ASK PC "The Largest Arabic Technical Support Community Online"
Sponsored by "Microsoft" and "GITCA"
Author: Eslam Abd El-Fattah Moselhy Soliman
Supervision: Dr. Mohamed N. El-Guindy, PhD, MBCS, CITP

المحتويات

تعريف البحث العلمي:

تعريف بسيط للبحث العلمى : هو عمليه يقوم به الشخص سواء لحل مشكله ما او لتقصى حقيقه ممكنه ويطلق على مايقوم بتلك العمليه "الباحث" والموضوع الذى يبحث عنه الباحث يسمى "موضوع البحث" حيث يتبع طرق علميه تسمى تلك العمليه "منهج البحث" وفى النهايه يصل الباحث الى مايسمى "نتائج البحث".

أهميه البحث العلمي :

يعتبر البحث العلمى من أهم الوسائل التى تؤدى الى إرتقاء الشعوب وتقدمها فى كافه المجالات إضافه الى ذلك فإنه يؤدى الى تصحيح الكثير من الافكار والمعلومات الخاطئه لدى الانسان ودعنا نذكر ان الدول المتقدمه فإنهم يخصصون ميزانيات سنويا للبحث العلمى بما يمثل من أهميه قصوى حيث على العكس تماما فى الوطن العربى فالبحث العلمى مهدر حقه وغير مهتم به بالمرة ولايخصص له ميزانيات كما الحال فى الدول المتقدمه وذلك نجد ان هذه الدول سباقه دائما بكل جديد من أكتشافات وتجارب الى أخره حيث يحتاج البحث العلمى الى إدرات جامعيه مؤهله إداريا وقياديا والبحث العلمى بإختصار هو الطريق لمواكبه العصر الحديث .

هذه مقارنه بين البحث العلمى فى الدول العربيه مقارنه بإسرائيل

الشكل رقم (1-1)

الدولة	الإنفاق على البحث العلمي (مليون دولار)	مقارنة مع ما ينفق في إسرائيل
مصر (2007)	927.917	10%
الاردن (2004)	60.403	0.6%
الكويت (2005)	111.357	1.2%
المغرب (2006)	761.726	7.4%
السعودية (2007)	273.072	3.0%
السودان (2005)	179.085	2.0%
تونس (2005)	660.607	7.0%
السلطة الفلسطينية	11.5	0.12%
الدول العربية مجتمعة	4,700.000	53%
إسرائيل (2007)	8,817.635	

تقرير اليونسكو حول العلوم والتكنولوجيا 2008

كانت هذه نبذه بسيطه على أهميه البحث العلمى فى تقدم العلوم وإرتقاء الشعوب.

تمهيد:

فى تلك الفترة والانتشار الهائل لإنترنت أنتشر مفهوم التجارة الالكترونيه والتى من خلاله إتاحت الكثير من المزايا منها

- **توفير الوقت**
- **توفير المجهود**
- **السرعه**

فالنسبه لرجال الاعمال أصبح فى إمكانهم تجنب السفر بنسبه ما وتخليص كل معاملتهم والترويج لمنتجاتهم فى وقت قصير جداً وايضا بالنسبه للزبائن فليس عليهم التنقل كثيراً والوقوف ساعات كبيره لتقضيه أمراً ما فالتجارة الالكترونيه وفرت ذلك بطرق أسرع بكثير وكل مايحتاجه الفرد كمبيوتر – أنترنت – وان يكون على درايه بطريقه أستخدام الكمبيوتر ومبادئ الانترنت .

والكثير يرى ان التجارة الالكترونيه تهدف فقط للقيام بعمليات البيع والشراء على الانترنت ولكن تحوى شيأ اخر وهو معالجه حركات البيع والشراء وإرسال المعاملات الماليه عبر شبكه الانترنت وتشمل فى طيها الكثير سواء شراء المعلومات مثال على ذلك شراء الكتب العلميه وهناك الكثير من المواقع المشهورة فى ذلك.

ما هو مفهوم التجارة الإلكترونيه :

هى عمليه تتم عن طريق الانترنت تتيح هذه العمليه القيام بعمليات الشراء والبيع عن طرق الانترنت كبيع السلع والخدمات حيث ان التجارة الالكترونيه تتيح عبر الانترنت عمليات دعم العملاء سواء من توفير خدمات خاصه بهم وتوفير أرقام مخصصه لهم عند مواجهتم مشكله ما حيث أن التجارة الالكترونيه تماثل السوق الالكترونى الذى يشمل (موردون-مؤسسات-أفراد-هيئات) الوسطاء (الوكلاء-المشترين) ويتم تقديم تلك الخدمات والمنتجات وعرضها على الجمهور ويتم الحصول على المقابل فى صورة رقميه من خلال طرق الدفع المختلفه.

شكل يوضح مفهم التجارة الالكترونيه (2-1)

أشكال التجارة الالكترونيه :

هناك شكلين حاليين حتى الان

1 - تجارة إلكترونيه من الشركات الى الزبائن (Business-to-Customer) ويمكن إختصارها الى B2c حيث تماثل التبادل التجارى بين الشركات من جانب والزبائن من جانب اخر ويمكن ان نوضح ذلك فى الشكل التالى .

2- تجارة ألكترونيه من الشركات الى الشركات (Business-to-Business) ويمكن أختصارها الى B2B حيث تماثل التبادل التجارى "الالكترونى" بين الشركات بعضهم البعض ويمكن ان نوضح ذلك فى الشكل التالى

الفوائد التى تجنيها الشركات من التجارة الالكترونيه :

تقدم التجارة الالكترونيه العديد من المميزات التى تحصل عليها الشركات تجاه ممارستها للتجارة الالكترونيه .

الحصول على الارباح فى وقت صغير وبمعدلات كثيرة

- التسوق يكون أكثر فعاليه وبالتالى فأن أعتماد الشركات على الانترنت فى عمليات التسويق يتيح لها عرض منتجاتها وخدماتها المختلفه فى كثير من بلدان العالم دون إنقطاع مما يؤدى ذلك الى حصول الشركات على فرصه كبير جداً لحصد الكثير من الارباح فى فترات كثيراً علاوة على ذلك وصولها الى عدد كبير من الزبائن فى أسرع وقت دون تعب او عناء .
- تخفيض مصارف الشركات: حيث تعد عمليات بناء مواقع تجارة ألكترونيه على الويب أكثر إقتصاديه من بناء أسواق التجزئه او صيانه المكاتب وبالتالى لاتحتاج الشركات الى تكاليف باهظه من أجل الامور الترويجيه او تركيب تجهيزات باهظه الثمن تخدم خدمه الزبائن وبالتالى لن يكون هناك الحاجه الى الكثير من الموظفيين للقيام بعمليات الجرد والاعمال الاداريه ولكن يحفظ كل ذلك فى قواعد البيانات على الإنترنت ويسجل فيها كل الحركات سواء حركات البيع وتاريخ العمليات وأسماء الزبائن ويمكن بسهوله أسترجاع بيانات عميل بدون أى مشكله
- خلق نوع من التواصل الفعال: بين الشركات والعملاء حيث ان التجارة الالكترونيه تطوى المسافات مما يوفر طريقه فعاله لتبادل المعلومات مع الشركاء.

الفوائد التى يجنيها الزبائن من التجارة الالكترونيه

أهم مايميز التجارة الالكترونيه توفيرها للوقت

- توفر التجارة الالكترونيه الكثير من الوقت حيث تفتح الاسواق الالكترونيه (E-market) بشكل يومى دائما دون وجود اى يوم عطله ولايحتاج العميل الى السفر او الانتظار لشراء منتج معين ولكن كل مافى الامران يختار العميل مايريد بعد إدخال المعلومات التى يطلبها الموقع منه وتكون هذه المعلومات هى إدخال بيانات البطاقه الائتمانيه الذى يحملها العميل
- حريه الاختيار: توفر التجارة الالكترونيه فرصه رائعه لزياره مختلف انواع المحلات التى تحوى معاملات ماليه على الانترنت وبالتالى توفر كل المعلومات الكامله عن المنتج .
- خفض الاسعار :يوجد العديد من الشركات على الانترنت التى تبيع السلع باسعار منخفضه مقارنه بالمتاجر التقليديه يرجع ذلك الى
  - سوق الانترنت: يوفر الكثير من التكاليف المنفقه فى عمليات التسويق مما يعود ذلك بالنفع الى مصلحه العميل
- نيل ثقه المستخدم: حيث يوفر الانترنت أتصالات مباشره بطريقه تفاعليه مما يدفع الشركات الموجوده فى السوق الالكترونى (E-market) الاستفاده من هذه المميزات للإجابه على الزبائن فى أسرع وقت مما يؤدى ذلك الى نيل ثقه المستخدم.

إحصائيات :

لقد بلغ حجم التجارة الإلكترونية في العالم حوالي 3.8 تريليون دولار في عام 2003، وذلك وفقا لتقديرات الأمم المتحدة، وقد تضاعف الرقم ليصل إلى 6.8 تريليون دولار في نهاية عام 2004، وإن نحو 80% من حجم التجارة في العالم يتم في الولايات المتحدة الأمريكية، 155 في أوروبا الغربية، 5% في بقية دول العالم، معظمها أو نحو 4% منها يتم في اليابان. كما ويشكل حجم التجارة الإلكترونية بين مؤسسات الأعمال (Business to Business) حوالي 80% من حجم التجارة الإلكترونية في العالم. وتراوحت قيمة التجارة بين مؤسسات الأعمال في الاتحاد الأوروبي بين 185 مليار دولار و200 مليار دولار في عام 2002، كما أن التجارة الإلكترونية بين مؤسسات الأعمال قد وصلت في أوروبا الوسطى والشرقية إلى حوالي 4 مليارات دولار في عام 2003.وقد نمت هذه التجارة بشكل متسارع في منطقة آسيا والمحيط الهادئ من حوالي 120 مليار دولار في عام 2002إلى حوالي 300 مليار دولار بنهاية عام 2003. وفي أمريكا اللاتينية بلغت قيمة الصفقات التجارية بين مؤسسات الأعمال على الشبكة مباشرة 6.5 مليارات في عام 2002 وارتفعت لتصل إلى 12.5 مليار دولار في عام 2003. إن نسبة مستخدمي الإنترنت الذين يشترون بواسطة الشبكة مباشرة كانت أعلى في الولايات المتحدة الأمريكية والمملكة المتحدة وشمال أوروبا الغربية خلال الفترة 2000-2001، إذ بلغت نسبت مستخدمي الشبكة بعمليات شراء على الشبكة مباشرة حوالي 38%، أما في المكسيك فقد بلغت النسبة أقل من 0.6%.

ووفقا لتقرير ماركيتر السنوى فى عام 2006 حجم سوق التجارة الإلكترونية فى أوروبا ليصل إلى 106'مليار (133 مليار دولار .(ويقول محللون انه من المحتمل جدا أن يذهب على زيادة معدل وعرض سريع للغاية للنمو السنوى 'ما يصل الى 25 ٪ .وسوف يكون الوضع مستقرا لخمس سنوات على الأقل والسوق سوف يصل الى نقطة '323مليار (407 مليار دولار بحلول عام 2011)

بريطانيا وفرنسا والمانيا تسود فى سوق التجارة الإلكترونية الأوروبية .هذه البلدان تملك أكبر حصة فى المعاملات الأرقام الإجمالية 'ما يصل الى 72 ٪ .التجارة الإلكترونية البريطانية تحتل المرتبة الأولى فى السوق والمحللين يعتقدون ان الامر سيصل الى 84 مليار دولار فى عام 2007 ، وهو 39 ٪ أعلى من أرقام عام 2006 .وتتولى المانيا في المركز الثاني .ومع ذلك ، فمن الأولى في عدد من هناك على شبكة الإنترنت ، للعملاء ما يصل الى 3 ملايين.

عيوب التجارة الالكترونيه

- عدم احساس المشترين بالامان التام فى حالة استخدام وسائل الدفع الالكترونية المتعددة
- كذلك فان البعض يعتبر عملية الشراء من المتاجر التقليدية هى عملية ممتعة فى حد ذاتها تتطلب دعوة الاصدقاء والاهل احيانا
- كما ان هناك نوعية من السلع مثل الملابس والاثاث يحب ان يراها المشترى بعينه بل يلمسها ويجربها حتى يقتنع بها .

التجارة الالكترونيه فى العالم الثالث

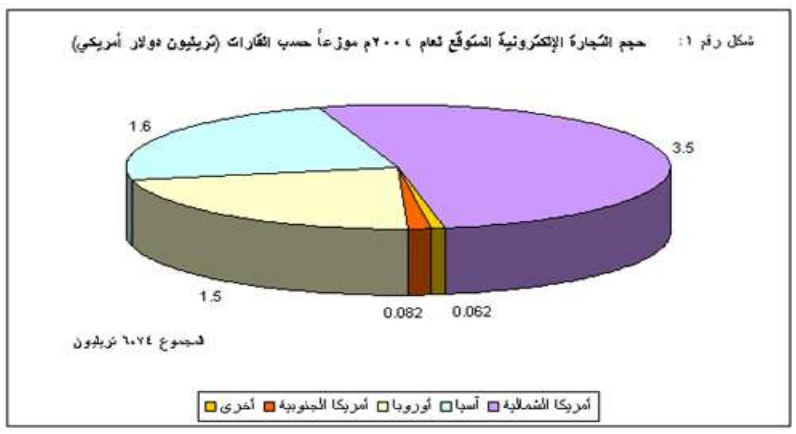
يعود ضعف التعامل بالتجارة الإلكترونية في الدول النامية إلى عدة أسباب أهمها

- انخفاض مستوى دخل الفرد
- عدم وجود وعي لما يمكن أن توفره تكنولوجيا المعلومات والتجارة الإلكترونية، والافتقار إلى ثقافة مؤسسات أعمال منفتحة على التغيير والشفافية
- عدم كفاية البنية التحتية للاتصالات اللاسلكية والوصول بشبكة الإنترنت أو ارتفاع كلفة الوصول إلى شبكة الإنترنت
- الافتقار إلى الأسس القانونية والتنظيمية المناسبة
- الافتقار إلى نظم دفع يمكن في دورها أن تدعم الصفقات التجارية التي تجرى على شبكة الإنترنت
- قلق الافراد من التجارة الالكترونيه بسبب ماينشره الإعلام دائما عن أختراق مواقع إلكترونيه

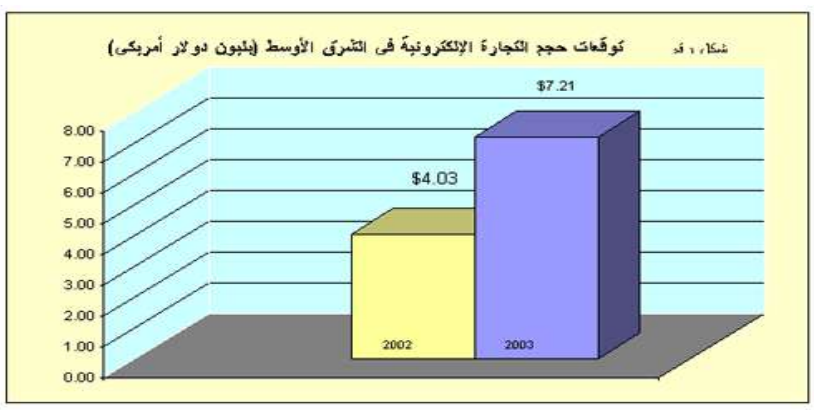
مستقبل التجارة الالكترونيه

هناك أراء متباينه بسبب مستقبل التجارة الالكترونيه على الرغم من ان المبيعات على الانترنت تتزايد بشكل مستمر الا ان بعض المحللون يروا ان التجارة الالكترونيه فى طريقها الى الانخفاض ويرجع ذلك الى ان هناك منتجات يمكن أن يرتفع سعرها بالرغم من مجانيتها وبالتالى فاذا لم يحصل عليها المتسوق فأنه سينطلق الى موقع اخر ,وايضأ ضعف العروض التى تقدمها المواقع العربيه مقارنه بالدول الاخرى, الشراء من خلال الانترنت يكون فى الغالب بالفيزا المخصصه للإنترنت وهى غير منتشرة فى العالم العربى بشكل كبير تاخر الكثير من الشركات فى الدخول لهذا النوع من الصناعه , وعدد كبير من يعملوا فى هذا النوع من الصناعه معظمهم يقتصر دورهم على تقديم السلع الخدميه(أستضافه وتصميم المواقع) والسبب ان هذه الفئه الوحيده القادره على الشراء من الانترنت وايضأ يرى بعض المحللين ان التجارة الالكترونيه قادمه وبقوة لتذليل العقبات التى يواجهها الزبائن حيث تسمح التجارة الالكترونيه للشركات الصغيرة حديثه العهد منافسه الشركات الكبيرة ويكون ذلك فى سريه كامله على المعاملات الماليه على الانترنت من خلال أستخدام تقنيات ssl (secure socket layer) وأدى ظهور هذه التقنيه الى إزاله الكثير من المخاوف لدى المتعاملين فى مجالات التجارة الالكترونيه وبالتالى فإن مستقبل التجارة الالكترونيه ومن المتوقع ان يكون مستقبل التجارة الالكترونيه متزايد بسبب زياده مستخدمى الانترنت

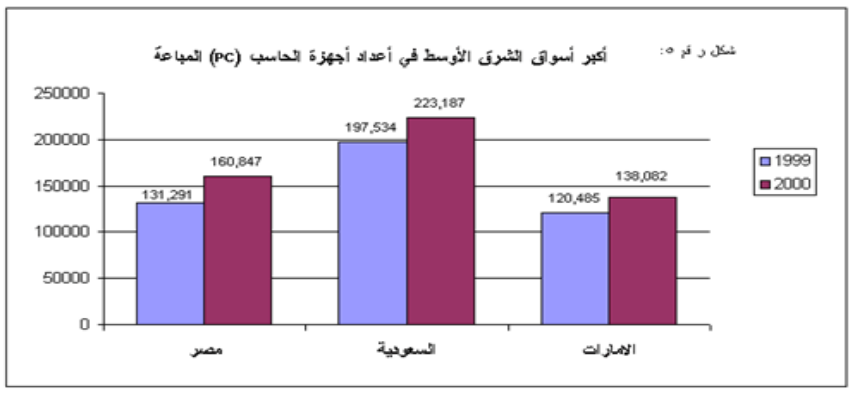
شكل يوضح مستقبل التجارة الإلكترونيه(1-3)



شكل يوضح حجم التجارة الالكترونيه فى الشرق الاوسط شكل(4-1)



شكل يوضح أكبر اسواق الشرق الاوسط فى أعداد أجهزة الحاسب المباعه(5-1)



الصعوبات القانونيه التى تواجه التجارة الالكترونيه :

الموقف القانوني من الرّسائل الإلكترونيةِ : ان عدم الاعتراف بقانونية هذا النمط من الرسائل يضعفِ إمكانيةِ الاعتراف بهذه التجارة الالكترونية ،وبالتالى يؤدى ذلك الى إعاقه تَطوّر التّجارةِ الإلكترونيةِ.

التعاقد بالطرق الالكترونية : تواجه التجارة الالكترونية صعوبات من حيث اعتراف القوانين التقليدية بقانونية ابرام العقود بهذه الوسائل

الاختصاص والولاية القضائية : ان التجارة الإلكترونيةِ باعتبارها تجارة بلا حدود تثير مشكلة الاختصاص القضائي بسبب حقيقة ان القوانين الداخلية ذات نطاق اقليمي محدد بحدود الدولة المعنية . .

