بحث عن أمن المعلومات

مع التقدُم التكنولوجي والاعتماد عليها في شتى المجالات، أصبح الاهتمام بأمن المعلومات من أهم القضايا التي ولىَ المُبرمجين نصب تركيزهُم عليها؛ حفاظًا على البيانات والمعلومات الخاصة بكافة المُستخدمين.

عناصر البحث

- مقدمة بحث عن أمن المعلومات.
- تعريف أمن المعلومات.
- تاريخ أمن المعلومات.
- أنواع أمن المعلومات.
- عناصر أمن المعلومات.
- تدابير أمن المعلومات.
- تحديات أمن المعلومات الآن!
- مجالات أمن المعلومات.
- خاتمة البحث.

مقدمة بحث عن أمن المعلومات

مع التقدُم التكنولوجي الذي شهدهُ العالم، زادت عمليات القرصنة والاختراق، على كافة مواقع التواصل الاجتماعي، فكان لا بُد الحفاظ على معلومات المُستخدمين والبيانات المتداولة.. من هُنا جاء الاهتمام بأمن المعلومات.

تعريف أمن المعلومات

ثمَّة عمليات تُقام من أجل حماية معلومات المُستخدمين من الأخطار، مثل: "السرقة، الاختراق، التخريب.. وغيرها"، هذا هو أمن المعلومات.

إنه يعتمد على حماية كافة أنواع وأماكن المعلومات، لكن يجب أن تُحدد السياسة المُتبعة إمّا من الشركة، أو الفرد المالك للمعلومات.. بالسماح بالطريقة الأفضل له.

تاريخ أمن المعلومات

مُنذ بداية التواصل عن بُعد، لا سيّما في فترة الحروب، ظهرت الحاجة لحماية المعلومات العسكرية من اختراق العدو، والحصول على البيانات اللازمة، فهذه كانت الغاية من أمن المعلومات.

للحفاظ عليها من السرقة، حتى تطورت لتشمل المعلومات السيبرانية والتقنيات الإلكترونية كاملة، فبدأ بحمايتها بتشفير المعلومات، وابتكار شيفرات سرية منعًا لاختراقها من السارق بسهولة.

مع التقدُم التكنولوجي في العالم، أصبحت طرق الحماية أكثر تعقيدًا بوسائل تشفير فعّالة، وهُنا كان التواصل أكثر أمانًا لكافة المعلومات دون الخوف من العدو واختراقُه للبيانات.

- تبنّت المخابرات الأمريكية "CIA" مبدأ أمن المعلومات، فلم يتمكن سواء الأعداء أو الفضوليين من الوصول للمعلومات السرية.
- اتخذت السياسية المُتبعة للحماية شكلها الحالي مع التطور التكنولوجي وظهور الإنترنت واختراع الحواسيب بكافة أنواعها.

أنواع أمن المعلومات

- أمن وسائل التخزين السحابي: هو رفع المعلومات عبر الإنترنت للاحتفاظ بها، والرجوع لها في أي وقت ومكان، لكن هذا النوع خطير ومُعرض للاختراق الإلكتروني.
- التشفير: هي الوسيلة المُتبعة منذُ القِدَم، ولكن الآن اشتمل على كافة أنواع المعلومات، فتُشفر المعلومة لرموز يصعب فهمها سوى من قِبل الجهات التابعة لها.
- أمن البرمجيات والتطبيقات: ثمَّة تطبيقات مُختلفة عبر الإنترنت مُعرضة للاختراق، وهذا النوع هو ما يُكافح كافة أنواع الاختراق.
- البنية التحتية الصلبة: شمس أمن المعلومات الأجهزة والأدوات المخولة بحفظ البيانات، مثل الحواسيب، وهُنا تقلّ فُرص السرقة والاختراق.
- مقاومة الثُغرات الأمنية: تُحاكى هُنا عمليات السرقة ونسب حدوثِها، فتحاول قدر الإمكان عدم حصولها وحفظ المعلومات.

عناصر أمن المعلومات

١- تأمين المعلومات للوصول لها

إخفاء المعلومات لحمايتها من الاختراق والسرقة يصعب عملية الوصول لها، إلا أن أمن المعلومات يحميها من السرقة ويوفر للمُستخدمين المخولين بالوصول لها الطرُق السلسة.

