أمن المعلومات

اشرف الرفاعي 0788322836

أمن المعلومات

- **علم أمن المعلومات** : هو علم يعمل على حماية المعلومات والمعدات المستخدمة في (تخزينها ومعالجتها ونقلها) من السرقة او الكوارث الطبيعية او غيرها من المخاطر مع ابقائها متاحة للأفراد المصرح لهم .
- **الهدف من أمن المعلومات** هو الاهتمام بكل ما يخص المعلومة من تخزين ومعالجة والحفاظ عليها

- **الخصائص الأساسية لأمن المعلومات** :

1- **السرية** : عدم القدرة على الوصول للمعلومات إلا من قبل الاشخاص المصرح لهم.
مثل : الموقف المالي لشركة قبل إعلانه المعلومات العسكرية

2- **السلامة** : حماية الرسائل والمعلومات والتأكد بأنها لم تتعرض لأي تعديل
والتعديل يشمل : اضافة / استبدال / حذف
مثل : نتائج الثانوية العامة نتائج القبول الموحد

3- **توافر المعلومات** : قدرة الشخص المخول بالحصول على المعلومات في الوقت الذي يشاء دون عوائق

- **مخاطر تهدد أمن المعلومات : 1- التهديدات 2- الثغرات**

1- التهديدات : أ – اسباب طبيعية : مثل (حرائق / زلازل / انقطاع الكهرباء)

ب- اسباب بشرية : وتقسم إلى

1-غير متعمده : تكون نتيجة اهمال أو خطأ غير متعمد

كتابة بريد الكتروني بشكل خاطئ ، مثل كتابة 45 بدلا 54

2- متعمده : وتكون :

A. غير موجهة لجهاز : نشر فايروس
B. موجهة لجهاز : وتكون هجوم الكتروني مثل

مثل سرقة جهاز من أجل التعديل على ملف او كشف عن بيانات سرية

الهجوم الإلكتروني (الاعتداء) : هو تهديد موجه ومتعمد لجهاز معين بقصد الإضرار به .

عوامل نجاح الهجوم الالكتروني: **أ- الدوافع** : تكون لاحد ما يلي (المال/اثبات الذات/الاضرار بالآخرين)

ب- الطريقة : وهي المهارات التي يتميز بها المعتدي ومدى توافر المعدات او البرمجيات اللازمة لنجاح الاعتداء ومعرفته بالنظام المستهدف وآلية عمله .

ج- فرصة النجاح : تحديد الوقت المناسب / وكيفية الوصول للأجهزة

أمن المعلومات

اشرف الرفاعي 0788322836

انواع الاعتداءات الإلكترونية على المعلومات :

1-**التنصت على المعلومات** : الحصول على المعلومة (إخلال بالسرية)
2-**التعديل على المحتوى** : اعتراض المعلومة وتعديلها ثم ارسالها للمستقبل دون علمه(إخلال بالسلامة)
3-**الإيقاف** : قطع قناة الاتصال ومنع المعلومة من الوصول إلى المستقبل (إخلال بتوافر المعلومة)
4-**الهجوم المزور (المفبرك)** : وهو ارسال المعتدي رسالة على الشبكة يطلب فيها معلومات او كلمات مرور سرية (اخلال بالسرية و السلامة)

2- الثغرات :

نقطة ضعف في النظام تتسبب في فقدان المعلومة او هدم النظام او جعله عرضة للاعتداءات الإلكترونية .

انواع الثغرات : 1- ضعف في الاجراءات المتبعة : مثل عدم تحديد الصلاحيات .
2- عدم كفاية الحماية المادية للأجهزة : كالأبواب وانظمة الحرائق .
3- مشكلة في تصميم النظام : أخطاء برمجية

الحد من مخاطر أمن المعلومات :

وهي ضوابط لتقليل المخاطر التي تتعرض لها المعلومات

ضوابط التي تحد من مخاطر امن المعلومات :

و يجب ان تعمل بشكل متكامل

أ- **الضوابط المادية :** مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار والأقفال وحراس الأمن وأجهزة الإطفاء

ب- **الضوابط الإدارية** : وهي الأوامر والاجراءات المتفق عليها لمنع دخول غير مصرح به مثل القوانين واللوائح والسياسات والاجراءات التوجيهية و حقوق النشر وبراءات الاختراع والاتفاقيات

ت- **الضوابط التقنية** : بنوعيها المعدات و البرمجيات مثل كلمات المرور ومنح صلاحيات الوصول وبرتوكولات الشبكات والجدر النارية والتشفير وتنظيم تدفق المعلومات في الشبكة .

