

الفصل السابع

امن المعلومات
والمسؤولية الاخلاقية
والاجتماعية

اعداد المدرس المساعد
عرفات اليوسف
جامعة البصرة / كلية الادارة والاقتصاد /
قسم نظم المعلومات الادارية

امن المعلومات المفهوم والعناصر

امن المعلومات // هي حماية التجهيزات الحاسوبية وغير الحاسوبية والتسهيلات والبيانات والمعلومات من الاخطار وتشمل الاتي :-

**** هي الاجراءات والتدابير الوقائية التي تستخدمها المنظمة للمحافظة على المعلومات وسريتها سواء من الاخطاء الداخلية والخارجية**

**** الحفاظ عليها من السرقة والتلاعب والاختراق او اتلاف غير المشروع سواء قبل او خلال او بعد ادخال للمعلومات الى الحاسب**
**** تسمية الاشخاص المخولين بالذين لهم حق الدخول والتعامل مع البيانات**

**** تحقق الامن عند ادخال البيانات وانتقالها داخل المنظمة وتخزينها واستخدامها .**

العناصر الأساسية لنظم امن المعلومات

- اولا :- الخصوصية** // هو ترك الافراد بدون مراقبة او تشويش من قبل افراد او منظمات او حكومات اخرى / المعلومات سرية ولا يطلع عليها الا المخولين
- الثانية // السلامة / التكامل** /// هي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مهولة
- ثالثا :- الاثبات** // ضمان استخدام الشبكة او النظام من قبل الشخص المخول بالاستخدام / بطاقة الذكية
- رابعا :- عدم الانكار** // منع انكار التصرفات الصادرة عن الشخص / والتوقيع الالكتروني وشهادات التوثيق الالكتروني بحيث تتوفر قدرة اثبات التصرف ماتم من قبل شخص في وقت محدد
- خامسا :- ضبط الدخول** // الشبكة وصادرها استخدمت بطريقة مشروعة ، انها تحدد السياسات والاجراءات والصلاحيات وتحديد مناطق الاستخدام المسموحة لكل مستخدم واوقاته
- سادسا :- الوفرة / توفر المعلومة** // استمرار عمل نظام المعلومات وتقديم الخدمة لمواقع المعلوماتية وضمان حماية النظام من أنشطة التعطيل

المخاطر الرئيسية في بيئة المعلومات

الأجهزة // كافة المعدات والادوات المادية التي تتكون منها النظم والشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية

البرامج // اختيار برامج صعبة الاختراق ووضع علامة السر المختلفة لإدارة وتشغيل النظام اما مستقلة او مخزونة بالنظام **الاتصالات** / ربط الأجهزة التقنية بعضها مع الآخر محليا ودوليا ولا بد من ان تتمتع بكفاءة في الكشف عن التسلسل عالية كونها سهلة الاختراق

الأفراد // يمثل الانسان محور الخطر ، سواء كان الشخص مستخدم او مخول مناط به مهام تقنية والرقابة في حدود احترام حقوقه القانونية الخاصة بانظمة الكمبيوتر وقواعد البيانات

تصنيف المخاطر

اختراق الحماية المادية //

١- التفتيش في المخرجات // قيام المهاجم بالبحث في مخلفات تقنية المؤسسة بحثا عن اي شيء يساعده على اختراق النظام كاوراق المدون عليها كلمة السر / مخرجات النظام

٢- الالتقاط السلبي // التواصل السلبي المادي مع الشبكة او توصيلات النظام لجهة استراق السمع او الاستيلاء على المعطيات المتبادلة عبر الاسلاك

٣- استراق الامواج // باستخدام لواقط الكترونية تقنية لتجميع الموجات الكمبيوتر المنبعثة من النظم باختلاف انواعها كالتقاط كوجات شاشات الضوئية او موجات صوتيه

٤- انكار او الغاء الخدمة // هو الاضرار المادي بالنظام لمنع تقديم الخدمة او ضح الرسائل البريدية الالكترونية دفعة واحدة لتعطيل النظام

اختراق حماية العمليات

((هي المخاطر المتصلة بعملية الحماية التي تستهدف استراتيجية الدخول ونظام ادخال ومعالجة البيانات)) وتشمل الآتي :-

١- **العبث بالبيانات** // هي تغيير البيانات او انشاء بيانات وهمية في مراحل الادخال او الاخراج

٢- **خداع بروتوكولات الانترنت** // وسيلة تقنية بحثه بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسله بحيث يظهر للنظام بانه عنوان صحيح

٣- **تخمين كلمة السر** // تخمين بسهولة نتيجة لضعفها عموما

٤- **المسح** / هو برنامج احتمالات يقوم على فكرة تغيير التركيب او تبديل احتمالات المعلومة فهو يعتمد على اسلوب المسح بدل التخمين البشر

٥- **استغلال المزايا الاضافية** // عندما يتم زيادة مزايا الاستخدام للنظام داخل المؤسسة دون الاخذ بالحسبان للمخاطر التي يتسبب بها ذلك ، حيث ان المستخدم يعطى مزايا تتجاوز اختصاصه لذلك يستطيع المخترق التلاعب بالملفات اذا اخترق حسابه .

نهاية المحاضرة الثانية