طراحی وب سایت‌های اینترنتی

فصل دوم

تدوین استانداردهای وب

در حالیکه مع الاسف اکثر طراحان سایت و شرکت‌های مدعی عرصه وب داخلی، حتی نیم نگاهی به استانداردهای بسیار قوی منتشر شده از سوی مجامع بین المللی ناظر وب نظیر کنسرسیوم جهانی وب ندارند، واحد تحقیق و توسعه شرکت توسعه مجازی با آینده نگری فراوان و طی عملی ابتکاری، برای اولین بار در کشور اقدام به گردآوری، تدوین، ترجمه و تلخیص استانداردهای وب نمود تا علاوه بر استفاده در تمامی پروژه‌های شرکت، مرجعی راهنما و سرمایه‌ای ارزشمند برای تمامی پروژه‌های آتی شرکت باشد. بر همین اساس، این شرکت سرویس‌های زیر را ارائه می‌نماید.

پاسخ به استعلام در مورد میزان انطباق یک سایت با استانداردهای جهانی

در این سرویس، مدیران و صاحبان یک سایت اینترنتی می‌توانند در مورد میزان انطباق سایت خود با استانداردهای جهانی، از شرکت توسعه مجازی استعلام نمایند تا طی یک پژوهش دقیق فنی، تمامی مغایرت‌های سایت مورد نظر با استانداردهای وب – در صورت وجود – گزارش گردد. این گزارش جامع شامل: عنوان مغایرت، شرح مغایرت، متن کامل استاندارد تخطی شده، سال انتشار و منبع منتشر کننده آن و احیانا راه حل اصلاح این مغایرت خواهد بود. در انتها بر اساس پارمترهای امتیاز دهی تدوین شده توسط شرکت توسعه مجازی، از صد نمره، نمره‌ای به سایت مورد نظر داده می‌شود که در صورت کسب نمره بالای ۸۰، وب سایت مذکور استاندارد و در غیر اینصورت غیر استاندارد تلقی خواهد شد.

ارایه اشتراک بهره مندی از استانداردها طی شرایط خاص به شرکت‌های طراح سایت

با توجه به محرمانه بودن مستندات استانداردهای تدوین شده، شرکت‌های فعال در عرصه فن آوری اطلاعات و وب، تنها پس از متعهد شدن به شرایط خاصی که به متقاضیان اعلام خواهد شد، می‌توانند اشتراک جدیدترین استانداردهای وب را به شرط تمدید سالیانه داشته باشند. هرگونه نشر غیر مجاز این مستندات به هر شکل ممکن توسط شرکت‌های مذکور، پیگیری قانونی و درخواست مجازات شدید برای فرد یا شرکت خاطی را در پی خواهد داشت. البته ذکر این نکته خالی از لطف نیست که شرکت توسعه مجازی در راستای گسترش فرهنگ بهره وری فن آوری اطلاعات و جهت افزایش جایگاه ایران در بین شرکت‌های دارای استاندارد، هر ۵ سال یکبار، استانداردهای پنج سال پیش خود را بصورت رایگان منتشر کرده در اختیار عموم قرار خواهد داد.

دیجیتال کردن اطلاعات و وارد کردن اطلاعات در حجم بالا به بانک اطلاعاتی تحت وب

احیانا در بعضی از پروژه‌های تحت وب که دارای بانک اطلاعاتی معظم هستند و یا در دائره المعارف‌های اینترنتی لازم می‌شود که اطلاعات و داده‌های موجود که به‌صورت اسناد غیر دیجیتال موجود است، بفرمت فایل‌های کامپیوتر تبدیل و در بانک سایت آپلود شود. یکی دیگر از خدمات شرکت توسعه مجازی پوشش دادن این نیاز است.

