الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

النشرة الربعية للأمن السيبراني

تصنيف الوثيقة: متاح
إشارة المشاركة: أبيض

الربع الرابع - 2019

المحتويات

ملخص النشرة

نظرة عامّة موجزة عن الربع الرابع من العام 2019 (أكتوبر – ديسمبر)

برمجيات الفدية لا تزال تشكل تهديداً عالمياً – بالرغم من تراجع هجمات برمجيات الفدية (على الأقل بنسبة 5%) خلال العام، ظلت دول العالم تشهد زيادة في نمو هذه البرمجيات ليصل متوسط قيمتها في بعض الحالات إلى أكثر من 3,500,000 ريال سعودي. وتعود هذه الزيادة إلى استهداف بشكل متناسق القطاعات التي تمتلك بيانات ذات قيمة عالية مثل قطاع الرعاية الصحية والقطاع الحكومي وذلك بهدف زيادة العائدات من كل هجمة سيبرانية.

استمرار ارتفاع تكلفة تسريب البيانات– تنطبق هذه الحقيقة على المؤسسات الصغيرة التي يقل عدد العاملين فيها عن 1,000 موظف حيث تفتقر مثل هذه المؤسسات للمهنيين من ذوي المؤهلات العالية الأمر الذي يترك آثاراً سلبية على المؤسسات في منطقة الشرق الأوسط وشمال أفريقيا التي سجلت ارتفاعاً في تكلفة تسريب البيانات بنسبة 5% أعلى من المتوسط العالمي.

زيادة في المعلومات المضللة – تعود الزيادة في الاتجاه العام للمعلومات المضللة إلى التقنيات الجديدة ومواقع التواصل الاجتماعي، ومن غير المحتمل أن تتراجع هذه الظاهرة في المستقبل القريب.

تحديات الحوسبة الكمية – خلال عقد من الزمن، سوف توفر الحوسبة الكمية قوة حوسبية كبيرة التي يمكن استخدامها لأغراض مختلفة، وينطوي هذا الأمر على وجه الخصوص على فرض تحديات جديدة على التشفير والذي قد يعرض لاختراق الخوارزميات الموثوقة.

بيانات سيبرانية : سايبر بايت

الإحصاءات الرئيسيّة في الربع الرابع وأبرز القطاعات المستهدفة على الصعيد العالمي

الحاجة لزيادة القوى العاملة في الأمن السيبراني

145%

يعتقد أكثر من 51% من المهنيين العاملين في مجال الأمن السيبراني أن النقص الذي تعاني منه المؤسسات في القوى العاملة يعرّضها إلى المخاطر السيبرانية، وينطوي هذا الأمر على تحديات بشكل خاص للمؤسسات الصغيرة التي غالباً ما تكون غير قادرة على تعيين المهنيين من ذوي المؤهلات العالية[1]

الهجمات السيبرانية

أكثر من 60% السنة الماضية

في السنة الماضية 2019، تعرضت أكثر من 170 جهة حكومية في العالم للمخاطر السيبرانية ، ويتوقع الخبراء زيادة هذه المخاطر في السنة الحالية 2020 [2]

متوسط تكلفة تسريب البيانات للمؤسسات الصغيرة والمتوسطة

13,255 ريال/لكل موظف

بالنسبة للمؤسسات التي يتراوح عدد العاملين فيها بين 500 – 1000 موظف. أما المؤسسات الأكبر (أكثر من 25,000 موظف) فإنها تعاني من تكلفة أقل تبلغ تقريباً 765 ريال/موظف[3]

متوسط تكلفة البيانات التي تم تسريبها في الشرق الأوسط وشمال أفريقيا

أكثر من 38,000 ريال/لكل حادثة

وهذه نسبة أعلى بـ50% من المتوسط العالمي الذي بلغ 25,757 سجل[4]

أبرز 5 قطاعات مستهدفة في العالم في الربع 4 من عام 2019[5]

1. القطاع العام: 17.9%
2. الرعاية الصحية: 17.6%
3. المالية: 10.4%
4. التعليم: 10.1%
5. العلوم والتقنية: 9.8%

