Security of E-commers

سینا حمزه نژاد
Hamzenejad@yahoo.com:

امید علی عسگری
Omidasgary@yahoo.com

چکیده:

این مقـاله می خواهد در مـورد اهمیت امنیت در E -commers صحبت کند و به طور کل بیان کند که امنیت چیست و به چه علت ضرورت دارد ، در کجا به کار می رود و تکنولوژی های آن چیست بنابراین چکیده این مطالب را می توان اینگونه نمایان ساخت که می خواهیم بدانیم اگر امنیت نباشد چه خواهد شد و دیگر اینکه با این پدیده مهم و ضروری چگونه باید برخورد کرد و عدم توجه به آن چه مشکلاتی را به همراه خواهد داشت.

کلمات کلیدی : E -commers ,internet,security

مقدمه :

همانطور که کاملامشخص است و دیده می شود E -commers محیطی بسیار بزرگ در اختیار داردکه از ایـــن محیط مشترک افراد مختلف استفاده می کنند در این محیط داد و ستد های بزرگ و کوچک انجام

می شود و ذات هر داد و ستدی این امر را با خود به همراه دارد که باید مراقب بود و از سرمایه خود حفاظت کرد حال این داد و ستد ها هر جا که باشد و در هر محیطی که انجام شود و با هرکس که انجام شود .

پس همانطور که گفته شد این رعایت این امر در تمام محیط ها باید رعایت شود بخصوص در محیـطهای بسیار بزرگی مانند E -commers بنابراین شناخت امنیت در چنین محیطهایی نه تنهـــا لازم ، بلکه واجـب است و باید آن را شناخت تا بتوان در زمـــان لازم و مکان مناسب از این پدیـــده اســـتفاده مناسب کرد و محیطی مسطح و بدون هیچ آلودگی پدید آورد .

با رعایت مطالب ذکر شده می توان در کارهای مربوط به هر محیطی و داد و ســـتدهای مربـــوط به آن موفقیت لازم را به دست آورد و با عث آسودگی خاطر می شود و در مقابل عدم رعایت آن برای هرکس و هرچیز نابودی و فنا را به همراه دارد .

بنابراین با توجه به مطالب ذکرشده باید و باید امنیت را به طور دقیق مورد بررسی قرار داد تا محیطی با امنیت بالا و ایجاد آسودگی خاطر فراهم آورد و روی هم رفته تجارتی بدون مشکل ودردسر داشت پس برای اینکه بتوان به این مهم دست یافت باید شناخت مختصری از محیط داشت و محیط مورد بحث ما در این مقاله محیط E -commers است . پس کار را با این سؤال شروع می کنیم .

E - commerce **چیست ؟**(www.obit-ecommerce.com)

برای اینکه بتوان در مورد امنیت در E –commerce بحث و بررسی کرد و آن را مورد مطالعه دقیق قرار داد ابتدا باید خود E -commerce را مورد یک بحث و بررسی مختصر قرار داد بنابراین اگربخواهیم یک تعـــریف ســـــاده و بدون خدشه ازاین واژه داشـــته باشیم می توانیم آن را بدین صورت بیان کنیم که

E- commerce نیز نوعی تجارت است متفاوت با بقیه تجارت ها (از نظر فیزیکی) که تفاوت آن در نوع ارتباط مشتریان و کمپانی هاست یعنی نوعی داد و ستدئ است ازطریق محیط الکترونیکی که به طور ساده می توان آنرا تجارت الکترونیک معرفی کرد این تجارت شامل پردازشهایی است که می توان این پردازشها را به صورت زیر دسته بندی کرد .

Commiunication-1

Transacting-2

Interasting-3

Reaserching-4

Organising-5

Managing-6

پس از اینکه پردازشهای ایـن محیط را مـورد بررسی قراردادیم و تا حـدودی با آن آشنا شدیم حال

می توان به طرز دقیق در مورد امنیت بحث کردپس این موضوع را نیز با ایـن سـوال شـروع مـی کنیم .

