6-المحاضرة السادسة: إدارة مخاطر أمن المعلومات

1-مراحل إدارة مخاطر أمن المعلومات:

هناك ثلاثة مراحل تمثل الأعمدة الرئيسـية التي تكون برنامج ناجح لإدارة مخاطر تكنولوجيا المعلومات، ولكل مرحلة . منها أنشطتها ومهامها وتتمثل هذه المراحل فيمايلي:

أولا-مرحلة تحديد وقياس المخاطر: في هذه المرحلة الأولى يتم التعرف على المخاطر التي تتعرض لها المؤسسة أو المكتبة وأهم التكنولوجيات المستخدمة بها، مع زيادة التوعية بتلك المخاطر وتحديد التأثير المتوقع حدوثه على دورة العمل في المؤسسة في حال حدوث الكارثة، وتتم عملية تحديد وقياس الخطر وفق مايلي:

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

ثانيا-مرحلة إدارة المخاطر: بمجرد أن تقوم إدارة المؤسسة أو المكتبة بالتعرف على المخاطر ومنهجية تنفيذ برنامج إدارة . والتخفيف من المخاطر بالمؤسسة تبدأ في الاختيار بين عدة إجراءات أهمها:

* تجنب المخاطر عن طريق تجنب اسـتخدام معدلات تقنية لا تسـتطيع المؤسـسـة حصـر التعامل مع المخاطر. المحتملة الناتجة عن تشغيلها.
* تقليل المخاطر من خلال تنفيذ ضوابط التخفيف من المخاطر
* قبول المخاطرة لفترة زمنية محددة، إذا كانت التكلفة تزيد عن العائد المتوقع
* نقل الخطر ليتحمله طرف آخر (مثلا التامين على التكنولوجيا المستخدمة لدى شركة التامين)

ثالثا-مرحلة رصـد وتقييم المخاطر: بعد التنفيذ المبدئي لبرنامج إدارة مخاطر تكنولوجيا المعلومات، يجب تأسـيس مجموعة من الآليات لضمان استمرار عمليات التعريف والتوعية وقياس إدارة المخاطر، وتعتبرإجراءات دمج تقنيات إدارة مخاطر تكنولوجيا المعلومات في دورة حياة المشـروع خطوة جيدة للحفاظ على اسـتمرارية ثقافة إدارة المخاطر بالمؤسسة وهناك عناصر رئيسية مكونة لهذه المرحلة منها:

- _ المحافظة على اسـتمرارية تحديث قائمة الأصـول المعلوماتية والتكنولوجية للتأكد من أن كل وحدة عمل بالمؤسسة تقوم بتنفيذ إجراءات إدارة المخاطر
- _ إجراء تقييم ذاتي سنوي لتحقيق متطلبات أمن المعلومات للمشروع بأكمله
- _ مراجعة دورية لسياسات أمن المعلومات للتأكد من أنها وما يتبعها من متطلبات تستطيع التعامل مع المخاطر التي استجدت نتيجة لاستخدام تقنيات جديدة في العمل

2-أدوات وإجراءات أمن المعلومات:

أولا-تقنيات الحماية ضد البرامج الخبيثة: إن البرامج الخبيثة هي أي برنامج يكون كل مهامها واحداها عمل خبيث من تجسس أو تخريب أو استنزاف للموارد (الوقت، المعالج، الذاكرة، وحدة التخزين، سعة النقل الشبكي) وهناك العديد من الإجراءات 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 أو إدخالها في الحاسوب
- استعمال الجدران النارية لسد المنافذ غير الآمنة وتقليل المخاطر على الأجهزة

ثانيا-استخدام الأنظمة الذكية وتقنية التشفير: ومن بين الإجراءات والأدوات التي من شأنها توفير الحماية والأمن للمنظومة المعلوماتية وهو استخدام الأنظمة الذكية، وهي أنظمة تمتاز بالكشف المبكر للتهديدات التي ستلحق بنظام المعلومات، وفي حالة عجز المنظمة عن توفير هذه الأنظمة بمفردها تستطيع اللجوء الى وكالات أو هيئات خاصة بتقديم هذه الخدمة وذلك بسرية تامة، ومن بين هذه الأنظمة مايلي:

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

-استخدام البيولوجيا الإحصائية: وهي طريقة تستخدم للتعرف على الأشخاص وتستند على الخصائص البيولوجية أو السيكولوجية للفرد

3-الرقابة على أنظمة المعلومات في المنظمة:

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

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

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

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

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

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