حماية المستهلكِ وفى هذا الامر يجب ضمان حمايه المستهلك من اى عمليات نصب او تحايل بحيث يضمن ان تتم هذه العمليات بدون اى مشاكل للمستهلك أو الجمهور ، خاصة ان بعضها قد يتعارض مع قواعد التجارةِ إلكترونيةِ من جهة وبعضها غير كاف للحماية من مخاطر التجارة الالكترونية من جهة اخرى.

الملكية الفكرية : تحديات حمايةِ الملكيةِ االفكرية للمصنفات الرقمية ومحتوى المواقع في بيئة التجارةِ إلكترونيةِ.

انظمة الدفع الالكتروني : تثير التجارة الالكترونية تحديات من حيث تقديم الخدمه والحصول مقابل الخدمة ، وتتصل هذه التحديات بمفهوم النقود الالكترونية **"بطاقات الائتمان"** ، الحوالات الالكترونية ، وآليات الدفع النقدي الالكتروني .

المسؤولية القانونية للجهات الوسيطة في انشطة التجارة الالكترونية : مثل مسؤولية مزودي خدمةِ شبكة الانترنتِ ، ومسؤولية الجهات القائمة بخدمة التسليم المادي ، ومسؤولية جهات الاعلان ، ومسؤولية جهات التوثيق واصدار الشهادات..

البنية التحتية : وتتعلق بالاستراتيجيات الوطنية وبالتنظيم القانوني لخدمات الاتصال وتزويد خدمة الانترنت وجهات الاشراف على التجارة الالكترونية.

الضرائب والجمارك والتعريفة : آليات وقواعد السياسة التشريعية الضريبية والجمركية في بيئة التجارة الالكترونية **"هل سيتم دفع ضرائب نظير هذه التجارة"**

مسائل الخصوصية وامن المعلومات: أدى أختراق كثير من المواقع الى وجود حاله من القلق لدى المتعاملين بهذا النوع من التجارة ويجب توفير الحمايه أللازمه لهم **"تشفير البيانات"**

التنظيم القانوني والإداري:من خلال جهات منح شهادات موثوقه وما يتصل به من تنظيم مسؤولياتها الالكترونية ..

التجارة الالكترونيه وتغيرها لنمط حياتك:

كيف تبدأ

الكثيرون مقتنعون بالفكرة، ولكنهم لا يعرفون كيف أو من أين البداية، وهو شئ سهل، ولكن فكرنا هو الذى يجعلنا لا نعرف كيف نبدأ. فعندما تمرن فكرك على قبول الفكرة، فإنك ستعرف من أين أو كيف ستبدأ، لأن حماستك فقط لا تكفي، لأن قلبك سيكون به شكك وتسأل نفسك ألف سؤال وماذا إذا لم أنجح كالسابقين؟

درّب نفسك على ان تكون دوما اسئلتك على شاكلة (ماهى المواقع التى يجب ان ازورها ؟) ماهي متطلبات المرحلة المقبلة ؟ من هم الذين يجب ان اتواصل معهم ؟ ماهى معلوماتى عن هذا المجال الذى انوى الدخول فيه ؟ كيف استطيع تثقيف نفسى للحاق بهذا المجال ؟ فى دولتى من هم الاشخاص الذين يجب ان اتعرف عليهم ؟ ان التجارة الالكترونية فى مخيلة الكثيرين هو جهاز كمبيوتر متصل بالانترنت فى غرفتك وبريد الكترونى وجوال وهاتف المنزل مهلا هذه ليست تجارة اطلاقا

اذا كنت من هولاء لا تضيع وقتك واعرف لماذا لم تنجح وساعطيك مثال بسيط جداً فاذا كنت تملك سيرفر وتملك الخبرة وتدير عملك من المنزل يوماً ما سيتصل بك عميل يسألك عن موقع شركتك سوف تجد نفسك فى ورطة حقيقية وبالتالى فقد العميل وربما كنت ستجنى ربح وفير من هذا العميل.

اذاً لو اردت ان تمارس التجارة الالكترونية اولا عليك ان تسجيل شركة او اسم عمل لدى المسجل التجارى وتستاجر مكتب على قدر مادّيتك وموقع على الانترنت وان تكتفى فى المرة الاولى بموظف واحد اذا كان باستطاعتك ذلك ليكون عملك رسمياً بالاضافة الى ورق مروس باسم شركتك وختم الى كل احتياجاتك المكتبية.

حدد مجالك

يظن الاغلبية والذين يريدون ممارسة التجارة الالكترونية بان التجارة الالكترونية هى تقديم خدمات استضافة وتصميم او تقديم خدمات بيع بعض المقتنيات على الانترنت.

لا اريد ان احبطك ولكن انظر للكميات الهائلة من مقدمى تلك الخدمات شركات عالمية ومحلية وافراد ايضاً لكن هذا الا يجعلك تصرف النظر عنها ايضاً وحتى لا اناقض نفسى ساخبرك لماذا ستنجح رغم كثرتهم؟

ابدا كبيراً بخبرتك وطموحك وخطط جيداً وقدم خدماتك بافضل من المتواجدين معك فى السوق فان الخبرة سوف تساعدك فى حل مشاكلك بنفسك وبالتالى ينعكس على جودة الخدمة المقدمة وليس تطلب فى كل مرة من صديقك معالجة مشاكلك التقنية وقد يكون مشغولاً فيتاخر حل المشكلة وينعكس على سمعة عملك.

والتخطيط السليم هو اول سلالم النجاح فان خططت جيدا اعلم ان النجاح سيكون حليفك ولا تستعجل النجاح فبمرور كل يوم سوف تجد نفسك تنجح فيما كنت تراه مستحيلاً بالامس وستجد راحة نفسية واجعل افكارك خلاقة ولا تركن للنجاح البسيط فتنصرف الى الاحتفال بنجاحك الموقت لان النجاح الحقيقى هو الاستمرار فيه وليس التوقف عند حد معين.

معلومة مهمة جداً لكل من حدد هدفه ويريد ان يبدأ عملية التنفيذ لا تجعل نفسك صغيراً ابداً فى اعين منافسيك حتى ولو كانوا يتفوقون عليك فى المبنى والموظفين وراس المال فى البنك فأنت كبير بالمعلومة التى لديك وانت كبير بفكرك لان التفكير والتنفيذ الجيد هو الذى يجلب المال ويجعل الاخرين يرونك كبيراً فى نظرهم لامتلاكك الاموال اذا كثرة الاموال ناتجة من حسن التفكير وانت تملك عقلاً مثله ولو وظفته فى المكان والزمان المناسبان ستملك مالاً وفيراً مثل من تراهم اصحاب ملايين اليوم لذلك انت لست اصغر منهم.

انطلق الان

الان بعد ان اسست شركتك وحددت مجال عملك انطلق فى العمل وعليك ان توقف كل نشاطاتك الجانبية او اى وظيفة اخرى ولتنجح فى الامر حتى لا تشغل بالك باى تاثيرات اخرى عليك ان توفر مصاريف شهرين كادنى حد لمصاريفك اليومية حتى تتفرغ لعملك وتستطيع التفكير بذهن صافى لا يشغلك منها مشاكل بسيطة على شاكلة قرب نهاية الشهر لدفع ايجار المكتب او قرب تسديد فاتورة الكهرباء وهناك اشياء يجب ان تاخذها معك لتعينك فى تحقيق هدفك.

التثقيف :

مهم جداً ان تكون ملماً بكل صغيرة وكبيرة فى مجالك الذى حددته وهذا الامر لا يتطلب منك ان تكون خريجاً فى نفس المجال فكم من خريج لا يعرف كيف يطبق اساسيات درسها فى الجامعة لان الجهل بتلك الاسس يجعل العملاء يتخوفون من التعامل معك لذلك اقراء كثيراً فى مجالك وادخل دورات تدريبية بين الحين والاخر لتكون رائداً فى مجالك ولا توقف نفسك من التفكير ومحاولة ان تخلق افكار اخرى افضل من التى درستها او سمعتها من شخص ما .

بناء علاقات عامة

العلاقات العامة مهمة فى مجال عملك مهما كان فلا تحصر نشاطك فى الانترنت فقط ففى كل مكان هناك عميل محتمل سيعجب بخدماتك اذا سمع عنها ولكن احرص ان تكون فى المكان المناسب دوما لتتحدث عن نشاطك، فلا يعقل ان تتحدث عن خدماتك وانت فى بيت عزاء مثلاً، لان المكان المناسب والاشخاص المناسبين.

دوما لهم دور فى توسيع عملك فانت مثلا تعرف اناس يعملون منذ فترة طويلة ولكن حياتهم ودخلهم المادي لم يتغير واخرين تجدهم فجاة اصبحوا اصحاب ملايين حتى تتشكك انت نفسك وتسأل من اين لهم هذا؟ سأخبرك لماذا هناك اشخاص يكونوا دوما فى المكان الغير مناسب لذلك يعملون بكل اجتهاد ولا يحصدون شيء، وهناك اخرين يكونون فى المكان المناسب لذلك يكون النجاح والدخل الجيد لاعمالهم .ولأقرّب لك الفكرة، اسال نفسك، كم ستكسب اذا قمت ببناء حوض سباحة بجوار ساحل البحر الابيض؟ لن تكسب شئياً! هذه الاجابة التلقائية لكل من ينظر مثل الاخرين، لكنى لو وجه السؤال إلي، فإني سأكسب الكثير، لأنى ساقدم أشياء يعجز البحر بتقديمه للسياح، مثلا، يمكن ان يكون منتجع كامل بطبيعة الساحل ودون تكلف، بالاضافة الى توفير اسمال ملونة فيها لان الكثيرين لن يشاهدوها الا اذا غطسوا فى اعماق بعيدة وفيها خطورة على الكثيرين والاغلبية لا تستطيع الذهاب الى هناك.

متطلبات إنشاء موقع إلكترونى

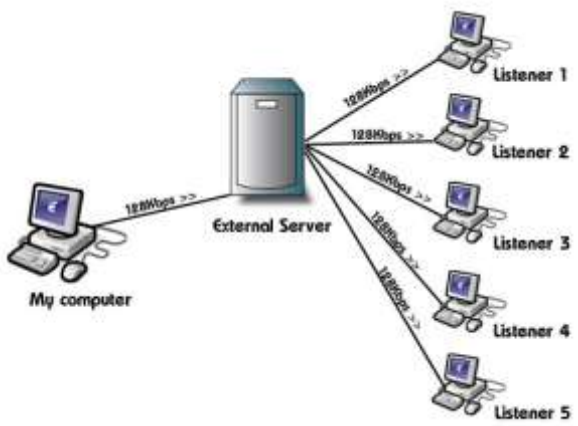
يتطلب وجود عاملين مهمين من أجل إنشاء موقع إلكترونى

مكونات ماديه(Hardware)

مكونات برمجيه(software)

المكونات الماديه: وهى أجهزة الكمبيوتر التى من خلالها يعمل الموقع الالكترونى ويطلق على تلك الاجهزة اسم الخادم server يتميز ذلك الجهاز بإمكانيات كبيرة جداً على خلاف الكمبيوتر الشخصى

شكل يوضح جهاز السيرفر مرتبط بعدد من الاجهزة (1-6)



المكونات البرمجيه :

وهى البرمجيات التى تحتاجها أجهزة الكمبيوتر سواء client, server حيث فى ذلك الامر يمكن تقسيم برمجيات السيرفر الى نوعين :

- Server operating systems
- Server applications

server operating systems حيث

يشمل:

Mac OS X Server, Windows Small Business, Server 2008 Linux, Solaris, FreeBSD, Windows NT, NetWare 6.5, HP-UX 11i v1.6 & HP-UX 11i v2, AIX 5L 5.2,

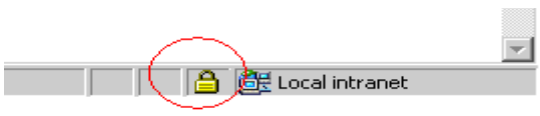
وايضاً يشمل server applications

Web server وهى التى تستضيف صفحات الويب

Database server: وهى التى تخزن بها كل محتويات الموقع من بيانات ومعلومات عن العملاء على سبيل المثال Oracle, Sql server2000, mysql

Certificates: توفر عمليات الامان للمواقع الالكترونيه من خلال عمليات authentication والتشفير Encryption

شكل يوضح زيارة موقع أمن نظراً لوجود رقم القفل فى الاسفل(1-7)



Secure icon in Microsoft Internet

شكل يوضح زيارة موقع أمن (1-8)

Secure icon in Mozilla Firefox

مراحل إنشاء موقع ألكتروني

إختيار الفريق :

ويشمل الاتى مدير المشروع,والدعم التقنى بعد ذلك إختيار التصميمات والبحث عن مدقق لغوى للبحث عن اذا كانت هناك كلمات تحتاج الى إعاده صياغ مرة أخرى وأستخدام كلمات أكثر شمولا.

وضع خطه عمل :

إستخدام مخطط هيكلى ووضع خطه طريق لنفسك وللمستخدمين الاخرين وعمل قائمه عن ماذا أريد والغرض من كل صفحه وماهو المحتوى الذى يكون بها.

الفئه المستهدفه :

وبالتالى عمل دراسه مسبقه لمعرفه ماهو الجمهور المستهدف وطرق مخاطبته ومعرفه ماهى أفضل طريقه مناسبه لمخاطبته

أنواع السلع المقدمه :

وذلك لمعرفه الطريقه الذى تصل بها السلعه الى العميل سواء اذا كانت هذه السلعه ماديه او غير ماديه

طرق الدفع :

تعتبر من الاشياء المهمه فى التجارة الالكترونيه حيث يمكن إيجاز تلك الطرق فى عدد من أشهر الطرق المتعارف والمتبادله بين كثير من المواقع نذكر منها **Vista,Mastercard,American Express**

إختيار النطاق:

وتعد هذه المرحله مهمه جداً لانها تمثل واجهه الموقع بحيث هناك الكثير من المواقع أسماء نطاقتها كبيرة الى حد ما وفى هذه المرحله يجب أختيار مسميات تكون أكثر سهوله.

إنشاء موقع أولى "تجربه أوليه للموقع"

ابدأ مع الصفحات التي تركز على المنتجات والخدمات الخاصة بك أبتداء بالعلامة التجارية مع صفحات غنية حيث لابد ان نضع فى الاعتبار ان الصفحات التى يمكن ان يزورها الزائر فى كثير من الاحيان لن تكون الصفحه الرئيسيه فلابد من وضع معلومات الاتصال لتسهل على الزائر عمليه التواصل

إستخدام سياسه الخصوصيه

أستخدام سياسه الخصوصيه للحفاظ على المعلومات الشخصيه للزوار الموقع وكذلك إعضائه

أختبار الموقع

أختبار الموقع بعد ذلك وقياس مدى توافقه مع كل المتصفحات وقياس كفاءة الخادم وأستخدام المدقق أتش تى أم أل **Html** لمعرفه اذا كان هناك أخطاء فى الصفحات ام لا بعد ذلك دعوة الاصدقاء والاخرين لزيارة الموقع ومعرفه ردود أفعالهم والتواصل معهم

إستمراريه الموقع

يكون من خلال الاتى

الحفاظ على الموقع : وذلك من خلال إضافه محتويات جديده ,بجانب أضافه وصلات جديده والاستجابه لرغبه زوار الموقع ومعرفه الصفحات التى لاتعمل والعمل على إصلاحها.

الترويج

ويتم ذلك من خلال تبادل الوصلات بين المواقع بينهم البعض

طرق التسوق عبر الانترنت

تتم عن طريق الدخول الى الموقع اولا ثم بعد ذلك كتابه اسم المستخدم ثم بعد ذلك يتم كتابه كلمه المرور وتتبع تلك المواقع طرق من أجل الحفاظ على سريه المعلومات وبيانات المستخدم وينصح القائمين على هذه المواقع ان تكون كلمه المرور تحتوى على أرقام

وحروف ورموز وذلك لزياده تأمين كلمه المرور وصعوبه أكتشافها بعد الدخول الى الموقع وعند الشراء يتم كتابه معلومات حامل بطاقه الائتمان وتشمل

الاسم الذى على البطاقه .....

رقم البطاقه.....

رقم الامان ويتكون من ثلاث أرقام .....

شكل يوضح الفيزا ورقم الامان (1-2)

حيث الرقم المشار اليه وهو 484 هو رقم الامان الخاص بالفيزا

وفى كثير من الاحيان لتفعيل بطاقه الانترنت يتطلب الامر الذهاب الى البنك لتفعيل هذه البطاقه ويقوم البنك بطلب معلومات عن حامل هذه البطاقه لمعرفه هل هو بالفعل صاحب البطاقه ام لا وتكون هذه الاسئله عبارة عن تاريخ الميلاد- العنوان-رقم البطاقه وذلك للتأكد من حامل البطاقه هو الشخص الصحيح .

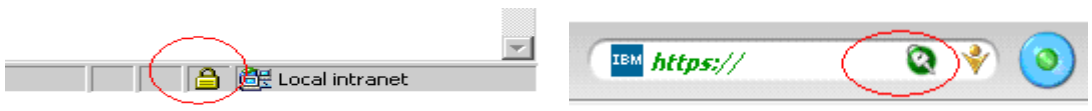
هل التسوق عبر الانترنت أمن

تتم هذه العمليات فى سريه تامه ومحميه فى نفس الوقت حيث يقوم مستعرض الانترنت بمنح الشهادات الامنيه وهي صادرة من سلطة شهادات معترف بها تساعد على تبادل الكلمات السرية بين المستخدم و موقع التسوق و بعد أن يتحقق النظام أن الشهادة الأمنية قد صدرت عن سلطة شهادات يثق بها المستعرض عند قبول الشهادة يستعمل موقع التسوق الآمن تقنية تشفير(ssl) وهي إعادة ترتيب البيانات بطريقة معقدة و ذلك لجعل الإتصال بين النظام و بين موقع التسوق محمى من عيون الآخرين .

مواصفات مواقع التسوق الامن

بعض مواقع التسوق الآمنة لها تدابير أمنية مشددة لمنع الأشخاص غير المرخص لهم من رؤية المعلومات المرسلة من و إلى الموقع من هذه التدابير الأمنية : أنه عادة ما يبدأ عنوان موقع التسوق الآمن ب https بدلا من http و إضافة الحرف s يعني secure آمن و يتم وضع رمز القفل بجانب شريط العنوان أو في أسفل إطار المستعرض يستعمل موقع التسوق الآمن تقنية تسمى Secure Sockets Layer طبقة المقابس الآمنة (SSL) تعمل على التحكم بالعمليات اللازمة لإبقاء البيانات آمنة أثناء انتقالها عبر الإنترنت تقوم بعض مواقع التسوق الآمنة بتشفير البيانات باستخدام تقنية تشفير يقاس مستواها بعدد البتات و تستخدم المواقع الآمنة التشفير ب 128 بت لإجراء عمليات تبادل للبيانات إضافه الى ذلك البحث عن الموقع عن الانترنت ومعرفه سمعته جيداً اذا كانت جيده ام لا ويمكن عمل ذلك بطرق اخرى من خلال سؤال الاصدقاء او من كان على تجربه به سابقا

شكل يوضح زيارة موقع أمن (2-2)



وعند زيارة موقع أمن لابد من ظهور تلك العلامات سؤءا ظهور رمز القفل ويختلف من متصفح الى أخر وايضاً تغير http الى https فى هذه الحاله نعلم أن الموقع أمن .

