العطاء الرقمي
Attaa Digital

أمن الشبكات والامن السيبراني

العطاء الرقمي
Attaa Digital

العطاء الرقمي
Attaa Digital

الأمن السيبراني مصطلح لا يساوي ولا يعني أمن المعلومات إطلاقاً

م . صالح بن عبدالله الشمري

- ماجستير علوم حاسب مرتبة الشرف الاولى
- بكالوريوس هندسة حاسب
- متخصص في امن الشبكات والامن السيبراني
- خبرة 20 سنة في تقنية المعلومات
- حاصل على العديد من الشهادات المهنية في مجال الشبكات وامن المعلومات
- CCNA ,CCNP , CISSP, PMP, security + ,ITILv3 , F5 consultant
- مدرب معتمد من المؤسسة العامة للتدريب المهني والتقني في مجال تقنية المعلومات
- حاصل على شهادة TTTالتدريب واعداد المدربين
- دورة امن المعومات في هيئة المهندسين السعوديين
- دورات ومحاضرات توعوية

مستشار أمن معلومات وشبكات وامن سيبراني ، مدرب معتمد

0555161888
salnahi@gmail.com

اجندة المحاضرة

تعريف امن الشبكات والامن السيبراني

امن الشبكات وايجابيات وسليبات

الاختراق والهجمات الالكترونية

نصائح في امن الشبكات

مستقبل الامن السيبراني

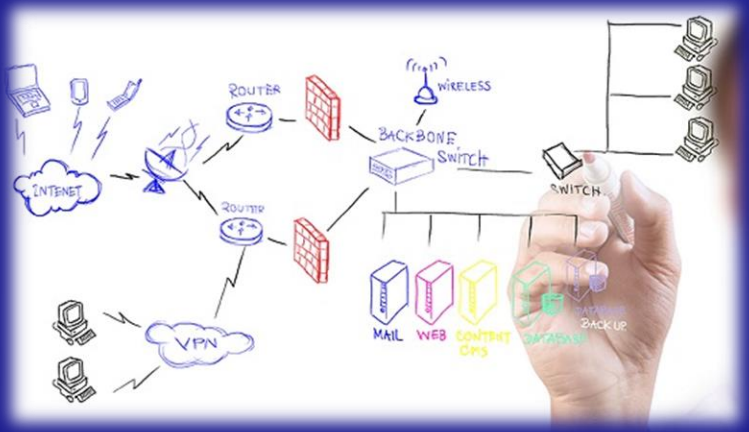
أسئلة الحضور

تعريف امن الشبكات والامن السيبراني

أمن الشبكات

أي نشاط تم تصميمه لحماية استخدام وسلامة شبكتك وبياناتك.
ويشمل هذا المجال كلا من تكنولوجيا الأجهزة والبرمجيات.

يدير أمن الشبكات الفعال إمكانية الوصول إلى الشبكة ويستهدف مجموعة متنوعة من التهديدات ويمنعها من الدخول إلى شبكتك أو من الانتشار.



كيف يعمل مجال أمن الشبكات ؟

يجمع أمن الشبكات بين طبقات متعددة من الدفاعات في الشبكة و على حافتها.

حيث تقوم كل طبقة أمن الشبكات بتنفيذ السياسات وعناصر التحكم.

يحصل المستخدمون المخول لهم على إمكانية الوصول إلى موارد الشبكة،

ولكن يتم منع الجهات الفاعلة الخبيثة من تنفيذ عمليات الاستغلال والتهديدات.

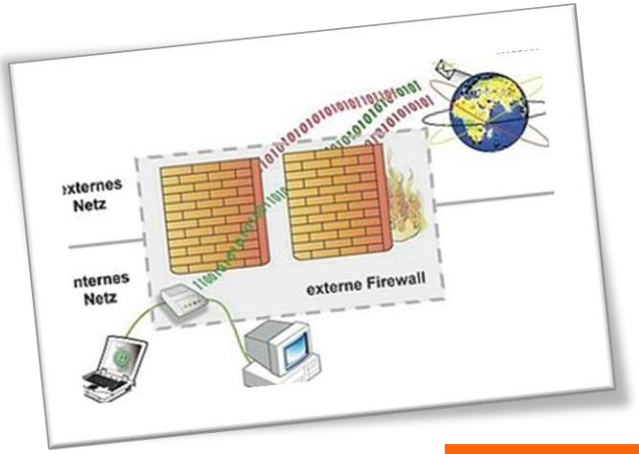
كيف أستفيد من أمن الشبكات ؟

لقد حولت الأرقام عالمنا، حيث تغير كل شيء؛ طريقة عيشنا، عملنا، لعبنا و تعلمنا.

