الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority

النشرة الربعية للأمن السيبراني

الربع الرابع – 2020

تصنيف الوثيقة: متاح
إشارة المشاركة: أبيض


698.11
226.34

جدول المحتويات

ملخص النشرة

الربع الرابع من العام 2020 (أكتوبر – ديسمبر)

اختلف العام2020 عن الأعوام السابقة، فقد ألقت جائحة كوفيد-19 بظلالها على العالم بأسره وأثّرت على كلّ جانب من جوانب المجتمع، ولم يستثني تأثير الجائحة مجال الأمن السيبراني. تتطرّق هذه النشرة الربعية إلى آثار جائحة كوفيد19 على الأمن السيبراني ومدى جاهزية وصمود الحكومات والقطاع الخاص. لقد شهد العام2020 عددًا كبيرًا من الحوادث السيبرانية بما في ذلك الهجمات التي طالت البنى التحتية الخاصة بقطاع الصحة إضافة إلى الحادثة التي تعرّضت لها شركة سولار ويندز (SolarWinds) في نهاية العام، ممّا أظهر بوضوح الآثار بعيدة المدى لمخاطر اختراقات سلسة إمدادات البرمجيات .

لا شك أن مشهد التهديدات السيبرانية سيتطور في عام2021 غير أنّه من الواضح أنّ ملخّص السنوات السابقة لا يعرض سوى نظرة بسيطة حول مخاطر العام المقبل، إذ يختلف كلّ عام عن الآخر. في هذا السياق، من الضروري أن يتّسم العام المقبل بسمتين قيّمتين: الجاهزية والصمود السيبراني.

بيانات سيبرانية: سايبر بايت

إحصاءات وتوقعات رئيسيّة من الربع الرابع

76.5
مليار ريال سعودي
مع حلول العام 2025

يتوقّع أن يزداد حجم سوق التأمين السيبراني العالمي بثلاثة أضعاف مع حلول العام 2025[1]
العامل الأساسي هو استمرار زيادة عدد الهجمات والحوادث السيبرانية.

x2

يتوقّع أن يتضاعف حجم سوق الأمن السيبراني لتأمين المركبات على الصعيد العالمي مع حلول العام 2025[2]
من الضروري حماية مشاركة المعلومات بين المركبات ومحيطها.

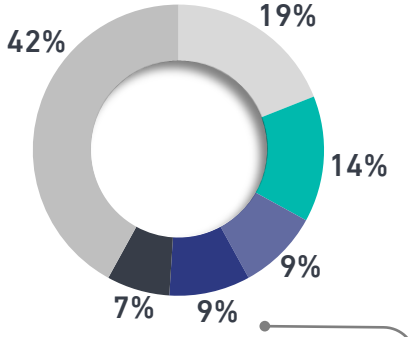
80%

من الشركات أعادت هيكلة البنى التحتية السيبرانية الخاصة بها بسبب جائحة كوفيد-19[3]
قادت كبرى الشركات هذا التغيير.

+25.7%

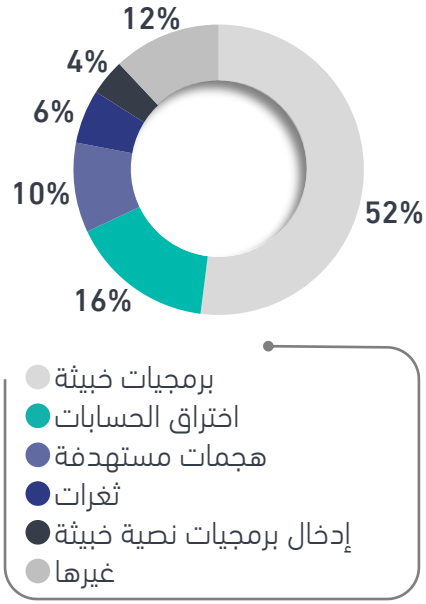
يتوقّع حدوث نمو كبير في استخدام الذكاء الاصطناعي في قطاع الأمن السيبراني خلال السنوات العشر القادمة[4]
من المتوقّع أن يشهد العالم نموًا بنسبة 25.7% لمعدّل النمو السنوي خلال الفترة ما بين 2020 و2030.