الهندسة الاجتماعية

الهندسة الاجتماعية : هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل المستخدم للنظام يعطي معلومات سرية او تسهيل الوصول إلى الأجهزة او المعلومات .

هي انجح الوسائل التي تستخدم للحصول على المعلومة غير المصرح بها من جانب المعتدي

بسبب : أ- قلة اهتمام المتخصصين في مجال امن المعلومات

ب: عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة على ذلك

مجالات الهندسة الاجتماعية :

مجال البيئة المحيطة	مجال الجانب النفسي: كسب ثقة المستخدم
مكان العمل : كتابة كلمات المرور على الشاشات مما يسمح للآخرين الاطلاع عليها	**الإقناع :** اقناع المستخدم للنظام بحجج وبراهين منطقية للحصول منه على معلومات تخص النظام ويجعل المعتدي من نفسه مثيلا (الصفات ، والاهتمامات) للمستخدم للنظام لإقناعه
الهاتف : الحصول على معلومات من خلال الدعم الفني ليتم استخدامها في الاعتداء	**انتحال الشخصية والمداهنة :**تقمص لشخصية حقيقية او وهمية (فني صيانة ، عامل نظافة ،مدير وغيرهم) وبما أن الشخصية المنتحلة غالبا ما تكون ذات سلطه يظهر الموظفين خدماتهم ولن يترددوا بإعطاء أي المعلومات لهذا للمعتدي
النفايات الورقية : من خلال النفايات الورقية يمكن تتبع الموظفين وهواتفهم وبياناتهم الشخصية او كلمات مرور	**مسايرة الركب :** وهو عند قيام الموظف بأمر ما اذا قام به جميع الموظفين دون تفكير (مثل قيام الموظفين بتحديث نظام اجهزتهم فإذا سمح له موظف سمح له بقية الموظفين للقيام بنفس الأمر)
الإنترنت : استخدام الاشخاص لنفس كلمات المرور في جميع التطبيقات فيقوم المعتدي بإنشاء موقع يقدم خدمات يكون	

أمن المعلومات

اشرف الرفاعي 0788322836

فيها هدف المعتدي معرفة كلمات السر المستخدمة	

أمن الانترنت

**** اعتماد الافراد والمؤسسات والحكومات على تكنولوجيا المعلومات بشكل واسع ****

**** الاعتداءات الالكترونية على الويب :**

1- اعتداءات إلكترونية على المتصفحات الانترنت :

المتصفح : هو برنامج ينقل المستخدم إلى الصفحة التي يريديها من خلال كتابة العنوان والضغط على زر الذهاب

**** تزداد الاخطار في المتصفح بسبب انها قابلة للتغير دون ملاحظة المستخدم *****

طرق الاعتداء :

1- **عن طريق الكود حيث** يمكن اضافة كود إلى المتصفح هذا الكود قادر على القراءة والنسخ وارسال المعلومات التي يتم ادخالها إلى المعتدي
(من خلال هذا الكود يستطيع المعتدي الاطلاع على الحسابات المالية وكلمات المرور والبيانات الحساسة)

2- توجيه المستخدم إلى صفحة اخرى غير الصفحة التي يريدها .

2- الاعتداءات الالكترونية على البريد الالكتروني :

من خلال ارسال رسائل مزيفة إلى المستخدم حيث يقدم عرض لمنتجات مزيفة وتحتوي هذه الرسائل على روابط يتم الضغط عليها للحصول على المزيد من المعلومات .

**** يعتمد المعتدي على عدم وعي المستخدم سواء للمتصفح او لروابط البريد الالكتروني ***

تقنية تحويل العناوين الرقمية

العناوين الرقمية الإلكترونية(IP Addresses):هو رقم خاص يعطى لكل جهاز او هاتف خلوي يميزه عن غيره من الاجهزة داخل الشبكة.