ماهو الصراف الالى (Automated teller machine)

تعريف الصراف الالى : هو جهاز ألكترونى يتم وضعه فى مكان ما متصل بشبكات أتصالات سلكيه ولاسلكيه ويكون همزة الوصل بين العميل والبنك من أجل عمليات السحب النقدى دون الحاجه للرجوع للبنك مرة أخرى من أجل عمليات السحب النقدى ويطلق عليه "ماكينه النقود"

وبإمكان العميل عقب عمليه السحب معرفه رصيده الحالى والرصيد المتبقى من خلال حصوله بعد عمليه السحب على تقرير صغير يفيد العمليات التى تم تنفيذها

صورة توضح شكل الصراف الالى(3-2)

الانظمه التى يعمل عليها الصراف الالى:

هناك الكثير من المصارف تفضل نظام يونيكس أو نظام لينكس وهناك من يفضل ويندوز

صورة توضح أستخدام نظام ويندوز (4-2)

متى ظهر الصراف الالى:

ظهر الصراف الالى فى نيويورك عام 1939 حيث قام لوثر جورج سيجمان بإختراع تلك الاله وتركيبها فى مصرف ستى بانك ولكن الآلة أزيلت بعد 6 أشهر بسبب عدم تقبل العملاء لفكرتها فيما بعد لم تطرح فكرة الآلة مرة أخرى إلا بعد أكثر من 25 عام قامت De La Rue بطرح أول جهاز صراف آلي إلكتروني، جرى تركيبها في مدينة 'Enfield' وهي مدينة في شمال لندن في 27يونيو 1967 من قبل بنك باركليز ويعد جون شبرد - بارون هو أول من اخترع آلة صراف آلي إلكترونية لصالح بنك باركليز بالرغم من أن هنالك الكثير من براءات الإختراع التي سجلت إلى مخترعين آخرين في الوقت نفسه في 2005 منح جون شبرد-بارون وسام OBE البريطاني كما أضيف إلى قائمة الشرف حيث أنه أضاف إلى العالم الكثير بسبب اختراعه المهم.

- **وأستخدمت أجهزة الصراف الآلي لأول مرة على نطاق واسع في المملكة المتحدة في عام 1973**

كيف يعمل الصراف الالى :

تحتوي آلات الصراف الآلي على وحدتين لإدخال البيانات (فتحة قارئ البطاقات ولوحة المفاتيح) وعلى أربع وحدات لإخراج البيانات (شاشه العرض,جهاز الصرف التلقائى,ووحده طباعه الايصال,والسماعات) ولا تكون آلية الاتصالات التي تربط بين آلة الصراف الآلي مباشرة بشبكة مضيف آلة الصراف الآلي، مرئية للعميل .وهناك شبه كبير بين عمل آلات الصراف الآلي وجهاز الكمبيوتر، حيث تأتي مزودة بنظام تشغيل غالبا نظام التشغيل2 /Os)وبرنامج تطبيق معين خاص باتصالات وواجهة المستخدم .وحيث إن معظم آلات الصراف الآلي تستخدم البطاقات ذات الشرائح الممغنطة وأرقام التعريف الشخصي(pin) لتحديد هوية أصحاب الحسابات، قد تستخدم الأنظمةالأخرى البطاقات الذكية المزودة بميزة التحقق ببصمة الأصبع تقوم آلة الصراف الآلي بتوجيه قراءة المعلومات من بطاقة العميل وطلب العميل إلى المعالج المضيف، والذي بدوره يقوم بتوجيه الطلب إلى المؤسسة المالية الخاصة بالعميل .وإذا كان صاحب الحساب يطلب نقوداً، فيصدر المعالج المضيف إشارات من شأنها تحويل الأموال إلكترونياً(EFT) من الحساب المصرفي للعميل إلى حساب المعالج المضيف .وبمجرد تحويل الأموال، تتلقى آلة الصراف الآلي رمز اعتماد يمنحها صلاحية صرف النقود .هذا ويمكن تنفيذ الاتصال والتحقق والاعتماد بعدة طرق .كما يمكن استخدام الخط المؤجر أو الاتصال الهاتفي أو روابط البيانات اللاسلكية في الاتصال بالنظام المضيف حسب التكلفة وكفاءة البنية الأساسية .ويمكن وضع الأنظمة المضيفة في مؤسسة العميل أو أن تكون جزءاً من شبكة تحويل الأموال إلكترونياً .كما يمكن أن تدعم شبكة تحويل الأموال إلكترونياً معاملات بطاقات الخصم باستخدام أرقام التعريف الشخصي أو معاملات بطاقات الائتمان باستخدام التوقيع .وتتوفر أيضاً

رسوم الخدمة السنوية أو الشهرية مقابل الدعم

تكاليف الاتصالات الخاصة بالاتصال الهاتفي أو الخط المؤجر أو روابط البيانات اللاسلكية

تكون التكاليف الأولية مرتفعة، وبالأخص إذا قامت المؤسسة بإنشاء شبكة خاصة بها .يتراوح سعر شراء آلة الصراف الآلي الواحدة بين2 ألف إلى 35 ألف دولار أمريكي .بينما تتراوح تكلفة البطاقات الممغنطة بين 0.25 إلى 0.50 دولار أمريكي للبطاقة الواحدة، وعادة ما تبلغ تكلفة البطاقات الذكية من 6 إلى 10 دولارات أمريكية للبطاقة الواحدة .ولا توجد ضرورة لاستخدام اتصال إنترنت متزامن مع آلات الصراف الآلي التي تستخدم البطاقات الذكية، طالما كان بإمكان آلة الصراف الآلي الحصول على بعض بيانات العميل المالية من خلال الرقاقة الإلكترونية الدقيقة الموجودة على البطاقة الذكية .علماً بأنه قد يلزم وجود الرقاقة الإلكترونية الدقيقة وخدمة الإنترنت اللاسلكية عندما تكون أنظمة الاتصالات باهظة التكلفة أو لا يمكن الاعتماد عليها.

فوائد وتكاليف الصراف الالى

المنافع:

- يتيح الوصول المرن للعملاء إمكانية الوصول إلى حساباتهم حسبما يتراءى لهم
- عدم الحاجة إلى تواجد موظفي مؤسسات التمويل الأصغر للقيام بالمعاملات مما يفسح لهم مجالاً أكبر لخدمة العملاء
- تلائم ساعات التشغيل المتزايدة جداول مواعيد العملاء
- إمكانية الوصول إلى مزيد من العملاء خارج نطاق شبكة الفرع، كما هو الحال في المراكز السكانية الأصغر حجماً
- توفير مزيد من الأموال بتكلفة منخفضة حيث تعمل آلات الصراف الآلي على تيسير إيداع المدخرات بالنسبة للعملاء.

التكاليف

تختلف التكلفة باختلاف جهة تقديم التكنولوجيا وبالكيفية التي يتم بها تشغيل شبكة آلة الصراف الآلي إذا كان بإمكان مؤسسات التمويل الأصغر عقد شراكة مع شبكة آلة صراف آلي قائمة بالفعل و/أو شركة تشغيل الشبكة، فسيحد ذلك من النفقات التشغيلية التي تقع على عاتق مؤسسة التمويل الأصغر.

- تكلفة امتلاك المعدات مقدماً أو رسوم الاشتراك بالشبكة
- رسوم الإعداد الخاصة بتركيب آلات الصراف الآلي وتوصيلها بالشبكة
- رسوم الاستخدام، سواء على أساس المعاملة الواحدة أو على أساس شهري.

متطلبات تشغيل الصراف الالي

- بنية أساسية يمكن الاعتماد عليها لشبكتي الكهرباء والاتصالات
- أسعار اقتصادية لخطوط الاتصال الهاتفي أو الخطوط المؤجرة والمخصصه من أجل إرسال البيانات واستقبالها من وإلى آلة الصراف الآلي
- قاعدة بيانات مركزية حيث يتم تخزين بيانات العملاء عليها للتحقق من الرصيد
- توفير خدمة ما بعد البيع ودعم يعتمد عليه من قبل المورد أو من الطرف الثالث
- موارد وإجراءات عمليات راسخة لتوزيع البطاقات ومراقبة أرقام التعريف الشخصي
- توفير فئات صحيحة من العملة
- أنظمة لإتمام التحويلات النقدية إلى آلات الصراف الآلي بأمان
- إجراء بعض التعديلات لضمان تحقيق الاستخدام الفعال، كأن يتم تضمين إرشادات شفوية لتوجيه المستخدمين غير الملمين بالقراءة والكتابة

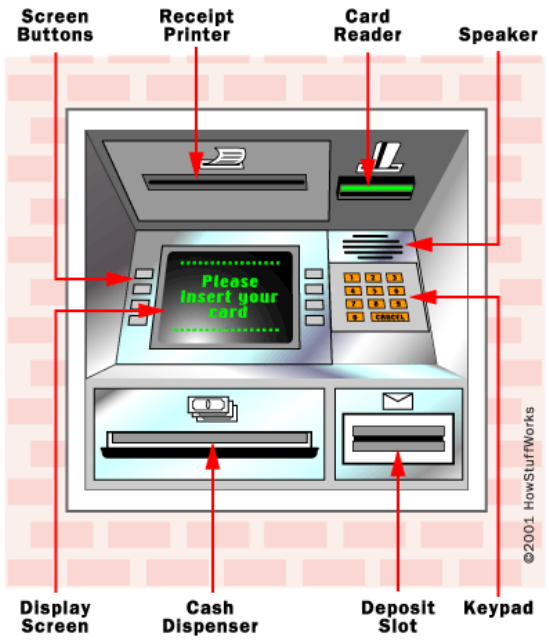
أجزاء الصراف الالي

يتكون الصراف الالى من :

وحده معالجه مركزيه (للتحكم فى الاله)

- بطاقه ممغنطه
- بين باد(PIN Pad) ، وهو جزء مشابه للآلة الحاسبة وكثيراً ما يصنع كجزء من الآلة.
- شاشة وعادة ماتكون LCD قابلة للمس
- وحدة صرف النقدية
- وحدة طباعة اليومية
- وحدة الاشعارات
- وحدة قراءة الكروت
- وحدة الايداعات
- وحدة المظاريف
- الانكريبتور(الخاص بالشفرة)
- وحده لوحه المفاتيح

صورة توضح أجزاء الصراف الالى (2-5)



أفضل مواقع التجارة الالكترونيه

Amazon, Dell, IQVC, EBay, OnSale, My Simon, Dash.com, Productopia, Esmarts, Fogdog, Clinique, Petopia, Wine.com, Cyberian Outpost, RocketCash.com, TheKnot.com, Disney, DVD Express, Preview Travel, REI, Lands' End , Garden.com, Drugstore.com, WorldSpy

إرشادات أمنيه لإستخدام الصراف الالى

- اختر رقما سريا فريدا يصعب على الآخرين توقعه، ولا تربط رقمك السري مع أية بيانات شخصية مثل تاريخ الميلاد وأرقام الهواتف أو أية أرقام أخرى معروفة .
- قم بتغيير رقمك السري بشكل دوري واحتفظ به لنفسك مخزنا في ذاكرتك وليس مكتوبا في أي مكان .
- لا تكشف رقمك السري لأي شخص كان .
- تجنب استخدام الصراف الآلي في الأماكن البعيدة وغير المحمية وتجنب أجهزة الصراف الآلي المجاورة لأماكن يسهل الاختباء فيها .
- ينصح بمراجعة حساباتك البنكية بشكل منتظم وذلك للتأكد من أن أحداً لم يدخل عليها، وأيضا للتعرف على أية حركة غير اعتيادية تم تنفيذها على حسابك. إذا كنت ترغب بان يقوم البنك بتنبيهك عن أية حركة تتم على حسابك أو بطاقتك الائتمانية، يمكنك الاشتراك في خدمة ألرسائل القصيرة .
- كن حذرا عندما يعرض عليك أشخاص لا تعرفهم المساعدة عند جهاز الصراف الآلي .
- إذا ما لاحظت أي شئ مشبوه عند جهاز الصراف الآلي مثل وجود أشخاص يتلاعبون بالمكان المخصص لإدخال البطاقة أو لوحة الأرقام أو أي نشاط مشبوه آخر، لا تستخدم ذلك الجهاز وقم بإبلاغ البنك بشكوكك فورا .
- لا تدخل بطاقتك بالقوة في المكان المخصص لها إن شعرت أن جهاز الصراف الآلي لا يعمل جيدا لأي سبب. اضغط على زر الإلغاء، اسحب بطاقتك وقم بتبليغ البنك. وفي حالة ضياع البطاقة أو سحبها في الصراف، أبلغ البنك فورا ليقوم بإيقاف البطاقة .
- وقع على بطاقتك واحتفظ بها دائما في مكان آمن أو معك ولا تعيرها لأي شخص .
- استخدم بطاقتك فقط على أجهزة الصراف الآلي ونقاط البيع في الأماكن العامة المشهورة والمعروفة لديك وتأكد من استرداد البطاقة بعد كل عملية .
- لدى استخدامك أجهزة الصراف الآلي المخصصة لخدمة السيارات، أبق النافذة بجانب الراكب الأمامي والنوافذ الخلفية مغلقة .
- قم بإلغاء البطاقات غير المستخدمة وإتلاف البطاقات الملغاة .

صور توضح أستخدام الصراف الالى

طرق حمايه الصراف الالى:

هناك طرق كثيرة لعمل ذلك

حمايه الصراف الالى من الكاشطات

دائما يكون الصراف الالى قطعه واحده مستقله بذاتها ولاتكون اكتر من قطعه فهناك من يقوموا بوضع هذه الكاشطات لمعرفه رقم بطاقه الائتمان وكلمه المرور والاستيلاء على الرصيد

صور توضح ذلك (6-2)

نرى فى الصور السابقه ان هناك أختلاف واضح بين لوحه المفاتيح المزورة ولوحه المفاتيح الاصليه كما قلنا سابقا ان الصراف الالى عبارة عن قطعه واحده وليست أكثر من قطعه كما فى الصورة السابقه ويجب الانتباه عند أستخدام الصراف الالى

صورة توضح طريقه وضح لوحه مفاتيح مزورة (7-2)

الصورة السابقه توضح وضع لوحه مفاتيح غيرأصليه "مزورة" على لوحه مفاتيح أصليه
حيث تقوم هذه اللوحه بتخزين كل الارقام السريه

مثال

اذا قام أحد الاشخاص بإستخدام هذه الماكينه وعند كتابه كلمه المرور فبساطه سيتم معرفه كلمه المرور الخاصه بك فيجب توخى الحذر جيداً عند أستخدم ماكينات الصراف الالى

ويجب توخى الحيطه والحذر:

طرق التغلب على خطر الكاشطات

معظم لوحات المفاتيح وأجهزة الصراف الآلي هي مجموعة داخل الجسم وليس جزء مركب فوق القاعده

- دائما تأكد بان فتحة ادخال البطاقه هي ايضا داخل جسم الالة وليس جزء مركب
- من عمليات سرقة الارقام السريه وضع الة تصوير فوق الة السحب الالي , لذا كن حذر وانظر حولك
- استخدم يدك كغطاء اثناء عملية ادخال الرقم السري.
- استخدم دائما أجهزة الصراف ذات نظام الإدخال باللمس على الشاشة
- استخدام أجهزة الصراف الآلي داخل البنوك بدلا من التركيز على الشارع
- لا تعتمد مطلقا على مساعدة الغرباء لطريقه أستخدام بطاقه الائتمان.

حمايه أجهزة الصراف الالى من التزوير

عند أستخدامك لماكينه الصراف الالى عليك بعمل الاتى

- عند كتابه كلمه المرور قم بتغطيه لوحه المفاتيح بيدك وباليد الاخرى قم بكتابه الرقم السرى
- دائما قم بأستخدام ماكينات الصراف الالى الموجوده داخل البنك
- قبل أستخدام ماكينه الصراف الالى قم بالنظر حول الماكينه لانه فى بعض الاحيان يكون هناك كاميرات يتم وضعها فى الاعلى لمعرفه الارقام السريه لكلمات المرور
- البحث عن وجود بعض من المرايا حول أجهزة الصراف الالى فإنها عاده ماتكون فى مكان ما وهى تعطى أفضليه أكثر من الكاميرا من حيث رؤيه كلمات المرور التى تكتبها

صورة توضح وضع كاميرا داخل مصرف ألى (8-2)

فى الصورة السابقه من الواضح وجود كاميرا ترصد كل تحركات العميل الخاصه بعمليات السحب من خلال تلك الكاميرا سيتم سرقه رقم الهويه وكلمه المرور الخاصه بالعميل ويجب الحذر قبل أستخدام الصراف الالى

صورة توضح تركيب قطعه مزورة (1-3)

صورة توضح أستخدام قطع غير أصليه "مزورة" لسرقه الهويه وكلمات المرور

عند تركيب هذه القطه سيتلقى مجموعه من الافراد معلومات عن رقم الحساب الخاص بك عن طريق الإرسال اللاسلكى تتم قراءة المعلومات من خلال القطعه التى تم تركيبها فى فم فتحه الصراف الالى وفى الوقت نفسه يتم وضع كاميرا لاسلكيه كما فى الصورة التاليه شكل(2-3)

ويتم بعد ذلك تثبيت هذه الكاميرا على الحامل بعد ذلك كما فى الصورة التاليه

شكل الكاميرا بعد تثبيتها على الحامل(3-3)

وبعد تثبيت الكاميرا نلاحظ تم وضعها فى مكان لتصوير كل الحركات الماليه التى تتم على هذا الصراف وإرسال كل معلومات العميل سواء كلمه المرور او رقم البطاقه

شكل يوضح تركيب الكاميرا بالداخل(4-3)

توضح الصورة السابقه تركيب الكاميرا بالداخل

حمايه أنفسنا من خطر كاشطات الصراف الالى How to Protect Yourself from ATM Skimmers

- قبل أستخدام الصراف الالى إنظر اليه جيداً اذا وجدت أسلاك او ماشابه ذلك ,ماسح ضوئى لاتستخدم هذه الجهاز وقم بالإبلاغ عنه فى الفرع التابع له
- لاتستخدم الصراف الالى اذا وجدت أن هناك شخصا ما يمد لك عون المساعده فى كيفيه الإستخدام لان فى كثير من الاحيان من يضعوا الكاشطات يكونوا قريين من الصراف الالى أقرب مسافه ممكنه
- عند وضع البطاقه فى الفتحه المخصصه لها وكتابه كلمه المرور تأكد من ان المكان خالى من الكاميرات وقم بتغطيه لوحه المفاتيح بيد وكتابه كلمه المرور باليد الأخرى
- أستخدم دائما أجهزة الصراف الالى التى تعمل بالمس
- تحقق دائما من رصيدك حيث اذا كان هناك من يسرق رصيدك ف بألإطلاع على رصيك بصفه دوريه سيحد ذلك من السرقه

تعريف مصطلح مواقع التجارة الإلكترونيه :

هو موقع تم وضعه على الانترنت لبيع المنتجات عبر الانترنت للعملاء المعلومات عاده مايتم تشفيرها والمزايا التى تشملها مواقع التجارة الالكترونيه خفض التكاليف ,الانتشار فى وقت صغيرخفض تكاليف الموظفين ,فتح أسواق جديده فى مناطق مختلفه بسهوله ويسرجذب عدد كبير من العملاء فى كل دول العالم

كيف تختار أستضافه تؤهلك للعمل على الانترنت

متطلبات الموقع

أولا وقبل كل شيء .الخطوة الأساسية هى عملية اختيار الاستضافة المناسبه على شبكة الانترنت لابد ان نعرف ما نحتاجه بعد ذلك ، وسوف تكون قادرعلى ايجاد حلول تناسب هذه الاحتياجات .على سبيل المثال ، .تحتاج إلى أن يكون لديك فكرة عن حجم الصور المنتج الخاص بك لتحديد المساحه الكافيه التى تحتاجها واذا كانت هناك ملفات فلاش على موقعك فالطبع ستحتاج مساحه أكبر،قم بعمل محاولة لتقدير عدد الزوار شهريا لموقعك