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



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

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



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

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

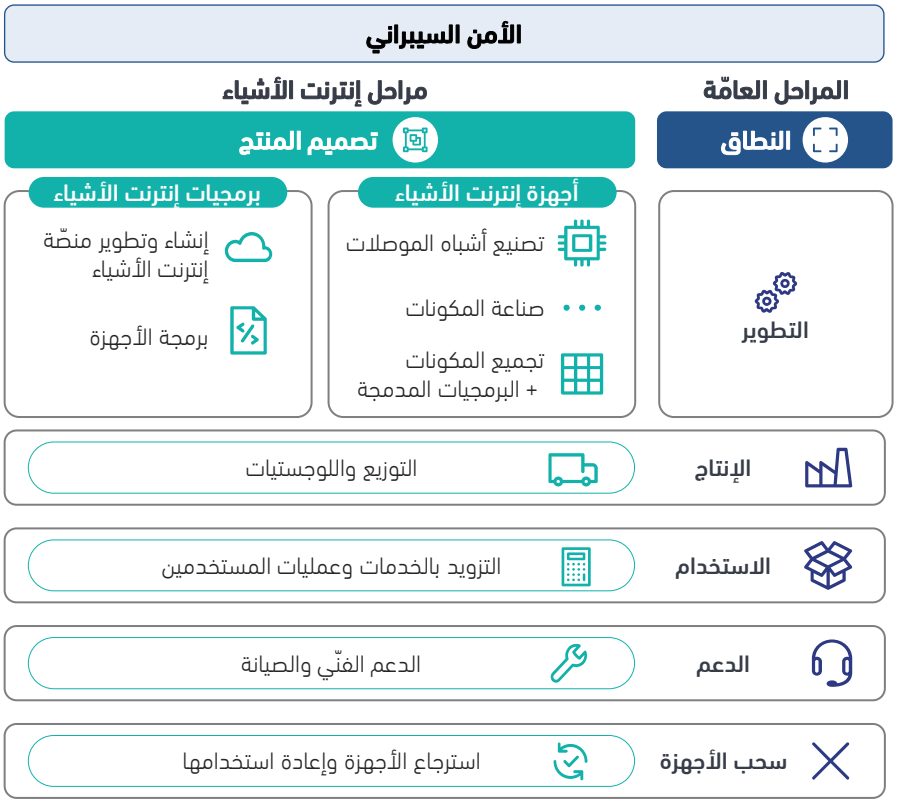
الأمن السيبراني من منظور عالمي

عناوين الأمن السيبراني الرئيسيّة من مختلف أنحاء العالم

حماية سلسلة إمدادات إنترنت الأشياء

كلّف القانون الأميركي لتعزيز الأمن السيبراني لإنترنت الأشياء (الموقّع ليصبح قانوناً في ديسمبر 2020) المعهد الوطني للمعايير والتقنية (NIST) لوضع الحدّ الأدنى من المعايير والإرشادات في مجال الأمن السيبراني لأجهزة إنترنت الأشياء.[5] وعلى الرغم من أنّ هذا القانون ينطبق فقط على الأجهزة التي تبتاعها الحكومة الأميركية، إلّا أنّه قد يحفّز الموردّين على تعزيز الأمن السيبراني في سلسلة إمدادات إنترنت الأشياء.[6]

أصدرت وكالة الاتحاد الأوروبي لأمن الشبكات والمعلومات (ENISA) إرشادات حول حماية سلسلة إمدادات إنترنت الأشياء (أنظر النموذج المرجعي إلى اليسار) ممّا قد يشكّل خطّة تنفيذية لتطوير معايير إنترنت الأشياء في العام 2021.[7]



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

ضوابط الأمن السيبراني للحوسبة السحابية[8]

تحدّد متطلبات الأمن السيبراني للحوسبة السحابية من منظور مزوّدي الخدمات السحابية والمستفيدين منها.

