العنوان:	الأمن السيبراني: تعريفه - أهميته - أنواعه - استراتيجيات الوقاية من الهجمات السيبرانية
المصدر:	مجلة الدراسات الدولية
الناشر:	وزارة الخارجية - معهد الأمير سعود الفيصل للدراسات الدبلوماسية
المؤلف الرئيسي:	آل مداوى، علي
المجلد/العدد:	ع34
محكمة:	نعم
التاريخ الميلادي:	2023
الشهر:	محرم
الصفحات:	115 - 124
رقم MD:	1454807
نوع المحتوى:	بحوث ومقالات
اللغة:	Arabic
قواعد المعلومات:	EcoLink
مواضيع:	الأنظمة الإلكترونية، الأمن الرقمي، الجرائم الإلكترونية
رابط:	http://search.mandumah.com/Record/1454807

© 2026 المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو المنظومة.

للإستشهاد بهذا البحث قم بنسخ البيانات التالية حسب إسلوب الإستشهاد المطلوب:

إسلوب APA

آل مداوى، علي. (2023). الأمن السيبراني: تعريفه - أهميته - أنواعه - استراتيجيات الوقاية من الهجمات السيبرانية.مجلة الدراسات الدولية، ع34 - 115 ، 124. مسترجع من http://:search.mandumah.com/Record/1454807

إسلوب MLA

آل مداوى، علي. "الأمن السيبراني: تعريفه - أهميته - أنواعه - استراتيجيات الوقاية من الهجمات السيبرانية."مجلة الدراسات الدوليةع34 (2023): 115 - 124. مسترجع من http://:search.mandumah.com/Record/1454807

© 2026 المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو المنظومة.

الأمن السيبراني

تعريفه – أهميته – أنواعه – إستراتيجيات للوقاية من الهجمات السيبرانية

د.علي آل مداوي

معهد الامير سعود الفيصل لدراسات الدبلوماسية

مقدمة

يلعب الأمن السيبراني دورًا حيويًا ومهمًا للغاية في حماية المعلومات والأنظمة الإلكترونية، وكذلك حماية البنية التحتية وكيفية إدارة مخاطرها، وإيجاد السبل في معالجة الأزمات السيبرانية؛ لاستمرار الحياة وعمل المنشأة دون حدوث تعطل أو خلل يؤثر في مسار الحياة الطبيعية للمنشأة .

وازداد الاهتمام بالأمن السيبراني، وذلك مع تطور التقنية والتكنولوجيا التي بات الاعتماد عليها كبيرًا في تعاملاتنا اليومية، وكذلك في التعاملات الحكومية والصفقات التجارية، وغيرها.

كما يغطي الأمن السيبراني جميع التدابير التي يتم تنفيذها في التطبيقات عبر الإنترنت لضمان الحماية الكافية لكافة معلومات من كافة الهجمات المحتملة من قبل (الهكر)، كما يتضمن أنظمة مصممة لحماية وتأمين الكمبيوتر والأنظمة والشبكات والبرامج من الهجمات الإلكترونية.

الهدف الأساسي من البحث هو كتابة نبذه تاريخية عن الأمن السيبراني؛ تعريفه، وأهميته، وأنواعه، وكتابة أبرز جهود المملكة في قطاع الأمن السيبراني، وذكر إستراتيجيات – بإذن الله – ستكون وقاية من الوقوع تحت الهجمات السيبرانية، وحماية المعلومات الشخصية، وكذلك الحد من الهجمات الإلكترونية المحتملة التي قد تؤدي إلى خسائر مالية وفنية ضخمة للمنظمات والحكومات والأفراد.

وتشمل كذلك الاهتمام بقطاع الأمن السيبراني؛ وذلك بوضع برامج تقنية حديثة ومطورة، يتم تبنيها بشكل شائع في كل المنظمات الحكومية وغير الحكومية، وعلى مستوى الأفراد كذلك، وتركيب أحدث

البرامج الدفاعية للتصدي للبرمجيات الخبيثة؛ بداية من الاستخدام الخاضع للرقابة، للترخيص الإداري، وتدقيق السجلات ومراقبة النظام بشكل مستمر، واتخاذ كافة التدابير لضمان أمن المعلومات وحمايتها من الهجمات المحتملة.