٢- سرية المعلومات

التشفير للمعلومات يؤمن عدم القدرة للوصول لها دون اختراق، فكانت الوسائل لحفظها في سرية:

- إنشاء كلمات مرور قوية، من أرقام ورموز وحروف.
- تشفير المعلومات إلى رموز لا سيّما عند إرسالها وتبادُلِها.
- المستشعرات الحيوية، مثل وضع البصمات، وقرنية العين للتعرف من خلالها.

٣- حفظ المعلومات من البرامج الضارة

لا يحفظ أمن المعلومات ما يدوّن فقط من الاختراق، بل وأيضًا من البرامج الضارة التي تؤدي لتخريبها أو فقدها، فيحتاج للاحتفاظ بنسخ احتياطية آمنة تُحفظ من أي تلف.

تدابير أمن المعلومات

إن الشركات كانت أكثر حرصًا مؤخرًا لحفظ معلوماتها من الاختراق، فكانت التدابير اللازمة:

١- الاهتمام بالكفاءات البشرية

- انتقاء مسؤولين الأمن السيبراني بدِقة، ليكونوا أكثر دقة في تقديم الأفضل.
- زيادة وعي الموظفين بأهمية الحفاظ على أمن المعلومات، وكيفية التعامُل مع عمليات الاختراق.

٢- التنظيم والتخطيط

تُرسم هيكلة شاملة لبرنامج أمن المعلومات، على أن يُحدد الشيفرة المُناسبة، والأشخاص المخول لهم بالوصول إلى البيانات.. صلاحيات كثيرة تُحدد.

٣- الأمن الرقمي

إن الشركات تعتمد في تثبيت كافة الأحداث من برامج حماية الفيروسات، ليصعب اختراقها بكافة الأشكال، فتكون محمية في سرية تامة، وتُحذف أي برامج ضار عند تنزيلها مُباشرةً.

٤- تحديد الخطة المالية

تختلف الإمكانيات المادية من شركة لأخرى، فلا بُد أخذها في الاعتبار عند اختبار الخبراء البرمجيات المُناسبة لحماية المعلومات، وتُقدم ندوات لتوعية العاملين بالقدر المُناسب لهم ماديًا.

تحديات أمن المعلومات الآن!

- سيفٌ ذو حدين.. التقدُم التكنولوجي؛ لأنه يزيد من عدد المُخترقين ويُساعدهم على اكتشاف الثُغرات الأمنية التي توصلّهُم إلى معلومات سرية وتُعرضها للسرقة.
- الفيروسات، البرمجيات الخبيثة التي تُلحق الضرر بالملفات، وقد تؤدي لتلفها، وتحتاج لتطور دائم في برامج مقاومة الفيروسات وإلا يتملكون منها.

- التجسس دون اختراق للأجهزة المعنية بحماية المعلومات، مثل الاستعانة بالكابل فيتسبب في إظهار ما خُفيّ.
- يتجه بعض المخترقين إلى انتحال شخصيات المخول لهم الوصول إلى المعلومات السرية، وهذه الأصعب تعامُلًا، فيصعب كشفهم ومنعهم من الاختراق والسرقة.

مجالات أمن المعلومات

المجال	المهام
مسؤول أمن المعلومات Security specialist	المُختص والمالك للخبرة الكبيرة في مجال أمن المعلومات.
مهندس أو مسؤول تحليل البيانات الأمنية Security analyst/engineer	يتتبع محاولات الاختراق.
مختص إدارة المخاطر Chief risk officer	المسؤول عن تقييم حالة الشركات، وتحديد نقاط الضعف والقوة.
المخترقون الأخلاقيون Ethical hackers	المسؤولون عن الإلمام بطرق تفادي الاختراق.
مسؤول أمن الشبكات Web security manager	هو المسؤول عن حماية المعلومات وتخزينها بشكل سري.
مسؤول البرمجيات والتطبيقات Apps Specialist	المُكلّف بمهام حفظ المعلومات على مواقع التواصل والتطبيقات المُختلفة.

خاتمة البحث

مع التطور التقني الكبير الذي يشهده العالم بالكامل اليوم، ولى الاهتمام الكبير لمجال أمن المعلومات حفاظًا على معلوماتهم الشخصية، والمهنية.. ومعه شهد هذا المجال تطور كبير.

واحدًا من المجالات المُهمة في كافة المِهن، فالسرية أصبح مُتطلب في شتى الأعمال! لذا فانتقاء أمن المعلومات للدراسة والتعمُق اختيارٌ صائب.