انواع العناوين الرقمية :

1- IP4: يتكون 32 خانة ثنائية مقسم لـ 4 مقاطع
2- IP6: يتكون 64 خانة ثنائية مقسم لـ 6 مقاطع

ازدياد عدد المستخدمين للإنترنت أدت إلى الحاجة إلى عنوانين اكثر مما ادى لظهور تقنية تحويل العناوين الرقمية

تقنية تحويل العناوين الرقمية هي تقنية تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة.

استخدمها يؤدي إلى الحماية من أي هجوم يعتمد على معرفة العناوين الرقمية .

السلطة المسؤولة عن منح العناوين الرقمية هي إينا (IANA)

- حيث تقوم بإعطاء عنوان للشبكة يختلف عن عناوين الشبكات الأخرى
- الشبكة الداخلية تعطي عناوين لكل جهاز داخل الشبكة نفسها فقط يكون مخصصا لتواصل الأجهزة مع بعضها البعض داخل الشبكة
- عند طلب احد الأجهزة التوال مع جهاز خارج الشبكة يتم استخدام تقنية تحويل العناوين الرقمية بحيث يقوم (الراوتر / الجدار الناري) بتحويل الرقم الداخلي إلى العنوان الرقمي الخارجي ويحتفظ به في سجل للمتابعة .

آلية عمل تحويل العناوين الرقمية :

1- **النمط الثابت :** تخصيص عنوان رقمي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير
2- **النمط المتغير :** الجهاز الوسيط لديه عناوين رقمية خارجية تكون اقل من عدد الاجهزة في الشبكة ويتم استخدامها لكل جهاز يرغب بالتراسل خارجيا ويكون بشكل مؤقت بحيث يكون الرقم متاحا لجاهز آخر . في حال رغب الجهاز التراسل مرة أخرى يأخذ رقما جديدا متاحا

أمن المعلومات

اشرف الرفاعي 0788322836

التشفير

** **التشفير :** هو تغير محتوى الرسالة الأصلية من خلال مزجها بمعلومات أخرى أو استبدال الأحرف الأصلية أو تغير لمواقع الاحرف بحيث لن يفهما إلا المرسل والمستقبل.

** **الهدف من التشفير هو الحفاظ على سرية المعلومات في اثناء تبادلها بين المرسل والمستقبل**
فاذا تم اعتراض الرسالة فان المعتدي لن يستفيد منها او فهم محتواها

** **الخوارزمية : هي مجموعة من الخطوات المتسلسلة منطقيا ورياضيا اللازمة لحل مشكلة ما**

عناصر عملية التشفير

1- **خوارزمية التشفير** : هي الخطوات المستخدمة لتحويل الرسالة الاصلية الى رسالة مشفرة
2- **مفتاح التشفير** : سلسلة الرموز المستخدمة في خوارزمية التشفير
(قوة المفتاح هي قوة التشفير)
3- **النص الأصلي** : وهي محتوى الرسالة الأصلية قبل التشفير وبعد فك التشفير
4- **نص الشيفرة** : الرسالة بعد عملية التشفير

خوارزميات التشفير

تصنف خوارزميات التشفير بناء على :

1- **العملية المستخدمة في التشفير : أ- التعويض :** استبدال حرف مكان حرف او مقطع مكان مقطع
ب- التبديل : تبديل مكان الحرف دون تغيره (خوارزمية الخط المتعرج)

2- **المفتاح المستخدم :** امن الرسالة يعتمد على سرية المفتاح وليس تفاصيل خوارزمية التشفير
أ- مفتاح خاص (التناظرية): نفس المفتاح في التشفير والفك يُعتمد قبل البدء بالتراسل
ب- مفتاح عام (اللاتناظرية) : تستخدم مفتاحين الاول عام يستخدم للتشفير يكون معروفا للمرسل والمستقبل والمفتاح الثاني يستخدم للفك ويكون معروفا فقط للمستقبل

3- **كمية المعلومات المرسلة : أ – التدفق :** تقسيم الرسالة إلى مجموعة اجزاء يشفر كل جزء منها على حده ثم يرسل
ب- الكتل : تقسم إلى أجزاء أكبر من أجزاء التدفق كل كلتة تشفر لوحدها
الفرق بأن الكتل أكبر حجما من التدفق لذلك أبطأ