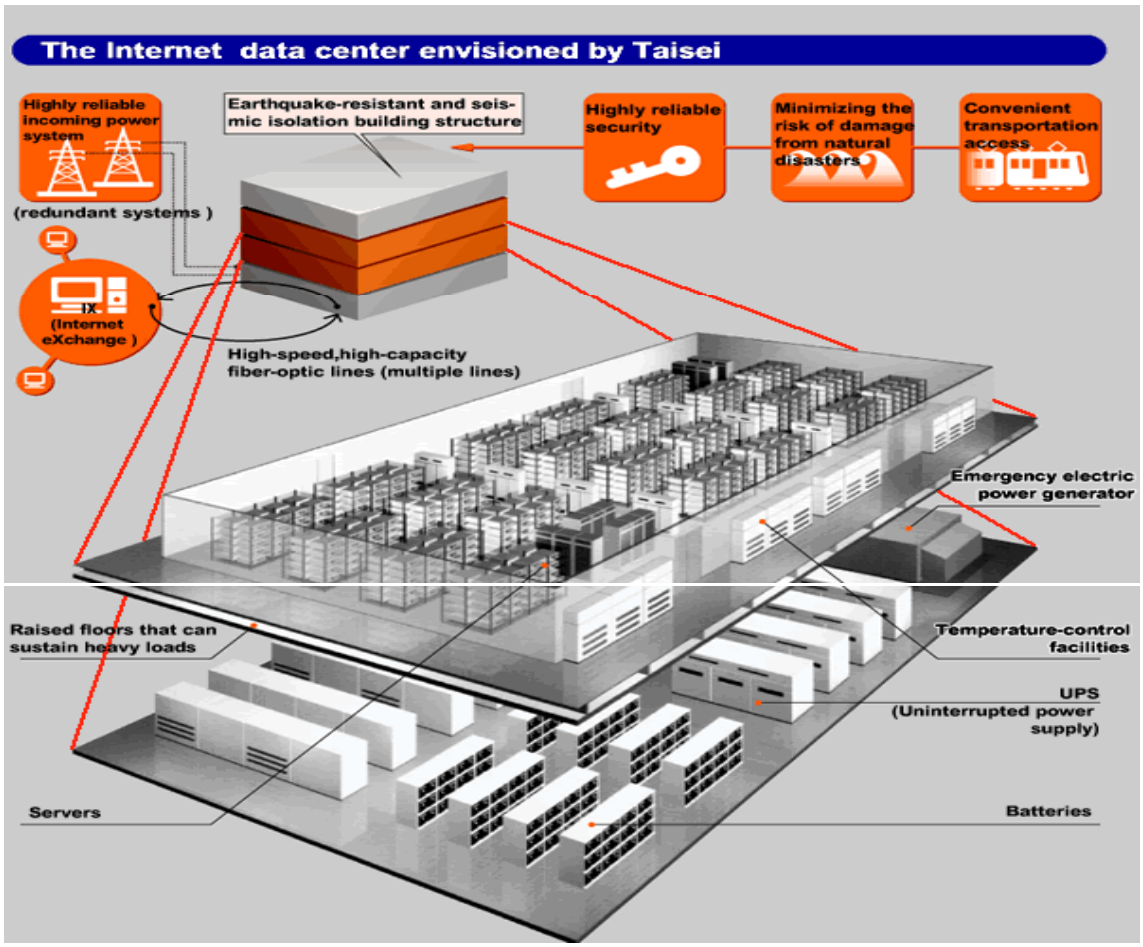
آئین نامه

مرکز خدمات داده اینترنتی(IDC)



مقدمه

در راستای توسعه فن آوری ارتباطات و اطلاعات در سطح کشور و باتوجه به اهمیت روز افزون ارتباطات اینترنتی و تجارت الکترونیکی، استفاده از شبکه های امن با امکانات قابل قبول بعنوان بستری مناسب برای ارائه سرویس های متنوع اطلاعاتی بخش دولتی و غیردولتی مورد نظر قرار گرفته است.مراکز خدمات داده اینترنتی به عنوان راه حلی مناسب برای نیل به این هدف مطرح گردید و وزارت ارتباطات وفناوری اطلاعات در نظر دارد نسب به صدور مجوز برای مرکز خدمات داده اینترنتی بر اساس این آئین نامه وبه استناد بند الف ماده ۱۲۴ قانون برنامه سوم توسعه اقتصادی , اجتماعی و فرهنگی جمهوری اسلامی ایران و آیین نامه اجرایی آن اقدام نماید .

۱ - تعاریف

۱-۱ مرکزخدمات داده اینترنتی: مجتمع ایمن و مقاوم در برابر تهدید و خطا ودارای ارتباطات پر سرعت و پایدار به منظور میزبانی تجهیزات , سرویسها وکاربردهای اطلاعاتی

۱-۲ مدیریت: نظارت، تغییر و کنترل فرآیندهای خرابی، ظرفیت، حسابرسی، کارایی و امنیت در شبکه

۱-۳ SLA: تعیین و توافق سطح و کیفیت خدمات ارائه شده به مشتری

۱-۴ وزارت: وزارت ارتباطات و فناوری اطلاعات

۲ - ویژگیها و مشخصه های مرکز خدمات داده اینترنتی

۲-۱ امکانات و ظرفیت های فنی:

فضا و توان به ساختمان و امکانات ساختمانی مرکز خدمات داده اینترنتی اشاره می کند و حداقل امکانات و شرایط به شرح زیر می باشد. توضیحات بیشتر در ضمیمه فنی آورده شده است.

