الـــدرس الثالث : أمن المعلومات La sécurité informatique

مـــدخل:

الأمن في الإعلام الآلي هو مجموع التدابير المتخذة لحماية الحاسوب والمعطيات التي يحتويها. وهو يتعلق بطبيعة النظام وأهمية المعلومات. في كل الحالات يجب ضمان الأمن بصورة إجمالية للنظام.

فإذا قمنا بتقسيم النظام إلى مجموعة من الحلقات فالنظام في الحقيقة يمتلك درجة أمان الحلقة الأضعف فيه.

يمكننا عموما توصيف الخطر Le risque بالمعادلة الآتية:

$$\text{الخطر} = \frac{\text{الضعف} \times \text{التهديد}}{\text{التدابير المتخذة}}$$

التهديد (Le menace) : يمثل نوع العملية التي يمكن أن تحدث الضرر.

الضعف (La vulnérabilité): (كما يمكن أن نسميها ثغرة أو فتحة) تمثل درجة التعرض للخطر في مجال محدد.

التدابير المتخذة (La contre mesure): هي مجموع الإجراءات المتخذة والمطبقة كاحتياط في مواجهة التهديد.

ضرورة المقاربة الإجمالية

الأمن يجب أن يتخذ في إطار سياق إجمالي وبالخصوص الأخذ في الحسبان النواحي التالية:

تكوين المستعملين وتحسيسهم بالمشاكل الأمنية.
الأمن المنطقي La sécurité logique ، وهو الأمن على مستوى المعطيات، خاصة المعلومات المتعلقة بالمؤسسة، التطبيقات، وأيضا أنظمة التشغيل.
أمن الإتصالات: تقنية الشبكة، موزعات الشركة، ....

الأمن الفيزيائي La sécurité physique، ويقصد به الأمن على مستوى البنى التحتية المادية: قاعات مؤمنة، أماكن مفتوحة، الأماكن العامة للمؤسسة، أماكن عمل المستخدمين، الخ .

الهجمات Les attaques

كل جهاز موصول بشبكة إعلام آلي هو معرض لهجوم.

أ) الهجـــوم :

هو استغلال ثغرة في النظام من أجل أهداف غير معلومة من طرف المستعمل. تكون الهجمات على شبكة الانترنت بصورة دائمة وتنطلق آليا من أجهزة مصابة (فيروسات ديدان حصان طروادة) دون علم المستعمل. و من أجل مواجهة هده الأخطار يجب معرفة أهم أسبابها وأنواعها .

ب) أسباب الهجمات :

1. الحصول على منفذ في النظام،
2. سرقة المعلومات (كأسرار المستعملين، حقوق التأليف)،
3. تجميع معلومات خاصة على المستعمل،
4. الحصول على معلومات بنكية،
5. الحصول على معلومات المؤسسة،
6. استعمال نظام المستعمل كوسيلة للهجوم،
7. ....

أنواع الهجمات Les types d'attaques

1)الهجوم المادي : يتم عندما يكون للمهاجم إمكانية الوصول إلى الأماكن حيث توجد المعلومات، ويهدف إلى :

1. إتلاف الأجهزة،
2. سرقة المعدات،
3. سماع الشبكة،

2) قطع الاتصالات (أو اعتراضها) : ويتسم هذا الهجوم بعدة أوجه:

1. انتحال الشخصية،
2. تعطيل الرسائل أو تحويل اتجاهها،

3) التجسسL'espionnage: وهو الحصول على معلومات غير مرخصة.

4) تعطيل الخدمة Le déni de service: تهدف إلى تشويش العمل، وفي هذه الحالة لا تكون سرقة المعلومات هدفا.

5) الدراسة أو الهندسة الاجتماعية l'ingénierie sociale: في أغلب الحالات تكون أضعف حلقة في النظام الأمني هي المستعمل لأنه عن غير علم يفتح ثغرة في النظام وذلك بإعطاء معلومات حساسة (كلمة سر مثلا) إلى قرصان أو يقوم بتنفيذ برنامج يحتوي على فيروس.

الفيروسات Les virus

الفيروس هو برنامج تنفيذي (ذات نوع .com, .exe,.bat,.pif,.scr) صغير يوجد وسط برنامج آخر. يقوم برنامج الفيروس بأعمال ضارة من إفساد الملفات والتجسس، إلى إحداث أعطاب في الأجهزة.

أنواع الفيروسات

1. الفيروسات المتغيرة (Les virus mutants)

هي فيروسات تمت إعادة صياغتها من أجل تغيير توقيعها أو طريقة تصرفها، وذلك لجعل عملية اكتشافها من طرف مضادات الفيروسات عملة أصعب.

2. الفيروسات المتحولة (Les virus polymorphes)

هي فيروسات ذات قدرة على تغيير توقيعها (La signature virale) بطريقة آلية مثل الحرباء. ما يجعلها تبدو كل مرة بمظهر مختلف.