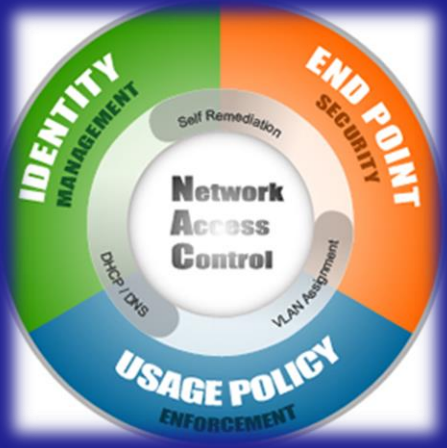
لذا، و في ظل عالم الأرقام هذا، يجب على كل مؤسسة ترغب في تقديم الخدمات التي يطلبها عملاءها وموظفوها حماية شبكتها.

هنا تظهر أهمية أمن الشبكات، حيث يساعد المؤسسات على حماية معلومات الملكية من الهجوم.

أمن الشبكات هو مجال يحمي مكانتك و سمعتك.



أنواع أمن الشبكات



1- التحكم في الوصول NAC

يجب ألا يكون لدى كل مستخدم حق الوصول إلى شبكتك.

لمنع المهاجمين المحتملين ، تحتاج إلى التعرف على كل مستخدم و على كل جهاز.

ثم يمكنك فرض سياسات الأمان الخاصة بك.

يمكنك حظر أجهزة نقطة النهاية غير المتوافقة أو منحها وصولاً محدودًا فقط.

تسمى هذه العملية Network Access Control

أي التحكم في الوصول إلى الشبكة

2- برامج مكافحة الفيروسات والبرمجيات الخبيثة

تتضمن البرمجيات الخبيثة

Malwareو هي اختصار لـ Malicious Software

الفيروسات والديدان وأحصنة طروادة وبرامج الفدية وبرامج التجسس.

تصيب البرمجيات الخبيثة الشبكة أحيانا ولكنها تظل كامنة لمدة أيام أو حتى أسابيع.

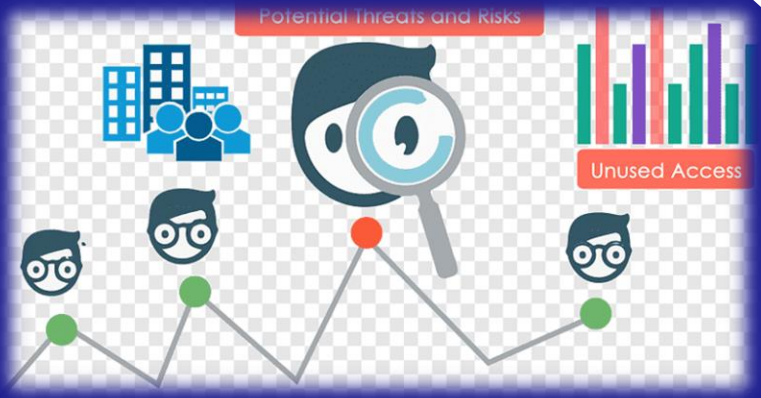
تقوم أفضل برامج مكافحة البرمجيات الخبيثة بفحص البرامج الضارة عند الدخول إليها فقط، بل تتبع أيضا الملفات بعد ذلك باستمرار للعثور على الحالات الشاذة وإزالة البرامج الضارة وإصلاح التلف.

3- أمان التطبيقات

أي برنامج تستخدمه لإدارة أعمالك يحتاج إلى الحماية ، سواء أكان فريقك لتكنولوجيا المعلومات يقوم ببناء تلك البرامج أو تقوم بشرائها.

قد يحتوي أي تطبيق على ثغرات، أو ثغرات أمنية، يمكن للمهاجمين استخدامها لاختراق شبكتك.يشمل أمان التطبيقات الأجهزة والبرامج والعمليات التي تستخدمها لإغلاق هذه الثغرات.

4- التحليل السلوكي



للكشف عن سلوك الشبكة غير الطبيعي، يجب أن تعرف كيف يبدو السلوك الطبيعي.

أدوات التحليل السلوكي تميز تلقائيا الأنشطة التي تحيد عن القاعدة.

