وزارة التعليم العالي والبحث العلمي

جامعة الفرات الاوسط

المعهد التقني /السماوة

قسم تكنولوجيا المعلومات والاتصالات

مدرس المادة :م.م بيداء هادي محمد سعودي

https://au.edu.sy/images/courses/dentistry/١-١/١٢٩_computer-in-dentistry.pdf

المحاضرة الاولى والثانية

أمنية الحاسبات والبيانات

COMPUTER & DATA SECURITY

إن التطورات الحديثة في تقنية المعلومات ألحديثة تغييرات مستمرة ومضطربة في أساليب العمل والميادين كافة، إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسوب من الامور الروتينية في عصرنا الحالي واحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خيال تقليل حجم الاعمال وتطوير أساليب خزن المعلومات وتوفيرها. حيث إن انتشار أنظمة المعلومات المحوسبة أدى إلى أن تكون عرضة للاختراق، لذلك أصبحت هذه التقنية سلاحاً ذا حدين تحرص المنظمات على اقتنائه وتوفير سبل الحماية له.

إن موضوع امن المعلوماتي يرتبط ارتباطاً وثيقاً بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراع أمن الحاسوب، وفي ظل التطورات المتسارعة في العالم التي أثرت على امكانات التقنية المتقدمة المتاحة والرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب، كان لا بد من التفكير الجدي لتحديد الاجراءات الدفاعية والوقائية وحسب الامكانات المتوفرة لحمايتها من أي اخترق أو تخريب، وكان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها.

وهكذا، تمثل نظم المعلومات الحاسوبية أهمية قصوى في جميع المجالات، حيث أصبحت التكنولوجيا المعتمدة على الحاسب هي الوسيلة الرئيسية لنقل البيانات داخل معظم المؤسسات الحكومية وغير الحكومية. وأدى ذلك إلى ظهور أهمية أمن البيانات والمعلومات كأحد العناصر الرئيسية المكونة لنظام الحاسب.

مفهوم أمن المعلومات

تشكل المعلومات للمنظمات البنية التحتية التي تمكنها مي أداء مهامها، إذ إن نوع المعلومات وكميتها وطريقة عرضها تعدّ الاساس في نجاح عملية صنع القرارات دخول المنظمات المعاصرة وعليه يكون للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا كانت المشكلة التي يجب أخذها بالحسبان هي توفير الحماية اللازمة للمعلومات وابعادها عن استخدام غير المشروع لها.

ومن أجل فهم امن المعلوماتي Information Security لا بد من تحديد معناه

باختصار يمكن القول إن أمن المعلومات، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها. ومن زاوية تقنية، هو عبارة عن الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية وهو العلم الذي يدرس كيفية توفير تدابير حماية سرية وسلامة المعلومات وكيفية مكافحة أنشطة الاعتداء عليها واستغلال نظمها.

مراحل تطور مفهوم الأمن المعلوماتي

إن مفهوم الامن المعلوماتي مر بعدّة مراحل تطويرية أدت إلى ظهور ما يسمى بأمنية المعلومات. ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، حيث كان همهم كيفية تنفيذ البرامج، ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الاجهزة. وكان مفهوم امن يدور حول تحديد الوصول أو الاطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة، لذلك ظهر مصطلح أمن الحواسيب Computer Security والذي يعني حماية الحواسيب وقواعد البيانات.

ونتيجةً للتوسيع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق بمعالجة الحجوم الكبيرة من البيانات، تغيير اهتمام يمثل السيطرة على البيانات وحمايتها. وفي السبعينيات تم الانتقال إلى مفهوم أمن البيانات (Data Security) ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول إلى البيانات، إضافةً إلى وضع إجراءات الحماية لمكان الحواسيب من الكوارث واعتماد خطط لخزن نسخ إضافية من البيانات والبرمجيات بعيداً عن مكان الحاسوب.

وفي مرحلة الثمانينيات والتسعينيات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لا اكثر من مستخدم بالمشاركة في قواعد البيانات، كل هذا

أدى إلى الانتقال من مفهوم امن البيانات الى امن المعلومات واصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة وتوقيتها حيث ان الاجراءات الامنية المناسبة يمكن ان تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها وكانت شركة IBM الامريكية أول من وضع تعريف لامن المعلومات، وكانت تركز على حماية البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات وأشارت الشركة إلى أن أمنا تاماً للبيانات لايمكن تحقيقه ولكن يمكن تحقيق مستوى مناسب من الامنية.

والسؤال الذي يطرح هذا ماذا سيكون بعد أمن المعلومات؟ البعض يقول أمن المعرفة knowledge Security وذلك لانتشار أنظمة الذكاء الاصيطناعي وازدياد معدلات تناقل البيانات بسرعة الضوء أو التفاعل بين المنظومات والشبكات وصغر حجم أجهزة الحاسوب المستخدمة.

الاخطار التي يمكن أن تتعرض لها أنظمة المعلومات المحوسبة

لقيد أصبح اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الاخيرة. ومع مرور الزمن نجد أنه على الرغم من سبل الحماية التي تتبعها المنظمات ارتفاعاً واضحاً في معدل الاختراقات مع تنوع الوسائل المستخدمة في الاختراق، بالإضافة إلى طبيعة الاخطار التي يمكن أن تواجهها نظم المعلومات، فإن الاخطار عديدة والبعض منها قد يكون مقصوداً كسرقة المعلومات أو إدخال الفيروسات وغيرها وهي الاشد ضرراً على نظم المعلومات ويكون مصدرها أحياناً من داخل المنظمة أو خارجها، وقد يصعب أحياناً التنبؤ بالدوافع العديدة للاشخاص الذين يقومون بها، أما بعض الاخطار فقد يكون غير مقصود كالاخطاء البشرية والكوارث الطبيعية.

يمكن تصنيف الاخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات:

أ . الاخطاء البشرية : Human Errors

وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات للمستخدمين. وتشكل هذه الاخطاء الغالبية العظمى للمشاكل المتعلقة بأمن نظم المعلومات في المنظمات وسلامتها.

ب. الاخطار البيئية :Environmental Hazard

وهذه تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق، إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد وغيرها. وتؤدي هذه الاخطار إلى تعطيل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبياً لاجراء الاصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.

ج. الجرائم المحوسبة Computer Crime:

تمثل هذه الجرائم تحدياً كبيراً لادارة نظم المعلومات لما تسببه من خسارة كبيرة. وبشكلٍ عامٍ يتم التميز بين ثلاثة مستويات للجرائم المحوسبة وهي:

١. سوء استخدام جهاز الحاسوب: وهو الاستخدام المتعمَّد الذي يمكن أن يسبب خسارة للمنظمة أو تخريباً للاجهزة بشكلٍ منظمٍ.

٢. الجريمة المحوسبة: وهي عبارة عن سوء استخدام ألاجهزة الحاسوب بشكل غير قانوني يؤدي إلى ارتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب.

٣. الجرائم المتعلقة بالحواسيب: وهي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة. ويمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة يقومون (باختراق نظام الحاسوب)غالباً من خلال الشبكات أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة .

أهمية أمن المعلومات:

١.القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.

٢.حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.

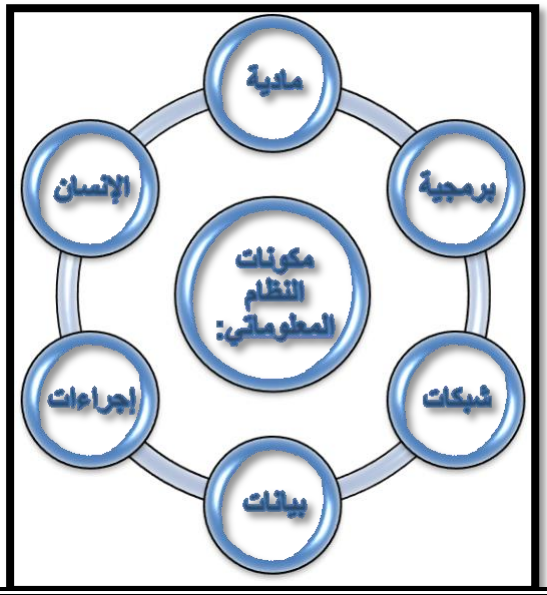
٣.الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم مختلف القطاعات

٤.النمو السريع في استخدامات التطبيقات الالكترونية والتي تتطلب بيئة آمنة.

٥.الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.

٦.مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني.

مكونات النظام المعلوماتي:



أ. منظومة الأجهزة الإلكترونية وملحقاتها:

إن أجهزة الحواسيب تتطور بشكل كبير وبالمقابل هنياك تطور في مجال السبل المستخدمة لاختراقها، ممن يتطلب تطوير القابلية والمهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب والعبث المقصود في الاجهزة أو غير المقصود.

ب. الأفراد العاملين في أقسام المعلومات:

إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم، وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الافراد، إضافةً إلى وضع الخطط لزيادة الحس الامني والحصانة من التخريب. كما يتطلب المراجعة الدورية للتدقيق في الشخصية والسلوكية لافراد العاملين من وقت إلى آخر وربما يتم تغير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محدّدين.

ت. البرمجيات المستخدمة في تشغيل النظام:

اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن أن تحقق حماية للبرامج وطرق حفظ لكلمات السر وطريقة إدارة نظام التشغيل وأنظمة الاتصالات، إن أمن البرمجيات يتطلب أن يؤخذ بعين الاعتبار عند تصميم النظام، كتابة برامجه من خلال وضع عدد من اإلجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام، وذلك من خلال تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها.

ث. شبكة تناقل المعلومات:

وضع إجراءات حماية وضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات وتوفير الاجهزة الخاصة الفحص. كما أن نظم التشغيل المستخدمة المسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عاليتين على الكشف عن التسلل إلى الشبكة وذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المشفرات وربطها بخطوط الاتصال، وهذه المشفرات تستخدم الخوارزميات الرياضية أو أجهزة ومعدات لغرض تشفير تناقل المعلومات أو الملفات.

هـ. مواقع منظومة الأجهزة الإلكترونية وملحقاتها:

يجب أن تعطى أهمية للمواقع والبنيية التي تحوي أجهزة الحواسيب وملحقاتها، وحسب طبيعية المنظومات والتطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية الموقع وتحصينه من أي تخريب أو سطو وحمايتيه من الحريق أو تسريب المياه والفيضانات، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها وتحديد أساليب التفتيش واجراءاتها والتحقق من هوية الأفراد الداخلين والخارجين من الموقع وعمل سجل لذلك.