منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

تقريـــر

الأمن السيبراني
في المملكة العربية السعودية

سياسة الاستخدام

إن المعلومات الواردة في هذا التقرير جُمِعَت ونُسِّقت بجهود موظفي مركز ذكاء التابع لـ الهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات نرجو التواصل عبر البريد الإلكتروني support@thakaa.sa

الفكرة العامة للتقنية وتاريخها

يعتمد الاقتصاد الحديث بشكل متزايد على الحواسيب، والهواتف المحمولة، وشبكات الإنترنت، والأجهزة الذكية، وتقنيات إنترنت الأشياء، والذكاء الاصطناعي وغيرها من التقنيات التي اكتسحت عالمنا ضمن موجة التحوّل الرقمي بشكلٍ عام؛ وهو ما أعطى الأمن السيبراني أهمية مفصلية لضمان حماية العمليات والمعلومات الحساسة التي تديرها هذه التقنيات، ممّا يجعل الأمن السيبراني أحد أبرز توجُّهات هذا العصر، كما يتّصل الأمن السيبراني بالجوانب الأمنية، والسياسية، والاجتماعية والاقتصادية أيضًا.

لقد ظلّت الحواسيب في مأمن لفترةٍ طويلةٍ بعد اختراعها، وذلك لمحدودية عدد الناس الذين يستطيعون الوصول إليها والذين يجيدون تشغيلها، والأهم من ذلك لعدم ارتباطها بشبكات الاتصال اللاسلكية.

ثم بدأ التحدّي مع ظهور الاختراقات الخبيثة التي رافقت انتشار استخدام الهواتف المحمولة، وكان معظمها في البداية يهدف لإجراء المكالمات المجانية، وتتابعت التطوّرات في المجال سريعًا مع ظهور الإنترنت.

الخط الزمني لتطوّر الأمن السيبراني

1970s

ولادة أمن الحواسيب

يُمكن القول أن الاهتمام بأمن الحواسيب بدأ مع مشروع "أربانت ARANET" (شبكة وكالة مشاريع الأبحاث المتطورة)، إذ أسس المشروع أحد أوائل شبكات الإنترنت البدائية التي تربط عددًا من الجامعات والمؤسسات البحثيّة في الولايات المتحدة، ليقوم حينها الباحث بوب توماس بكتابة برنامج "كريبر" القادر على التحرك عبر شبكة أربانت، ثم أنشأ راي توموليسون برنامج ريبير لمطاردته وحذفه، ليكون أول مثال على برنامج ذاتي النسخ لمكافحة الفيروسات.

1980s

ولادة الأمن السيبراني

بدأ في هذا العقد انتشار البرمجيات التجارية لمكافحة الفيروسات، وهي أدوات فحصٍ بسيطة تُجري عمليات بحث منهجية لاكتشاف تسلسل رموز الفيروسات، ولكن مع ازدياد عدد الفيروسات إلى المئات، سرعان ما أصبحت هذه البرمجيات غير فعالة، وغير قادرة على مجاراة تغيّر الفيروسات لصعوبة تحديثها دون توفّر شبكة اتصال عالمية واسعة الانتشار.

1990s

أصبح العالم متصلًا بالإنترنت

اتصل العالم بالإنترنت، وحدثت ثورة في أعداد الفيروسات والبرامج الضارّة التي تستخدم تقنيات وأساليب جديدة ومبتكرة، مما وضع سوق برامج مكافحة الفيروسات أمام تحدّيات كبيرة، حتى طوّر أحد باحثي ناسا أول جدار حماية حاسوبي. مع وصول المزيد من أجهزة وبرامج فحص الفيروسات إلى السوق، كان قراصنة الإنترنت يُطوّرون من قدراتهم أيضًا، وفي عام 1992م ظهر أول برنامج مضاد للفيروسات، وهو (Dr.WEB Anti-virus).

2000s

استمرار تنوّع التهديدات وتوسّعها

مع توسّع استخدام الإنترنت وتواجده في كل مكان وفي يد جميع أفراد المجتمع، أصبح لدى قراصنة الإنترنت المزيد من الأجهزة ونقاط الضعف والثغرات التي يمكنهم استغلالها، بل وتجاوز ذلك إلى تهديد أمن الدول، وصاحب ذلك تظافر الجهود لصدّ الجرائم الإلكترونية، ومن أهم هذه الجهود:

- توفير أول محرك مفتوح المصدر لمكافحة الفيروسات OpenAntivirus.
- إطلاق أول محرك مفتوح المصدر لمكافحة الفيروسات يُسوّق تجاريًّا ClamAV.
- إطلاق برنامج مجاني لمكافحة الفيروسات متكامل الميزات Avast.
- ابتكار الأمن السيبراني المدمج في نظام التشغيل.

2010s

الجيل الماضي

ازدادت حدّة الهجمات الإلكترونية حتى هدّدت الأمن القومي للدول، ومن أشد هذه التهديدات:

- هاجم الفيروس شمعون عددًا من القطاعات الحكومية في المملكة العربية السعودية ودمّر 30 ألف حاسوب شخصي.
- استهدفت هجمة سيبرانية مصنع بتروكيماويات في المملكة العربية السعودية.
- تسريب معلومات سرية من وكالة الأمن القومي في الولايات المتحدة.
- أجبرت هجمات حجب الخدمة سوق الأسهم النيوزيلندية على الإغلاق المؤقت.

نتج عن ذلك الجيل التالي من الأمن السيبراني الذي يستخدم أساليب مختلفة للكشف عن الاختراقات، مثل: تحليل سلوك الشبكة، مصادقة متعددة العوامل، النسخ الاختياطي، وجدران حماية تطبيقات الويب.

2020s

التحوّل الرقمي

ساعدت الإجراءات المصاحبة للجائحة العالمية كوفيد-19 إلى تسريع التحوّل الرقمي في جميع القطاعات، صاحبه ارتفاعٌ كبيرٌ في عدد الهجمات السيبرانية في اليوم الواحد، حيث تشير الإحصاءات إلى أن هناك هجوم سيبراني جديد يبدأ كل 40 ثانية، وأنَّ المُخترقين يهاجمون أكثر من 30 ألف موقع/ جهاز يوميًّا.

Avast, Cyber Magazine, IT Chronicles

أنواع الأمن السيبراني

الأمن السيبراني للبنية التحتية

يتضمن تأمين المؤسسات الحيوية ومقدّمي الخدمات العامة.

أمن السحابة

يتضمن تأمين البيانات، التطبيقات، والبنية التحتية في السحابة.

أمن التطبيقات

يتضمن معالجة نقاط الضعف المصاحبة لعمليات التطوير غير الآمنة في تصميم البرامج وترميزها ونشرها.

أمن الشبكات

يتضمن تأمين الخوادم، المضيفين، جدران الحماية، نقاط الوصول اللاسلكية، وبروتوكولات الشبكة.