فالمراقبة المستمرة للأنظمة والشبكات، واستخدام المراقب – من خلال التفويض الإداري – هو أيضًا وسيلة لحماية البيانات الشخصية من الهجمات المحتملة.

إن تبني هذه التدابير ضرورة لتوفير الدفاعات السيبرانية، كما أنها تحمي البيانات والأنظمة والشبكات من الهجمات. وتضمن الإجراءات لمستخدمي الإنترنت – سواء الأفراد أو المنظمات أو الحكومات أمن المعلومات الخاصة وسلامتها.

نبذة تاريخية عن الأمن السيبراني

- بداية وضع الأسس الأولى لمكافحة المؤسسية الخطرية لمخاطر الأمن السيبراني كانت مع حلول الثمانينات، وقد أقر الكونجرس أول قانون في العالم لمكافحة الجريمة السيبرانية سنة ١٩٨٤م، وهو قانون الاحتيال وإساءة استخدام الحاسوب.
- أما في مرحلة التسعينات وبعد عام ٢٠٠٠م، فقد تطورت هذه الجرائم، ووصلت لنطاق أوسع، وتم استخدام المعلومات في الإرهاب المنظم من خلال ضرب البنى التحتية للدول؛ سواء كانت مرافق عامة أم خدمات، وأيضا البنى العسكرية والاقتصادية المتمثلة في البنوك وغيرها.
- وأول من استخدم كلمة cyber هو ويليام جيبسون في كتابه الكلاسيكي عام ١٩٨٤م، وأضيفت إليه جهود نيل ستيفنسون عام ١٩٨٩م؛ ليرسم صورة أقرب إلى الشمولية عن ماهية مفهوم الفضاء الذي يتشارك فيه الناس.
- وفي عام ١٩٩١م، استخدمت كلمة سايبر مقترنة بالفضاء، وأصبح هذا المفهوم أشمل وأوسع من الإنترنت؛ ليضم كل الاتصالات والشبكات، وقواعد البيانات، ومصادر المعلومات.
- وفي يوم ٢ نوفمبر ١٩٨٨م أطلقت موريس – أحد طلاب جامعة كورنيل في الولايات المتحدة الأمريكية – أول دودة حاسوب في تاريخ الإنترنت. وكان إطلاق هذه الدودة هو النقطة الأولى التي بدأ عندها الاهتمام الجدي بكيفية تعزيز الأمن السيبراني.
- وفي ١٩٨٩م ظهر فيروس المنتقم الأسود، ويعتبر أول فيروس يحتوي على خصائص العدوى، وظهر في نفس السنة فيروس فرودو مع إمكانية التخفي.
- ومع بداية التسعينات أصبح القراصنة أكثر قوة، وأصبحوا يشاركون الفيروسات فيما بينهم، ومع حلول عام ١٩٩٥م ظهر ما يعرف باسم الفيروسات الجزئية، التي تستهدف الملفات العادية؛ مما سهل الإيقاع بالضحية.
- وفي فجر الثورة الرقمية في منتصف العقد الماضي، انتبه الغرب إلى قضية الإرهاب الإلكترونية

ومخاطره؛ حيث قام الرئيس الأمريكي السابق بيل كلينتون في عام ١٩٩٦م بتشكيل لجنة حماية منشآت البنية التحتية الحساسة.