كوادر الأمن السيبراني يواجهون جائحة كوفيد-19

على الرغم من ندرة كوادر الأمن السيبراني على الصعيد العالمي، إلّا أنّ الكوادر العاملة حاليّاً في عدد من الجهات تمكّنت من مواجهة التحديات التي أسفرت عنها جائحة كوفيد-19.[9]

هذا وتدرك الهيئة الوطنية للأمن السيبراني الدور الرئيسي الذي تقوم به تلك الكوادر من أجل التصدي للهجمات السيبرانية، لذا اعتمدت الهيئة تدابير عديدة من أجل تجهيز الخبراء السعوديون بالمهارات السيبرانية لتأهيلهم لسوق العمل.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

سايبر برو+ (CyberPro+) بالتعاون مع صندوق تنمية الموارد البشرية (HRDF) والشركة السعودية لتقنية المعلومات (SITE) [10]

يستهدف التدريب في مجال الأمن السيبراني 500 خريج وخريجة لمدّة 6 أشهر

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الإطار السعودي للتعليم العالي في الأمن السيبراني (SCyber-Edu) [11]

دليل مرجعي لتطوير برامج التعليم العالي في الأمن السيبراني

نتائج الدراسة التي أطلقتها (ISC)[2] حول القوى العاملة في مجال الأمن السيبراني[12]

92%
من كوادر الأمن السيبراني على استعداد للعمل عن بُعد.

54%
قلقون بشأن استهلاك الكوادر خلال العام 2021.

3.1 مليون
حاجة سوق العمل العالمي لكوادر الأمن السيبراني.

+89%
يؤمنون بأنّه يجب تعزيز ودعم وزيادة الكوادر العاملة في الأمن السيبراني على الصعيد العالمي.

56% جهة مشمولة بالدراسة الاستقصائيّة
تعتبر أنّ النقص في كوادر الأمن السيبراني يشكّل خطراً.

الأمن السيبراني من منظور وطني

النموذج السعودي لتعزيز صمود الأمن السيبراني خلال سنة رئاسة مجموعة العشرين

تعزيز صمود الأمن السيبراني خلال سنة رئاسة مجموعة العشرين

تولّت المملكة العربية السعودية رئاسة مجموعة العشرين لعام 2020م. بالتزامن مع جائحة كوفيد-19، فقد تمّ تنظيم معظم الفعاليات خلال سنة رئاسة المملكة لمجموعة العشرين، عبر الاتصال المرئي ممّا أدّى إلى تغير في أنماط التهديدات السيبرانية، ومواجهة تحديات سيبرانية جديدة؛ مما استوجب اتخاذ عدد من التدابير الإضافية لتعزيز الأمن السيبراني.

عملت الهيئة الوطنية للأمن السيبراني على تعزيز الصمود السيبراني خلال سنة رئاسة مجموعة العشرين، بما في ذلك قمّة القادة الافتراضية. ويرتكز تصميم النموذج السعودي على نهج ذا مستويين مع القدرة على التكيّف، والتحسين المستمرّ.

تعزيز الأمن السيبراني في قمة العشرين بالأرقام

حوكمة البرنامج

400+
مختصّ ومختصّة في مجال الأمن السيبراني شاركوا في البرنامج

350+
جهة تم رفع جاهزيتها السيبرانية

450+
تقرير تمّ إصداره

400+
يوم من الإعداد والتنفيذ

التقييمات السيبرانية

120+
تقييم سيبراني تم إجراؤها بما في ذلك:
1. تقييم المخاطر
2. اختبارات الاختراق وتقييم الثغرات
3. تقييم إعدادات ومعمارية الأمن السيبراني
4. تقييم الاختراق السيبراني
4. تقييم استمرارية الأعمال
6. تقييم مدى الالتزام
7. تقييم صلاحيات الوصول للمستخدمين

