جامعة طرابلس
كلية تقنية المعلومات - قسم نظم المعلومات

المقرر الدراسي ITGS222

أساسيات نظم المعلومات
Foundation of Information Systems

إعداد

أ.إبتسام العاشوري
ebtesamalashouri@gmail.com

أ.فاطمة القاضي
algadyfatma@gmail.com

المحاضرة التاسعة

أمن نظم المعلومات

Information Systems Security

تعريف أمن نظم المعلومات (ISS):

- مجموعة من الإجراءات والتدابير الوقائية التي تستخدم للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال.
- الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية.
- يشير إلى السياسات والإجراءات، والتدابير التقنية المستخدمة لمنع الوصول الغير المصرح به، التغيير والسرقة، أو الأضرار المادية لنظم المعلومات.

عناصر أمن المعلومات

من المهم توافر عناصر أمن المعلومات في المعلومات المطلوب الحفاظ عليها وعدم كشفها للآخرين، ويختلف مدى أهمية توافر هذه العناصر جميعًا باختلاف أهمية المعلومات محل الحماية واستخداماتها، لدينا ثلاث عناصر أساسية في أمن المعلومات:

1. السرية (الموثوقية): هي حماية المعلومات من أن يطلع عليها أشخاص غير مرخص لهم الوصول إليها وكشفها وربما استخدامها استخداماً سلبياً يضر المنظمة سواء بشكل مباشر أو غير مباشر، لذلك تعتبر السرية أول وأهم عناصر أمن المعلومات والتي ينبغي تطبيقها في تعاملاتنا الإلكترونية.

عناصر أمن المعلومات

2. سلامة المحتوى: هي سلامة المعلومات من التغيير أو التعديل عليها أو حذفها من قبل أشخاص غير مرخص لهم، ويترتب على انتهاك هذا العنصر عواقب شديدة تبعًا لأهمية المعلومات المستهدفة، قد يكون هذا التغيير من الصعب اكتشافه وبالتالي قد يؤثر على مكانة المنظمة وجودة عملها، لذلك لابد من التأكد من عمل جميع التحصينات التي تحمي أمن المعلومات وتضمن العنصر الثاني سلامة المحتوى.

3. التواجد والاستمرارية: توفر المعلومات متى ما تم الحاجة إليها ومن ثم إمكانية الاستفادة منها من خلال قنوات أمنية سليمة، مثال على ذلك: تعطل القرص الصلب في الحاسوب مما يؤدي إلى تعذر الوصول إلى المعلومات والاستفادة منها أو تعطل نظام معلوماتي كامل على مستوى أكبر، إذاً الاستمرارية عنصر مهم ذات تأثير جذري على أمن المعلومات ينبغي توفرها في أنظمة المعلومات.

الأخطار التي تتعرض لها نظم المعلومات

عندما يتم تخزين كميات كبيرة من البيانات في شكل إلكتروني، فهي عرضة لأنواع كثيرة من التهديدات، من خلال شبكات الاتصالات، فالترابط بين نظم المعلومات والمواقع المختلفة، يمكن يؤدي بدخول لأشخاص غير مرخص لهم، وبالتالي يمكن الوصول إلى البيانات المتدفقة عبر الشبكات، وسرقة البيانات القيمة أثناء الإرسال، أو تغيير الرسائل دون إذن. كما يمكن تعطيل شبكة في نقاط مختلفة، كذلك يمكن إطلاق المتسللين هجمات الحرمان من الخدمة أو البرامج الضارة لتعطيل تشغيل المواقع على شبكة الإنترنت، كل هذه الأخطار قادرة على اختراق أنظمة المؤسسات وتدمير أو تغيير بيانات المؤسسات المخزنة في قواعد البيانات أو الملفات. كذلك استخدام الشبكات العامة الكبيرة، مثل الأنترنت Internet أكثر عرضة للاختراق من الشبكات الداخلية internal لأنها متاحة للجميع.

انواع الأخطار التي تتعرض لها نظم المعلومات

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

أ . الأخطاء البشرية Humane Errors

وهي التي يمكن أن تحدث أثناء تصميم نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو تجميع البيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن وسلامة نظم المعلومات في المؤسسات، وتشمل المشاكل العرضية الناجمة عن كل من العاملين والموظفين، مثل: الموظف الذي يسيء فهم إجراءات التشغيل بطريق سجلات العملاء عن غير قصد.

