الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies

تصنيف الوثيقة : متاح
إشارة المشاركة: أبيض

النشرة الربعية للأمن السيبراني

الربع الثاني – 2020

جدول المحتويات

ملخص النشرة

نظرة عامّة موجزة عن الربع الثاني من العام 2020 (أبريل – يونيو)

لا تزال آثار الجائحة العالمية تشكّل العامل الأكبر الذي أثّر مؤخرًا على قطاع الأمن السيبراني، غير أنّ عددًا من الأحداث برزت أيضًا خلال هذا الربع الثاني.

أطلق المعهد الدولي للتطوير الإداري الترتيب التنافسي العالمي للعام 2020 حيث احتلّت المملكة العربية السعودية المرتبة الثانية "للتطوير المستمرّ للأمن السيبراني للمؤسسات".

يشكّل الذكاء الاصطناعي والحوسبة الكمومية تقنيات يمكنها أن تعزز قدرات الأمن السيبراني.

بيانات سيبرانية: سايبر بايت

الإحصاءات الرئيسيّة في الربع الثاني وأبرز القطاعات المستهدفة على الصعيد العالمي

+38 مليار

أجهزة متصلة بالإنترنت مع حلول العام 2020[1]

يبلغ النمو السنوي الإجمالي المتوقع نسبة 28.7% في الفترة ما بين العامين 2018 و2025 ممّا سيوسّع سطح الهجوم المتوفّر للاستخدام.

الدافع #1

مكاسب مالية جراء الهجمات ضدّ قطاع الرعاية الصحية[2]

إنّ 88% من الهجمات ضدّ قطاع الرعاية الصحية هي بدافع الكسب المالي في حين 12% منها هي بدافع التسلية أو الملاءمة.

+50%

ارتفاع نسبة اختراق البيانات الناتجة عن الأخطاء البشرية من 2019-2020[2]

يبلغ هذا الارتفاع في الأخطاء البشرية حوالى 17% من اختراق البيانات على المستوى العالمي.

74%

تفكّر المؤسسات في العمل عن بُعد بشكل دائم لبعض موظفيها[3]

قد ينتقل معدّل 5% من الموظفين في كلّ شركة للعمل عن بُعد بشكل دائم. سيؤدّي الأمن السيبراني دورًا اساسيًا في هذا الانتقال.

أبرز 5 قطاعات تعرّضت لتهديدات سيبرانية عالميًا في الربع الثاني من العام 2020 *

01 القطاع العام	17%
02 قطاع العلوم والتقنية	13%
03 قطاع الرعاية الصحية	12%
04 القطاع المالي	11%
05 قطاع وسائط الإعلام والاتصالات	8%

أبرز 5 تهديدات سيبرانية عالمية في الربع الثاني من العام 2020 *

01 برمجيات خبيثة	42%
02 قرصنة الحسابات	21%
03 الهجمات المستهدفة	11%
04 الثغرات	6%
05 إدخال برمجيات خبيثة	3%

أبرز 5 تهديدات سيبرانية في المملكة العربية السعودية في الربع الثاني من العام 2020 **

01 برمجيات خبيثة
02 الاختراق/محاولة الاختراق
03 الدخول، التعديل والاستخدام غير المصرح به
04 تسرّب البيانات
05 هجوم الاستطلاع

[1] IBM Security، X-Fore Threat Intelligence Index 2020، فبراير 2020.
[2] فيريزون، تقرير التحقيق في خرق البيانات 2020.
[3] جارتنر، بيان صحفي: تكشف الدراسة الاستقصائية CFO التي أجراها جارتنر أنّ 74%ينوون نقل بعض الموظفين إلى العمل عن بُعد بشكل دائم، أبريل 2020.

* تبيّن الأرقام التوزيع (%) على مجموع عدد الهجمات المسجّلة عالميًا للربع الثاني.
** تحليل الهيئة الوطنيّة للأمن السيبراني، تبيّن أبرز التهديدات التي تمّ تسجيلها في المملكة العربية السعودية للربع السنوي الثاني.