أمن إنترنت الأشياء

يتضمن تأمين الأجهزة الذكية والشبكات المتصلة بإنترنت الأشياء.

الأمن التشغيلي

يتضمّن توعية الموظفين بأفضل الممارسات للحفاظ على أمان المعلومات الشخصية والتجارية.

Triadanet, Mindcore

أهمية الأمن السيبراني لروّاد الأعمال

1. حماية أفضل لبيانات وعمليات النشاط التجاري.
2. حماية السمعة التجارية وكسب ثقة العملاء.
3. يساعد في تسيير العمل عن بعد وتأمين تبادل البيانات بين الموظفين.
4. تحسين الموقف السيبراني وسهولة تتبُّع جميع الأنظمة بسهولة.
5. تحسين إدارة البيانات بما يدعم الخصوصية ويرفع الكفاءة التشغيلية.
6. التحكم المنطقي في الوصول إلى الموارد وحواسيب المنشأة.
7. الاستجابة السريعة للتهديدات السيبرانية.

شرح التقنية

ماهو الأمن السيبرانى؟

يشمل مفهوم الأمن السيبراني عمليات حماية الشبكات والأنظمة وما تتضمنه من معلوماتٍ وبيانات، باستخدام التقنيات والممارسات المختلفة بهدف منع الوصول غير المصرح به أو الهجمات السيبرانية التي تتسلَّل عبر الثغرات، ويُعرَف كذلك بأمن تقنية المعلومات أو أمن المعلومات الإلكترونية. وتُصمَّم تدابير الأمن السيبراني لمكافحة التهديدات ضد الأنظمة والتطبيقات المتصلة بالشبكة، سواءً كانت تنشأ من داخل المنظمة أو خارجها.

يستهدف قراصنة الإنترنت معلومات تحديد الهوية الشخصية للعملاء، مثل الأسماء، العناوين، أرقام التعريف الوطنية، ومعلومات بطاقة الائتمان. وغالبًا ما تؤدي سرقة معلومات الهوية الشخصية إلى فقدان ثقة العملاء بالمنشأة التجارية، وقد تصِل العواقب أيضًا إلى الغرامات والإجراءات القانونية.

تقنيات الأمن السيبراني الرئيسية وأفضل الممارسات:

من خلال تطبيق أفضل ممارسات الحماية التقنية، يُمكن تقليل تعرُّض منشأتك للاختراقات الأمنية وحماية أنظمة المعلومات دون التأثير على خصوصية العميل وتجربة المستخدم، وسنستعرض هنا بعض أفضل الممارسات في المجال:

- **إدارة الهوية والوصول (IAM)**

تتضمن امتيازات الوصول لكل مستخدم، تسجيل الدخول الأحادي، المصادقة متعددة العوامل، وإدارة دورة حياة المستخدم، والتي تدير هوية كل مستخدم وامتيازاته. كما يمكن لأدوات إدارة الهوية والوصول أن تمنح متخصصي الأمن السيبراني رؤية أعمق للنشاط المشبوه على أجهزة المستخدم النهائي، مما يختصر من وقت التحقيق والاستجابة لعزل واحتواء الاختراقات وآثارها.

- **منصة أمن البيانات**

تعمل منصات أمن البيانات على حماية المعلومات الحساسة عبر بيئات متعددة، مثل البيئات المختلطة متعددة الأوساط السحابية، وتوفر رؤية مؤتمتة فورية لنقاط الضعف في البيانات ومراقبتها باستمرار لتفادي حدوث الاختراقات.

- **إدارة المعلومات والأحداث الأمنية (SIEM)**

تتضمن تجميع البيانات من الأحداث الأمنية وتحليلها لاكتشاف أنشطة المستخدم المشبوهة تلقائيًا، وتفعيل الاستجابة الوقائية أو العلاجية. وتستخدم حلول إدارة المعلومات والأحداث الأمنية طرق كشف متقدمة، مثل: تحليل سلوك المستخدم والذكاء الاصطناعي.

Kaspersky, IBM

نضج التقنية بين الواقع والمأمول

فرض تداخل التقنيات والرقمنة تحديّاتٍ جمّةً أمام المنشآت في سبيل تعزيز أمنها السيبراني، ويُظهر الارتفاع المطرد في عدد الاختراقات وخطورتها مدى حاجة هذه المنشآت إلى تركيز إنفاقها وأبحاثها في ممارسات الأمن السيبراني وتحسين موقفها السيبراني. حيث أظهرت دراسة استقصائية أجرتها تينابل Tenable في عام 2020م أنَّ 95% من المنشآت في المملكة العربية السعودية تعرّضت لهجوم سيبراني العام الماضي، فيما أفاد 85% من المشاركين السعوديين في الدراسة بأنهم شَهِدوا زيادةً كبيرةً في عدد الهجمات خلال العامين الماضِيَيْن.

أبرز التحديّات التي تواجه المنشآت في مجال الأمن السيبراني:

المدة الزمنية لرصد الاختراق

يُشكّل الوقت العنصر الأهم في رصد الاختراقات، لذلك يُعَد توظيف الروبوتات والذكاء الاصطناعي من المجالات الواعدة والتي من شأنها تقديم الكثير في تطوير الأمن السيبراني، وذلك لتفوُّقها على البشر في معالجة عنصر التوقيت وأهميته في مكافحة الاختراقات كونها تعمل على مدار الساعة.

55 يوم هو متوسط عدد الأيام بين حدوث الاختراق واكتشافه!

تهديدات إنترنت الأشياء

كشفت إحدى الدراسات أنَّ 70% من أجهزة إنترنت الأشياء بها ثغراتٌ أمنيةٌ خطيرة، حيث تؤدي واجهات الويب غير الآمنة، وعمليات نقل البيانات، ونقص المعرفة للمستخدمين إلى تعريضهم للهجمات، ويتضاعف خطرها إثر حقيقة اتصال الأجهزة ببعضها، فالوصول إلى جهازٍ واحد يعني الوصول إلى جميع الأجهزة المتصلة به.

تأمين السحابة

على الرغم من أنَّ 64% من المتخصصين في تقنية المعلومات يعتقدون أنَّ السحابة أكثر أمانًا كبنية تحتية، إلا أنَّ هناك الكثير من تحدّيات الأمان أمام جميع الأطراف من مزوّدي خدمة أو مستخدمين، حيث يجب أن تتكامل الحلول تكاملًا جيّدًا دون ترك ثغراتٍ يتسلَّل من خلالها المخترقون.

نقص الخبرات

مازال هناك نقصٌ كبيرٌ في عدد متخصصي الأمن السيبراني لتغطية الاحتياج المتزايد في أنحاء العالم، حيث أنَّ أكثر من نصف المنشآت تعاني من نقص في مهارات الأمن السيبراني.