انواع الأخطار التي تتعرض لها نظم المعلومات

ب . الأخطار البيئية Environmental Hazard

وتشمل الزلازل، العواصف، الفيضانات والحرائق والمشاكل المتعلقة بأعطال التيار الكهربائي، وغير ذلك من أعمال الطبيعة، إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد أو نشوب الحروب وغيرها، وتؤدي هذه الأخطار إلى تعطل عمل نظم المعلومات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات. فالحوادث الطبيعية والكوارث هي مصدر للمشاكل الأمنية فمشاكل هذه الفئة تشمل ليس فقط الفقدان الأولي للقدرة والخدمات، ولكن أيضا الخسائر الناجمة عن إجراءات استرداد النظام من المشكل الأول مثل حدوث خطأ بشري في النسخ الاحتياطي.

انواع الأخطار التي تتعرض لها نظم المعلومات

ج. جرائم الحاسوب Computer Crime

تواجه أنظمة المعلومات بعض المشكلات الشائعة التي تغزوها وتساهم في تدميرها أو تخريبها أو سرقة التخزين المعلوماتي المحفوظ في أجهزة الحاسوب، حيث أن بعض الهجمات تستهدف جهاز حاسوب واحد، في حين بعضها يمكن أن يستهدف الآلاف منها. ومع زيادة تواصل المؤسسات فيما بينها عبر الأنترنت، زادت الهجمات الإلكترونية والتي تمثل تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة، فجرائم الحاسوب هي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة، ويمكن أن تتم هذه الجرائم المحوسبة من قبل أشخاص خارج المؤسسة يقومون باختراق نظام المعلومات (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المؤسسة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة.

انواع الأخطار التي تتعرض لها نظم المعلومات

بعض أنواع الهجمات الإلكترونية الشائعة	تعريفـــــها
فيروس الكمبيوتر Computer Virus	عبارة عن وحدة صغيرة من التعليمات البرمجية التي تغزو برنامج الحاسوب أو الملفات، وعند تنفيذ البرنامج أو فتح الملف المصاب، يقوم الفيروس بنسخ نفسه ليغزو البرامج والملفات الأخرى في الحاسوب. فيفعل أشياء سيئة كمحو الملفات وإفساد البرامج، وهكذا ينتقل الفيروس لجهاز آخر عبر الملفات والبرامج المصابة بالفيروسات.
الدودة Worm	هي برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت, و إلحاق الضرر بهم أو بالمتصلين بهم.
أحصنة طروادة Trojan Horse	برامج تقوم بكسر الأمن، يتم إدخالها في جهاز الحاسوب دون الإحساس بها، قد تكون على شكل بطاقة تحية إلكترونية، أو لعبة، وتعمل كوسيلة لمتسلل يدخل للكمبيوتر لاحقا.
القنبلة المنطقية Logic Bomb	برامج أدخلت في جهاز الحاسوب الذي تم تصميمه لاتخاذ إجراءات في وقت معين أو عندما يحدث حدث معين.
هجمات حجب الخدمة Denial of Service Attack	عدد كبير من أجهزة الحاسوب على الأنترنت ترسل في نفس الوقت رسائل متكررة لحاسوب مستهدف، مما يؤدي إلى التشويش على الجهاز وخطوط الاتصالات وبالتالي حرمان المستخدم من الحصول على الخدمة.

الحماية من أخطارنظم المعلومات

تعتبر الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية:

- العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات .
- توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة .
- وجود التجهيزات المحوسبة لدى أفراد عديدين في المؤسسة وأحيانا خارجها.
- صعوبة الحماية من الأخطار الناتجة عن ارتباط المؤسسة بالشبكات الخارجية.
- التقدم التقني السريع يجعل الكثير من وسائل الحماية عديمة الفائدة من بعد فترة وجيزة من استخدامها.
- التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمؤسسة إمكانية التعلم من التجربة والخبرة المتاحة.
- تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المؤسسات تحملها .

نظام إدارة أمن المعلومات

Information Security Management Systems

نظام إدارة أمن المعلومات (ISMS) يشمل إيجاد بنية تنظيمية ، ووضع سياسات أمنية وتخطيط أنشطة الأمن المعلوماتي، وتحديد المسؤليات، والممارسات والإجراءات، والعمليات والموارد اللازمة لإدارة أمن المعلومات بكفاءة وفاعلية.

الهدف من نظام إدارة أمن المعلومات هو التأكد من أن نظام المعلومات قد تم تنفيذه كما هو مخطط، ومن أن النظام يعمل فعلاً لتحقيق الأهداف التي وضع من أجلها،ومن أن العمليات امنة من الاستخدام السيئ، حيث ان غياب نظام ادارة امن المعلومات (نظام الرقابة) يمكن أن يؤدي إلى انتهاك امن البيانات والمعلومات انتهاكاً متعمداً او غير متعمد،وينتج عن ذلك تعديل او تدمير او افشاء للمعلومات.