الأمن السيبراني من منظور عالمي

عناوين الأمن السيبراني الرئيسيّة من مختلف أنحاء العالم

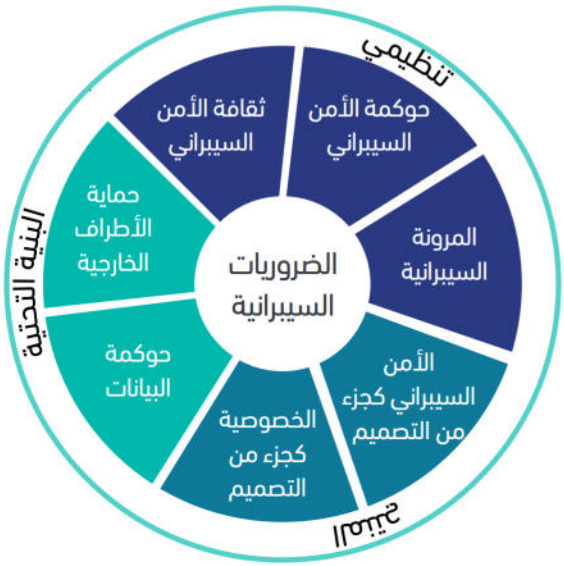
بعد مرور عامين: كيف تغيّر منظور الخصوصية العالمية مع النظام الأوروبي العام لحماية البيانات

يصادف شهر مايو 2020 الذكرى الثانية لسريان النظام الأوروبي العام لحماية البيانات والذي يهدف إلى لتنظيم كيفيّة إدارة وحماية المؤسسات لبيانات المستخدمين وإلى تمهيد الطريق لسوق أوروبي رقمي موحّد.

لم يعمل نظام GDPR على تصميم حماية البيانات فحسب بل شكّل مصدر إلهام لقانون كاليفورنيا لحماية خصوصية المستهلك والقانون البرازيلي العام لحماية البيانات الشخصية وقانون حماية المعلومات الشخصية في اليابان.[4]

نظرًا لأهمية نظام GDPR، نشرت الهيئة الوطنية للأمن السيبراني إرشادات ترتكز إلى 7 ركائز لمساعدة المؤسسات السعودية على تحديد مدى تطبيق هذا النظام ومساعدتها على التعامل مع أحكامه بشكل أفضل.[6]

أطلق المنتدى الاقتصادي العالمي إطار عمل سيبراني للمستثمرين وأصحاب المشاريع



بناء على تقرير صادر عن المنتدى الاقتصادي العالمي، تعاني صناعة الأمن السيبراني من خلل في التوازن ما بين "الوقت إلى السوق" و"الوقت إلى الأمن" إذ من المتوقّع أن تطلق الشركات تقنيات جديدة بوتيرة سريعة.

يشير التقرير كذلك إلى أنّه يمكن تفادي هذا المأزق عبر اعتماد نهج "الأمن حسب التصميم" الذي يركّز على إدراج الأمن السيبراني في المنتجات والخدمات منذ مراحل تطويرها. لذلك، يتضمّن التقرير إطار عمل يساعد المستثمرين وأصحاب المشاريع الذين يعملون بهذه الوتيرة السريعة على تطبيق الأمن السيبراني في منتجاتهم وخدماتهم. ويحتوي هذا التقرير أيضًا على مجموعة من الضروريات السيبرانية التي يمكن اعتمادها من قبل أصحاب المصلحة من أجل تحسين الأمن.[7]

[4] The New York Times، .G.D.P.R، New Privacy Law, Makes Europe World's Leading Tech Watchdog، يونيو 2018.

[5] المشرف الأوروبي على حماية البيانات. تاريخ لوائح حماية البيانات العامة. المفوضية الأوروبية.

[6] إرشادات نظام GDPR بحسب الهيئة الوطنية للأمن السيبراني.

[7] المنتدى الاقتصادي العالمي، Incentivizing Responsible and Secure Innovation: A framework for investors and entrepreneurs، يونيو 2020.

الأمن السيبراني من منظور وطني

عناوين الأمن السيبراني الرئيسيّة في ما يتعلّق بالمملكة العربية السعودية

أطلقت الهيئة الوطنية للأمن السيبراني ضوابط الأمن السيبراني للعمل عن بُعد

نتيجة جائحة كوفيد 19، ارتفعت نسبة العمل عن بُعد بشكل كبير في كلّ أنحاء العالم، وقد شهدت المملكة هذا التغيير أيضًا، ممّا يؤدّي إلى اعتبارات جديدة حول الأمن السيبراني.

