مقدمة بحث كامل عن الأمن السيبراني

إنّ الأمن السيبراني هو أحد أبرز عوامل الدفاع عن أنظمة الحواسيب والأجهزة المحمولة والخوادم، وغيرها من الأنظمة الإلكترونية، وهو ضروري جداً لحماية البيانات والشبكات من الهجمات الخبيثة، يمتاز بطرائق خاصة في مجال الحوسبة، وتصميم وبنية أمنية قوية وفعالة، وفي هذا البحث سيتمّ التعرف على مفهوم هذا الأمن ونشأته، وذكر نبذة كاملة عن أنواعه وأهدافه وغيرها من المعلومات الوفيرة عن الأمن السيبراني.

بحث كامل عن الأمن السيبراني

لطالما عرف الأمن السيبراني كونه فرعاً من فروع التكنولوجيا التي عرفت بين الناس باسم أمن المعلومات، حيث يتضمن حماية المعلومات والبيانات والشبكات من السرقة أو الإلتلاف، وفيما يأتي سيتمّ تقديم بحث كامل عن الأمن السيبراني.

مفهوم الأمن السيبراني

الأمن السيبراني أو بالإنجليزية cyber security أو ما يُعرف باسم أمن المعلومات الإلكترونية أو أمان تكنولوجيا المعلومات، وهو من الأنظمة التي تعمل على الحماية والدفاع عن المعلومات والبيانات الإلكترونية الخاصة بأجهزة الكمبيوتر والخوادم والأجهزة الذكية المحمولة، كذلك تمارس الدفاع ضدّ الهجمات الإلكترونية على الشبكات والبيانات ضمن الأنظمة الإلكترونية، وينقسم هذا النظام الدفاعي إلى عدّة فئات أو عدّة أقسام مختلفة يتولّى كلّ قسمٍ منها مهماتٍ معيّنة، منها الدفاع ضدّ البرامج المتطفلة والفيروسية والحفاظ على البيانات والبرامج والأجهزة بعيداً عن التهديدات والهجمات والمخترقين، كذلك الحفاظ على خصوصية بيانات المستخدمين وحمايتها من التلف عند نقلها أو في حالة حدوث الكوارث وغيرها.

نشأة الأمن السيبراني

قد سُجّل أوّل ظهور للأمن السيبراني في عام ١٩٧٠، حيث طُرح مشروع الأمن السيبراني في الوسط بعد عدّة عقود من اختراع الحواسيب، وكان المشروع نامياً متناسباً مع بيانات الحواسيب التي لم تكن تُستخدم إلا من قبل هيئاتٍ معيّنة، ولم يكن انتشارها واسعاً كما الآن، فكان من السهّل التعرف على نواحي الهجمات ومصدرها لو حدثت، ومن ثمّ تمّ تطوير هذا المشروع في الثمانينات نتيجة انتشار الحواسيب والأنظمة الإلكترونية بشكلٍ أوسع، ممّا مهّد إلى هجماتٍ متطورة أكثر لسرقة البيانات واختراقها، كذلك بسبب اختراع أوّل نظامٍ فيروسيّ يسبب بدمار البيانات في الخوادم، وفي تسعينيات القرن الماضي بدأ التطور الهائل في الأجهزة الإلكترونية والأنظمة الافتراضية، وتزامن ذلك مع تطور البرامج الفيروسية والهجمات الإلكترونية، لذا تمّ تطوير بروتوكولات الحماية للمواقع الإلكترونية، والتي من خلالها يستطيع المستخدم الوصول للبيانات المحفوظة بشكلٍ آمن دون التعرض لخطر الفيروسات والسرقة لبياناته الخاصة.

أنواع الأمن السيبراني

توجد العديد من الأنواع للأمن السيبراني، والتي سيتمّ التعرف عليها فيما يأتي، وهي:

- **أمن الشبكات:** وهو يعمل على حماية خصوصية الجهاز الإلكتروني الخاص بالمستخدم من الهجمات والفيروسات التي قد تكون متواجدة ضمن الشبكات أو خارجها، وأهمّ التطبيقات فيه هو جدار الحماية الذي يتمّ تشكيله افتراضياً ليكون بمثابة الحاجز الذي يمنع انتقال البيانات الخاصة من جهازٍ إلى غيره من الأجهزة التي تعمل ضمن الشبكة الإلكترونية الواحدة، كذلك يحمي البريد الإلكتروني الخاص بالمستخدم من الاختراق أو التلف.
- **أمن التطبيقات:** ويكون من خلال الحماية الموجودة في مختلف التطبيقات التي يمكن استخدامها على الأجهزة الإلكترونية، وتتمثل في كلمات المرور وعمليات المصادقة، كذلك الأسئلة والأدوات التي تُطرح على المستخدم عند فتح التطبيقات الجديدة.