۲-۱-۱ امکان ارتباط پر ظرفیت با شبکه دیتا و اینترنت
۲-۱-۲ امکان دسترسی به خطوط تلفنی با ظرفیت بالا
۲-۱-۳ بکارگیری سیستم برق بدون وقفه و مولد برق اضطراری با قابلیت تامین برق بمدت ۲۴ ساعت
۲-۱-۴ استفاده از سیستمهای اعلام و اطفا حریق
۲-۱-۵ بکارگیری سیستمهای تهویه مطبوع برای تثبیت میزان گرما و رطوبت
۲-۱-۶ استفاده از فضای متناسب با سرویسهای درخواستی IDC
۲-۱-۷ مقاومت لازم در برابر مخاطرات و بلایای طبیعی و جوی

۲-۲ امنیت

سیستم امنیت، حفاظت و نگهداری از تجهیزات، اطلاعات و سرویسهای موجود در مرکز خدمات داده اینترنتی را فراهم می کند. حداقل سیستم ها و مشخصه های زیر به منظور تامین امنیت IDC مورد نیاز می باشد. توضیحات بیشتر در ضمیمه فنی آورده شده است.

۲-۲-۱ امنیت فیزیکی

امنیت فیزیکی شامل پارامترهای فیزیکی در ارتباط با امکانات وتجهیزات مرکز خدمات داده اینترنتی می‌شود که حداقل می بایست شامل: سیستم مانیتورینگ، سیستم کنترل ورود و خروج و سیستم مقاوم در برابر زلزله، صاعقه، سیل، سیستم تشخیص و اتفاء حریق باشد.

۲-۲-۲ امنیت زیرساخت IDC

موارد امنیتی را شامل می شود که زیرساخت IDC را در برابر تهاجم های داخلی و خارجی محافظت می نماید و حداقل ایجاد سرویس های امنیتی زیر الزامی است.

۲-۲-۲-۱ سیستم های دیوارهای آتش

۲-۲-۲-۲ شناخت تهاجم و اخطارهای متعاقب آن(سیستم IDS)

۲-۲-۲-۳ سیستم شناسایی، تعیین اعتبار و حسابرسی (AAA)

۲-۲-۲-۴ استفاده از سیستم های پشتیبان اطلاعات (بهره گیری از سیستم های Backup گیری و Mirroring)

۲-۲-۲-۵ استفاده از سیستم بازیابی نقصان (disaster recovery)

۲-۲-۲-۶ استفاده از سیستم های هوشمند ضد ویروس

۲-۳ زیر ساخت شبکه

زیرساخت شبکه مرکز خدمات داده اینترنتی در تبادل و انتقال داده‌ها و ارائه سرویس نقش اصلی را ایفا ء می کند IDC بایستی حداقل امکانات و مشخصه های زیر را فراهم آورد. توضیحات تکمیلی در ضمیمه فنی آمده است.

۲-۳-۱ ارائه ارتباطات افزونه (Redundant) به شبکه دیتا

۲-۳-۲ ایجاد لایه فیزیکی مطمئن برای انتقال اطلاعات

۲-۳-۳ استفاده از ساختار ماژولار و افزونه

۲-۳-۴ بکارگیری سوئیچینگ و مسیریابی استاندارد در لایه های مختلف شبکه

۲-۳-۵ بکارگیری متعادل کننده های ترافیک

۲-۳-۶ امکان بکارگیری و ارائه کیفیت خدمات (QoS)

۲-۳-۷ استفاده از سیستم های ذخیره سازی

۲-۳-۸ امکان بکارگیری VPN در ارتباطات مشترکین

۲-۴ مدیریت مرکز خدمات داده اینترنتی

مدیریت مراکز خدمات داده اینترنتیباید مبتنی بر استانداردهای ISO 17799 و BS7799 طراحی و پیاده‌سازی گردد و مسئولیت موارد زیر به عهده مدیریتIDC می باشد.

۲-۴-۱ امکان بررسی، تشخیص و بازیابی اطلاعات

۲-۴-۲ مدیریت و تضمین سطح خدمات قید شده در قرارداد مشتری

۲-۴-۳ مدیریت SLA بر اساس سرویس

۲-۴-۴ حسابرسی و صدور صورتحساب مشتری

۲-۴-۵ ارائه مدیریت از راه دور

۲-۴-۶ پاسخگویی تمام وقت به شکایات و خواسته های مشترکین

۳ – سرویس های مرکز خدمات داده اینترنتی

سرویسهای ارائه شده توسط مرکز خدمات داده اینترنتی به شرح زیر می باشند:

۳-۱ سرویس های عمومی مانند caching, email, DNS, chat, FTP, web hosting و . . .

۳-۲ سرویس های دسترسی پهن باند مانند Ethernet وxDSL جهت دسترسی به IDC از طریق شرکت های دارای مجوز PAP

۳- ۳ سرویس ارائه اشتراک مکان (collocation)

۳- ۴سرویس دسترسی به IDC از طریق اینترنت و شبکه دیتا

۳- ۵سرویس VPN درسطح برنامهٔ کاربردی

۳- ۶ سرویسهای مدیریت شده مانند: امنیت، مدیریت و .....

۳-۷ سرویس پشتیبانیIDC (داده ها، نرم افزار و سخت افزار)

۳-۸ سرویسهای کاربردی فناوری اطلاعات (ASP)

۴ -مقررات عمومی اخذ مجوز

هر مرکز خدمات داده اینترنتی برای اخذ مجوز علاوه بر تامین مشخصات مذکور در بند ۲ این دستور العمل، باید شرایط ذیل را دارا باشد:

۴-۱ دارا بودن هویت حقوقی ایرانی ثبت شده در یکی از ادارات ثبت شرکتها در ایران با موضوع فعالیت در زمینه رایانه

۴-۲ مدیر عامل و اعضاء هیئت مدیره شرکت بایستی فاقد سوء سابقه کیفری باشند و دارای صلاحیت عمومی مورد تأیید مراجع ذیصلاح باشد .

۴-۳ مجوز تاسیس مرکز خدمات داده اینترنتی به مدت ۵ سال توسط سازمان تنظیم مقررات و ارتباطات رادیویی صادر می گردد و این مجوز در پایان پنج سال مطابق ضوابط قابل تمدید می باشد.

۴-۴ مرکزخدمات داده اینترنتی بایستی تحت قوانین و ضوابط جاری کشور و همچنین ضوابط و مقررات ابلاغی از سوی وزارت ارتباطات و فناوری اطلاعات عمل نماید .

۴-۵ مجوز صادر شده قابل واگذاری به غیر نمی باشد و در صورت تغییر اعضاء هیئت مدیره, مدیران جدید می بایست دارای شرایط لازمه باشند .