استجابة منها لذلك، أصدرت الهيئة الوطنية للأمن السيبراني ضوابط مخصّصة ترتكز على 8 خطوات لمساعدة المستخدمين في المحافظة على الأمن السيبراني أثناء العمل عن بعد:[8]

الخطوات التي وضعتها الهيئة الوطنية للأمن السيبراني للعمل عن بُعد بشكل آمن

1. الحد من ثغرات شبكات الواي - فاي المنزلية
2. حماية الحسابات الشخصية والهواتف الذكية من خلال أدوات متخصّصة.
3. استخدام الحواسيب التي تزوّدها المؤسسات.
4. قراءة دقيقة للتعليمات المتعلقة بأي أدوات عمل تقنية
5. تعلّم كيفيّة التعاون بشكل آمن مع الزملاء من خلال المنصات الإلكترونية
6. الامتثال للتوجيهات الأمنية والتقنيات التي تزوّدها المؤسسة.
7. اعتماد نهج آمن أثناء السفر أو العمل من المنزل أو المكتب.
8. تعزيز الوعي الذاتي المتعلّق بالمسائل التقنية أو الأمنية

حصلت المملكة العربية السعودية على المرتبة الثانية لتطوير الأمن السيبراني

أطلق المعهد الدولي للتطوير الإداري مؤخرًا الترتيب التنافسي العالمي للعام 2020 والذي يقيّم أكثر من 60 دولة من حيث القدرة التنافسيّة بما في ذلك الأمن السيبراني، وقد احتلّت المملكة العربية السعودية هذا العام المرتبة الثانية "التحسن المستمر في مؤشر الأمن السيبراني للشركات".[9]

يؤكّد هذا دور المملكة العربية السعودية في مجال الأمن السيبراني على المستوى العالمي، ويبيّن التزام المملكة في تحسين الأمن السيبراني المحلي. لذلك، وبهدف دعم رؤية المملكة 2030، نفّذت المملكة إصلاحات ومبادرات وبرامج متعلّقة بالأمن السيبراني، وقد تحقق ذلك بفضل دعم القيادة السعودية والجهود التي بذلتها الهيئة الوطنية للأمن السيبراني.

لقد عملت الهيئة الوطنية للأمن السيبراني على تنفيذ السياسات السيبرانية وآليات الحوكمة والهيكليات والمعايير والضوابط والإرشادات التي تمّ تعميمها على الجهات المعنيّة داخل المملكة العربية السعودية وخارجها.

ستستمرّ الهيئة الوطنية للأمن السيبراني في مسيرتها بهدف تعزيز وضعيّة الأمن السيبراني في المملكة ممّا يصبّ في مصلحة المواطنين والمؤسسات في كلّ أنحاء المملكة.[10]

[8] CERT.SA، دليل العمل عن بُعد، 2020.

[9] IMD World Competitiveness ranking 2020, 2020

[10] أخبار الهيئة الوطنية للأمن السيبراني، احتلت المملكة المرتبة الثانية في "التحسن المستمر في مؤشر الأمن السيبراني للشركات"، في تقرير التنافسية العالمية، يونيو 2020.

أحداث سيبرانية

نظرة على أبرز أحداث الأمن السيبراني في الربع الثاني – عام 2020

حجم قياسي لهجمات تعطيل الخدمات الموزعة (DDoS) [11]

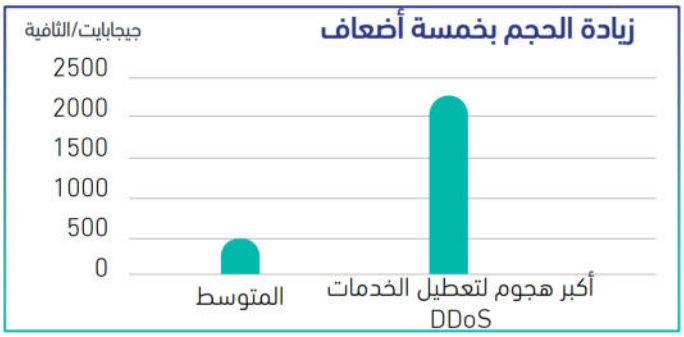
المكان: عالميًا

القطاع: خدمات سحابية / شبكية

تاريخ الإفصاح: 13 يونيو 2020

نوع الهجوم: هجمات تعطيل الخدمات الموزعة (DDoS)

الوصف: وقع نظام أمازون ويب سيرفيسز (AWS) ضحية هجمات تعطيل الخدمات الموزعة 2.3 تيرابايت لمدة 3 أيام خلال شهر فبراير وكان أكبر هجوم من نوعه.