Singtel, WEI

أمثلة على حالات الاستعمال المُمكنة

تأمين الأنظمة والعمليات:

مصادقة الحسابات

المصادقة هي عملية التحقُّق من الهوية، وتعمل من خلال مطابقة بيانات اعتماد المستخدم مع بيانات الاعتماد في قاعدة بيانات المستخدمين المصرح لهم للتحكم في الوصول إلى الأنظمة، ومنها: المصادقة أحادية العامل، مثل: طلب اسم المستخدم وكلمة المرور، والمصادقة الثنائية التي تتطلَّب عوامل إضافية، مثل: رمز التحقُّق المُرسَل على الهاتف المحمول، بصمة الإبهام، والتعرُّف على الوجه.

رصد التهديدات:
آلية تتبُّع السياق

تعمل بعض شركات الأمن السيبراني على تضمين الذكاء الاصطناعي وتعلم الآلة في مستشعراتها بما يسمح بتتبُّع الملفات أثناء نقلها عبر الشبكة وإرسالها لفحصها، وتكمن فائدة توظيف الذكاء الاصطناعي وتعلم الآلة في اكتشاف البرمجيات الضارّة وتتبُّع سياقها بما يتضمن اسم الملف وقيم التجزئة وبروتوكول النقل، مما يُمكّن متخصصي الأمن السيبراني من معرفة كيفية وصول الملف ومعالجة المشكلة وتعزيز الحماية المستقبلية.

الاستجابة السريعة:
توحيد البيانات

يبذل المُحلِّلُون جهدًا في تتبُّع تنبيهات الشبكة والأجهزة المرتبطة بها لمعرفة أين تنتهي الهجمة السيبرانية، بينما يتيح توحيد البيانات للعمليات الأمنية إمكانية ربط هذه المعلومات ورسم صورة شاملة تُمكّن المُحلِّل من فهم جلسة المستخدم، ومعرفة العمليات التي كانت تعمل عند تشغيل تنبيه البرامج الضارّة، واكتشاف الإجراءات غير الروتينية، وكان ذلك يستغرق ساعة أو أكثر، بينما توحيد البيانات يدعم المُحلِّل بطريقة سهلة ويُمكِّن المؤسسات من تقديم استجابة أسرع وأكثر تركيزًا.

Techtarget , Bricata

أمثلة على تطبيقات تجارية عالميةٍ ومحليةٍ للتقنية في قطاعاتٍ مختلفةٍ

الخدمات اللوجستية:

إدارة الهوية والوصول

تندرج حلول إدارة الهوية والوصول تحت أمن تقنيات المعلومات، وهو من أهم المجالات في مختلف القطاعات التي تخضع للتحوّل الرقمي، وهو يعني تقييد الوصول إلى البيانات الحساسة مع السماح للموظفين بمشاهدة ونسخ وتغيير المحتوى المتعلق بوظائفهم فقط، ويهدف إلى منع الأطراف غير المُصرَّح لهم من الوصول غير المشروع للموارد في الوقت المناسب، وهو من أفضل الطرق للحماية من الاحتيال وخسائره.

قدَّمت شركة أوكتا Okta، وهي شركة لإدارة الهوية والوصول نظامًا حديثًا لإدارة الهوية والوصول لموظفي شركة فيدكس FedEx العالمية، بحيث يمنح الموظفين إمكانية الوصول التي يحتاجون إليها، ويسمح لهم بتنفيذ عملهم بسرعة وأمان. وقد تمكَّنت فيدكس من دمج تطبيقاتها الهامَّة مثل Workday و Office 365 و WebEx في غضون 36 ساعة، حيث توفّر شركة أوكتا برامج سحابية لإدارة وتأمين مصادقة المستخدمين وإنشاء عناصر تحكم في الهوية سواءً في التطبيقات، خدمات الويب، أو الأجهزة الإلكترونية.

كما توفّر الشركة السعودية لاختبارات الاختراق (SPTC) حلول إدارة الهوية والوصول ضمن حلول الأمن السيبراني وتقنيات المعلومات التي تُقدِّمها للمؤسسات الحكومية والخاصة، ويعمل عليها خبراء سعوديون في مجال الأمن السيبراني والشبكات والاتصالات.

البيع بالتجزئة:
جدران الحماية

تستخدم الكثير من الشركات والشبكات المتطورة أسلوب تقنيات جدران الحماية ودمجها مع أنظمة منع اختراق الشبكات لتوفير حماية شاملة، حيث تعمل جدران الحماية على التحكم بحركة المرور عبر الشبكة وتصفية المخاطر وفرز الموثوق من غير الموثوق.

تعمل شركة فورتينت "Fortinet" الأمريكية متعددة الجنسيات على تطوير وتسويق منتجات وخدمات الأمن السيبراني، ومن أبرزها الجيل التالي من جدران الحماية وشبكة فورتينت الآمنة والمحددة بالبرمجيات واسعة النطاق (SD-WAN)، وإدارة الثغرات الأمنية وحلول التحليل الخاصة. واستفادت من هذه الخدمات سلسلة متاجر التجزئة الأمريكية Batteries Plus، وهي شركة متنامية تضم 740 موقعًا، ووظَّفت حلول فورتينت في عملياتها وشبكاتها لتتمكَّن من إدارة احتياجات الأمن السيبراني الخاصة بها بكفاءة، وفي وضع يُمكِّنُها من توسيع نطاق خدماتها الأمنية حسب الحاجة.

كما تُقدّم شركة سجل السعودية ضمن خدماتها الأمنية خدمة اختبار الاختراق، وهو نظام متعدد الخطوات لرصد نقاط الضعف باستخدام منهجيات قياسية، تتضمن الاختبارات اللاسلكية والفيزيائية، والاختبار الداخلي والخارجي، وعدد من الاختبارات الأخرى.

القطاع الصحي:
تأمين الأجهزة الطبية

يُعَدّ القطاع الصحي قطاعًا غزيرًا بالبيانات الخاصة والحرجة، ممّا يجعله من أبرز القطاعات المستهدفة من التهديدات السيبرانية، وأدّى هذا إلى ظهور الكثير من الشركات التي تُقدّم الحلول المتخصصة بتأمين المنشآت الصحية، منها: منصة بروتينوس Protenus، المعنية بتحليلات الاختراقات المتعلقة بمنشآت الرعاية الصحية، وتصدر تقريرًا سنويًّا حولها، مع تقديم الحلول التي تتضمن مراقبة خصوصية المريض وتكشف الانتهاكات التي تحدث حيالها.