scurity **چیست** ؟

به طور ساده می توان این امر را بیان کرد که امنیت نوعی بیمه است . ایـن بیمـه از افـراد مختلـف نسبت به نوع کار آنها و مکان شغلی آنها و الویت کاری آنها از این افراد حمایـت مـی کنـد از ایـن بیمه که همان امنیت است دارای تکنولوژی های مختلف است که نسبت به ایـده آلهـای ذکـر شـده ایـن تکنولوژی ها متفـاوت هستند به عبارت دیگـر امنیـت در هـر محیطـی از روشـهای خـاص خـود که مناسب بـرای آن محـیط اسـت استفاده می کند پـس در محیطهـایی چـون E -commerce و اینترنت نیز سـیسـتمهای امنیتی خاص وجود دارد مثلا در اینترنت دارای تجهـیزات خـاص خـود است که با استفاده از حفاظت داده های اطلاعاتی این کار را انجام می دهند و همین طور در E -commerce ولـی بـرای اینکه بتوان امنیت را در این محیطها فـراهم کـرد بایـد ایـن سـوال را ازخود پرسید که خطر در کجاست ؟ بـرای پاسخ دادن به ایـن سؤال باید به این نکته توجـه کـرد در E -commerce این امر که به افـراد و مشـتریان اجازه داده می شود تا به اطلاعات مـورد نیـاز خود دستری داشته باشند خود یک ویژگی است . یعنی یک مشتری هرچه بتواند بـا دسترسـی بـه اطلاعات بیشتر خواسته های خود را فراهم کند راضی تر است ولی آیا می تـوان بـه هـر مشـتری این اجازه را داد که به هر جا که مد نظرش است دسترسی پیدا کند و آیا اگر ایـن امـر فـراهم

شود منطقی است ؟ حتما اینگونه نخواهد بود پس باید یک مرز برای این دسترسی فراهم کرد تا ازایجاد این خطر بزرگ جلوگیری کرد که اگر چنین نکرد باید مطمئن بود که محیطی که از این روش پیروی نمی کند یک محیط پر درد سر و مخاطره خواهد بود و سرانجام آن نابودی و فناست .

شناخت مردم و مشتریان نسبت به مسئولیت های خود و تکنولوژی ها و پردازش آنان

باتوجه به مطالب ذکر مطالب ذکر شده در قسمت قبلی این مورد به نظر می رسد که باید به مشتریان و کمپانی ها اطلاعات لازم در این مورد را داد و دانش آنان را در این مورد بالا آورد تا آنان با استفاده ازاین دانش بتوانند استفاده بهینه از این پدیده کنند و از سرمایه خود در مقابل حمله های نا خواسته محافظت کنند . مشتریان و کمپانی ها باید این امر را بدانند که برای دست یابی به این مهم باید و بایداز هیچ گونه مشکل و خطری چشم پوشی نکنند و ایجاد این امر مهم به عهده محیط است دیده شده که محیطهایی که از خطر ها چشم پوشی کرده ان سر انجام نابود و نیست شدند بسیاری از کمپانی ها برای رفع این مشکل دست به کار شدند ولی هنوز هم این مشکل به طور کامل حل نشده و در بعضی از مواقع دیده می شود که اطلاعات محرمانه مورد تعرض قرار می گیرند . برای مثال می توان به این مثال پرداخت که مثلا officer هایی را در این محیط به کار گرفتند وظیفه این officer ها این بود که با داشتن اطلاعات امنیتی خاص خود و با استفاده از مدیریت هوشمند خود از اطلاعات حفاظت می کردند .

بنابراین با توجه به مطالب ذکر شده در فوق این امر نماد پیدا می کند که برای اینکه کمپانی ها بتوانند در E -commerce موفق باشند باید دارای امنیت بالایی باشند و ایجاد این امنیت به عهده محیط است پس این امر زمانی تحقق پیدا می کند که اکثر کمپانی ها از سیستمهای fire wall قوی برخوردار باشند و با پیشرفت این سیستمها آنان نیز پیشرفت می کنند اولین سیستمهایی که در این رابطه به بازار آمدند ومورد استفاده نیز قرار گرفتند سیستمهای VPNs وPKL بودند ولی این روش ها هم راه حل کامل این مسئله نبودند ولی می توانستند تا حدی از چشم پوشی های بی مورد جلو گیری کنند پس باید راه حلهای بهتری طراحی می شد که بهترین راه حل ایجاد مامورین امنیتی بود .این مامورین دارای وظائف خاص خود بودند که در بلاکهای خاص خود قرار داشتند . طرز کار این مامورین به این صورت بود که با سر زدن به مشتریان خود می فهمیدند که کدام مشتدی احتیاج به حفاظت دارد و اگر احتیاج به این امر دارد در چه درجه ای است بنا براین با ابداع این روش باز هم تا حدی به ایده آل ها نزدیک ترشد ند ولی بازهم کافی نبود پس احتیاج به ابداع روشهایی با کارایی بیشتر هستیم .