100+
جهة تمّ تقييمها

العمليات السيبرانية

600+
تنبيه سيبراني تمّ إرساله للجهات ذات العلاقة

10K+
ساعة متواصلة من المراقبة الأمنية المستمرّة

الوعي السيبراني والتمارين السيبرانية

100
جهة شاركت في التمارين السيبرانية

9
تمارين سيبرانية تمّ إجراؤها للجهات ذات العلاقة

60+
ورشة عمل تمّ تنظيمها للجهات ذات العلاقة بمشاركة كبار مسؤولي أمن المعلومات

أحداث سيبرانية

SolarWinds[13]

solarwinds

الموقع: الولايات المتحدة

القطاع: تقنية المعلومات

تاريخ الاكتشاف:
13 ديسمبر 2020

نوع الهجوم:
اختراق تحديث إحدى البرمجيات

الوصف

وقعت شركة SolarWinds المزوّدة للبرمجيات والتي يقع مقرّها في الولايات المتحدة ضحية لهجوم سيبراني حصل في ربيع العام 2020 حيث اخترق المهاجمون شبكة الشركة وأدخلوا برمجيات خبيثة في تحديثات تطبيق Orion الذي يُعنى بإدارة ورصد مخزون معدات تقنية المعلومات. تأثرت التحديثات التي تم إطلاقها في الفترة بين مارس ويونيو 2020 بهذا الاختراق ويرجح أنّه تمّ تثبيتها من قبل 18000 عميل لدى SolarWinds على الأقل، بما في ذلك الجهات الحكومية والتقنية والجهات المختصّة بالاتصالات في كلّ أنحاء أميركا الشمالية وأوروبا وآسيا والشرق الأوسط.

التأثير

يُعتبر التجسّس الدافع الأساسي للهجمات السيبرانية خاصة على الحكومة الأميركية.[14] وقد صدر بيان مشترك عن الوكالات الأميركية الأربعة المسؤولة عن الاستخبارات والأمن السيبراني مفاده أنّ الحكومة تمكّنت حتى الآن من تحديد عدد لا يزيد عن 10 وكالات فدرالية تعرّضت أنظمتها الداخلية إلى عمليات اختراق.

الدروس المستفادة

يمكن للبرمجيات التي تُستخدم بشكل واسع أن تشكّل نقطة الدخول الوحيدة إلى آلاف الجهات، ممّا يدعو إلى ضرورة الانتباه بشكل دائم وسليم. ويبرز هذا الحادث أهمّيّة الأمن السيبراني في سلسلة الإمدادات في مجال تقنية المعلومات والاتصالات.

FireEye[15]

FIREEYE

الموقع: الولايات المتحدة

القطاع: الأمن السيبراني

تاريخ الكشف:
8 ديسمبر 2020

نوع الهجوم:
اختراق محدّث إحدى البرمجيات
(أنظر أعلاه)

الوصف

تمكّن المهاجمون من اختراق تحديث إحدى برمجيات SolarWinds (المشار إليه أعلاه) واستخدامه للوصول إلى شبكات شركة FireEye[16] المختصّة في مجال الأمن السيبراني والتي يقع مقرّها في الولايات المتحدة. وقد استخدم المهاجمون هذا الوصول بهدف الحصول على أدوات "الفريق الأحمر" في شركة FireEye، وهي عبارة عن برامج تعمل على تطوير أساليب الاختراق للبحث عن الثغرات الموجودة بشبكات تقنية المعلومات. وعلى الرغم من أنّ أدوات "الفريق الأحمر" هذه لم تتضمّن هجمات (zero-day) وهي الهجمات السيبرانية التي استغلت ثغرات غير معروفة مسبقاً، حيث لا يزال المهاجمون قادرين على استخدامها لإخفاء أدلّة حدوث الهجمات السيبرانية والعبث بالأدلة التي تفيد التحقيقات الرقمية.

