الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

مركز الدراسات الاستراتيجية للأمن السيبـراني
Center For Cybersecurity Strategic Studies

النـشـرة الربعية للأمن السيبراني

الربع الأول - 2020

تصنيف الوثيقة: متاح

إشارة المشاركة: أبيض

جدول المحتويات

ملخص النشرة	3
بيانات سيبرانية : سايبر بايت	3
الأمن السيبراني من منظور عالمي	4
الأمن السيبراني من منظور وطني	5
أحداث سيبرانية	6
ومضة سيبرانية	7
التطلّع : لتوجهات جديدة	8
تسليط الضوء على الابتكارات السيبرانية	9

ملخص النشرة

الربع الأول من العام 2020 (يناير – مارس)

- نظّمت الهيئة الوطنية للأمن السيبراني المنتدى الدولي للأمن السيبراني وهو أكبر وأهمّ حدث تمّ تنظيمه في المنطقة حول الأمن السيبراني..
- في هذه الأثناء، أثرت جائحة كوفيد 19 على الربع الأول من العام 2020 وأدّت حالة الطوارئ العالميّة إلى تداعيات على مستوى الأمن السيبراني. برز العمل عن بعد بشكل غير مسبوق على المستوى العالمي، وتزايدت التهديدات السيبرانيّة بالتزامن مع الجائحة حيث تركزت هجمات الهندسة الاجتماعيّة على استغلال الوباء والأزمات الاقتصادية الناجمة عنه

بيانات سيبرانية: سايبر بايت

الإحصاءات الرئيسيّة في الربع الأول وأبرز القطاعات المستهدفة على الصعيد العالمي

أجهزة غير آمنة متّصلة بشبكات الشركات

+1,000 يوميًا

قدّرت الشركات في أوروبا وأميركا الشمالية ارتفاعًا حادًا لأجهزة الموظّفين غير الآمنة المتّصلة بشبكات الشركة من دون معرفة إدارات تقنية المعلومات بذلك.[2]

العدد المتوقّع للعاملين عن بُعد خلال أزمة كوفيد 19

+300,000,000

ارتفعت نسبة العمل عن بُعد من 27% إلى 60% منذ مارس 2020. ففي إيطاليا فقط – حيث كانت إجراءات الإغلاق صارمة – تم ملاحظة ارتفاع النشاطات شهرياً بنسبة 775% على منصّة التعاون الخاصّة بأحد مقدمي الخدمات.[1]

موقع إلكتروني خبيث حول كوفيد 19

9 من أصل 10

في الفترة ما بين 9 و23 مارس، تمّ إنشاء +315,000 موقع إلكتروني متعلق بموضوع كوفيد 19. من بينها 9 من أصل 10 خبيثة أو مرتبطة بعمليات الاحتيال أو الخداع.[3]

تكلفة خريطة كوفيد 19 الخبيثة الجاهزة للاستخدام

بمعدّل 750 ريال سعودي

يتم بيع أدوات تصيّد على غرار الخرائط التفاعليّة التي تبيّن البيانات حول انتشار كوفيد 19 والتي تكون مزوّدة ببرمجيات خبيثة.[4]

أبرز 5 قطاعات تعرضت لتهديدات سيبرانية عالميًا في الربع الأول من العام 2020 [5]

1. القطاع العام - 21,58%
2. قطاع الرعاية الصحية - 13,37%
3. قطاع التعليم - 12,16%
4. القطاع المالي - 11,55%
5. قطاع التصنيع - 7,29%

أبرز 5 تهديدات سيبرانية عالمية في الربع الأول من العام 2020 [5]

1. البرمجيات الخبيثة - 42,09%
2. قرصنة الحسابات - 19,66%
3. الاختراق \ محاولة الاختراق - 11,97%
4. الثغرات الأمنية - 6,20%
5. البريد غير المرغوب به - 4,70%

أبرز 5 تهديدات سيبرانية في المملكة العربية السعودية في الربع الأول من العام 2020[6]

1. البرمجيات الخبيثة -
2. الدخول، التعديل والاستخدام غير المصرح به -
3. الاختراق/محاولة الاختراق -
4. الاستخدام غير الصحيح -
5. تسرّب البيانات -

