الحاسوب

الكورس الاول

امن المعلومات

والجرائم الالكترونية

الجزء الاول

م.م. زينة رجب الالوسي

كلية القانون/ جامعة بغداد

المرحلة الثانية

١. امن المعلومات Information Security

مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق الكترونية مختلفة (نقل البيانات) اصبح استخدام الحواسيب ونقل المعلومات عبر الشبكات المحلية والدولية من الامور الروتينية في يومنا هذا واحدى علامات العصر المميزة التي لايمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الاعمال وتطوير اساليب الخزن وتوفير المعلومات ، اذ ان انتشار انظمة المعلومات المحوسبة أدى الى أن تكون عرضة للإختراق او الضياع. فأصبحت هذه التقنية سلاحاً ذو حدين يحرص الجميع على اقتناؤه وتوفير سبل الحماية له. واصبح النظر إلى أمن تلك البيانات والمعلومات يشكل جزء اساسي ومهم للغاية.

يمكن تعريف امن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية. ووضع المعايير والإجراءات الامنية اللازمة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين.

يتمثل امن المعلومات بشكل عام بحماية معلومات معينة من أن تعاين، أو تستخدم من قبل أشخاص غير مخول لهم بذلك، أو من أن تكشف للعلن، أو توزع، أو أن تعدّل، أو من أن تدمر أو تحذف. هذا التعريف ينطبق على أي نوع من المعلومات سواء كانت المعلومة مكتوبة على ورق أو موجودة في ملف ما على الإنترنت

أمن المعلومات ، من *زاوية اكاديمية* ، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها . ومن *زاوية تقنية* ، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية . ومن *زاوية قانونية*، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت) .

واستخدام اصطلاح أمن المعلومات Information Security وان كان استخداما قديما سابقا لولادة وسائل تكنولوجيا المعلومات ، الا انه وجد استخدامه الشائع بل والفعلي ، في نطاق انشطة معالجة ونقل

البيانات بواسطة وسائل الحوسبة والاتصال ، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت - احتلت ابحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة ، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات .

٢. عناصر أمن المعلومات

أ. السريّة: تعني منع اطلاع أي شخص غير مخوّل من الوصول إلى البيانات .

ب. التكامليّة وسلامة البيانات: وتعني التكامليّة هنا المحافظة على البيانات من التعديل أو التغيير من قبل الأشخاص غير المخوّلين بالوصول لها.

ج. توفر البيانات: وتعني توفر البيانات كاملةً عند الحاجة إليها بحيث تكون معلومات صحيحة ودقيقة غير معدّلة أو ناقصة، مما يجعل عناصر النظام تعمل بشكلٍ صحيح.

٣. اشكال التجاوزات في العالم الرقمي

هنالك اشكال مختلفة للمخالفات القانونية في عالم الانترنيت والحاسوب والتي تصدر من بعض المستخدمين لغرض الوصول الى اهداف تخالف القانون والخلق العام وانتهاك خصوصية الاخرين، وتشمل:

أ. التخريب

ب. الاطلاع أو التزوير

ج. جرائم الملكية الفكرية (التقنية)[١]: وتشمل نسخ البرامج بطريقة غير قانونية وسرقة البرامج التطبيقية سواء كانت تجارية او علمية او طبية، اذ تمثل هذه البرامجيات جهوداً تراكمية من البحث.

د. الاحتيال Fraud احتيال التسويق ، سرقة الهوية، الاحتيال على البنوك والاحتيال عن طريق الاتصالات، وسرقة الارصدة والاموال من خلال التحويل الالكتروني من البنوك او الاسهم.

هـ. سرقة البيانات الخاصة والتشهير بالاخرين وابتزازهم.

[١] الملكية الفكرية هي كل ما ينتجه العقل الانساني من اختراعات وابداعات وغيرها كما عرفتها المنظمة العالمية الفكرية بأنها اعمال الفكر الابداعية من الاختراعات والمصنفات الفنية والادبية والرموز والاسماء والصور والنماذج والرسوم الصناعية.