الدعم الفنى:

ماهو الدعم الفنى : الدعم الفنى هو المعالجه الفنيه التى قد تواجهك أثناء قيامك بعمليات التحديث والتطوير لموقعك على الانترنت

مما يتألف الدعم الفنى :

ويتألف فريق الدعم الفني من الأفراد الذين على دراية كامله ,ومعرفه شبه كامله لإكتشاف المشاكل ، وهم قادرون على إكتشاف معظم المشاكل التي يمكن للمستخدم ان يقع بها والعمل على حلها

متى نحتاج الى الدعم الفنى

- عند الوقوع فى مشاكل وأزمات

- عند الرغبه فى إضافه تحسينات جديده للموقع

نصائح للمتعاميلن مع الدعم الفنى

- حاول بقدر الامكان توصيل وجهه نظرك والمشكله التى تقابلك بطريقه سهله
- أستخدام أسلوب لائق فى الحوار
- عدم العصبيه وحاول دائما ضبط النفس
- تدوين المشكله فى ورقه ثم بعد ذلك عرضها على الدعم

إمكانيه التفاعل مع العملاء:

هل كان لديك موقع ويب خاص بالتجارة الإلكترونية وكان غير حسن المظهر فبهذه الخاصيه تفيد ان يكون لديك التفاعل مع العملاء سواء بالتعديل على الموقع وإضافه تحسينات جديده للموقع والتفاعل بين القائمين على الموقع وزوار الموقع، على سبيل المثال فكرة لدمج منتج مع منتج أخر اذا كان من نفس النوعيه وحيث تعتبر من أفضل الطرق للحفاظ على الاتصال المباشر بين موقع الويب والعملاء وإنها ايضأ تتيح للمشترين فرصة لاظهار فكر خاص بهم اطلب من مزود الخدمه "الاستضافه" ما إذا كانت تقدم هذه الميزات بحيث يمكنك بسهولة إضافة هذه الوظيفة إلى موقع الويب الخاص بك أم لا لأن ذلك يغرس الثقة بين الموقع والزوار وهى وسيلة رائعة لزيادة زوار موقعك

التدابير الامنيه :

لابد من اتخاذ تدابيرأمنيه لحماية امن المعاملات الخاصة بك على الانترنت حيث تتم هذه العمليه في أمان وينبغي أن تكون مشفرة حتى لاتتعرض تلك المعاملات الماليه للتحايل والسرقه ومعرفه التقنيات التى تستخدمها مواقع الاستضافه ولذلك ، تحتاج إلى التأكد من أن لدى مزود الاستضافة شهادة خدمة تصميم المواقع بالنسبة لك المواقع المخصصة ، قد تحتاج إلى شراء المزيد من المال .للمساعدة في تأمين البيانات المعاملة من اللصوص عبر الانترنت ، من المستحسن أن ما لا يقل عن عقد خدمة تصميم المواقع المشتركة على موقع للتجارة الإلكترونية الخاصة بك

ويجب مراعاه الاتى :

لاتستعمل أبدا كلمات مرور سهله التخمين لان ذلك يؤدى الى إرتفاع معدلات الاختراق
جعل كلمات المرور لكل حساب على الانترنت تكون فريده من نوعها
حاول الجمع بين الكلمات الصغير والكبيرة والرموز فى نفس الوقت
اذا كنت تواجه صعوبه فى إنشاء كلمه مرور يمكنك أستخدام مولد كلمات المرور Generate password

الثقافه والإطلاع :

يجب على شركات الاستضافه الاطلاع على كل ماهو جديد سواء الثغرات التى تظهر بشكل يومى وطرق الحمايه وكيفيه سد هذه الثغرات وذلك من اجل بث الثقه لدى العملاء التى تتعامل معهم حاليا وايضأ العملاء المتوقعين بعد ذلك

الإختلافات بين أستضافه كل من لينكس, ويندوز

- لينكس هو نظام مفتوح المصدر وبالتالى فهو الاقل تكلفه من حيث التشغيل والصيانه مقارنه بالويندوز وهذا معناه ان أستضافه لينكس ستكون بالضرورة الاقل تكلفه من ويندوز ,ويتميز لينكس بالسرعه والاستقرار وبالتالى فأن كثير من العمليات تتم إدراتها بطرق أسرع من ويندوز حيث يفضل الكثير من المطورين أستضافه لينكس لانها تستنفذ الاقل من موارد المعالج إضافه لذلك يحمله الكثير من المطورين كونه نظام مجانى والسيرفرات التى تستضيف موقعك سوف تعمل على نظام لينكس

لينكس تدعم عدد كبير من البرمجيات والتطبيقات واللغات وقواعد البيانات نذكر منها PHP, Perl, PostGre, MySQL, PostgreSQLوغيرها الكثير من التطبيقات والبرمجيات على العكس تماما لينكس غير متوافقه تماما مع بعض تقنيات مايكروسوفت اذا كنت تستخدم ASP, MS SQL, or VB وأدوت التطوير سيكون الخيار الافضل لك هو الويندوز .

- الميزة الرئيسيه لخودام مايكروسوفت هو دعمها الكامل لكل برمجيات مايكروسوفت حيث يمكن تشغيل برامج مايكروسوفت على سبيل المثال MS SQL databases , Access وتتيح ايضا خودام مايكروسوفت لمطورى الويب أستخدام بيئات تطويريه مثل Active Server Pages (ASP), Visual Basic Scripts, MS Index Server ويمكن للمستخدمين تطوير موقع

على شبكه الأنترنت بأستخدام واجهه مألوفه من الادوات مثل Visual Interdev, and Microsoft Access مع مستخدمى asp بأمكانهم تطوير مواقع على شبكه الانترنت بأستخدام قواعد بيانات مدفوعه مثل Microsoft Access and Microsoft SQL

نظرة عامه عن الحمايه :

التجارة الالكترونيه والحمايه من الغش

كل يوم على شبكه الانترنت يتم سرقه الملايين والسيطرة على المواقع ومن يقوموا بذلك ليسوا لصوص عادين لانهم بكل بساطه يعرفون جيداً كيف تعمل بطاقات الائتمان وبالتالى فمن الاهميه ان تقوم هذه المواقع بعمل شبه تصفيه للمستخدمين الغير صالحين والكشف عنهم والابلاغ عنهم وبالتالى الحد من المعاملات المشبوهه

ويمكن السيطرة بسهوله على هذا الامر والحد من الإحتيال عبر الانترنت من خلال لوحه التحكم يمكن لصاحب الموقع عمل الاتى

حظر عناوين معينه على سبيل المثال حظر الاى بى ,الرقم البريدى
وضع ضوابط لعدد المعاملات التى تتم يوميا
عمل قائمه تحتوى على عملاء جيدين السمعه واخرى تحتوى على عملاء سيئين السمعه

تامين التجارة الالكترونيه حقيقه ام خيال

أراء خبراء أمن الانترنت التجارة الالكترونيه تعتبر الاكثر أمنا من التجارة التقليديه
هل يمكن للصوص الانترنت الإستيلاء بطاقات أئتمان العميل
فى حقيقه الامر يصعب ذلك لان نظام التجارة الالكترونيه مبنى بطرق تجعله من الصعب السيطرة عليه وبالتالى سرقه عدد من بطاقات الائتمان

لان الموقع يستخدم تقنيات التشفير قبل إرسال المعلومات وايضأ هذه البيانات تبقى مشفرة على خادم صاحب الموقع وحتى لو تم أعتراض هذه البيانات لم يجدوا وسيله لقراءتها لانها مشفرة

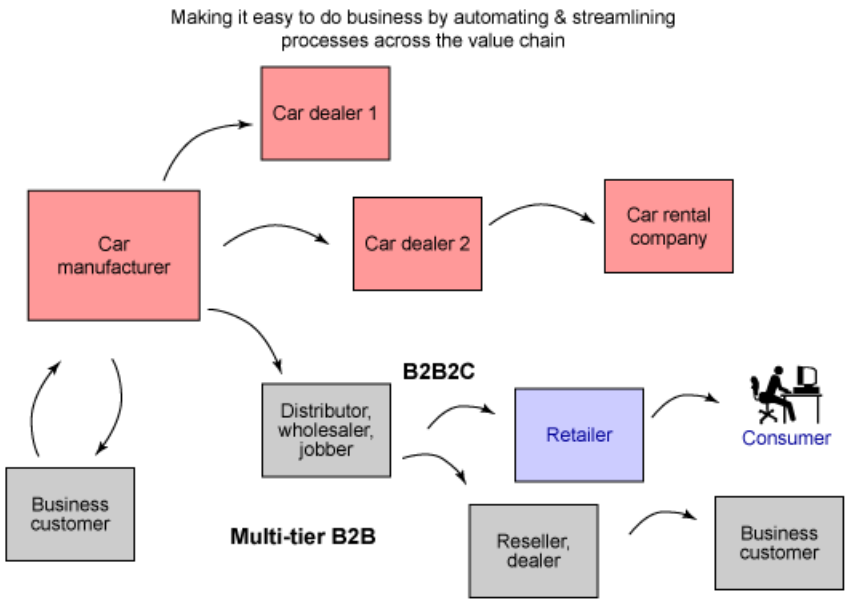
وبالتالى يجب اليقظه دائما ويجب معرفه المشاكل المحتمله وطرق إصلاحها ويجب الاستعانه بشركات أستضافه ذات سمعه جيدة حيث الشركات الصغيرة لاتمتلك الخبرة اللازمه لمواجهه تلك المشاكل

وبالتالى ماذا يحدث اذا قام أحد الاشخاص بسرقه رقم بطاقه الائتمان من العميل

- معظم البنوك توفر للمستهلك الحمايه اللازمه قبل أستخدام هذه البطاقات على سبيل المثال تنشيط البطاقه من عدمه

التجارة الالكترونيه الهجمات الوقائيه والاستراتيجيات e-Commerce security: Attacks and preventive strategies

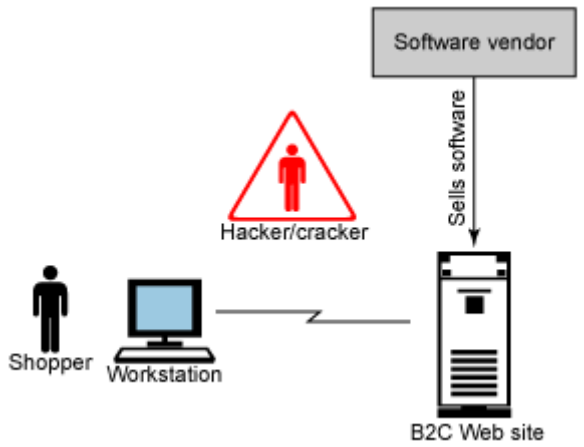
شكل يوضح الاعمال التجاريه المشتركه(5-3)



اللاعبين: The players

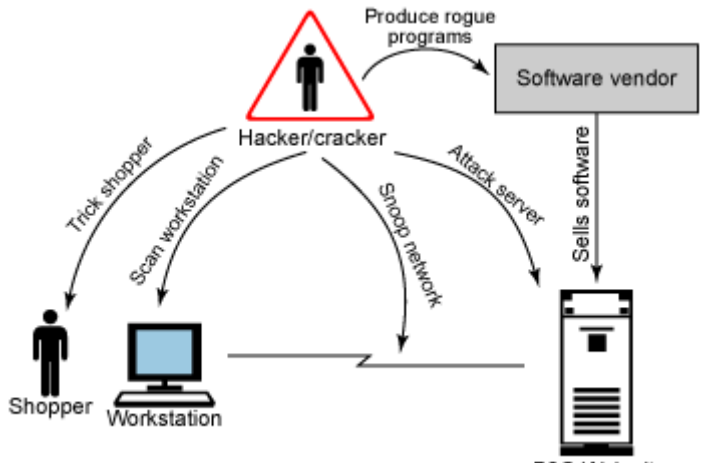
عادات المتسوق على شبكه الانترنت وقيامه بعمليه الشراء هذا النشاط يوضح أربع لاعبين أساسين وهما "أربع عناصر مشتركه" لاعب رقم واحد وهو المتسوق : وهو الذى يستخدم المتصفح لتحديد الموقع الذى يريد الشراء منه

شكل يوضح وجود "المتسوق" وبدئه مرحله التسوق (3-6)



نرى فى الشكل السابق ان يتم محاصرة اللاعب"المتسوق" من قبل اللاعب الاخر " المهاجم" الهاكرز وأستغلال العميل والسيطرة عليه سواء وذلك عن طريق:
ببرمجيات حديثه تؤدى الى أستغلال النظام
على سبيل المثال
اذا حاول لص الدخول الى المنزل ووجد ان الباب مقفل فإنه بالضرورة سيحاول الدخول الى المنزل بطريقه اخرى

النقاط التى يمكن للمهاجم تحديدها "الهاكرز"(3-7)



خداع المتسوق Tricking the shopper

يعتبر خداع المتسوق من الهجمات الأسهل والأكثر ربحية تعتمد على خداع المتسوق،وأستخدام تقنيات الهندسة الاجتماعية,وتشمل هذه الهجمات مراقبة سلوك المتسوق، وجمع المعلومات لإستخدامها ضد المتسوق وخداعه بصفحه تحتوى على طلب بكتابه كلمه المرور وتأكيدها وذلك لكى يتمكن من السيطرة على الموقع وبالتالى السيطرة على أرقام بطاقات الائتمان.

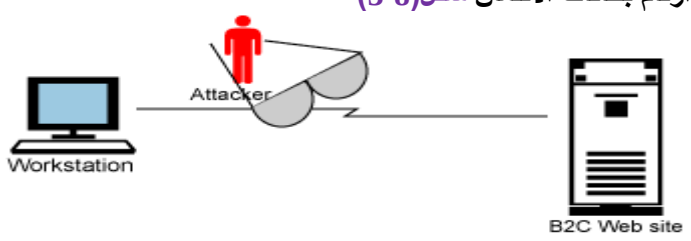
التجسس على جهاز المتسوق Snooping the shopper's computer

فى الفترة الاخيرة أصبح لدى كثير من المستخدمين يملكون إجهزة كمبيوتر وبسبب أنخفاض خدمه توصيل الانترنت أصبح الاقبال على توصيل تلك الخدمه متزايد يوم عن أخر معظم المستخدمين ليس لديهم درايه كامله بالثغرات الامنيه security vulnerabilities إضافه الى ذلك ان بائعى أجهزة الكمبيوتر والبرمجيات يضمنون ان أجهزتهم وبرامجهم تتمتع بمميزات الامان مثال يقوم عدد كبير من المستخدمين بتعطيل وفتح منافذ معينه فى الجهاز لتمكين برنامج ما من العمل وهذا مايستغله الهاكرز

على سبيل المثال عند قيام أحد المستخدمين بشراءبرنامج جدار حمايه ورأى ان هناك تعارض بين الجدار النارى والبرنامج الاخر يقوم على الفور بتعطيل الجدار النارى

التعرف على الشبكه Sniffing the network

فى هذا الشكل يراقب المهاجم"الهكرز" البيانات الموجوده بين الكمبيوتر والمتسوق والخادم بعد ذلك يتم جمع البيانات الخاصه بالمتسوق ثم بعد ذلك سرقه المعلومات الشخصيه مثل أرقام بطاقات الائتمان شكل(3-8)

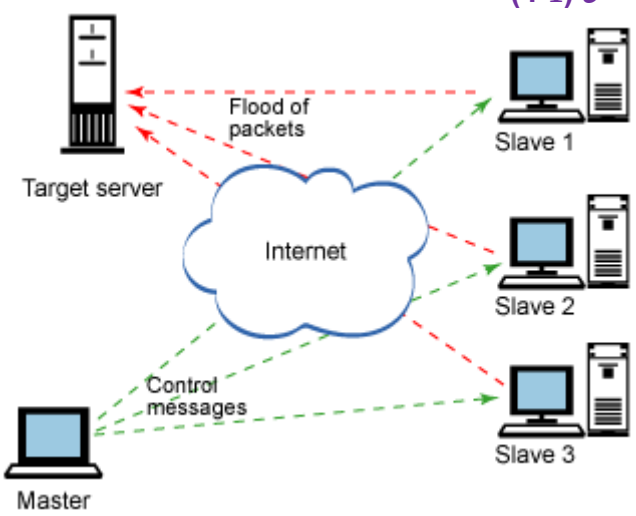


تخمين كلمات المرور Guessing passwords

وهناك هجوم أخر يعتبر الاكثر شيوعا وهو تخمين كلمات المرور وهذا النمط يكون إما يدوى او ألى حيث تعتبر الهجمات اليدويه شاقه والنجاح فيه يعتبر ضئيل الى حد ما على سبيل المثال اذا كان المهاجم "الهاكرز" يعرف اى معلومات عن المتسوق "الضحيه" فهذه الحاله ستكون العمليه سهله والعكس تماما والنوع الاخر هو الهجوم الالى وهو الاعتماد على البرمجيات المنتشرة على الانترنت لتخمين كلمات المرور وتعتبر هذه الاكثر قوة.