password

این روش نیز برای کارایی بیشتر است تا بتوان از این محیط استفاده بهتری کرد . اکثر کمپانی ها و شرکت ها بر این مبنا کار می کنند و دارای رمزهای خاص خود هستند این رمزها باید ویژگیهای خاص خود را داشته با شند که این ویژگیها را به صورت زیر دسته بندی می کنیم

1- این رمزها باید بسیار قوی باشند و بتوانند از ورود بیگانگان جلوگیری کنند

2- این رمز ها را نتوان تقسیم کرد

3- این رمزها قابل تعویض به طور خودکار در فواصل معین باشند

بنابراین با استفاده از روشهای فوق که به طور مختصر در مورد آنها بحث شد می تولن به این نکته قابل توجه دستری یافت که اگر مردم دانش صحیح از استفاده این محیط داشته باشند و بتوانند پردازش صحیح در این محیط انجام دهند بنابراین خواهند دید که به محیطی با آرامش و بدون هیچ دست اندازی دستری یافته اند و این امر رضایت آنان را فراهم خواهد کرد واین احساس رضایت باعث رشد این محیط می شود پس به طورکل می توان به این نکته رسید که با فهم0صحیح End user ها از امنیت و این امر که با یک سیستم که زیر نظر یک بیمه فعال و قانونمند است می توان یک محیط هوشمند و فعال فراهم آورد .که این مورد را می توان تا حدی آن ایده آل مورد نظر E-commerce دانست.

احتیاجات

همانطور که گفته شد E-commerce یک سیتم جها نی است و همانطور که مشخص است هرسیستمی دارای یک سری احتیاجات است واین احتیاجات برحسب وسعت سیستم و مشخصات آن تعیین می شود حال هرچه سیستم وسیع تر باشد احتیاجات آن نیز بیشتر خواهد بود پس E-commerce که یک سیستم بسیار وسیع است احتیاجات زیادی هم دارد که ما به قسمتی از این احتیاجات می پردازیم .یکی از این احتیاجات که نوعی مشکل هم ایجاد می کند یک زبان مشترک است که باید برای تمام آنهاو Frame Work هاو اتصالات داخلی کدهای امنیتی ایجاد شود. بنابراین اگر کمی دقت کنیم خواهیم دید که ایجاد این امکانات به طور یکجا تولید ابهام می کند در ضمن باید دقت داشت که کمپانی ها و دفاتر و مشتریان به این امر رسیده اند که استفاده از E -commerce به همان خوبی عمل می کند که اگر بخواهند آن کار را به طور مستقیم انجام دهند ، بنابراین این امر خود با عث توسعه این محیط می شود بنابراین ایجاد امکانات ذکر شده یک امر اجباریست .پس ایجاد زبان مشترک برای کمپانی ها و دفاتر مختلف برای صحبت کردن باهم امری است که باید پیاده سازی شود ولی پیاده سازی این زبان به چه صورت است و باید چه ایده آلهایی را بر آورده کند مامی توانیم این ایده آل ها را به صورت زیر دسته بندی کنیم :

1- زبان مشترک حتما احتیاج به یک مدیر دارد

2- احتیاج به یک سیستم امنیتی فوق العاده قوی دارد.
3- احتیاج به یک سری تجهیزات مخصوص برای رسیدن به اهداف خود دارد

بنابراین برای ایجاد یک زبان موفق باید تمام موارد فوق را رعایت کرد تا بتوان یک زبان مشترک با کارایی بالا بدست آورد در غیر اینصورت زبان مشترک طراحی شده کارایی مورد نظر را نخواهد داشت و این امر باعث نا رضایتی مشتریان و دیگر استفاده کنندگان می شود و چنین چیز ی مطلوب این محیط نیست و باعث از دست رفتن اهمیت آن می شود . برای دستیابی و رسیدن به این امر تلاش زیادی صورت گرفت و حاصل این تلاش به وجود آمدن متدهای مختلفی بود چه برای مدیریت و چه برای امنیت یکی از متدهای مهمی که در طی این تلاش به دست آمد متد آنالیز لایه ای درختی بود این متد یک متد بسیار قوی است و همین امر باعث شد که بر روی آن :کارهای بسیار زیادی صورت گرفت و باعث به وجود آمدن سیستمی شد به نام سیستم لایه ای حال می خواهیم در مورد این سیستم بحث کوتاه و مختصری داشته باشیم و تا حدی از عملکردآن مطلع شویم برای شروع این بحث سؤال زیر را مطرح می کنیم :