أبرز 5 تهديدات في السعودية في الربع 4 من عام 2019 [6]

- البرمجيات الضارة
- الدخول بدون تصريح
- الاستخدام غير الصحيح
- الاختراق/محاولة الاختراق
- تسرب البيانات

[1] المنتدى الدولي لشهادات أمن أنظمة المعلومات: استراتيجيات بناء وتنمية فرق الأمن السيبراني القوية (دراسة أعدها المنتدى عن القوى العاملة في الأمن السيبراني، 2019، ص 8

[2] كاسبيسكي، قصة العام 2019: مدن تحت حصار برمجيات الفدية، ديسمبر 2019

[3] تقرير تكلفة تسريب البيانات لعام 2019، معهد بونيمون وأمن IBM، ص 7

[4] تقرير تكلفة تسريب البيانات لعام 2019، معهد بونيمون وأمن IBM، ص 7

[5] تشير الأرقام إلى التوزيع (%) على العدد الإجمالي للهجمات التي تم تسجيلها في العالم خلال الفصل 4، 2019

[6] تحليل الهيئة الوطنيّة للأمن السيبراني، تبيّن أبرز التهديدات التي تمّ تسجيلها في المملكة العربية السعودية للربع السنوي الرابع.

الأمن السيبراني من منظور عالمي

أبرز عناوين الأمن السيبراني من مختلف دول العالم

تسمية برمجيات الفدية التهديد الأول للعالم في عام 2019 حسب اليوروبول

نشرت منظمة اليوروبول مؤخراً تقريرها بعنوان "تقييم تهديد جرائم الإنترنت المنظمة" الذي أكد على أن برمجيات الفدية على قمة التهديدات السيبرانية في العالم. كما ذكر التقرير أن المهاجمين قد أخذوا بتغيير أساليبهم حيث يستهدفون ضحاياهم باستخدام تقنيات جديدة مثل التصيد الالكتروني وذلك في محاولة منهم لزيادة عائداتهم بمجهود أقل[7] . ونتيجة لذلك انخفض العدد الإجمالي للهجمات السيبرانية خلال العام 2019، ولكن ارتفع متوسط قيمة العائدات من هذه الهجمات. وهذا ما أكدته بيانات القطاع الخاص التي أشارت إلى تراجع بنسبة 5% سنوياً لهذه الهجمات ليصل عددها إلى 150 مليون هجمة.[8]

كما نشرت منظمة اليوروبول تقريراً آخر بعنوان "التصيد الالكتروني من منظور الجهات القانونية والمؤسسات المماثلة" أكدت فيه المخاطر الجدية التي يشكلها التصيد الالكتروني على المؤسسات من مختلف الأحجام.[9] وقد بين هذا التقرير أهمية اتباع دفاعات تقنية كافية، والتدريب والتوعية، كما شدد على الحاجة للتعاون ولا سيما مع المؤسسات المسؤولة عن فرض القوانين.

المجلس الأطلسي ينشر نتائج الاستبيان العالمي الأول حول الأمن السيبراني للملاحة الجوية

جاءت نتائج الاستبيان في تقرير بعنوان "الأمن السيبراني للملاحة الجوية: رسم نطاق التحديات" الذي يسلط الضوء على عدد من التحديات التي تواجه قطاع الطيران المدني.[11] ويلاحظ التقرير على نحو خاص أن أطر الأمن والسلامة التي ينعم بها قطاع الطيران المدني منذ وقت طويل قد وُضعت في وقت لم تبرز أهمية الأمن السيبراني حيث يستخدم هذا القطاع العديد من التقنيات التقليدية (مثل الموجات اللاسلكية/الراديو) المحصنة نسبياً ضد الهجمات السيبرانية. وفي زمن أصبح فيه الأمن السيبراني ضرورة تفرض نفسها، بدأت شركات تشغيل المطارات تبذل جهوداً هائلة لمراجعة أساليب عملها وطريقة تفكيرها.