۴-۶ ارائه تضمین سطوح خدمات (SLA) به مشترکین برای سرویس های درخواستی IDC الزامی است

۴-۷ دارنده مجوز ملزم به رعایت امانت اطلاعاتی است که از طرف مشتریان در محل IDC قرار داده می شود .

هرگونه بهره برداری و انتشار غیر مجاز اطلاعات بدون هماهنگی با صاحب اطلاعات (حقیقی ، حقوقی) منجر به پیگیری های قانونی شده و می تواند موجب لغو مجوز گردد.

۴-۸ شبکه دسترسی به مراکز مخابراتی، برای مرکز IDC در چارچوب طرح پیشنهادی و مورد توافق و تأیید معاونت فناوری اطلاعات حداکثر برای مدت ۲ سال بصورت رایگان از طرف وزارت و توسط شرکت های مخابراتی و حداکثر ظرف مدت ۴ ماه تأمین خواهد شد. (شبکه دسترسی شامل ایجاد خطوط مورد نیاز فیبر نوری تا اولین مرکز مخابراتی و یا ارتباط با شبکه ملی دیتا به صورت موازی جهت تأمین امنیت فیزیکی قابل قبول).

۴-۹ درصورت بروز اختلاف مابین دارنده مجوز و شرکت های تابعه وزارت، سازمان تنظیم مقررات و ارتباطات رادیویی مرجع حل اختلاف خواهد بود.

۵- لغو مجوز :

در صورت تخلف از مفاد این آیین نامه و قوانین جاری کشور مبنی بر حفظ امانت، اجرای فعالیتها در چارچوب مجوز و غیره، در بار نخست برای دارنده مرکز خدمات داده اینترنتی تذکر کتبی داده شده و در صورت تکرار پس از رسیدگی های لازم نسبت به لغومجوز اقدام خواهد شد در صورتیکه اقدامات دارنده مجوز منجر به ورود هرگونه خسارت به وزارت ارتباطات و فناوری اطلاعات یا استفاده کننده شود , دارنده ملزم به جبران آن خواهد بود .(مرجع تشخیص فنی وزارت ارتباطات و فناوری اطلاعات می باشد و برای لغو مجوز از طریق ارجاع موضوع به دادگاه صالحه کشور پیگیری خواهد شد.)

ضمیمه ۱: شیوه صدور مجوز

۱- اعلام فراخوان عمومی در جراید و مطبوعات جهت دریافت تقاضای اخذ مجوز در سطح کشورچاپ می‌شود.
۲-کلیه واجدین شرایط ایجاد مراکزخدمات داده اینترنتی (IDC) میتوانند تقاضای خود را در مدت زمان اعلام شده در فراخوان به وزارت ارتباطات و فناوری اطلاعات ارائه نمایند.

۳- در صورت وصول تقاضای بیش از تعداد مورد نیاز که شامل سه مجوز خواهد بود، پس از تائید مدارک متقاضیان و بر اساس امتیازات تخصیصی مجوز برای دارنده، بالا ترین امتیاز صادر خواهد شد.

۴- عواملی که در کسب امتیاز مؤثر هستند عبارتند از:

الف) کیفیت و جامعیت طرح فنی و اقتصادی پیشنهادی

ب) میزان سرمایه پیشنهادی جهت راه اندازی

ج) تعداد و سطح علمی و تجربی نیروهای فنی مورد نظر

د) کیفیت متراژ و محل ساختمان پیشنهادی

ه) مشارکت فنی شرکت معتبر خارجی که دارای سابقه اجرایی در این خصوص می باشد.

۵- برای تضمین حسن انجام تعهدات دارنده مجوز؛ معادل ده میلیارد ریال سپرده نقدی یا ضمانت بانکی از دریافت کننده مجوز اخذ خواهد شد.

۶- پس از اعلام فراخوان کمیته ای جهت ارزیابی تقاضاهای واصله متشکل از نماینده تام الاختیار سازمان تنظیم مقررات و ارتباطات رادیویی، معاونت فن آوری اطلاعات، شرکت ارتباطات زیر ساخت، شرکت ارتباطات داده‌ها و مرکز تحقیقات مخابرات ایران بعنوان مشاور مادر تشکیل خواهد شد.

۷- متقاضیان شرکت در فراخوان می بایست مبلغ ۱۰۰ میلیون ریال به صورت ضمانت بانکی به نام وزارت به عنوان سپرده شرکت در فراخوان تسلیم نمایند .

۸- پس از تعیین حداکثر ۳ شرکت حائز شرایط, شرکت های مذکور موظفند ظرف ۲۰ روز از تاریخ ابلاغ نسبت به پرداخت سپرده یا تسلیم ضمانت نامه (موضوع بند ۵، ضمیمه ۱) اقدام نمایند. در غیر اینصورت وزارت نسبت به ضبط سپرده شرکت در فراخوان اقدام خواهد نمود و به اولویت بعدی مراجعه خواهد کرد.

۹- سپردهٔ سایر شرکت کنندگان در فراخوان بجز نفرات اول تا چهارم پس از تعیین شرکت های منتخب مسترد خواهد شد و سپرده مربوط به شرکت های اول تا چهارم نیز پس از انقضای ۲۰ روز و رعایت بند ۸ مسترد می شود.

۱۰- برنده از زمان اعلام موظف است ظرف مدت شش ماه نسبت به راه اندازی سرویسهای اولیه IDC و در مدت یکسال به راه‌اندازی اکثر سرویسهای آن اقدام نماید.