هجمات الحرمان من الخدمه Using denial of service attacks

وتعتبر هجمات الحرمان من الخدمه واحده من أفضل الامثله التى تؤثر على الموقع
شكل يوضح هجمات الحرمان من الخدمه شكل (1-4)



تعريف هجمات الحرمان من الخدمه (DOS Attacks)

هي هجمات تتم عن طريق إغراق المواقع بسيل من البيانات غير اللازمة يتم إرسالها عن طريق أجهزة مصابة ببرامج فى *هذه الحالة تسمى* ***DOS Attacks*** تعمل نشر هذ الهجمات بحيث يتحكم فيها القراصنة الإلكترونيين لمهاجمة (الإنترنت)عن بعد بإرسال تلك البيانات إلى المواقع بشكل كثيف مما يسبب بطء بهذه المواقع ويسبب صعوبة وصول المستخدمين لها نظرًا لهذا البطء، خصوصا وأنه يبدو، وباعتراف الكثير من خبراء الأمن على الانترنت، وكأنه لا يوجد علاج في الوقت الحالي لهذا الأسلوب في الهجوم على مواقع (الإنترنت)، وعلى هذا الأساس فإن هذا النوع من الهجمات يُدعى في بعض الأوساط " بإيذ الإنترنت ".ويتم هذا الهجوم بدون كسر ملفات كلمات السر أو سرقة البيانات السرية، هجمات حجب الخدمة تتم ببساطه بان يقوم المهاجم بإطلاق أحد البرامج التي تزحم المرور للموقع الخاص بك وبالتالي تمنع أي مستخدم آخر من الوصول إليه. وبشكل عام تتواجد مثل هذه الهجمات منذ أعوام إلا أن قوتها الآن أصبحت أكبر من أي فترة مضت، كما أنها وصلت إلى مرحلة من النضج بحيث تستهدف أهدافًا محددة ومقصودة لأغراض تجارية هذا وتذكر شركة سمانتك المتخصصة في الأمن الإلكتروني أن متوسط عدد هجمات الحرمان من الخدمة وصل إلى 927 هجمة في النصف الأول من عام 2004 بزيادة قدرها 679% عنها في النصف الثاني من عام 2004

انواع هجمات الحرمان من الخدمه

هجمات Ping Of Death وTeardrop

الهجمات التى تستخدم خطأ برمجى bus فى بناء Tcp/ip
الهجمات التى تستغل تقصير فى مواصفات Tcp/ip
الهجمات التي تعيق المرور في شبكتك حتى لا تستطيع أي بيانات ان تصل إليها أو تغادرها

تعريف ssl (Secure Sockets Layer)

هي اختصار لـ Secure Sockets Layer وهو بروتوكول يستخدم لحماية مواقع الانترنت عن طريق تشفير البيانات وهو من تطوير Netscape وقوة التشفير اما 40-bit و 128 bit-والاخير كان مستخدما في الولايات المتحدة فقط وتمت الموافقة على استخدامه منذ فترة وجيزة ، ومعظم مواقع الاستضافة تقدم هذه الخدمة مجانياً

تويزة طبقة الفتحات الآمنه SSL

هو برنامج به بروتوكول تشفير متخصص لنقل البيانات و المعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة امنه بحيث لا يمكن لأحد من الناس قراءتها غير المرسل و المستقبل وفي نفس الوقت تكون قوة التشفير فيها قوية و يصعب فكها ، وهي تختلف عن بقية طرق التشفير في شئ واحد الا وهو عدم الطلب من مرسل البيانات اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها وكل الذي يفعله المستخدم هو التأكد من استخدام هذا البروتوكول بالقوة المطلوبة ،ولقد ساعدت هذه التقنية التي طورتها شركة نت سكيب على زيادة الثقة بالتجارة الإلكترونية ومستوى الأمان فيها مما جعلها أساس التجارة الإلكترونية الناجحة على مستوى العالم ولقد قامت جميع الشركات المنتجة لمتصفحات الإنترنت بالأخذ بها وتزويد متصفحاتها بهذه التقنية

كيفية عمل هذه التقنية

يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم (المشتري) بجهاز الخادم الخاص بالموقع المراد الشراء منه وهذا طبعا إذا كان الخادم مزود بهذه التقنية أساسا، و يقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح وصولا الى جهاز الخادم الخاص بالموقع باستخدام بروتوكول التحكم بالإرسال و بروتوكول الإنترنت وهو ما يعرف ب

TCP/IP

و لقد سميت بالطبقة الآمنه لأن هذا البرنامج يعمل كطبقة وسيطه تربط بين بروتوكول التحكم بالنقل و بروتوكول

HTTP:// (HyperText Transfer Protocol)

و تتلخص خطوات استخدام هذه التكنولوجيا في ثلاث خطوات وهي

أولا

يقوم الموقع بالتقدم الى احدى الهيئات المستقلة و التي تصدر شهادة رقمية تثبت صحة هوية الموقع ، و بعد التأكد من نشاط و حسن سيرة تلك المواقع المتقدمة بالإضافة لاستكمال بعض المتطلبات الأخرى ذات العلاقة تقوم تلك الهيئه بإصدار الشهادة الرقمية الخاصة بالموقع بحيث يدون فيه كل المعلومات الهامه مثل اسم الشركة وتاريخ اصدار الشهادة و تاريخ الإنتهاء ، و كذلك يتم اصدار المفتاح العام و المفتاح الخاص للموقع و يقوم الموقع أيضا بتأمين جهاز خادم "مزود الخدم" ببرنامج التشفير إس إس إل ليتم تخزين المفتاح العام للموقع به

ثانيا

عند دخول المشتري(زائر الموقع) للصفحة الآمنه التي يدخل بها البيانات و المعلومات المطلوبة للشراء يقوم المتصفح المزود بهذا البرنامج بالإرتباط بالجهاز الخادم الامن للموقع ويطلب منه التالي: الشهادة الرقمية، مصدرها ، تاريخ انتهاءها وكذلك تتم المقارنة بين اسم الموقع على الشهادة مع اسم الموقع في جهاز الخادم و المقارنة بين الرقم العام المرسل من الجهاز الخادم الى المتصفح مع التوقيع الإلكتروني للشركة و كل هذه الخطوات تتم للتأكد من مصداقية الموقع و حمايتك من الشركات الوهمية علما بأن جميع هذه الخطوات تتم بواسطة المتصفح لديك دون علمك أو تدخلك وبعدما يتم التأكد من كل ذلك يقوم المتصفح بإعلامك بالنتيجة في حال عدم المطابقة أو اذا كانت هناك ملاحظات

ثالثا

بعد خطوة التأكد من مصداقية الموقع والإرتباط بجهاز الخادم الآمن يتم تشفير المعلومات على أساس المفتاح العام لذلك الموقع ليتم نقل المعلومات بطريقة آمنه دون أي تدخل منك و لا يستطيع أحد سرقة المعلومات أو الإطلاع عليها سوى الموقع المعتمد في الطرف الاخر و الذي يملك المفتاح الخاص لفتح واعادة المعلومات الى وضعها الطبيعي

كيف تحمي المواقع المعلومات الخاصة بالزبائن

طبعا لأهمية موضوع الأمن بالنسبة لمواقع البيع الإلكترونية فهي تتخذ الكثير من الإجراءات الإحترازية بخلاف ماتتخذه من ترتيبات متعلقة بتكنولوجيا الحماية لأن معظم العملاء يودون معرفة المزيد عن سرية تناول وتداول هذه المعلومات بعد وصولها الى الموقع بسلام و ماذا يحدث بعد فتح التشفير ولذلك فإن معظم المواقع تقوم بعدة خطوات اخرى لحماية العملاء لأن أي اهتزاز للثقة يعني فقدان الكثير للموقع ولذلك فهي

تتعامل بكل جدية في هذا الموضوع و اليكم ملخص لما تتخذه كل المواقع العالمية من اجراءات لحماية البيانات الخاصة بالعملاء

أولا : حصر فتح المعلومات المشفرة على عدد قليل من الموظفين الموثوق بهم

ثانيا : يتم توزيع المعلومات بعد فتحها وفرزها الى الأقسام المتخصصة الكترونيا بحيث لا يتم اعطاء أي قسم سوى المعلومات التي يحتاجها فعليا فمثلا لا يتم اعطاء رقم بطاقة الإئتمان الا لقسم المحاسبة لخصم المبلغ و يتم تشفيرها مرة أخرى ولايمكن لاي شخص أن يطلع عليها

ثالثا : يقوم الموقع بإضافة جميع البيانات الخاصة بك في بنك المعلومات الخاصة بالموقع و هي محمية بجدران الحمايه وكلمات المرور ولا يمكن لأي شخص غير مخول له بالوصول اليها

رابعا : تقوم المواقع بعمل عدة طبقات من الصلاحيات للموظفين بحيث لا يمكن لأي موظف الوصول الى معلومات غير مصرح له بالوصول اليها فمثلا موظف في قسم الشحن والتخليص ليس له من صلاحيات الا الوصول الى معلومات عن رقم الطلبية وتاريخها والعنوان المرسل اليه

خامسا : التحكم بالحركة في بعض اقسام الشركة فمثلا لا يسمح بالدخول الى قسم بنك المعلومات الا للموظفين المصرح لهم و الذين يملكون ارقام سرية للدخول

سادسا : يتم الإحتفاظ بأرقام بطاقات الإئتمان مشفرة في أجهزة مستقلة داخل قسم بنك المعلومات و هي غير مرتبطة بالإنترنت

سابعا : أي تداول للمعلومات بين الأقسام المختلفة بالشركة لا تحمل رقم بطاقة الإئتمان وان حصل فإنها لا تظهر سوى نوع البطاقة واخر اربعة ارقام

ثامنا : في أي تعاملات مالية مستقبلية بينك وبين الموقع يتم كل شئ الكترونيا دون أي تدخل أو اطلاع من الموظفين على معلوماتك مرة أخرى.

- متطلبات الامان Security requirements
- مبادئ التشفير Cryptography principles
- SSL/TLS
- التنسقيات التى تستند الى البروتوكلات و XML
- كيف يمكن الاستفاده من السابق لتنفيذ تجارة إلكترونيه أمنه

متطلبات الأمان Security Requirements

عناصر أساسيه لتوفير الأمن

- المصادقه Authentication
- التفويض Authorization
- السلامة Integrity
- السريه Confidentiality
- عدم التنصل Non-repudiation

المصادقه Authentication

- فى هذا الامر يتطلب التحقق من هويه الكيان "المكان" المخصص للعمل
- وهو عمل من أعمال التحقق من ادعاء الهوية على سبيل المثال قيام احد الاشخاص فلان الفلاني عندما يذهب الى البنك ليقوم بعمليه السحب ، يطلب الصرف الالي من فلان الفلاني مطالبته بالهوية "وضع بيانات البطاقه واذا حدثت مشكله ما يطلب منك شئ للتأكد من الاسم الذى على البطاقه خاصه بك وقد يطلب رخصه قياده ان وجدت للتأكد من ان الاسم الذى على البطاقه هو الاسم الذى فى رخصه القياده، ،

ويتم المقارنه بعد ذلك بين البيانات

- **وهناك ثلاثة أنواع مختلفة من المعلومات التي يمكن استخدامها من أجل المصادقة ، .ومن الأمثلة رقم التعريف الشخصي ، كلمة السر ، أو اسم قبل الاخير من عائلتك على سبيل المثال**

هذا الامر يتطلب خطوتين

- **تحديد الهويه Identification**
- **التحقق Verification**

السريه Authorization

حق الوصول الى موارد النظام بمعنى "من له الحق الإطلاع على كل صغيرة وكبيرة فى النظام

وبالتالى يتم تحديد عمليات الترخيص وماهى الحقوق التى لديك

السلامه Integrity

وفى هذا الامر يتم التأكد من سلامه أمن المعلومات اى لايمكن الحصول على البيانات بدون تصريح بذلك على سبيل المثال بيانات العملاءلايمكن الإطلاع عليها الا بدون إذن بعمل ذلك وبالتالى لايمكن تعديل البيانات ويكون هذا الامر منفعه للعملاء للتأكد من ان بياناتهم وخصوصيتهم لايتم تعديلها ، قادرعلى قيامه بعمليات التصويت أكثر من مرة في الطرق التى تؤدى الى إنتهاك السلامه ولكن بدون يمكن تغيير البيانات بطريقة غير صحيحة .

مثال على ذلك عندما يقوم شخص ما استطلاع على الانترنت وهناك العديد من قصد ومعظم التحديثات فى قاعدة بيانات

السريه Confidentiality

هو مصطلح يستخدم لمنع الكشف عن المعلومات الى نظم وافراد غير مرخص لهم بذلك على سبيل المثال يتطلب معامله بطاقه الائتمان على شبكه الانترنت معرفه "رقم الى التاجر وفى هذا الامر يحاول النظام فرض عند الإرسال حيث قد تظهر فى قواعد البيانات عليها فسيعتبر ذلك أنتهاك للسريه وبالتالى فأن خرق سرقه كمبيوتر يحتوى على معلومات مهمه للعاملين الهاتف يعتبر أنتهاكا للسريه اذا كان الطالب غير

بطاقه الائتمان" التى تحال من المشترى السريه عن طريق تشفير بطاقه الائتمان ,والنسخ الاحتياطى لذا اذا تم الإطلاع السريه يأخذ أشكال كثيرة منها اذا تم أيضا اذا تم إعطاء معلومات سريه عبر مخول له للحصول على هذه المعلومات

عدم التنصل Non-Repudiation

في القانون، يعني عدم الإنكار نية المرء الوفاء بالتزاماتها لعقد ما قم أبرم مسبقا التجارة الإلكترونية تستخدم تكنولوجيا مثل التشفير والتواقيع الرقمية لإثبات صحتها تأكيد على أن مُرسِل المعلومات حاصل على إثبات ورد له إثبات لهوية المُرسِل بحيث لا يستطيع هي الخدمة الأمنية التي بها لا تستطيع الكيانات إنكار تلك المشاركة وبشكل أكثر تفصيلاً فان بإرسال رسالة (دليل عدم إنكار المصدر) والكيان الرسالة (دليل عدم إنكار التسليم.

لتسليمها وأن متلقي تلك المعلومات قد أحدهما إنكار قيامه بمعالجة المعلومات المشاركة فيها أحد عمليات الاتصال الكيان المُرسِل لا يستطيع إنكار قيامه المستقبل لا يستطيع إنكار تسلمُه لتلك

المخاطر Risks

هو أحتمال ان شيئا سوف يحدث نظير مشكله فى تامين الموقع او أستخدام سياسات غير متوافقه مع العملاء كل ذلك يندرج تحت مسمى "الخطر"

أنواع المخاطر Types of Risks

المصادقه Authentication

الترخيص Authorization

السلامه Integrity

السريه Confidentiality

مقدمه عن علم التشفير

عُرف علم التشفير أو التعمية منذ القدم، حيث استخدم في المجال الحربي والعسكري, فقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة, وكذلك ذكر أن العرب لهم محاولات قديمة في مجال التشفير, و استخدم الصينيون طرق عديدة في علم التشفير والتعمية لنقل الرسائل أثناء الحروب, فقد كان قصدهم من استخدام التشفير هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو فإنه تصعب عليه فهمها, وأفضل طريقة استخدمت في القدم هي طريقة القصير جوليوس وهو أحد قياصرة الروم, أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذا العلم "التشفير" وذلك لإرتبط العالم ببعضه عبر شبكات مفتوحة, وحيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين او بين المنظمات الخاصة والعامة، عسكرية كانت أم مدنية. فلابد من طرق تحفظ سرية المعلومات. فقد بذلت الجهود الكبيرة من جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات

ما هو التشفير أو التعمية:(Cryptography)

التشفير هو العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات, التشفير يُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنه- مثل الإنترنت- وعليه لا يمكن قراءتها من قبل اي شخص ما عدا الشخص المرسل لـه, وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (Cryptoanalysis)هو علم لكسر و خرق الاتصالات الآمنة.

أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

- السرية أو الخصوصية:(Confidentiality)

هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الإطلاع عليها.

- تكامل البيانات:(Integrity)

وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

- إثبات الهوية:(Authentication)

وهي خدمة تستخدم لإثبات هوية التعامل مع البيانات (المصرح لهم).

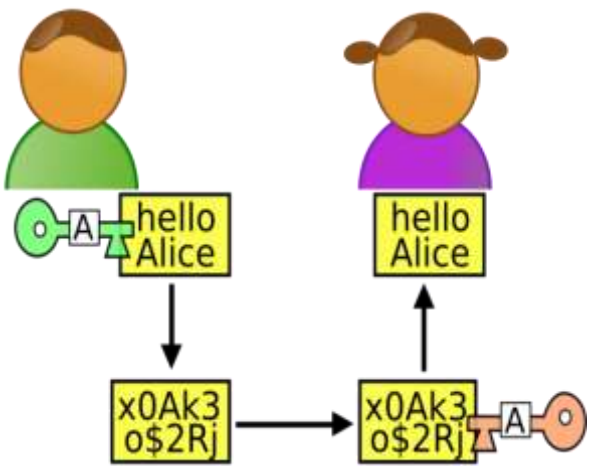
- عدم الجحود:(Non-repudiation)

وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات للأشخاص ليتم الحفاظ على أمن معلوماتهم.

كيفية عمل التشفير:

خوارزمية التشفير دالة رياضية تستخدم في عملية التشفير وفك التشفير وهو يعمل بالاتحاد مع المفتاح أو كلمة السر أو الرقم أو العبارة، لتشفير النصوص المقروءة شكل يوضح طريقه عمل التشفير (2-4)



نفس النص المقروء يشفر إلى نصوص مشفرة مختلفة مع مفاتيح مختلفة

والأمن في البيانات المشفرة يعتمد على أمرين مهمين قوة خوارزمية التشفير وسرية المفتاح

أنواع التشفير:

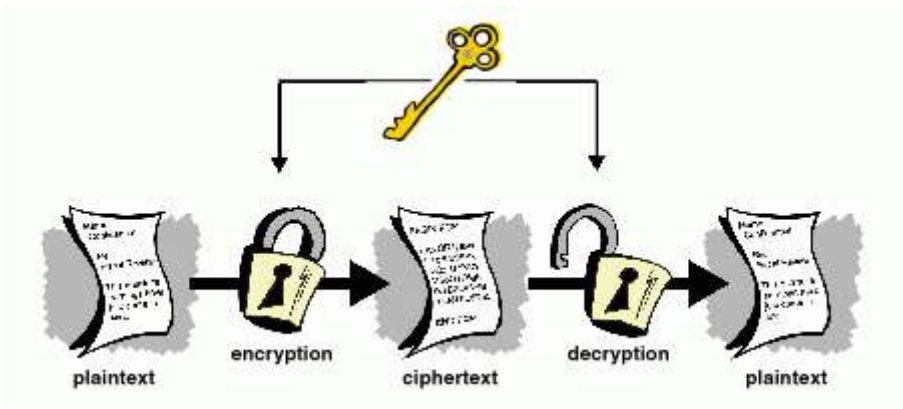
حالياً يوجد نوعان من التشفير وهما كالتالي:

2 - التشفير التقليدي.(**Conventional Cryptography**)
3 - تشفير المفتاح العام .(**Public Key Cryptography**)

التشفير التقليدي:

وهو يستخدم مفتاح واحد لعملية التشفير وفك التشفير (Cryptography Symmetric) يسمى أيضاً التشفير المتماثل للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. مثال على ذلك؛ إذا أراد زيد إرسال رسالة مشفرة إلى عبيد، عليه إيجاد طريقة آمنة لإرسال المفتاح إلى عبيد. فإذا حصل أي شخص

شكل يوضح أستخدام التشفير بالمفتاح الواحد (3-4)



بعض الأمثلة على أنظمة التشفير التقليدي:

- **شيفرة قيصر** :وهي طريقة قديمة ابتكرها القيصر جوليوس لعمل الرسائل المشفرة بين قطاعات الجيش وقد أثبتت فاعليتها في عصره. ولكن في عصرنا الحديث ومع تطور الكمبيوتر لا يمكن استخدام هذه الطريقة وذلك لسرعة كشف محتوى الرسائل المشفرة بها .المثال التالي يوضح طريقة عمل شيفرة قيصر: إذا شفرنا كلمة "SECRET"واستخدمنا قيمة المفتاح 3، فإننا نقوم بتغيير مواضع الحروف ابتداءً من الحرف الثالث وهو الحرف "D"، وعليه فان ترتيب الحروف سوف يكون على الشكل التالي:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" تكون على الشكل الحالي:

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

الآن قيمة الـ A à D، B à E، C à F، وهكذا.

بهذا الشكل فان كلمة "SECRET" سوف تكون ."VHFUHW"لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة؛ يجب أن ترسل له قيمة المفتاح "3".

- تشفير البيانات القياسي :(DES) طور هذا النظام في نهاية السبعينيات من قبل وكالة الأمن القومي الأمريكية، وهذا النظام بات من الجدوى عدم استخدامه مع تطور أنظمة الكمبيوتر وزيادة سرعة معالجته للبيانات، حيث أنه قد يتم كشف محتوى رسائل مشفرة به في وقت قصير.