يمكن لفريق أمن المعلومات: عندئذٍ تحديد مؤشرات التسوية التي تطرح مشكلة محتملة ومعالجة التهديدات بسرعة

5- منع فقدان البيانات

يجب على المنظمات / الجهات / الشركات

التأكد من أن موظفيها لا يرسلون معلومات حساسة خارج الشبكة.

يمكن أن تمنع تقنيات منع فقدان البيانات أو DLP

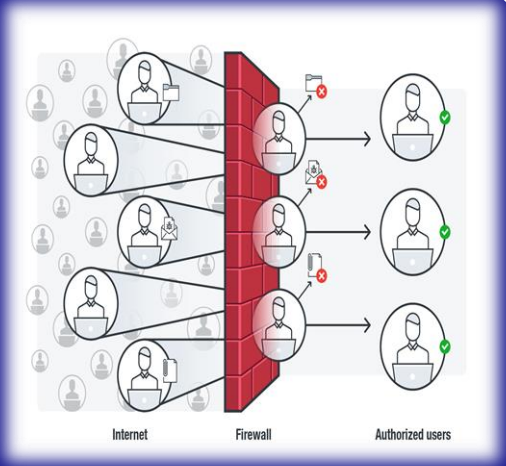
الأشخاص من تحميل أو إعادة توجيه أو حتى طباعة المعلومات المهمة بطريقة غير آمنة.

بوابات البريد الإلكتروني (Mail Gateway) هي ناقلات التهديد رقم واحد لخرق الأمان.

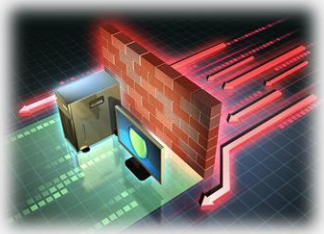
6- أمان البريد الإلكتروني

يستخدم المهاجمون المعلومات الشخصية وتكتيكات الهندسة الاجتماعية لإنشاء حملات تصيّد متطورة لخداع المستلمين وإرسالها إلى مواقع تخدم برامج ضارة.

يحظر تطبيق **أمان البريد الإلكتروني** الهجمات الواردة ويتحكم في الرسائل الصادرة لمنع فقدان البيانات الحساسة.



7- جدران الحماية Firewalls



وضعت جدران الحماية حاجزًا بين شبكتك الداخلية الموثوقة والشبكات الخارجية غير الموثوق بها، مثل الإنترنت.

تستخدم جدران الحماية مجموعة من القواعد المحددة للسماح بالزيارات أو منعها.

يمكن أن يكون جدار الحماية عبارة عن أجهزة أو برامج أو كليهما.

8- أنظمة منع التطفل

Intrusion Prevention systems (IPS)

Intrusion Detection and **Prevention Systems (IDPS)**

يقوم نظام منع التطفل IPS بفحص زيارات وحركة مرور الشبكة لمنع الهجمات بشكل فعال.

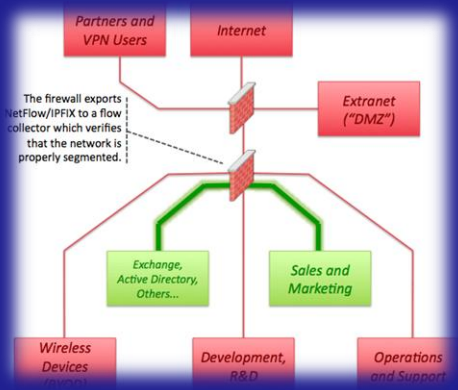
تعمل أجهزة (IPS (NGIPS من خلال ربط كميات هائلة من الذكاء العالمي للتهديد ليس فقط لمنع النشاط الخبيث بل أيضا لتتبع تقدم الملفات المشبوهة والبرمجيات الخبيثة عبر الشبكة لمنع انتشار التفشي وإعادة الإصابة مرة أخرى.

9- أمان الجهاز المحمول

يستهدف مجرمو الإنترنت بشكل متزايد الأجهزة المحمولة والتطبيقات.
في غضون السنوات الثلاثة المقبلة، قد تدعم 90 في المائة من مؤسسات تكنولوجيا المعلومات تطبيقات الشركات على الأجهزة المحمولة الشخصية.

تحتاج إلى التحكم في الأجهزة التي يمكنها الوصول إلى شبكتك. ستحتاج أيضًا إلى تهيئة اتصالاتها للحفاظ على خصوصية زيارات الشبكة.