ضمیمه ۲ : ویژگیهای فنی مرکز خدمات داده اینترنتی

مقدمه

در حال حاضر بیشتر سازمان ها و شرکت ها در بخش دولتی و خصوصی به واسطه نیاز های کاربران و محرک های بازار می‌بایست سرویس های خود را در محیط اینترنت و به روشی امن و کنترل شده ارائه نمایند. پایداری در دسترسی و قابلیت گسترش برای پاسخگویی نیازهای روبه رشد کاری از اصلی ترین مشخصه های این سرویس ها به شمار می‌روند. مراکزخدمات داده اینترنتی (Internet Data Center) به عنوان شبکه ای واسط بین محیط باز اینترنت و شبکه های خصوصی سازمانی , مدل بسیار مناسبی را برای پیاده سازی سرویس های عمومی و اختصاصی یک سازمان معرفی می نماید و با متمرکز و یکپارچه نمودن تدارک و ارائه سرویس ها در شبکه باعث صرفه جویی و بهره وری در سازمان ها می گردند.
در این قسمت مشخصه ها و ویژگیهای مرکزخدمات داده اینترنتی و نکات فنی قابل طرح و پیاده سازی در این مراکز آورده شده است:

۱- فضا و توان

۱-۱ کف کاذب و جعبه کابل هوایی(cable tray)

سیستم cabling در مرکز دیتا باید شامل سیستم کف کاذب و جعبه کابل هوایی(cable tray) باشد. کفهای کاذب علاوه بر ایجاد ظاهری زیبا دسترسی آسان به کابلهای پنهان را فراهم می‌نمایند. مسیر هدایت کابلها در زیر کف کاذب توسط کانالهای کابل (Raceway) صورت می‌پذیرد.

۱-۲ نصب لدر و استراکچر

جهت هدایت کابلهای رابط دیتا و تغذیه بین تجهیزات مرکز دیتا، واسطهای داخل سایت و سایر بخشهای مرکز نیاز به نصب لدر و استراکچر می‌باشد که امکان هدایت آسان کابلهای دیتا و تغذیه توسط واحدهای توسعه و نگهداری و امکان فیکس کردن و نصب و توسعه آسان Rack های تجهیزات دیتا و جلوگیری از واژگونی و جابجایی آنها در اثر حوادث احتمالی را فراهم می آورد.

۲- امنییت

۲-۱ امنیت فیزیکی

امنیت فیزیکی شامل ایجاد محدودیت دسترسی افراد و نظارت بر سیستم می باشد. به طور نمونه استفاده از سیستمهای امنیتی که بر اساس اثر انگشت افراد کار می کنند و اجازه دسترسی افراد را صادر می کنند لازم و ضروری است. به منظور حفاظت فیزیکی باید از تجهیزات زیر استفاده نمود.

۲-۱-۱ سیستم دوربین مدار بسته

باید با نصب دوربینهای مدار بسته در نقاط مختلف سایت مرکزی کلیه نقاط سایت را از یک نقطه،کنترل نمود.

۲-۱-۲سیستم مانیتورینگ

استفاده از سیستم مانیتورینگ دسترسی کاربران و کامپیوترهای مختلف را کنترل نموده و از دسترسی های غیر مجاز پیشگیری می کند.

۲-۱-۳سیستم کنترل و ورود با کارت هوشمند

با استفاده از کارتهای هوشمند، کنترل ورود و خروج پرسنل و افراد مجاز تحت نظارت می شود.

۲-۱-۴سیستم قفل هوشمند ورود و خروج

از دیگر سیستمهای کنترل امنیت فیزیکی سیستمهای قفل هوشمند ورود و خروج می باشند که استفاده از آنها لازم و ضروری است. با استفاده از این قفلها باید از ورود/خروج افراد مشکوک به/از سایت جلوگیری کرده و در مواقع اضطراری دربها را قفل نمود.

۲-۱-۵سیستم کامپیوتری گزارش تردد پرسنل

لازم است که بطور حتم از سیستم های کامپیوتری و نرم افزاری ثبت و گزارش گیری تردد پرسنل و کنترل دسترسی فیزیکی استفاده گردد تا مسئولان کنترل سایت ورود و خروج پرسنل و ساعات تردد آنها را کنترل نمایند.

۲-۱-۶سیستم مقاوم در برابر زلزله، صاعقه، سیل و ....

برای جلوگیری از بروز خسارت در زمان زلزله، صاعقه، سیل و .....می‌بایست:

- محل ساختمان در مکانهای پر خطر مانند لبه گسلهای فعال یا در معرض سیل و یا ریزش کوه و امثال آن قرار نداشته باشد.
- لازم و ضروری است کلیه تجهیزات اعم از هاب، روتر، سوئیچ، pc ها و .... در داخل راک قرار گیرند.
- باید کلیه راکها را کاملاً به کف کاذب و لدر ثابت نمود تا در زمان زلزله از تکان های شدید و ریزش تجهیزات جلوگیری شود.
- ضروری است کلیهٔ تجهیزات داخل راک با بست های مخصوص به دیواره های راک محکم بسته شود و توسط سینی از یکدیگر جدا شوند.

۲-۱-۷سیستم اطفاء حریق

تجهیزات تشخیص دود و حریق خاموش کردن آتش در زمان بروز حریق مطابق استانداردهای ملی را امکانپذیر ساخته و بایستی در طرح و پیاده سازی IDC در نظر گرفته شود.

۲-۲ *امنیت زیرساخت*

این سرویسها شامل مشخصات و تکنولوژیهایی می باشند که باعث امنیت زیرساخت IDC و برنامه های کاربردی می شوند.

۲-۲-۱دیوارهای آتش و سرویس های مدیریت شده دیوارهای آتش

دیوار آتش سیستمی است که در بین کاربران یک شبکه محلی و یک شبکه بیرونی(مثلاً اینترنت) قرارمی گیرد و بر تمام اطلاعات ورودی شبکه نظارت داشته و از عبور اطلاعات بدون مجوز جلوگیری کرده و آنها را متوقف می کنند. دیوار آتش به ۲ صورت سخت افزاری و نرم افزاری در شبکه وجود دارد و از بروز حملات(البته نه به طور قطعی) جلوگیری می کند.سرویسهای مدیریت شده دیوار آتش مدیریت، پیکربندی و تنظیم دیوار آتش متعلق به مشتری را بر عهده دارند.سرویسهای نگهداری دیوار آتش مدیریت دیوار آتش و پشتیبانی آنها را بر عهده دارند و بایستی در IDC از آنها بهره گرفته شود.

