل هادئ ومتوازن على المسرح الدبلوماسي. الخطط المدروسة والإستراتيجية الدبلوماسية السيبرانية ساهمت بالفعل في تسهيل إقامة شراكات عبر وطنية مع المؤسسات الدولية الرائدة في مجال الأمن السيبراني. بعد أن وضعت قطر نفسها في الطليعة في ما يخصّ الأمن السيبراني ، ومع وجود بيئة رقمية معقدة بشكل متزايد ، والتي تشكل اليوم خطرًا على جميع البلدان ، من الممكن أن يتحول موقع القيادة في الأمن السيبراني إلى دولة قطر.