٤. خصوصية الحاسوب Computer Privacy

يستخدم هذا المصطلح ليشير الى الحق القانوني في الحفاظ على خصوصية البيانات المخزنة على الحاسوب او الملفات المشتركة. وتظهر حساسية مسألة خصوصية الحاسوب او البيانات الخاصة عندما يتعلق الامر ببيانات التعريف الشخصية المحفوظة في اي جهاز رقمي (سواء كان حاسوب او غيره) ومن اكثر المشاكل التي تكون محور خصوصية البيانات فهي:

- **المعلومات الصحية**
- **السجل العدلي**
- **المعلومات المالية**
- **المعلومات المحددة للشخصية : وهي معلومات تحدد شخصية مستخدم الإنترنت كتاريخ الميلاد, الاسم الحقيقي ,الصورة الشخصية , عنوان الشخص أو رقم جواز سفره**

٥. مهددات أمن المعلومات

- **البرمجيات الخبيثة Malware**

مصطلح Malware هو اختصار لكلمتي"Malicious Software"وهو يشمل الكثير من انواع البرمجيات الخبيثة التى تتسبب في العديد من المشاكل وهناك أنواع مختلفة منها، وتشمل هذه البرامج الضارة الفيروسات، الديدان، أحصنة طروادة، الجذور الخفية، و برامج التجسس ، Keylogger والكثير من الأنواع الأخرى.

معظم الناس يستخدم لفظ فيروس للدلالة علي اي نوع من تلك البرمجيات الخبيثة ولكن في الحقيقة الفيروس نوع من هذه البرمجيات الخبيثة. وللحصول على فكرة عامة عن الفرق بين كل هذه الأنواع من التهديدات و طرق عملها ، فمن المنطقي تقسيمها إلى مجموعات:

أ. الفيروسات

الفيروسات نوع من البرمجيات الخبيثة مصممة بغرض تغيير خصائص الملفات التي تصيبها، لتقوم بتنفيذ بعض الأوامر مثل الإزالة والتعديل أو التخريب وتقوم بالسيطرة على الجهاز أو سرقة بياناته، وما يشبهها من عمليات أخرى.

تؤثر الفيروسات في الملفات التنفيذية وملفات نظام التشغيل، و يمكنها أن تدمر أجزاء في البيانات والملفات على الجهاز أو تمسحها وتقوم بنقلها من جهازك للأجهزه أخرى.

من أبرز طرق الانتقال لحد الآن الشبكة العنكبوتية Internet ، بحيث تعتبر بوابة سهلة لانتقال

الفيروسات من جهاز لآخر. تأتي ضمن رسائل البريد الإلكتروني و كثيرا ما ترسل الفيروسات كمرفقات مثل الصوروالبطاقات، أو ملفات الصوت و الفيديو التي ترفق رسائل البريد الإلكتروني أو في الرسائل الفورية. او قد تتسرب إلى الجهازعبر وسائط التخزين مثل ذواكر الفلاش (Flash Memory)والأقراص المدمجة (CD, DVD). يمكن أن تنتشر أيضا من خلال تنزيل بعض الفايلات (Download) عبر شبكة الإنترنت. لأنها يمكن أن تكون مخفية ضمن برامج او ملفات غير مشروعة.

ب. الدودة (Worm)

هذا النوع مشابه للفيروس ولكنه يختلف في طريقة انتشاره وبدلا من الاعتماد علي الشخص المستخدم في تشغيله ونقله من جهاز لاخر , يقوم هذا النوع بنشر نفسه بنفسه عبر الاجهزة في الشبكة وهذا النوع ينتشر عبر سيرفرات الشبكة وخاصة الانترنت ولكن هذا النوع قد قل هذه الايام وذلك لان الويندوز اصبح مدعم بجدار ناري قوي Firewall[٢] عند تثبيته بخلاف ويندوز xp ولكن الـ wormيمكن ان ينتشر ويجد طريقه بطرق اخري مثل ارسال نفسه عبر البريد اللكتروني للجهاز المصاب الي جميع العناوين الموجوده علي هذا الايميل وبالتالي نشر نفسه علي كل الاجهزة صاحبة هذه العناوين ومثل الفيروس هذا النوع يمكن ان يحدث اي ضرر بجهازك كالذي يصنعه الفيروس الاختلاف فقط في طريقة انتشاره وهو ما اكسبه هذا الاسم.

[٢] جدار الحماية الناري Firewall هو برنامج أو جهاز يقوم بفرز وتصفية البرامج الخبيثة والمتسللين الذين يحاولون الوصول إلى جهاز الكومبيوتر عبر الإنترنت.

ج. حصان طروادة (Trojan Horse)

احد انواع البرمجيات الخبيثة والذي يتنكر في احد الملفات الشرعية الموثوق بها وعندما تقوم بتحميل الملف وتشغيله سيقوم بتشغيل نفسه (Trojan) ايضا في الخلفية وهذا النوع من الممكن ان يقتحم خصوصياتك كمراقبة كل نشاطك علي الجهاز او ربط جهازك مع روبوت ويمكنه كذلك فتح المجال امام جهازك لاصابته بالعديد من البرمجيات الخبيثة الاخرى. سمي هذا البرنامج بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة ، اذ اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها.

