الأمـــــن السـيـبرانـــــي

إعداد

هيئة الإعلام

قسم الدراسات والاتصال والعلاقات العامة

2021

الأمــن السيبراني

المقدمة

يعد الأمن السيبراني أمراً مهما نظراً لأن المؤسسات الحكومية والعسكرية والشركات والمؤسسات المالية والطبية تقوم بجمع ومعالجة وتخزين كميات كبيرة من البيانات على أجهزة الكمبيوتر والأجهزة الأخرى. يمكن أن يكون جزء كبير من تلك البيانات معلومات حساسة ، سواء كانت ملكية فكرية ، أو بيانات مالية ، أو معلومات شخصية أو أنواع أخرى من البيانات التي يمكن أن ينتج عن الوصول أو الكشف غير المصرح به عواقب سلبية و مدمِّرة.

تنقل المؤسسات بيانات حساسة عبر الشبكات وإلى الأجهزة الأخرى أثناء ممارسة الأعمال التجارية ، ويصف الأمن السيبراني الخطوات و الإجراءات اللازمة لحماية تلك المعلومات والأنظمة المستخدمة لمعالجتها أو تخزينها مثل السيرفرات و أجهزة الحاسوب و أجهزة التخزين و الشبكات و الخ.

مع نمو حجم الهجمات الإلكترونية وتطورها، تحتاج الشركات والمؤسسات، خاصة تلك التي تتولى مهمة حماية المعلومات الحساسة المتعلقة بالأمن القومي أو السجلات الصحية أو المالية، إلى اتخاذ خطوات لحماية معلوماتها الحساسة المتعلقة بالأعمال والموظفين و المستخدمين. حيث تمثل الهجمات الإلكترونية والتجسس الرقمي أكبر تهديد للأمن القومي، حتى أنه يتفوق على الإرهاب.

التعريف

الأمن السيبراني (Cyber security) : يُطلق عليه أيضاً " أمن المعلومات " و"أمن الحاسوب"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

يعرّفه "إدوارد أموروسو" (Edward Amoroso) "صاحب كتاب " الأمن السيبراني " الذي صدر عام 2007 بأنه "مجموع الوسائل التي من شأنها الحدّ من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات"، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات الرقمية ووقفها، وتوفير الاتصالات المشفرة .

ويعرفه قانون الأمن السيبراني الأردني لعام 2019 والمنشور في الجريدة الرسمية بأنه الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في إتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك.

مصطلحات مرتبطة بالأمن السيبراني

يتبّع الأمن السيبراني نهجاً محدّداً يتكون عادة من عدّة طبقات للحماية تُثبَت في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المستخدم حمايتها .توجد العديد من المصطلحات المرتبطة بالأمن السيبراني نذكر منها:

الفضاء السيبراني :(Cyberspace) عبارة عن بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية، مكوّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين، ويُطلق عليه "الذراع الرابعة للجيوش الحديثة".

الردع السيبراني :(Cyber Deterrence) يعرّف على أنه منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية.

الهجمات السيبرانية :(Cyber Attacks) أيّ فعل يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام.

الجريمة السيبرانية (Cybercrime) : مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية عبر شبكة الإنترنت، وتتطلب تحكماً خاصاً بتقنيات الكمبيوتر ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

حادث الأمن السيبراني: الفعل أو الهجوم الذي يشكل خطرا على البيانات أو المعلومات أو نظم المعلومات أو الشبكة المعلوماتية أو البنى التحتية المرتبطة بها ويتطلب استجابة لإيقافه أو للتخفيف من العواقب أو الآثار المترتبة عليه.

عمليات الأمن السيبراني: مجموعة من الإجراءات المرتبطة بإدارة ومراقبة واكتشاف حوادث الأمن السيبراني والتهديدات التي تقع ضمن حيز الفضاء السيبراني ووضع خطط الاستجابة لها وتنفيذها.

خدمات الأمن السيبراني: الأنشطة الفنية والإدارية والاستشارية في مجال الأمن السيبراني بما فيها خدمات التقييم الأمني والمراقبة والتدقيق والخدمات الاستشارية.