10- تقسيم الشبكة



تضع البرامج المعرفة بالتقسيم زيارات الشبكة ضمن تصنيفات مختلفة وتجعل فرض سياسات الأمان أكثر سهولة.

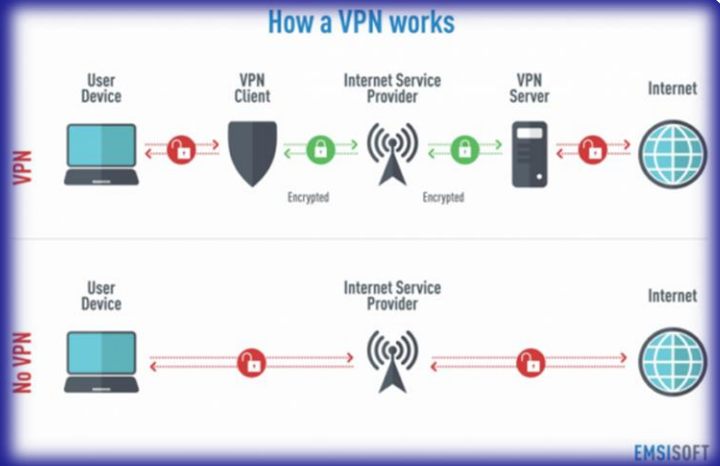
من الناحية المثالية، تعتمد التصنيفات على هوية نقطة النهاية، وليس على مجرد عناوين IP.

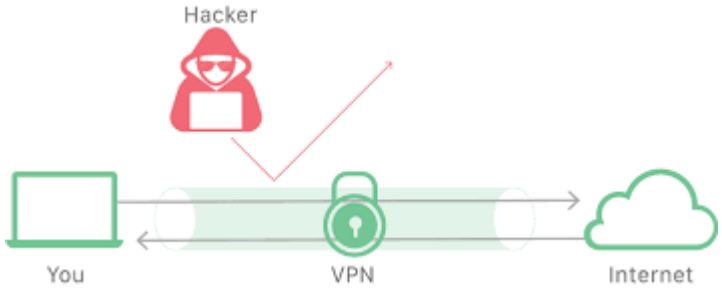
يمكنك تعيين الوصول المناسب استنادًا إلى الدور والموقع وأكثر من ذلك بحيث يتم منح المستوى المناسب للوصول للأشخاص المناسبين ويتم تضمين الأجهزة المشبوهة ومعالجتها.

11- معلومات الأمان وإدارة الأحداث

SIEM

تجمع منتجات SIEM المعلومات التي يحتاجها أفراد الأمن لديك لتحديد التهديدات والاستجابة لها. تأتي هذه المنتجات بأشكال مختلفة، بما في ذلك أجهزة مادية وافتراضية وبرامج الخادم.





VPN -12

Virtual **P**rivate **N**etwork

تقوم شبكة خاصة افتراضية VPN بتشفير الاتصال من نقطة نهاية إلى شبكة، غالبًا عبر الإنترنت.

عادةً ما تستخدم VPNالوصول عن بعد IPsecأو طبقة Sockets الآمنة لمصادقة الاتصال بين الجهاز والشبكة.

فمفهوم VPNشبكة تخلق شبكة خاصة داخل شبكة عمومية، مثل الإنترنت

13- أمن الويب

سيعمل حل أمن الويب على التحكم في استخدام موظفيك على الويب ومنع تهديدات الويب ومنع الوصول إلى مواقع الويب الضارة. سيحمي أمن الويب بوابة الويب خاصتك في الموقع أو في السحابة.

يشير "أمن الويب" أيضًا إلى الخطوات التي تتخذها لحماية موقعك على الويب.

14- أمن الشبكات اللاسلكية

الشبكات اللاسلكية ليست آمنة مثل الشبكات السلكية.

وبدون إجراءات أمنية صارمة، يمكن أن يكون تثبيت الشبكة المحلية اللاسلكية LANمثل وضع منافذ Ethernet في كل مكان ، بما في ذلك مكان الانتظار.

لمنع الاستغلال من الاستيلاء ، تحتاج إلى منتجات مصممة خصيصًا لحماية شبكة لاسلكية.

