هـ- مصادر المعلومات : وتشمل جميع المصادر التي يمكن أن تولد هذه المعلومات ومنها القوى الكهربائية والماء ، الحاسبات ، الأبنية والفضاءات والتسهيلات الأخرى، شبكات الاتصالات ، الأفراد العاملون ، الأجهزة والمعدات ، السلع والخدمات ، المخازن ، رؤوس الأموال ، السيارات ووسائط النقل .

ـ طرق اختراق أمن المعلومات

على الرغم من اختلاف الباحثين المختصين في مجال أمنية المعلومات بخصوص الطرق التي يمكن من خلالها اختراق أمن المعلومات (عمار ، ١٩٩٠) (منيب ، ١٩٩٠) (قشقوش، ١٩٩٢) (الشوا ، ١٩٩٤) (Ewing 1992) (Hill, 1995) (Tanzer , 1993) (Parker, 1997) لا أنه وكما أسلفنا فإن هناك أربع طرق مهمة يحصل بوساطتها الاختراق لأمن المعلومات وفيما يأتي توضيح لهذه الطرق :

١ ـ التجسس التنافسي (الصناعي) : ويتمثل في الاطلاع غير المخول به على المعلومات ، فالتهديد الخطير الذي يواجه أمن المعلومات هو الدخول (الوصول) غير المرخص إليها من قبل شخص ما ويعرف مثل هؤلاء الأشخاص عادة بمصطلح «المأجورين » (Hackers) وقد أحست منظمات كثيرة بوجودهم ، ويعزى السبب في ظهور مثل هذه الشريحة إلى زيادة حدة المنافسة بين المنظمات ، قصر دورة حياة المنتجات ، انخفاض هامش الربح ، انخفاض ولاء العاملين ، ويأخذ هذا التجسس أشكالا عدة أهمها (Abernathy,1991:77)

أ- التقاط المعلومات التي تظهر على الشاشة المرتبطة بالحاسب من خلال الاطلاع عليها وهو ما يصطلح عليه بالالتقاط الذهني .

ب- التقاط المعلومات من خلال التصنت المجرد عليها بين الحاسب والمحطات الطرفية بوساطة خطوط تحويلية أو مرسلات صغيرة أو استخدام الهوائيات في حالة البث عبر الأقمار الصناعية .

جـ- التقاط المعلومات مباشرة من الخطوط الهاتفية عن طريق وضع مركز تصنت أو مكبرات صوت صغيرة .

د- التقاط المعلومات من خلال الإشعاعات الصادرة من الحاسب والأجهزة الملحقة به وفك رموز هذه الإشعاعات لتحوليها إلى اللغة الأصلية .

هـ- التفتيش الدقيق في نفايات الشركات بحثا عن المعلومات .

و- الدخول إلى النظم الحاسبية للمنظمة باعتماد ذرائع مختلفة مثل الادعاء بأنه باحث أكاديمي أو محلل شركات أو أخصائي معلومات أو مشتر يرغب بكسب ثقة الأفراد العاملين .

٢- سوء استخدام المعلومات . ويشير إلى الحالة التي تسخر وتوظف فيها المعلومات لتحقيق أهداف غير مشروعة أو في مجالات غير مسموح بها لتحقيق مصالحه الشخصية أو مصالح جهات أخرى حتى في الحالات التي يحق للمستفيد في الوصول إلى هذه المعلومات ، ويحصل هذا الاختراق بسبب استغلال أحد الأفراد من قبل الشركات المنافسة من أجل المال أو الرغبة في التجسس أو بسبب طرد الفرد العامل ومن ثم قيامه بعرض معلوماته وكشف أسرار المنظمة وإستراتيجيتها ، وتأخذ هذه الطريقة صيغا عدة هي :

أ- سرقة المعلومات المخزونة في ذاكرة الحاسب أو في الأقراص والأشرطة من خلال استنساخها .

ب-زرع برنامج فرعي معروف لدى الفرد في البرنامج يتم إخفاؤه بسرية تامة ومهارة لتحقيق أغراض غير مشروعة .

جـ- التعديل في برامج الحاسب أثناء تصميم البرنامج أو تنفيذه أو تحديثه وصيانته .

د- استخدام الحاسب والمعلومات المخزونة فيه لارتكاب الخروقات وتنفيذها ومتابعة التنفيذ من خلال تصميم برنامج يخصص لهذا الغرض .

هـ- إجراء تحويلات وهمية للنقود من خلال مستحقات مصطنعة .

و- دفع مستحقات لشركات وهمية وتغذية الحاسب بقوائم دفع وهمية .

ز- استبدال رقم حساب بآخر أو إحلال بطاقة بأخرى أو مضاعفة الرواتب .

حـ- طبع قوائم حسابات غير حقيقية واستغلال ثقة الزبائن بالحاسب .