التشريعات الأردنية فيما يخص الأمن السيبراني

تنص المادة 3- أ من قانون الأمن السيبراني لسنة 2019 والمنشور في الجريدة الرسمية: يشكل في المملكة مجلس يسمى (المجلس الوطني للأمن السيبراني) يتألف من رئيس يعين بإرادة ملكية سامية وعدد من الأعضاء يمثلون الجهات التالية:-

- وزارة الاقتصاد الرقمي والريادة.
- البنك المركزي الأردني.
- القوات المسلحة الأردنية- الجيش العربي.
- دائرة المخابرات العامة.
- مديرية الأمن العام.
- المركز الوطني للأمن وإدارة الأزمات.
- ثلاثة أعضاء يسميهم مجلس الوزراء بناء على تنسيب رئيس المجلس لمدة سنتين قابلة للتجديد لمرة واحدة على أن يكون اثنان منهم من ذوي الخبرة من القطاع الخاص.

وتنص المادة 4 من نفس القانون: يتولى المجلس المهام والصلاحيات التالية:

- إقرار الاستراتيجيات والسياسات والمعايير المتعلقة بالأمن السيبراني.
- إقرار الخطط والبرامج اللازمة لقيام المركز بمهامه وواجباته بما فيها برامج التعاون الدولي والإقليمي.
- اعتماد التقارير ربع السنوية عن الوضع الأمني السيبراني للمملكة والتقرير السنوي عن أعمال المركز.
- تشكل اللجان التنسيقية من ذوي العلاقة لتمكين المركز من تحقيق أهدافه على أن تحدد في قرار تشكيلها مهامها وواجباتها وكيفية انعقاد اجتماعاتها واتخاذ قراراتها.
- إقرار الموازنة السنوية للمركز.

وتنص المادة 5- أ: ينشأ في المملكة مركز يسمى (المركز الوطني للأمن السيبراني) يتمتع بشخصية اعتبارية ذات استقلال مالي وإداري وله بهذه الصفة تملك الأموال المنقولة وغير المنقولة والقيام بجميع التصرفات القانونية اللازمة لتحقيق أهدافه بما في ذلك إبرام العقود وله حق التقاضي وينوب عنه في الإجراءات القضائية وكيل إدارة قضايا الدولة.

كما تنص المادة 5- ب: يرتبط المركز برئيس الوزراء.

وتنص المادة 6- أ: يهدف المركز إلى بناء منظومة فعالة للأمن السيبراني على المستوى الوطني وتطويرها وتنظيمها لحماية المملكة من تهديدات الفضاء السيبراني

ومواجهتها بكفاءة وفاعلية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة الأشخاص والممتلكات والمعلومات.

من ابرز ما تتناوله المادة 6- ب: يتولى المركز في سبيل تحقيق أهدافه المهام والصلاحيات التالية:

- إعداد استراتيجيات وسياسات ومعايير الأمن السيبراني ومراقبة تطبيقها ووضع الخطط ولبرامج اللازمة لتنفيذها ورفعها للمجلس لإقرارها.
- تطوير عمليات الأمن السيبراني وتنفيذها وتقديم الدعم والاستشارة اللازمين لبناء فرق عمليات الأمن السيبراني في القطاعين العام والخاص وتنسيق جهود الاستجابة لها والتدخل عند الحاجة.
- تحديد معايير الأمن السيبراني وضوابطه بموجب تعليمات يصدرها لهذه الغاية.
- منح الترخيص لمقدمي خدمات الأمن السيبراني.
- التعاون والتنسيق مع الجهات ذات العلاقة لتعزيز امن الفضاء السيبراني.
- تطوير البرامج اللازمة لبناء القدرات والخبرات الوطنية في مجال الأمن السيبراني وتعزيز الوعي به على المستوى الوطني.
- إعداد مشروعات التشريعات ذات العلاقة بالأمن السيبراني بالتعاون مع الجهات المعنية ورفعها للمجلس.
- دعم البحث العلمي في مجال الأمن السيبراني بالتعاون مع الجامعات.