الامن السيبراني

الامن السيبراني

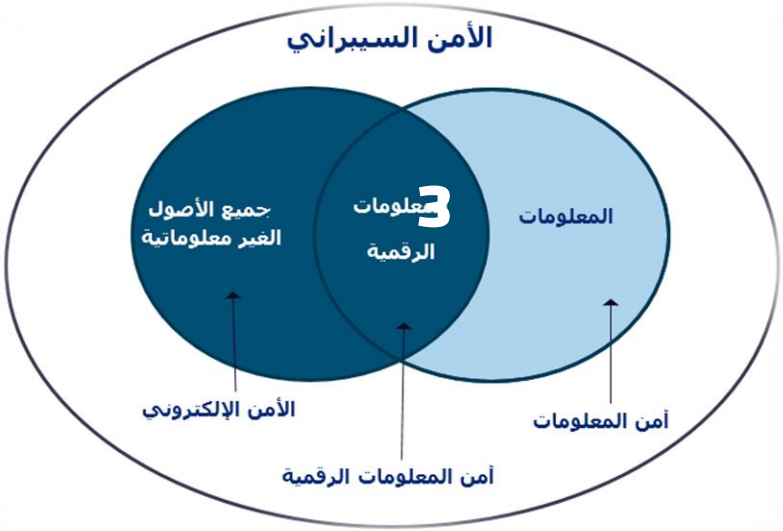
هو الأمن الذي يتعلق بالحماية من الأخطار الخارجية المحتملة والخاصَّة على الإنترنت .

حيث يعمل مختصو الأمن السيبراني على حماية الحواسيب المكتبية أو الهواتف المحمولة من أيِّ نوع من الهجمات والاختراقات والتهديدات التي قد تحدث، عن طريق السيرفرات .

حيث يوفِّر محترفي الأمن السيبراني الحماية للشبكات والخوادم والشبكات الداخلية وأنظمة الكمبيوتر.

امن الشبكات والمعلومات والامن السيبراني

ما الفرق بين الأمن السيبراني وأمن المعلومات والشبكات ؟



ما الفرق بين الأمن السيبراني وأمن المعلومات؟

على الرَّغم من أنَّ الأغالبية يعتقدون أنَّهما مصطلحان لنفس المفهوم ألا وهو **حماية المعلومات**

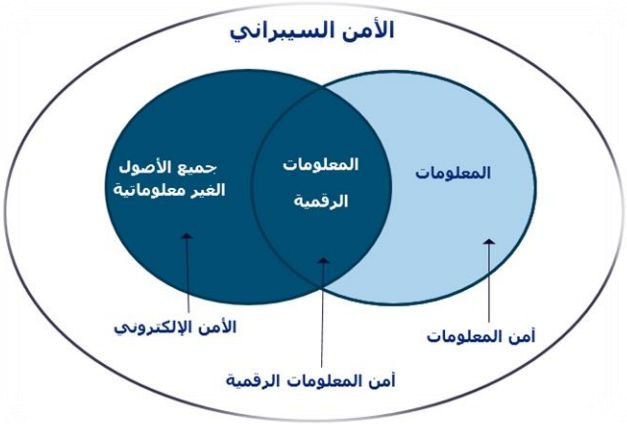
بما أنَّ المعلومات لا تحتاج أن تكون محفوظة على الحاسوب حتى تحتاج للحماية بل قد توجد أيضاً ضمن أحد الملفات

- الأمن السيبراني يهدف إلى حماية المعلومات من قبل أيِّ مصادر خارجية من تعرُّضها للسرقة على شبكة الإنترنت،

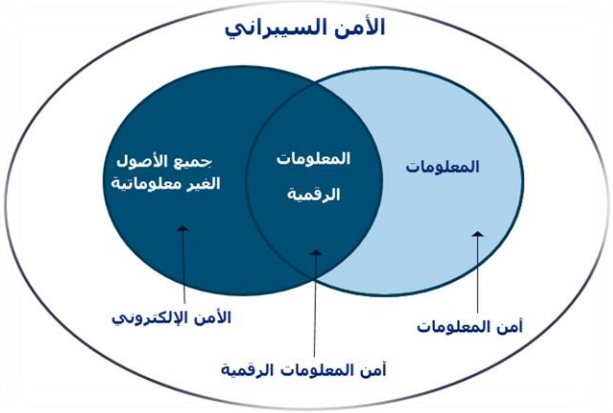
- أمن المعلومات يهتم بهذه المعلومات أينما كانت.