- ومع مطلع عام ٢٠٠١م، وبتعاون خبراء مع وزارة العدل الأمريكية – عرفت الوزارة الجريمة السيبرانية.
- وأما المرحلة الثانية من القمة العالمية لمجتمع المعلومات فقد أقيمت في تونس في نوفمبر٢٠٠٥م، عَهِدَ قادةُ العالم فيها بأن تكون مسالة تعزيز الأمن السيبراني على رأس جهود التنسيق الدولية.
- ويعد المنتدى الدولي للأمن السيبراني منصة عالمية تتناول موضوعات الأمن السيبراني وبناء أسس التعاون، تنظمه الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، وكان انعقاد الدورة الأولى بالتزامن مع رئاسة المملكة لمجموعة العشرين، ويمثل المنتدى منصة تفاعلية عالمية لكافة المعنيين والمختصين بمجال الأمن السيبراني من ممثلي القطاعات الحكومية والخاصة، والمنظمات غير الربحية، والأوساط التعليمية والأكاديمية حول العالم، بهدف نقل المعرفة حول موضوعات الأمن السيبراني، وبناء أسس التعاون بين الدول والمنظمات؛ ليصبح قطاع الأمن السيبراني عنصراً ممكناً في مواجهة التحديات المستقبلية، وصناعة التنمية الاقتصادية والاجتماعية في السعودية وحول العالم.
- وقد عقدت الهيئةُ المنتدى الدولي للأمن السيبراني في دورته الأولى خلال الفترة ٤ –٥ فبراير ٢٠٢٠م في مدينة الرياض، تحت شعار (تضافر الجهود نحو عالم سيبراني أفضل). وجاء عقد المؤتمر تزامناً مع رئاسة السعودية لمجموعة العشرين. وقد شهد المنتدى مشاركة ١٤٧ متحدثاً من داخل المملكة وخارجها، كما تجاوز عدد الحضور ٣٥٠٠ مشارك.
- وقد نظمت الهيئة الوطنية للأمن السيبراني حوارًا افتراضيًا، جمع كبار المسؤولين حول العالم، المعنيين بالأمن السيبراني. وأقيم الحوار في ٧ أبريل ٢٠٢١م تحت شعار (واقع الفضاء السيبراني اليوم وغدًا). وقد جاء تنظيم هذا الحوار، بالتزامن مع التهديدات السيبرانية، التي تواجه العالم بشكل مستمر.
- ونظمت الهيئة الوطنية للأمن السيبراني النسخة الثانية من المنتدى الدولي للأمن السيبراني تحت شعار (إعادة التفكير في الترتيبات السيبرانية العالمية)، يومي ٩ و١٠ نوفمبر ٢٠٢٢ في العاصمة الرياض، بمشاركة نخبة من صناع القرار والرؤساء التنفيذيين، وكبار المسؤولين الحكوميين، وممثلي أبرز الشركات العالمية، والمنظمات غير الحكومية، والأوساط الأكاديمية من حول العالم؛ لمناقشة القضايا الإستراتيجية، وفرص التعاون بين الشركاء الدوليين في مجال الأمن السيبراني. وشهد المنتدى انعقاد أكثر من ٣٠ جلسة حوارية، تناولت مجموعة من الموضوعات التي ناقشت آفاق التغيير في المشهد السيبراني، والاقتصادات السيبرانية، والتطور الجيوسيبراني، ومستقبل العمل السيبراني، والأمن السيبراني للجميع. وتطرق المنتدى كذلك إلى أهمية التعاون الدولي وبحث الحلول العملية لسد الفجوة السيبرانية عالمياً، واستكشاف مستقبل الأمن السيبراني، وضمان تحقيق الأمن السيبراني لجميع المجتمعات.

تعريف الأمن السيبراني

لا شك أن هناك تعريفات كثيرة للأمن السيبراني، سنذكر أهم تلك التعريفات الحديثة؛ فبداية كلمة السيبراني تعني بلغة اللاتينية الفضاء.

يعرف الأمن السيبراني على أنه:

- عبارة عن مجموع من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع: الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء المعلوماتي.
- الأمن الذي يعني بحفظ المعلومات وشبكات وأجهزة الحاسب الآلي.
- سلاح إستراتيجي بيد الحكومات والأفراد – لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول –.
- أنظمة دفاع حديثة عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات ضد الهجمات الخارجية.

لاشك أن مصطلح الأمن السيبراني أو الحروب السيبرانية مرتبط بخدمة الإنترنت؛ لكون العالم يشهد في الفترة الراهنة نوعًا جديداً من سباق التسلح، لكنه ليس بالشكل المعروف التقليدي، بل سباق يقوم على استحداث أو تطوير برامج إلكترونية معدة لأغراض عسكريه، تعرف اختصارًا بالسايبر.

