بحث عن الأمن السيبراني

مع التقدم التكنولوجي في شتى المجالات، زادت عمليات الاختراق والسرقة، مما دفع المُبرمجين لوضع الاستراتيجيات التي تحمي الأنظمة والشبكات من الهجمات الرقمية، وبعد مراحل كثيرة من التطور جاء مفهوم الأمن السيبراني.

عناصر البحث

- مقدمة بحث عن الأمن السيبراني.
- ما هو الأمن السيبراني؟
- 53 عام من تطور الأمن السيبراني.
- أنواع الأمن السيبراني.
- خصائص الأمن السيبراني.
- أهمية الأمن السيبراني.
- تهديدات الأمن السيبراني.
- خاتمة البحث.

مقدمة بحث عن الأمن السيبراني

تكمُن قوة الشركات في ثرواتها، تلك المُعرضة للاختراق، وبفقدها تفقد الشركات أموالًا كثيرة، فكان يجب حماية أجهزة الكمبيوتر والخوادم، والهواتف، وبدأ مجال أمن المعلومات منذُ بداية البشرية لا سيّما العمليات العسكرية، حتى تطور للأمن السيبراني.

ما هو الأمن السيبراني؟

يكمُن عمل الأمن السيبراني في حفظ أجهزة الكمبيوتر، والشبكات، وكافة الأنظمة التي تضُم البيانات المُهمة المُعرضة للتهديدات الرقمية.

لذا تسعى كافة المؤسسات العمل بجدّ حفاظًا على ثقة العملاء، وحماية البيانات الحساسة، ومنع الانقطاعات التجارية بسبب انقطاع الشبكة، وهي بالدفاع الرقمي بين العمليات والتقنيات.

53 عام من تطور الأمن السيبراني

مرّ الأمن السيبراني بكثير من المراحل حتى تطور ليومنا هذا، باختراعات أفادت البشرية وكانت لها نقلة نوعية في التكنولوجيا، لا سيّما مع انتشار الإنترنت.

1- سبعينيات القرن العشرين

- اخترع العالِم بوب توماس برنامج "Creeper"، ينتقل عبر شبكة "ARPANET'S".

2- ثمانينات القرن العشرين

- أنشأ راي توملينسون -مُخترع البريد الإلكتروني- برنامج "Reaper" الحديث عن غيرِه، وأصبح هو أول وأفضل البرامج المُكافحة للفيروسات.
- لكن تسبب في أعطال بالأنظمة، حتى حُكِم على راي بالحبس ودفع غرامة.

3- تسعينات القرن العشرين

- انتشر الإنترنت، وتطورت الأجهزة حتى أصبحت تُستخدم بشكل واسع، ولهذا كان لا بُد من إنشاء البروتوكولات التي تحمي المواقع الإلكترونية مثل "http"، وهذا يُساعده للوصول بأمان للشبكة.

أنواع الأمن السيبراني

1- الأمن السحابي (Cloud Security)

لذيوع استخدام تكنولوجيا الذكاء الاصطناعي والسحابات التخزينية، فكان لا بُد من حماية البيانات التي تحتويها، وقدمت شركات في هذا المجال خدمات لحل ما يواجه العُملاء:

- Google Cloud.
- Microsoft Azure.

2- أمن المعلومات (Information Security)

إن عميات النقل والتخزين ونشر البيانات مُعرضة للتلف، أو التعديل، أو التعطيل، وهُنا يكمُن عمل أمن المعلومات.

3- أمن الشبكات (Network Security)

ثمَّة مُتطفلين لاختراق البيانات المدوّنة على شبكات الحاسوب، سواء كانوا أفراد مُستهدفين، أو برامج انتهازية ضارة، ويشمل الأمن هُنا أنواع عِدة:

- برامج مكافحة الفيروسات.
- البرامج الضارة.
- جدار الحماية.
- تأمين البريد الإلكتروني.

4- أمن التطبيقات (Application Security)

هذا النوع هو ما يُركز على حماية البرامج من كافة الفيروسات الضارة، والمُهددة لبيانات الجهاز، وفي مرحلة التصميم يتم تنفيذ كافة إجراءات الأمان.

