
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority
مركز الدراسات الاستراتيجية للأمن السيبراني
Center For Cybersecurity Strategic Studies
النشرة الربعية للأمن السيبراني
الربع الثالث – 2020
التصنيف: عام
إشارة المشاركة: أبيض

جدول المحتويات

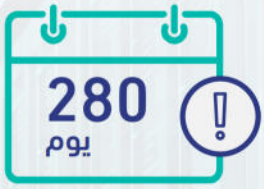
ملخص النشرة

الربع الثالث من العام 2020 (يوليو – سبتمبر)

- على المستوى الوطني، موافقة مجلس الوزراء للاستراتيجية الوطنية للأمن السيبراني في الخامس عشر من شهر سبتمبر. وتهدف الاستراتيجية الوطنية للأمن السيبراني التي وضعتها الهيئة الوطنية للأمن السيبراني إلى بناء فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار.
- على المستوى العالمي، وعلى الرغم من أنّ الجائحة لا تزال تؤثّر على قطاع الأمن السيبراني، صدرت خلال هذا الربع توصيات وتوجهات لمواجهة المخاطر السيبرانية. فبالإضافة إلى الممارسات الجيّدة التي تهدف إلى حماية المؤسسات من جائحة سيبرانية، تمّ أيضًا إصدار إرشادات رئيسيّة. وفي هذا السياق، أطلقت MITRE إطار الدفاع والذي يسمّى "الدرع" لمواجهة التهديدات السيبرانية على الشبكة في حين تمّ إنشاء خرائط طرق جديدة أخرى لمساعدة المؤسسات لنشر نموذج عدم الثقة.

بيانات سيبرانية: سايبر بايت

إحصاءات رئيسيّة من الربع الثالث



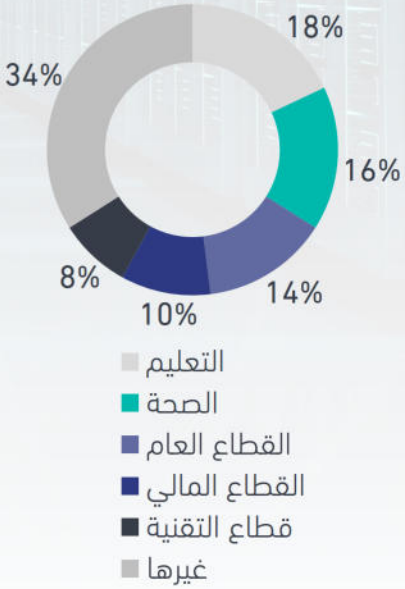
متوسّط المدة الزمنيّة لاكتشاف واحتواء اختراق للبيانات[1]
إنّ متوسّط المدة الزمنية لاكتشاف اختراق البيانات هو 207 يوم و73 يوم لاحتواء هذا الاختراق.

متوسّط الادخارات لاحتواء اختراق سيبراني في أقلّ من 200 يوم[2]
بلغ متوسّط التكلفة للاختراقات السيبرانية التي تجاوزت مدة الاحتواء 200 يوم مبلغ 16.2 مليون ريال سعودي مقابل 12 مليون ريال سعودي للاختراقات السيبرانية التي لم تتجاوز 200 يوم.

من المؤسسات واجهت اختراقًا سيبرانياً نتيجة العمل عن بُعد بشكل غير آمن[3]
أدّى ذلك إلى زيادة تكفلة الاستجابة للحوادث السيبرانية.

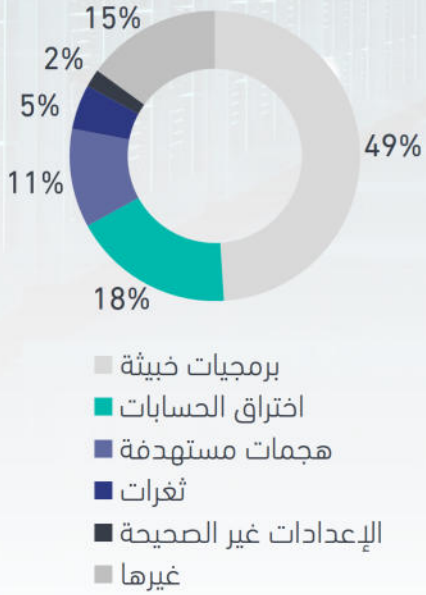
القطاع الصحي سجل المدة الزمنية الأعلى من بين القطاعات عالمياً[4]
يتفاوت متوسّط الوقت لاكتشاف واحتواء الاختراق السيبراني بشكل كبير بين القطاعات.