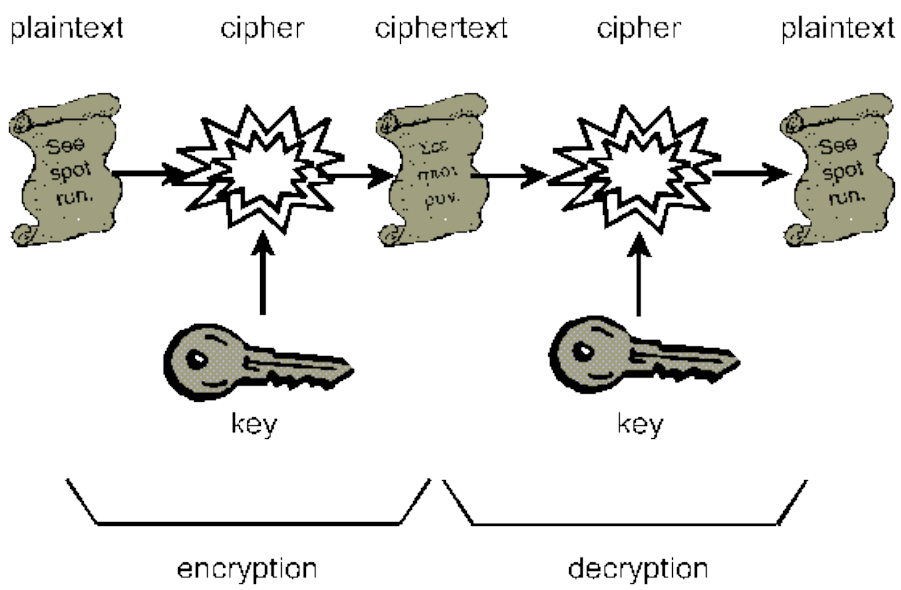
- وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير :AES, IDEA, 3DES, blowfish,

كل ما ذكر من الأمثلة السابقة يعتمد على مبدأ المفتاح الواحد لعملية التشفير وفك التشفير

تشفير المفتاح العام:

أو ما يعرف بالتشفير اللامتماثل (Cryptography Asymmetric)تم تطوير هذا النظام في السبعينات في بريطانيا وكان استخدامه حكراً على قطاعات معينة من الحكومة ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاصPrivet key ، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. المفتاح العام يرسل لجميع الناس أما المفتاح الخاص فيحتفظ به صاحبه ولا يرسله لأحد. فمن يحتاج أن يرسل لك رسالة مشفرة فإنه يستخدم المفتاح العام لتشفيرها ومن ثم تقوم باستقبالها وفك تشفيرها بمفتاحك الخاص

شكل عمل التشفير بالمفتاح العام والمفتاح الخاص (4-4)



- بعض الأمثلة على أنظمة تشفير المفتاح العام:

PGP, DSA, Deffie-Hellman, Elgamal, RSA

جميع هذه الأنظمة تعتمد على مبدأ التشفير اللاتماثلي أو التشفير باستخدام المفتاح العام والمفتاح الخاص

مزايا وعيوب التشفير التقليدي والتشفير باستخدام المفتاح العام:

التشفير التقليدي أسرع بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه يستخدم مفتاح واحد فقط. فهو عرضة أكثر للاختراقات. أما تشفير المفتاح العام فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة للاختراقات، ولكنه أبطأ من التشفير

التقليدي.

ونتيجة لهذه المزايا والعيوب أصبحت الأنظمة الحديثة تستخدم كلا الطريقتين حيث أنها تستخدم الطريقة التقليدية للتشفير وأما تبادل المفتاح السري الواحد بين الأطراف المتراسلة تتم من خلال استخدام طريقة تشفير المفتاح العام

قياس قوة التشفير:

التشفير قد يكون قوياً أو ضعيفاً، حيث أن مقياس القوة للتشفير هو الوقت والمصادر المتطلبة لعملية كشف النصوص غير مشفرة من النصوص المشفرة. نتيجة التشفير القوي هو نص مشفر يصعب كشفه مع الوقت أو توفر الأدوات اللازمة لذلك.

التوقيعات الرقمية Digital Signatures

وهى تكمن فى قيمة التشفير إلحاقها بالبيانات المستخدمة للتحقق من مصدر البيانات وسلامتها

مثال على ذلك

Aيرغب فى التوقيع على رساله m بعد ذلك يرغب فى إرسالها الى e

$A \rightarrow B: \quad M, \{M\}_{KApriv}$

Eيستطيع التحقق من a ثم بعد ذلك ترسل m للتحقق من الوجود

$\{\{M\}_{KApriv}\}_{KApub} = M$

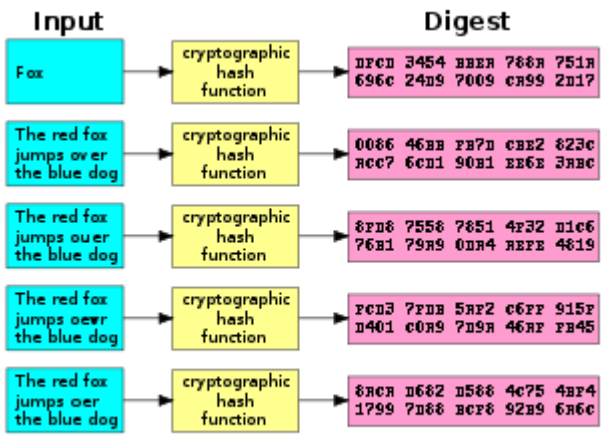
دالات التجزئه Hash Functions

تعريف المصطلح

دالة تحول سلسلة نصية من وحدات البت ذات الطول غير المحدد إلى سلسلة محددة الطول من وحدات البت تتميز دالة الاختزال الصادر بشأنها موافقة بالمواصفات التالية:

(وحيدة الاتجاه) بمعنى أنه من غير المُمكن حسابياً يتحول مدخل إلى مخرج محدد سلفاً

(مقاومة للتعارُض) بمعنى أنه من غير الممكن حسابياً أن يتحول مدخلان مختلفان إلى نفس المخرج .دالة حسابية صادر بشأنها موافقة تقوم بتحويل سلسلة نصية ذات طول غير محدد إلى سلسلة نصية محددة الطول. يمكن استخدامها لإنتاج مجموع تدقيقي يُسمّى بـ "قيمة الاختزال" أو"موجز الرسالة" لسلسلة نصية أو رسالة طويلة.



وظيفة تجزئة تشفير مثالية بالخصائص الأربعة الرئيسية أو كبيرة

ومن السهل حساب قيمة التجزئة لأي رسالة معينة بسبب

فإنه لا يصلح للعثور على الرسالة التي تحتوي على مزيج معين
وغير عملي التعديل على رسالة دون تغيير التجزئة
وغير عملي للعثور على رسالتين مختلفتين مع نفس التجزئة

إنشاء التواقيع الرقمية Generating Digital Signatures

والتوقيع الرقمي أو مخطط التوقيع الرقمي هو نظم رياضية لإثبات صحة رسالة أو وثيقة رقمية , والقيام بعمل توقيع رقمي صالح يعطي سببا للاعتقاد المتلقي أنه تم إنشاء الرسالة من قبل المرسل "معروف ",ويشيع استخدام التوقيعات الرقمية لتوزيع البرامج والمعاملات المالية ، وفي حالات أخرى ، حيث من المهم للكشف عن التزوير والتلاعب .

وغالبا ما تستخدم التوقيعات الرقمية لتنفيذ التوقيعات الالكترونية ، وتوسيع النطاق يشير إلى أي البيانات الإلكترونية التي تحمل نية للتوقيع ، والتوقيعات الالكترونيه ولكن ليس كل المواقع الالكترونية تستخدم التوقيعات الرقمية وفي بعض البلدان ، بما في ذلك الولايات المتحدة ، والهند ، وأعضاء في الاتحاد الأوروبي ، والتوقيعات الالكترونية وأهميتها القانونية .ومع ذلك ، القوانين المتعلقة بالتوقيعات الالكترونية لا تجعل من الواضح دائما ما إذا كانت التواقيع الرقمية للتشفير ، ملزمه ام لا .

التوقيعات الرقمية تستخدم نوع من الترميز غير المتناظر .للحصول على الرسائل المرسلة من خلال قناة غير آمنة ، وتنفذ بشكل صحيح يعطي التوقيع الرقمي سبب للاعتقاد بأن المتلقي عند إرسال الرسالة من قبل المرسل المطالب بها .التوقيعات الرقمية وتعادل التوقيعات الخطية التقليدية في كثير من النواحي

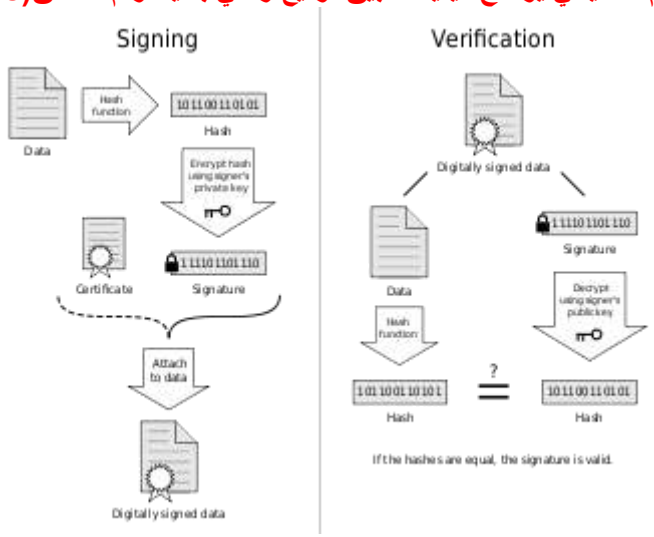
جانبا: الوضع القانوني Aside: Legal Status

التواقيع الرقمية ملزمة قانونا

الشهادة الرقمية Digital Certificate

- تتألف من البيانات والتوقيع على البيانات
- بناء جمل للشهادات

رسم تخطيطي يوضح كيفية تطبيق توقيع رقمي بسيط وثم التحقق(5-4)



إبطال شهادة Certificate Revocation

- شهادات لها من العمر من 10 الى 20 سنه
- قد تصبح الشهاده بعد إبطالها ليس لها اى قيمه وتفقد معناها
- الحاجة إلى إلغاء الشهادة
- شهادة إلغاء قوائم باستخدامLDAP

مقارنة التشفير المتماثل وغير المتماثل Comparing Symmetric and Assymetric Cryptography

التشفير بالمفتاح العمومي Public key cryptography

- مكثفة حسابيا
- تتطلب مفاتيح طويلة جدا ، ومثال على ذلك ، 2048 بت
- المفتاح الخاص يحتاج فقط إلى أن تكون أكثر سرية
- المفاتيح قد تبقى صالحة لفترات طويلة من الوقت

تشفير مفتاح متماثلSymmetric key cryptography

- فعالة حسابيا
- مفاتيح أقصر، مثلاً، 128 بت
- تشفير المفتاح العمومي المستخدم لإنشاء مفتاح جلسة العمل Public key cryptography used to establish session key
- تشفير مفتاح متماثل مستخدم لتبادل البيانات الفعلية

التطبيق : تجارة الويب Application: Web Commerce

- المشكله : رغبات العملاء للتفاعل مع خادم الويب لوضع معرفه حاله النظام
- احتياجات العملاء لمعرفة هوية الخادم
- رقم بطاقة الائتمان للعملاء وما إلى ذلك، يجب أن تبقى سرية
- يجب أن تحال رقم بطاقة الائتمان بشكل صحيح

متطلبات تجارة الويب Web Commerce Requirements

- معرفة برقم بطاقة الائتمان وتاريخ انتهاء الصلاحية، ويرتبط بها اسم/عنوان ما يكفي لمصادقة المستهلك
- عدم التنصل ليس شرطا للأوامر على الانترنت

طبقة المقابس الآمنة Secure Sockets Layer

مقدمة :

نظرا لكون بيئة الشبكة العنكبوتية " الانترنت " بيئة مفتوحة للجميع ، فمن خلال تناقل البيانات عبر آلاف الشبكات والتي تعمل على شكل الوسيط بين المرسل والمستقبل لتلك البيانات ، فإن سرية البيانات المنقولة مهددة بالاختراق أو الاستيلاء .
ومع اختلاف أهمية تلك البيانات المرسلة ، فجميعا نتفق على أهمية الحفاظ على سرية البيانات الحكومية والاقتصادية وحتى البيانات الشخصية والسماح بالاستيلاء عليها يعتبر تهديدا بصورة أو بأخرى وعلى ذلك فوجود خدمة SSL والتي تعمل على تشفير البيانات المرسلة عبر الانترنت والعمل على نقلها بصورة مشفرة يساعد على منع أي استيلاء يحصل في مرحلة نقل البيانات.
بدأت فكرة SSL من قبل شركة نتسكيب والتي عملت على تقديم تلك التقنية في تشفير البيانات المنقولة عبر الانترنت باستخدام (cryptography) والتي تستخدم مفتاحين للقيام بعملية التشفير إحداهما معروف مسبقا والآخر لا يعرفه سوى المرسل والمستقبل فقط ، وبالإمكان معرفة المواقع التي تقدم خدمة التشفير من عدمها من خلال جعل رابط الموقع يبدأ https:// بدلا من http:// ، كما هو المعتاد في غالب المواقع .

ماهو الـ SSL ؟

هو عبارة عن اختصار لكلمة " secure socket Layer " بروتوكول يقوم بتشفير البيانات المنتقلة من وإلى متصفح الانترنت و الخادم "server" باستخدام مفتاحين للقيام بعملية التشفير ، المفتاح الأول وهو مفتاح عام " public key" يقوم المفتاح الأول بتشفير العملية "http transaction" ، ويقوم المفتاح الثاني وهو مفتاح خاص "private key"

لماذا الـ SSL ؟

إن ثقة مواقع التجارة الالكترونية و مواقع الحكومات ومواقع البنوك في SSL لم يكن عبثا أو مصادفة ، إنما هي بسبب واقع تفرضه طبيعة شبكات الانترنت وقوة مميزة تقدمها SSL في عملية نقل البيانات بشكل آمن وما يمنح الـ SSL كل هذه المميزات للأسباب التالية :
- طبيعة شبكة الانترنت غير الآمنة : كما نعلم حتى يصل طلب من متصفح الانترنت لدى العميل إلى موقع الانترنت المطلوب ، يمر هذا الطلب على عدد من الشبكات المتصلة لإيصال ذلك الطلب ، ولأننا لا نعلم عن طبيعة تلك الشبكات الموصلة ومدى حجم الأمان التي تقدمه أو الحفاظ

على سرية البيانات ،مع استحالة التأكد من أمان تلك الشبكات بشكل كامل مع معرفتنا المسبقة بأن الطلب ربما يتغير من مسار إلى مسار آخر في شبكة الانترنت ، يجعل من أن طريقة تشفير البيانات طريقة آمنة ومنطقية وسهلة الاستخدام أيضا.
- استحالة تغيير البيانات : كما نعلم أن من أسس أمن المعلومات هو وصول البيانات بشكل صحيح دون تغيير ،فعند حصول الاختراق بالإمكان تغيير محتوى الطلب بدلا من 100 على سبيل المثال إلى 100000 ، من خلال عملية التشفير تمنع المخترق من تغيير البيانات بسبب تشفيرها واستحالة فك ذلك التشفير بسبب وجود طريقة التشفير الصعبة .
- استحالة قراءة البيانات : مع عملية التشفير للبيانات عبر الـSSL يمنع أي متسمّع للبيانات من قراءة بيانات حقيقية ، إنما كل ما يستطيع قراءته هي بيانات مشفرة ، لا يستطيع فكها مطلقا.

كيف يعمل الـ SSL ؟

طبيعة بروتوكول SSL تعمل على الطبقة السفلى من التشفير لتدعم بروتوكولات الطبقة العليا مثل بروتوكول نقل البيانات "FTP"، بروتوكول تصفح الانترنت"HTTP" و بروتوكول الأخبار عبرالشبكة "NNTP" .
كما ذكرنا آنفا أن بروتوكول الـ SSL يعمل على تشفير البيانات وحتى تتم عملية التأكد من الخادم من قبل المتصفح ، وللقيام بذلك يتم إنشاء مفاتيح التشفير "العام والخاص" ، وتمم هذه العملية من خلال عدة خطوات حتى يتم التأكد من موثوقية الطرف الآخر ويتم إنشاء المفاتيح أيضا

،وتلك الخطوات هي :

- يقوم المتصفح بطلب شهادة الوثوق من الخادم.

* يقوم الخادم بالرد على المتصفح ويقوم بإرفاق شهادة الوثوق عبر الرد.

* إرسال المفتاح الخاص للتأكد من امتلاك الخادم له.

* إعادة تأكيد من الخادم على امتلاك المفتاح الخاص .

*إرسال الطلب الرئيسي من قبل العميل.

*رد الخادم على الطلب.

أنواع الـ SSL ؟

يوجد نوعان من SSL اعتمادا على قوة التشفير ، وهو يعبر عن طول مفتاح التشفير :

- 128 بت.
- 40 – 56 بت.

نستطيع أن نقول أن اختيار النوع الأول هو الخيار الأفضل والآمان ، فمن خلال مقارنة بسيطة بين النوعين نجد أن النوع الأول يتفوق على النوع الثاني مقارنة بوقت البحث برقم خرافي " تريلون تريلون مرة " ، وبالتأكيد من خلال هذا الرقم نعرف أن محاولة البحث التي تحصل لفك التشفير باستخدام 128 بت نجزم أنها مستحيلة.

كيفية اقتناء خدمة SSL ؟

كما نعلم بأن خدمة SSL هي اتصال بين العميل والخادم والتأكد من شهادة الوثوق من خلال مقدم خدمة SSL وهو الوسيط الثالث للخدمة وحتى تتم عملية توفير تلك الخدمة ، يجب أن يقوم الخادم بتنفيذ بعض الإعدادات ، وتختلف تلك الإعدادات باختلاف بيئة العمل ما إن كانت ويندوز أو لينكس .
عند الاشتراك في خدمة SSL لدى مقدمة الخدمة ، من الواجب توفير معلومات الخدمة والتي عادة ما تكون على الهيئة التالية :

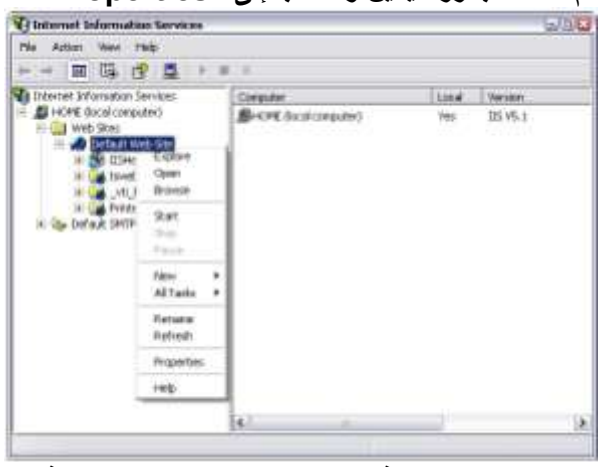
```
-----BEGIN CERTIFICATE-----
[encoded data]
-----END CERTIFICATE-----
```

هذه المعلومات تعبر عن مفتاح الاتصال بالوسيط للتعريف بالخادم ، بعد ذلك يقوم الخادم بتركيب خدمة الـ SSL على الخادم على حسب بيئة نظام التشغيل .
للقيام بعملية التركيب على بيئة ويندوز ، يجب اتباع الخطوات التالية :

التركيب على بيئة نوافذ "Windows":

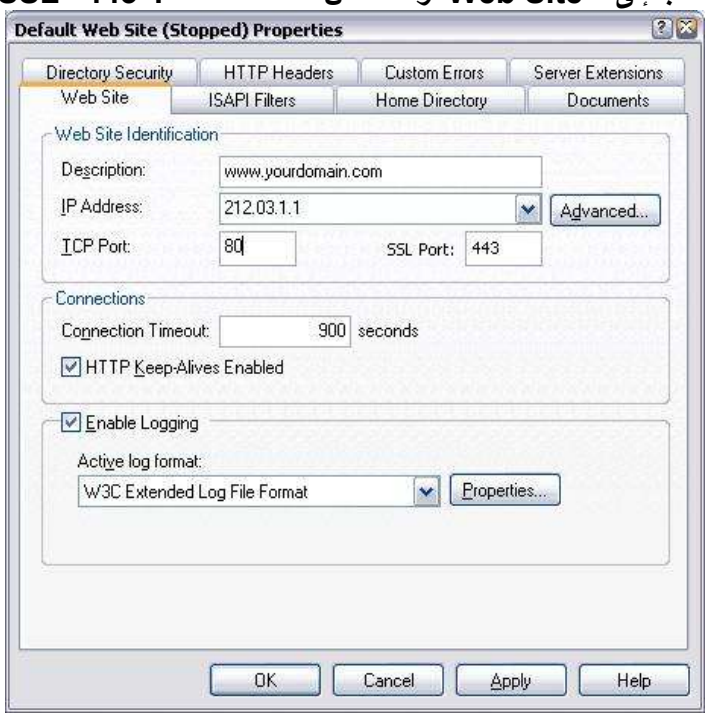
- بداية يجب توفر IIS على نظام التشغيل.
- اذهب إلى "Control Panel" ، "Administrator Tools" ، "Internet Information Services" .