أمن الشبكات Network Security

هناك الكثير من شبكات نظم المعلومات "الإنترانت" المكتفية ذاتياً وغير الموصولة بالعالم الخارجي، وتُعد هذه الشبكات محصنة ومعزولة من الناحية الفيزيائية عن غيرها من الشبكات، ولكن تكون المشكلات الأمنية ذات مصدر داخلي، وهذا النوع من المشكلات يعد الأكثر انتشاراً بين المنظمات مثل (تأمين النفاذ للمستخدمين دون عقبات فنية، تحديد مستويات السماح بالوصول إلى كل المعلومات لكل مجموعة من مجموعات العمل) لكن عندما توصل شبكة نظم المعلومات الداخلية "الإنترانت" بالشبكة العالمية " الإنترنت" تتغير المسائل الأمنية بقوة وتظهر مشكلة كيفية ضمان الأمن من المخترقين الخارجيين، وحماية المعلومات السرية والحساسة من النفاذ غير المشروع.

يعرف أمن الشبكات بأنه :"مجموعة الإجراءات الواجب اتخاذها لضمان استخدام الشبكة من قبل الأشخاص المرخص لهم فقط ووفق الكيفية المسموح بها".

السياسة الأمنية Policy Security

يقصد بالسياسة الأمنية مجموعة الأسس والإجراءات الواجب إتباعها لضمان أمن شبكة الإنترانت وردع المتطفلين، وتتكون هذه الإجراءات من وسائل تقنية وقرارات أمنية تتآلف فيما بينها لجعل موارد الشبكة منيعة وصعبة المنال .فبعد الانتهاء من وضع الخطة الأمنية الخاصة بالمنظومة الشبكية للمنظمة يمكن البدء بتنفيذ الإجراءات المختارة واقتناء التجهيزات الأمنية المناسبة للحصول على محيط عمل آمن، ومن أكثر التقنيات الأمنية تداولاً الجدران النارية وأجهزة كشف الاقتحام.

1. الجدار الناري Firewall:

يعد الجدار الناري من أكثر الوسائل الدفاعية فعالية في حماية الشبكة الخاصة بالمنظمة من الاختراق والاستعمال غير المشروع من قبل مستخدمي الشبكات الخارجية غير الموثوقة المتصلة بشبكة الداخلية للمنظمة، إذ يقوم الجدار الناري بضمان منع النفاذ للشبكة وذلك بعمله كبوابة بين شبكتين.

تابع السياسة الأمنية

الجدار الناري عبارة عن نظام أمني من البرمجيات Software والتجهيزات Hardware مخصص لحماية شبكة منظمة ما من الأخطارالخارجية كالمخترقين (الهاكر) hacker النافذين من شبكات أخرى كالإنترنت، وذلك عبر آليتين اساسيتين، الأولى تتحكم بمنع الاتصال وفق قواعد وشروط محددة، أما الثانية فتتحكم بالسماح بالاتصالات وفق قواعد وشروط صريحة، ويقوم الجدار الناري بمنع حواسب شبكة المنظمة من الاتصال المباشر بأي حاسب خارجي سواء كانت طالبة أو مطلوبة، كما يتولى تسيير جميع الاتصالات إلى مخدم وكيل موجود خارج شبكة المنظمة لكي يفحص الرسائل الواردة ويقرر فيما إذا كان تمريرها إلى شبكة المنظمة آمن أم لا، ومن الجدير بالذكر أن الجدار الناري لا يشكل الحل المتكامل لأمن الشبكة فهو لا يعالج التهديدات الداخلية لذلك لابد من إتباع إجراءات أمنية دقيقة داخل المنظمة تضمن أمن شبكتها.

تابع السياسة الأمنية

2. كشف اقتحام الشبكات:

تقوم أجهزة كشف الاقتحام بدور أمني علاجي شديد الأهمية، فهي تحاول كشف عملية اقتحام الشبكة واكتشاف وجود أي تصرف شاذ أو مريب على الشبكة، والتنبيه له خلال أجهزة كشف الشذوذ وأجهزة كشف سوء الاستخدام، إن أجهزة كشف الشذوذ تستخدم الطرق الإحصائية لمحاولة التعرف إلى أية نشاطات تخرج عن السلوك الطبيعي عبر تدوين سجلات للداخلين إلى الشبكة وتنبيه مديري نظم المعلومات عند اكتشافها لأي نشاط مريب، بالمقابل تفحص أجهزة سوء الاستخدام حركة نقل المعلومات مستخدمة عينات منها، فتقوم بمقارنة هذه العينات ببصمات أو سيناريوهات معروفة خطرة أو مريبة، ولايستخدم هذا النوع من التجهيزات إلا لكشف نماذج محاولة اختراق معروفة.

