أهمية أمن المعلومات في مجتمعنا

أفكار و حلول للمحافظة على بيئة معلوماتية آمنة.

المهندس: عبد الله يحي المبارك
ماجستير أمن المعلومات والشبكات
قسم الحاسب الآلي- الكلية التقنية بالرياض
almubark@hotmail.com

المعلوماتية... والذي يطلق على عصرنا هذا «عصر المعلوماتية» حملت معها من الأهمية والفائدة في انتشارها وتبادلها بين القارات الخمس، والتي أصبحت ركيزة من ركائز هذا العصر الذي نعيشه.

وبانتقالها من قارة لقارة أخري عبر الأثير أو عبر الكبلات البحرية و البرية حملت معها الكثير من الأشياء الرائعة والرائدة للإنسانية.

وعلى عكس ذالك حملت معها من المخاطر والمخاوف الأمنية مما قد يجعل هذه التقنية المعلوماتية في زاوية من زوايا النسيان والخوف والإهمال.

مع دخول طوفان الشبكة العنكبوتيه «الانترنت» والتزايد المستمر لمستخدمي هذه التقنية، أصبح هناك مهاجمون ومقتحمون ومتطفلون يقضون الساعات في محاولة اختراق أو سرقة موقع أو الوصول إلي معومات مهمة تودي بصاحبها إلي عمليات الابتزاز المادي والمعنوي.

لذالك أصبح هاجس أمن المعلومات يقلق بال الكثير من المستفيدين و موفري هذه التقنية الحديثة.

قبل البدء في طرح بعض المخاطر والحلول المساعدة في عملية زيادة الوعي الأمني المعلوماتي، لابد من معرفة العناصر الأساسية لامن المعلومات والتي تكتمل في ثلاثة عناصر رئيسية وبفقدان احد هذه العناصر نفقد معنى الامنية المعلوماتية.

عناصر أمن المعلومات

السرية او الموثوقية : وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك .

التكاملية وسلامة المحتوى : التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به في اي مرحلة من مراحل المعالجة او الإرسال والاستقبال.

الاستمرارية : التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع.

المخاطر في بيئة أمن المعلومات

المخاطر عديدة في عالم المعلومات، ومحاولة إحصاء تلك المخاطر قد تكون شبة مستحيلة وذالك لأسباب تلك المخاطر بشكل سريع ومستمر . ولاكن يمكن تصنيف المخاطر إلى ثلاث مجموعات رئيسية وهي:

المخاطر الطبيعية: والتي قد تحدث اما عن طريق الكوارث الطبيعية او الحرائق.

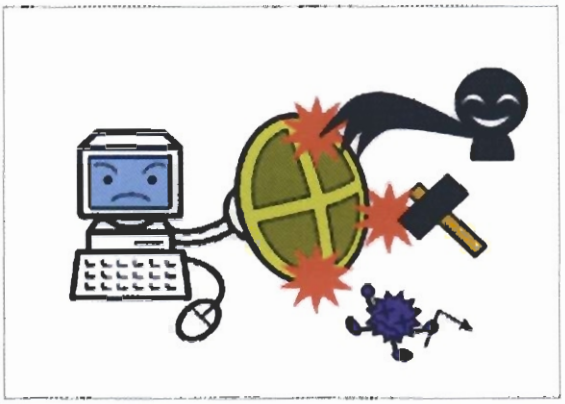
المخاطر العامة: والتي تحدث بشكل عام كانقطاع التيار الكهربائي أو سرقة الأجهزة بشكل مباشر.

نستطيع ان نقول انه يمكن التعامل مع المخاطر الطبيعية والعامة من حيث توفير وسائل وإجراءات الحماية للأجهزة الكمبيوتر والشبكات والبنى التحتية من ومسائل الطاقة والتوصيلات ومدى توفر وسائل الوقاية من الحوادث والكوارث الطبيعية او المتعمدة اضافة غالى وسائل حماية مكان وجود الأجهزة والوسائط ، والوسائل المادية للوصول إلى الأجهزة واستخدامها من المخولين بذلك كاستخدام مفاتيح الأبواب الذكية.

المخاطر الالكترونية :

وهنا نعني المخاطر التي قد تحدث للمعلومات داخل النطاق الإلكتروني،مثل تلك المعلومات المخزنة في الحاسب الشخصي client مرورا بالشبكة حتى جهاز الخادم server

وتتضمن تلك المخاطر اساليب مختلفة. فهناك انتحال الشخصية، والاستخدام الغير مرخص له، وعرقلة الخدمة، والتصنت،والاقتحام. ولا ننسى اكثر المخاطر إمعانا في الشر هي عمل ونشر الفيروسات، ولا يسعني في هذا المقال شرح جميع



تلك المخاطر وسوف اكتفي بشرح مبسط عن الفيروسات نظرا لما تشكل من اهمية وانتشار واسع بين أطياف المجتمع العزيز.