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



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

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



* تبيّن الأرقام التوزيع (%) على مجموع عدد التهديدات السيبرانية المسجّلة عالميًا خلال الربع الثالث

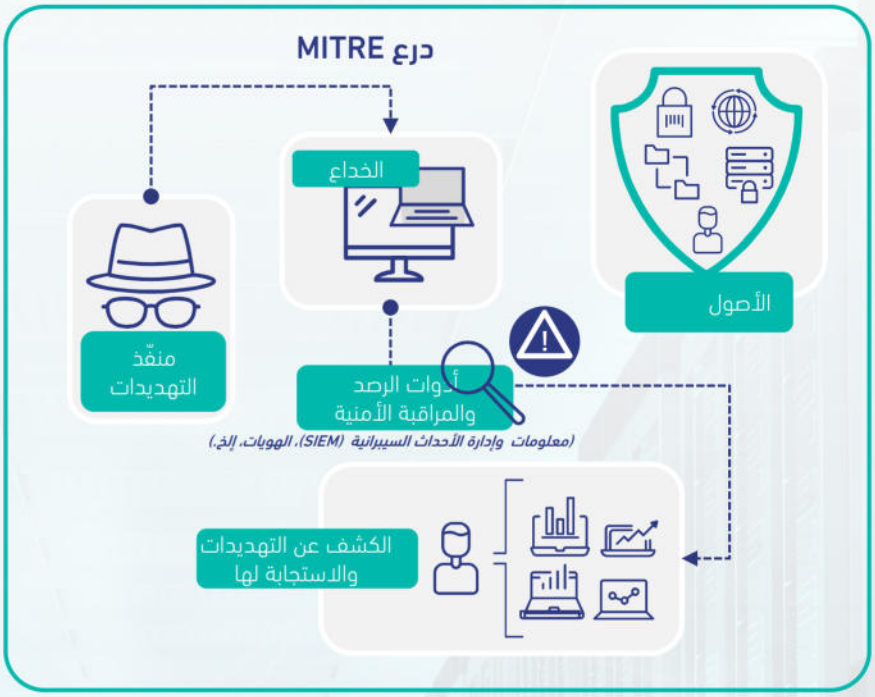
** تحليلات الهيئة الوطنية للأمن السيبراني. تبيّن أبرز التهديدات التي تم تسجيلها في المملكة العربية السعودية خلال الربع الثالث.

الأمن السيبراني من منظور عالمي

عناوين الأمن السيبراني الرئيسيّة من مختلف أنحاء العالم

درع MITRE: لمواجهة التهديدات السيبرانية

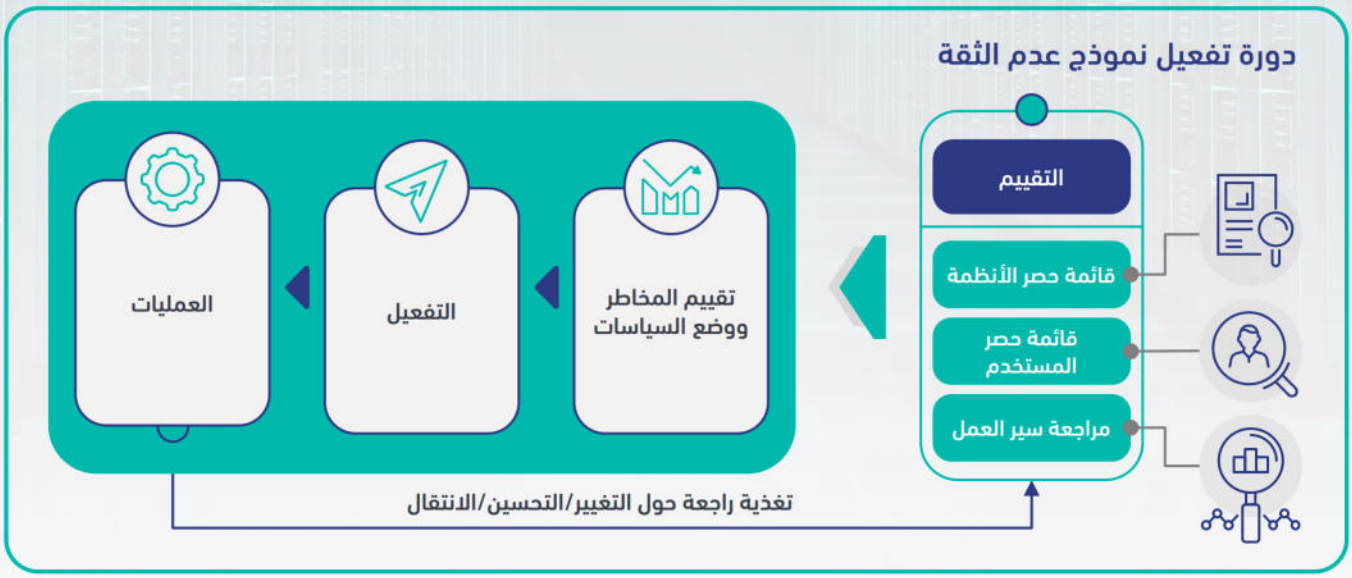
إنّ درع MITRE هو قاعدة معرفية تزوّد الخبراء في مجال الأمن السيبراني بالتقنيات والأساليب التي تمكّنهم من التعامل مع المهاجمين وحماية الشبكات من الهجمات السيبرانية [5].