دیجیتال کردن اطلاعات غیر دیجیتال و تبدیل داده‌ها به فایل‌های کامپیوتری

در این سرویس، اسناد کاغذی شامل عکس ها، مدارک و اسناد اسکن شده به فرمت‌های استاندارد jpg. و gif. برای استفاده در وب تبدیل می‌شوند. همچنین اطلاعات صوتی به فرمت‌های استاندارد و کم حجم ra. و mp۳. تبدیل می‌شود. همچنین فیلم‌های ویدیویی به فرمت‌های استاندارد و بهینه mpg. و wmf. تبدیل می‌شود. همچنین اسناد مکتوب متنی که می‌بایست وارد بانک اطلاعات شوند، با OCR (تبدیل عکس به متن از طریق تشخیص هوشمند نوشته‌های درون عکس) شده و بصورت نرم افزاری تبدیل به متن کامپیوتری می‌شوند و یا توسط تایپیست‌های ماهر و تندست شرکت، تایپ شده بصورت فایل‌های txt. ذخیره می‌گردد. در نهایت اطلاعات دیجیتال تولید شده، آماده استفاده در فاز بعدی می‌باشد.

بازبینی، خطایابی و رفع مشکل اطلاعات دیجیتال شده و وارد کردن آن به بانک اطلاعاتی سایت

در این سرویس، اطلاعات دیجیتال شده توسط تیم کنترل کیفی، مورد بازبینی واقع می‌شوند تا اشکالات آنها مشخص و مرتفع گردد. ترمیم عکس‌های اسکن شده در فتوشاپ، ادیت و ویرایش فایل‌های صوتی و تصویری دیجیتال شده و رفع ایرادهای املایی و انشایی یا غلط های تایپی متون تایپ شده از وظایف تیم بازبینی خواهد بود.

در نهایت اطلاعات دیجیتال کنترل کیفی شده آماده استفاده در فاز بعدی و درج در سایت وب می‌باشد. اطلاعات دیجیتال با فرمت کامپیوتری بصورت Offline و یا Online به بانک اطلاعاتی سایت وارد می‌شوند.

این اطلاعات در قالب جداول بانک‌های اطلاعاتی و دائره المعارف‌های اینترنتی آپلود می‌شوند تا سپس از طریق سایت قابل جستجو باشند.

شیاطین تکنولوژیک – تهدیدهای امنیتی که از آن بی خبریم

فصل سوم

با توجه به نتایج به دست آمده از Anti-Phishing Working Group، با وجود آن‌که در آوریل گذشته ۱۸۰ نوع از این برنامه‌ها کشف شده است که نسبت به آمار ۷۷ تایی آوریل گذشته رشد چشمگیری را نشان می‌هد، ولی از سه ماه پیش این آمار به کندی رو به کاهش گذاشته است.

Sitesاین گونه نتیجه می گیرد که امروزه بیشتر تمرکز نرم‌افزارهای مخرب تجاری بر پردازش اطلاعات دزدیده شده است تا بتوانند براساس آن بهره‌وری مناسبی از این اطلاعات دریافت کنند. او می‌گوید هم اکنون جمع‌آوری، مرتب کردن، دستکاری و ارجاع اطلاعات به بانک‌های اطلاعاتی SQL اهمیت بیشتری پیدا کرده است؛ چرا که بعد از آن هکرها می‌توانند آنچه را که در بین حجم عظیم اطلاعات می‌خواهند راحت‌تر به دست آورند.

به هر حال برای حفاظت از اطلاعات خود نکات زیر را در نظر داشته باشید:

۱- از فایروال مناسبی استفاده کنید تا بتواند برنامه‌های ناشناخته‌ای که سعی دارند از طریق اتصال به خط تلفن اقدام به جابه‌جایی اطلاعات دور از چشم کاربر نمایند را شناسایی و غیرفعال کند. مثلا فایروال رایگان Zone Alarm می‌تواند این کار را برعهده گیرد، اما فایروال ویندوز نمی‌تواند از عهده آن برآید.

۲- استفاده از کلمات عبور گوناگون؛ هیچ‌گاه برای حساب‌های متعدد خود از یک کلمه عبور مشابه استفاده نکنید.

حقه‌های سایت‌های سیادی

سطح خطر: بالا

احتمال خطر: بالا

مقصد: تمامی کاربران اینترنت

فیشینگ (سیادی) یکی از پرسودترین فریب‌کاری‌هایی است که می‌توان در اینترنت انجام داد و استفاده از آن نیز به سرعت درحال رشد است. در ماه آوریل ۲۰۰۶ تعداد سایت‌های جدیدی که از این روش برای فریب‌دادن کاربران استفاده می‌کردند، رکورد جدیدی برجای گذاشت؛ یعنی ۱۱۱۲۱ سایت. این در حالی است که در آوریل ۲۰۰۵ این مقدار تنها ۲۸۵۴ مورد گزارش شده‌بود.