سیتم لایه ای چیست ؟

این سیستم یک سیستم سطح بالا و مناسب است و طراحی این سیستمها بر مبنای محیط اطراف آن

و احتیاجات آن صورت می گیرد مثلا ممکن است این طراحی ها براساس دسترسیها باشد که چه کاربرانی به آن دسترسی دارند چه درصدی از اطمینان را نیاز دارند (bernie cowens) پس به طور کل سیستم لایه ای یک سیستم با درصد اطمینان بالا می تواند باشد یک سیستم کنترل کننده کنترل برای ورود و خروج اطلاعات ، کنترل برروی دسترسی آنها وکنترل بر روی خیلی چیزهای دیگر. بنابر- این این سیستم را می توان یک سیستم موفق دانست بدلیل اینکه تا حدود زیادی می تواند نیازهای مورد نظر را رفع کند و کاربران را به خواسته های خود برسا ند پس ویژگیهای خاص این سیستم یعنی لایه- ای بودن آن در امر امنیتی بسیار مؤثر است حال می توان این امر را بیان کرد در هر لایه پروتوکولهایی می تواند. وجود داشته باشد وظیفه این protocol ها خا لی کردن مسیر از مشکلات و ایجاد یک مسیر صاف و بدون دست انداز می باشد بنابراین protocol ها می توانند وسیله ای برای طی کردن راه یا سر حدها باشند ک بوسیله که با حفظ آنها وپاک کردن آنها از هر مشکلی می توان یک مسیر صاف و هموار داشت به طور مثال : پرو توکل M Q که برای همین منظور ساخته شده است . تمام این روشها و این بحثها گفته شده به این امر منتهی می شود که اگر در سیستمی Application وجود داشته باشد باید از آن حفاظت شود و باید برای هر Application کد خاص خودش تولید شود پس امنیت Application

ها جزو احتیاجات است یعنی اگر بخواهیم محیط خوب و مناسبی داشته باشیم قطعا باید امنیت Application ها را نیز در نظر گرفت که در غیر این صورت نمی توان از این محیط به عنوان یک محیط موفق نام برد به دلیل اینکه بسیاری ازایده آلهای آن از بین رفته است و به طور خواه یا ناخواه مشتری از آن دلزده می شود و از آن دوری می کند پس باید تمام احتیاجات یک محیط برای استفاده کننده گان ، از آن محیط مشترک فراهم شود تا کاربر بتواند از آن استفاده کند در غیر اینصورت آن محیط به هیچ عنوان محیط موفق و قابل قبولی نخواهد بود بحث دیگری که بسیار مهم است و باید به آن توجه کرد ، همانطور که، در ابتدای بحث نیز گفتیم خطر را باید شناخت دشمن را نیز باید شناخت تا بتوان با سلاح مناسب در مقابل آن ایستادگی کرد پس هم خطر باید شناخته شود و هم عامل آن یعنی ایجاد کننده آن روشهای امنیتی برای خطرها و دشمنان خاص طراحی شده اند هر روشی برای جلوگیری از نفوذ دشمنی خاص می باشد بنابر این با یک روش خاص نمی توان در برابر تمام دشمنان محیط ایستاد و یک دشمن نیز نمی تواند در مقـابل تمام روشها ایستادگی کنـد پس اگر بتوان یک دشمن را کاملا شناخت و راه نفوذ آن را گرفت