ومن الحلول المؤتمتة، تُقدّم شركة سابري السعودية نظام أتمتة الاستجابة لهجمات البريد الإلكتروني من خلال تحليل وفحص البريد الإلكتروني وعزله بشكل آلي وحذفه بشكل كامل، بالإضافة إلى نظام محاكاة هجمات البريد الإلكتروني، والذي يهدف لمحاكاة الهجمات والحملات التصيُّدية للبريد الإلكتروني لرفع مستوى التوعية السيبرانية واختبار الحس الأمني السيبراني لدى الموظفين.

ولكون قطاع الرعاية الصحية من أكثر القطاعات استفادةً وتوظيفًا لتقنيات إنترنت الأشياء، تأتي شركة سايبرميدكس لتأمين إنترنت الأشياء للأجهزة الصحية وما يتعلق بها، وتتبنَّى هذه الشركة أسلوبًا هندسيًّا متعدد الطبقات في حماية الأجهزة، وتتبع في ذلك منهجًا شاملًا في البحث والتتبُّع والتحقُّق واقتراح الحلول، بالإضافة إلى كونها تُوفّر مكانًا واحدًا للعمل على جميع الأجهزة المعرضة للخطر، ممّا يسهّل إغلاق حلقة الاتصال عند حدوث مشكلات الأمان.

البيانات والسحابة:

انتشر خيار الخدمات السحابية لتخزين البيانات بسبب سهولة توافرها وتوفيرها للتكاليف، إلا أنَّه يصاحبها عددٌ من المخاوف الأمنية، لكونها طريقة مختلفة لتقديم موارد تقنية المعلومات، ولذلك تأتي منتجات الأمان السحابية لتغطي جوانب التحكم في الوصول، الخصوصية، الامتثال، أمان عبء العمل، وغيرها.

يو أس سيجنال هو مركز بيانات وخدمات سحابية يُوفّر تطبيقاته لمجموعة من العملاء، ويستعين بحلول شركة بالو ألتو الأمريكية متعددة الجنسيات، والتي تُقدّم حلولها المتخصصة لتأمين مراكز البيانات والسحابة وغيرها للصناعات الغنية بالمعلومات، وذلك من خلال جدران الحماية المتقدمة والتقنيات التي تتكامل مع بعضها لتشمل جميع جوانب الأمان. ونتج عن تعاون يو أس سيجنال وبالو ألتو توفير منصة آلية سهلة التشغيل يتم تحديثها فوريًّا مع توفّر جدران حماية افتراضية لجميع شبكاتها، وهي حلول قابلة للتطوير تدعم جهود توسع يو أس سيجنال.

كما تُوفّر شركة نورنت السعودية نظام الحماية السحابي عبر الويب، حيث يعمل على فحص الملفات غير المألوفة بحثًا عن التهديدات المتقدمة مع توفير الحماية كاملة. ويتميز وضع الحماية "ساندبوكس" السحابي بالإدراك الذكي لوجود بنية تحتية ضخمة، ويُقدّم تحليلًا متعدد الطبقات، التنميط السلوكي، وتحليل السياق.

Protenus, Sabry, Cybermdx, Sejeltech, Nournet, EsecurityPlanet

المنظومة البيئية للأمن السيبراني في المملكة العربية السعودية

المنشآت التشريعية والتنظيمية:

- **الهيئة الوطنية للأمن السيبراني**

صدرت الموافقة على تنظيم الهيئة الوطنية للأمن السيبراني في عام 1439هـ، من منطلق أهمية البيانات والأنظمة التقنية والبُنى التحتية الحساسة، ولتكون الجهة المختصة بالأمن السيبراني والمرجع الوطني لشؤونه. ومن مهامها: وضع السياسات والمعايير، وضع أطر إدارة المخاطر والاستجابة للحوادث، بناء مراكز المعلومات الوطنية، مساندة الجهات المختصة، بناء القدرات المتخصصة، وتحفيز نمو قطاع الأمن السيبراني، وأهمّها: إعداد الاستراتيجية الوطنية للأمن السيبراني، والتي تعكس الطموح الاستراتيجي للمملكة ورؤيتها (فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار)، وتُركّز الاستراتيجية على تشجيع الأبحاث ودعم الابتكار والاستثمار في مجال الأمن السيبراني لتحويل مخرجات الأبحاث والتطوير إلى منتجات وخدمات، بالإضافة إلى تحفيز قطاع الأمن السيبراني والمنشآت العاملة فيه لضمان بناء قدرات وطنية.

- **هيئة الاتصالات وتقنية المعلومات**

تُعنَى هيئة الاتصالات وتقنية المعلومات برفع مستوى نضج الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات، ورفع الثقة لدى مقدمي الخدمات في القيام بالتدابير اللازمة، وزيادة الثقة في خدمات الاتصالات وتقنية المعلومات وقدرتها على حماية المصلحة العامة ومصلحة المستخدمين. وقد أصدرت الهيئة الإطار التنظيمي للأمن السيبراني لمقدّمي الخدمة في القطاع، ويتضمن متطلبات وضوابط الأمن السيبراني، ومتطلبات تحسين إدارة مخاطر الأمن السيبراني، وأفضل الممارسات العالمية وأُطر الأمن السيبراني المحلية.

- **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز**

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، هو مؤسسة وطنية تندرج تحت مظلة اللجنة الأولمبية السعودية، ويسعى الاتحاد إلى بناء قدراتٍ محليةٍ واحترافيةٍ في مجال الأمن السيبراني، وتطوير البرمجيات والدرونز بناءً على أفضل الممارسات والمعايير العالمية، وذلك من خلال تنظيم المعسكرات والفعاليات التقنية، مثل: معسكر طويق للأمن السيبراني، ومعسكر طويق البرمجي، وعددٌ من المسابقات والهاكثونات.

- **المبادرات والفعاليات التقنية**

تُنظّم الهيئة الوطنية للأمن السيبراني المنتدى الدولي للأمن السيبراني سنويًّا منذ عام 2020م، حيث يجمع صُنّاع القرار والخبراء وكبرى الشركات الرائدة من أنحاء العالم. كما شهدت المملكة العربية السعودية في أغسطس 2021م أكبر إطلاقٍ تقنيّ للمبادرات والبرامج بقيمة تُناهز أربعة مليارات ريال، بالتعاون مع عشرة من أهم عمالقة التقنية في العالم، بهدف تطوير المهارات والكفاءات التقنية وتمكين المملكة رقميًّا لتصبح مركزًا تقنيًّا رائدًا، منها: تنظيم فعالية Hack@، وهي من أكبر الفعاليات التقنية على مستوى العالم تجمع المخترقين الأخلاقيّين لمناقشة المخاطر السيبرانية الدولية، يصاحبها منتدى للأعمال التقنية والدورات التدريبية وورش العمل، بالإضافة إلى إطلاق مؤتمر ليب Leap التقني الأكبر من نوعه، ليكون جزءًا من مبادرات تنفيذية تقنية تُقام على مدار السنة.