الإستراتيجية الوطنية الأردنية للأمن السيبراني 2018-2023

رؤية الأمن السيبراني

تنص رؤية الأمن السيبراني للمملكة الأردنية الهاشمية على ما يلي:

(أردن واثق وآمن ضمن العالم الرقمي ومقاوم للتهديد السيبراني)

يمكن تحقيق ذلك من خلال تأسيس وتنمية وتطوير الكفاءات الوطنية في مجال الأمن السيبراني والاستجابة الأمنية الملائمة لتحقيق التميز في الأمن الوطني والتجارة والتعاون الدوليين ودعم التحول الحكومي الرقمي لزيادة الرفاه على المستويين الفردي والوطني.

الأهداف الإستراتيجية

تبين الأهداف الإستراتيجية الأربعة الغايات الوطنية لتحقيق الأمن السيبراني في الأردن كما وتبين كذلك آلية تحقيقها:

- **الحماية**: تعزيز الثقة والمرونة لدى الحكومة والبنى التحتية الوطنية الحساسة وقطاعات الأعمال والجمهور لمواجهة التهديدات السيبرانية والتصدي لها، ويتأتى ذلك من خلال:
  - نشر السياسات والإجراءات اللازمة لوضع منهجية وطنية موحدة للأمن السيبراني.
  - إنشاء نموذج حوكمة ملائم ومؤسسات تضمن تحقيق الأمن السيبراني الفعال.
  - بناء الهيكل المؤسسي اللازم لتطوير وتشغيل الأمن السيبراني الوطني وتوفير مصدر موحد للمشورة على مستوى الحكومة من اجل معالجة التهديدات الإستخباراتية والتثبت من المعلومات.
  - إعداد برامج خاصة بنشر الوعي وبناء القدرات في مجال الأمن السيبراني.
- **الكشف والتحري**: تعزيز فهم واعتراض الأعمال العدوانية التي تستهدف المملكة وأصولها المعلوماتية وهو ما يتم باعتماد التدابير التالية:
  - تطوير القدرات الحالية لكشف التهديدات السيبرانية.
  - فهم طبيعة أعداء الفضاء السيبراني الوطني وأساليبهم.
  - التأكد من جاهزية الدفاعات الأمنية وفعاليتها واستمرارها في كشف الحوادث الأمنية السيبرانية.
  - تعريف المستوى الطبيعي في هذا السياق ومن ثم ضبط الحوادث غير الاعتيادية من خلال نطاق واسع من المهارات والقدرات.
- **الاستجابة**: تطوير وتوظيف القدرات الملائمة للاستجابة للهجمات السيبرانية بنفس طريقة الاستجابة لأي هجوم آخر ضد الأمن الوطني، وذلك باتخاذ التدابير التالية:
  - وضع عمليات وكفاءات ونشاطات لإدارة الحوادث بقصد الحد من الأخطار، بحيث تكون محددة بعناية وفعالة.
  - تقليل واحتواء آثار حوادث الأمن السيبراني.
  - إستعادة الخدمات الأساسية.
  - استخدام التحليل للأسباب الجذرية والأدوات الجنائية بعد وقوع الحوادث من اجل تحسين عمليات الاستجابة.
- **التطور**: تطوير المعرفة والمهارات والقدرات السيادية المستدامة والملائمة من اجل المحافظة على أمن سيبراني متين من خلال الوسط الأكاديمي

والقطاع الخاص والبحث والتطوير بالإضافة إلى الشراكات الدولية، وذلك من خلال:

- الشراكة مع المنظمات والشركاء المختصين بهدف التعاون وتبادل المعرفة.
- تحديد الشركاء الأكاديميين من اجل تشكيل فريق عمل مؤهل ومتمرس بالإضافة إلى إنشاء أكاديمية وطنية للأمن السيبراني.
- تفعيل التشريعات والأنظمة اللازمة لإنشاء وإدارة الأمن السيبراني الوطني.
- توفير الأدوات اللازمة لتطوير القدرات السيادية المستدامة والشركات التي يمكنها إطلاق مبادرات فعالة في مجال الأمن السيبراني.
- إنشاء قنوات التواصل الوطنية والدولية الملائمة والمتينة.

