راه‌کارهای امنیتی مراکز داده

هومن مرجانی، مهدی حولکیان

چکیده: مراکز داده مجموعه‌ای از تجهیزات است که برای ذخیره‌سازی داده، مدیریت و پخش اطلاعات سازمان داده شده برای صنایع و شرکت‌های خصوصی و دولتی به‌کار می‌رود و می‌تواند به‌صورت مجازی یا فیزیکی وجود داشته باشد. به‌صورت فیزیکی مراکز داده‌ها، میزبان سیستم‌های کامپیوتری و زیرساختاری شامل سیستم‌های ذخیره‌سازی دیتا، ارتباطات و اتصالات دیتا، تجهیزات میزبان و حمایتی، واحدهای توزیع برق، سیستم‌های پشتیبان نیرو، سیستم‌های محیطی، سیستم‌های اطفاء حریق و سیستم‌های امنیتی هستند

کلمات کلیدی: مراکز داده، شبکه‌های مراکز داده، بحران مراکز داده، بازیابی مراکز داده.

مقدمه: امروزه در ایران نیز مانند سایر کشورهای جهان، نیاز به داشتن فضایی برای ذخیره اطلاعات موجود و مدیریت داده‌ها، برای بخش خصوصی و دولتی یک الزام محسوب می‌شود و با رشد قابل توجهی رو به رو است. مراکز داده ابزار با ارزشی در تکنولوژی‌های نوین، مدیریت و امنیت هستند. از آنجایی که فعالیت‌های کلاهبرداری و فریب‌کاری به‌صورت فزاینده‌ای افزایش یافته است، بنابراین امنیت اطلاعات بسیار مهم بوده و ایجاد حفاظی در اطراف سیستم‌ها، کاربردها و داده‌ها کار آسانی نیست. از آنجایی که تهدیدها از طریق هکرها یا نرم‌افزارهای بداندیش یا از اشخاصی که دسترسی اجازه داده شده به سرورها و سخت‌افزارها را ندارند، ناشی می‌شود، بنابراین ایمنی و امنیت محلی که برای نگهداری، حفظ و دسته‌بندی اطلاعات به‌کار می‌رود، از دغدغه‌های اصلی هر سازمانی است. و سرورهای میزبانی مراکز داده و Co-location راه حل‌های بسیار خوبی برای حفاظت و پاسخگویی به چالش‌های ایمنی، سخت‌افزارهای فیزیکی و کاربردهای نرم‌افزاری و اطلاعات ثبت شده هستند. مزایای بسیاری برای انتخاب یک مرکز داده با کیفیت بالا به‌عنوان یک راه‌حل IT وجود دارد. امنیت تجهیزات و داده باعث پیشگیری از حملات بداندیش malicious attack و تقلب‌ها می‌شود. برای داشتن ایمنی و امنیت نیاز به سنجش‌های کنترلی بیشتری مانند onsite monitoring است و از آنجایی که مراکز داده بخش حیاتی برای هر سازمان است، بنابراین بایستی بیشتر مورد پایش قرار گیرد تا از تهدیدات امنیتی محافظت شود.

1- ملاحظات ساختاری و تجهیزاتی در مراکز داده

1-1- فضاهای مورد نیاز ارتباطات مراکز داده و توپولوژی‌های مرتبط

فضاهای معمولی که در یک مراکز داده وجود دارند، به شرح هستند.

- Network Operation Center
- Entrance Room
- Main Distribution Area
- Horizontal Distribution Area
- Equipment Distribution Area

- Network Attached Storage
- Storage Area Networks
- Tape Storage / Virtual tape Library

البته باید توجه داشت بسته به اندازه مراکز داده، تمامی این فضاها لازم نیستند. برای حصول اطمینان از کارکرد صحیح هر مرکز داده‌ای باید ساختار فیزیکی آن از لحاظ کلیه شرایط محیطی، فیزیکی، ارتباطی، الکتریکی و مکانیکی مطابق استاندارد باشد.
اولین و کامل‌ترین استانداردی که برای مراکز داده‌ها در این زمینه وجود دارد، استاندارد TIA 942 است. در این استاندارد به کلیه موارد مذکور اشاره شده است و در آن میزان دسترس‌پذیر بودن مراکز داده در 4 سطح مطرح شده است که برای اطمینان از بالاترین سطح دسترس‌پذیر بودن مراکز داده، آخرین سطح در نظر گرفته می‌شود.
در هر مراکز داده‌ای ابعاد زیر مطرح هستند:

- افزونگی
- نیازمندی‌های ارتباطی
- نیازمندی‌های معماری و ساختاری
- نیازمندی‌های سیستم‌های الکتریکی
- نیازمندی‌های سیستم‌های مکانیکی