برخی سایت‌های فیشینگ به حدی حرفه‌ای طراحی شده‌اند که حتی می‌توانند به راحتی کاربران حرفه‌ای را نیز فریب دهند، بر اساس تحقیقات صورت گرفته در پروژه Why Phishing Works که دانشمندان US Berkely و Harvardدر آن روی چگونگی فریب خوردن کاربران تحقیق می‌کنند، مشخص شد که در بسیاری مواقع کاربران حرفه‌ای نیز که حتی به جعلی بودن وب‌سایت‌ها پی می‌برند، با سناریویی بسیار جالب روبه‌رو می‌شوند که معمولا در کنکاش برای کشف آن سید می‌شوند. از سوی دیگر کاربران غیرحرفه‌ای معمولا فرق بین سایت اصلی و جعلی را درک نمی‌کنند و به راحتی سید می‌شوند. در این مطالعه مشخص شد که سایت‌های خوب فیشینگ می‌توانند بیش از نود درصد کاربران خود را فریب دهند.

مرورگر تحت نظر رادار

می‌توان گفت که تمام فعالیت‌های فیشرها روی این مسئله تمرکز دارد که چگونه باید کاربر را به سایت‌های جعلی خود هدایت کنند و اطلاعات لازم را از آن دریافت کنند. ممکن است شما به قدری حرفه‌ای باشید که حتی به ایمیل رسمی بانک خودتان که از شما درخواست می‌کنند اطلاعات مربوط به حساب‌هایتان را مجددا وارد کنید نیز جواب ندهید. اما امروزه سیادان از روش‌های جدیدی استفاده می‌کنند که کاربر در پاسخ دادن به چنین ایمیل هایی یا در کل دادن اطلاعات مورد نیاز به آن‌ها اجبار بیشتری داشته باشد.

به‌طور مثال به تازگی یک نرم‌افزار مخرب کشف شده است که به آن Smart redirection نیز می‌گویند. این برنامه هنگامی که شما به سایت اصلی بانک خود رفته‌اید و کلمه عبور و شناسه کاربری حسابتان را وارد می‌کنید، به‌طور مخفی و دور از چشمان شما، آن‌ها را به سازنده یا سرور اصلی خود ارسال می‌کند؛ به همین راحتی!

حتی برخی دیگر از نرم‌افزارهای مخرب این قابلیت را دارند که با در اختیار داشتن نسخه جعلی صدها سایت بانکی و ساکن شدن در مرورگر پی‌سی شما، هنگامی که بخواهید به سایت بانکی خود دسترسی داشته باشید، به راحتی شما را به سایت جعلی هدایت کنند. تا هنگامی که این روش برای سیادان درآمدزا باشد، باید انتظار به وجود آمدن روش‌های جدیدی را برای فریب دادن کاربران داشته باشیم تا پول‌های بیشتری نصیب آن‌ها شود. Michael Rothschild، فعال در زمینه ساخت سخت‌افزارهای امنیتی در شرکت Counter Storm، می‌گوید: اطلاعات دزدیده شده مربوط به حساب‌هایی که اعتبار خوبی دارند هفتاد دلار به ازای هر کارت فروخته می‌شوند. سیادان حتی اطلاعات مربوط به یک حساب را دو بار می‌فروشند!

حیله‌های ماهرانه برای فریب هوشیاران

حتی اگر آدم محتاطی باشید، با خواندن شیوه کار سیادان در خواهید یافت که باید بیش از این‌ها مراقب بود؛

۱- ابتدا کاربر آگاه و دقیق، به صورت دستی URL بانک خود را در نوار آدرس مرورگر خود وارد می‌کند.

۲- نرم‌افزار مخرب روی پی‌سی کاربر، وی را مستقیما به سایت جعلی و ساختگی سیاد می‌فرستد.

۳- با قرار دادن متون و تصاویر از سایت اصلی بانک به صورت بی‌درنگ، سایت جعلی کاملا مشابه سایت اصلی می‌شود. تا جایی که کاربر جعلی بودن آن را تشخیص نمی‌دهد.

۴- تمام این کارها باعث می‌شود کاربر هر چند هم با دقت باشد، اطلاعات مربوط به حساب خود را در سایت جعلی وارد کند.