يرسم التقرير 4 خطوات لتحسين الأمن السيبراني في قطاع الطيران المدني: وضع معايير عالمية، زيادة الشفافية، تعاون أقوى، وأساليب مشاركة المعلومات. وتنسجم هذه الخطوات بشكل وثيق مع نتائج المبادرات الأخرى المخصصة لقطاع الطيران المدني. على سبيل المثال، أطلقت منظمة الطيران المدني الدولية مسودة "استراتيجية الأمن السيبراني لقطاع الطيران المدني" أوردت فيها سبع ركائز لزيادة الأمان في هذا القطاع.[12] كما تبنت الجمعية العمومية لمنظمة الطيران المدني الدولية "القرار A40-10: الاهتمام بالأمن السيبراني في الطيران المدني" الذي يعيد التأكيد على الضرورة المهمة والملحة لحماية أنظمة وبيانات البنى التحتية الحساسة لقطاع الطيران المدني من التهديدات السيبرانية، كما دعا الدول الأعضاء إلى تنفيذ استراتيجية الأمن السيبراني التي وضعتها المنظمة.[13]

[7] الشرطة الأوروبية، تقييم تهديدات جرائم الإنترنت المنظمة، 2019، أكتوبر 2019
[8] مختبرات SonicWall لجمع البيانات، أكتوبر 2019
[9] الشرطة الأوروبية، البوليس الأوروبي ينشر تقرير إنفاذ القوانين حول التصيد الاحتيالي، نوفمبر 2019
[11] المجلس الأطلسي، الأمن السيبراني للملاحة الجوية، رسم نطاق التحديات، ديسمبر 2019
[12] منظمة الطيران المدني الدولية، استراتيجية الأمن السيبراني للطيران المدني، أكتوبر 2019
[13] منظمة الطيران المدني الدولية، القرار الذي تبنته المنظمة في الاجتماع الأربعين للجمعية العمومية، أكتوبر 2019

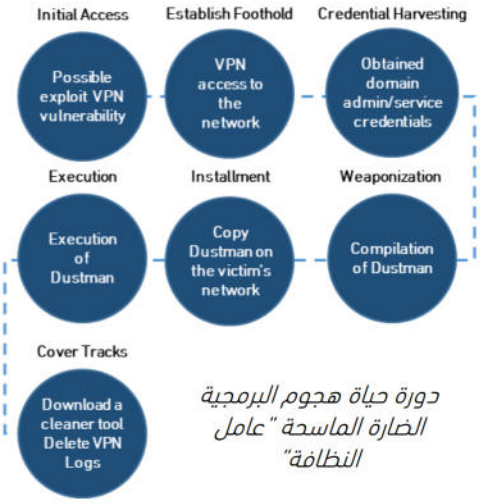
الأمن السيبراني من منظور وطني

أبرز أحداث الأمن السيبراني في المملكة العربية السعودية

الهيئة الوطنية للأمن السيبراني تكتشف برمجية ضارة ماسحة جديدة

في نهاية العام 2019، أعلنت الهيئة الوطنية للأمن السيبراني في السعودية عن اكتشاف برمجية ضارة ماسحة جديدة تُسمى "عامل النظافة" (Dustman) والتي تعتبر نوع جديد من البرمجيات الضارة "الماسحة" التي تعمل على حذف المحتويات الموجودة في أجهزة التخزين التي تهاجمها. ويُعتقد أنه تم استخدام هذه البرمجية الضارة في سلسلة من الهجمات المدمرة التي استهدفت العديد من المؤسسات في الشرق الأوسط في أواخر العام 2019.

وقد أظهرت التحقيقات أن هذه البرمجية الضارة قد ظهرت في يوليو 2019 عندما بدأت تخترق الأنظمة التي تستهدفها مع احتفاظها ببنيتها المعقدة والمتطورة بما يكفي بحيث لا يمكن كشفها بواسطة البرمجيات المضادة للفيروسات. وقد أشارت التحليلات إلى احتمال ابتكار هذه البرمجية من قبل إحدى الدول وليس منظمة أو أفراد.