بناءً على تقنيات الأمن السيبراني للخداع والارتباط المعاكس، يهدف "الدرع" إلى استدراج المهاجمين إلى أنظمة الخداع المستهدفة إلى جانب إبعادهم عن الأصول الخاصة بالمؤسسة. على عكس تقنيات الأمن السيبراني التقليدية مثل جدار الحماية، يساعد الارتباط المعاكس الخبراء في مجال الأمن السيبراني على تعلّم سلوك المهاجمين وعلى الحصول على بعض من الأدوات التي تمّ استخدامها.

خارطة طريق لنشر نموذج "عدم الثقة"

يفترض نموذج عدم الثقة أنّه لا يمكن لأحد سواء من داخل أو خارج الشبكة الحصول على صلاحية الوصول بشكل ضمني. وذلك وفقًا لمبدأ التأكّد من هوية المستخدم والجهاز والبنية التحتية قبل منح الوصول المشروط و بأقل صلاحيات، بات نموذج عدم الثقة الأمني جزءًا من المبادئ الرئيسيّة للحدّ من المخاطر السيبرانية.[6] وقد أدرجت الهيئة الوطنية للأمن السيبراني مفهوم عدم الثقة في الوثيقة التي نشرتها مؤخرًا بعنوان "المبادئ العامة للتصميم الآمن"[7]



كشف المعهد الوطني للمعايير والتقنية عن وثيقة حول معمارية عدم الثقة[8] التي تؤمّن خارطة طريق لتفعيل هذا النموذج انطلاقًا من تعريف الأصول الحساسة وصولًا إلى التشغيل. كما تتطرّق هذه الوثيقة إلى تهديدات نموذج عدم الثقة وتقنيات الحدّ منها.

الأمن السيبراني من منظور وطني

عناوين الأمن السيبراني الرئيسيّة في المملكة العربية السعودية

الاستراتيجية الوطنية للأمن السيبراني (تاريخ اعتمادها: 15 سبتمبر 2020)[9]

أطلقت الهيئة الوطنية للأمن السيبراني الاستراتيجية الوطنية للأمن السيبراني والتي تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو. تمكن تحقيق الرؤية الوطنية التي تهدف الهيئة الوطنية للأمن السيبراني إلى تحقيقها في ما يلي: فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار. وبهدف تحقيق ذلك، وضعت الهيئة الوطنية للأمن السيبراني 6 أهداف رئيسيّة.