يبلغ متوسط ذروة هجمات DDoS 500 جيجابايت في الثانية الواحدة وتخطّى هذا الهجوم 5 أضعاف هذه الهجمات. في الواقع، لا تزال دوافع هذه الهجمات مجهولة ولكن يبدو أنّ الطريقة المعتمدة هي نوع جديد من "هجوم انعكاس" DDoS. إنّ هذه التقنية تجعل هجوم DDoS أكثر فعالية وأقلّ عرضة للحجب بواسطة التدابير الأمنية المضادة لهجوم DDoS.

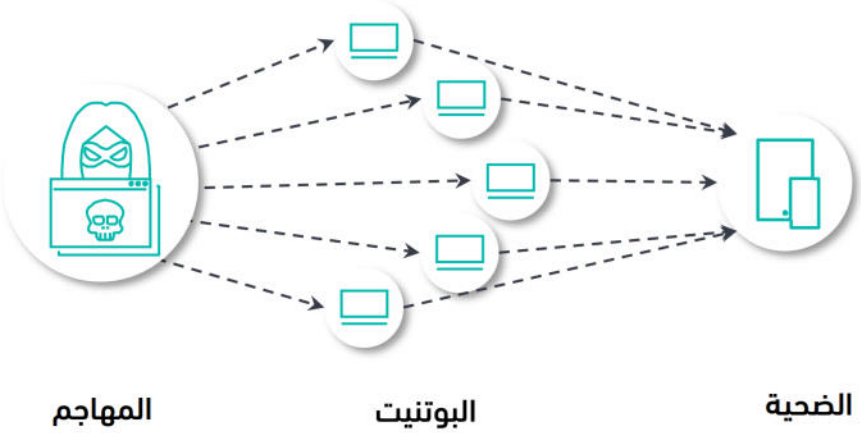
التأثير: شكّل الهجوم سابقة من نوعها بحيث فاق أي هجوم من نوعه بنسبة 44%. تمّ الإفصاح عن الحادث بعد أشهر من حدوثه.

الدروس المستفادة: لقد برهن الحادث أنّه من الممكن التعرض لهجمات تعطيل الخدمات الموزعة DDoS الضخمة. وللحد من آثارها يجب : أوّلًا، تصميم الشبكة الخاصة بكم لتفادي" نقاط الفشل الفردية" وعزلها بطريقة تحمي الأجزاء الأكثر حيوية في الشبكة من تدفقات المعلومات الخارجية. ويتبع ذلك التأكد من الوضوح الكامل للشبكة إضافة إلى وضع أنظمة الإنذار في حال تخطّت حركة الشبكة حدودًا معيّنة.

معلومات حول هجوم DDoS

يستغلّ هجوم DDoS قدرة البيانات المحدودة للشبكات، حيث يعمل المهاجمون على إغراق الهدف بكمية كبيرة من البيانات وعندما يتمّ تخطّي قدرة الشبكة، من المرجح أن تتأثّر الخدمات المستضافة سلبًا أو قد تصبح غير متوفّرة.

بهدف إرسال كمية كبيرة من البيانات، يستخدم المهاجمون أجهزة متضرّرة سابقًا تدعى "البوت" والتي يتحكّم بها المهاجم. تسمّى هذه الأجهزة مجتمعة "البوتنيت" ويتمّ استخدامها لتوليد الحركة الضرورية لإغراق الضحية.[12]



[11] AWS Shield، تقرير منظور التهديدات – الربع الأوّل 2020.

[12] كاسبيرسكي، ما هو هجوم DDoS؟ معنى DDoS.