دورة حياة هجوم البرمجية الضارة الماسحة "عامل النظافة"

وبالإضافة إلى التحليل الشامل الذي أجرته لتاريخ هذه البرمجية وطريقة عملها، قدمت الهيئة الوطنية للأمن السيبراني مجموعة من التوصيات التي من شأنها مساعدة المؤسسات على التخفيف من آثار ومخاطر هذه البرمجية. وتشمل هذه التوصيات 16 إجراء وقائياً (مثل المحافظة على مستوى كافٍ من النظافة السيبرانية) و 12 إجراء تحرياً (مثل تحديد ما هي الأجهزة والأنظمة التي يجب أن تبقى تحت المراقبة للكشف عن البرمجيات الضارة في حين ظهورها).

حظي اكتشاف هذه البرمجية الضارة بتغطية إعلامية واسعة في مختلف دول العالم، وقد أُطلق عليها أحياناً اسم "هجوم بابكو" (نسبة لإحدى الشركات التي كانت من أبرز ضحاياها) وقد استشهدت عدة وسائل إعلامية بهذه البرمجية الضارة المكتشفة وتقرير الهيئة الوطنية للأمن السيبراني السعودية، كما تحدثت عنهما عدة شركات تعمل في مجال الأمن السيبراني مثل كاسبيرسكي (Kaspersky) و سايوير (Cyware).[14]

مجموعة العشرين : أولوية الأمن في الاقتصاد الرقمي

تسلمت المملكة العربية السعودية مؤخراً رئاسة مجموعة العشرين من اليابان للعام 2020 وذلك خلال اجتماع لوزراء خارجية دول المجموعة الذي انعقد في مدينة ناغويا اليابانية.

تم تحديد الأمن في الاقتصاد الرقمي كأحد أولويات فريق عمل الاقتصاد الرقمي بالموائمة مع عنوان وأهداف سنة الرئاسة لعام 2020.

سمو الأمير فيصل بن فرحان آل سعود، وزير خارجية المملكة مع نظيره الياباني السيد توشيميتسو موتيجي

ومع تسلم المملكة لرئاسة مجموعة العشرين، سيعمل فريق عمل الاقتصاد الرقمي طيلة عام 2020 على أولوية الأمن في الاقتصاد الرقمي مع مجموعة الأعمال (B20) وعدد من المؤسسات الدولية ذات الصلة.

ومن الآن وحتى انعقاد قمة مجموعة العشرين المقرر في الرياض في نوفمبر 2020، سوف تستضيف المملكة أكثر من 100 فعالية من بينها مؤتمرات واجتماعات وزارية تضم ممثلين من المجتمع المدني. وأحد الأمثلة البارزة على هذه الفعاليات التي تزخر بها الأجندة الطموحة للمملكة هو "حوار الأمن السيبراني لمجموعة العشرين".[16]

G20
SAUDI ARABIA 2020

[14] الهيئة الوطني للأمن السيبراني، الهجمات المدمرة للبرمجية الضارة (Dustman)، التقرير التقني، ديسمبر 2019
[16] الموقع الرسمي لمجموعة العشرين

أحداث سيبرانية

نظرة على أبرز أحداث الأمن السيبراني في الربع الرابع – عام 2019

مدينة بنساكولا

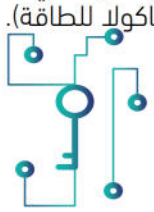
المكان: الولايات المتحدة

القطاع: الإدارة العامة

تاريخ الإفصاح: ديسمبر 2019

نوع الهجوم: برمجية الفدية

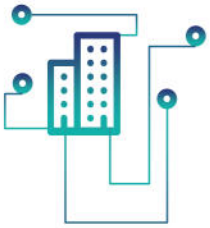
الوصف: تعرضت مدينة بينساكولا في ولاية فلوريدا الأمريكية لهجمة سيبرانية تعتمد على برمجية الفدية مما أثر على شبكة المدينة (بما في ذلك خطوط الهاتف والبريد الإلكتروني في مجلس المدينة) وبعض خدمات الدفع الإلكتروني (من بينها شركة بينساكولا للطاقة).