- اذهب إلى "Default Web Site" ثم الضغط بالزر اليمين والذهاب إلى "Properties".



اذهب إلى "Directory security" ثم "Server Certificate" ثم اتمام اعدادات ال.SSL

اذهب إلى "Web Site" والتأكد من اضافة منفذ الـ "443". SSL



التركيب على بيئة لينكس :

-قم بالبحث عن إعدادات الاباتشي "Apache" من خلال الملف"/etc/httpd/httpd.conf" :

-قم باضافة النص التالي في ملف اعدادات الاباتشي :

```
DocumentRoot /path/to/website
SSLEngine on
SSLCertificateFile /path/to/www.virtualdomain.com.crt
SSLCertificateKeyFile /path/to/www.virtualdomain.com.de.key
```

-مع العلم بأن xxx.xxx.xxx.xxx هو IP Addressللموقع .

-في رغبة عدم حصول مشاكل بعد إعادة تشغيل الخادم قم بالعمليات التالية :

```
$ openssl rsa -in www.virtualdomain.com.key
–out www.virtualdomain.com.de.key
```

-أخيرا قم بإعادة تشغيل خدمة Httpd :

```
# /etc/init.d/httpd stop
# /etc/init.d/httpd start
```

التأكد من امتلاك SSL ؟

لا شك بأنه يجب على العميل عند الدخول إلى مواقع البنوك أو مواقع التجارة الالكترونية التحقق من امتلاك تلك المواقع خدمة SSL والتأكد من فعاليتها ومصدر تلك الرخصة ، هناك طريقتين لعملية التأكد :

- يظهر في متصفح الانترنت للعميل صورة قفل صغيرة مجاورة لها مقدار التشفير عادة ، 128bit .
- في عنوان الموقع يظهر العنوان مبتدئا بـ Https بدلا عن Http كما هو معتاد .
- تستطيع التأكد من خلال الضغط بالزر اليمين على الصفحة ثم الذهاب إلى خصائص.

عيوب الـ SSL ؟

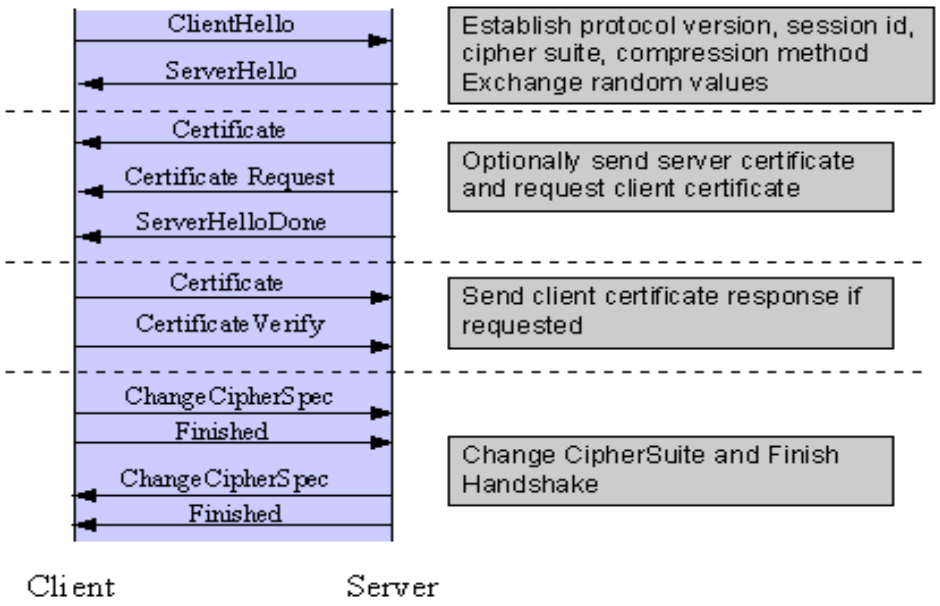
يكاد حجم فائدة الـ SSL ومميزاته لا توصف في إيجادها لحلول فعلية لمشاكل أمن المعلومات في نقل البيانات من العميل والخادم ، ولكن نتفق أن لكل تقنية مميزات وعيوب ، ونذكر هنا أكبر عيوب الـ SSL :

-تحتاج عملية التأكد من شهادة الوثوق والقيام بعملية فك التشفير في كل طلب ، يقوم بعمل ضغط على CPUمما يسبب من ارتفاع حجم الاستهلاك "LOAD"على الخادم ، كما القيام بعملية أخذ نسخة من المفاتيح والاحتفاظ فيها في كل مرة يستهلك أيضا الذاكرة العشوائية بشكل كبير.

-كما ذكرنا آنفا بأن SSLيقوم بدعم HTTP,FTP,NNTP، ومع اختلاف طرق التصفح للانترنت في الوقت الحاضر ومع تعدد الخدمات المقدمة من الانترنت في كل مرة ، يحد من الاستفادة من الـ SSLخارج نطاق البروتوكولات السابقة.

شكل يوضح تهيئه ssl(4-6)

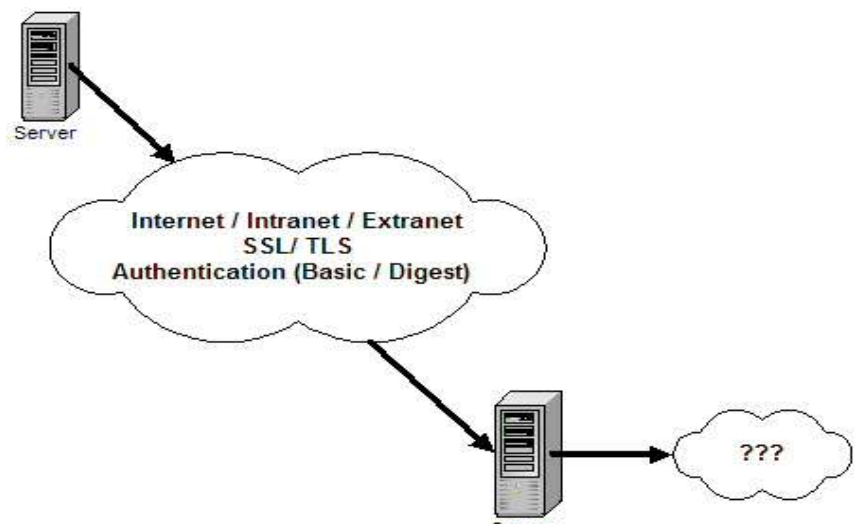
-بسبب الحاجة للقيام والتأكد ، فإن هيكلية الصغيرة مثل الأجهزة لا تحتمل القيام بتلك مستمر



بعملية فك التشفير وطاقة الأجهزة الكفية أو الجوالات العمليات بشكل

. تهيئة SSL

نقل البيانات عبر SSL/TLS(4-7)



حزم التشفير

حزم الشفرات ، التي يشار إليها أحيانا **Cipher Suite** ، هو مزيج من اسم والتوثيق ، والتشفير ، ورسالة رمز التوثيق والخوارزميات المستخدمة للتفاوض على إعدادات الأمان لاتصال الشبكة باستخدام طبقة النقل الامن (tls) أو طبقة المقابس الآمنة ويتم تعريف الهيكل واستخدام الشفرات مفهوم حزم الوثائق التي تحدد بروتوكول RFC 5246القياسية للنسخة 1.2 tlsوترد إشارة حزم الشفرات اسمه في المضيقين 2434 ، والصفرTlsحزم التسجيل.

أمثلة عن الخوارزميات المستخدمة

key exchange
RSA, Diffie-Hellman, ECDH, SRP, PSK
authentication
RSA, DSA, ECDSA
bulk ciphers
RC4, Triple DES, AES, IDEA, DE

المصادقة المقايضات

الأكثر أمانا المفتاح الاولى

- أكثر الاستخدامات إستخدام http
- لايوجد امان كافى
- معتدل الأمن

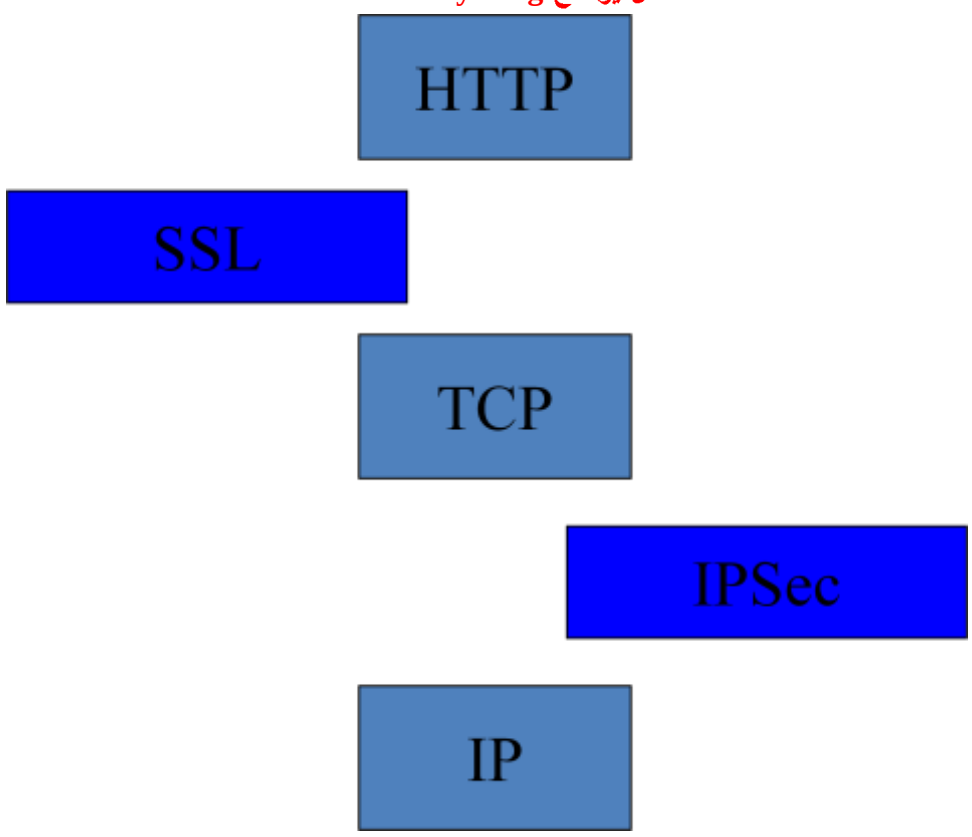
- لا توفر السرية
- إلى حد ما ضعيفة

أمان طبقة النقل Transport Layer Security

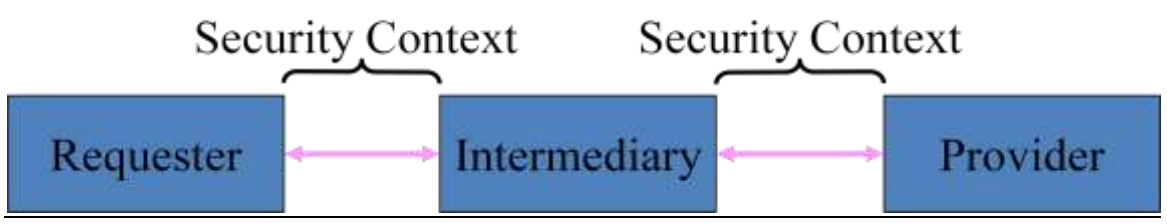
- IPSec

- تدعم وسائط النقل
- تكون فى مستوى الشبكه وشفافه بالنسبه للتطبيقات
- مفيدة لإنشاء الشبكات الافتراضية الخاصة
- من السهل عمل آلية لتوفير قناة آمنة بين اثنين من الشركاء التجاريين

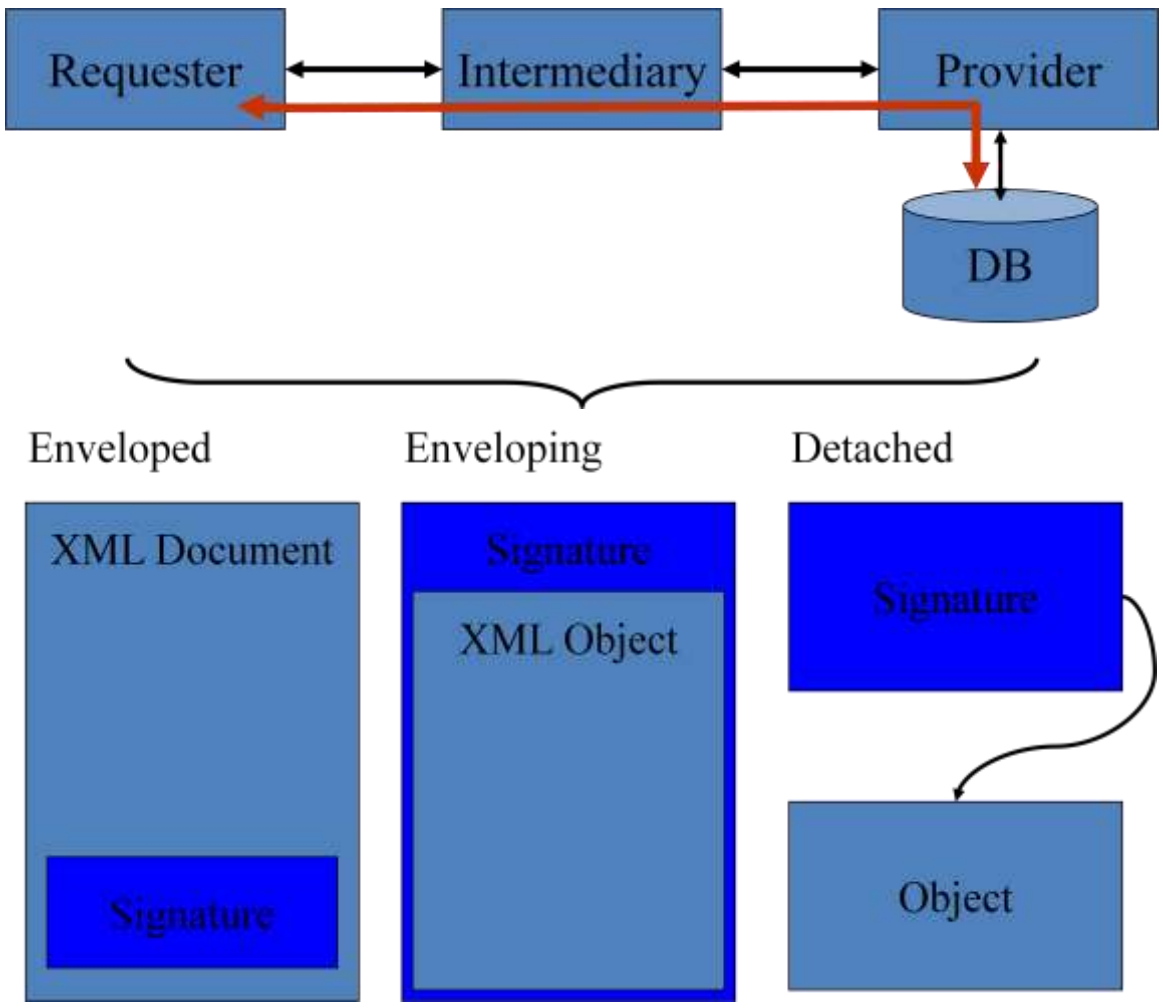
شكل يوضح **Protocol Layering**



شكل يوضح **Transport-Based Security**



Message-Based Security



XML Signature Structure بنية توقيع XML

```
<Signature ID?>
   <SignedInfo>
      <CanonicalizationMethod/>
      <SignatureMethod/>
      (<Reference URI? >
          (<Transforms>)?
          <DigestMethod>
         <DigestValue>
      </Reference>)+
   </SignedInfo>
   <SignatureValue>
   (<KeyInfo>)?
</Signature>
```

```
<ds:Signature
  xmlns:ds="http://www.w3.org/2000/09/xml
  dsig#">
   <ds:SignedInfo>
      <ds:CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/200
        1/REC-xml-c14n-20010315"/>
      <ds:SignatureMethod
        Algorithm="http://www.w3.org/2000/0
        9/xmldsig#dsa-sha1"/>
      <ds:Reference URI="#Body">
         <ds:DigestMethod
           Algorithm="http://www.w3.org/200
           0/09/xmldsig#sha1"/>
         <ds:DigestValue>2jmj7l5rSw0yVb/vlW
           AYkK/YBwk=</ds:DigestValue>
      </ds:Reference>
   </ds:SignedInfo>
```

- مشاكل xml
- التوافق Canonicalization

مثل المسافات تباعد ، وما إلى ذلك ، والمسائل عند توقيع / تشفير

- التحويلاتTransforms

- شكل التشفير فى xml(XML Encryption Format)

```
<EncryptedData Id? Type? MimeType? Encoding?>
   <EncryptionMethod/>?
   <ds:KeyInfo>
      <ds:KeyName>?
      <ds:RetrievalMethod>?
   </ds:KeyInfo>?
   <CipherData>
      <CipherValue>?
      <CipherReference URI?>?
   </CipherData>
   <EncryptionProperties>?
</EncryptedData>
```

- **خدمات ويب Web Services**

نموذج خدمات الإنترنت مبنية على

- **SOAP/XML Protocol**
- **WSDL**
- **UDDI**

تامين soap

- **SOAP رسائل يمكن إرسالها باستخدام SSL/TLS**
- **مصادقة باستخدام PKI المستندة إلى SSL (شهادات العميل والخادم)**

WS-Security

تم تطويرها من قبل شركات IBM, Microsoft, and Verisign

خدمات الأمن امتدادات مرنة وميزة غنية لتطبيق الأمن خدمات الويب .

يتم أستخدام تواقيع xml وايضا يتم أستخدام تشفير xml

بروتوكول يحدد كيف يمكن فرض التكامل والسرية على الرسائل ويسمح للاتصالات من مختلف الأشكال الأمنية رمزية ، مثل SAML ، Kerberos، و X.509.