- **الأمن السحابي:** وهي برامج سحابية تعمل على حماية البيانات المخزنة على شبكة الإنترنت، حيث توفر الحماية والخصوصية اللازمة لبيانات كلِّ مستخدم، حيث لجأ الكثير من النَّاس بعد انتشار الشبكات الإلكترونية لتخزين البيانات الخاصة بهم على شبكة الإنترنت، فلا بدَّ من حمايتها وحفظها.
- **الأمن التشغيلي:** وهو الأمن الخاص بأنظمة الحماية السيبرانية، حيث يتكوَّن من أنظمة حماية داخلية يعمل عليها خبراء إدارة المخاطر، وذلك للحصول على الخطط البديلة لاستعادة المعلومات الخاصة بالمستخدمين إذا ما تعرَّضت للهجمات الإلكترونية، كذلك يتضمَّن برامج توعية للموظفين في حالات الطوارئ ليعملوا على أفضل الممارسات لتجنُّب المخاطر الإلكترونية.

أهداف الأمن السيبراني

سيتمَّ في الآتي الحديث عن الأهداف التي من أجلها تمَّ تطوير نظام الحماية والأمن السيبراني، حيث يسعى الأمن السيبراني لخلق أفضل أنظمة الحماية للحفاظ على معلومات المستخدمين وبيانات الأجهزة محمية ضد الخرق والسرقة والضياع والتلف.

توافر البيانات

ويُستخدم فيها الحماية المادية والدعم الاحتياطي الحاسوبي، حيث يشير هذا الهدف إلى توفير المعلومات للمستخدم في وقت سريع ومناسب، ويضمن أن تصل المعلومات والبيانات إلى المستخدم المصرَّح له بالوصول فقط إليها، لنسخها أو تعديلها أو سحبها.

النزاهة

النزاهة تعني الوصول للمعلومات ذاتها في كلِّ مرّة، خاليةً من التشويه والتحريف والتعديل غير المصرَّح به من قبل المستخدم، فتضمن وصول المعلومة الحقيقية للمستخدم وذلك من خلال تطبيق النسخ الاحتياطية للبيانات والمعلومات ومجاميع الاختبار ووضع رموز تعديل لمعلومات والبيانات الخاصة بالمستخدم.

السرية

يوفر الأمن السيبراني حماية خصوصية المستخدم، ومنع الآخرين من الوصول للمعلومات الخاصة به ومعرفة محتواها، كذلك يتمَّ من خلالها تجنُّب الكشف غير المصرَّح به عن المعلومات وتعديلها ونقلها، وذلك يكون من خلال تشفير البيانات وعمليات المصادقة وكلمات المرور والتحكُّم بصلاحيات الوصول للبيانات والتفويض والأمن المادي.

مشاكل الأمن السيبراني

تواجه النظام الأمني السيبراني الكثير من المشاكل والتحديات وهو أمرٌ طبيعيٌّ، فلا بدَّ من وجود بعض التَّغرات في تطبيقات الحماية، ومن أهمَّ المشاكل نذكر الآتي:

- زيادة تعقدي وتطور الهجمات الإلكترونية على البيانات.
- انتشار عمليات الاحتيال من خلال إخفاء هوية المستخدمين.
- نقص الخبراء والمطورين في قطاع الأمن السيبراني.
- انهيار أنظمة الحماية بسبب استخدام الاتصال غير الآمن بالإنترنت.
- استخدام الروبوتات الآلية لنشر المعلومات الخاطئة.
- كثرة عمليات الاحتيال والسرقة الإلكترونية والخداع وتطورها.
- زيادة الهجمات الإلكترونية كسرقة بيانات محطات المياه والكهرباء وغيرها.
- استخدام مواقع التواصل الاجتماعي التي تتيح الدخول إلى معلومات المستخدم بكل سهولة.

أهمية الأمن السيبراني

تكمُن أهمية الأمن السيبراني في الحماية والدِّفاع عن الأنظمة البيانية والمعلومات الخاصة ضد السرقة على المستوى العالمي والفردي، فهذا الأمن يحمي معلومات المؤسسات كالمستشفيات والمدارس والشركات وغيرها، كذلك يعمل على حماية بيانات الفرد بحيث يحفظها ضدّ كافة المخاطر والأضرار، من خلال أنظمة الدِّفاعات الإلكترونية المتقدمة، فتحمي المستخدمين من السرقة والابتزاز والجرائم الإلكترونية الأخرى.

خاتمة بحث كامل عن الأمن السيبراني

وفي ختام هذا البحث لا بدّ من التنويه على أهميّة الأمن السيبراني لحماية الصناعات المختلفة وغيرها من البرمجيات التي تعمل أنظمة الحاسوب، فهو جوهره يتعلّق بسلامة الحاسوب وجميع البيانات المحفوظة في ذواكره وعلى أنظمتها، نسال الله القدير أن ينفعنا وإياكم بما كتبتناه من المعلومات الوفيرة في بحثنا هذا، والسلام عليكم ورحمة الله وبركاته.