أهمية الأمن السيبراني

للأمن السيبراني أهمية كبيرة في حماية البيانات، وخصوصية المؤسسات والأفراد، والكثير من المجالات المختلفة التي يختص بها، ويمثل الأمن السيبراني أهمية كبيرة للكثير من المنظمات الحكومية وغير الحكومية، مثل: الشركات والمؤسسات العامة والخاصة، فهو بمثابة جدار الحماية الأساسي لكافة المعلومات السرية لكل جهة مستفيدة. ولا شك أن بانهياره أو اختراقه سوف تكون المؤسسة أو الشركة هدفًا سهلًا للجهات الإجرامية والهاكرز بكل سهولة.

كما يحمي الأمن السيبراني كذلك مختلف أنواع البيانات الحساسة والمهمة – سواء للحكومات أو الشركات، أو حتى الأفراد العاديين – من تعرّضها للسرقة أو التدمير أوالتلف. إن تعرّض الأمن السيبراني للاختراق من شأنه أن يُحدث الكثير من الأضرار التي تلحق بسمعة الشركة أو المؤسسة، وبالتالي تؤثر على مستوى التعاملات التي تقوم بها في الأسواق التجارية.

يؤدي اختراق الأمن السيبراني لأي جهة إلى تهديدًا كبيرًا ومباشرًا للكثير من البيانات الشخصية

للعملاء، وهي عملية من شأنها أن تفسد علاقة العميل مع هذه الجهة، وبالتالي تعرض الشركة لخطر الانهيار إذا ما قرر العملاء وقف التعاون معها بسبب هذا الخرق أو الانتهاك.

ويساهم الأمن السيبراني بشكل كبير في الحد من هذه الجرائم الإلكترونية التي تطورت بشكل كبير نتيجة لاتصال أعداد مهولة من الأجهزة على الإنترنت، والتي بلغ عددها في عام 2021 حوالي 21.1 مليار جهاز. وتتمثل الجرائم الإلكترونية في مثل التصيد الاحتيالي عن طريق إرسال الروابط الضارة عبر البريد الإلكتروني.

ويحمي الأمن السيبراني جميع المعلومات والبيانات الحساسة من السرقة، بما في ذلك المعلومات الشخصية، والمعلومات الحكومية، والمعلومات الخاصة بالملكية الفكرية، والمعلومات الصحية المحمية (PHI)، ومعلومات التعريف الشخصية (PII). ويُساعد الأمن السيبراني على صد هجمات السرقة باستخدام برامج الدفاع الإلكترونية، ومنع احتمالية استخدام المعلومات بشكل غير مصرح به وإحداث الضرر، ومنع حدوث محاولات ابتزاز تُضر بالفرد، كما يُحافظ على كيان المجتمع بحماية معلوماته الخاصة بالخدمات المالية، والمستشفيات، ومؤسسات الرعاية الصحية الأخرى، ومحطات الطاقة، وغيرها.

ويُساعد كذلك الشركات والمؤسسات على حماية نفسها، والدفاع عنها ضد هجمات خرق البيانات؛ إذ تُعد المؤسسات والشركات هدفًا سهلًا لمجرمي الإنترنت، بسبب استخدامها للخدمات السحابية، ولتخزين معلوماتها الشخصية والحساسة فيها، وتُعد أغلب الخدمات السحابية وخاصة ذات التكوين السيئ هدفًا لهجمات الكثير من المجرمين الإلكترونيين المتطورين.