حددت الإستراتيجية ابرز التهديدات السيبرانية التي يمكن أن تؤثر على الأردن، وهي:

- خدمات الاستخبارات الأجنبية.
- الإرهاب والاضطرابات الجيوسياسية.
- القراصنة الناشطون.
- المطلعون الداخليون.
- الجريمة والفساد.

أهمية الأمن السيبراني وكيفية تحول المعلومات إلى أموال

تنبع أهمية الأمن السيبراني من ثلاثة محاور رئيسية هي:

السرية:(Confidentiality) أي التحكم في الولوج إلى البيانات وإتاحتها لمن يُسمح لهم فقط.

السلامة (Integrity) : الحفاظ على سلامة البيانات والمعلومات وحمايتها من الهجمات التخريبية أو السرقة.

الجاهزية (Availability) : جاهزية جميع الأنظمة والخدمات والمعلومات وإتاحتها حسب طلب الشركة أو عملائها.

5% فقط من إجمالي المعلومات والملفات الافتراضية المخزنة حول العالم آمنة. وهو في الواقع رقم منخفض جداً مقارنة بأهمية المعلومات والبيانات في عصرنا الحالي. لذلك من المتوقع أن يصل الإنفاق على قطاع الأمن السيبراني إلى 170.4 مليار دولار بحلول عام 2022 لمنع الهجمات وعمليات القرصنة.

والأمن السيبراني اليوم من أكثر القضايا التي لا غنى عنها للأفراد والشركات والحكومات. وتستدعي الزيادة الهائلة الأخيرة في جرائم الإنترنت والإرهاب السيبراني دراسات مكثفة حول أسبابها وعواقبها.

وتظهر أبرز نتائج البحث والدراسات الشاملة في المنطقة أن أهم سبب لنجاح هجمات الجرائم الإلكترونية للمنظمات الإرهابية هو "الخطأ الفردي" أو "الجهل الفردي" للطرف المعرض للهجوم.

لهذا السبب، يوصي الخبراء بتنظيم أنشطة توعية واسعة النطاق إضافة إلى زيادة الخدمات العامة والتدريب عبر الإنترنت من أجل إحباط معظم الهجمات الإلكترونية.

فعلى سبيل المثال تعرضت 88% من الشركات في جميع أنحاء العالم في عام 2019 و91% منها في عام 2020، لهجمات إلكترونية تهدف إلى الحصول على كلمات المرور الخاصة بها. وتشير حوالي 68% من شركات وممتلكات عالم الأعمال إلى أنها تتعرض لهجمات إلكترونية أكثر شدة كل عام.

لذلك، ولمنع هذه الهجمات، من المتوقع أن يصل قطاع الأمن السيبراني الذي ينتج برامج وأجهزة لحماية أنظمة المعلومات والبيانات من الهجمات الإلكترونية، إلى 130 مليار دولار عام 2021 و170.4 مليار دولار عام 2022.

وتهدف الهجمات على الشركات في جميع أنحاء العالم إما إلى سرقة البيانات منها أو انتهاك أمنها وجعلها غير قابلة للاستخدام والمطالبة بفدية في المقابل، ففي عام 2020 وحده تم الحصول على أكثر من 70 مليار دولار مقابل هذه الممارسات. كما أجريت حوالي 86% من هذه الهجمات لأجل تحويل المعلومات المقرصنة إلى أموال من خلال عمليات تهديد الشركات وابتزازها.

في المقابل، 10% من هذه الهجمات تتم لأغراض تجسس مباشرة ضد شركة أو حكومة ما. ومن بين أكثر من 70 مليار هجوم نجد أن 45% منها لأغراض القرصنة، و17% منها محاولة تسلل إلى نظام الحوسبة الخاص بالشركة أو الحكومة، و22% منها للحصول على كلمات مرور الشركة أو الوكالة الحكومية ذات الصلة.

وبالرغم من كل هذه الهجمات، فإن عدد الهجمات الإلكترونية أو أعمال الإرهاب الإلكتروني التي يمكن اكتشافها أو الإبلاغ عنها رسمياً من الشركات والوكالات الحكومية بين عامي 2005 ومنتصف 2020، كان فقط 11.762 عملية.