۲-۲-۲ سیستم IDS

شناخت مزاحمین و اخطارهای متعاقب آن به منظور ایجاد یک مرکزخدمات داده اینترنتی کامل و ایمن الزامی است. IDS توانایی شناسایی حمله و دسترسی به منابع سرورها را قبل از آنکه اجازه دسترسی انجام شود را دارا می‌باشد. از اینرو وجود این سرویس در شبکه ها بسیار ضروری می باشد.

۲-۲-۳ Authorization, Authentication, Accounting (AAA)

این سیستم یک لایه امنیتی ضروری را به وجود می آورد که تصدیق هویت کاربران، اجازه دسترسی ها و فرایند حسابرسی کاربران را کنترل می کند و امنیت سیستم را در سطح بالایی حفظ می کند.

۲-۲-۴ Software Patch

ضروری است که علاوه بر تجهیزات فیزیکی توسط آخرین تصحیح های برنامه های نرم افزاری امنیت سیستم را تامین نمود.

۲-۲-۵ پشتیبانی اطلاعات

لازم است همواره منظم از سیستم ها و اطلاعات شبکه Backup گرفته شود تا از دسترسی به آن اطمینان حاصل شود. رونوشت راه دور اطلاعات برای توزیع محتوا ، آزمایش برنامه های کاربردی ، پشتیبانی خطا و انتقال (جابجایی) data center انجام می شود و راه حل‌های بازیابی اشتباه Real-time مانند بازتاب همزمان، به شرکتها اجازه می دهد تا تضمین بدون وقفه سرویس های mission – critical و داده ها و اطلاعات مشتریان را به خوبی پشتیبانی نمایند

۲-۲-۶ امنیت یکپارچه

علاوه بر امنیت اولیه ایجاد شده در لبه اینترنت، سیاستهای امنیتی در شبکه برای اینترانت به عنوان لایه دوم امنیت عمل می نماید. این آماده سازیهای امنیت داخلی همچنین حفاظت و پشتیبانی در برابر کاربران داخلی بدون اجازه ورود به سیستم های داخلی و کاربران دور با دسترسی به شبکه داخلی را ایجاد می کند.

۲-۲-۷ دسترسی غیر مجاز

به منظور اجتناب از دسترسی های غیر مجاز و حفظ امنیت داده ها، لازم است تا AAA برای ایجاد تأیید login، مبنای تائید دستوری و محاسبه اطلاعات کاربر استفاده شود. به منظور مقیاس پذیری و مدیریت پذیری، استفاده از سرور سیستم کنترل دسترسی ترمینال کنترل کننده دسترسی برای نگهداری و پشتیبانی جایگاه مرکزی اطلاعات username و password مناسب و لازم می باشد.
تجهیزات محلی AAA از پایگاه داده محلی username و password روی سوئیچ برای تصدیق کردن تلاشهای کاربر استفاده می کنند. اختیار دستور هر کاربر می تواند از طریق تنظیم سطح دسترسی کاربر خاص در پایگاه داده username و password ایجاد شود.

۲-۲-۸ شناسایی شبکه / ویروسها / کرمها

از کاربردهای گوناگون مانند NMAP، DSNIFF و Ethereal برای انجام packet sniffing و port scanning در تجهیزات شبکه و میزبانها برای کشف سریع رخنه های امنیتی، باید استفاده شوند. این برنامه های نرم افزاری در جهت جستجوی آسیب پذیری هایی که می توانند اتفاق بیافتند، استفاده می‌گردند.

۲-۲-۹ کاهش حملات لایه ۲

طراحی و تجهیز سیاست امنیت برای پشتیبانی در برابر حملات و تجاوزات محلی لایه ۲ به شرح زیر می باشد:

- غیر فعال نمودن Redirect های IP
- غیر فعال نمودن مسیریابی منبع IP
- استفاده از یک password رمزی فعال
- استفاده از تنظیم های امن خواندن و نوشتن SNMP
- Anti Spoofing ورود ACL ها.
- تصدیق مسیریابی.
- غیر فعال نمودن سرویس Finger
- استفاده از پیکربندی NTP امن
- تنظیمBanner های Login

- غیر فعال نمودن سرورهای کوچک TCP و UDP
- فقط در رابط‌های (interface) ضروری CDP را فعال کنید.
- غیر فعال نمودن broadcast مستقیم و هدایت شده IP
- غیر فعال نمودن پروکسی ARP
- استفاده Unicast RPF.
- استفاده AAA.
- استفاده از SSH برای دسترسی راه دور امن.

۳- زیر ساخت IDC

۳-۱ لایه فیزیکی

این لایه قابلیت دسترسی به رسانه های فیزیکی(فیبر نوری،...) و همچنین تکنولوژی های انتقال(SONET، ...) را مشخص می کند.

۳-۲ لایه ۲

در حقیقت این لایه ارتباط بین سرور ها و وسایل سرویس دهنده را فراهم می کند.

- حمایت از 802.1s MST
- حمایت از 802.1 wRSTP
- حمایت از uplink fast
- حمایت از loop guard
- حمایت از Uni-Directional link detection

۳-۳ لایه۳

این لایه مسیریابی شبکه را برای سرویس های ارائه شده انجام می دهد.

- ارائه قابلیت static routing
- حمایت از پروتکل Border Gateway Protocol
- حمایت از پروتکل Interior Gateway Protocol
- حمایت از OSPF
- حمایت از EIGRP

۳-۴ برنامه های کاربردی

با توجه به نیاز مشتری هر مرکز داده باید برنامه های کاربردی خاصی را ارائه دهد. تعدادی از برنامه های کاربردی مورد استفاده عبارتند از:

- نرم افزار های کاربردی مانند Back Office
- نرم افزار های پایگاه داده
- سیستم های عامل مانند Windows NT, Linux, Dos, Unix, OS/2

۳-۵ متعادل کننده بار

مرکز داده باید دارای متعادل کننده بار باشد تا ترافیک شبکه را بین سرور ها تقسیم کند. با این روش سرعت انتقال داده در مرکز داده تضمین می شود.

- هر مرکز داده با توجه به تعداد سرور ها و مشخصات کلی زیرساخت آن باید از متعادل کننده های بار مناسب استفاده کند.