استاندارد TIA 942 برای 4 سطح معرفی می‌شود که وابسته به سطوح مختلف دسترس‌پذیری زیر ساختار تسهیلات مراکز داده است. برای سطوح بالاتر به همان اندازه که دسترس‌پذیری بیشتری دارند، قیمت‌های ساخت مراکز داده مبتنی بر آن‌ها نیز بالاتر است. سطوح بالاتر شامل موارد مطرح در سطوح پایین‌تر هم می‌شوند. باید توجه داشت که یک مراکز داده در بخش‌های مختلف خود می‌تواند از سطوح مختلف این استاندارد استفاده کند و این امر کاملاً بستگی به کاربرد و سیاست‌هایی دارد که مراکز داده به منظور آن ساخته می‌شوند. هر 4 سطح باید در ابعاد پنج‌گانه فوق الذکر در نظر گرفته شوند.

1-2- افزونگی در سطح 4

افزونگی در این سطح، مقاوم به تحمل خطا است، زیرا باید بتواند ظرفیت زیرساختار سایت و قابلیت‌های آن را بدون وقفه در بارهای بحرانی حفظ کرده و به کار خود ادامه دهد. بنابراین، دارای چند منبع تغذیه فعال و چندین تغذیه ورودی برای تجهیزات و چندین مسیر توزیع‌کننده خنک‌کنندگی بوده و مسیرهای توزیع فعالی به‌صورت همزمان، در هر سیستم و هر پیکربندی وجود دارد و امکان توقف فعالیت در صورت آلارم‌های آتش یا فرمان قطع اضطراری به‌صورت دستی باید وجود داشته باشد.

1-3- نیازمندی‌های ارتباطی در سطح 4

در سطح 4 باید نیازمندی‌های سطح 3 برآورده شود و کابل‌کشی‌ها حفاظت شده باشند و در مورد کابل کشی backbone باید Redundant باشد. پشتیبان‌ها باید موجود بوده و اتصالات اجزا به پشتیبان‌هایشان، باید وجود داشته باشند. مراکز داده باید یک Distribution اصلی و یک Distribution Area فرعی با حداقل 20 متر فاصله از هم، و میان این دو نیز باید pathway وجود داشته باشد و ترجیحاً در دو انتهای مقابل مراکز داده باشد. سوئیچ‌ها و روترهای توزیع Redundant میان این دو توزیع شده باشند. سیستم‌های حیاتی باید به دو Horizontal Distribution Area به‌صورت Redundant کابل‌کشی شده باشند.

1-4- نیازمندی‌های معماری و ساختاری در سطح 4

از دید معماری نصب مراکز داده در سطح 4 باید کلیه نیازمندی‌های سطح 3 را پوشش دهد و علاوه بر آن نیازمندی‌های اضافه‌ای که در ضمیمه G از این استاندارد به ان اشاره شده است را نیز در نظر بگیرد. در این نوع مراکز داده باید در برابر کلیه اتفاقات فیزیکی بالقوه، اتفاقات طبیعی یا اتفاقاتی که منشا انسانی دارند، حفاظت‌های Redundant درنظر گرفته شود و مراکز داده باید بر کلیه تسهیلات و تجهیزات خود کنترل داشته باشند. در ضمن باید یک پد ژنراتور امن در فضایی در ساختمان دیگر یا فضایی خارج

از محیط مراکز داده برای تانکرهای سوخت تعبیه شود و تا حد امکان نزدیک ژنراتور باشند. حداقل بار قابل تحمل نیز مطابق ضمیمه G از این استاندارد باشد.

1-5- نیازمندی‌های الکتریکی در سطح 4

از دید الکتریکی نصب مراکز داده در سطح 4 باید کلیه نیازمندی‌های سطح 3 را پوشش دهد و علاوه بر آن نیازمندی‌های اضافه‌ای که در ضمیمه G از این استاندارد به آن اشاره شده است را نیز در نظر بگیرد. کلیه تسهیلات در سطح 4 باید به‌صورت پیکربندی 2(N+1) در تمامی ماژول‌ها، سیستم‌ها و pathwayها طراحی شوند. کلیه خطوط تغذیه باید قابلیت بای پس به‌صورت دستی برای هدف نگهداری یا در شرایط خطا را داشته باشد. سیستم مانیتورینگ باطری با قابلیت مانیتورینگ امپدانس و دمای ظرف باطری و آلارم دادن خطای قریب‌الوقوع باطری را داشته باشد. پست‌های انشعاب برق باید از تسهیلات غیربحرانی مجزا شوند و ساختمان باید حداقل دارای دو تاسیسات خطوط تغذیه باشد.