ومن الضروري اليوم أن نعلم أن جميع كلمات المرور البالغ عددها 300 مليار كلمة التي يستخدمها الأفراد والمؤسسات في جميع أنحاء العالم، تتعرض للهجوم عن طريق البرامج المقرصنة الموضوعة في رسائل البريد الإلكتروني، التي يقوم فيها الأفراد وموظفو الشركة بتمكين هذه البرامج من التسلل إلى أجهزة الكمبيوتر الخاصة بهم أو نظام معالجة معلومات الشركة دون أخذ الاحتياطات الواجبة أو عن طريق الخطأ بنسبة 37% من الرسائل التي تحمل مرفقات من النوع doc أوdot ، وبنسبة 19.5% من الرسائل ذات الملحق.exe .

فوائد الأمن السيبراني

يمكن تلخيص أهم فوائد الأمن السيبراني فيما يلي:

- حماية الشبكات والبيانات من الدخول غير المصرح به؛
- تحسين مستوى حماية المعلومات وضمان استمرارية الأعمال؛
- تعزيز ثقة المساهمين وأصحاب المصلحة في الشركة؛
- استرداد البيانات المُسربة في وقت أسرع في حالة حدوث خرق للنظام الأمني السيبراني.

العالم يعتمد على التكنولوجيا أكثر من أي وقت مضى، نتيجة لذلك، ينتهج الأمن السيبراني الناجح نهجاً معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها، وفي أي دولة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً، ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية.

تحديات الأمن السيبراني

لتحقيق الأمن السيبراني (الأمن الالكتروني) الفعال ، تحتاج المنظمة إلى تنسيق جهودها في جميع أنحاء نظام المعلومات الخاص بها. تشمل عناصر الأمن السيبراني كل ما يلي:

- أمن الشبكة
- أمان التطبيق

- أمن الكمبيوتر
- أمن البيانات
- أمن قاعدة البيانات والبنية التحتية
- أمن الأنظمة السحابية (Cloud security)
- امن الهاتف
- خطة التعافي من الكوارث / استمرارية الأعمال

إن التحدي الأكثر صعوبة في الأمن السيبراني التطور المستمر لمخاطر الأمن نفسها باستمرار. التهديدات تتقدم وتتغير بسرعة أكبر مما تستطيع المنظمات مواجهته. لذلك ، يجب إتباع نهج أكثر إستباقية في مجال الأمن السيبراني. من خلال دراسة المخاطر المحتملة و اتخاذ إجراءات وقائية لتجنب حدوثها ، و وضع خطة للتعافي من الكوارث في حال وقوعها لتقليل الخسائر و التعافي بسرعة .

إدارة الأمن السيبراني

الشركات يجب أن تكون على استعداد للاستجابة للهجمات السيبرانية المحتملة ، ويجب أن تكون قادرة على استعادة العمليات الأساسية في حال تم فقدها بسبب الهجمات السيبرانية ، وضمان حماية أصول وسمعة الشركة . تركز إرشادات NCSA الخاصة بالأمن السيبراني لإجراء تقييمات مخاطر الإنترنت على ثلاثة مجالات رئيسية: تحديد العمليات الحرجة و البيانات الأكثر أهمية التي تتطلب الحماية ؛ تحديد التهديدات والمخاطر التي تواجه تلك البيانات و العمليات ؛ وتحديد الضرر الذي قد تتعرض له مؤسستك في حالة فقد البيانات أو كشفها بطريقة غير مشروعة. بعد تقييم مخاطر الإنترنت ، قم بوضع وتنفيذ إجراءات وقائية للتخفيف من مخاطر الإنترنت مثل برامج مكافحة الفيروسات و الجدران النارية و أنظمة كشف الاختراق ، وحماية العمليات و البيانات الأكثر أهمية الموضحة في تقييمك ، واكتشاف الحوادث الأمنية والاستجابة لها بشكل فعال. يجب أن تشمل هذه الخطة كل من العمليات والتقنيات اللازمة لإنشاء برنامج أمن سيبراني ناجح. ومع تزايد و تطور الهجمات السيبرانية ، يجب أن تطوير أفضل الممارسات للأمن السيبراني لاستيعاب الهجمات المتزايدة و المتطورة التي يقوم بها المهاجمون. يوفر الجمع بين مقاييس الأمن السيبراني السليمة والوعي الأمني لدى الموظفين والأفكار الأمنية أفضل دفاع ضد مجرمي الإنترنت الذين يحاولون الوصول إلى بيانات

شركتك الحساسة. على الرغم من أنها قد تبدو مهمة شاقة ، إلا أن الأمن السيبراني عنصر مهم و أساسي لاستمرار الأعمال في ظل ظهور هجمات و فيروسات جديدة في كل يوم .