۳-۶ سوئیچ های لایه ۲ و ۳

- دارا بودن ظرفیت کافی با توجه به ترافیک شبکه مورد نظر.
- قابلیت متعادل کردن بار.

- حمایت پروتکل OSPF.
- حمایت پروتکل های Multicast.
- حمایت IEEE 802.1Q و VLAN.
- دارا بودن حداقل ۶۴ پورت fast-ethernet.
- دارا بودن حداقل ۲ پورت giga-ethernet .
- قابلیت قرار دادن در rack.

۳-۷ ذخیره سازها

با استفاده از این سرویس ها امکاناتی از قبیل storage to IP و storage to storage فراهم می شود. از این سیستم ها حتماً باید در مواردی که سرویس های پست الکترونیکی با میزبانی اینترنت ارائه می شود، استفاده شود.

- استفاده از چند سیستم خنک کننده و تامین انرژی
- قابلیت حمایت پروتکل SNMP.
- قابلیت اتصال مستقیم به سیستم های پشتیبانی با نوار (tape backup systems).
- قابلیت استفاده و هماهنگی با نرم افزار های ضد ویروس.
- حمایت از سرویس telnet.

۳-۸ سرویس های هوشمند شبکه ای

کاربرد اصلی این سرویس ها در multicast و QoS می باشد. این سرویس‌ها شامل مشخصاتی هستند که باعث اجرا شدن سرویس های برنامه های کاربردی در شبکه می شود. بعنوان مثال می توان از Policy Based Routing(BPR) و PVLANS نام برد. با استفاده از این ویژگی ها امکان اجرای برنامه های کاربردی نظیر IP Telephony و demand video streaming بوجود می آید.

۳-۹ قابلیت تحمل پذیری در برابر خطا

با استفاده از این روش می توان در صورت بروز خطا سیستم را به حالت قبلی بر گرداند.

- فراهم کردن مکانیزمی برای ثبت حالات سیستم با زمان بندی های از پیش تعیین شده .

- امکان برگرداندن تنظیمات سیستم به هر یک از حالات ذخیره شده در صورت بروز خطا.

۴- مدیریت مرکزخدمات داده اینترنتی

۴-۱ توابع مدیریتی

مدیریت خطا: باید در صورت بروز نقصان در مرکز باید امکان اطلاع دادن به مدیر شبکه را فراهم نماید و می تواند از سیستم‌های زیر تشکیل شود.

- اعلام اتوماتیک خطا نظیر Trap
- نمایش اطلاعات مربوطبه تجهیزات مرکز
- تست اتصالات شبکه، حافظه و رابط‌ها
- داشتن سیستمLOG
- عیب‌یابی موضعی در یک مسیر
- سیستم دسته بندی مشکلات
- داشتن سیستم Debug

مدیریت پیکربندی(Configuration): امکانی رافراهم می‌کند که براحتی می‌توان‌پیکربندی‌تجهیزاتIDC را نظارت و کنترل نمود و شامل موارد زیر می باشد:

- امکان baselining تجهیزات
- امکان تصحیح پیکربندی تجهیزات
- برای بازیابی هرچه سریع‌ترامکان دنبال‌کردن‌تغییرات در پیکربندی‌تجهیزات
- مدیریت نسخه‌های نرم افزاری‌موجود

مدیریت حسابرسی: میزان استفاده از سرویسهای ارائه شده را مدیریت کرده و حسابرسی آنها را انجام می دهد.

مدیریت اجرا و عملکرد: بر موارد زیر نظارت کرده و کارایی سیستم را مدیریت می کند.

- با انتقال فریم‌ها، پاکتها و سگمنتها
- پرتکل‌های انتفال
- برنامه‌های کاربردی
- زمان پاسخ‌دهی
- سطح کیفیت (ازسطحی که در قرارداد قید شده پایین تر باشد اخطار دهد)

مدیریت امنیت: مرکز و قلب مدیریت بوده و شامل موارد زیر می باشد:.

- مدیریت پیکربندی مربوط به تجهیزات
- امکان استفاده از سنسورهایIDS
- مدیریت با متدهایی که خود امن هستند مثلSNMP نسخه ۳
- امکان مدیریت و کنترل LOGها
- پروتکل‌های لازم
- نیروی انسانی

۲-۴ *نوع سرویس مدیریت*

مدیریت out of band

خدمات مدیریتی که با استفاده از یک کانال اختصاصی ارائه می‌گردد و بر روی انتقال داده تاثیر نمی گذارد.

مدیریت in band

مسیر ارائه خدمات مدیریتی مشترک با مسیر دیتا می باشد. در این روش لازم است که مسیر خدمات مدیریتی با استفاده از روشهای IPSec، SSH و SSL امن گردد.

۴-۳ سرویس مانیتورینگ کل سیستم (ESM)

ESM بخشی از سیستم است که نیاز مدیریتی و مانیتورینگ را در سطح انعطاف‌پذیر و قابل گسترش مهیا می‌سازد و دارای ویژگیهای زیر می باشد:

۴-۳-۱ مانیتورینگ سیستم عامل Operating System Monitoring

مانیتور کردن به لحظه مشکلات سرویس‌دهنده می‌باشد. این سرویس با داشتن یک رمز عبور (Password Protected) و بر مبنای مرورگر (Browser – based) امکان دیدن سرویسها را به ما می‌دهد.

۴-۳-۲ اخطار 7*24

اعلام اخطار برای گذشتن از زمان آستانه حق اشتراک با استفاده از پیغام دهنده‌ها و یا E – mail در طول زمان 24*7 .

۴-۳-۳ مانیتورینگ سیستم پیشرفته

این سرویس تمام ویژگیهای مانیتورینگ سیستم عامل بعلاوه جمع‌آوری و ترسیم متریک‌های عملکرد را شامل می‌شود.

۴-۳-۳ مانیتورینگ پروتکل SNMP

با این سرویس تمام ورودیها به سیستم از راه دور مشاهده می‌شود و می‌توان از پیکربندی SNMP آگاه شد.