- **دعم روّاد الأعمال**

أقيم تحدّي الأمن السيبراني بالتعاون بين الهيئة الوطنية للأمن السيبراني ومنشآت وشركة سايت – إحدى شركات صندوق الاستثمارات العامة –، ويهدف التحدّي إلى إيجاد الحلول المبتكرة في مجال الأمن السيبراني، وتوطين هذه التقنيات من خلال عرض مشاريع الشركات الناشئة وروّاد الأعمال. كما تضطلع الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت) بتنظيم جائزة ابتكر الموجّهة للمنشآت المتوسطة والصغيرة والمُتناهية الصِغَر، بهدف تشجيع الابتكار وتسليط الضوء على المنشآت الابتكارية في المملكة. كما تُقام مسابقة منتدى إم آي تي (MIT) لريادة الأعمال في السعودية سنويًّا منذ عام 2015م، حيث تُروّج المسابقة للابتكار والإبداع على مستوى العالم، ودعم الشركات الناشئة بالسعودية، والتواصل مع روّاد الأعمال المحليّين لتحويل أفكارهم إلى واقعٍ ملموسٍ.

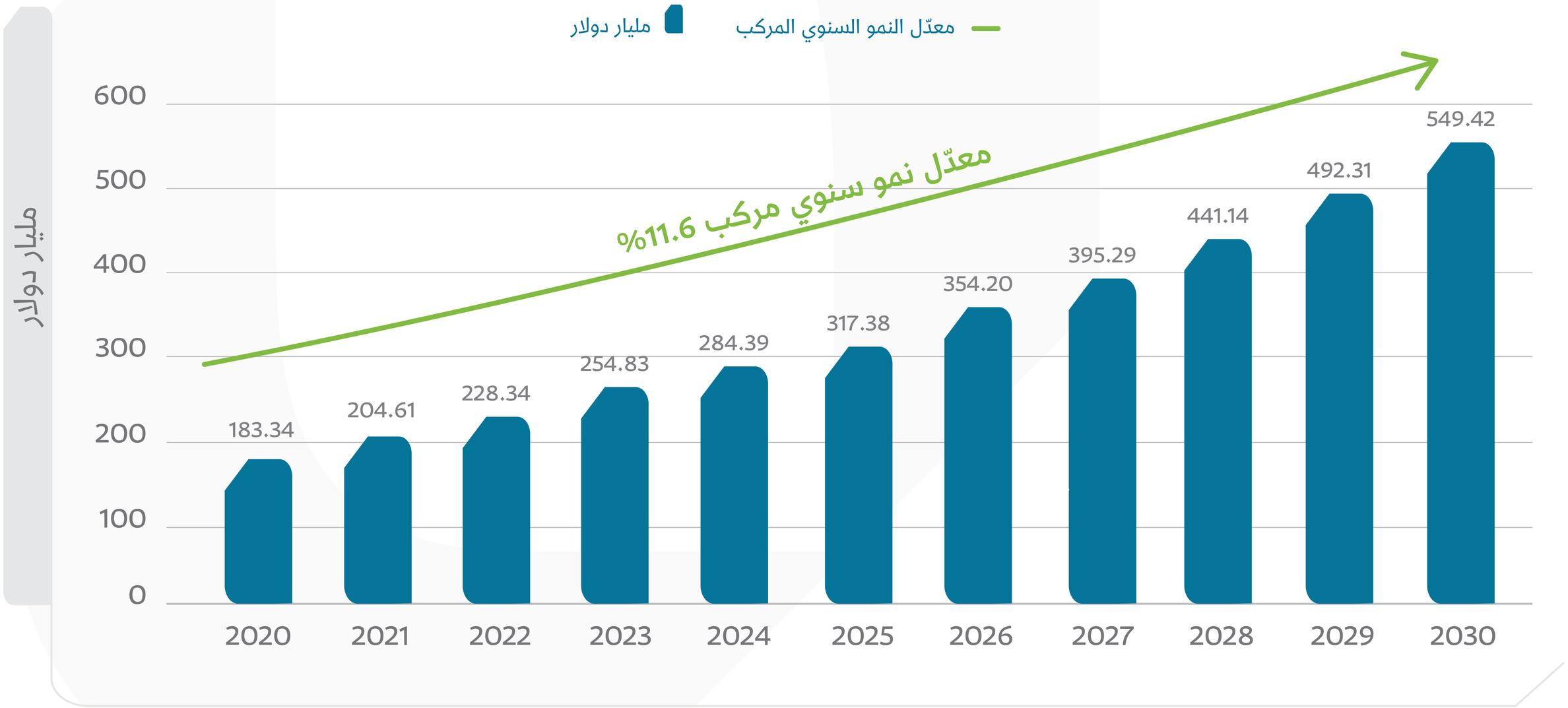
ويَنشَط في هذا المجال مركز ذكاء لإنترنت الأشياء والأمن السيبراني التابع لهيئة منشآت، والذي يعمل على تقديم الخدمات التدريبية والاستشارية لروّاد الأعمال والمنشآت الصغيرة والمتوسطة، وتنظيم اللقاءات والتحدّيات الجماعية، حيث نُظِّم تحدّي ذكاء للأمن السيبراني لتصميم الحلول المبتكرة الداعمة لقطاع الأمن السيبراني، ومن أهدافه: زيادة عدد شركات الأمن السيبراني الناشئة في المملكة، توطين تقنيات الأمن السيبراني، تمكين المواهب الوطنية، المساهمة الاقتصادية، وخلق الوظائف.

التقنية من منظور استثماري

الواقع الاقتصادي للأمن السيبراني عالميًّا

استجابت الحكومات في جميع أنحاء العالم للوتيرة المتسارعة والمتزايدة للتهديدات السيبرانية بتوجيه منشآتها العامة والخاصة إلى تطبيق الممارسات الفعّالة للأمن السيبراني، حيث بلغ متوسط تكلفة اختراق البيانات 3.86 مليون دولار أمريكي على مستوى العالم في عام 2020م، تشمل هذه التكاليف: نفقات اكتشاف الاختراق والاستجابة له، وتكلفة وقت التوقّف عن العمل، وخسارة الإيرادات، والأضرار طويلة المدى التي تلحق بسمعة الشركة وعلامتها التجارية.

كما ازداد الإنفاق العالمي على حلول الأمن السيبراني بشكلٍ ملحوظ خلال الأعوام القليلة الماضية، حيث تتوقّع مؤسسة البيانات الدولية أن يصل الإنفاق العالمي على حلول الأمن السيبراني إلى 133.7 مليار دولار أمريكي بحلول عام 2022م، وقُدِّر حجم سوق الأمن السيبراني العالمي بحوالي 180 مليار دولار أمريكي في عام 2020م، ومن المُتوقَّع أن يصل إلى أكثر من 500 مليار دولار أمريكي بحلول عام 2030م، بمُعدّل نُموٍّ سنويٍّ مُركّب يبلغ 11.6%.