التأثير

على الرغم من أنّ المهاجمين تمكّنوا من الوصول إلى النظام الداخلي الخاص بشركة FireEye، غير أنّه ليس هنالك أي دليل على أنّ المهاجمين قد تمكّنوا من الوصول إلى المعلومات الخاصّة بالعملاء. إضافة إلى ذلك، لا يوجد ما يُثبت استخدام المهاجمين لأدوات الفريق الأحمر التي تمت سرقتها. ولكن، لا يزال المهاجمون قادرين على استخدام أدوات كهذه لتعزيز قدراتهم الهجوميّة.

الدروس المستفادة

يبرز هذا الهجوم القدرات المتقدّمة للمهاجمين خاصة عندما يتوفر لديهم عاملي الوقت والموارد الكافية لتطوير أساليب لاستخدامها في الهجمات السيبرانية.

ومضة سيبرانية

وجود تحديات كثيرة في إدارة المخاطر السيبرانية الناجمة عن الأطراف الخارجية

وفقًا لتقرير بونمون (Ponemon)، وخلال العامين الماضيين، واجهت ما نسبته 82% من الجهات التي شملتها الدراسة اختراقًا للبيانات من قبل أطراف خارجية، حيث بلغ متوسّط التكاليف 7.5 مليون دولار أميركي للحدّ من الآثار الناجمة عن تلك الاختراقات[17]

تشمل الثغرات 5 **مجالات رئيسيّة**: الأجهزة المحمولة (بالإضافة إلى أجهزة سطح المكتب) وحماية الخوادم وحماية الأجهزة الافتراضية (سواء كانت متواجدة داخل الجهات أو على الحوسبة السحابية) وحماية البيانات في حال تخزينها أو في حال نقلها. وتجدر الإشارة إلى أنّ معظم المخاطر ذات الصلة هي عبارة عن مخاطر متعلّقة بهجمات برمجيات الفدية وتشويه المواقع الإلكترونية وتغيير البيانات والاستخدام الخبيث لمعلومات الهوية الشخصية.[18]

تتضمّن الضوابط الأساسية للأمن السيبراني الخاصّة بالهيئة الوطنية للأمن السيبراني ضرورة حماية الجهات المحلية من المخاطر التي قد تنجم عن الأطراف الخارجية (ECC – 1: 2018، الضابط رقم 4-1)[19]

تطوير اجراءات للكشف عن الحوادث السيبرانية وتقييمها: الركائز الرئيسيّة[20]

باتت عملية الكشف عن الحوادث السيبرانية عنصرًا رئيسيًا في مواجهة المخاطر، وإنّ العاملين الأساسيّين لتحديد الحوادث هما مؤشرات الاختراق (الخارجية أو الداخلية ضمن الجهة) والتحليل الدقيق الذي يجريه الخبراء في المجال.

بهدف تطوير إجراءات فعالة للكشف عن الحوادث السيبرانية وتقييمها، على الجهات أن تعتمد نهجًا دقيقًا وشاملًا يرتكز على الركائز الخمسة الرئيسيّة التالية:

تتضمّن الضوابط الأساسية للأمن السيبراني الخاصّة بالهيئة الوطنية للأمن السيبراني ضرورة إبلاغ الهيئة الوطنية للأمن السيبراني عن حوادث الأمن السيبراني ومشاركة الإخطارات بالحوادث والمعلومات الاستباقية ومؤشرات الاختراق والتقارير (ECC – 1: 2018، الضابط رقم 3-13-2).[21]

التطلّع لتوجّهات جديدة

الاستعداد من أجل المستقبل: كيفيّة مواجهة المخاطر السيبرانية المستجدّة

دراسة جديدة حول الآثار الناجمة عن جائحة كوفيد-19 على مستوى الأمن السيبراني

انتشرت جائحة كوفيد-19 في كلّ أنحاء العالم، وفي حين أصبحت الآثار أكثر وضوحًا، بات من الواضح أيضًا أنّه من الضروري تعزيز الأمن السيبراني لمواجهة آثار هذه الجائحة ووضع أسس متينة للنمو الاقتصادي والقيام باستثمارات تستمرّ حتى ما بعد هذه الأزمة.