ووفقاً للتحقيقات، فقد تم زرع هذه البرمجية في نظام المدينة بين 5 – 7 ديسمبر، وجرى تفعيلها في وقت لاحق من صباح يوم 7 ديسمبر ما ألحق الضرر بـ 27 نظاماً.

استفاد منفذ الهجوم من نظامين على الإنترنت لم يتم تطبيق متطلبات الأمن السيبراني عليها. وبعد تنفيذ عملية الاختراق، سمح هذان النظامان للفيروس بالانتشار عبر الشبكة وذلك بسبب ضعف إجراءات الأمن في الشبكات الداخلية.

التأثير: تسبب الحادث بانقطاع العديد من الخدمات باستثناء الخدمات الرئيسية (مثل خدمة الطوارئ 911 والمستشفيات).



لغاية يوم 22 يناير، وفي حين زعم منفذو الهجوم بأنهم تمكنوا من اختراق ما يزيد عن 30 جيجا بايت من البيانات، أكدت التحقيقات بأن ما تم خسارته من النظام لا يتجاوز 6 جيجا بايت من البيانات التي تم اختراقها.

طلب المهاجمين في البداية فدية قدرها 3,750,000 ريال سعودي قبل أن يخفّضوا المبلغ إلى 1,900,00 ريال، إلا أن مسؤولو المدينة رفضوا دفع المبلغ. في شهر ديسمبر، نشر المهاجمين 2 جيجا بايت من البيانات المسروقة من الهجوم، مؤكدين أن لديهم أكثر من 30 جيجا بايت من البينات المسروقة من شبكات المدينة.

وفي حين قررت السلطات المحلية عدم دفع الفدية، بلغت التكلفة التقديرية للمدينة المتعلقة بالحادثة 400,000 دولار أمريكي (نحو 1,504,000 ريال سعودي) لغاية 31 يناير 2020. علاوة على ذلك، وبهدف جمع احتياطات للتكاليف المرتبطة بالهجوم، قررت مدينة بينساكولا تخصيص مبلغ 699,576 دولار أمريكي إضافي (نحو 2,632,000 ريال سعودي) لصندوق التأمين الداخلي الخاص بها.

الدروس المستفادة: يؤكد هذا الهجوم على أهمية بناء قدرات الصمود السيبراني في كافة مجالات القطاع العام.

إن وجود إجراءات الاستجابة للحوادث السيبرانية والنسخ الاحتياطية ساعد المدينة على التقليل من الأضرار. والتي كان لها دور كبير في إعادة الأنظمة إلى الخدمة يوم 13 ديسمبر.

17 مدينة بينساكولا، تحديث عن حادثة الهجوم السيبراني على مدينة بينساكولا، ديسمبر 2019، مدينة بينساكولا، التقرير المالي السنوي الشامل، السنة المالية 2019، مدينة بينساكولا، الأسئلة الشائعة عن الهجوم السيبراني، ديسمبر 2019، مدينة بينساكولا، ديلويت-مشروع لوروس، يناير 2020، سيكيوريتي بوليفارد، متاهة فيروس الفدية المستخدم في الهجوم السيبراني على مدينة بينساكولا، ديسمبر 2019، مجلة CISO، برنامج الفدية في بينساكولا: قراصنة الإنترنت ينشروع 2 غيغا بايت من البيانات كدليل، ديسمبر 2019، موقع Bleeping Computer، فيروس الفدية ينشر ملفات مسروقة من مدينة بينساكولا، ديسمبر 2019.

ومضة سيبرانية

في عام 2019، تم تصنيف برمجية الفدية كأحد أكثر أساليب الهجمات السيبرانية شيوعاً [18]. تقدم الهيئة الوطنية للأمن السيبراني مجموعة من التوصيات للتقليل من المخاطر الناجمة عن هذا النوع من الهجمات السيبرانية.