أنواع الأمن السيبراني

- أمن البنية التحتية الحيوية: يعتمد على البنية التحتية الفيزيائية الإلكترونية للشبكة، وتتواجد عادة في وسائل النقل، والمدارس، والمستشفيات، والدوائر الحكومية، وفي شبكات المراكز التجارية. وهذا النوع يتطلب دراسة إلكترونية لنقاط ضعف المنظومة، والقاعدة الفيزيائية للشبكة لتطويرها وحمايتها من عمليات الاختراق.
- تطبيقات الأمن: وهو الاختيار السليم للبرامج التي تحمي الأجهزة والشبكات من عمليات الاختراق الإلكتروني، ولها عدة أنواع معروفة؛ أهمها: برامج مكافحة الفيروسات، والجدران النارية، وبرامج التشفير المعلوماتي. هذه الطرق الثلاثة تضمن لك حماية محتواك من عمليات الاختراق الإلكترونية؛ فكلما كان مستخدم الإنترنت أكثر اطلاعا على تكوير برامج الحماية ويستخدمها، كان أبعد عن احتمالية وقوعه رهن الابتزاز والاختراق.
- أمن الشبكة: يهتم بالاختراقات الخارجية التي تهدد المنظومة الإلكترونية والمواقع التكنولوجية، فإن أمن الشبكة هو عملية تهتم بحماية الشبكة من الاختراقات الخارجية للشبكات والأجهزة. وهنالك

عدة أنواع تضمن حصول أمن الشبكة؛ وهي: كلمات مرور جديدة، وبرامج الحماية من الفيروسات، وبرامج مكافحة التجسس، والجدران النارية.

- سحابة الأمان: وهي نظام مراقبة وحماية لكل مصادر المعلومات والبيانات التابعة للمستخدم عبر المواقع والمنصات الإلكترونية، ولكن إذا تم تفعيل هذه الخاصية لا يعني أنه بإمكانك تجاهل كل الأمور السيبرانية الأخرى، فمن الضروري الاهتمام بحماية المعلومات والبيانات الخاصة بك بشكل مستمر.
- إنترنت الأشياء: يشمل عدة منظومات أساسية، مثل: أجهزة التلفاز، وأجهزة الاستشعارات والطابعات، وهذا النوع صنف كنوع من الأمن السيبراني، الذي يحمي البيانات لدى الأجهزة المذكورة، ولكنه كباقي التقنيات؛ إذا لم يتم الاهتمام والمتابعة به يمكن أن يصل المخترق إلى نظام الحماية ويفك شفرته.

دوافع اهتمام الدول بالأمن السيبراني

البعد العسكري

لاشك أن الفضاء السيبراني بات أحد أهم النطاقات الرئيسة للعمليات العسكرية، مثل: النطاق البري والبحري والفضائي. وتقوم العديد من الدول بزيادة نفقاتها على بناء وتعزيز إمكانياتها السيبرانية. وقد أصبح للفضاء السيبراني مكاناً مهمًا في إستراتيجيات الأمن القومي، والإستراتجيات العسكرية في العالم اليوم. ويرى العديد من الباحثين أن هذا ينذر ببدء ما يطلق عليه سباق التسلح الرقمي.

البعد السياسي

تقوم القيادات السياسية العليا في أي دولة بتنظيم مؤسساتها المعلوماتية والأمنية وتقويتها، لكي تحمي مصالحها الوطنية والقومية، وكذلك تساعد المعلومات على تهيئة قيادة الدول باتخاذ القرارات المناسبة لإدارة الأزمات وحلها، أو إحباط الهجمات التي يشنها العدو.

ويعتبر الفضاء السيبراني من أهم مجالات التأثير السياسي في العالم اليوم؛ حيث تهدف الهجمات السيبرانية إلى إحداث هذا التأثير من خلال استهداف المصالح القومية للدول من ناحية، ومن ناحية أخرى استهداف مواطني الدولة.

البعد الاجتماعي

تؤدي الجريمة السيبرانية إلى العديد من الأضرار والآثار السلبية على المجتمع؛ حيث إنها تعتمد بصورة رئيسة على انتحال هوية الضحية في تعاملاته المالية والاجتماعية، وهذه الآثار لا تقتصر على الأفراد، ولكنها تمتد أيضًا إلى المنظمات والشركات، كما أن الحكومات من الأهداف الجذابة للأعمال الإجرامية السيبرانية، وهذه الجرائم تهدف بالأساس إلى إحداث العديد من الأضرار تجاه المجتمع ككل،

وهذه الأضرار تستهدف تعطيل مصالح المواطنين في شبكات المواصلات والطاقة والشبكات المصرفية.