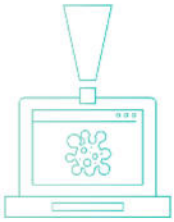
[1] BGC، إدارة المخاطر السيبرانية للعمل عن بُعد، مارس 2020.
[2] ديلويت، الموجز التنفيذي الأسبوعي الخاص بكوفيد 19 السيبراني العالمي، مارس 2020.
[3] فوربس، تكشف بيانات جوجل ارتفاعًا بنسبة 350% للمواقع الإلكترونيّة للتصيّد خلال فترة وباء فيروس كورونا
[4] ظلال رقميّة، كيف يستفيد المجرمون السيبرانيّون من كوفيد 19، مارس 2020.
[5] تبيّن الأرقام التوزيع (%) على مجموع الهجومات التي تمّ تسجيلها عالميًا للربع السنوي الأوّل.
[6] تحليل الهيئة الوطنيّة للأمن السيبراني، تبيّن أبرز التهديدات التي تمّ تسجيلها في المملكة العربية السعودية للربع السنوي الأوّل.

الأمن السيبراني من منظور عالمي

عناوين الأمن السيبراني الرئيسيّة من مختلف أنحاء العالم

حملات كوفيد 19 وانعكاساتها على منظمة الصحة العالمية

تتزايد الحملات السيبرانية حول موضوع كوفيد 19 في مختلف أنحاء العالم والتي تستغل الحاجة بالاطلاع على أحدث **الأخبار والمعلومات** عن الوباء. تقع منظمة الصحة العالمية كأحد أبرز الضحايا للهجمات السيبرانية المستهدفة (مع محاولة المهاجمين الوصول إلى حسابات موظّفي منظمة الصحة العالمية لاستخراج بيانات حول لقاحات وأدوية كوفيد19) [7]



منذ بداية الأزمة، ازدادت الحملات الخبيثة من المهاجمين الذين يتظاهرون بأنّهم من منظمة الصحة العالمية بهدف الحصول على المال (مثلًا من خلال التبرعات الزائفة) أو الاعتمادات (من خلال خدمات الاشتراك **الزائفة مثلاً**)، **ونظرًا** لخطورة الوضع أصدرت منظمة الصحة العالمية بيانًا رسميًا تحذّر فيه من حملات الهندسيّة الاجتماعيّة. وقد تكرّرت أيضًا هجمات مماثلة تشمل المؤسسات مثل المركز الأميركي للسيطرة على الأمراض والوقاية منها و منظمة الأمم المتحدة للطفولة (اليونيسيف) [8]

التهديد السيبراني المستهدف للرعاية الصحية والاستجابة من المجتمع السيبراني

أعادت التهديدات والهجمات السيبرانية تركيز جهودها على حملات كوفيد 19 وبشكل خاص ضدّ قطاع الرعاية الصحية. [9] ، حيث شكلت العديد من التهديدات السيبرانية على قطاع الرعاية الصحية مصدر قلق في كلّ أنحاء العالم، نظراً لأن هذا القطاع يشهد عالميًا ضغطًا تشغيليًا هائلًا في محاولته احتواء حالات الطوارئ الصحية. حيث يكافح المشغلون من أجل تأمين الموارد الضرورية لحماية المستشفيات والطاقم الطبي والمرضى، وعلى الرغم من ادعاءات بعض مجموعات الاختراق السيبرانية بعدم استهداف قطاع الرعاية الصحية خلال حالات طوارئ كوفيد 19، إلا أن الهجمات ارتفعت بشكل ملحوظ على هذا القطاع، ممّا يشكّل خطرًا على فعاليّة الوقاية والمعالجة والاستجابة للوباء. [10]

[7] رويترز، حصري: نخبة القراصنة يهاجمون منظمة الصحة العالمية في حين يرتفع عدد الهجمات السيبرانية الخاصة بفيروس كورونا، مارس 2020.
[8] منظمة الصحة العالمية، حذار من المجرمين الذين يدعون بأنّهم منظمة الصحة العالمية.
[9] ديلويت، ارتفاع التهديدات السيبرانية في مارس وأبريل وسط كوفيد 19، أبريل 2020؛ ديلويت، الموجز التنفيذي الأسبوعي الخاص بكوفيد 19 السيبراني العالمي. عدد 3، أبريل 2020.
[10] فوربس، القراصنة يعدون "لا مزيد من الهجمات السيبرانية ضدّ قطاع الرعاية الصحية" خلال أزمة كوفيد 19، مارس 2020؛ الإنتربول، المجرمون السيبرانيون يستهدفون مؤسسات الرعاية الصحية برانسوماواري، أبريل 2020.