الحماية من الهجوم

- إجراء النسخ الاحتياطي للأنظمة بصورة منتظمة
- المحافظة على الأجهزة و الأنظمة محدّثة
- استخدام برامج الحماية من البرمجيات الضارة ورسائل التصيّد الإلكتروني والبريد غير المرغوب به
- إدارة البرمجيات وسياسات إدارة الوصول للمستخدمين
- تطبيق التصميم الآمن للشبكة
- استخدام اتصالات آمنة للوصول للبنية التحتية
- استخدام المعلومات الاستباقية حول التهديدات السيبرانية للكشف عن حملات برمجيات الفدية المحتملة

الكشف عن الهجوم

- استخدام أنظمة حماية البريد الإلكتروني
- مراقبة حملات التصيد الالكتروني المحتملة، مثل:
  - الضعف الإملائي في الكتابة والقواعد النحوية الرديئة.
  - عناوين البريد الإلكتروني التي تنتحل جهات الاتصال
  - الطلبات غير المتوقعة للنقر على رابط أو تنزيل ملف أو مشاركة معلومات شخصية

الاستجابة

- بدء عملية إزالة فيروس الفدية بأسرع وقت ممكن
- فصل الأجهزة عن الإنترنت أو الشبكة المحلية
- إجراء عملية مسح باستخدام برنامج الحماية
- حذف الملفات المتضررة من الشبكة
- استخدام أدوات تشفير فيروس الفدية (إذا امكن) أو استعادة البيانات من أحدث النسخ الاحتياطية

التعافي من الهجوم

- عمل نسخ احتياطية للبيانات والتطبيقات للمساعدة في التعافي
- تقييم الهجمات وأسبابها الجذرية من أجل تحديد الدروس المستفادة وتحسين قدرات الوقاية

الضوابط الأساسية للأمن السيبراني

في عام 2018، أطلقت الهيئة الوطنية للأمن السيبراني " الضوابط الأساسية للأمن السيبراني"، التي تهدف إلى "وضع الحد الأدنى من متطلبات الأمن السيبراني للأصول التقنية والمعلومات في الجهات الوطنية" في المملكة العربية السعودية[19].

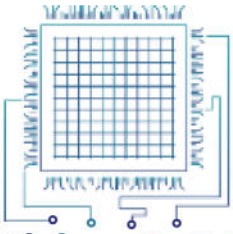
بإمكان الجهات الرجوع إلى الضوابط الأساسية للأمن السيبراني للاطلاع على الضوابط والإجراءات للتقليل من المخاطر السيبرانية الناجمة عن التهديدات الداخلية والخارجية. .

[18] الشرطة الأوروبية (يوروبول)، تقييم تهديدات جرائم الإنترنت المنظمة، 2019، أكتوبر 2019
[19] الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني (ECC – 1:2018)

تسليط الضوء على الابتكارات السيبرانية

نسلط الضوء في هذا العدد على تأثيرات الحوسبة الكمية (الكمومية) في قطاع الأمن السيبراني.

رغم أن مصطلح "الحوسبة الكمومية" يعود إلى ما قبل 30 سنة، إلا أنه يحظى حالياً باهتمام سائد. تعتمد أجهزة الحوسبة التقليدية كالحواسب المحمولة والهواتف الذكية في عملياتها على الأرقام الثنائية، وهي تستطيع أن تقبل فقط قيمة 0 أو 1. في المقابل، الوحدة الأساسية في الحوسبة الكمومية هي الكيوبت وتستطيع أن تقبل قيمة 0 و1 في الوقت ذاته ما يمكّن الحواسب الكمومية من العمل بسرعات تتفوق بشكل مطرد على سرعات الحواسب التقليدية وبذلك تفتح إمكانيات جديدة لمهام الحوسبة التي كانت مستحيلة سابقاً.