نکاتی که در ادامه آمده‌اند به شما کمک می‌کنند دچار این حملات نشوید:

۱- به ایمیل هایی که از شرکت‌های ناآشنا ارسال می‌شوند و به نظر می‌رسد قابل اعتماد نباشند، اعتنا نکنید.

2- URLبانک را خودتان تایپ کنید یا از Bookmark استفاده کنید. روی لینک‌های درون ایمیل‌ها کلیک نکنید.

۳- هنگامی که به سایت‌هایی مراجعه می‌کنید که استفاده از آن‌ها مستلزم داشتن امنیت بالایی است، باید آیکونی شبیه قفل آویز را در مرورگرتان ببینید، این مسئله می‌تواند تا حدی بر امن بودن سایت صحه بگذارد.

۴- از نوارابزارهای ضدسیادی استفاده کنید. این نوار ابزارها می‌توانند از ورود شما به سایت‌های جعلی جلوگیری کنند.

نقش فناوری اطلاعات در مدیریت ریسک

در جهان کنونی، عناوین و پارامترهای مختلفی در امر مدیریت مطرح است که اداره آنها نیازمند شناخت و درک صحیح و دانش مخصوص به خود است. پرداخت به هریک از این عناوین و تعیین وجه اشتراک و افتراق هر کدام، نیازمند فرصت کافی به خود است، اما آنچه که امروزه مهم‌تر از همه عناوین مدیریتی، به عنوان اصلی‌ترین عامل در تعیین برنامه‌ها و تصمیم گیری‌ها در محیط های پر فرآیند تاثیر گذار است، بکارگیری و استفاده از تکنینک‌های مدیریت ریسک و به همان میزان سیستم‌های مبتنی بر I,ICT است. فناوری اطلاعات، به نحو فزاینده‌ای بر چگونگی عملکرد و نحوه کارآیی سازمانها، ارگانها، شرکت‌های دولتی و خصوصی اثر گذاشته است، و نقش سیستم‌های مبتنی بر فن آوری اطلاعات در انجام کارآمد امور اداری و تجاری انکار ناشدنی جلوه می کند.

تنوع و گستره فعالیتها موجب می گرددتا امکان پرداختن به همه امور میسر نباشد بنابراین طبقه بندی کردن امورو اولویت دادن به برخی امورمهم نسبت به برخی دیگراز اهمیت زیادی برخوردار نمی باشندضرورت پیدا می کند. امروزه بهره گیری از فناوری اطلاعات در مدیریت ریسک حدیث متفاوتی را باز می گوید و تاثیری عمیق بر چگونگی سر و سامان دادن به فعالیتهای اتوماسیون سازمانها و مدیریت چرخه ایجاد سیستم‌های مکانیزه می گذارد.

مدیریت ریسک، یک مدیریت مهم و ضروری محسوب می شود که تصمیم گیری دقیقی را بر اساس میزان ریسک و خطر میسر می سازد و در اکثر نقاط دنیا توسط پرسنل اجرایی IT مورد بهره برداری قرار می گیرد. ریسک در معنای عام عبارت است از تاثیر منفی ناشی از یک آسیب پذیری و در نظر گرفتن احتمال وقوع و اثر آن در فرآیندهای یک سیستم. فلذا بایستی سطح ریسک پایین؛ متوسط؛ بالاو احتمال وقوع آن و پیامدهای آن مورد شناسایی قرار گیرد تا بتوان برای رفع آن تصمیم گیری کرد. ریسک یعنی: میزان و امکان سرپیچی از قانون که به خسارت و زیان علیه تجارت؛ صنعت و مردم منجر خواهد شدیا به تعبیر دیگر را! بسک امکان وقوع یک خسارت و زیان اعم از مالی و یا غیر مالی در نتیجه انجام یک کار است. مدیریت ریسک، فرآیند تشخیص و ارزیابی ریسک و کاهش آن تا یک سطح قابل قبول می‌باشد و با هدفگذاری امکان پذیر است. هدف از اجرای مدیریت ریسک این است که سازمان بتواند به اهداف ذیل جهت سیستم‌های مبتنی بر فن آوری اطلاعات خود دست یابد: تامین امنیت بیشتر برای سیستم‌های مبتنی بر ذخیره سازی، پردازش و انتقال اطلاعات سازمانی. اعمال مدیریت برای توجیه و بهینه سازی هزینه‌های IT. تصویب و تائید سیستم ها.