تُشير التوقُّعات إلى استحواذ أمريكا الشمالية على أكبر حصة في السوق خلال السنوات القادمة، حيث تتمتَّع منطقة أمريكا الشمالية بالعديد من اللاعبين البارزين في السوق الذين يُقدِّمون حلولًا متقدمة لجميع قطاعات الصناعة وتليها أوروبا، ويُتوقَّع أن تُقدِّم منطقة آسيا والمحيط الهادئ فرص نمو كبيرة للبائعين في سوق الأمن السيبراني للتوجُّه نحو الاستثمار في هذا المجال، حيث تتَّجه دول الهند والصين توجُّهًا سريعًا نحو الرقمنة، ممّا يعني احتمالية أن يُصاحب ذلك زيادة أنشطة الجرائم الإلكترونية، كما يُؤدِّي التحوُّل الرقمي السريع إلى فتح احتمالات جديدة للتهديدات السيبرانية في بلدان الشرق الأوسط وأفريقيا، لاسيّما المملكة العربية السعودية والإمارات العربية المتحدة.

Kaspersky, IBM

أهم الاتجاهات الاستثمارية المتعلقة بالأمن السيبراني

تستحوذ الشركات الكبيرة على حصة سوقية أعلى من حيث الإيرادات في سوق الأمن السيبراني العالمي، بينما تُعَدُّ ميزانية المنشآت الناشئة غير كافية لتوظيف التقنيات المتقدمة والمُكلِفة في مجال الأمن السيبراني، مثل: الجيل التالي من جدران الحماية، وأدوات الحماية من التهديدات المتقدمة، لذا يُعد نقص الاستثمارات ومحدودية التمويل من العوامل الرئيسية التي تؤدي إلى نقص البنية التحتية المناسبة لأمن تقنيات المعلومات، وينعكس ذلك على تأخر اعتماد التقنيات والحلول الأمنية الجديدة. وتشير تقارير الصناعة إلى تباين نمو بعض منتجات وخدمات الأمن السيبراني أكثر من غيرها، وهي تمثل الاتجاهات الاستثمارية المستقبلية.

سنستعرض هنا أبرز منتجات وخدمات الأمن السيبراني والقطاعات المستفيدة منها من ناحية حصصها السوقية ونموها المستقبلي:

- **أمن الشبكات (Network Security):**

تعد منتجات أمن الشبكات من منتجات الأمن السيبراني الأكثر جاذبية والأكبر حجمًا سوقيًّا.

- **إدارة الثغرات الأمنية (SVM):**

يُتوقّع لقطاع المنتجات المعنية بإدارة الثغرات الأمنية أن يستمر في النمو ويستحوذ على نحو 22% من إجمالي سوق منتجات الأمن السيبراني بحلول عام 2027م.

- **إدارة الهوية والوصول (IAM):**

من أهم قطاعات المنتجات من حيث الحجم وآفاق النمو، حيث استحوذ على حوالي 17% من إجمالي سوق منتجات الأمن السيبراني في عام 2020م.

بينما تُشير الاحتمالات إلى انخفاض نمو منتجات أمن الرسائل وأمن الويب.

خدمات الأمن السيبراني

يُهيمن قطاع الخدمات على سوق الأمن السيبراني أكثر من قطاع المنتجات بشكلٍ عام، ويُتوقّع للخدمات التالية استمرار النمو فيها:

- **خدمات الأمن المُدارة**، حيث استحوذت على أكبر حصة من سوق خدمات الأمن السيبراني في عام 2020م.
- **خدمات الاستشارات الأمنية**، حيث استحوذت على أكثر من 17% من إجمالي سوق خدمات الأمن السيبراني في عام 2020م.

بينما حصل قطاع التعليم والتدريب على أقل حصة من سوق خدمات الأمن السيبراني.

القطاعات المستفيدة:

- **الحكومات:** حيث استحوذت على أكبر حصة من سوق الأمن السيبراني العالمي في عام 2020م.
- **قطاع البنوك والخدمات المالية والتأمين (BFSI):** حيث استحوذ على ما يقرب من 24% من سوق الأمن السيبراني العالمي في عام 2020م.
- **قطاع تقنية المعلومات والاتصالات (ICT):** حيث استحوذ على حوالي 10% من سوق الأمن السيبراني العالمي في عام 2020م.
- **قطاع الرعاية الصحية:** حيث استحوذ على حوالي 7% من حصة سوق الأمن السيبراني العالمي في عام 2020م.

MarketsandMarkets, Globen

أبرز اللاعبين والمُمكِّنين على المستويَيْن العالمي والمحلي

- **فورتينت Fortinet**

هي شركة أمريكية متعددة الجنسيات تأسَّست عام 2000م، وهي أكبر مؤسسة ومُزوِّد خدمة حول العالم في مجال تطوير وتسويق منتجات وخدمات الأمن السيبراني، وقدمت جدار حماية سمّته بـ"فورتي جيت" كأول منتج تقدمه الشركة. وتُقدّم فورتينت لعملائها حماية ذكية وسلسة، بالإضافة إلى القدرة على تحمّل متطلبات الأداء المتزايدة، ولديها بنية Fortinet Security Fabric، بحيث توفّر الأمان لمواجهة التحدّيات الأكثر أهمية في بيئات الشبكات، التطبيقات، السحابة، أو الأجهزة المحمولة.

- **تريند مايكرو Trend Micro**

هي شركة أمريكية يابانية لبرمجيات الأمن السيبراني متعددة الجنسيات، ومقراتها العالمية في طوكيو باليابان وتكساس بالولايات المتحدة. تأسست عام 1988م لتطوير برامج مكافحة الفيروسات، واستمرت في التطور والتوسّع على مدار العقود الثلاثة الماضية، وتعدّ اليوم من الأسماء الرائدة في سوق أمان السحابة المختلطة، ودفاع الشبكة، وحماية المستخدم، وإدارة المخاطر وأمن الأجهزة الطرفية.

- **بالو ألتو Palo Alto Networks**

شركة أمريكية متعددة الجنسيات للأمن السيبراني، تقدم خدماتها لأكثر من 85 ألف عميل في 150 دولة حول العالم، تُقدِّم خدماتها بشكلٍ رئيسي في الحلول الأمنية كجدران الحماية المتقدمة، الخدمات الأمنية عبر السحابة، خدمات الوصول الآمن، الاستشارات الأمنية، وغيرها.

- **كراود ستريك Crowdstrike**

شركة أمريكية لتقنيات الأمن السيبراني، تُؤمِّن المجالات الأكثر أهمية حول المخاطر التي تتعرَّض لها المنشآت، كأعباء العمل السحابي وحماية النقاط الطرفية والهوية والبيانات. من منتجاتها: منصة فالكون، وهي منصة لكشف الاختراقات من خلال مؤشرات الوقت الفعلي ومراقبة أولويات نقاط الضعف.