أهداف الاستراتيجية الوطنية للأمن السيبراني:

إدارة فعّالة للمخاطر السيبرانية

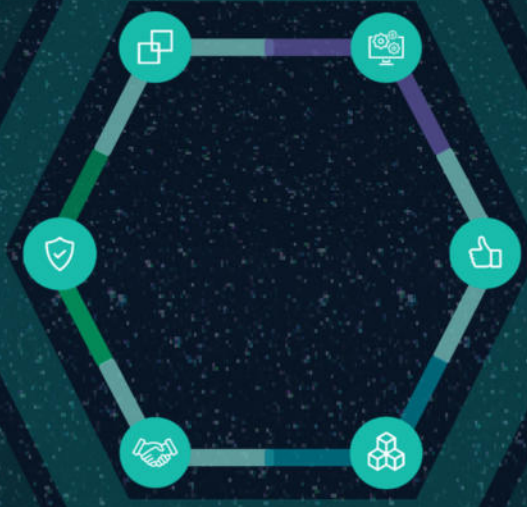
إدارة المخاطر السيبرانية على مستوى الجهات والقطاعات وعلى المستوى الوطني، وتحديد العناصر المتضررة في الفضاء السيبراني ومدى حدّة الضرر، واختيار أفضل الطرق لمعالجتها أو الحد من آثارها.

حوكمة متكاملة للأمن السيبراني على المستوى الوطني

من أجل ضمان تحقيق درجات عالية من التنسيق والمواءمة، من المهم تبني توجه وطني شامل للأمن السيبراني.

التنظيم

التكامل



التوكيد

الدفاع

التعاون

البناء

تعزيز الشراكات والتعاون في الأمن السيبراني

يتطلب الأمن السيبراني وجود شراكات محلية ودولية فعالة، ومعززة بآليات متطورة لمشاركة المعلومات.

تطوير صناعة الأمن السيبراني

حماية الفضاء السيبراني للمملكة تتطلب وجود قاعدة قوية من الكوادر الوطنية المؤهلة في هذا المجال بالإضافة لصناعة أمن سيبراني وطنية مزدهرة.

حماية الفضاء السيبراني

إن وجود ضوابط شاملة ومعايير وطنية ونظام لمتابعة الالتزام يحقق حماية منظومة الأمن السيبراني.

تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية

التعزيز والتطوير المستمر للقدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وذلك لكشف الهجمات والتهديدات السيبرانية، والتعامل معها، والاستجابة والتعافي منها في حال الإصابة بها.

أحداث سيبرانية

حادثة أمن سيبراني على وسائل التواصل الاجتماعي

الموقع: كلّ أنحاء العالم (بخاصة الولايات المتحدة)

القطاع: ويب / وسائل التواصل الاجتماعي

تاريخ الكشف: 15 يوليو 2020

نوع الهجوم: هندسة اجتماعية

الوصف: بدأت حسابات لشخصيات مؤثرة على وسائل التواصل الاجتماعي تغرّد برسائل ضارّة لمتابعيها وقد وصلت الرسائل الضارة إلى ما يقارب 350 مليون مستخدم. ومن خلال لوحة الإدارة الخاصة بالشركة فقد تمكن المهاجمون من اعادة تعيين عنوان البريد الإلكتروني المرتبط بالحساب وتعطيل خاصية التحقق الثنائي[10]

التأثير: من أصل 130 حساب مستهدف، استخدم 75 منها لتغريد رسائل مخادعة وتمكّنوا من رؤية معلومات شخصية مثل عناوين البريد الإلكتروني وأرقام الهاتف وغيرها من البيانات الحساسة.

الدروس المستفادة: أهمية تعزيز قدرات وصمود الأمن السيبراني لمنصات وسائل التواصل الاجتماعي. كما على الجهات رفع الوعي السيبراني لدى الموظفين للحماية من هجمات الهندسة الاجتماعية، إضافة إلى إدارة صلاحيات الوصول للموظّفين للحدّ من استخدام البيانات ضمن نطاق عملهم.

