

القرصنة الالكترونية

عندما يتبادر إلى أسماعنا كلمة قرصنة فإننا نتخيل عصابات سرقة السفن البحرية والسطو عليها ونهب ما فيها وأسر طاقمها، وهو ذاته ما يفعله قرصان الأنظمة الالكترونية بالضبط لكن بوسائل حديثة ودون إن يعرض نفسه للخطر .

فالقرصنة الإلكترونية أو المعلوماتية هي عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت غالباً لأن اغلب حواسيب العالم مرتبطة عبر هذه الشبكة او حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب ، ويقوم بهذه العملية شخص او عدة اشخاص متمكنين في برامج الحاسوب وطرق ادارتها أي انهم مبرمجون ذوو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين التعرف على محتوياته ومن خلالها يتم اختراق باقي الاجهزة المرتبطة معها في نفس الشبكة .



تصنيف قرصنة المعلومات:



يمكن تصنيف قرصنة المعلومات إلى قسمين :-

1- الهاكرز Hackers

نستطيع أن نعتهم بالمبتدئين أو الهواة الذي يكون الهدف من وراء اختراقهم للأنظمة الالكترونية التعلم والتسلية على الأغلب .



2- الكراكرز Crackers

وهم المخترقون المحترفون والذي يكون دخولهم إلى الحواسيب من اجل غاية معينة تحقق لهم ما يهدفون إليه .



اهم طرق اختراق الحاسوب:

تتم اغلب عمليات الاختراق عن طريق زرع برنامج معين في جهاز الضحية يقوم هذا البرنامج بعمل معين وكما يلي :-

1- الفايروسات Virus

هو برنامج له القدرة على نسخ نفسه اكثر من مرة ويمتاز بقدرته على التخفي وله آثار تدميرية على انظمة تشغيل الحاسوب لأن عملية النسخ والتكرار الدائم لملفاته تجعل هذه الملفات تحل محل الملفات الاصلية الموجودة على القرص الصلب Hard Disk للحاسوب .

2- أحصنة طروادة Trojans

هو برنامج تجسسي يقوم بعمل معين يحدده الشخص الذي صممه او زرعه في جهاز الضحية تمكنه من الحصول على مبتغاه .

3- الديدان Worms

هو برنامج ينتقل غالباً عبر البريد الالكتروني ويمتاز بقدرته على التنقل عبر شبكات الانترنت لغرض تعطيلها او التشويش عليها عن طريق شل قدرتها على تبادل المعلومات .



تقوم الأجهزة الأمنية لمختلف البلدان بالبحث عن العباقرة في مجال الحاسوب بهدف الصراع ضد الإرهابيين والمجرمين. حتى ان ممثلي اجهزة الامن في الولايات المتحدة الامريكية شاركوا خلال الصيف الماضي باجتماع دولي لقراصنة الانترنت في مدينة لاس فيغاس. ان التهديد باستخدام الشبكة العنكبوتية اصبح اكثر فاكثرا امرا واقعيا. فاي من المؤسسات والتشكيلات تقع في "منطقة الخطر" وعليها الدفاع ضد الهجمات الالكترونية؟ ومن يهدد امن الدول وسلامة المواطنين باستخدام الانترنت عدا الارهابيين؟ وهل تمتلك البلدان المختلفة اختصاصيين جاهزين للحرب في الانترنت؟ عن هذه الاسئلة وغيرها يجيب ضيوف برنامجنا.

معلومات عامة حول الموضوع:

ما الذي يمكن ان يقوم به القرصنة؟؟

الكوارث تتوالى في المؤسسات الصناعية الكبرى، وحركة المرور متوقفة. واجهزة التحكم الإلكترونية معطلة. لا معلوماتٍ ولا اتصالات. الجيش والأسطول مشلولان. مجرمون مجهولون يستولون على ادارات السيطرة والتحكم في البنى العسكرية الدفاعية دون ان يطلقوا رصاصة واحدة. ويوجهون الصواريخ النووية على هواهم.

هذا ليس فيلما من افلام هوليوود. كلا. فإن كارثة كهذه يمكن ان تحصل، الآن، في اية لحظة. سلاح الهجوم جاهز، وتُجرى عليه تحسينات متواصلة. انه الحاسوب، الكمبيوتر... وجنود هذه الحرب الإلكترونية هم "الهاكرز". هذه المفردة باتت مرادفة لكلمات مجرم الحاسوب... مخترق الكمبيوتر. الا ان لها معنى ايجابيا بين الهاكرز انفسهم. ويقصدون بها مصمم برامج الكمبيوتر

ما يفعله ويبدعه الهاكر يتوقف على
الجهة التي تدفع له. فهو يمكن ان يضع
برامج تطبيقية نافعة ويمكن ان يضع
برامج تجسسية. والحقيقة فإن مخترق
الكمبيوترات لا يختلف بشئ عن اللص
العادي، والفارق الوحيد انه لا يفتح قفل
الباب بل يدخل بوقاحة كمبيوترات
الغير، ويسرق المعلومات بدلا من
الحاجيات.

كبار المجرمين في عالم المال والأعمال
يجندون الهاكر اليوم لسرقة اموال
منافسيهم او إلحاق الضرر بهم.

وتنتشر اكثر فأكثر سرقة البنوك من خلال الشبكة العنكبوتية، ما يسمى انترنت بانكينغ. وقد ظهر رأسا جمهور كبير جدا من الراغبين في الإثراء من سرقة واختطاف المعلومات المصرفية. الهاكر الخبيث، مصمم برامج التجسس على البنوك، يضع يده على شفرة كود دخول أو وصول شخص أو عدة اشخاص الى الحسابات المصرفية الشخصية ويحوّل المبالغ منها الى الحسابات والعناوين التي يريدّها. وهناك اتجاه أحدث. الهاكر يستولي على موارد الإنترنت الحيوية بالنسبة للشركة المنافسة. ويمكن ان تكون تلك الموارد أو المصادر بشكل موقع الكتروني لمتجر يبيع من خلال الإنترنت أو دار نشر أو كازينو إلكتروني. يقوم الهاكر بمهاجمة الموقع فيعطله. ويبعث رسالة الى صاحبه يطالبه فيها بكلفة الهجوم، والا فإن الهجوم سيتكرر.

ذلك في الحقيقة نوع من انواع الإبتزاز المعهود،
ولكن على النطاق الدولي.
هجمات الفيروسات يمكن ان تضر بأناس لا علاقة
لهم بالتقنيات الرقمية. فالمعلومات المتعلقة بالرواتب
والأجور والمعاشات والمعونات الإجتماعية والمرافق
والخدمات تحفظ في اجهزة الحاسوب. ولذا فإن اي
عطل في الشبكة الموضعية او المحلية لدائرة حكومية
يمكن ان يضر بمئات الآلاف من الناس.









أمن المعلومات



عمل الطالبة: العنود الاحبابي

الصف الثامن