أنواع شائعة من الأمن السيبراني (الأمن الالكتروني)

1. أمن الشبكات (Network Security): يحمي حركة مرور البيانات على الشبكة من خلال التحكم في الاتصالات الواردة والصادرة ومنع التهديدات من الدخول أو و خارج الشبكة.

2. أنظمة منع فقد البيانات (DLP): يحمي البيانات من خلال التركيز حماية أجهزة تخزين البيانات و قواعد البيانات و حماية البيانات في أماكن تخزينها و أثناء انتقالها على الشبكة.

3. أمن أنظمة السحابية (Cloud Security) : يوفر الحماية للبيانات المستخدمة في الخدمات والتطبيقات المستندة إلى الأنظمة السحابية .

4. أنظمة كشف التسلل (IDS) أو أنظمة منع التسلل (IPS) : تعمل على الكشف عن الهجمات السيبرانية و اتخاذ تدابير لإيقافها .

5. إدارة الهوية والوصول (IAM): تستخدم خدمات المصادقة للحد من صلاحيات وصول الموظفين وتتبعه و مراقبة عمليات الوصول لحماية الأنظمة الداخلية من هجمات الوصول غير المصرح.

6. التشفير: هو عملية تشفير البيانات لجعلها غير مفهومة، وغالبًا ما يتم استخدامها أثناء نقل البيانات لمنع السرقة أثناء النقل.

7. برامج مكافحة الفيروسات(Antivirus): تفحص أنظمة الكمبيوتر بحثًا عن التهديدات المعروفة. برامج مكافحة الفيروسات الحديثة قادرة حتى على اكتشاف التهديدات غير المعروفة سابقًا بناءً على سلوكهم.

أنواع تهديدات الأمن السيبراني

تهديدات الأمن السيبراني تنقسم إلى ثلاث أنواع بناءا على الهدف من الهجوم :

- مكاسب مالية
- التدمير و الإتلاف
- التجسس (بما في ذلك التجسس على الشركات لسرقة براءات الاختراع)

تقريبًا، يقع كل تهديد عبر الإنترنت في أحد هذه الحالات الثلاثة. من حيث تقنيات الهجوم ، فإن المهاجمين لديهم خيارات عديدة. هناك عشرة أنواع شائعة من التهديدات السيبرانية:

1. البرمجيات الخبيثة: البرامج التي تؤدي مهمة ضارة على جهاز أو شبكة الضحية ، على سبيل المثال إتلاف البيانات أو الاستيلاء على النظام.

2. التصيد/الخداع (Phishing): الهجوم الذي يتم إرساله عبر البريد الإلكتروني والذي ينطوي على خداع مستلم البريد الإلكتروني للكشف عن المعلومات السرية أو تنزيل البرامج الضارة عن طريق النقر فوق ارتباط تشعبي في الرسالة او تنزيل مرفقات مثل ملف او صورة.

3. هجوم "رجل في الوسط" (MITM): عندما يقوم المهاجم باعتراض الاتصال بين المرسل والمستلم للرسائل الإلكترونية والاطلاع عليها ، وربما يقوم بالتعديل عليها قبل إعادة توجيهها للطرف الآخر. يعتقد المرسل والمستلم أنهما يتواصلان مباشرة مع بعضهما البعض ولكن في الحقيقة يكون هناك طرف ثالث بالمنتصف يطلع على الرسائل . قد يتم استخدام هجوم رجل بالمنتصف في الجيش لإرباك العدو و اعتراض الرسائل بين الجنود و القيادة.