البعد الإعلامي

تلعب وسائل الإعلام المختلفة دورًا كبيرًا في توعية المجتمع، باستخدام التقنية الحديثة للكشف عن الجرائم السيبرانية؛ لتوخي الحذر من الوقوع ضحية الهجمات السيبرانية المباشرة والموجهة، فيجب التعامل بحذر، بأخذ الحيطة والحذر، ورفع مستوى الأمان والتوعية، مثل: وضع كلمة مرور قوية، وتحديث الأجهزة وفق آخر ما وصلت إليه التقنية الحديثة، وتوجيه أبناء المجتمع نحو استخدام التقنية الحديثة استخدامًا سليمًا، من خلال عمل برامج تلفزيونية توعوية، وتوزيع نشرات توعوية عبر الصحف الورقية أو الإلكترونية، أو عبر وسائل التواصل الاجتماعي.

البعد التعليمي

يعتبر التركيز على إيجاد جيل متخصص في مجال الأمن السيبراني أمرًا مطلوبًا وحيويًا، وذلك للعمل كمتخصصين في هذا المجال الذي يعد من المجالات الحديثة والمهمة للتصدي للهجمات السيبرانية العابرة للقارات في هذا الفضاء السيبراني الكبير.

البعد الاقتصادي

تكمن أهميته في أن معظم الهجمات السيبرانية الخبيثة تستهدف المصالح الاقتصادية للأفراد والحكومات والقطاع الخاص؛ حيث يعتبر الاستغلال المالي هو الدافع الأول للجريمة السيبرانية التي تستهدف الأفراد والمؤسسات الحكومية وغير الحكومية؛ من أجل سرقة الأموال من حسابات الضحايا، وتحويلها إلى حسابات خارجية. ويقوم القراصنة باستخدام برامج تجسس، وهذه البرامج تساعد في الحصول على المعلومات السرية من الجهاز الخاص بالضحية، مثل: كلمات المرور في المواقع الإلكترونية المختلفة.

جهود المملكة العربية السعودية في مجال الأمن السيبراني

إن الأمر الملكي القاضي بإنشاء (الهيئة الوطنية للأمن السيبراني) وارتباطها بمقام مولاي خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود – تعد بمثابة قفزة نوعية رائدة للمحافظة على أمن وسلامة المجتمع السعودي واستقراره، وتأمين سلامة عمل كل قطاعات الدولة المختلفة، كما أن الجهود التي تقدمها هيئة الأمن السيبراني – التي تعد الجهة المختصة بالأمن السيبراني في المملكة والمرجع الوطني في شؤونه – تؤدي إلى توفير البيئة التشريعية والتنظيمية الداعمة لتحفيز نمو وتنافسية القطاع، وإصدار مجموعة من السياسات والضوابط ومتابعة التزام الجهات الوطنية بها.

جاءت رؤية المملكة 2030م منسجمة ومتناغمة مع تعزيز الأمن السيبراني؛ لدورها الحيوي في حفظ، ودعم استخدام تقنيات المعلومات وتعزيز البنية التحتية الرقمية؛ لكي تكون مركزًا أساسياً لبناء أنشطة صناعية متطورة، وتحقيق مراكز متقدمة عالمياً في مؤشر الأمم المتحدة للحكومة الإلكترونية؛ فقد حققت المرتبة الثانية عالمياً في محور التحسن المستمر في مؤشر الأمن السيبراني من بين 193 دولة ضمن تقرير الكتاب السنوي للتنافسية العالمية لعام 2022م.

إستراتيجيات للوقاية من الهجمات السيبرانية

هناك استراتيجيات أنصح الموظفات والموظفين الذين يمثلون الخطوط الأمامية الأولى في أعمالهم، الذين يعملون في المنشآت الحكومية وغير الحكومية الخاصة، باتباعها لتفادي أي هجوم سيبراني قد يقع – لا سمح الله –؛ مما قد يؤدي إلى خسائر ربما تكون مؤثرة وتنعكس سلباً؛ وهي كالآتي:

1. أخذ دورات توعوية لتعزيز الثقافة في الأمن السيبراني، ومواكبة التطورات، ولأهميتها الحيوية في حياتنا اليومية والتجارية، والاطلاع باستمرار على كل جديد؛ لكي لا يجد المهاجم ثغرة لتحقيق هدفه في استهداف الأفراد أو المنشآت.
2. وضع رقم سري يكون قوياً؛ حتى لا يتم استهدافك من قِبل المهاجمين (الهاكر) بكل سهولة.
3. استخدام نظام الأمان الثلاثي الأبعاد D3 Secure لكلمة المرور، لتجنب عملية الاحتيال الإلكتروني، وحماية بياناتك.
4. وضع جدار ناري؛ للحماية من أي تهديد سيبراني خارجي أو داخلي.
5. كن حريصاً عند فتح أي بريد إلكتروني مرفق أو رابط، وذلك بالتأكد من مصدره؛ لكي لا تكون ضحية أي هجوم سيبراني، وإبلاغ المختصين بالإيميلات المشبوهة لكي يتم التعامل معها.
6. احتفظ بنسخة احتياطية من بياناتك بشكل منتظم.
7. تأكد من تحديث جميع أنظمة المنشأة بشكل منتظم.
8. خذ كامل الاحتياطات والمتابعة الدقيقة في التفاعل مع الإعلام الجديد، وتوخ الحذر من أي هجوم سيبراني يستهدف الحساب في فيسبوك، تويتر، سناب شات، إنستقرام، أو أي تطبيق آخر.
9. عند تصفح بعض الأعمال التجارية الحساسة، مثل البنوك أو التسوق، يجب أن يتم ذلك على جهاز يخصك، والحذر من استخدام جهاز عام، ربما تكون ضحية في حال حفظ كلمة المرور بالجهاز.
10. يجب تفادي الروابط الوهمية، والتأكد من أي مصدر؛ لتفادي أي نصب واحتيال، والتأكد من مصدر الواي فاي، وعدم الارتباط بأي واي فاي متاح مشبوه.
11. التأكد من أي أجهزة خارجية مثل الفلاش، أو أجهزة الجوال أو الحاسوب من أن تكون بها مواد ضارة قد تتسبب في الإضرار بالأجهزة الأخرى الخاصة، أو بأجهزة المنشأة.
12. متابعة الأطفال وعدم إفلاتهم في ظل عالم الإنترنت الذي يحتوي على إيجابيات وسلبيات؛ لكي لا يكونوا ضحية الجانب السلبي، وحثهم على الاستفادة بالجانب الإيجابي.

التشريعات التي وضعتها المملكة في مكافحة الجرائم الإلكترونية

الجرائم المعلوماتية حسب المادة رقم (1) من نظام مكافحة جرائم المعلوماتية في المملكة، التي تم تعريفها بأنها: الأفعال التي ترتكب متضمنةً استخدام الشبكة المعلوماتية بصورة مخالفة لأحكام نظام الجرائم المعلوماتية.

وتعد المملكة العربية السعودية من دول مجموعة العشرين G20 وأكثر دول العالم من حيث

الأهمية الاقتصادية والإستراتيجية في العالم. وتسعى المملكة في عالم الأعمال والاقتصاد للوصول إلى أعلى مستوى من الأداء؛ من أجل تحقيق الميزة التنافسية في السوق؛ لذا فإن معظم الهجمات السيبرانية الخبيثة تستهدف المصالح الاقتصادية للأفراد أو الشركات؛ حيث يعد الاستغلال المالي هو الدافع الأول للجريمة السيبرانية التي تستهدف الأفراد أو المؤسسات التجارية؛ للحصول على معلومات مصرفية للضحايا؛ من أجل سرقة الأموال من حسابات الضحايا وتحويلها إلى حسابات خارجية. ويقوم القراصنة بتنفيذ هذه الهجمات باستخدام برامج التجسس.