ما الفرق بين الأمن السيبراني وأمن المعلومات والشبكات ؟

- الأمن السيبراني مهتم بحماية معلوماتك من الأخطار الخارجية والوصول الخارجي لغير المصرَّح لهم بالوصول لهذه المعلومات، وهذا يشمل حماية البيانات الشخصية مثل الحسابات الشخصية على مختلف مواقع التواصل الاجتماعي
- يهتم أمن المعلومات بسرية المعلومات وتوافرها، وقد يشمل ذلك المعلومات غير الإلكترونية أيضاً.
- لسيطرة التكنولوجيا على العديد من الجوانب المختلفة يتخذ أمن المعلومات شكله الأساسي ليوفِّر هذه الحماية التقنية للمعلومات كافة.



ما الفرق بين الأمن السيبراني وأمن المعلومات والشبكات ؟



تكون قيمة المعلومات وحمايتها نقطة اهتمام لنوعي الأمن (المعلومات والسيبراني)

- إلّا أنَّ الأمن السيبراني يركّز على الوصول غير المصرَّح به لهذه المعلومات.
- يركّز أمن المعلومات على سرية هذه المعلومات وتوافقها مع بعضها وتوافرها الدائم.

باختصار يمكن اعتبار الأمن السيبراني جزءً أو تخصّصاً من أمن المعلومات،
ويهتم القائمين على النوعين بكل ما يتعلَّق بحماية البيانات من الأخطار المختلفة
وبتشبيه آخر فالاختلاف يشبه الفرق بين العلم والكيمياء

ما الفرق بين الأمن السيبراني وأمن المعلومات والشبكات ؟

امن المعلومات	الامن السيبراني
حماية المعلومات من الاستخدام و الوصول و التعديل غير مصرح به	حماية البيانات من المصادر الخارجية على الإنترنت.
إنه يتعامل مع حماية البيانات من أي شكل من أشكال التهديد	حماية استخدام الفضاء الإلكتروني من الهجمات الإلكترونية.
لحماية المعلومات بغض النظر عن مكان وجودها او شكلها	لحماية أي شيء في عالم الإنترنت.
حماية البيانات من أي شكل من أشكال التهديد	يتعامل مع الخطر القادم من الفضاء الإلكتروني.
منع الوصول **غير المصرح به** وتعديل و اتلاف البيانات	يهاجم الأمن السيبراني جرائم الإنترنت والاحتيال عبر الإنترنت وإنفاذ القانون من خلال الوصول للمهاجمين و معاقبتهم

ايجابيات وسلبيات أمن الشبكات

الايجابيات

- القدرة على الحصول على اي معلومة ترغب معرفتها
- الرواتب مجزية
- يعتبر التخصص مطلوب في المستقبل
- توفر فرص العمل
- اكتساب الكثير من المهارات التفكير المنطقي
- تطوير الكفاءات ومستوى الاحترافية في مجال الحاسب

الايجابيات

- حماية البيانات والمعلومات من التسرب والسرقة والانتحال
- مواكبة التطور التكتولوجي
- الجد من الجرائم الالكترونية
- توفير مستوى متطور من الحماية
- استيعاب وفهم المسؤوليات المهنية والتقنية والقانونية وحتى الامنية

السلبيات

- يتطلب ضمان امن الشبكات وامن التطبيقات وامن البيانات
- صعوبة في التعامل مع بعض الاجهزة التقنية – مثلا الجدر النارية
- يؤدي امن الشبكات الى التقليل من سرعة البرمجيات
- التحديث المستمر ضد البرمجيات الخبيثة
- استهلاك الكثير من الوقت
- الحاجة الى خبرة عالية

الاختراق والهجمات الالكترونية

ما معنى الهجمات الالكترونية (الهجمات السيبرانية) ؟

خلال السنوات الماضية واجه امن الحاسب صعوبات شديدة بداية من سرقة البنوك ووصولا الى الهجمات شبه المفتوحة Semi-Open Attacks

تعريف الهجمات الالكترونية (الهجمات السيبرانية)

الهجمات الالكترونية عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الاجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات .
يمكن تقسيم الهجمات الالكترونية (الهجمات السيبرانية) الى نوعين رئيسيين على النحو التالي:

- هجمات يكمن الهدف من ورائها الى تعطيل جهاز الكمبيوتر المستهدف
- هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه.

انواع من الهجمات الالكترونية (الهجمات السيبرانية)

ومن اجل تحقيق تلك الأهداف في الوصول الى عمليات التشغيل او تعطيلها، يقوم مجرمو الفضاء الإلكتروني بنشر عدد من الوسائل التقنية المختلفة .