4. حصان طروادة (Trojans): هو نوع من البرامج الضارة التي تدخل نظام الضحية وهي متخفية داخل برنامج او ملف ، على سبيل المثال تكون مخفية داخل برنامج أو لعبة .

5. هجمات الفدية (Ransomware) : الهجوم الذي يتضمن تشفير البيانات على النظام المستهدف والمطالبة بفدية مقابل السماح للمستخدم بالوصول إلى البيانات مرة أخرى.

6. هجوم رفض الخدمة أو هجوم رفض الخدمة الموزع (DDoS): عندما يستولي المهاجم على العديد من الأجهزة (وربما الآلاف) ويستخدمها لإغراق الهدف بعدد ضخم من الطلبات و البيانات ، مثل إرسال عدد ضخم من الطلبات (Request) أو الدخول لموقع الكرتوني في نفس اللحظة ، مما يؤدي لاستهلاك جميع موارد السير فر و بالتالي يؤدي لتوقفه عن العمل .

7. الهجمات على أجهزة إنترنت الأشياء (IoT): أجهزة إنترنت الأشياء مثل أجهزة الاستشعار الصناعية عرضة لأنواع متعددة من التهديدات السيبرانية. وتشمل قيام المهاجمين بالاستيلاء على أجهزة انترنت الأشياء لجعلها جزءا من هجومات الحرمان من الخدمة DDoS والوصول غير المصرح به إلى البيانات التي يتم جمعها من قبل الجهاز. نظرًا لان كثرة إعداد أجهزة انترنت الأشياء مثل الكاميرات و المستشعرات و غيرها، وتوزيعها الجغرافي وأنظمة التشغيل القديمة التي تعمل بها، لذلك تعد أجهزة إنترنت الأشياء هدفًا رئيسيًا للهجمات الالكترونية.

8. خروقات البيانات: خرق البيانات هو الوصول غير المصرح للبيانات و سرقتها من قبل الهاكرز. تشمل دوافع انتهاك البيانات الجريمة (أي سرقة الهوية) ، والرغبة في إحراج مؤسسة والتجسس.

9. البرامج الضارة على تطبيقات الجوال: الأجهزة المحمولة عرضة لهجمات البرامج الضارة تمامًا مثل أجهزة الحوسبة الأخرى. قد يقوم المهاجمون بتضمين برامج ضارة في التطبيقات ، ومواقع الجوال أو رسائل البريد الإلكتروني والخداع والرسائل النصية. بمجرد اختراقها، يمكن للجهاز المحمول منح المهاجمين حق الوصول إلى المعلومات الشخصية وبيانات الموقع والحسابات المالية والمزيد.

ما هو الفرق بين الأمن السيبراني وأمن المعلومات؟

يرتبط الأمن السيبراني و أمن المعلومات ارتباطًا وثيقًا لدرجة أنه غالبًا ما يُعتقد أنهما مرادفين لنفس المعنى. ولكن ، هناك بعض الفروق الهامة بين الاثنين.

يهتم أمن المعلومات بالتأكد من الحفاظ على أمان البيانات بأي شكل من الأشكال سواء كانت الكترونية أو مستندات ورقية او غيرها وهو أوسع قليلاً من الأمن السيبراني. لذا ، من المحتمل أن يكون شخص ما خبيرًا في أمن المعلومات دون أن يكون خبيرًا في الأمن السيبراني.

أما الأمن السيبراني يدور حول حماية البيانات الموجودة في شكل إلكتروني (مثل أجهزة الكمبيوتر والخوادم والشبكات والأجهزة المحمولة وغيرها) من التعرض للخطر أو الهجوم القادمة من الفضاء الالكتروني . جزء من ذلك هو تحديد البيانات المهمة ، وأين توجد ، والمخاطر المحتملة ، والتكنولوجيا التي يجب عليك تنفيذها من أجل حمايتها.

هذا يجعل الأمن السيبراني (Cyber Security) مجموعة فرعية من أمن المعلومات (الرأي الأكثر شعبية على الإنترنت). لكن جرائم الإنترنت التي لا تنطوي على تهديد للمعلومات ليست جزءًا من أمن المعلومات ولكنها في الواقع مصدر قلق للأمن الإلكتروني. على نفس المنوال ، فإن تهديدات المعلومات الغير الكترونية ، تخضع لأمن المعلومات ولكنها ليست تحت الأمن السيبراني (CyberSecurity).