الأمن يصف ثلاث آليات رئيسية

- **كيفية تسجيل رسائل soap لضمان سلامتها**
- **كيفية تشفير الرسائل soap لضمان السرية**
- **كيف نعلق على الرموز الأمنية**

مواصفات يسمح لمجموعة متنوعة من الأشكال التواقيع وخوارزميات التشفير ومجالات الثقة متعددة ، ومفتوحة لمختلف نماذج رمزية متعلقه بالأمن مثل

- **X.509 User Names (and Passwords)**
- **Binary Security Tokens (X.509 Certificates and Kerberos Tickets)**

UDDI Security Features

وهو أختصار لكلمه Universal Description, Discovery and Integration

- **اكتشاف وتكامل الأعمال التجارية لصفحة ويب**
- **UDDI V3.0 يسمح لكيانات UDDI أن يتم التوقيع**
- **المطالبون يمكن إلا أن ننظر للبيانات وقعت**
- **يمكن للناشرين حماية ضد المحتالين**
- **قد يضمن تأمين الوصول إلى خدمة UDDI SSL**

الجدار النارى فى xml

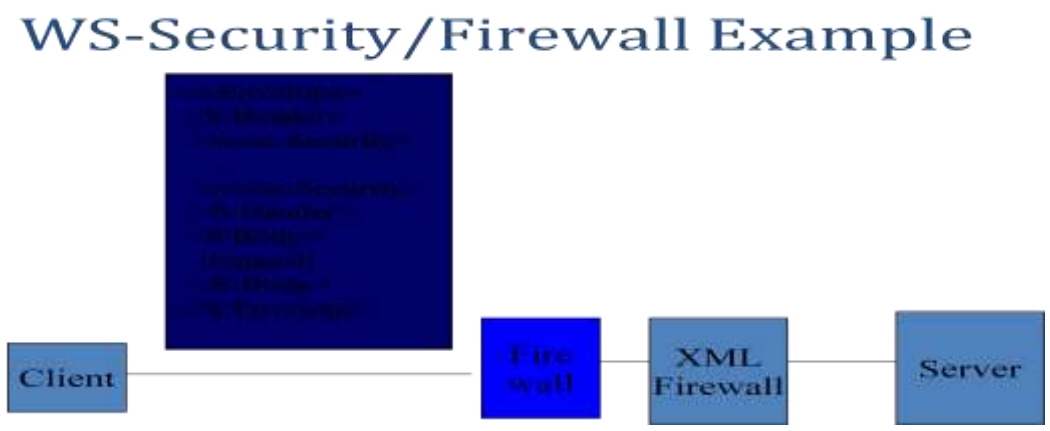
هى جدارن الحماية المتخصصة المستخدمة لتوفير الأمن xml الرسائل مثل خدمات ويب

وتكون مفصولة من النظم الحاسوبية الداخلية

جدران الحماية التقليدية تقوم بفحص البيانات على مستوى الحزم

جدران الحماية XML فحص البيانات على مستوى رسالة XML

تتم عمليات المعالجة المصادقة تلقائيا



اختصارات أخرى

XKMS

- وهى أختصار لكلمه XML Key Management Specification
- توفر البروتوكولات التي تستند إلى XML لتوزيع وتسجيل المفاتيح العامه، وتمكين عملاء
- X-KISS: البروتوكول المتعلق بمعالجة المعلومات الرئيسية XML seg
- X-KRSS: البروتوكول الخاص بتسجيل معلومات المفتاح العام

SAML

- وهى أختصار لكلمه Security Assertions Markup Language

ويوفر أليه للمطالبات الترميز في ملف XML وتمرير هذه جنبا إلى جنب
أوراق بيانات المصادقة لتمريرها

إدراة المخاطر فى التجارة الالكترونيه

تحديد المخاطر فى التجارة الالكترونيه Identifying risks in e-commerce

- التهديات التى توجه للبنيه التحتيه لتكنولوجيا المعلومات على سبيل المثال الحرائق والفيضانات
- تهديات البيانات ونذكر منها التهديات التى يتعرض لها البرنامج "الموقع",قواعد البيانات,الفيروسات ,أحصنه طرواده
- أخطاء من قبل الموظفين على سبيل المثال النقر فوق الارتباطات الموجوده فوق الرسائل الوارده على مواقع الشبكات ربما تكون هذه الارتباطات ضارة او حذف البيانات عن طريق الخطأ من قبل المتسخدمين
- خطأ تقنى على سبيل المثال عيوب فى البرمجيات
- فشل البنيه التحتيه على سبيل المثال تعطل server
- بطاقات الائتمان والتحايل على هذه البطاقات عن طريق الغش
- الهجمات الضارة من داخل أو خارج العمل الخاص بك.
- يعتبر هاكر أجهزة الكمبيوتر من اخطر مايواجه أمن التجارة الالكترونيه بما يتمتعون من خبرة وذكاء فى إستغلال الثغرات حيث لاتوجد حمايه كامله

تهديدات نظم التجارة الالكترونيه

- الحرص على معلومات الشركات والملكية الفكرية من الموظفين داخل المنظمة وشركائها التجاريين ومن الصعب مراقبة كيف سيتم معالجة المعلومات الحساسة بواسطة الأطراف الثلاثة أو العمال المتعاقدين عدد قليل من المنظمات بالأنظمة المعمول بها لضمان معايير مشتركة في فحص الموظفين وتوفير آليات الأمن بين الشركاء التجاريين

- استغلال القراصنة أخطاء في تصميم تطبيقات البرمجيات، والتنفيذ التقني أو أنظمة التشغيل وعلاوة على ذلك، نقاط الضعف في آليات الأمن التقنية وأصبح الان من السهل قراءه كتب على الانترنت ثم بعد ذلك محاوله الاختراق او التدريب على ماقرأ.
- يمكن تشويه صورة الموقع وذلك من خلال اذا تم غير اى محتوى من الموقع يؤدي إلى الإحراج التجارى والأضرار التي تلحق بالموقع وبالتالى ماهى الطريقه التى يظهر بها سواء أمام شركاء الموقع او المتعاملين التجاريين.
- هجمات الحرمان الخدمة التي تستخدم فيض كبير من الوسائل الخاطئة التى تؤدى الى تعطل الاعمال التجاريه يمكن أن يكون له تأثير مدمر على الأعمال التجارية، خاصة إذا كانت تعتمد على نظام التجارة الإلكترونية يعني أن هناك فرصاً أوسع لشن مثل هذا هجوم، بمعنى أن هناك خطرا في المقابل أقل من التعقب ويتزايد استخدام القراصنة botnets-وهى مجموعة من أجهزة الكمبيوتر المصابة مع البرامج الضارة والتحكم فيها عن بعد و تعمل وهذه الهجمات على بطئ السيرفر

ما لم يتم اتخاذ إجراءات سريعة ، فإن أي مشاكل تواجهك مع موقعك التجارى الإلكترونى سيكون ذلك واضحا على الفور إلى العالم وبالتالى الى الزبائن "عملاء" التجارة الإلكترونية والعملاء يكون إخلاصهم قليل الى حد ما واذا دعى الامر ذلك فإنهم سوف يذهبوا الى موقع اخر وبالإضافة نظير لما حدث لموقعك ،اذا أصاب الموقع بعطل فني يمكن أن يكون لها أيضا تأثير كبير على الشركاء التجاريين الرئيسيين.

ولذلك فمن المهم أن تتخذ الخطوات اللازمة لمنع حدوث مشاكل ، بمعنى حل المشكله قبل وقوعها "التنبؤ بالمشكله "

الاتجاهات الاخيرة

وتستخدم هذه الطريقة الخبيثة أستخدام الفيروسات والديدان وأحصنة طروادة وبرامج التجسس قد تغيرت أيضا العدوى عادة ما تكون الخطوة الأولى تهدف إلى سرقة البيانات السرية أو فتح ثغرات بعد ذلك يستغلها القراصنه.

كيفيه حمايه أعمالك من الفيروسات

- شراء أحد برامج الانتى فيرس وجعلها محدث بشكل يومى
- اذا كان لديك برنامج مكافح فيروسات تخلص من المرفقات الموجوده لديك فى البريد الالكترونى وفحصها جيداً اذا كان سليمه "غير ضارة او العكس اذا كانت ضارة تخلص من منها
- قم بتحديد ماهى المسارات التى يمكن أن تتخذها الفيروسات "اماكن وجودها"
- قم بالتركيز جيداً اذا كنت قد تحدثت مع أحد الاشخاص ثم بعد ذلك تأثر جهازك راقب ذلك

تقييم المخاطر

ويشمل تقيم المخاطر الاتى

يمكن أن يتم إجراء تقييم المخاطر بالتوصل إلى فهم واضح للمخاطر التي تواجه نظام التجارة الإلكترونية وعمليات الأعمال المرتبطة بها، والأثر المحتمل إذا ثار خلاف حول حادث أمني وكان جزءا رئيسيا من تقييم للمخاطر وهو تحديد شروط الوصول إلى المعلومات للأعمال التجارية وستشمل هذه القواعد للوصول لفئات المخول لهم الإطلاع على المعلومات

تأمين أنظمة التجارة الإلكترونية الخاصة بك

قيمة تنفيذ سياسة الأمن

يجب تحديد سياسة الأمن أيضا خطط الإنعاش لنظام للتجارة الإلكترونية في حال وقوع هجوم على النظام أو الكوارث المادية وهذا ينبغي أن تشكل جزءا من خطط الطوارئ للأعمال التجارية الخاصة بك

ISO/IEC 27001

ISO/IEC 27001 يوفر أساسا سليما للتنمية السياسة الأمنية. هذا معيار بريطاني لإدارة المخاطر لأصول المعلومات واعتمد فيما بعد بالمعايير الدولية كما ISO 17799

الفائدة الرئيسية اعتماد المنظمة ISO/IEC 27001 هو قبول الحاجة إلى حماية أصول المعلومات للأعمال التجارية وبيان بالتدابير اللازمة لتلبية هذه الحاجة. إذا كانت بشكل صحيح يتم تطبيق الضوابط المحددة في المعايير واتباعها، ثم اذا كان هناك خطر على المعلومات الخاصة بك سوف يؤدى ذلك تخفيض الخطر بشكل كبير

سياسة الاستخدام المقبول (المراقبة) Acceptable use policy (AUP)

كثيرا ما يتم تضمينها كجزء من سياسة الأمن لعمل تجاري،والمراقبة ووصف خطط العمل لتوعية موظفيها حول حماية أصولهم. ويتضمن أيضا شرحاً لكيفية تنفيذ التدابير الأمنية.

هذه السياسة يجب أن تكون مفصلة بما فيه الكفاية ليشمل ممارسات مثل "المدونات" واستخدام مواقع المراسلة والويب

مراجعة سياسة الأمن

وتشمل العوامل التي تعني ينبغي إعادة النظر في سياسة الأمن:

تغييرات النظام * استحداث أنظمة جديدة للمعدات والمستخدمين والأعمال * التغييرات في الشركاء التجاريين * الموظفين الذين يتركون الشركة

السياسة الأمنية Security policy

- ***ويحدد في هذا الاساس وجود سياسه او نهج يتفاعل معه كل القائمين على السياسيه الامنيه.***
- ***ويجب الالتزام بهذه السياسه وان تلتزم بيها الادارة.***
- ***يعطي وصفاً مختصراً للأمن و متطلبات السياسات، ومبادئ ومعايير الامتثال***

منظمة الأمن Security organization

ضوابط تحديد توزيع المسؤوليات الأمنية الفردية

*** يتناول الحاجة إلى المعرفة الأمنية المتخصصة.**

*** تتعلق بفي العلاقات نظم المعلومات مع الأطراف خارجية مثل الاستعانة بمصادر خارجية الشركات والشركاء والمقاولين.**

تصنيف الأصول والتحكم Asset classification and control

- **يتطلب تجميع قائمة جرد للموجودات لجميع نظم المعلومات.**
  تفاصيل الملكية ، والموقع وأهميته.
  تراخيص البرامج لجميع أنظمه التشغيل وبرامج التطبيقات الحالية

يحدد الفحص السليم والتحقق من تفاصيل الموظف في وقت التعاقد.

ينبغى تدريب المستخدمين على المسائل الأمنية.

أهمية الإبلاغ عن الحوادث الأمنية

الأمن المادي والبيئي Physical and environmental security

يسعى إلى تحديد عناصر تحكم الوصول المادي في المكان.

*** الضوابط المدرجة لحماية المعدات من المخاطر البيئية.**

*** يتطلب وجود مكاتب نظيفة.**

إدارة الاتصالات والعمليات

تسعى لإثبات ما إذا كانت ضوابط الشبكه المعمول بها يتم تنفيذها ام لا.

*** تتضمن عناصر نظام التخطيط والقبول.**

*** تتضمن إجراءات للتعامل مع وسائل الإعلام.**

مراقبة الدخول Access control

سياسه مراقبه الدخول تشمل.

*** تسعى الى كيفيه منح الصلاحيات .**

*** تهدف الى تحديد من لهم الحق فى تحديث معلومات قاعده البيانات.**

تطوير النظم وصيانتها Systems development and maintenance

**** تفاصيل الضوابط التي يمكن أن تساعد في بناء الأمن في النظم التي وضعت داخل المنظمة.***

**** الضوابط المدرجة على استخدام التشفير.***

**** يتم تناول شرط للسيطرة على التغيير***

إدارة استمرارية الأعمال Business continuity management

* وصف العمليات لضمان استمرارية الأعمال.
* تفاصيل الخطط التي تم وضعها للحفاظ على الاستمراريه أو استعادة العمليات التجارية.
* يوفر إطارا لتشكيل هذه الخطط.

الامتثال Compliance

* تضم عناصر تحديد الحاجة إلى الامتثال بالمعايير القانونية.
* تسعى لتحديد ما إذا كان هناك أمان.
* ويحدد إذا كانت النسخ الاحتياطية تم تنفيذها فعلا ام كانت فى وضع أختبار.

الضوابط الأمنية المشتركة للتجارة الإلكترونية Common e-commerce security controls

وينبغي إدخال ضوابط أمنية كافية للحد من المخاطر لنظم التجارة الإلكترونية ومع ذلك ينبغي إلا تكون عناصر التحكم هذه تقييدية حتى أنها تضر بأداء الموظفين.

مصادقة المستخدم User authentication

وهناك العديد من الأساليب التي يمكن التعرف والتحقق من أي شخص يسعى إلى الوصول إلى نظم التجارة الإلكترونية. وتشمل معرفه أسم مستخدم , كلمة المرور ، حيث يمكن لكلمة المرور أن تختلف في الطول وتشمل أرقام وأحرف وبالتالى يجب تغيير كلمات المرور الخاصة بالموظفين في فواصل زمنية منتظمة

العامل الثاني " المصادقة التي تتطلب شيئا للمستخدم (على سبيل المثال رمز المصادقة) وما يعرف المستخدم (على سبيل المثال رقم تعريف شخصي)

شهادة رقمية يمكن تصديقها عن طريق استخدام مفتاح توقيع فريد للفرد.

السمة المادية فريدة من نوعها للشخص المشار إليه كالتحقق من الهوية هذا يمكن أن تتراوح من إجراء فحص بصمات الأصابع أو من خلال الاعتراف بالشبكية أو عن طريق الوجه بالكامل .

مراقبه الدخول Access control

وهذا يحد الفئات المختلفة من المستخدمين ويتم تقسيمها الى مجموعات فرعية من المعلومات ويضمن من لهم الحق فى الوصول إلى البيانات والخدمات

تشفير البيانات Data encryption

تشفير تشفير البيانات، وتستخدم لحماية المعلومات التي تجري على جهاز كمبيوتر، عبر شبكة الاتصال. وتستخدم تقنيات مثل الشبكات الخاصة الظاهرية (VPN)

جدار الحماية Firewall

هذا هو جهاز الأمن أو برنامج يستخدم للقيام بعمل تصفية تمرير المعلومات بين الشبكات الداخلية والخارجية ويتم السيطرة عليها للوصول إلى شبكة الإنترنت من المستخدمين الداخليين، ومنع الأطراف خارجية من الوصول إلى الأنظمة والمعلومات على الشبكة الداخلية.

جدار حماية يمكن تطبيقها على مستوى الشبكة، لتوفير الحماية للعديد من محطات العمل أو الشبكات الداخلية، أو على المستوى الشخصي

كشف التسلل Intrusion detection

هذه المنتجات تقوم بمراقبة نشاط الشبكة والكشف عن اى محاوله تسلل إذا اشتبه نظام الكشف عن وجود اى هجوم، يمكن أن تولد إنذار، مثل تنبيه البريد إلكتروني على سبيل المثال

اختراق موقع هيئة السوق المالية

اخترق مخربون (هكرز) موقع هيئة السوق المالية على الانترنت مساء أمس الاول وألغوه بالكامل بعد أن أزالوا جميع ما فيه من بيانات ومعلومات، ليفاجأ متصفحوه بظهور عبارات انجليزية تفيد بخلو بيانات الموقع وأن خطأ حدث في الخادم (السيرفر) لكن الهيئة تلافت الموقف بتحديث الموقع واسترجاع محتوياته ظهر أمس الاثنين في ذات الوقت برأت مدينة الملك عبدالعزيز للعلوم والتقنية نفسها من تحمل أي أعباء تقنية وغير تقنية وقالت على لسان منسقها الاعلامي منصور العتيبي أن المدينة لا علاقة لها بمواقع الجهات والادارات وأن الجهة المخولة بالنواحي التنظيمية والرقابية وفرض العقوبات على المتسببين هي هيئة الاتصالات

وتقنية المعلومات.
وأشار العتيبي الى ان المسؤولية تظل في النهاية على الجهة صاحبة الموقع للزوم توفير وسائل حماية فائقة وحديثة.. وهي في نفس الوقت تملك كامل الأحقية في رفع مطالبة نظامية لهيئة الاتصالات والتي تقوم بدورها في معرفة المتسبب وفق الوسائل الأمنية المتوفرة ليتم عقبها معاقبة المتسبب (الهكر)

المراجع

http://www.itsyourmoney.ie/index.jsp?pID=662&nID=810
https://www.websteronline.com/about-webster/webster/safety-and-security/our-safety-and-security-commitment/ways-to-protect-yourself.html
http://www.commerce.gov.sa/ecomm/book.asp
http://www.access-ecom.info/article.cfm?id=45&xid=MN
http://www.syrianboy.net/club/t8476.html
http://www.alzaytouna.net/arabic/?c=201&a=112963
http://www.haaretz.com/print-edition/news/israel-ranks-fourth-in-the-world-in-scientific-activity-study-finds-1.4034
http://www.gspay.com/the-e-commerce-market.php
http://www.freeessays.cc/db/48/tvh54.shtml
http://www.snopes.com/fraud/atm/atmcamera.asp
/http://www.identity-theft-tips.com/protect-yourself-from-atm-fraud
http://www.webopedia.com/didyouknow/Computer_Science/2009/Card_skimming.asp
http://www.scribd.com/doc/2025995/Ecommerce-Fraud-Protection
http://www.allbusiness.com/sales/internet-e-commerce/440-1.html
http://www.ibm.com/developerworks/websphere/library/techarticles/0504_mckegney/0504_mckegney.html
http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1075385944&type=RESOURCES
http://www.windowsecurity.com/whitepapers/ECommerce_Security_Technologies_Fire_Wall.html
https://www.isaca.org/Pages/default.aspx
http://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems
–http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/57
cryptography-and-steganography-and-pki/622-cryptography.html
http://www.okaz.com.sa/okaz/osf/20060314/Con200603142432.htmtml
http://www.alriyadh.com/2008/10/11/article380091.html
http://www.time.com/time/digital/reports/ecommerce/25best.html
/http://www.ibm.com/developerworks/lotus/library/ls-SSL_basics
/http://www.verisign.com/ssl
http://library.thinkquest.org/27158/today.html
http://cyber.law.harvard.edu/ecommerce/encrypt.html