توصّلت دراسة الهيئة الوطنية للأمن السيبراني إلى ما يلي:

1. مع زيادة نسبة العمل عن بُعد، شهد سطح الهجمات السيبرانية المتوفّر لمنفّذي التهديدات مجالات جديدة.
2. إن الخبرات المحدودة في مجال الأمن السيبراني سيكون لها آثار على المدى القصير في توظيف الكوادر المؤهلة في المجال وعلى المدى البعيد في تنمية قدراتهم.
3. إنّ المستويات المرتفعة للضغوطات وعدم اليقين تقدّم فرصًا جديدة لهجمات التصيّد وبرمجيات الفدية.

كيفيّة مواجهة المخاطر السيبرانية الناجمة عن التقنيات الحديثة

تنطوي التغيّرات في المشهد التقني على مخاطر سيبرانيّة كبرى. فقد تطرّق المنتدى الاقتصادي العالمي في تقريره الأخير إلى التدابير الضرورية لمواجهة المخاطر المنهجيّة الكامنة في التقنيات الحديثة. وقد ركّز التقرير بشكل خاص على الاتصال السائد (ubiquitous connectivity) والذكاء الاصطناعي والحوسبة الكمية والهوية الرقمية.[22]

التقنيات الحديثة	الاتصال السائد	الذكاء الاصطناعي	الحوسبة الكمية	الهوية الرقمية
التدابير السيبرانية	تحديد وتصنيف **البنية التحتية الحساسة** لتشغيل الخدمات المتعدّدة	الاستثمار في **التقنيات التي تعمل بالذكاء الاصطناعي** لتوقّع التهديدات السيبرانية واستراتيجيات الهجوم	تطوير **القدرة الكمية السيادية** من خلال الشراكات بين القطاعين العام والخاص	وضع **إطار عمل مشترك للحوكمة** من أجل إدارة الهوية الرقمية

من الضروري أن يتمّ وضع نهج مشترك لمواجهة المخاطر السيبرانية الناجمة عن التقنيات الحديثة بشكل فعال. تؤدّي كلّ مجموعة من الجهات ذات الصلة دورًا مهمًا في مواجهة المخاطر السيبرانية في المستقبل.

دور الجهات ذات الصلة في إدارة المخاطر السيبرانية المستجدّة

الأمن السيبراني والقطاع التقني
تحديد مخاطر الأمن السيبراني الحديثة ووضع الضوابط المشتركة.

القطاع الخاص والحكومي
تعزيز معايير الأمن السيبراني لتعزيز الثقة والأمن السيبراني على مستوى التقنيات الحديثة.

المجتمع الدولي
بناء قدرة سيبرانية للحدّ من التهديدات السيبرانية وتمكين الاعتماد الآمن للتقنيات الحديثة عالميًا.