- **سيسكو Cisco**

شركة تقنية أمريكية متعددة الجنسيات تهتم بتطوير وتصنيع أجهزة الشبكات والبرمجيات وأدوات الاتصالات السلكية واللاسلكية، والخدمات الأمنية كجدران الحماية، وحماية النقاط الطرفية والبريد الإلكتروني والاتصال.

- **سبلانك Splunk**

شركة تقنية أمريكية عالمية تتواجد في 21 دولة حول العالم وحاصلة على 850 براءة اختراع، وهي عبارة عن منصَّة بيانات تستخدم البيانات في حلول المراقبة والحلول الأمنية وتقنية المعلومات. وتُوفِّر المنصَّة بيانات مفتوحة المصدر وقابلة للتوسُّع، تُمكِّن جميع الفرق في المؤسسة الواحدة من مشاركة البيانات والحصول على رؤية شاملة حول تفاعلات الشركة وعملياتها التجارية.

- **ستارلنك Starlink**

هي شركة رائدة في مجال تقنيات المعلومات ومزوّد لحلول أمنيّة تقنية من الجيل القادم المحفّزة بالتهديدات السيبرانية. تقدّم ستارلنك حلولًا مُتطوِّرةً باستمرار عبر مجالات مختلفة لمواجهة تحدِّيات البنية التحتية لتقنية المعلومات والأمن السيبراني. وتُزوّد شركاءها بحلول متكاملة في ستة مجالات رئيسية للأمن السيبراني: مركز البيانات والسحابة، المخاطر والامتثال، حماية البيانات، التحكم بالوصول، الإدارة، والاتصالات.

- **سايت SITE**

تأسَّست الشركة السعودية لتقنية المعلومات «سايت» عام 2017م، وهي شركة وطنية مملوكة بالكامل لصندوق الاستثمارات العامة، لتعمل على توفير خدمات وحلول رقمية وسيبرانية بكوادر وطنية للمساهمة في إثراء المحتوى المحلي. تُقدِّم شركة سايت خدمات الاستجابة والتحليل الرقمي للحوادث السيبرانية على مدار الساعة، من خلال تحديد التهديد وعزل مصدره، ثم إجراء التحليلات المفصّلة وتنفيذ الأنشطة اللازمة للتخفيف من حِدّة الحادثة واحتوائها وإنهائها، وفقًا لما يتلاءم مع بيئة تقنية المعلومات لكل عميل.

- **تقنية سايبر Taqnia Cyber**

شركة سعودية مُتخصِّصة في مجال تقنية وأمن المعلومات والاتصالات، الأمن السيبراني الصناعي، والاستخبارات الإلكترونية. تُقدِّم خدماتها من خلال مركز عمليات أمن المعلومات، بتوفير مراقبة للأحداث الأمنية وكشف أي تسلُّل أو اختراق للشبكة كخدمة مُدارة على مدار الساعة، بالإضافة إلى خدمات الحوكمة وإدارة المخاطر والالتزام، واهتمامها ببرامج التدريب والتطوير.

- **الشركة المُتقدِّمة للتقنية والأمن السيبراني (Sirar)**

شركة أمن سيبراني تابعة لمجموعة شركة الاتصالات السعودية تأسسَّت عام 2020م، مُتخصِّصة في مجال أمن الأعمال وحمايتها، وتُوفِّر مجموعة متكاملة من الحلول المتطورة والأدوات التي تُمكِّن الكشف عن الهجمات السيبرانيّة والتصدِّي لها مُبكِّرًا.

- **صحارى نت Sahara Net**

هي شركة سعودية بدأت عملها منذ عام 1994م، كأول مُقدِّم لخدمات الإنترنت في السعودية. تساعد صحارى نت عملاءها في تخطيط وبناء وتشغيل برامج أمن المعلومات بنجاح من خلال عِدَّة خدمات، كتقديم الاستشارات، والتأكُّد من أمان البيئة، وجدار صحارى نت لحماية تطبيقات الويب. بالإضافة إلى مركز عمليات الأمن السيبراني الذي يعمل على مدار الساعة، حيث يُراقب فيه فريق المُحلِّلين الأمنيِّين جميع الأحداث باستمرار.

- **القرار الآمن Safe Decision**

تأسَّست شركة القرار الآمن المحدودة السعودية في عام 2012م، وتعمل على معالجة تحديات الأمن السيبراني عبر تقديم حلول فعّالة وذات كفاءة، مثل: الخدمات المُدارة، الخدمات السحابية، ومنتجات الأمن السيبراني. حيث تُقدّم خدمة الكشف الاستباقي عن التهديدات والمخاطر المحتملة من خلال سيناريوهات واقعية لكشف نقاط الضعف وتقليل خطر التهديدات إلى الحدّ الأدنى، بالإضافة إلى خدمة العلوم الجنائية الرقمية التي تحدّد وقت وأسباب وكيفية وقوع الحوادث.

- **حلول أمن المعلومات Security Matterz**

هي شركة مُتخصِّصة في أمن تقنية المعلومات، ويقع مقرّها الدولي في لندن بالمملكة المتحدة، ومكتبها الرئيسي في الرياض بالمملكة العربية السعودية، وهي من الشركات الرائدة والمبتكرة في تقديم الخدمات والمنتجات الأمنية، وتُركِّز على معالجة التحدِّيات في ثلاثة جوانب رئيسية هي: الحماية، الشبكات، والبنية التحتية.

فرص التقنية في السعودية على المديَيْن القصير والبعيد

يأتي الاهتمام بالأمن السيبراني مدفوعًا بتصاعد التهديدات الأمنية على مستوى العالم، وبالتحوّل الرقمي الذي تشهده المملكة العربية السعودية، والذي يدفع المنشآت إلى تبنّي الرقمنة في جميع عملياتها. وتبرز أهمية حلول الأمن السيبراني في محيط الأعمال لارتباطها ارتباطًا مباشرًا بالحفاظ على سمعة المنشأة بين موظفيها وعملائها، الحفاظ على ميزتها التنافسية، والحفاظ على استمرارية الإنتاجية من خلال تجنب الوقت الضائع الناتج عن التعرض لأي تهديد سيبراني.

تُعَدُّ حلول الأمن السيبراني مجالًا جذَّابًا لروّاد الأعمال في المملكة العربية السعودية، حيث يُشير المنهج الحالي السائد في السوق السعودي فيما يتعلَّق بالأمن السيبراني أنَّ الشركات المالية هي الأقل استعدادًا من ناحية البنية التحتية مقارنةً بالاحتمالية العالية لتعرُّضها للتهديد دونًا عن الشركات الأخرى، حيث من المُحتمَل أن تستهدف الهجمات السيبرانية الشركات المالية بواقع 300 مرة أكثر من الشركات الأخرى.