5- الأمن التشغيلي (Operational Security)

إن كان المخاطر الداخلية للأمن السيبراني يُركز عليها هذا النوع، فيُعالج أصول البيانات، ويحميها من الاختراق، بتحديد الإجراءات اللازمة لكيفية وموقع تخزين أو مُشاركة البيانات.

خصائص الأمن السيبراني

- **الثقة:** إنه يُساعد الجهاز على تحميل البرامج أو الدخول للمواقع الموثوق منها عدم الإضرار بالجهاز، وتمنع البرامج الخبيثة المُتطفلة، أو تلك التي تستغل الثغرات للحصول على البيانات.
- **الحماية:** فيحفظ الجهاز من كافة تهديدات المخاطر الخارجية، من الرسائل الإلكترونية الخطيرة والخبيثة المُستهدفة بالفيروس، والمخاطر الداخلية الناجمة عن اللمس غير الآمن من المُستخدم.
- **المُراقبة:** إن نظام الأمن السيبراني يعمل طوال الوقت لسُرعة اكتشاف أي خلل يُلحق بالجهاز، وإصلاحه على الفور قبل الإضرار ببياناتُه.
- **التنوع:** يجد النظام حلول كثيرة للتعامُل مع كافة التهديدات التي تهز سلامة أمن المعلومات.
- **الالتزام بالقوانين:** هدف الأمن السيبراني هو حماية البيانات الهامة، وسرية الخصوصية، ولكن هذا جميعه لا يخرج عن إطار القوانين والسياسات التشريعية لأمن المعلومات.

أهمية الأمن السيبراني

يأتي الاعتماد الأول في شتى المجالات على الإنترنت، لذا لا بُد من حفظ البيانات والاتصالات الإلكترونية أكثر من أي وقت مضى، وهُنا تعزى الحاجة للأمن السيبراني، لزيادة الاعتماد على التكنولوجيا، والحماية من الاختراقات والقرصنة.

إلى الآن، ما زالت الجرائم الإلكترونية التحدي الكبير في القطاع التكنولوجي؛ لذا سيحتاجون لوجود أنظمة أمان من التهديدات الضارة، وهُنا لا بُد من التوعية بأهمية الأمن السيبراني لجميع مُستخدمين الإنترنت، لا سيّما بزيادة أعدادهم يوميًا.

تهديدات الأمن السيبراني

برغم أهميته، إلا أن له كثير من المخاطر، والتي ازدادت بشكل بيّن في السنوات الماضية مع كثرة اختراقات البيانات في شتى القطاعات، ومما يواجه:

- كثرة البرامج الضارة، والمواقع التي تُصيب الجهاز بفيروس يُهدد أمان المعلومات.
- سهولة سرقة كلمات السر للتطبيقات، وإيميلات المُستخدمين.
- هجوم DDoS من منصات معروفة يعملون بها.
- التنصت على الاتصالات، باختراق أجهزة الكمبيوتر، وهو ما يعود بعواقب وخيمة على الأفراد والشركات.
- تصيد المجرمون لمُستخدم بعينِه؛ للوصول للمعلومات الشخصية أو المالية بالتنكُر في هيئة كيانات موثوق بها.

- كثرة هجمات ثقب المياه المُستهدفة لنقاط ضعف الأنظمة والشبكات، فيسهل لها اختراق الجهاز لا سيّما عبر حسابات التواصل الاجتماعي.

خاتمة البحث

نحنُ في عصر الإنترنت المفتوح على مصراعيه، مع ازدياد عدد المُستخدمين يوميًا، تزداد عمليات الاختراق والقرصنة، فكان لا بُد من حفظ ثقة العُملاء بحماية بياناتهم الهامة، تلك التي ساعدت على توسع الإنترنت في شتى المجالات.

يتميز القرن العشرين بالابتكارات الصناعية، والميكانيكية، والتكنولوجية.. ساهمت في توسع غيرِها من المجالات، حتى أصبح العالم قرية صغيرة ناجحة مُحققة إنجازات كثيرة مُبهرة.