ومضة سيبرانية

نصائح مفيدة لتطبيق تقنيات الذكاء الاصطناعي بشكل آمن

بات الذكاء الاصطناعي يؤدّي دورًا رئيسيًا في عملية التحول المؤسسي[13]. بالفعل، يوفّر الذكاء الاصطناعي فرصًا وقدرات جديدة. ولهذا، على المؤسسات أن تسعى إلى فهم التطبيقات وتوجهات الأمن السيبراني من أجل ذكاء اصطناعي آمن.

التطلّع إلى مستقبل الذكاء الاصطناعي - بشكل آمن

إنّ انتشار أنظمة الذكاء الاصطناعي في القطاعات الرئيسيّة بما في ذلك قطاعات النقل والصحة والمالية وغيرها يسلّط الضوء على أهميّة تعزيز الأمن السيبراني في هذه الأنظمة. يتطلّب ذلك فهم كيفيّة حماية أنظمة الذكاء الاصطناعي من خلال إرشادات الشفافية والمصادقة وتدابير المساءلة.[14]

نصائح من أجل تطوير وإدارة الذكاء الاصطناعي بشكل آمن

- **فهم حاجات المستخدمين وأصحاب المصلحة.** نظرًا لمخاطر الأمن السيبراني، من المهمّ اعتماد الذكاء الاصطناعي عندما يتمّ تحديد نماذج الاستخدام الواضحة والتحقق منها.
- **وضع وتعزيز القدرات المتعلقة بالأدلة الجنائية.** من الضروري أن يتّسم الذكاء الاصطناعي بالشفافية والمساءلة من أجل المحافظة على الأمن السيبراني وبناء الثقة في نشر هذه التقنية المتقدمة.
- **المحافظة على رقابة مستقلّة.** دعم المهنيين في مجال الأمن السيبراني الذين يتمتّعون بفهم واضح ودقيق للذكاء الاصطناعي.
- **النظر في البرمجيات.** عند تطوير تقنيات الذكاء الاصطناعي، على الخبراء في مجال الأمن السيبراني أن يتحققوا من التطبيق الآمن للبرمجيات والخوارزميات ذات الصلة.
- **رصد منظور التهديدات.** يمكن لمنفّذي التهديدات اختيار تقنية الذكاء الاصطناعي لأتمتة الهجمات ضدّ المؤسسات. يُنصح بفهم كيفيّة استخدام المهاجمين للذكاء الاصطناعي من أجل حماية المؤسسات من هذا النوع من التهديدات على أفضل وجه.

[13] المنتدى الاقتصادي العالمي، إرشادات للتأمين الحكومي للذكاء الاصطناعي، سبتمبر 2019.

[14] كيفيّة تعزيز الأمن السيبراني للذكاء الاصطناعي، Brookings، 2020.

التطلّع لتوجّهات جديدة

نظرة إلى التوجهات الأخيرة المتعلّقة بالذكاء الاصطناعي وكيفيّة تعزيزها للأمن السيبراني

كيف يمكن للذكاء الاصطناعي تعزيز الأمن السيبراني[15]

كما تحتاج أنظمة الذكاء الاصطناعي إلى أدوات وأساليب الأمن السيبراني من أجل تعزيز مصداقيتها وصمودها، كذلك يمكن للأمن السيبراني استخدام الذكاء الاصطناعي لتعزيز فعاليته[16]. ثمّة طرق أساسيّة عدّة لاستخدام الذكاء الاصطناعي لتعزيز الأمن السيبراني:

على الرغم من أنّ الذكاء الاصطناعي لا يزال في مرحلته الأولى ويتوقّع أن يشهد نموّا كبيرًا، أصبح ذلك واقعًا بالنسبة إلى عدد كبير من المؤسسات. فوفقًا للدراسات، يستخدم أكثر من 70% الذكاء الاصطناعي في مجال الأمن السيبراني أو أكثر، في حين أنّ أمن الشبكة هو التطبيق الأكثر شيوعًا.[17]

التعلّم

يستخدم الذكاء الاصطناعي كمية هائلة من المعلومات المنظّمة وغير المنظّمة ويمكن استخدام الذكاء الاصطناعي من خلال التعلّم الآلي والتعلّم المتعمّق لفهم التهديدات والمخاطر السيبرانية بشكل أفضل.