من العوامل الجاذبة الأخرى لحلول الأمن السيبراني عامةً، هو نمو حجم سوق الأمن السيبراني السعودي بمُعدَّل نمو سنوي مُركّب يبلغ 16.59% حتى عام 2023م إلى ما يُقدَّر بنحو 21 مليار ريال سعودي وَفْقًا لمجلس الأعمال السعودي الأمريكي، مصحوبًا بالتوجُّه نحو تعزيز القطاع، حيث حصدت المملكة ترتيب الأول عربيًّا والمرتبة 13 من بين 175 دولة في مؤشر الأمن السيبراني العالمي الصادر مُؤخّرًا عن الاتحاد الدولي للاتصالات (ITU).

ومع ذلك ما تزال المملكة العربية السعودية تُسجِّل أكبر عدد من الهجمات السيبرانية في الشرق الأوسط، ما يتبعه زيادة طلب المنشآت على حلول الأمن السيبراني، يُصاحبه وجود عجز بين الطلب والعرض في قطاع الأمن السيبراني السعودي، ممّا دفع 95% من شركات الأمن السيبراني المحلية إلى التركيز على تقديم الخدمات والعمليات السيبرانية، بينما تُركّز 5% منها فقط على تطوير منتجات سيبرانية تواكب تغيُّر التهديدات ومستواها.

من التحدِّيات التي برزت مُؤخّرًا أيضًا، نقص الكوادر الوطنية المُتخصِّصة اللازمة لتحقيق أهداف التوطين في قطاع الأمن السيبراني، ممّا دفع الهيئة الوطنية للأمن السيبراني إلى إنشاء الأكاديمية الوطنية للأمن السيبراني لتأهيل الكوادر الوطنية المُتخصِّصة وتقليل الفجوة بين العرض والطلب، وتستهدف الأكاديمية تدريب 20 ألف متدرب من الجنسين بنهاية عام 2022م، ولقد درّبت الأكاديمية في مبادرتها الأولى (CyberPro) أكثر من 1000 متدرب من 113 جهة وطنية و23 جامعة سعودية.

من ناحية أخرى أنشأت شركة مُلكيّة للاستثمار أول صندوق استثماري في مجال الأمن السيبراني في المملكة العربية السعودية، باسم "صندوق مُلكيّة للأمن السيبراني" بالشراكة بين شركة مُلكيّة للاستثمار ومجموعة بالادين المالية الأمريكية. ويهدف الصندوق إلى إتاحة فرصة الاستثمار في شركات قطاع الأمن السيبراني وتقنياته على مستوى العالم، لتحقيق نمو رأس مالي على المديَيْن المتوسط والطويل.

كما تفتح الاستراتيجية الوطنية للأمن السيبراني عددًا من الفرص المستقبلية من خلال تركيزها على تحقيق الحوكمة المتكاملة على المستوى الوطني، الإدارة الفعّالة للمخاطر السيبرانية، حماية الفضاء السيبراني، تعزيز الشراكات والتعاون المحلي والدولي، وبناء القدرات الوطنية. وجميع هذه الأهداف تُعطي تصوُّرًا لتوفير منظومة بيئية داعمة لمشاريع ومنشآت الأمن السيبراني في المملكة العربية السعودية.

FintechSaudi, Saudigazette, Arabnews

التوصيات

تتعرَّض المنشآت الصغيرة للكثير من المخاطر، وتُعَد تهديدات الأمن السيبراني من أهمّها، إلا أنَّ التركيز على تقليل التكاليف قد يدفع المنشآت إلى تقليل حظ الأمن السيبراني من الاهتمام والميزانية، فيُتغاضى عن تطبيق أفضل المُمارسات من أجل بدء الأعمال وتشغيلها بصورةٍ أسرع وبأقل تكلفة مُمكنة.

في الواقع، ينبغي أن يكون لحماية المنشأة أولويَّة قُصوى للحفاظ على تشغيل آمن، مستقر، وطويل المدى، وسنستعرض هنا أهم التوصيات للمنشآت عامةً، والمنشآت الصغيرة على وجه الخصوص، من أجل الحفاظ على الأعمال بعيدًا عن التهديدات:

1. تقييم المخاطر الأمنية:

ينبغي على كل منشأة فهم التهديدات الأكثر أهمية بالنسبة لمجال المنشأة، مثل فشل النظام، والكوارث الطبيعية، وتهديدات القراصنة، وتحديد تأثيرها عليها، وأن تجري كل منشأة تقييمات أمنية روتينية للتأكُّد من أنَّ إجراءات الأمان المُطبَّقة تُلبِّي مستوى الأمان المأمول.

2. النسخ الاحتياطي:

من المهم عمل نسخ احتياطي للبيانات والملفات المهمة، وعدم الاحتفاظ بها في مكانٍ واحد، مع النظر في مدى مناسبة خيارات التخزين السحابي مع طبيعة تلك الملفات، وربما تتطلَّب بعض البيانات الاحتفاظ بنسخ ورقية أيضًا.

3. التشفير:

يكون النسخ الاحتياطي آمنًا إذا كانت جميع المعلومات التي نُسِخَت احتياطيًّا آمنة، ولا يكون ذلك إلا بتثبيت التشفير على جميع الأجهزة ومُحرِّكات الأقراص، وتشفير رسائل البريد الإلكتروني ذات المعلومات الحساسة.

4. استخدام طبقات حماية متعددة:

كتنفيذ سياسة كلمة المرور التي تتطلَّب كلمات مرور قوية، مراقبة أمان حسابات عمل الموظفين، استخدام الجدران النارية وجعلها أولوية لحماية شبكتك، والتأكُّد من تثبيت أفضل برامج الحماية ضد الفيروسات، وتحديثها باستمرار وتعيين شخص مسؤول عن متابعة تحديثها وإجراء الفحوصات الدورية لكل جهاز متصل بالإنترنت.

5. تدريب الموظفين:

تحدث معظم الاختراقات السيبرانية نتيجة لأخطاء بشرية، لذلك على المنشأة تنظيم الدورات التدريبية لموظفيها، والتأكُّد من امتلاكهم للمهارات المطلوبة ذات الصلة الوثيقة بالتهديدات المُحتمَلة، وتطبيقهم لأفضل المُمارسات، ووضع سياسات واضحة للأمن السيبراني.

6. التحكُّم في الوصول إلى الحواسيب:

ينبغي حصر وصول الموظفين إلى البيانات التي يحتاجونها لأداء مهامهم فقط، حيث أنَّ كل نقطة وصول تُمثِّل خطرًا وتهديدًا، على أن يقتصر منح الامتيازات الفردية للوصول للموظفين الموثوق بهم.

CMITSolution, ITResource

منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

شكرًا