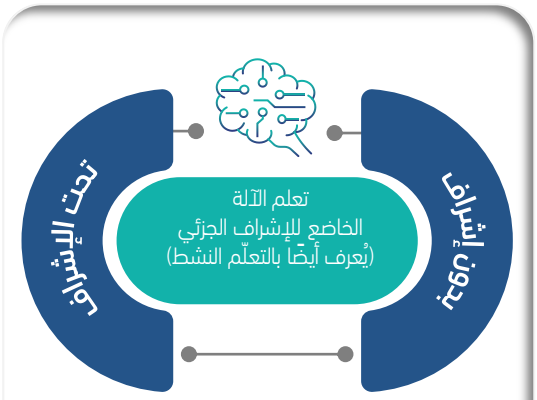
تسليط الضوء على الابتكارات السيبرانية

حلول مبتكرة لتحديات الأمن السيبراني المستفيدة من برامج مسرّعات الأعمال

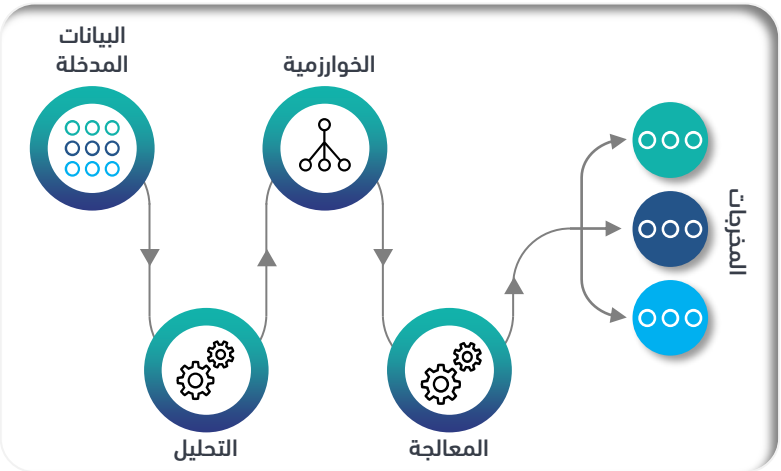
تعلم الآلة بدون إشراف: ابتكار بين القطاعات

إنّ تعلم الآلة يشمل التعلّم تحت الإشراف والتعلّم بدون إشراف. ويعتمد التعلّم تحت الإشراف على عملية وصف لجمع المعلومات بإشراف الإنسان، في حين يعمل التعلّم بدون إشراف على التقاط استدلالات من مجموعات البيانات من دون أي وصف أو تدخّل بشري.

إنّ تعلم الآلة بدون إشراف بالغ الأهمّيّة في مجال الأمن السيبراني إذ لا يبحث عن أي وصف معيّن بل يبلّغ عن خطورة أي نمط مشتبه به (وبالتالي يشكّل تهديدًا محتملًا). ثمّة عدد متزايد من الشركات الناشئة التي تستثمر بشكل كبير في تعلم الآلة بدون إشراف للكشف عن طرق جديدة لتنفيذ الهجمات السيبرانية.[23]



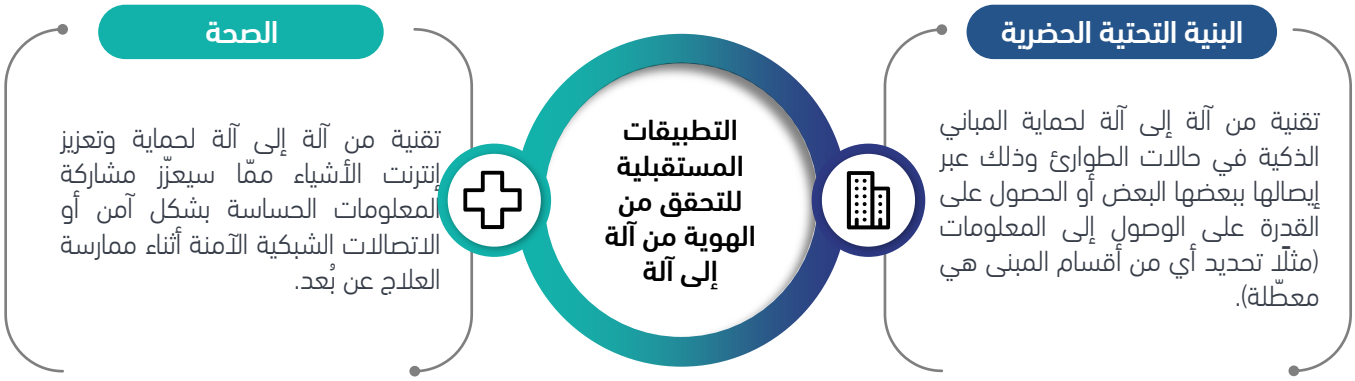
إنّ تعلم الآلة الخاضع للإشراف الجزئي يقدّم توقعات حول كيفيّة عمل الشبكة، فيبحث عن أنماط شاذة (تمامًا مثل تعلم الآلة بدون إشراف)، وبمجرد اكتشاف تلك الأنماط المشتبه بها، يتمّ الإشارة إليها على أنها تهديدات سيبرانية محتملة (كما في تعلم الآلة تحت الإشراف).[24]