ما هو الفيروس؟

هو برنامج صغير مكتوب بأحد للغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعني انه يتركز علي ثلاث خواص وهي التخفي،التضاعف،والحاق الاذى.

مصادر الفيروس!

يكمن مصادر الفيروس من خلال الرسائل الالكترونية المجهولة، صفحات الانترنت المشبوهة، نسخ البرامج المقلدة، استخدام برامج غير موثقة، كذالك تبادل وسائل التخزين دون عمل فحص مسبق مثل الاقراص والذاكرة المتنقلة.

ما هو التاثير؟

كما أسلفت اعلاه ان للفيروس ثلاث خواص مؤثرة وهي:

التضاعف: تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملاين العمليات مما يسبب البطء في العمل او توقف الحاسب عن العمل.

التخفي: لابد للفيروس من التخفي حتى لا ينكشف ويصبح غير فعال، ولكي يتخفي فانة يقوم بعدة اساليب منها علي سبيل المثال، صغر حجم الفيروس لكي سينائه الاختباء بنجاح في الذاكرة أو ملف اخر.

الحاق الاذى: وهنا الجانب الملموس والمؤلم لدي الكثيرين الذين أصيب جهازه بفيروس خفيف أو مدمر، قد يتراوح الاذى الذي يسببه الفيروس بالاكتفاء بإصدار صوت موسيقي او مسح جميع المعلومات المخزنة لديك، ومن الامثلة الاخري في الحاق الاذى:

إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الانترنت مثلا او إلغاء البرنامج المكتوب على BIOS

أنواع الفيروسات:

تنقسم الفيروسات إلي عدة أنواع، الفيروس (Virus)، والدودة (Worm)، وحصان طروادة(Trojan horse)، وبرامج الهجوم (Attack scripts).

وكما قمنا بتعريف الفيروس والذي يعتبر بدورة الأب الأكبر لبقية أنواع الفيروسات يجدر بنا معرفة بقية الأنواع لأهمية تكاثرها في وقتنا الحالي.

الدودة (Worm): يتميز هذا النوع من الفيروسات عن بقية الانواع، انة يتميز بكونها ترسل نفسها منفردة إلى قائمة البريد الالكتروني او إلى كل جهاز بالشبكة وهى تنتشر بسرعة هائلة.

حصان طروادة(Trojan horse): يحمل بين طياته أهدافا شرسة وشريرة والتي تبدو للوهلة الاولي انها اهداف نبيلة، اكثر مصادرة هي البرامج المجانية.

برامج الهجوم (Attack scripts): وهي تصنف أنها برامج وقد تحمل بداخلها جميع ما ذكر أعلاه من انواع الفيروسات، وهي برامج قام علي كتابتها أناس محترفون جدا ولهم اهداف غير واضحة، قد يكون احد هذه الاهداف هي الحرب الالكترونية.

سبل الوقاية:

يعتبر الإنسان من أكثر المخاطر علي أمن المعلومات لذالك يجب ان تتركز الخطوة الاولي في عملية الحفاظ علي أمنية المعلومات هو عمل سياسة أمنية، شاملة لأفراد العائلة في المنزل أو لشركات علي نطاق أوسع، وان تحدد هذه السياسة بالتفصيل حقوق الوصول لتلك المعلومات ومسؤوليات الموظفين تجاه حماية تلك المعلومات، والإجراءات التي سوف تتخذ في حالة اختراق تلك المعلومات.

الخطوة الثانية وهي عملية تشفير المعلومات، تختلف درجة الأمن مع اختلاف أهمية تلك المعلومات، لذالك ينصح دائما بتغير شكل تلك المعلومات المنتقلة عبر الشبكة وهو ما يسمي بتشفير، وبالتالي لا يمكن لأحد تعديل او حذف جزء من تلك المعلومات.

الخطوة الثالثة وهي الناحية البرمجية، لاشك انه إذا كان هناك نسخة احتياطية من البيانات الهامة لديك سيكون ذلك عنصر من عناصر الأمان في استرجاع أخر نسخة موجودة قبل حدوث أي تخريب أو فقدان في البيانات المخزنة.

أيضا لا ننسي الجانب البرمجي الأهم وهو الحرص علي اقتناء برامج الحماية الأصلية، والتي اصبحت عنصر اساسي من عناصر الحاسب الشخصي، والابتعاد عن برامج الحماية المنسوخة، مع الأخذ بالاعتبار وجود الجدار الناري والذي بدورة يبقيك بعيدا عن برامج المتطفلين.