امن المعلومات	الأمن السيبراني
الأمر كله يتعلق بحماية المعلومات من الاستخدام و الوصول و التعديل غير مصرح به.	إنها ممارسة لحماية البيانات من المصادر الخارجية على الإنترنت.
إنه يتعامل مع حماية البيانات من أي شكل من أشكال التهديد.	إنه يتعلق بالقدرة على حماية استخدام الفضاء الإلكتروني من الهجمات الإلكترونية.
أمن المعلومات هو لحماية المعلومات بغض النظر عن مكان وجودها أو شكلها.	الأمن السيبراني لحماية أي شيء في عالم الإنترنت.

يتعامل أمن المعلومات مع حماية البيانات من أي شكل من أشكال التهديد.	الأمن السيبراني يتعامل مع الخطر القادم من الفضاء الإلكتروني.
يسعى أمن المعلومات إلى منع الوصول غير المصرح به وتعديل و إتلاف البيانات.	يهاجم الأمن السيبراني جرائم الإنترنت والاحتيال عبر الإنترنت وإنفاذ القانون من خلال الوصول للمهاجمين و معاقبتهم.

باختصار، الأمن السيبراني (الأمن الالكتروني) يوفر حماية ضد الخطر القادم من الفضاء الإلكتروني. أمن المعلومات يوفر حماية البيانات من أي شكل من أشكال التهديد.

نصائح الأمن الإلكتروني ـ حماية نفسك من الهجمات الإلكترونية

يمكن للشركات والأفراد حماية أنفسهم من التهديدات الإلكترونية بإتباع مجموعة من أهم نصائح الأمن الإلكتروني:

1. تحديث التطبيقات ونظام التشغيل :يعني هذا الاستفادة من أحدث التصحيحات الأمنية.
2. استخدام برامج مكافحة الفيروسات :حلول الأمن مثل Kaspersky Total Security ستكتشف التهديدات وتزيلها. أبقِ برنامجك محدَّثًا للحصول على أفضل مستوى من الحماية.
3. استخدام كلمات مرور قوية :احرص على ألا تكون كلمات المرور الخاصة بك سهلة التخمين.
4. لا تفتح مرفقات البريد الإلكتروني من المرسِلين الذين لا تعرفهم :قد تكون مصابة ببرامج ضارة.
5. لا تفتح أي روابط في رسائل البريد الإلكتروني المرسلة من مرسلين لا تعرفهم أو على مواقع إلكترونية غير معروفة :هذه طريقة شائعة لنشر البرامج الضارة.
6. تجنّب استخدام شبكات Wi-Fi غير آمنة في الأماكن العامة :تعرّضك الشبكات غير الآمنة لخطر الهجمات الوسيط.

الأمن السيبراني مهم في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني. فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية، أو محاولات الابتزاز، أو فقدان البيانات المهمة. كما تعتمد الدول على البنية التحتية الحيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية؛ لذا فإن تأمينها أمر ضروري.

الأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد، وفي عصر التكنولوجيا أصبح للأمن السيبراني الدور الأكبر في صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدول المختلفة.

المصادر

- الإستراتيجية الوطنية للأمن السيبراني 2018-2023. وزارة الاتصالات وتكنولوجيا المعلومات. الأردن.
- قانون الأمن السيبراني رقم 16 لسنة 2019.
- ما هو الأمن السيبراني؟ موقع "مجتمع تكنولوجيا المعلومات IT Technology".
- ما معنى الأمن السيبراني؟ موقع " هارفارد بزنس ريفيو Harvard Business Review".
- أهمية الأمن السيبراني وكيفية تحول المعلومات إلى أموال. كرم ألكن. صحيفة "Daily Sabah".
- ما هو الأمن السيبراني؟ د. فاطمة عبدا لله ألدربي. صحيفة "البيان".
- ما المقصود بالأمن الالكتروني؟ موقع "Kaspersky".