26 خوارزمية من المحتمل أنها مقاومة للكمومية

ساعات هو الوقت اللازم لفك خوارزمية تشفير حديثة باستخدام الحوسبة الكمومية

في تجربة أجريَت مؤخراً، قام حاسب كمي "quantum computing" بعملية حسابية خلال 3 دقائق وحسب التقديرات كانت هذه العملية لتستغرق 10 آلاف سنة بالنسبة لنظام يمتلك القدرة الحوسبية لـ 100 ألف حاسب مكتبي تقليدي.[27] يمكن لهذه القدرة الحوسبية أن تحدِث تغييرات هائلة في قطاع الأمن السيبراني وخاصةً في مجال التشفير. وفقاً للباحثين، سيكون للحوسبة الكمومية تأثير على نطاق واسع.[28]

يعمل الباحثون حالياً لتعزيز تقنيات وقدرات الأمن السيبراني في هذا العصر "quantum age" حيث وضع المعهد الوطني الأمريكي للمعايير والتقنية (NIST) قائمة مختارة تضم 26 خوارزمية ليتم اختبارها كخوارزميات محتملة "مقاومة للكمومية" (quantum resistant).

قد يستلزم سنوات– حسب تقديرات متفائلة – لجعل التقنية الكمومية في المتناول على مستوى المستهلك.[29] ولكن يجب على المؤسسات أن تستعد لذلك.

لنتحرك الآن

يجب على الجهات أن تعزز حماية البيانات، فبالإضافة لأهمية تشفير البيانات ، يجب التأكد من تطبيق ضوابط حماية البيانات من الوصول غير المصرح. قد تتعرض البيانات لخطر أساليب "الجمع وفك التشفير" التي تركز على الحصول على منفذ إلى البيانات المشفرة وتخزينها إلى أن يُتاح فك تشفيرها بواسطة الحواسب الكمومية.[30]

لنستعد للمستقبل

يجب على الجهات أن تستعد للحوسبة الكمومية بالقدرة على التحديث المستمر للخوارزميات وتشفير البيانات وحمايتها باتباع الضوابط الوطنية للتشفير.[31] [32]

27 مجلة "نيتشر" (الطبيعة)، مرحباً بعالم الكموم! موقع "جوجل" ينشر ادعاءً مميزاً بالتفوق الكمومي، أكتوبر 2019.

28 كريغ جيدني وآخرون، كيف نحلل إلى عوامل الأعداد الصحيحة لخوارزمية "أر إس إيه" 2048 بت خلال 8 ساعات بواسطة 20 مليون كيوبت تطفلي، ديسمبر 2019.

29 "سيبيكترم"، القضية ضد الحوسبة الكمومية، نوفمبر 2018.

30 ديلويت، التوقعات للتقنية والإعلام والاتصالات، 2019.

31 المعهد الوطني للمعايير والتقنية، تقرير عن التشفير بعد الكموم، أبريل 2016.

32 المعهد الأوروبي لمعايير الاتصالات، التشفير الآمن كمومياً.

طُوّرت هذه النشرة الربعية من قبل الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، والتي تهدف لمنح لمحة عامة للقراء عن أهمّ أحداث الأمن السيبراني للربع الرابع من العام 2019م، وتسليط الضوء على أهمّ التطورات في المجال والتي تهدف إلى:

- تعزيز القدرات و المعرفة في مجال الأمن السيبراني
- نظرة على أبرز للاتجاهات والتهديدات والمخاطر في المجال الأمن السيبراني

يحتوي هذا التقرير على بيانات من عدة جهات وأفراد ، مع ملاحظة أن جميع المعلومات الواردة في التقرير هي إرشادية فقط. أيضًا ، لا تتحمل الهيئة الوطنية للأمن السيبراني أي مسؤولية - تحت أي ظرف من الظروف - تجاه أي طرف نتيجة لأي قرار أو إجراء تم اتخاذه أو سيتخذه هذا الطرف بناءً على محتوى هذا التقرير. تؤكد الهيئة الوطنية للأمن السيبراني أنها ليست مسؤولة كليًا أو جزئيًا عن أي خطأ أو تقصير مباشر أو غير مباشر قد يحدث.

معلومات عن الهيئة الوطنية للأمن السيبراني

تأسست الهيئة الوطنية للأمن السيبراني عام 2017، وهي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، وتهدف إلى تعزيزه حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية، وللهيئة مهام تنظيمية وتشغيلية

https://nca.gov.sa @NCA_KSA