٣ـ الإهمال : وهو يمثل الطريقة الأكثر شيوعا لاختراق المعلومات ويعزى السبب في ذلك إلى إهمال الأفراد العاملين وتهاونهم أو ضعف إدراكهم لأهمية الاحتفاظ بسرية المعلومات والعواقب الوخيمة المترتبة لاختراق أمن المعلومات . إلى جانب عدم معرفتهم المعلومات التي تحتاج إلى الحماية ومن يمتلك الدافع إلى سرقة هذه المعلومات من داخل المنظمة وخارجها وكيف يمكن كشفه وإيقافه في الوقت المناسب(Marine,1990 : 24) (Wood&Banks,1993:51) .

٤ ـ تدمير المعلومات من خلال استخدام الفيروسات التي شغلت المتخصصين في السنوات الأخيرة بسبب اتساع مخاطرها وسهولة انتشارها والأضرار الكبيرة المترتبة عليها والتي تشتمل على مهاجمة البيانات والمعلومات والبرامج وإتلافها وحذفها وتعديلها جذريا من خلال تشويهها وتحريفها وإدخال معلومات غير صحيحة ، حذف الملفات و إعادة تسميتها وتغيير تواريخ الملفات المخزونة ، فضلا عن إيقاف الحاسب عن العمل او إبطاء تشغيله وتقليص السعة التخزينية . وتجدر الإشارة هنا الى صعوبة حصر وتعداد جميع أنواع الفيروسات المستخدمة حاليا في اختراق أمن المعلومات وذلك لتعددها وتنوعها وتزايد انتشارها باطراد فضلا عن تطور صيغها وأشكالها باستمرار .

ـ مجالات اختراق أمن المعلومات

تعد مجالات اختراق أمن المعلومات من أكثر الموضوعات مثارا للجدل والاهتمام من قبل المختصين في نظم المعلومات الإدارية بسبب كونها الأساس في توفير الفرص الملائمة لحدوث الاختراق، من هنا تقتضي الضرورة البحث في بعض الجوانب التفصيلية لهذه المجالات وعلى النحو الآتي : (Parker,1993:10-14)

١ ـ الملفات الورقية . على الرغم من استخدام النظم الحاسوبية إلا أن الملفات الورقية لازالت تستحوذ على النسبة الأكبر من الملفات المستخدمة في أغلب المنظمات، وأهم الفرص المتاحة في هذا المجال هي :

أ- عدم تصنيف الملفات على النحو الذي يمكن معه معرفة مدى سرية المعلومات التي تنطوي عليها ومن ثم حفظ هذه الملفات بشكل منفصل في مواقع أمينة أو في خزانات مقفلة .

ب- الاستعمال الواسع النطاق لأجهزة النسخ واستنساخ ما هو أكثر من النسخ المقررة سواء أكانت المعلومات حساسة أم لا . أو محاولة بعض الأفراد نسخ صور من الوثائق الحساسة والاحتفاظ بها لأنفسهم ، أو نسيان النسخة الأصلية في الجهاز .

جـ- رمي النسخ الرديئة الطبع التي تحتوي على معلومات حساسة دون إتلافها بشكل ملائم .

د- فشل إدارة المنظمة في التعامل مع البحوث الداخلية التي تنشرها المنظمة أو في جرائد أخبارها الداخلية او المجلات أو غيرها من النشرات التي تنشرها والتي قد تضم معلومات حساسة مثل إعلان الشروع بطرح منتج جديد أو نتائج البحوث التسويقية أو تفاصيل عن الأفراد العاملين في المناصب الحساسة .

هـ- ضعف التعامل مع المعلومات التي انتفت الحاجة لها ، إذ يتم في الأغلب التخلص منها من خلال رميها في سلة النفايات وهو أسلوب غير سليم ، فقد تستغل هذه النفايات من قبل الأفراد الذين يتعاملون بها مثل الفراشين أو غيرهم لدوافع شخصية كما قد يندفع من يريد الحصول على المعلومات إلى البحث وبشكل قانوني وبقرار من المحكمة إلى هذه النفايات باعتبارها نفايات مهملة في مركز تجميع النفايات .

و- اللجوء إلى طريقة بيع الأجهزة المنتهية والقديمة (Printouts)من الحواسيب التي قد تضم معلومات سرية يتوجب عدم الاطلاع عليها .

٢- وباء أجهزة الفاكس : لقد ازداد استخدام هذه الأجهزة منذ منتصف الثمانينيات وبشكل كبير بسبب المزايا العديدة التي تتصف بها والمتمثلة بالسرعة والسهولة العاليتين في نقل البيانات والمعلومات إلى جانب انخفاض التكلفة . ومع هذه المزايا فإن هذه الأجهزة تتيح الفرص لاختراق أمن المعلومات ومن أهمها :