الهجمات السيبرانية
cyber attacks

كلمة سيبراني تعتبر ترجمة حرفية لكلمة Cyber والمشتقة من كلمة Cybernetics والتي استخدمت في الماضي للدلالة عن كيفية تواصل الآلات والكائنات الحية مع بعضها. وقد أُصطلح على أن تُطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت.

معظم التعاريف التي وردت بشأن الهجمات السيبرانية تشترك في معنى متقارب وهو استهداف مواقع إلكترونية أو نظام كمبيوتر أو جهاز كمبيوتر من خلال وسائل اتصال إلكترونية أخرى، مما يهدد سرية أو سلامة أو توفر المعلومات المخزنة عليه، وعادة ما تكون صادرة من مصدر مجهول إما يسرق أو يغير أو يدمر هدفاً محدداً عن طريق اختراق نظام حساس.

خصائص الهجمات السيبرانية

تعتبر هذه الهجمات (الجرائم) ذات خصائص خاصة لا تتوفر في الجرائم التقليدية، فهي ذات بعد عالمي لا حدود جغرافية لها، كذلك هناك تبادل الخبرات الإجرامية فيما بين المجرمين لابتكار أساليب جديدة مواكبة، ولا تتطلب مجهودا بل تنفذ بأقل جهد ممكن ولا تتطلب عنفاً، وتعد أهم خصائصها:

- صعوبة الاكتشاف لأنها لا تترك أثراً يسهل تعقبه، بالإضافة إلى أن الضحية لا تلاحظها إلا بعد وقت من وقوعها.
- السرعة وغياب الدليل وصعوبة إثباته بالإضافة إلى توفر وسائل تقنية تعرقل الوصول للدلائل والبراهين.
- التقنية العالية والخبرة الفائقة للمجرم في مجال الاتصالات، الشبكة العنكبوتية، استخدام الحاسوب والتكنولوجيا المعاصرة.
- ضعف الأجهزة الأمنية والقضائية تجاهها نتيجة نقص الخبرة التقنية لديها نظراً لما تتطلبه هذه الجرائم من تقنية لاكتشافها والبحث عنها.

الأمن السيبراني
Cyber Security

الأمن السيبراني :هو الأمن الذي يتعلق بالحماية من المخاطر المحتملة عن طريق مصادر خارجية وخاصة الإنترنت، حيث يعمل مختصو الامن السيبراني على حماية الحواسيب المكتبية أو المحمولة من أي نوع من الهجمات والاختراقات والتهديدات التي تحدث عن طريق السيرفرات والحواسيب الأخرى وشبكة الإنترنت بشكلٍ عام، كما ويحاول مختصو الأمن السيبراني ضمان عدم السماح لأحد غير مصرح له بالدخول والوصول إلى المعلومات بالوصول إليها، حيث يمكن لهذا الشخص أن يثبت بعض البرامج الخطيرة وأن ينسخ المعلومات أو يعدلها، وفي هذه الحالة يكون الامن السيبراني ضعيفًا ويحتاج لتقوية، بالتالي فإن مهمة هذا النوع من الأمن تكمن في حماية الحاسب كله من المصادر الخارجية.

الفرق بين الأمن السيبراني وأمن المعلومات

تعتبر قيمة المعلومات وحمايتها هي نقطة اهتمام نوعي الأمن، إلا أن الأمن السيبراني يركز على حماية المعلومات من الأخطار الخارجية والوصول الخارجي غير المصرح به لهذه المعلومات، في حين يركز أمن المعلومات على سرية هذه المعلومات وتوافقها مع بعضها وتوافرها الدائم، وقد يشمل ذلك المعلومات غير الإلكترونية أيضًا، لكن في ظل سيطرة التكنولوجيا يتخذ امن المعلومات شكله التقني ويوفر حماية تقنية للمعلومات كافة.

باختصار يمكن اعتبار الامن السيبراني جزءًا أو تخصصًا من أمن المعلومات، ويهتم القائمين على النوعين بكل ما يتعلق بحماية البيانات (التي تعتبر أصل المعلومات) من التهديدات المختلفة، وبتشبيه آخر فالاختلاف يشبه الفرق بين العلم والكيمياء.