1-6- نیازمندی‌های مکانیکی در سطح 4

سیستم HVAC در سطح 4 باید شامل واحدهای تهویه هوا با ظرفیت خنک‌کنندگی به منظور نگاه داشتن دما و رطوبت مورد نیاز باشند. وقتی سیستم‌های تبخیری برای این نوع در نظر گرفته می‌شوند، باید منابع جایگزین از ذخیره آب در نظر گرفته شود.

2- اهمیت امنیت در شبکه‌های مراکز داده

نظر به اهمیت راهبردی مراکز داده در حفظ و نگهداری اطلاعات و برنامه‌های حساس و مهم، این قبیل اطلاعات آماج حملات و تلاش برای دسترسی‌های غیرمجاز قرار می‌گیرد. دو بخش اصلی این مراکز یعنی شبکه‌های LAN و شبکه‌های SAN ساختارهای خاص و در نتیجه ملاحظات ویژه‌ای برای حفظ امنیت دارند. عمدتاً دو نوع اساسی حمله در مراکز داده مطرح می‌شود: Data Theft یا دزدی اطلاعات و Worm Propagation یا انتشار کرم. در نوع اول، اطلاعات مرکز مورد دستبرد قرار می‌گیرد و در نوع دوم، برنامه‌ها و اطلاعات غیرقابل دسترس می‌شوند که نوعی حمله DOS است.

2-1- انواع حملات در مراکز داده

الف - **حمله دزدی اطلاعات :** این حمله در دو مرحله انجام می‌گیرد. در مرحله اول با کاوش و بررسی هدف، اطلاعات لازم برای شناخت ویژگی‌های سیستم هدف به‌دست می‌آید. درمرحله دوم، حمله‌کننده نقاط آسیب‌پذیر سیستم هدف را شناسایی کرده و با نصب بخشی از نرم‌افزار در سیستم میزبان به انجام عملیات غیرمجاز پرداخته وکنترل سرور را برای دستیابی به سیستم‌های دیگر به‌دست می‌گیرد.

ب - **حمله انتشار کرم :** دراین نوع حمله حجم زیاد ترافیک و درخواست‌های غیر واقعی به سمت سیستم هدف ارسال می‌شود. لذا به‌دلیل تقاضای ارتباط زیاد و بیش از حد توان سرور سیستم، دسترسی متقاضیان واقعی به سیستم مختل یا امکان‌ناپذیر می‌شود. کرم‌ها امکان تکثیر سریع و خودکار، بدون دخالت انسان دارند و باعث پیچیده‌تر شدن شرایط بحرانی می‌شوند. به‌عنوان مثال کرم SQL Slammer هر 8/5 ثانیه دو برابر می‌شود. به‌دلیل آسیب‌پذیری بسیاری از سیستم عامل‌ها و در دسترس بودن آسان ابزارهای حمله، حفاظت تجهیزات داخلی و برنامه‌ها و اطلاعات، در مراکز داده بسیار ضروری است.

3- بحران در مراکز داده

حوادث احتمالی که مراکز داده با آنها مواجه هستند به دو دسته کلی تقسیم می‌شوند :

1- حوادث ناشی از بلایای طبیعی : مانند آتش‌سوزی، سیل ، طوفان، گردباد، زلزله، آتشفشان و ...

2- حوادث ناشی از دخالت انسان : مانند خراب‌کاری، تروریسم، شورش و آشوب، ایجاد خسارت توسط پرسنل و هر موردی که باعث تخریب و نقصان در عملکرد نرمال پردازش اطلاعات می‌شود.

3-1- بازیابی مراکز داده در اثر سوانح

هدف نهایی در بازیابی مرکز داده در اثر سوانح، رسیدن به زمان Down time صفر است. برای رسیدن به این هدف 3 رده کلی تعیین شده است :

Disaster Recovery : یعنی حفاظت از داده‌ها از طریق ایجاد نسخه پشتیبان و رونوشت از اطلاعات

Business Continuance : بازگرداندن سیستم به حالت قبل، بعد از بروز هرگونه خطا

Business Resilience : عملکرد بدون وقفه در خلال بروز خطا

طرح‌ریزی بازیابی مراکز داده در حوادث غیر مترقبه در 3 مرحله انجام می‌شود :

1- تحلیل تاثیر حوادث غیر مترقبه بر عملکرد، شامل تعیین انواع تاثیرات ناشی از حوادث مختلف بر عملکرد سیستم و تجهیزات و دارایی‌ها

2- تحلیل ریسک، شامل تعیین عملکردها و دارایی‌های حیاتی که سیستم باید در زمان بروز حوادث با اولویت بالا از آنها پشتیبانی کند.