الأمن السيبراني من منظور وطني

عناوين الأمن السيبراني الرئيسية في المملكة العربية السعودية

حوار الأمن السيبراني لمجموعة العشرين

كجزء من الجهود التي تبذلها المملكة لأولوية الأمن السيبراني في سنة رئاسة المملكة لقمة العشرين، قامت المملكة بعقد حوار الأمن السيبراني في تاريخ 3-فبراير-2020 وبالتزامن مع الاجتماع الأول لفريق عمل الاقتصاد الرقمي كفعالية جانبية رسمية في جدول أعمال الرئاسة [12]

يهدف الحوار إلى تعزيز النقاش حول الأمن السيبراني في مختلف القطاعات وتوسيع نطاق النقاش حول أولوية الأمن السيبراني في مسار الاقتصاد الرقمي ومناقشة الأفكار المبتكرة لبناء القدرات والتفاعل مع القطاعات الخاصة والدول ذات الاقتصادات الناشئة. حضر هذا الحدث نخبة من أصحاب المصلحة بما في ذلك ممثلو مسار الاقتصاد الرقمي في مجموعة العشرين، وعدد من أعضاء مجموعة الأعمال، بما في ذلك ممثلين من أبرز شركات القطاع الخاص و التقنيات المتقدمة، وقادة الفكر العالمي، والمنظمات الدولية.

استضافة المملكة العربية السعودية للمنتدى الدولي للأمن السيبراني

في 4 – 5 فبراير 2020م، استضافت الهيئة الوطنية للأمن السيبراني المنتدى الدولي للأمن السيبراني في الرياض، وهو أضخم حدث في مجال الأمن السيبراني تمّ تنظيمه في الشرق الأوسط حتى اليوم، حيث جمع أكثر من 3,500 مشارك من 58 بلداً بما فيه مسؤولين حكوميّين وأكاديميّين وقادة في مجال الأعمال؛ وذلك من أجل مناقشة الأمن السيبراني العالمي. سنحت الفرصة للحاضرين لحضور حلقات نقاش في مجال الأمن السيبراني والتهديدات والمخاطر الناجمة عنها بالإضافة إلى مواضيع أخرى مثل السلوك الأمني والتعاون الدولي.

- تمّ عقد عدّة اجتماعات بين الهيئة الوطنية للأمن السيبراني وأصحاب المصلحة المحليين والإقليميّين والدوليين، حيث وقّعت الهيئة الوطنية للأمن السيبراني خلال هذه الاجتماعات 5 مذكرات تفاهم أساسيّة لتعزيز التعاون ما بين الشركاء المحليين والدوليين وذلك لتعزيز واقع الأمن السيبراني في المملكة.[13]

بيان الرياض للأمن السيبراني

أطلقت الهيئة الوطنية للأمن السيبراني خلال المنتدى الدولي للأمن السيبراني **"بيان الرياض للأمن السيبراني"** إدراكاً منها لفرص النمو الاقتصادي والاجتماعي الهائلة، والمنبثقة عن التقدم التقني المتسارع وربط الأنظمة التقنية عالمياً عبر الفضاء السيبراني، وبالرغم من خلق هذه التطورات لفرص جديدة وواعدة، إلا أنها مصحوبة بتزايدٍ ملموس للتحديات والمخاطر السيبرانية على مستوى الأفراد والمنظمات سواءً محلياً أو دولياً.

وبناءً على ذلك، تم التوصل إلى توصيات بيان الرياض للأمن السيبراني، وتدعو الهيئة الجميع للانضمام إليها في دعم هذه التوصيات الرامية إلى تضافر الجهود نحو فضاء سيبراني أفضل للجميع..

يمكن الحصول على البيان على globalcybersecurityforum.com/declaration

Global Cybersecurity Forum

[12] الموقع الإلكتروني الرسمي لمجموعة العشرين.
[13] المنتدى الدولي للأمن السيبراني، توقيع 5 مذكرات تفاهم بارزة خلال المنتدى الدولي للأمن السيبراني، فبراير 2020.