دائما ما تكون هناك وسائل جديدة مبتكرة ، وتتداخل بعض هذه الفئات لكن هذه هي المصطلحات التي ربما تسمعها كثيرا.

انواع من الهجمات الالكترونية (الهجمات السيبرانية)

- البرامج الضارة (البرمجيات الخبيثة) (Malware)
- التصيد (Phishing)
- حجب الخدمات ((Denial Of Service
- الرجل في المنتصف (Man in the middle)
- التعدين الخبيث Cryptojacking
- حقن هجوم SQL
- هجمات دون انتظار ((Zero-Day

انواع من الهجمات الالكترونية
(الهجمات السيبرانية)

- حصان طروادة (Trojans)
- هجمات الفدية (Ransomware)
- البرامج الضارة على تطبيقات الجوال
- خروقات البيانات

اشهر الهجمات السبرانية (الهجمات الالكترونية)

- هجوم WannaCry هو هجوم باستخدام برامج الفدية الضارة وانتشر سريعًا في مايو2017
- NotPetya كان هجوم Petyaمجرد جزء من أجزاء البرامج الضارة عندما بدأ تداوله عبر البريد العشوائي المتصيد في 2016
- Equifax إحدى وكالات التصنيف الائتماني الكبيرة أعلنت في يوليو 2017 أن مجرمون قد استغلوا ثغرةً بأحد مواقع الويب الأمريكية الخاصة بتقديم الطلبات للحصول على بعض الملفات،" وتمكنوا من الحصول على معلومات شخصية لحوالي 150 مليون شخصًا. وقد زادت النتائج المترتبة على ذلك من غضب الأشخاص، ولاسيما عندما كان موقع الويب

اشهر الهجمات السبرانية (الهجمات الالكترونية)

- **Yahoo** تم اختراق اكثر من 500 million accounts compromised في عام 2013-2014
- **GitHub** في 28 فبراير، 2018، تم اختراق الإصدار المتحكم في خدمة المضيف GitHub بهجوم حجب الخدمات، حيث تم إرسال بيانات بلغت 1.35 تيرابايت في الثانية إلى الموقع المشهور. ورغم أن GitHub قد تعرض فقط لعملية قطع اتصاله بالإنترنت بصورة متقطعة ورغم نجاحه في صد الهجوم كلياً بعد أقل من 20 دقيقةً، كانت الآثار الهائلة المترتبة على الاعتداء مثيرة للقلق؛ وتجاوز الهجوم الضخم على Dyn في أواخر 2016 حيث بلغ الحد الأقصى للبيانات المرسلة 1.2 تيرابايت في الثانية.

نصائح في امن الشبكات

نصائح في امن الشبكات

- عليك إنشاء و تكوين كلمات سر يصعب تخمينها
- عليك تغيير معلومات تسجيل الدخول المعدة مسبقاً
- تفادي الإتصال الأوتوماتيكي بالشبكات العمومية، أي الشبكات الغير خاصة
- احرص على تحديث مكافح الفيروسات الذي تستخدمه بشكل دوري
- قم بإجراء النسخ الاحتياطي بشكل دوري ومنتظم

نصائح في امن الشبكات

1. تذكر تسجيل الخروج : الوصول إلى الحسابات عبر الإنترنت هو أحد أكبر تهديدات أمن المعلومات التي يواجهها الأفراد اليوم.

نظرا لأن استخدام حسابات وسائل التواصل الاجتماعية مثل Google و Facebook واسع ومنتشر بشكل كبير جدا، فإنك قد تسجل الدخول في أماكن مختلفة ولكنك تنسى تسجيل الخروج.

نصائح في امن الشبكات

- لا تدخل إلى الحسابات السرية على الشبكات أو الأجهزة العامة بالنسبة للعديد من الأشخاص، هناك أنواع مختلفة من المعلومات الحساسة. قد تكون مثل ملفات تعريف وسائل التواصل الاجتماعي ورسائل البريد الإلكتروني أو تفاصيل عائلية أخرى.
- البيانات المالية مثل بطاقات الائتمان وحسابات PayPal

نصائح في امن الشبكات

ما لم تثق في مقدم الخدمة أو مالك الجهاز تماما، فمن المستحسن تجنب هذه العادة.