3- ایجاد طرح بازیابی سیستم در زمان بروز حوادث غیر مترقبه شامل ایجاد قابلیت بازیابی سیستم، کاربردها و سایر موارد در مراکز ثانویه بعد از بروز حوادث غیر مترقبه. اهداف بازیابی مراکز داده در صورت بروز حوادث غیر مترقبه، شامل تعیین نقطه بازیابی، یعنی زمانی که قبل از آن زمان سیستم و داده‌ها باید بازیابی شوند و تعیین مدت زمان بازیابی به معنی محدوده زمانی و حداکثر زمان قابل قبول برای انجام بازیابی اطلاعات است.

2-3 انواع طراحی مراکز داده با در نظر گرفتن مدیریت بحران

1-2-3 طراحی به‌صورت Warm Standby : در این حالت مرکز داده به سخت‌افزار و واسطهایی از شبکه مخابراتی مجهز می‌شود تا امکان پشتیبانی از تهیه نسخه پشتیبان را داشته باشد. آخرین نسخه پشتیبان باید همواره به‌صورت امن نگهداری شود. تجهیزات دسترسی به شبکه باید فعال شده باشند.

2-2-3 طراحی به‌صورت Hot Standby : مرکز داده در این حالت دارای سخت‌افزار و نرم‌افزارهای لازم جهت ارائه سرویس‌های پردازش داده با حداقل زمان Down Time است. وجود نسخه پشتیبان به‌صورت Hot به بازیابی اطلاعات با حداقل مداخله یا عدم مداخله انسانی کمک می‌کند. یک سایت پشتیبانی Hot باعث بهبود زمان‌های آماده‌سازی و ریکاوری قبل و بعد از بروز رخداد شده که این امر باعث عملکرد بی وقفه سرویس‌ها می‌شود.

4- نکاتی مهم در بازیابی مراکز داده در مدیریت بحران

مکانیزم‌های انتخاب مکان سایت شامل: مکانیزم‌های انتخاب مکان مرکز داده بسته به نوع تکنولوژی یا ترکیبی از تکنولوژی‌ها براساس روتینگ در یکی از سه حالت:

الف) HTTP Redirect

ب) DNS Based

ج) L3 Routing With Route Health Injection

توانایی و قدرت سرورها باید محاسبه شود و دیگر شاخص‌های اختیاری مانند بار شبکه و تجهیزات باید برای رسیدن به انتخاب درست در نظر گرفته شوند.

چینش سرورها به‌منظور بالا بردن سطح دسترسی با روش Clustering یا خوشه‌بندی. خوشه‌بندی دارای منافعی از جمله دسترسی‌پذیری، قابلیت اطمینان، مقیاس‌پذیری و قابلیت مدیریت بهتر است. خوشه با دسترسی بالا چندین کپی از کاربردها با دسترسی خواندن و نوشتن اطلاعات را دارا است. همچنین خوشه‌بندی به‌منظور بالانس بار بر روی سرورها نیز مورد استفاده قرار می‌گیرد.

برای رسیدن به دسترسی بالا، خوشه‌بندی به 3حالت عملیات تقسیم‌بندی شبکه را انجام می‌دهد:

الف) شبکه عمومی

ب) شبکه خصوصی
ج) بخش ذخیره اطلاعات
برای بالابردن دسترسی کاربردها در 4 حالت می‌توان تجهیزات را مدیریت کرد:

Active / Standby
Active / Active
Shared Everything
Shared Nothing

نتیجه‌گیری : در این مقاله ما ابتدا به معرفی کلی مراکز داده پرداختیم و سپس راهکارهای امنیتی مراکز داده مورد بررسی قرار گرفت. سپس فضاهای مورد نیاز ارتباطات مراکز داده و توپولوژی‌های مرتبط معرفی شدند که به‌منظور حصول اطمینان از کارکرد صحیح هر مرکز داده ای باید ساختار فیزیکی آن از لحاظ کلیه شرایط محیطی، فیزیکی، ارتباطی، الکتریکی و مکانیکی مطابق استاندارد باشد. در انتها نیز استاندارد TIA 942 معرفی شد که در این استاندارد از لحاظ میزان دسترس‌پذیر بودن، مرکز داده در 4 سطح مطرح شده است که برای اطمینان از بالاترین سطح دسترس‌پذیر بودن مرکز داده، آخرین سطح در نظر گرفته می‌شود.

منابع:

[1] ANSI/TIA-942
[2] Cisco," Data Center High Availability Clusters Design Guide", Cisco corporation,2006.
[3] R.Cocchiara, H.Davis, D.Kinnaird,” Data center topologies for mission-critical business systems”, IBM SYSTEMS JOURNAL, VOL 47, NO 4, 2008, pp.695-706.