مدیریت ریسک دارای سه مرحله است: مدیریت ریسک، ارزیابی ریسک و کاهش ریسک.

مدیریت ریسک:

مدیریت ریسک یعنی شناسایی؛ ارزیابی؛ تجزیه و تحلیل؛ چگونگی رفتار و اداره کردن آن. مدیریت ریسک فرآیندی است که به مدیران امکان می دهد تا هزینه‌های اقتصادی و عملیاتی مورد نظر را مقایسه کنند و با بهره گیری و حمایت از سیستم‌های IT، امکانات و قابلیتهای آنها را بهینه سازندو یا به تعبیر دیگر مدیریت ریسک روشی است برای استفاده بهینه از امکانات و منابع موجود. این روند تنها منحصر به محیط IT نیست و در تمام تصمیم گیری‌های روزانه ما تاثیر به سزایی دارد. به عنوان مثال، امروزه بسیاری از مردم تصمیم به نصب دزدگیر می کنند و بر این اساس هزینه‌ای را به شرکت مربوط می‌پردازند تا این سیستم‌ها را جهت حفاظت بهتر از اموال و دارایی‌های خود به کار گیرند. مسلما افراد هزینه نصب و کنترل اینگونه سیستم‌ها را به نسبت اسباب و دارایی خود می‌پردازند و به همان مقیاس تامین امنیت را برای خانواده خود فراهم می‌آورند. بهره گیری از مدیریت ریسک در چرخه ایجاد یک سیستم: کاهش اثر منفی درسیستم و سازمان و رسیدن به یک پایه اساسی در تصمیم گیری، دلایلی هستند که که سازمان را وادار به اجرای روند مدیریت ریسک برای سیستم‌های مبتنی بر IT می سازند. چرخه ایجاد یک سیستم مکانیزه دارای ۵ مرحله است: شروع، ایجاد و تهیه سیستم، اجرای سیستم، بازبینی مجدد، حفاظت و واگذاری. ارزیابی ریسک: ارزیابی ریسک اولین قدم در روش مدیریت ریسک به شمار می‌آید. سازمانها با استفاده از ارزیابی ریسک، می‌توانند محدوده تهدیدات احتمالی و ریسک مربوط به یک سیستم مبتنی بر IT را در سراسر چرخه ایجاد سیستم مشخص کنند. بازده و نتیجه این امر به تعیین کنترل‌های مربوطه جهت کاهش یا حذف ریسک در طول روند کاهش ریسک کمک می کند. ارزابی ریسک خود دارای ۹ مرحله اساسی است که عبارت است از: تعیین سیستم، تشخیص تهدید، تشخیص آسیب پذیری، تحلیل کنترل، تعیین احتمال، تحلیل اثر سوء، تعیین ریسک، ارایه نظریه و پیشنهاد جهت کنترل سیستم و نهایتا مستند سازی نتایج. کاهش ریسک: کاهش ریسک عبارت است از اولویت دادن، ارزیابی و اجرای کنترل‌های کاهش ریسک که در روند ارزیابی ریسک پیشنهاد شده اند. از آنجایی که از بین بردن تمامی ریسک‌ها عملا امکان ندارد، مدیران با اعمال کنترل‌های مناسب، کاهش ریسک را تا یک سطح قابل قبول به انجام می‌رسانند. کاهش ریسک را از طریق موارد ذیل می توان انجام داد.

الف- تقبل ریسک:

پذیرفتن ریسک احتمالی و ادامه عملیات سیستم IT جهت پیاده سازی کنترل‌ها تا رسیدن به یک سطح قابل قبول. ب- اجتناب از ریسک: دور کردن ریسک با از میان برداشتن عامل و پیامدهای ریسک. ج- برنامه ریزی ریسک: کنترل ریسک از طریق ایجاد یک برنامه کاهش ریسک که به کنترل‌ها اولویت بخشیده و آنها را اجرا و اداره می کند. د- تصدیق و تحقیق: قبول نقطه ضعف یا آسیب پذیری و تحقیق در خصوص کنترل‌ها جهت اصلاح آسیب پذیری. ه- انتقال ریسک: انتقال ریسک برای جبران خسارت، به طور مثال بیمه کردن سیستم. سازمانها می توانند حدود کاهش ریسک را بر حسب احتمال یا تاثیر تخفیف تهدید (دو عاملی که سطح کاهش یافته ریسک را در یک عملیات سازمانی تعیین می کنند) بررسی کنند. به ریسکی که بعد از اجرای کنترل‌های جدید می ماند، ریسک باقی مانده می گویند. عملا هیچ سیستم IT بدون ریسک نیست و تمام کنترل‌های صورت گرفته را ریسک برطرف نمی کند. چنانچه ریسک باقی مانده تا یک سطح قابل قبول تقلیل نیابد، چرخه مدیریت ریسک باید تکرار گردد تا روشی را که برای کاهش ریسک باقی مانده مشخص سازد.