أنواع الهندسة الاجتماعية

التهديد السيبراني على شركة "تسلا" Tesla

الموقع: الولايات المتحدة

القطاع: النقل

تاريخ الكشف: 19 أغسطس 2020

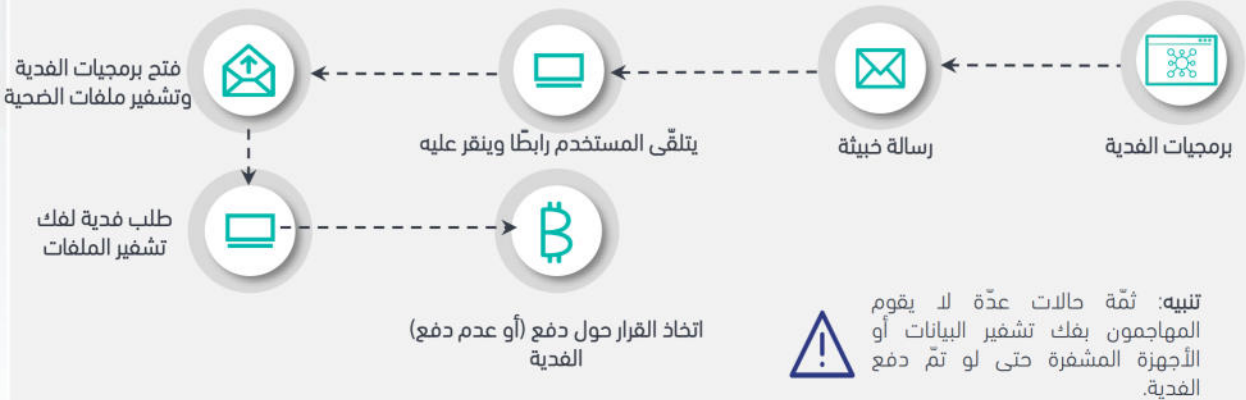
نوع الهجوم: برمجيات الفدية

الوصف: إنّ محاولة الهجوم السيبراني كانت عبارة عن محاولة لاستغلال موظف شركة تسلا Tesla لإدخال برمجية خبيثة في شبكة مصنع نيفادا. وكان المخطط بعد تفعيل البرمجية الخبيثة، أن يتمّ تفعيل هجمات تعطيل الخدمات الموزعة لاستخراج البيانات من شبكة الشركة والتهديد بنشرها للعلن مع طلب فدية من شركة تسلا Tesla[11]

الأثر: كانت محاولة الهجوم وشيكة الوقوع. وعلى الرغم من ذلك، تشكّل هذه المحاولة قصّة تحذيريّة للشركات.

الدروس المستفادة: على الجهات تطبيق ضوابط للحماية من هجمات برمجيات الفدية والتي تتضمّن تزويد الموظفين بتحديثات منتظمة حول الوضع الحالي لنشاطات الاستجابة للأزمات إضافة إلى تعزيز السياسات الأمنية ومراقبة حسابات الموظفين للكشف عن النشاطات غير الاعتيادية.

مراحل هجوم برمجيات الفدية



تنبيه: ثمّة حالات عدّة لا يقوم المهاجمون بفك تشفير البيانات أو الأجهزة المشفرة حتى لو تمّ دفع الفدية.

ومضة سيبرانية

كيفيّة التعامل مع جائحة سيبرانية

إطلاق المركز الوطني الارشادي للأمن السيبراني (Saudi CERT) للدليل الارشادي للطلاب لجوانب الأمن السيبراني في التعليم عن بُعد

أطلق المركز الوطني الارشادي للأمن السيبراني (Saudi CERT) إرشادات حول الاستخدام الآمن للحاسب الآلي وحماية الأجهزة والخصوصية أثناء التعلم عن بعد. ونتيجة للأزمة الصحية العالمية، أتاحت المملكة العربية السعودية التعليم عن بُعد من خلال منصّاتها المعتمدة بما يتناسب مع التدابير الوطنية الاحترازية لمواجهة جائحة كوفيد 19. وتهدف حملة الأمن السيبراني إلى عون الطلبة وأولياء أمورهم على التبني الأمثل لتلك التقنية في بيئة تعزز من مستوى الأمن السيبراني لديهم[12]

نصائح للحماية من جائحة سيبرانية

قد تؤدّي جائحة سيبرانية إلى أثر كبير ينتج عنها تعطّل الأعمال والخدمات الحيوية . من الناحية الإيجابية، يتزايد إدراك الجهات بأهمية الأمن السيبراني و الذي يؤدّي دورًا أساسيًا في تمكين التحول الرقمي. إن اتباع ضوابط الأمن السيبراني تدعم رفع الجاهزية السيبرانية للجهات والتي تتضمن مايلي:

للحماية من...	يمكن للمؤسسات...	
خطأ بشري	تعزيز ثقافة الأمن السيبراني	من خلال شراكة ما بين إدارات الموارد البشرية والأمن السيبراني، يمكن للمؤسسات أن تنظّم تدريب توعوي لمساعدة الموظفين على تحديد الرسائل الالكترونية المشبوهة والامتثال لسياسات الأمن السيبراني.
ثغرات سيبرانية	تطبيق نموذج عدم الثقة	باتباع المبدأ "عدم الثقة" و اعتبار أنّ كلّ الأجهزة المتّصلة بشبكة المؤسسة غير موثوقة، يمكن للمؤسسات الحدّ من المخاطر السيبرانية. إنّ هذا النموذج هو بغاية الأهمية في ظل العمل عن بُعد المتزايد والاعتماد على الخدمات السحابية.
تهديدات سيبرانية	التعاون وتبادل المعلومات	إنّ الجائحة السيبرانية قد يكون لها أثر مشترك ولا شكّ في أنّ وضع المؤسسات سيكون أفضل في بيئة تعاونية حيث يتمّ مشاركة المعلومات. إن عمليات الدراية الأمنية تساهم في فهم أعمق لتهديدات الأمن الأمن السيبراني وتسهم في فعالية الدفاع ضد تلك المخاط
المخاطر السيبرانية المتعلقة الأطراف الخارجية	اعتماد إدارة مخاطر الأطراف الخارجية	من خلال إدارة مخاطر الأطراف الخارجية، يمكن للمؤسسات تحديد ورصد وإدارة المخاطر التي يتسبّب بها المورّدون الذين يؤدّون دورًا أساسيًا في أعمال المؤسسة.

التطلّع لتوجّهات جديدة

لمحة عن التوأم الرقمي والأمن السيبراني

يعد التوأم الرقمي (Digital Twin) من أبرز التوجهات الجديدة حيث أنّه يعرف ب "تمثيل إفتراضي لنظام مادي أو الكتروني خلال فترته الزمنية. يهدف النظام إلى تعزيز عملية اتخاذ القرارات من خلال الاعتماد على البيانات الفورية وغيرها من الموارد وذلك لتمكين التعلّم وإعادة المعايرة ديناميكيًا".[13] يمكّن التوأم الرقمي الشركات من تعزيز العمليات التنفيذية في بيئة إفتراضية قبل تطبيقها في البيئة الفعلية. ويكمن تنفيذ التوأم الرقمي في تطوير برمجيات نموذجيّة تمثل نظام مادي أو عملية أو مؤسسة، ويمكن شرح المراحل الأساسية كما في الشكل التالي:[14]

المعايير الأساسية للتوأم الرقمي

- آيزو (ISO) 23247 – يدعم إنشاء التوأم الرقمي لعناصر التصنيع التي يمكن رصدها؛
- آي إي سي (IEC) 62832 – يحدّد مبادئ إطار المصنع الرقمي؛
- آيزو تي أس (ISO TS) 18101-1 – يؤمّن الإرشادات لمعمارية النظام البيئي الرقمي والصناعي المحايد لجميع الموردين.

أبرز المخاطر السيبرانية الناجمة عن التوأم الرقمي[15]

- يمكن للفجوات السيبرانية ما بين التوأم الرقمي والنظام الفعلي أن تعرّض البيانات الحساسة للاختراق؛
- يمكن لتجميع البيانات الضخمة أن يعزّز مخاطر تلف البيانات،
- قد يشكّل التوأم الرقمي الذي تمّ اختراقه مخطّطًا مطابقًا للنظام الحقيقي والذي يقد يعرضه للتهديدات السيبرانية؛
- إنّ إدراج شركاء جدد في دورة إنتاج التوأم الرقمي يعزّز خطر التعرض للتهديدات السيبرانية.

التطبيق العملي للتوأم الرقمي[16]

أمثلة على استخدام التوأم الرقمي لتعزيز الأمن السيبراني :

يمكن استخدام التوأم الرقمي لإجراء اختبار على نسخه في البيئة الافتراضية عوضًا عن الاعتماد على التوثيق والنماذج نظرية للتهديدات السيبرانية.

إنّ استخدام مواصفات مفصّلة لنظام الإنتاج كنموذج للتوأم الرقمي يسمح للمؤسسة برصد التغييرات في النظام الأصلي والتبليغ عنها.

من خلال بيئة افتراضية مطابقة للبيئة الفعليه , يمكن للتوأم الرقمي الكشف عن نقاط الضعف والثغرات بالاضافة الى اختبار فعالية الضوابط قبل تطبيقها على بيئة الانتاج.

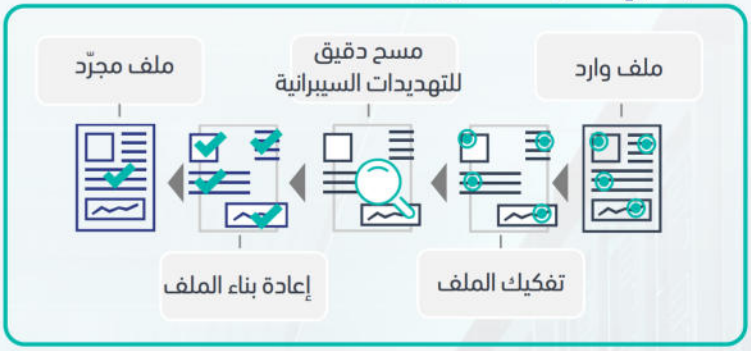
إنّ التوأم الرقمي يكشف عن عدم التطابق ما بين البيئة الفعلية والاعدادات الأساسية وذلك نتيجة لتعديل على الاعدادات أو نتيجة للتعرض لهجوم سيبراني.

تسليط الضوء على الابتكارات السيبرانية

حلول مبتكرة لتحديات الأمن السيبراني المستفيدة من برامج مسرّعات الأعمال

مع حلول العام 2021 يتوقّع أن تنمو نسبة الإنفاق على ابتكارات الأمن السيبراني لتبلغ **ترليون دولار أمريكي** بشكل تراكمي خلال السنوات الخمس الأخيرة الماضية.[17] تؤمّن برامج مسرّعات الأعمال منصّة كبرى لدعم الشركات الناشئة في مجال الأمن السيبراني، إضافة إلى أنّها تساهم في دعوة قادة هذا القطاع إلى استكشاف أبرز تحديات الأمن السيبراني.

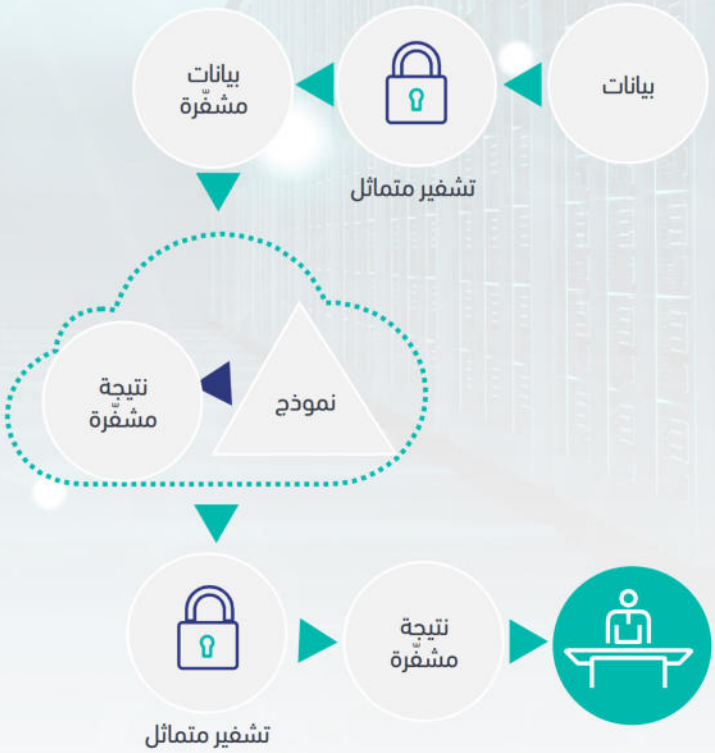
تفكيك وإعادة بناء المحتوى



عوضًا عن الاعتماد على الأدوات التقليدية للكشف عن التهديدات السيبرانية، تقدّم بعض الشركات الناشئة حلولًا في مجال الأمن السيبراني قائمة على تقنية تجريد المحتوى وإعادة البناء (CDR). تدقق هذه التقنية في مختلف مكونات الملفات الواردة عبر تفكيكها وإزالة المكونات التي لا تمتثل لسياسات الأمن السيبراني الخاصّة بالمؤسسة.[18]

تركّز شركات ناشئة أخرى على التشفير المتماثل[19] الذي يمكّن المؤسسات من تبادل البيانات لتحليل الأعمال ممّا يؤدّي إلى نتائج مشفّرة من دون تقديم مفتاح تشفير البيانات. وقد أدّت إمكانية الاستعانة بعملية إحصاء البيانات بشكل آمن إلى تسريع عملية وضع معايير لهذه التقنية.