د. ملفات التجسس (Spyware)

هو نوع من البرمجيات الخبيثة يقوم بالتجسس دون علم صاحب الجهاز ويقوم بجمع العديد من المعلومات المختلفة وأكثر هذه الانواع تقوم بالتواجد ضمن برامج مجانية وتقوم بمراقبة وفحص نشاطك علي الانترنت لتتعرف علي المواقع التي تتصفحها واهتماماتك وتقوم بارسال هذه المعلومات لاي سيرفر اعلاني ليستخدمها في الترويج لاعلاناته من خلال بياناتك.

هـ. ملفات دعائية (Adware)

هي برامج مصممة للدعاية والاعلان وتغيير الإعدادات العامة في اجهزة الحاسوب، مثل تغيير الصفحة الرئيسية للمتصفح وإظهار بعض النوافذ الدعائية اثناء اتصالك بالانترنيت وتصفحك للمواقع الألكترونية.

و. مسجل ضربات المفاتيح (Key logger)

وهو نوع من البرمجيات الخبيثة والتي تقوم بتسجيل كل ضغطة علي اي زر في لوحة المفاتيح وهذه الضغطات قد تتضمن عناوين حسابك واسم المستخدم وكلمات المرور لاي حساب او بطاقة ائتمان او غيرها والذي يقوم هذا النوع برفعها علي سيرفر لمطوري الـ Keylogger ثم يقومون بتحليل هذه الضغطات والبيانات التي تظهر لهم واستخلاص المفيد منها.

ز. برنامج الفدية Ransomware .

يقوم بتشفير الملفات الخاصة بالضحية وطلب مبلغ من المال (فدية) من اجل فك تشفير هذه الملفات.

- الاضرار الناتجة عن البرامج الخبيثة

أ. تقليل مستوى الاداء

ب. ايقاف تشغيل الحاسوب واعادة تشغيل نفسه تلقائياً كل بضع دقائق او اخفاقه بالعمل بعد اعادة التشغيل.

ج. حذف الملفات او تغيير محتوياتها

د. ظهور مشاكل في التطبيقات المنصبة وتغيير نوافذ التطبيقات والقوائم والبيانات.

ه. تكرار ظهور رسائل الخطأ في اكثر من تطبيق.

و. افشاء معلومات واسرار شخصية هامة.

- صفات الفيروسات

أ. القدرة على التناسخ والانتشار Replication

ب. ربط نفسها ببرنامج اخر يسمى الحاضن (المضيف Host).

ج. يمكن ان تنتقل من حاسوب مصاب الى اخر.

- مكونات الفيروسات

يتكون برنامج الفيروس بشكل عام من اربعة اجزاء رئيسة تقوم بالاتي:

١) آلية التناسخ : تسمح للفيروس ان ينسخ نفسه.

٢) آلية التخفي : تخفي الفيروس عن الاكتشاف.

٣) آلية التنشيط : تسمح للفيروس بالانتشار.

٤) آلية التنفيذ : تنفيذ الفيروس عند تنشيطه.

- **الاختراق او القرصنة الالكترونية (Hacking)**

الاختراق بشكل عام هو القدرة على الوصول لهدف معين(جهاز شخص ما) بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول الى جهاز آخر فهو مخترق (Hacker) أما عندما يقوم بالاختراق وحذف ملف أو تغييره أو تعطيله فهو مخرب(Cracker) .

تقسم هجمات المخترقين إلى نوعين، و ذلك بناءً على الضرر الذي ستسببه الهجمة، فإذا كان الهجوم سيُسبب ضرراً أو تعديلاً او تغييراً بالنظام فإنه يُسمى بالهجوم النشط *Active Attack*، و لكن إذا كان هدف الهجوم الحصول على البيانات فقط دون إحداث أي تعديل أو ضرر فيُسمى بالهجوم الخامل *Passive Attack*.

الهجمات النشطة Active Attacks

1. **التعديل Modification**
2. **الخداع Spoofing**
3. **إعادة الإرسال Replaying**
4. **الإنكارRepudiation**
5. **حجب الخدمة Denial of Service (Dos)**

الهجمات الخاملة Passive Attacks

1. **التجسس Snooping**
2. **تحليل البيانات المرسلة Traffic Analysis**

انواع المخترقون

١. أصحاب القبعات البيضاء White Hat Hackers

أصحاب القبعات البيضاء ويعرفوا أيضا بالـ Ethical Hackers أو الهاكر الأخلاقي .هذا الشخص يملك خبرات ومهارات الهاكرز وهو قادر على اختراق الأنظمة والشبكات بنفس الأسلوب والأدوات التي يستخدمها المخترقين لكنّه يستغل خبرته في الأمور الجيدة كأن يبلّغ الشركات عن وجود ثغرة في احدى منتجاتها أو يعمل Penetration Tester أو ان يكون مسؤول الحماية في احدى الشركات.

٢. أصحاب القبعات الرماديّة Gray Hat Hackers

أصحاب القبعات الرماديّة, يمكننا القول أنهم هاكرز أخلاقيين أيضاً وهم يشبهون الصنف الأول (أصحاب القبعات البيضاء) كثيراً لكن بنفس الوقت قد يقوموا ببعض الاختراقات بغرض التحدي مثلاً أو لاثبات وجود ثغرة أو لايصال رسالة معيّنة.

٣. أصحاب القبعات السوداء Black Hat Hackers

أصحاب القبعات السوداء ، هؤلاء الأشخاص يستغلون معرفتهم وخبراتهم في الأمور التخريبية ويخترقون المواقع والسيرفرات بغرض المتعة واثبات الوجود أو لغايات أخرى غالبا تكون غير شرعية كالابتزاز وسرقة المعلومات أو اختراق مواقع الشركات وحسب وجهة نظر مختصي امنية المعلومات فيجب اطلاق لقب Crackers عليهم وليس Hackers

٤. اطفال الاكواد Script Kiddies

ان هذه الفئه هي المنتشره على الانترنت وهي مجموعه من عديمي الخبرة يستخدمون البرامج الجاهزه لتقوم ببعض العمليات البرمجيه بشكل عشوائي للتخريب والاختراق.

كيف يتم الاختراق

لا يمكن ان يتم الاختراق الا فى حاله وجود ملف تجسس داخل الجهاز المّخترق ويعتمد الإختراق على السيطرة عن بعد وهي لاتتم إلا بوجود عاملين مهمين : الأول البرنامج المسيطر ويعرف ب العميل Client والثاني الخادم Server الذي يقوم بتسهيل عملية الأختراق ذاتها .

وبعبارة أخرى لابد من توفر برنامج على كل من جهازي المخترق والضحية ففي جهاز الضحية يوجد برنامج الخادم وفي جهاز المخترق يوجد برنامج العميل . تختلف طرق إختراق الأجهزة والنظم بإختلاف وسائل الإختراق ، ولكنها جميعا تعتمد على فكرة توفر إتصال عن بعد بين جهازي الضحية والذي يزرع به الخادم (server)الخاص بالمخترق ، وجهاز المخترق على الطرف الأخر حيث يوجد برنامج المستفيد او العميل Client

- **الجرائم الالكترونية Cyber Crimes**

عبارة عن نشاط اجرامي تُستخدم فيه تقنيات الحاسوب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الاجرامي كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت والجرائم التي قد تهدد أمن الدولة وسلامتها المالية، او والتجارة غير القانونية (كتجارة المخدرات)، كما تضم انتهاك خصوصية الآخرين عندما يتم استخدام معلومات سرية بشكل غير قانوني.

- **أنواع الجريمة الإلكترونية**

١. **جريمة إلكترونية تستهدف الأفراد ويُطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية كالبريد الإلكتروني وكلمة السر الخاصة بهم وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد.**

٢. جريمة إلكترونية تستهدف الملكيّة يستهدف هذا النوع من الجريمة الجهات الحكوميّة والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية

٣. جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنّها القراصنة على المواقع الرسميّة الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتيّة للموقع أو النظام الشبكي وتدميره بالكامل ومثل هذه الهجمات في الغالب يكون الهدف منها سياسيّاً.

٤. النصب والاحتيال الإلكتروني.

٥. الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول لسرقة المعلومات التي تتعلّق بأمن الدولة.

٦. سرقة المعلومات الموثّقة إلكترونياً ونشرها بطرق غير شرعيّة

٧. جرائم الشتم والسبّ والقدح.

٨. جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد.

٩. جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.

١٠. الوصول إلى مواقع محجوبة.

١١. الإرهاب الإلكتروني.

١٢. الجرائم الجنسية الإلكترونية.

١٣. الجرائم المالية (مؤسسات مصرفية ومالية وبنوك)