بنابر این توانسته ایم از ورود آن جلوگیری کنیم یا حتی اگر دشمنی توانست وارد سیستم شود و بعد ما توانستیم دست او را کوتاه کنیم آنگاه می توانیم ادعا کنیم که طراحی سیستم امنیتی ما یک طرح موفق بوده است در غیر این صورت سیستم یک سیستم محکوم به فنا خواهـد بـود بـه طـور کل شناخت خطر و شناخت دشمن مرحله اول طراحی سیستم هسـتند و بـرای طـرح یـک سیسـتم امنیتی خوب باید هر دوی آنها را شناخت تا بتـوان همانطورکـه گفتـه شـد بـرای ورود دشـمنهای مختلف باشگردهای مختلف روشهای مختلف طراحی کرد تا برای یک سیستم بتواند بـا آسـودگی خاطر به کار خود پرداخته و نگران از دست دادن سرمایه خـود نباشـد . بنـابر ایـن اگـر بخـواهیم دقیق تر بگوئیم سیستمی یک سیستم موفق است که بتواند از ورود دشمن بـه داخـل خـود کـاملا جلوگیری کند .

حال پس از بررسی های ذکر شده می خـواهیم مقـداری در مـورد تکنولـوژی امنیـت بـه صـورت بیشتر در مورد internet وE - commers صحبت کنیم .

همانطور که مشخص است internet یک امر رو به افزایش و اجتناب ناپـذیر اسـت و روز بـه روز به در خواست کننده های آن اضافه می شود طبق آمار هـایی کـه ذکـر شـده ایـن امـر در آمریکـا بیشترین سیر صعودی را دارد که دو ، سوم ، از کاربران دنیا در آمریکا هستند و اروپا یک رونـد 20 در صدی را طی می کند در هر حال این جمعیت رو به افزایش است و برای ایـن افـزایش بایـد فکری کرد البته تخمین زدن تجهیزات برای افراد زیاد سخت نیست به طور مثـال طبـق آمـاری کـه ذکر شده تخمین زدن تجهیزات برای 26 میلیون نفر به همان انـدازه وقـت گیـر اسـت کـه بـرای 6

میلیون نفر وقت گیر است اینک با توجه به اینکه اکثر کاربران internet افرادی هستند با سیستمهایی که البته این کار را خوب بلدند واین افراد بیشتر از e – mail استفاده می کنند ولی قابل توجه است که اکثر آنها دارای internet نیز هستند واین روند یک روند رو به افزایش است بنابر این با توجه به سخنان گفته شده و مورد بررسی قرار گرفته فوق اینطور به نظر می رسد که امنیت در E -commers امری اجتناب نا پذیر است.
ولی با تمام این اوضاع دیده می شود که افرادی هستند که به این پدیده توجه کامل ندارند و تصور
می شود که علت این امر کم اطلاع بودن از این قضیه است که چه حجمی از اشخاص در این شبکه مشغول به کارند.

محدودیت در internet

یک محدودیت در internet سرعت نسبتا پایین آن است به این نکته باید توجه داشت که ما به کاربران و افرادی که در internet مشغول به کار هستند این ارزو را دارند که بتوانند با سرعتی بسیار بالا فایلهای مورد نظر خو را download کنند ولی عملا این امر امری غیر ممکن است و این باعث ایجاد محدودیت می شود و سبب می شود که با آن سرعتی که کاربران احتیاج دارند و دوست دارند بتوانند فایل را download کنند
طبق آمار و تحقیقات نشان داده شده در رابطه با (find / svp Albert lodwings)و[FD/ SV 95] اکثر کار بران روی web برای down load کردن فایلهای grafic order25 , k , 35k , های خود را خاموش کنند.

سرعت یا امنیت:

همانطور که در بالا ذکر شد یکی از محدودیتهای بزرگ در internet سرعت است ولی یکی از احتیاجات بزرگ که سرعت را نیز تحت تأثیرخود قرار می دهد امنیت است . یعنی در فرض اگر سرعت کم است در عوض امنیت وجود دارد می توان با چشم پوشی کردن از بعضی چیزها از سرعت بهتری برخوردار شد ولی این امر بنظر منطقی نمی آید به هر حال سرعت و امنیت دو پا رامتری هستند که باید رعایت شوند و تا آنجا که ممکن است هیچ چیز نباید مانع آنها شود مثلا اندازه فایلها یا order grafic ها به هیچ عنوان نباید جلوی این امر را بگیرد.

مشکلات و نقاط قوت

حسن یک سیستم کجاست و از کجا می توان به حسن آن پی برد اگر از یک سیسنمی بتوان به راحتی استفاده کرد و یا کار با آن راحت باشد می توانیم بگوییم که این سیستم یک سیستم مناسب است که کار با آن راحت است.