التشفير المتماثل



يمكن للتشفير المتماثل أن يعزز حماية البيانات عبر معالجة وتحليل البيانات المشفّرة.[20]

تبرز الاستفادة من معالجة البيانات وهي مشفره دون الحاجه لفك التشفير في عدة حالات , أبرزها :

- الحاجة الى الاستعانة بالخدمات السحابية مع المحافظة على معالجة البيانات بطريقة آمنة؛
- يساهم التشفير المتماثل في حماية البيانات عند استخدام الحوسبة المتعدّدة الأطراف.

المراجع

[1] كلفة التبليغ عن خرق البيانات، IBM، 2020، https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[2] كلفة التبليغ عن خرق البيانات، IBM، 2020، https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[3] التحمّل المنزلي لتأثير كوفيد-19 على أمن الأعمال، Malware Bytes، 2020، https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals/

[4] كلفة التبليغ عن خرق البيانات، IBM، 2020، https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[5] موقع Mitre الإلكتروني https://shield.mitre.org/

[6] 2020 تقرير تقدّم الثقة المعدومة، Plus Secure، 2020، https://www.pulsesecure.net/resource/2020zero-trust-report/

[7] المبادئ العامة للأمن السيبراني للتصميم الآمن، الهيئة الوطنية للأمن السيبراني، https://nca.gov.sa/files/sbd_en.pdf (SBD – 1: 2020),

[8] دليل نشر الثقة المعدومة الخاص بمايكروسوفت بتطبيقاتكم، مايكروسوفت، 2020، https://www.microsoft.com/security/blog/2020/08/27/zero-trust-deployment-guide-microsoft-applications/

[9] الاستراتيجية الوطنية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني، 2020، https://nca.gov.sa/en/pages/strategic.html

https://twitter.com/nca_ksa/status/1306226229943640064?s=24

[10] تحديث عن حادثنا الأمني، مدونة تويتر، 2020، https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

[11] موظف Tesla يتخلى عن مليون دولار أميركي ويعمل مع مكتب التحقيقات الفدرالي لإحباط هجوم سيبراني، Tesla، 2020، https://www.teslarati.com/tesla-employee-fbi-thwarts-russian-cybersecurity-attack/

[12] دليل للطلاب حول جوانب الأمن السيبراني في التعليم عن بُعد، الهيئة الوطنية للأمن السيبراني، 2020، https://cert.gov.sa/ar/awareness/online_learning_guide/

[13] ورقة غش: ما هو التوأم الرقمي؟ IBM، يناير 2020، https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/

[14] التوأم الرقمي، مسرد غارتنر، https://www.gartner.com/en/information-technology/glossary/digital-twin;

التوأم الرقمي يسد الفجوة بين المادي والرقمي، ديلويت، 2020، https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/digital-twin-applications-bridging-the-physical-and-digital.html

[15] توقّع اعتماد التوأم الرقمي لهذه التجسيدات المتنوعة ينتشر بين الصناعات، ديلويت، 2020، https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/understanding-digital-twin-technology.html;

التوأم الرقمي: فهم ما هو ولماذا ضرورة حمايته، Security Infowatch، 2020، https://www.securityinfowatch.com/security-executives/article/21082742/digital-twins-understanding-what-they-are-and-why-they-need-to-be-protected

[16] إيكهارت الرقمي، م. وإيكهارت، أ.، نحو بيئات افتراضية أمنية حذرة للتوأم الرقمي، https://www.sqi.at/resources/Towards_Security-Aware_Virtual_Environments_for_Digital_Twins.pdf

[17] https://cybersecurityventures.com/cybersecurity-market-report/

[18] https://medium.com/@adam_20838/top-content-disarm-and-reconstruction-cdr-solutions-companies-2020-9aade28f6e15

[19] توحيد التشفير المتماثل، HomomorphicEncryption.org، 2020، https://homomorphicencryption.org/

[20] الفصل العاشر - إدماج إنترنت الأشياء مع سلسلة الكتل والتشفير المتماثل: المسائل الصعبة والفرص، RakeshShresthaShihoKim، 2019، https://www.sciencedirect.com/science/article/pii/S0065245819300269

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 للامن 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