التفكير المنطقي

يستخدم الذكاء الاصطناعي التفكير المنطقي لمعرفة الروابط بين مختلف التهديدات (مثل الملفات الضارة وعناوين الشبكة العالمية المشبوهة إلخ.) ممّا يسمح للخبراء في مجال الأمن السيبراني بتحسين وقت الاستجابة للتهديدات بشكل كبير.

التعزيز

يساهم الذكاء الاصطناعي في تعزيز كفاءة ودقّة المهام التي تتطلّب عددًا كبيرًا من العاملين، ممّا يقلّص مقدار الوقت المطلوب من أجل تحديد وتحليل التهديدات وإطلاق استجابة منسّقة.

دفاع الذكاء الاصطناعي: نماذج استخدام الأمن السيبراني[18]

لقد سبق لصناعة الأمن السيبراني أن بدأت باستخدام قدرات الذكاء الاصطناعي للدفاع عن الشبكات والأنظمة، وتتضمّن الأنشطة الرئيسيّة ما يلي:

- تمكين الاستجابة الآلية والحدّ من التهديدات.
- التنبؤ بالتهديدات ورصدها في الوقت الفعلي.
- التعمق في التحليلات الأمنيّة.
- تعزيز الرصد والتحليل لحركة الشبكة.

الذكاء الاصطناعي كتهديد سيبراني: تقنية التزييف العميق

إنّ الذكاء الاصطناعي فعّال في توليد محتوى سمعي وبصري مزيّف، ثمّ يستخدم منفّذو البرمجيات الضارة هذا المحتوى الذي يُعرف بالتزييف العميق لتشكيك وابتزاز الضحايا وإجبارهم على دفع فدية لإزالة المحتوى. يتمّ تطوير تقنية التزييف العميق أيضًا في حملات تشويه المعلومات.[19]

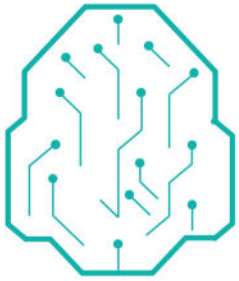
---

[15] IBM، الذكاء الاصطناعي لنوع أكثر ذكاء من الأمن السيبراني.
[16] NITRD، الذكاء الاصطناعي والأمن السيبراني: الفرص والتحديات، تقرير موجز عن ورشة العمل التقنية، مارس 2020.
[17] Velocity Global، كيف تستخدم الأعمال العالمية الذكاء الاصطناعي؟ يناير 2019.
[18] Built in، 30 شركة تنشئ الذكاء الاصطناعي والأمن السيبراني للمحافظة على حمايتنا وسلامتنا، مارس 2020.
[19] The Emergence of Technology Innovation Management Review، Deepfake Technology: A Review، نوفمبر 2019.

تسليط الضوء على الابتكارات السيبرانية

الحوسبة الكمومية وأحدث الابتكارات في مجال الأمن السيبراني

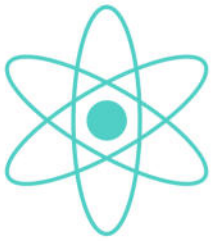
برز مصطلح "الحوسبة الكمومية" منذ 30 عامًا غير أنّه بات يحظى حاليًا بانتباه كبير، فتستخدم أجهزة الحوسبة التقليدية (مثل الكمبيوتر المحمول والهواتف الذكية) أرقامًا ثنائية أو بت من أجل عملياتها، ويمكن لهذه البت أن تفترض قيمة صفر أو واحد. غير أنّ الوحدة الأساسية في مجال الحوسبة الكمومية هي كيوبيت التي يمكنها أن تفترض قيمة صفر وواحد في الوقت نفسه، وهذا ما يسمح للحواسيب الكمومية بالعمل بسرعة قصوى تفوق الأجهزة التقليدية، كما تفتح إمكانيات جديدة لمهام الحوسبة التي كانت مستحيلة سابقًا.