التحقق من الهويات من آلة إلى آلة: آفاق جديدة لإنترنت الأشياء واتصالات الشبكة الآمنة

أصبحت تقنيات إنترنت الأشياء وتقنيات الآلة إلى الآلة (Machine-to-Machine (M2M)) سائدة في عدد كبير من القطاعات والذي يستدعي تعزيز الكفاءة وتطوير بدائل للتقنيات السيبرانية التقليدية للتحقق من الهوية (الأمر الذي غالبًا ما يتطلّب تفاعلًا بشريًا).[25]

لهذا السبب، تستثمر الشركات والحكومات بشكل كبير في التحقق من الهويات باستخدام تقنيات الآلة إلى الآلة، ويشمل ذلك شبكات أجهزة الاستشعار الذكية والموجهات وخوادم التحقق من الهويات. بالتالي، تتواصل هذه المكونات مع بعضها البعض وتكون مسؤولة عن إجراء عملية التحقق من الهوية.[26]



المراجع

[1] https://www.prnewswire.com/news-releases/global-cyber-insurance-solutions-analytics--cybersecurity-and-services-market-2020-2025-key-players-are-allianz-aig-chubb-aon-zurich-axa-and-berkshire-hathaway-301166366.html

[2] https://www.prnewswire.com/news-releases/automotive-cybersecurity-market-by-form-security-application-vehicle-type-ev-type-and-region---global-forecast-to-2025-301167143.html

[3] https://www.hackread.com/companies-re-structured-cybersecurity-infrastructure-2020/?web_view=true

[4] https://www.researchandmarkets.com/reports/5184623/ai-in-cyber-security-market-research-report-by?

[5] https://www.govtrack.us/congress/bills/116/hr1668

[6] https://www.helpnetsecurity.com/2020/10/29/iot-cybersecurity-improvement-act-of-2020/?web_view=true

[7] https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[8] https://nca.gov.sa/en/pages/ccc.html

[9] https://www.isc2.org/Research/Workforce-Study

[10] https://nca.gov.sa/en/pages/news/news44.html

[11] https://nca.gov.sa/en/pages/news/news42.html

[12] https://www.isc2.org/Research/Workforce-Study

[13] https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

[14] https://www.reuters.com/article/global-cyber-solarwinds/hackers-at-center-of-sprawling-spy-campaign-turned-solarwinds-dominance-against-it-idUSKBN28P2N8

[15] https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

[16] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[17] https://www.cybergrx.com/resources/research-and-insights/ebooks-and-reports/the-cost-of-third-party-cybersecurity-risk-management

[18] https://www.helpnetsecurity.com/2020/11/25/combating-third-party-cyber-risk/?web_view=true

[19] https://nca.gov.sa/files/ecc-en.pdf

[20] https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiic-incident-identification-and-assessment.aspx

[21] https://nca.gov.sa/files/ecc-en.pdf

[22] https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

[23] https://www.ibm.com/cloud/learn/unsupervised-learning

[24] https://www.technative.io/why-unsupervised-machine-learning-is-the-future-of-cybersecurity/

[25] https://www.researchgate.net/publication/319024120_A_Lightweight_Authentication_Mechanism_for_M2M

[26] https://eprint.iacr.org/2018/891.pdf

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 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، و لا تتحمل الهيئة الوطنية للأمن السيبراني أي مسؤولية - تحت أي ظرف من الظروف - تجاه أي طرف نتيجة لأي قرار أو إجراء تم اتخاذه أو سيتم اتخاذه 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