۴-۳-۵ VPN مدیریت ایمن

با این سرویس شبکه‌های سرویس‌دهنده بطور ایمن مدیریت شده و فضای آدرس‌دهی خصوصی ایجاد می‌شود. تمام مانیتورینگ و مدیریت مخفی‌سازی شده و بوسیله سیستم‌های VPN اختصاصی عبور داده می‌شود.

مانیتورینگ درگاه TCP

این سرویس اتصالات دستگاه به درگاههای TCP معین شده را مانیتور کرده و همچنین یک ارتباط TCP/IP به یک آدرس IP معین یا قلمرو نامی (Domain Name) بوسیله یک دستگاه مشخص برقرار می کند.

مانیتورینگ Ping پروتکلICMP

با این سرویس می‌توان دستگاههای شبکه را با استفاده از پروتکلهای استاندارد EchoRequest/ Echo Reply ICMPمانیتور کرد. سیستم‌ها هرپنج دقیقه یکبار تست شده و با ایجاد مشکل اخطار داده می‌شود.

۴-۴ تقسیم محدوده مدیریت مرکز خدمات

در مراکزخدمات داده اینترنتی سرویس مدیریت را می توان درمحدوده‌هایی (Domain) مطابق زیر تعریف کرد.

- تقسیم محدوده‌ها بر اساس فاصله جغرافیایی و یا تقسیم توابع کاربردی می باشد.

- هرمحدوده نیاز به سیستم جمع آوری اطلاعات و مدیریت مجزا دارد.
- این سیستم های مدیریت با یکدیگر در ارتباط بوده و تبادل اطلاعات می کنند.

۴-۵ مدیریت قراردادها و تضمین سطح خدمات

مرکزخدمات داده اینترنتی موظف است سطح خدماتی را که ارائه می دهد مدیریت نموده تا از سطحی که در قرادادها تضمین نموده کمتر نباشد. حداقل سرویسی که در سیستم مدیریت قرادادهاو تضمین سطح نیاز داردبه شرح زیر می باشد.

- برای هر سرویس به مشتری، سطح آن سرویس (SLA) را تعیین و مشخص کند.
- برای هر مشتری به تعداد سرویسهایی که ارائه می دهد SLA نیازمی باشد.
- مجموع SLAها را در قالب قراردادی که SLC نامیده می شودتنظیم کند.
- نیاز به سیستم مدیریتی می باشدکه این SLAها و SLCها را مدیریت کند

۵ - اتصالات در لبه اینترنت

۵-۱ ایجاد پهنای باند

در این سرویس نیاز به فراهم کردن پهنای باندهای متنوعی با سرعتهای مختلف می‌باشد.

- ارائه پهنای باند از طریق پروتکلهای WAN و MAN مثل ATM
- امکان اتصال با تکنولوژیهایEthernet با سرعتهای زیر
  - اتصالات Ethernet با پهنای باند 10Mbps
  - اتصالات Fast Ethernet با پهنای باند 100Mbps
  - تکنولوژی جدید Giga Ethernet با پهنای باند 1000Mb

۵-۲ سرویس چند خطه

این سرویس افزایش اطمینان و اتصال شبکه را از طریق چندین اتصال (up link) ایجاد می‌کند تا که هر زمان یکی از اتصالات قطع شد اتصال به شبکه از طریق خطوط دیگر برقرار شود.

۵-۳ سرویسهای دستیابی به اینترنت

این سرویسها دسترسی کامل با سرعتهای ۱/۵۴ Mbps تا ۴۵ Mbps را توانا ساخته و شامل ویژگیهای زیر می‌باشند:

- اتصالات T1 یا DS3 اختصاصی
- سرویسهای Flat Rate و Usage – based
- مانیتورینگ خط بطور شبانه‌روزی در هفته
- تهیه مدار Circuit Provisioning
- عیب‌یابی خطوط معیوب
- هماهنگی شرکت Telco برای مدارهای معیوب
- سرویسهای DNS

۵-۴ سرویس اتصال از راه دور

این سرویس دسترسی مشتریان از شرکتشان به IDC را از راه دور فراهم می‌سازد و شامل موارد زیر می‌باشد:

- تست و تعمیر و نگهداری خط
- ابزارهای شامل Patch Panel ها، کابلهای Cross – Connect و دستگاههای آزمایش و فیبر
- عیب‌یابی خطوط در زمان قطع
- هماهنگی با شرکت مخابرات در زمان قطع مدار
- سازگار کردن آدرسهای IP با سیاست IP ، IDC مورد نظر

۵-۵ سرویس گزارش‌های پهنای باند

این سرویس یک نمایش وب‌گونه و همراه با رمز عبور از میزان استفاده پهنای باند مشتریان فراهم می‌آورد. که این اطلاعات بطور روزانه و ماهانه می‌باشد ویژگیهای زیر را شامل می‌شود:

- جدول خلاصه‌ای از آمارهای ترافیک شبکه
- نمودارهای گرافیکی از آمارهای پهنای باند
- فهرست‌بندی جزییات اطلاعات

۵- ۶ امکان اتصال از طریق VPN

این سرویس به ساخت یک VPN بهینه برای محیط IDC کمک می کند .

- **سرویسهای دروازه به دروازه VPN**

این سرویس نیازهای امنیتی دروازه VPN (VPN Gateway)را توسعه و تعریف می‌کند. پس از آن به مدیریت و نصب آن می‌پردازد که شامل موارد زیر می‌باشد.

- **سرویسهای نرم‌افزاری دروازه VPN**

این سرویس یک ارتباط ایمن بین IDC و یک نقطه خارج از IDC با تکنولوژی پنهان‌سازی تولید می‌کند.

- **سرویسهای سخت افزاری دروازه VPN**

این سرویس ارتباطی ایمن، قابل انعطاف و با سرعت بالا برای شبکه‌هایی در سطح گسترده فراهم می‌آورد.