خلال اختبار أجري مؤخرًا، تمكّنت الحوسبة الكمومية من إجراء احتساب خلال 3 دقائق في حين كان لذلك أن يستغرق 10,000 عامًا لو أجراه نظام مع قوة حوسبية تبلغ 100,000 حاسوب مكتبي تقليدي، وذلك وفقًا لبعض الافتراضات[20]. يمكن لهذه القوة الحوسبية أن تؤدّي إلى تغييرات كبرى في مجال الأمن السيبراني وبخاصة فيما يتعلّق بالتشفير. وفقًا للباحثين، ستؤدّي الحوسبة الكمومية إلى وضع كسر سريع للخوارزميات المعتمدة. على سبيل المثال، اختبرت دراسة حديثة خوارزمية 2048-bit RSA وخلُصت إلى أنّه يمكن كسرها خلال 8 ساعات عبر استخدام الحوسبة الكمومية.[21]

يعمل الباحثون على تجهيز الأمن السيبراني لعصر الكمومية. مثلًا، وضع المعهد الوطني الأمريكي للمعايير والتقنية (NIST) قائمة مختصرة لاختبار 26 من الخوارزميات، على أمل العثور على بعض خوارزميات "مقاومة الحوسبة الكمومية" ضمن هذه القائمة .

ثمّة نهج آخر يدعى التشفير السيادي، والذي يحثّ الهيئات المحلية على توزيع خوارزميات متعدّدة، مثلًا خوارزمية للخدمات المالية على خوادم محلية وخوارزمية أخرى للخدمات الصحية. فقد يشكل استخدام خوارزميات متعددة خطرًا يتمثل في أنها قد تكون أقل دقّة في عملية الاختبار كما أنّها قد تحتوي على ثغرات، غير أنّ استخدام عددًا كبيرًا من هذه الخوارزميات يساهم في تجنب مخاطر نقاط الفشل الفردية (على سبيل المثال عند كسر الخوارزميات المعتمدة على نطاق واسع).



ليس هنالك أي إجماع علمي حول الوقت المطلوب لبناء حواسيب التقنية الكمومية، ففي حين يقدّر الخبراء الأكثر تفاؤلًا أن يستغرق ذلك 5 إلى 10 سنوات، يقدّر الخبراء الآخرون الأكثر حذرًا أن يتطلّب ذلك من 20 إلى 30 عامًا.[22] غير أنّ المؤسسات نصحت بالاستعداد للحوسبة الكمومية. من المفترض أن يشكّل ذلك عملية طويلة قد تتطلّب عشرات السنين بالنسبة إلى المؤسسات الأكثر تعقيدًا مثل الشركات الكبرى أو الهيئات المحلية.

الاستعداد من أجل الحوسبة الكمومية

العمل الآن

من الضروري تأمين حماية أقوى للبيانات، فالتشفير وحده لا يكفي ويجب منع وصول الأطراف غير المصرح لهم إلى البيانات، ذلك لأنّه يمكن للمهاجمين اللجوء إلى تقنيات "الحصاد وفك التشفير"، والتي تركز على الوصول إلى البيانات المشفرة، وتخزينها حتى يمكن فك تشفيرها باستخدام أجهزة الكمبيوتر الكمومية.[23]

الاستعداد من أجل المستقبل

على المؤسسات أن تستعدّ للحوسبة الكمومية مع "دعم التشفير" ممّا يعني القدرة على التحديث المستمرّ لحماية التشفير والخوارزميات لكي تبقى متجاوزة على المهاجمين.[24] كجزء من هذه العملية، سيكون من الضروري البحث بانتظام والعمل على تطوير خوارزميات التشفير المقاومة للحوسبة الكمومية.[25]

[20] الطبيعة، مرحبًا في عالم الحوسبة الكمومية! Google publishes landmark quantum supremacy claim، أكتوبر 2019.
[21] كرايج جيدني وآخرون، كيفيّة تصنيع الأعداد الصحيحة L RSA 2048 bit خلال 8 ساعات عبر استخدام 20 مليون كيوبيت، ديسمبر 2019.
[22] القضية ضدّ الحوسبة الكمومية، نوفمبر 2018.
[23] ديلويت، التوقعات في مجال التقنية ووسائط الإعلام والاتصالات، 2019.
[24] المعهد الوطني الأمريكي للمعايير والتقنية (NIST) ، تقرير حول ما بعد التشفير الكمومي، أبريل 2016.
[25] التشفير الكمومي الآمن (QSC)، المعهد الأوروبي لمعايير الاتصالات (ETSI)، ETSI White Paper رقم 8، يونيو 2015.

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 الثاني من العام 2020م، 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