أحداث سيبرانية

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

حملات الهجمات ضد منظمة الصحة العالمية [14]

المكان: عالميًا

القطاع: منظمة عالمية، الرعاية الصحية

تاريخ الإفصاح: فبراير 2020

نوع الهجوم: هجمات متعدّدة (تصيّد، تزوير المواقع الإلكترونيّة، وغيرها.) عبر استخدام تقنيات الهندسة الاجتماعية

الوصف: في 11 فبراير، حذّرت منظمة الصحة العالمية من حملات سيبرانية تواصل من خلالها المهاجمين مع الضحايا مدّعين بأنّهم موظّفي منظمة الصحة العالمية وذلك بهدف الحصول على بيانات حسابات و غيرها من المعلومات الحسّاسة من الضحايا.

تزايدت هذه الهجمات وبخاصّة حملات رسائل التصيّد الإلكترونيّة التي تحتوي على روابط تؤدّي إلى مواقع إلكترونيّة خبيثة أو تتضمّن برمجيات ضارّة تأتي على شكل مرفقات مزيّفة. تبدو هذه الرسائل الإلكترونيّة على أنّها لا تستهدف أفرادًا معيّنين وغالبًا ما تكون صياغتها تتضمّن أخطاء كتابيّة ولغويّة.

في كثير من الحالات، يستخدم المهاجمون رسائل تصيّد إلكترونيّة تحتوي على روابط لمواقع إلكترونيّة مزيفة , حيث يتم نسخ تصميم موقع إلكتروني و محتوياته ليبدو نسخة مطابقة للموقع الأصلي وذلك من أجل إقناع الضحايا بأنّ الموقع الإلكتروني سليم.

أشار باحثون في الأمن السيبراني أن من أكثر البرمجيات الخبيثة شيوعاً والتي تم استخدامها في الحملات السيبرانية على منظمة الصحة العالمية كان-برنامج " AgentTesla " والذي يعتبر راصداً للوحة المفاتيح؛ حيث يعمل على تسجيل جميع البيانات التي يدخلها المستخدمين عن طريق لوحة المفاتيح بما فيها كلمة المرور وغيرها من المعلومات الحساسة.

التأثير: بمقارنة الربع الأول من العام 2019، بالربع الأول من العام 2020 اتضح أن الهجمات السيبرانية باتت أعلى 5 مرات. استهدفت هذه الهجمات موظّفي منظمة الصحة العالمية كما أدعى المهاجمون بأنّهم موظّفي منظمة الصحة العالمية، الأمر الذي يشكّل عبئًا تشغيليًا إضافيًا في ظل ظروف جائحة كوفيد 19.

الدروس المستفادة: لقد برهنت أهمية الحوكمة في أوقات الأزمات والتي لها دوراً كبير في إدارة الأزمات (في هذه الحالة، أزمة صحيّة عالمية) وتداعياتها على مستوى الأمن السيبراني.

حيث يوصى في ظل الأزمات بما يلي:

- الحفاظ على مستوى عالٍ من المراقبة والرصد للتهديدات السيبرانية وخاصة فيما يتعلق بالهجمات السيبرانية التي تنتحل هوية الجهات الرسمية
- الابلاغ والتحذير عن حملات الهندسة الاجتماعية التي تم الكشف عنها
- رفع الوعي السيبراني عن الممارسات الجيّدة حول كيفيّة الاستجابة لعمليات الهندسة الاجتماعية.

[14] منظمة الصحة العالمية، حذار من المجرمين الذين يدعون أنّهم منظمة الصحة العالمية؛ CISA، الدفاع ضدّ الخدع السيبرانية الخاصة بكوفيد 19، مارس 2020؛ Bleeping Computer، تحذّر منظمة الصحة العالمية من هجمات تصيّد خاصة بفيروس كورونا، فبراير 2020؛ سوفوس، فيروس كورونا "تدابير السلامة" رسالة تصيّد إلكترونية خادعة، فبراير 2020؛ فورتينت، كوفيد 19 العالمي/حملة الخداع الإلكتروني الذي يكشف الهويات الخاص بفيروس كورونا بسرق المعلومات، أبريل 2020؛ كاربون بلاك، تحليل تقني: يعزز القراصنة وباء كوفيد 19 لإطلاق هجمات تصيّد، تطبيقات مزيّفة/خرائط، طروادیون، أبواب خلفيّة، Cryptominers, Botnets & Ransomware، مارس 2020؛ Proof Point، مهاجمون يوسعون هجمات ذات موضوع فيروس كورونا ويتصيّدون على نظريات المؤامرة، فبراير 2020.

ومضة سيبرانية

برهنت أزمة كوفيد 19 كيف يمكن أن تتغير بيئة و طبيعة العمل بشكل مفاجئ.

توضح الارشادات التالية خطوطًا توجيهيّة لأصحاب الأعمال حول كيفيّة التعامل مع الأزمات.[15]

نصائح للإدارة العليا

الاستجابة الفعالة للأزمات

- يجب أن يتم تفعيل فريق إدارة الأزمات.
- يجب التأكد من أنّ البنية التقنية للجهة وأنظمتها محدثة بآخر التحديثات الأمنية.
- يجب توفير أجهزة للعمل عن بُعد للموظفين، بحيث تتوافق مع متطلبات الأمن السيبراني للوصول الآمن لشبكة الجهة.
- يجب تفعيل وسائل الاتصال (مثلًا "خطّ ساخن") لدعم الموظفين في الانتقال إلى العمل عن بُعد.
- يجب اعتماد وسائل لدعم العمل عن بُعد (مثلًا تقنيات الاتصال الآمن عن بعد)، على أن يتم تقييم هذه الوسائل للتأكد من تحقيقها لمتطلبات الأمن السيبراني.

الاستعداد للأزمات

- توثيق معايير وضوابط الأمن السيبراني وتنفيذها والامتثال لها.[16]
- تحديد الأصول الهامة للمنظمة وضمان تطبيق ضوابط الأمن السيبراني وفقًا لذلك.
- تطوير خطة استمرارية الأعمال للمنظمة و للأنظمة الحساسة للمنظمة.
- تحديد خدمات المنظمة وموظفيها الذين يحتاجون إلى العمل من الموقع، و من يمكنهم العمل عن بُعد، و الأنشطة التي يمكن تعليقها أوقات الأزمات.
- تحديد "فريق إدارة الأزمات" المسؤول عن إدارة العمليات أوقات الأزمات، و التأكد من أن الفريق لديه القدرات والإمكانيات اللازمة لذلك، و كذلك حصوله على الدعم داخل المنظمة (مثل تقنية المعلومات والقانونية وغيرها).
- التأكد من أن شبكة المنظمة قابلة للتوسع لدعم احتياجات المنظمة في ظل الأزمات (مثل دعم الحجم الكبير للبيانات بسبب متطلبات العمل عن بعد، VOIP، وما إلى ذلك) و إجراء الاختبارات اللازمة لذلك.
- إجراء اختبارات لاستمرارية الأعمال تحاكي عمليات المنظمة أثناء الأزمات.
- مراجعة خطط إدارة الأزمات بشكل دوري.

نصائح للموظفين

- تعرف على خطة المنظمة لإدارة الأزمات.
- تأكد من استخدام شبكة آمنة، و تحديث جميع الأجهزة المتصلة بآخر التحديثات الأمنية، واستخدام كلمات مرور قوية تتوافق مع سياسات الأمن السيبراني للمنظمة.

[15] تمّ إعداد هذه الخطوط التوجيهيّة والنصائح من قبل الهيئة الوطنية للأمن السيبراني .مع الأخذ بالاعتبار الاقتراحات التي قدّمتها مؤسسات معروفة على غرار المعهد الوطني الأميركي للمعايير والتكنولوجيات (NIST SP 800-53 الضوابط الأمنيّة والخطوط التوجيهيّة لعمل المؤسسات عن بُعد، الوصول عن بُعد، وأمن "استخدم جهازك الشخصي (BYOD) 46-800)، معهد SANS (سياسة التخطيط للاستجابة للوباء، 2020)، اللجنة الفرنسية Commission nationale de l'informatique et des libertés (Les conseils de la CNIL pour mettre en place du télétravail)، وزارة الأمن الوطني الأميركية (اتصالات الإنترنت الموثوقة 3.0 الخطوط التوجيهيّة المؤقتة للعمل عن بُعد)، وديلويت (كوفيد 19: سايبر والقوة العاملة عن بُعد).

[16] بهدف تحديد الأمن السيبراني الأساسي المتعلّق بالمنظمة بطريقة فعالة، يرجى اللجوء إلى الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني.

التطلّع: لتوجهات جديدة

من المتوقّع أن تتسبب جائحة كوفيد 19 بآثار دائمة وستكون التكنولوجيا المحرك الداعم للتعافي من هذه الأزمة. نتطرق هنا للسيناريوهات المستقبليّة الممكنة والأثر المتوقّع على مجال الأمن السيبراني

السيناريو 1: العمل عن بُعد : طريقنا للخروج من الأزمة

ستؤثّر تدابير الاحتواء للجائحة على هذا السيناريو بطريقتين مختلفتين:

1.تراجع العمل عن بُعد إلى مستوى ما قبل الأزمة. سيحصل ذلك في حال جاءت الأزمة وتداعياتها على الاقتصاد بأثر شديد وتعافي سريع (6-12 شهر)، أو

2.استمرار العمل عن بُعد. سيتأقلم العاملون وتدرك المؤسسات قيمته ما بعد الطوارئ. كلّما استمرّ الإغلاق على المستويات الوطنية لفتره أطول، ارتفعت احتمالات استمرار العمل عن بُعد.

من المتوقّع التوسع بالعمل عن بعد على المستوى العالمي بعد انقضاء الجائحة[17] . سيشهد ذلك تزايداً في الهجمات السيبرانية التي تستهدف الموظفين وذلك نظرًا لأنّ الشبكات المنزليّة تعتبر أقلّ حماية مقارنة بشبكات المؤسسات. تبعاً لذلك، ستعزز المؤسسات من قدراتها و تفعّل استخدام الحلول الأمنيّة للوصول الآمن كما ستركز المؤسسات على تقديم برامج التدريب لزيادة نسبة وعي الموظفين في الأمن السيبراني واتباع ممارسات الأمن السيبراني للعمل عن بعد.

السيناريو 2: مشهد جديد للأعمال، مخاطر جديدة، فرص جديدة

سيؤثّر كوفيد 19 على مشهد الأعمال بطريقتين:

1.التغييرات على الأعمال القائمة في القطاع الصحي. إنّ بعض الشركات التي تصنّع المنتجات الطبية (مثل أجهزة التنفّس الصناعي، أقنعة العمليات الجراحية، المطهّر) أو التي تؤمّن الخدمات (مثل الخدمات اللوجستية الضرورية للمستشفيات) لمكافحة كوفيد 19 قد تمّ شملها كجزء من البنية التحتية الوطنيّة الأساسية على المستوى العالمي[18]. معظم الشركات ومقدمي الخدمات في هذا المجال غير جاهزين لتحقيق متطلبات الأمن السيبراني على هذا المستوى. لذلك عليها أن تستثمر في الأمن السيبراني للامتثال لهذه المتطلبات و لتعزيز قدرات الأمن السيبراني للقطاع على المستوى العالمي. هناك فرصة قائمة لمقدمي الخدمات في القطاع لتكون قدرات الأمن السيبراني ميزة تنافسيّة لديهم .

2.تأسيس أعمال وخدمات صحية جديدة. من المتوقّع أن يستمرّ الإنفاق الحالي المرتفع على المنتجات الصحية (منذ بداية حالة الطوارئ، سجلت عمليات الشراء عبر الإنترنت لمنتجات السعال والإنفلونزا ما يفوق 190%+) على المدى المتوسّط إلى المدى البعيد ممّا يؤثّر على الخدمات الطبية أيضًا. من المتوقع أن يزدهر الطب عن بُعد والاستشارات الطبية عن بُعد ممّا سيترتب عليه زيادة في التهديدات السيبرانية التي يواجهها القطاع (تقدر قيمة البيانات الصحية مرتفعة بنسبة 5000% مقارنة بقيمة المعلومات الشخصيّة)[19]

السيناريو 3: نمو سوق الأمن السيبراني

سيشجّع الأثر المشترك للتهديدات السيبرانية المرتفعة والاعتماد المتزايد على التكنولوجيا إلى تطوّر منتجات و خدمات الأمن السيبراني التي يتم تقديمها في سوق الأمن السيبراني .

وفقًا للتقديرات، من المتوقّع أن يشهد سوق الأمن السيبراني على المستوى العالمي نموًا بحوالي 699 مليار ريال سعودي عام 2019 إلى ما يفوق 863 مليار ريال سعودي مع حلول العام 2021. ستشهد تقنيات حماية الأجهزة والكشف والاستجابة عن التهديدات السيبرانية أكبر نسبة من النموّ وذلك بسبب حاجة عدد كبير من المؤسسات لهذه التقنيات لتلبية حاجات العمل عن بُعد. كما تشير التوقعات أن تشهد حلول أمن الشبكات والوصول الآمن نموًا مشابهًا.[21]

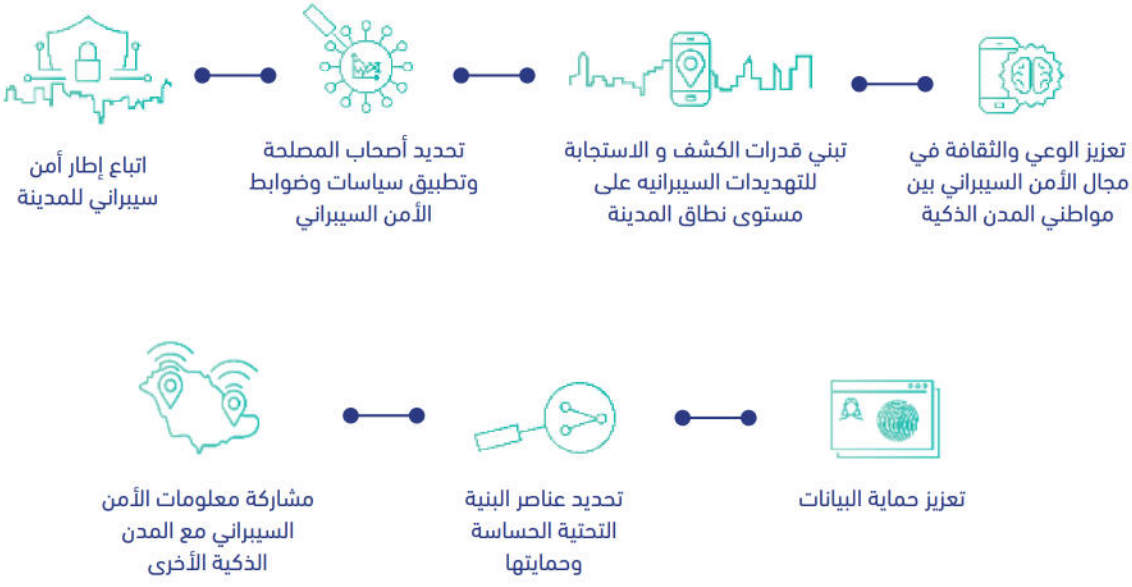
[17] ديلويت، كوفيد 19: الأشخاص، التكنولوجيا والمسار للمرونة المؤسسية، 2020
[18] ديلويت، جوهر القيادة المرنة. استرجاع الأعمال جراء كوفيد 19، 2020.
[19] شركة نيلسن، حدود سلوك المستخدم الرئيسي المحدّدة مع ارتفاع تفشّي فيروس كورونا، مارس 2020؛ ديلويت، الموجز التنفيذي الأسبوعي الخاص بكوفيد 19 السيبراني العالمي، عدد 3، أبريل 2020؛ The Financial Times، يؤدّي الإغلاق إلى ازدهار تطبيقات الرعاية الصحية، مايو 2020.
[20] الأسواق والأبحاث، تأثير كوفيد 19 على سوق الأمن السيبراني من خلال التكنولوجيا، Vertical, Region - التوقعات العالمية للعام 2021.

تسليط الضوء على الابتكارات السيبرانية

نظراً لمساهمة المدن الذكية في مكافحة الأوبئة نستعرض توصيات لتعزيز قدراتها السيبرانية

البنية التحتية التقنية المتكاملة والمتقدمة في المدن الذكية تعتبر أصولاً قويّة لمواجهة الأوبئة. نستعرض فيما يلي توصيات لتعزيز قدرات الأمن السيبراني للمدن الذكية.

إن تفعيل الإمكانيات التقنية للمدن الذكية لمكافحة الأوبئة يتطلب تعزيز قدرات الأمن السيبراني للمدن الذكية لمواجهة التهديدات السيبرانية. أهم التوصيات تتلخص فيما يلي:



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 الأول 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