

5-المحاضرة الخامسة-المخاطر المعلوماتية

1-تعريف المخاطر المعلوماتية:

وتتمثل في المخاطر المتعلقة باستغلال المعلومات أو سرقتها أو سوء استخدامها أو العبث في البرامج.

-هي ايضا جميع الاستخدامات الغير المسموح بها مثل تغير المعلومة أو إلغائها أو الاطلاع عليها، وانتهاك سريتها للاستفادة منها بطريقة شرعية، أو نشر معلومات غير صحيحة، أو منع وصولها، أو سرقة الأجهزة ووسائل التخزين . ويرتبط بهذا المفهوم أيضا بأمن البرامج والتطبيقات.

2-مجالات المخاطر المعلوماتية:

- المخاطر التكنولوجية: إن تبني تكنولوجيا جديدة (مبتكرة) مبكرا المؤسسة الوثائقية، يصاحبه في كثير من الأحيان مخاطر فشل التكنولوجيا الحديثة غير المجربة فتواجه المكتبة أو ومركز الأرشفة الكثير هدرا في مواردها.

- مخاطر العمليات: كثيرا ما يرافق استخدام التكنولوجيا الجديدة في عمليات كثيرا المعالجة الفنية واستخدام البرمجيات الوثائقية أو برمجيات التسيير الإلكتروني للوثائق في بداية إدخالها لأول مرة مخاطر تتعلق بتوقف العمليات نتيجة أخطاء في موائمة التكنولوجيا الجديدة مع إصدارات البرمجيات التي تمتلكها المكتبة وأو مركز الأرشفة، وكذلك إعادة تدريب وتأهيل المكتبيين أو الأرشفيين . وهذا يقود إلى إبطاء أو أخطاء في بداية استخدام التكنولوجيا الحديثة.

- المخاطر التنظيمية في كثير من الحالات ما تواجه المكتبات ومراكز الأرشفة افتقارا في التنظيم المرتبط بإحلال التكنولوجيا مثال في توزيع فضاءات المكتبة وفقا لنظام جديد مع الربط بشبكة.

3-مفهوم أمن المعلومات:

ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية مختلف مصادر البيانات خصوصا المسجلة على وسائل إلكترونية وما يهددها من مخاطر العمل في البيئة الإلكترونية.

-توفير الحماية للمعلومات من المخاطر التي تهددها والاعتداء عليها بتوفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية وكذا المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

4-مجالات أمن المعلومات:

* أمن وحماية الولوج أو الدخول إلى الأنظمة.

* أمن حماية أنظمة التشغيل

* أمن وحماية البرامج والتطبيقات

* أمن وحماية قواع البيانات.

5-مكونات أمن المعلومات:

أولا :كلمات المرور : كلمة المرور تعني للنظام أنك الشخص المرخص له بالدخول فعلا وتعمل على حماية البيانات. الأخطار التي تهدد كلمات المرور من اختراق أو تغيير أو تخريب. و للاختيار الأمثل لكلمة المرور لتفادي اختراق أو تغيير أو تخريب كلمة المرور يجب أن تكون قوية أو لا تكون صيدا سهلا لبرامج الاختراق يجب اتباع الخطوات التالية:

1. ألا تكون كلمة المرور كلمة واحدة.

2. لا تتضمن كلمات المرور معلومات شخصية.

3. ألا يقل عدد الخانات عن 10 أرقام أو حروف.

4. المزج بين الحروف والأرقام.

5. استخدام اختصار جملة أو عبارة ما.

6. تجنب تضمين اسم المستخدم داخل كلمة المرور.

كلمة المرور أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم، وفعاليتها تعتمد على درجة انضباط العنصر البشري في اختيار كلمة المرور والتأمل معها وفق الأساليب الصحيحة.

ثانيا :أمن وحماية البرامج والتطبيقات: فالفيروسات هي أحد أنواع البرامج الخبيثة التي تعمل على تخريب أو إفساد عمل برنامج ما أو نظام تشغيل ما أو انتحال صفة معينة داخل الجهاز وفي مجمل الأحيان لها تأثير سلبي غير معلوم بالنسبة للمستخدم ومن أمثلة البرامج الخبيثة كذلك نجد:الديدان، البرامج التجسسية، البرامج الإعلانية الأحصنة الطروادية...الخ.

6-التأمين ضد المخاطر المعلوماتية في مجال المكتبات والمعلومات:

والتأمين في مجال المعلوماتية وبالضبط في مجال المكتبات والمؤسسات الوثائقية هو تأمين النظام كاملا ككل أو تأمين جزء معين منه، ومع أننا بصدد دراسة المخاطر المعلوماتية فإن التأمين سوف يقع فقط على كل ما يتعلق بالحواسيب وأجهزة الإعلام الآلي ، سواء في شقها المادي أو على مستوى البرمجيات، وبما أن إجراءات التأمين في هذه الحالة تتم بشكل عادي ككل إجراءات التأمين الأخرى العادية في حياتنا اليومية، ومع أي شركة من شركات التأمين التي توفر هذه الفئة من عقود التأمين، وعلى سبيل المثال لا الحصر فإن المجالات التي يمكن أن تخضع للتأمين في المكتبات والمؤسسات الوثائقية هي:

✓ تأمين الأرصدة الوثائقية لما لها هناك من أخطار وكوارث طبيعية وبشرية تهددها.

✓ تأمين المباني ومحلات الحفظ.

✓ تأمين الأجهزة والمعدات والبرامج المعلوماتية.

✓ تأمين الأشخاص من عمال وموظفين