هنگامی که مسئولان و مدیران اعلام کنند که ریسک به سطح مناسبی رسیده، باید گزارشی را که بیانگر قبول ریسک باقی مانده است، قبل از تائید و معتبر سازی سیستم، قبول و به امضا رسانند. نکات اصلی در مدیریت موفق ریسک: از فواید مدیریت ریسک به طور خلاصه می توان به افزایش کارآئی؛ موثر بودن؛ تسهیلات و روان سازی؛ کاهش هزینه؛ سرعت عمل؛ کاهش زمان انجام عملیات اشاره نمود. اما یک برنامه موفق در مدیریت ریسک بستگی به موارد ذیل دارد:

۱- تعهد مدیریت ارشد در خصوص زمان و منابع ضروری

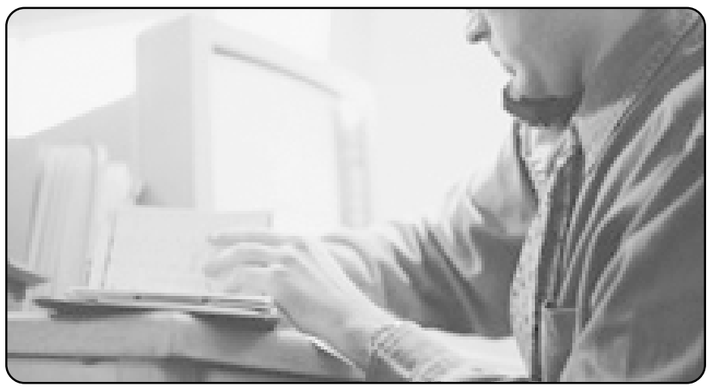
۲- پشتیبانی و همکاری همه جانبه گروه

۳ -ITصلاحیت تیم مدیریت ریسک

این گروه باید مهارت لازم را در پیاده سازی روش مدیریت ریسک در یک سیستم را دارا باشند. ریسک و احتمال خطر عملیات را تشخیص دهند و بر آن اساس، حمایت‌های مقرون به صرفه‌ای را جهت رفع احتیاجات سازمان ارایه نمایند.

۴- آگاهی و مسئولیت پذیری گروه کاری که باید از روش‌ها و آئین نامه‌ها پیروی کرده و کنترل‌های اجرا شده در خصوص حمایت از عملیات سازمانشان را بپذیرند.

www.itkar.com



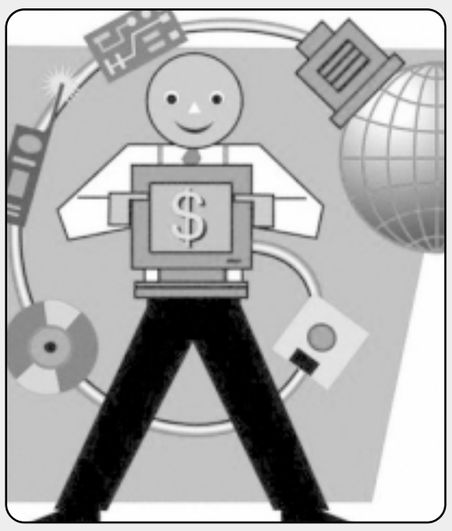
Proxy Server چیست؟

فصل پایانی

ویژگی چهارم: Proxy Server بعنوان نرم افزاری که می‌تواند با سیستم عامل شما مجتمع شود و همچنین با IIS (Internet Information Server)) سازگار می‌باشد، استفاده می‌گردد. خدمات Proxy Server سه سرویس در اختیار کاربران خود قرار می‌دهد:

۱-Web Proxy Service: این سرویس برای Web Publishingیا همان ایجاد Web Site های مختلف درشبکه LAN مفید می‌باشد. برای این منظور قابلیت مهم Reverse Proxing در نظر گرفته شده است Reverse Proxing .امکان شبیه سازی محیط اینترنت درمحیط داخل می‌باشد. به این ترتیب فرد بدون ایجاد ارتباط فیزیکی با اینترنت می‌تواند برنامه خود را همچنان که در محیط اینترنت عمل خواهد کرد، تست کرده و مورد استفاده قرا دهد. این قابلیت در بالا بردن سرعت و کاهش هزینه تولید نرم افزارهای کاربردی تحت اینترنت موثر است.

۲-Winsock Proxy Service: منظور، امکان استفاده از API Call های Winsock در Windows است. در Windows، Function Call های مورد استفاده در سرویسهای اینترنت مانند Telnet، FTP، Gopher و . . . ، تحت عنوان Winsock Protocols معرفی شده اند. در حقیقت برای استفاده از این سرویسها در نرم افزارهای کاربردی نیازی نیست که برنامه نویس چگونگی استفاده از این سرویسها را پیش‌بینی کند.



۳-Socks Proxy Service: این سرویس، سرویس Socks 4.3a را پشتیبانی می‌کند که در واقع زیر مجموعه‌ای از Winsock می‌باشد و امکان استفاده از Http 1.02و بالاتر را فراهم می‌کند. به این ترتیب می‌توان در طراحی Website خارج از Firewall، Security ایجاد کرد. معیارهای موثر در انتخاب

۱ -Proxy Server: سخت افزار مورد نیاز: برای هر چه بهتر شدن توانمندیهای Proxy Server، باید سخت افزار آن توانایی تحمل بار مورد انتظار را داشته باشد.

۲- نوع رسانه فیزیکی برای ارتباط با اینترنت: راه حلهای مختلفی برای اتصال به شبکه اینترنت وجود دارد. ساده ترین راه، استفاده از مودم و خطوط آنالوگ می‌باشد. راه دیگر استفاده از ISDN و خطوط دیجیتال است که هم احتیاج به تبدیل اطلاعات از آنالوگ به دیجیتال و برعکس در ارسال و دریافت اطلاعات ندارد و هم از سرعت بالاتری برخوردار است. روش دیگر استفاده از خط های E۱/T۱ با ظرفیت انتقال گیگا بایت می‌باشد. پیشنهاد می‌شود که در شبکه‌های با کمتر از ۲۵۰ کاربر از ISDN و از ۲۵۰ کاربر به بالا از E۱/T۱ استفاده شود. (البته در ایران به علت عدم وجود خطوط ISDN و کمبود خطوط E۱/T۱ این استانداردها کمتر قابل پیاده سازی هستند.)

۳- هزینه ارتباط با اینترنت: دو عامل موثر در هزینه اتصال به اینترنت، پهنای باند و مانایی ارتباط می‌باشد. هر چه مرورگرهای اینترنتی بیشتر و زمان استفاده بیشتر باشد، هزینه بالاتر خواهد بود. با توجه به اینکه Proxy Server می‌تواند با Caching اطلاعات این موارد را بهبود بخشد، بررسی این عامل می‌تواند در تعیین تعداد Proxy های مورد استفاده موثر باشد.

۴- نوع و نحوه مدیریت سایت: این عامل نیز در تعیین تعداد Proxyها موثر است. مثلا« اگر در شبکه‌ای مشکل راهبری وجود داشته باشد، با اضافه کردن تعداد Proxyها، مشکل راهبری نیز بیشتر خواهد شد.

۵- پروتکل های مورد استفاده: Proxy Server ها معمولا از پروتکلهای TCP/IP و یا IPX/SPX برای ارتباط با Client ها استفاده می‌کنند. بنابراین برای استفاده از Proxy باید یکی از این پروتکل‌ها را در شبکه استفاده کرد. پیشنهاد می‌شود در شبکه‌های کوچک با توجه به تعداد کاربرها Proxy Server و Web Server روی یک کامپیوتر تعبیه شوند و در شبکه‌های متوسط یا بزرگ تعداد serverها Proxy بیش از یکی باشد.

منبع: **golpesar**