حتى عندما تعتقد أنها موثوقة، تأكد من أنك شديد اليقظة، الأجهزة والشبكات العامة غير آمنة مما يعني أن المعلومات يمكن اختراقها بسهولة تامة.

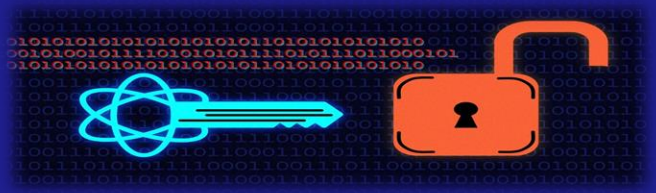
نصائح في امن الشبكات

لا تدع جهازك اللاسلكي يعلن عن وجوده

غيّر اسم SSID الخاص بجهازك

- عليك تغيير الاسم الافتراضي للشبكة
- عليك إخفاء عنوان SSID

نصائح في امن الشبكات



نصائح في امن الشبكات

شفّر بياناتك

نصائح في امن الشبكات

الحماية من البرامج الضارة وهجمات الإنترنت

مستقبل الامن السيبراني

ما أهمية الأمن السيبراني

يعتمد العالم على التكنولوجيا أكثر من أي وقت مضى. نتيجة لذلك، ارتفع إنشاء البيانات الرقمية. تقوم الشركات والحكومات اليوم بتخزين الكثير من هذه البيانات على أجهزة الكمبيوتر ونقلها عبر الشبكات إلى أجهزة الكمبيوتر الأخرى. الأجهزة والأنظمة الأساسية لها نقاط ضعف تؤدي عند استغلالها إلى تهديد سمعة المنظمة وأهدافها.

ما أهمية الأمن السيبراني

- يمكن أن يكون لخرق البيانات مجموعة من العواقب المدمرة لأي عمل تجاري. يمكن أن تكشف عن سمعة الشركة من خلال فقدان ثقة المستهلك والشريك.
- فقدان البيانات الهامة مثل الملفات المصدر أو الملكية الفكرية، يمكن أن يكلف الشركة ميزتها التنافسية للمضي قدماً، يمكن أن يؤثر خرق البيانات على إيرادات الشركات بسبب عدم الإمتثال لأنظمة حماية البيانات.
- من اجل ذلك يكون من الضروري أن تعتمد المؤسسات وتنفذ نهجًا قويًا للأمن السيبراني.

تحديات الأمن السيبراني

لتحقيق الأمن السيبراني (الامن الالكتروني) الفعال مجموعة تحديات منها

- أمن الشبكة
- أمان التطبيق
- أمن الكمبيوتر

تحديات الأمن السيبراني

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

فوائد الأمن السيبراني 1/3

1. حماية المعلومات الشخصية أو المالية أو المعلومات المهمة
2. العمل بأمان للموظفين
3. حماية الإنتاجية

فوائد الأمن السيبراني 2/3

3. حماية الموقع الالكتروني من التوقف
4. حجب برامج التجسس

فوائد الأمن السيبراني 3/3

5. منع البرامج الإعلانية Adware: البرامج الإعلانية
6. توحيد بيئة العمل
7. دعم موظفي تكنولوجيا المعلومات
8. ثقة العملاء

الوظائف المتوقعة في الأمن السيبراني 1/3

- أخصائي أمن معلومات تقني
- أخصائي اختبار الاختراق
- مختبر اختراق التطبيقات
- محقّق جرائم الحاسوب
- مدير قطاع الأمن
- محقّق جرائم/خبير أدلَّة جنائية في أمن المعلومات

الوظائف المتوقعة في الأمن السيبراني
2/3

- ضابط حماية البيانات
- خبير طوارئ
- محلّل الاحترافية الأمنية
- محلّل البرمجيات الخبيثة
- محلّل أمني
- مهندس أمني
- مراقب أمني
- مهندس أمن شبكات
- محلّل مركز عمليات الأمن

الوظائف المتوقعة في الأمن السيبراني
3/3

- مدَّعي عام متخصِّص في جرائم أمن المعلومات
- مطوِّر برامج الأمن الذَّكية
- باحث ثغرات / مطوِّر اقتحامات
- مختبر اختراقات النظام والشَّبكة والويب

أسئلة واستفسارات

للتواصل للتدريب والاستشارات والاستفسارات


salnahi@gmail.com


0555161888


@salnahi


linkedin.com/in/salnahi

العطاء الرقمي
Attaa Digital

شكراً لكم