۵-۷ امکان اتصال با شبکه PSTN

سرویس اتصال از راه دوراتصال به شبکه زیرساخت مرکزخدمات داده اینترنتی ازراه دوروازطریق شبکه تلفن را فراهم می کند. در طراحی این اتصال رعایت نکات زیرالزامی است:

- تعداد خطوط ارتباطی متناسب با تعداد کاربرهای پیش بینی شده
- برای امنیت از سرورهای دسترسی از راه دور (remote access server) مناسب مثل RADIUS استفاده شود
- برای دسترسی هرچه سریعتر از تعادل بار در سرورهای دسترسی از راه دور استفاده شود.
- برای بازیابی از حوادث از سرورهای افزوده استفاده گردد (Redundancy)

۶- سرویسهای مرکزخدمات داده اینترنتی

۶-۱ سرویس های عمومی

هر مرکز داده علاوه بر سرویس های خاص که با درخواست کاربر ارائه می دهد باید سرویس های عمومی زیر را نیز ارائه دهد:

۶-۱-۱ سرویس مدیریت شبکه

ارائه قابلیت کنترل مرکزی و مونیتورینگ تجهیزات.

۶-۱-۲ سرویس web hosting

قابلیت دسترسی به شبکه با این سرویس فراهم می شود. برای جستجو می‌توان از موتور های جستجوی رایج استفاده کرد. این سرویس باید مشخصات زیر را داشته باشد:

- حمایت پروتکل HTTP 1.1
- حمایت java و CGI.
- حمایت .HTTP compression
- حمایت SNMP برای کارهای مدیریتی.
- حمایت SSLو TLS.
- قابلیت ذخیره تمام تراکنش ها.
- قابلیت مقابله در برابر حمله های ویروسی.

۶-۱-۳ سرویس DNS

این سرویس یک نام معادل به هر IP نسبت می دهد.

۶-۱-۴ سرویس پست الکترونیکی

با استفاده از این سرویس خدمات پست الکترونیک به کاربران ارائه می شود.

۶-۱-۵ سرویسCaching

با استفاده از این سرویس پهنای باند قابل ملاحظه ای از gateway اینترنت صرفه جویی می شود.

- این سیستم باید دارای واسط fast Ethernet یا gigabit Ethernet باشد.
- خاصیت transparency در شبکه باید رعایت شود.

- تمام تراکنش ها باید در فایل ثبت شود.
- سیستم باید پروتکل web cache communication (WCCP-v2) را حمایت کند.

۶-۱-۶ سرویس FTP

- ظرفیت قابل قبول با توجه به مشخصات سیستم.
- حمایت پروتکل secure copy protocol
- حمایت تعیین هموت رمزگذاری شده (encrypted authentication)

۶-۱-۷ سرویس Chat

- قابلیت فیلتر کردن کلمات مورد نظر.
- قابلیت جلوگیری از اتصال کاربر مورد نظر.
- قابلیت اتصال به اینترنت با واسطه java.
- قابلیت تایید هویت کاربران.

۶-۲ خدمات Colocation.

برای ارائه خدمات Collocation نیاز است که IDC شرایط زیر را فراهم کند:

- سیستم برق بدون وقفه (UPS) و مولد برق اضطراری یا ژنراتور با قابلیت تامین برق مورد نیاز:
- پهنای باند کافی
- سیستمهای کنترل دما و رطوبت و تهویه HVAC
- سیستم Grounding قوی برای مقابله با مشکلات ESD و نویز Rack ها
- دارای افراد متخصص برای نصب و راه اندازی و تعمیرات تجهیزات مرکز دیتا
- فراهم کردن فضای Rack مناسب برای نصب تجهیزات و Server ها

۳-۶ خدمات پشتیبانی(Help Desk):

خدمات پشتیبانی برای انعکاس نظرات مشتریان و در نهایت بهبود خدمات و رفع سریع مشکلات ارائه می گردد که حداقل دارای مشخصات زیر می باشد.

- ارائه خدمات ۲۴*۷ (هفت روز هفته بصورت شبانه روزی).
- حضور متخصص برای رفع مشکلات فنی کاربران از راه دور.
- حضور متخصص برای رفع مشکلات سخت افزاری و نرم افزاری پیش آمده در مرکز داده در تمام ساعات شبانه روز.

Glossary

802.x: A set of standards developed by the IEEE.

A:
AAA: Authentication, Authorization, and Accounting
ACL: Access control list
ARP: Address Resolution Protocol.
ACS: Access Control Server.

B:
BGP: Border Gateway Protocol.
BPR: Business Process Reengineering

C:
CDP: Cisco Discovery Protocol.
CGI: Common Gateway Interface

D:
DNS: Domain Name Server.
DS3: dialup service 3
DSNIFF: It is a collection of tools for network auditing and penetration testing

E:
EIGPRP: Enhanced Interior Gateway Routing Protocol.
EMS: Enterprise Management System.
ESD:

F:
FCAPS: Fault, Configuration, Accounting, Performance and Security.

H:
HTTP: Hyper Text Transfer protocol.
HVAC: Heating Ventilation and Air Conditioning.

I:

IDC: Internet Data Center.

IDS: Intrusion Detection System.

IOS: Internetwork Operating System.

IP: Internet Protocol.

IPsec: IP Security Protocol efforts in the IETF (Internet Engineering Task Force).

M:

MAN: Metropolitan Area Network.

N:

NAS: Network Attached Storage

NMAP: Network Mapper

NTP: Network Time Protocol.

O:

OSPF: Open Shortest Path First.

P:

PSTN: Public Switched Telephone Network.

PVLAN: Private Virtual Local Area Network.

Q:

QoS: Quality Of Services.

R:

RADIUS: Remote Access Dial-In User Server.

RFP: Request Of Proposal

S:

SAN: Storage Area Networks.

SLA: Service Level Agreement.

SLC: Service Level Contract

SNMP: Simple Network Management Protocol.

SONET: Synchronous Optical Network.

T:

TACACS+: Terminal Access Controller Access Control System.

TCP: Transfer Control Protocol.

TLS: Transport Layer Security.

U:

UPS: uninterruptible power supplies.

V:

VACL: Virtual LAN Access Control List.

VPN: Virtual Private Network.

W:

WAN: Wide Area Network.

WCCP: Web Cache Communication Protocol.

فهرست مطالب: