الفصل الثالث (امان الحاسوب)

اولاً : اشكال التجاوزات في العالم الرقمي

تشمل عدد من المخالفات القانونية في عالم الانترنت والحاسوب ، والتي تصدر من بعض المستخدمين لغرض الوصول الى اهداف تخالف القانون والخلق العام والتجاوزات على خصوصية الاخرين ، وتشمل على :

١- جرائم الملكية الفكرية : وتشمل نسخ البرامج بطريقة غير قانونية وسرقة البرامج التطبيقية سواء كانت تجارية او علمية او عسكرية ، اذ تمثل هذه البرامجيات جهوداً تراكمية من البحث .
٢- الاحتيال : احتيال التسويق ، سرقة الهوية ، الاحتيال على البنوك والاحتيال عن طريق الاتصالات ، وسرقة الارصدة وسرقة المال من خلال التحويل الالكتروني من البنوك او الاسهم .
٣- سرقة البيانات الخاصة والتشهير بالآخرين وابتزازهم .

ثانياً : الاختراق الالكتروني وانواعه

هو قيام شخص غير مخول او اكثر بمحاولة الدخول (الوصول) الكترونياً الى الحاسوب او الشبكة عن طريق شبكة الانترنت وذلك بغرض الاطلاع والسرقة ، التخريب والتعطيل باستخدام برامج متخصصة .

يمكن تقسيم الاختراق الالكتروني من حيث الطريقة المستخدمة الى ٣ اقسام :

١- المزودات او الاجهزة الرئيسية للشركات والمؤسسات او الجهات الحكومية : وذلك باختراق الجدار الناري والتي توضع لحمايتها يتم ذلك باستخدام المحاكاة لغرض الخداع (Spoofing) هو مصطلح يُطلق على عملية انتحال شخصية للدخول الى النظام ، اذ ان حزم البيانات تحتوي على عناوين للمرسل والمرسل اليه وهذه العناوين يُنظر اليها على انها عناوين مقبولة وسارية المفعول من قبل البرامج واجهزة الشركة .
٢- الاجهزة الشخصية : والعبث بما فيها من معلومات . وتعد من الطرق الشائعة لقلة خبرة اغلب مستخدمي هذه الاجهزة من جانب ولسهولة تعلم برامجيات الاختراق وتعددها من جانب اخر .
٣- البيانات : من خلال التعرض والتعرف على البيانات اثناء انتقالها ومحاولة فتح التشفير اذا كانت البيانات مشفرة وتستخدم هذه الطريقة في كشف ارقام بطاقات الائتمان وكشف الارقام السرية لبطاقات البنوك .

ثالثاً : المخاطر الامنية الاكثر انتشاراً

١- الفايروسات : وتقسم الى ثلاثة انواع هي :
أ- الفايروس : برنامج تنفيذي ذو امتداد (com , exe , bat , pif , scr) ، يعمل بشكل منفصل ويهدف الى احداث خلل في الحاسوب ، وتتراوح خطورته حسب المهمة المصمم لاجلها ، فمنها البسيطة ومنها الخطرة ، وينتقل بواسطة نسخ الملفات من حاسوب يحوي ملفات مصابة الى حاسوب آخر عن طريق الاقراص المدمجة (CD) والذاكرة المتحركة (Flash Memory) .
ب- الدودة : تنتشر فقط عبر الشبكات والانترنت مستفيدةً من قائمة عناوين البريد الالكتروني (مثل تطبيق برنامج التحدث ماسنجر) فعند اصابة الحاسوب يبحث البرنامج الخبيث عن عناوين الاشخاص المسجلين في قائمة العناوين ويرسل نفسه الى كل الاشخاص في القائمة ، مما يؤدي الى انتشاره بسرعة عبر الشبكة .
ج- حصان طروادة : فايروس تكون آلية عمله مرفقاً (ملحقاً) مع احد البرامج ، اي يكون جزءً من برنامج دون ان يعلم المستخدم .
٢- ملفات التجسس : هي برامج مصممة لجمع المعلومات الشخصية مثل المواقع الالكترونية التي يزورها المستخدم وسجل بياناته وكلمة المرور للحسابات الالكترونية .
٣- ملفات دعائية : هي برامج مصممة للدعاية والاعلان وتغيير الاعدادات العامة في اجهزة الحاسوب مثل تغيير الصفحة الرئيسية للمتصفح واظهار بعض النوافذ الدعائية اثناء اتصالك بالانترنت وتصفحك للمواقع الالكترونية.

٤- قلة الخبرة في التعامل مع بعض البرامج : مع ازدياد استخدام الانترنت من عامة الناس غير المتخصصين ، واستخدامهم تعاملهم مع برامجيات متطورة الخاصة بخدمة تطبيقات الانترنت وبشكل مستمر وبدون خبرة كافية لكيفية التعامل مع تلك البرامجيات قد يفتح ثغرة في جهاز الحاسوب تُمكن الآخرين من اختراق الجهاز .
٥- اخطاء عامة : مثل سوء اختيار كلمة السر او كتابتها على ورقة مما يُمكن الآخرين من قراءتها ، او ترك الحاسوب مفتوح مما يسمح للاشخاص غير المخولين او الغرباء بالدخول الى ملفات الحاسوب او تغيير بعض الاعدادات .

رابعاً : الاضرار الناتجة عن فايروسات الحاسوب

١- تقليل مستوى اداء الحاسوب
٢- ايقاف تشغيل الحاسوب واعادة تشغيل نفسه تلقائياً كل بضع دقائق او اخفاقه في العمل بعد اعادة التشغيل .
٣- تعذر الوصول الى مشغلات الاقراص الصلبة والمدمجة (وحدات الخزن) وظهور رسالة تعذر الحفظ لوحدات الخزن .
٤- حذف الملفات او تغيير محتوياتها .
٥- ظهور مشاكل في التطبيقات المنصبة وتغير نوافذ التطبيقات والقوائم والبيانات .
٦- تكرار ظهور رسائل الخطأ في اكثر من تطبيق .
٧- افشاء معلومات واسرار شخصية هامة .

خامساً : صفات فايروسات الحاسوب

١- القدرة على التناسخ والانتشار.
٢- ربط نفسها ببرنامج آخر يسمى الحاضن او المضيف (Host) .
٣- ممكن ان تنتقل من حاسوب مصاب الى آخر سليم .

سادساً : اهم الخطوات اللازمة للحماية من عمليات الاختراق الالكتروني

١- استخدام نظم تشغيل محمية من الفايروسات كنظم يونكس ولينكس ومشتقاتها .
٢- تثبيت البرامج المضادة او المكافحة للفايروسات مثل (Norton) وتحديث النسخة .
٣- الاحتفاظ بنسخ للبرامجيات المهمة مثل نظام التشغيل ويندوز وحزمة اوفيس ونسخة من ملفات المستخدم .
٤- عدم فتح اي رسالة او ملف ملحق ببريد الكتروني وارد من شخص غير معروف للمستخدم او ملفات ذات امتدادات غير معروفة .
٥- تثبيت كلمة سر (Password) على الحاسوب والشبكة اللاسلكية الخاصة بالمستخدم مع تغييرها كل فترة ، وعدم السماح الا للمستخدمين الموثوقين بالاتصال واستخدام الحاسوب .