البته این امر تمام حسن نیست ولی خود یک حسن است به طور مثال factor key یک سیستم است که این مهم را فراهم می کند این امر باعث می شود user هایی که یکدیگر را نمی شناسند یا نا شناسند به راحتی یکدیگر را پیدا کنند ولی مشکلی نیز وجود دارد و آن شکل ناسازگاری است این شکل از کجا پدیدار می شود و علت چیست !

« برای این امر می توان این توضیح را داد که اگر بخواهیم یک facing serrice ویک end user ها و کارشناسی که وجود دارند بتوانندااین امر را به طور کامل و جدی و درک کنند خواهند دید که همکاری بسیار ساده و روانی با هم خواهند داشت و در ضمن توانسته از دست درازی دیگران جلوگیری کنند.

به هر حال گاهی internet به ان شدت قابل اطمینان نیست و Cracker و hacker ها به اطلاعات مهم دست پیدا می کنند در هر حال در هر سیستمی ایرادهایی وجود دارد ولی خوب تکنولوژی های برتری برای حل این مشکل وجود دارند که می توان از آنها مثلا در موارد زیر استفاده کرد.

(1 SSL) secure socket layer)

(2 TLS) tran sport layer secure)

(3 IPSEc

بنابر این دیده می شود که امنیت ذات اینترنت است و باید به آن توجه خاص شود

بلاکهای امنیتی اینترنت

تا به اینجای کار دیدیم امنیت چیست چگونه رفتار می کند و کمبود آن سبب ایجاد چه مشکلات می شود .

حال می خواهیم این را بدانیم که بلاکهای امنیتی اینترنت شامل چه چیزهایی هستند اگر آنها را به خواهیم به طریق دسته بندی بنویسیم می توانیم آنها را به چهار دسته زیر تقسیم کنیم Steve capp) :)

1- رمز سازی و رمز گشایی

2- امضاهای دیجیتالی

3- دریافت و درک پیام

4- رمزی سازی کردن

الگوهای امنیتی ولایه های امنیتی Steve Capp))

1- Digests message

این الگوریتم به طریق زیر عمل می کند و کار آن ایجاد رمزها و کدهای خاص است.
به این ترتیب رفتار می کند که یک سری بیت اطلاعاتی با طول متغییر دریافت می کند وبا پردازش بر روی آن به آن یک بیت امنیتی اضافه می کند سپس آنها را با طول ثابت استخراج می کند.
این نوع رمز سازی و رمز گشایی شامل 3 پراسس است :.

1- رمز سازی و رمز گشایی

2- امضاء دیجیتال

3- key exchang

باید دانست که این کلید توسط چه کسی و چه افرادی طراحی می شود آیا همه می توانند این کلید را طراحی کنند حتما این طور نیست این کلید را فقط کامپیوتر ها و افراد بسیار قابل اطمینان که از اطراف internet تصدیق می شوند طراحی می شود

2-**لایه** Ipsec

ابن لایه یک لایه ی امنیتی است که این لایه هامعادل هما ن T LS است این لایه دارای شرایط خاص خود است و چند چیز را شرط می کند

1- تولید رمز و باز کردن آن

2- ارتباط الگوریتمی

3-قبول و تایید کردن پیغامهای ارسالی

4-کلید ها وضد تعویض ها

لایه kerberos

این لایه یک client – server Network Ipاست و دارای رمز سازی قرینه است.

نتیجه :

بنابر این دیده شد که internet یا E-commerce باید و باید در آنها امنیت رعایت شود که در غیر اینصورت کاربران دیگر نخواهند توانست در این محیط ها با آسودگی خاطر و راحتی کار کنند و دیگر اینکه برای ایجاد امنیت ابتدا باید خطر را شناخت و دشمن را تا بتوان در مقابل آن با ایجاد یک روش صحیح از نفوذ و پخش آن جلو گیری کرد و امنیت دارای تکنولوژی های مختلف و روشهای مختلف است که هر محیطی روش و تکنولوژی حاص خود رادارد و وجود آن برای هر محیط مشترک یک چیز ضروری و اجتناب ناپذیر است و ذات هر محیط اشتراکی ایجاب می کند که در آن امنیت رعایت شود.

منابع

www. ca. com
www. Spectria. com
www. orbit – ecommerce . com
www. emrt . com