ومبادرة مسرعة الأمن السيبراني التي أطلقتها هيئة الأمن السيبراني مؤخراً، تستطيع الشركات الناشئة ورواد الأعمال الاستفادة منها؛ حيث تعمل المسرعة في مجالات التقنيات التأسيسية والتقنيات الناشئة ذات الأولوية في مجالات الأمن السيبراني والمجالات ذات العلاقة. وتشكل المسرعة إحدى الممكِّنات المهمة لتحفيز منظومة الصناعة المحلية في الأمن السيبراني، وتدعم التكامل بين القطاعين العام والخاص، وتسهم في تحفيز وتشجيع الابتكار وبناء منظومة وطنية لصناعة تقنيات الأمن السيبراني، وتوفير بيئة متميزة لتطوير المنتجات والتقنيات، وربط الشركات الناشئة بالمستثمرين؛ بهدف تمكين التحول الرقمي الآمن، واستقطاب أفضل الشركات والمشاريع في تقنيات الأمن السيبراني.

الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز

يُعدّ الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز من الهيئات الوطنية السعودية التي أُسّست تحت مظلة اللجنة الأولمبية السعودية، وكان الهدف من إنشائه هو العمل بشكل جاد وحثيث على رفع الكفاءات الوطنية، والعمل على تطوير مختلف أنواع البرمجيات، وكل ما يتعلق بتقنيات الطائرات بدون طيار.

يُقدّم الاتحاد السعودي للأمن السيبراني مختلف الأنشطة والبرامج التي ترفع الوعي الثقافي في المجتمع بكلّ ما يخصّ مجال الأمن السيبراني، والبرمجة والتقنيات الحديثة، كما يعمل في ذات الوقت على وضع البرامج التي تشجع الشباب السعودي على الدخول في هذا المجال المهم والحيوي.

الأكاديمية الوطنية للأمن السيبراني

تُعدّ الأكاديمية الوطنية للأمن السيبراني إحدى المؤسسات الوطنية التي جاء إنشاؤها بموجب مبادرةٍ أطلقتها وزارة الاتصالات وتكنولوجيا المعلومات من خلال التعاون مع صندوق تنمية الموارد البشري (هدف)، ومن أهمّ الأسباب التي دعت إلى إنشاء هذه الأكاديمية هي رفع مستوى القدرات الوطنية الرقمية في جميع مجالات التكنولوجيا الحديثة.

الخاتمة

تولي القيادة الرشيدة بالمملكة العربية السعودية أهمية بالغة لقطاع الأمن السيبراني، وقد حققت المملكة نجاحًا باهرًا بتحقيق المرتبة الثانية عالمياً في مؤشر الأمن السيبراني، وذلك ضمن تقرير الكتاب السنوي للتنافسية العالمية لعام 2022 الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا IMD، والذي يُعد واحداً من أكثر التقارير شمولية في العالم بمجال الأمن السيبراني.

المراجع

1. الشايع، خالدبن سعد (2019)الأمن السيبراني، الطبعة الأولى، الدار العالمية
2. https://www.almaal.org/essay-on-the-importance-of-cyber-security2
3. https://sotor.com/%D985%%D8%A7_%D987%%D98%A_%D8%A3%D987%%D98%5%D98%A%D8%A9_%D8%A7%D984%%D8%A3%D985%%D986%_%D8%A7%D984%%D8%B3%D98%A%D8%A8%D8%B1%D8%A7%D986%%D98%A%D89%F3
4. https://ar.wikipedia.org/wiki/%D8%A7%D984%%D985%%D986%%D8%AA%D8%AF%D989%_%D8%A7%D984%%D8%AF%D988%%D984%%D98%A_%D984%%D984%%D8%A3%D985%%D986%_%D8%A7%D984%%D8%B3%D98%A%D8%A-8%D8%B1%D8%A7%D986%%D98%A4
5. https://www.almaal.org/essay-on-the-importance-of-cyber-security5.
6. https://cyberone.co/%D985% %D8%A7-%D987% %D988-%%D8%A7%D984%%D8%A3%D985%%D986-%%D8%A7%D984%%D8%B3%D98%A%D8%A8%D8%B1%D8%A7%D986%%D98%A6/
7. https://mawdoo3.com/%D8%A3%D987%%D985%%D98%A%D8%A9_%D8%A7%D984%%D8%A3%D985%%D986%_%D8%A7%D984%%D8%B3%D98%A%D8%A8%D8%B1%D8%A7%D986%%D98%A7.
8. https://www.al-jazirah.com/writers/20222585.html