6-المحاضرة السادسة-ادارة مخاطر امن المعلومات

1-مراحل ادارة مخاطر أمن المعلومات:

هناك ثلاثة مراحل تمثل الاعمدة الرئيسية التي تكون برنامج ناجح لادارة مخاطر تكنولوجيا المعلومات، ولكل مرحلة منها انشطتها ومهامها وتتمثل هذه المراحل فيمايلي:

اولا-مرحلة تحديد وقياس المخاطر: في هذه المرحلة الاولى يتم التعرف على المخاطر التي تتعرض لها المؤسسة او المكتبة واهم التكنولوجيات المستخدمة بها، مع زيادة التوعية بتلك المخاطر وتحديد التاثير المتوقع حدوثه على دورة العمل في المؤسسة في حال حدوث الكارثة. وتتم عملية تحديد وقياس الخطر وفق مايلي:

- ✓ عمل قائمة بكل الاصول المعلوماتية والتكنولوجية التي تمتلكها المؤسسة
- ✓ تحديد مستوى الامتثال لسياسات امن المعلومات المعلنة في المؤسسة
- ✓ قياس وتقييم المخاطر التي تتعرض لها المؤسسة
- ✓ استعراض الخيارات المتاحة للتخفيف من حدة المخاطر

ثانيا-مرحلة ادارة المخاطر: بمجرد ان تقوم ادارة المؤسسة او المكتبة بالتعرف على المخاطر ومنهجية تنفيذ برنامج ادارة والتخفيف من المخاطر بالمؤسسة تبدأ في الاختيار بين عدة اجراءات اهمها:

* تجنب المخاطر عن طريق تجنب استخدام معدلات تقنية لا تستطيع المؤسسة حصر التعامل مع المخاطر المحتملة الناتجة عن تشغيلها.
* تقليل المخاطر من خلال تنفيذ ضوابط التخفيف من المخاطر
* قبول المخاطرة لفترة زمنية محددة، اذا كانت التكلفة تزيد عن العائد المتوقع
* نقل الخطر ليتحمله طرف اخر (مثلا التامين على التكنولوجيا المستخدمة لدى شركة التامين)

ثالثا-مرحلة رصد وتقييم المخاطر: بعد التنفيذ المبدئ لبرنامج ادارة مخاطر تكنولوجيا المعلومات، يجب تأسيس مجموعة من الاليات لضمان استمرار عمليات التعريف والتوعية وقياس ادارة المخاطر، وتعتبر اجراءات دمج تقنيات ادارة مخاطر تكنولوجيا المعلومات في دورة حياة المشروع خطوة جيدة للحفاظ على استمرارية ثقافة ادارة المخاطر بالمؤسسة وهناك عناصر رئيسية مكونة لهذه المرحلة منها:

- _ المحافظة على استمرارية تحديث قائمة الاصول المعلوماتية والتكنولوجية للتأكد من ان كل وحدة عمل بالمؤسسة تقوم بتنفيذ اجراءات ادارة المخاطر
- _ اجراء تقييم ذاتي سنوي لتحقيق متطلبات امن المعلومات للمشروع بأكمله
- _ مراجعة دورية لسياسات امن المعلومات للتأكد من انها وما يتبعها من متطلبات تستطيع التعامل مع المخاطر التي استجدت نتيجة لاستخدام تقنيات جديدة في العمل

2-ادوات واجراءات امن المعلومات:

اولا-تقنيات الحماية ضد البرامج الخبيثة: ان البرامج الخبيثة هي أي برنامج يكون كل مهامه ا واحداها عمل خبيث من تجسس او تخريب او استنزاف للموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي)وهناك العديد من الاجراءات للوقاية والحماية من البرامج الخبيثة كمايلي:

استخدام برامج مكافحة الفيروسات واستمرارية تحديثه

عمل مسح كامل ويومي لأجهزة الحاسوب بواسطة برامج الحماية

العمل على فحص كافة وسائط التخزين الخارجية عند توصيلها او ادخالها في الحاسوب

استعمال الجدران النارية لسد المنافذ غير الامنة وتقليل المخاطر على الاجهزة

ثانيا-استخدام الانظمة الذكية وتقنية التشفير: ومن بين الاجراءات والادوات التي من شانها توفير الحماية والامن للمنظومة المعلوماتية وهو استخدام الانظمة الذكية، وهي انظمة تمتاز بالكشف المبكر للتهديدات التي ستلحق بنظام المعلومات، وفي حالة عجز المنظمة عن توفير هذه الانظمة بمفردها تستطيع اللجوء الى وكالات او هيئات خاصة بتقديم هذه الخدمة وذلك بسرية تامة، ومن بين هذه الانظمة مايلي:

-البطاقة الذكية للتعرف على الشخص المستخدم: تستخدم هذه البطاقة الرقائق الالكترونية والتي تحمل عليها كلمة السر الخاصة بصاحب البطاقة.

-استخدام البيولوجيا الاحصائية: وهي طريقة تستخدم للتعرف على الاشخاص وتستند على الخصائص البيولوجية او السيكولوجية للفرد

3-الرقابة على انظمة المعلومات في المنظمة:

ويقصد بها الرقابة الشاملة وهي طريق العمل التي بواسطتها تتم الرقابة على التصميم والامن، واستخدام برامج الحاسوب الموجودة في المؤسسة، وللتأكد من فعالية العمليات الخاصة بإجراء البرمجة، ومن انواع هذه الرقابة مايلي:

-الرقابة على التصميم: يتم بناء خصائص ومعايير الرقابة على تصميم النظام من خلال محللي النظام ومديري قواعد البيانات مع مراعاة مبدا التكلفة والمنفعة.

-الرقابة على البرمجيات: وهي تغطي برامج تشغيل النظام، والتي تقوم بتنظيم ادارة موارد الحاسوب وهذا بهدف تسهيل استخدام وتنفيذ البرمجيات التطبيقية.

-الرقابة على المكونات المادية: يجب حماية الاماكن التي يوجد بها الحاسوب بالطريقة التي تسمح للأفراد المرخص لهم فقط بالتعامل معه، وتتضمن الحماية ايضا الظروف التي يعمل بها الحاسوب كدرجة الحرارة ونسبة الرطوبة...

-الرقابة على تشغيل واستخدام الحاسوب: وذلك للتأكد من ان اجراءات البرمجة متناسقة وتطبق بطريقة صحيحة بالنسبة لتشغيل وتخزين البيانات والمعلومات.

-الرقابة على عمليات تنفيذ النظام: وهي التأكد من ان نظم المعلومات المبنية على الحاسوب تقابل احتياجات المستخدمين من خلال التعرف على احتياجات كل مستخدم من المعلومات، تحديد معايير الاداء ووضع معايير التصميم والتشغيل لنظم المعلومات المبنية على الحاسوب وتحديد اختبار قبول النظام ومراجعته وصيانته من قبل المتخصصين.