طراحی مراکز داده با رویکرد پدافند غیر عامل

علی محمدی[1]

محمدرضا موحدی صفت[2]

چکیده:

مراکز داده[3] به عنوان قلب تپنده زیرساخت‌های فن‌آوری اطلاعات یک کشور هستند و از این رو نقش مهمی در امنیت یک کشور می‌توانند داشته باشند. با به خطر افتادن امنیت یک مرکز داده سرویس‌های حیاتی مبتنی بر آن به مخاطره می‌افتد.

با توجه به روند رو به رشد و سرعت گسترش فناوری اطلاعات در کشور ما، در حال حاضر لزوم ایجاد و توسعه مراکز داده امری اجتناب ناپذیر است. از سویی لحاظ نمودن ملاحظات پدافند غیرعامل[4] و امنیت در طراحی و پیاده سازی این مراکز بسیار ضروریست.

در این مقاله مدلی بومی جهت لحاظ نمودن ملاحظات پدافند غیر عامل و امنیت در این مراکز ارائه گردیده است. در این مدل ضمن سطح بندی مراکز داده به ۳ رده مهم، حساس و حیاتی، کنترل های لازم متناسب با هر سطح مرکز داده ارائه گردیده است.

واژهای کلیدی: مرکز داده، پدافند غیرعامل، تهدیدات مراکز داده، سطوح مراکز داده، الگوی بومی مراکز داده

---

[1] دانشجوی دکتری امنیت شبکه و عضو دانشگاه عالی دفاع ملی

[2] پژوهشگر ارشد امنیت شبکه و عضو هیات علمی دانشگاه عالی دفاع ملی

[3] Data Centers

[4] Passive Defense

مقدمه

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش و از سوی دیگر پیامدهای بحران را کاهش می دهد و امکان بازسازی مناطق آسیب‌دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

منظور از پدافند غیرعامل در واقع مجموعه تمهیدات و اقدامات و طرح هایی است که با استفاده از ابزار، شرایط و حتی المقدور بدون نیاز به نیروی انسانی بصورت خود اتکا، از یک سو توان دفاعی مجموعه را در زمان بحران افزایش می دهد واز سویی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می سازد (عابدینی-۱۳۸۶-۵).

طراحی و تدوین راهبرد پدافند غیرعامل کشور نیازمند یک نگاه جامع و دقیق است. دراین رابطه می باید ابتدا محیط ملی و داخلی را از نظر نقاط ضعف و قوت بررسی نموده و سپس محیط بین الملل شامل تهدیدات و فرصت ها را بررسی کرد و بعد از آن به برآورد راهبردی تهدید پرداخت. با تجزیه و تحلیل نقاط ضعف و قوت، تهدید و فرصت، تعیین اهداف راهبردی وکلان راهبرد مورد نظر را تدوین نمود. در این رابطه توجه به مؤلفه های اقتصادی و فرهنگی از اهمیت ویژهای برخوردار است (جلالی-۱۳۸۵-۴).

بیان مساله و اهمیت تحقیق

در این تحقیق ابتدا به صورت خلاصه به تعاریف، تاریخچه و وضعیت مرکز داده در ایران و جهان پرداخته شده است. سپس مروری بر معماری ها و استانداردهای مطرح مراکز داده شده و در ادامه تهدیدات متصور برای مراکز داده کشور با رویکرد پدافند غیرعامل دسته بندی گردیده است. این تهدیدات در ۳ حوزه ۱-تهدیدات ناشی از جنگ

(سایبر و فیزیکی) و مخاصمات بین المللی ۲- تهدیدات امنیتی ۳- تهدیدات محیطی و طبیعی، مورد توجه قرار گرفته است. در نهایت در ادامه مدلی برای لحاظ نمودن ملاحظات پدافند غیر عامل و امنیت در طراحی و پیاده سازی مراکز داده بومی کشور آورده شده است. در این مدل، ملاحظات پدافند غیر عامل به ۳ سطح بالا، میانی و پایین تقسیم بندی شده است. در ملاحظات سطح بالا، پارامترهای سطح بندی مراکز داده کشور و تعیین یکی از سطوح مهم، حساس یا حیاتی بیان می گردد. در ملاحظات سطح میانی، کنترل های پدافند غیر عامل و امنیتی متناسب با تهدیدات مشخص می شود و به تفکیک برای هر یک از سطوح مراکز داده مهم، حساس و حیاتی در قالب کنترل های سطح میانی بیان می گردد. و در نهایت در ملاحظات سطح پایین مراکز داده نیز موارد فنی پدافند غیر عامل و امنیت مرتبط با تجهیزات و تکنولوژی ها بررسی می گردد. ملاحظات سطح بالا و میانی برای همه مراکز داده کشور مشترک بوده و در قالب سندی بالادستی تدوین گردیده است. اما از آنجا که ملاحظات سطح پایین وابسته به محصولات و تکنولوژی ها می باشد و دائم در حال تغییر است، از سویی در هر مرکز داده خاص متفاوت خواهد بود، در زمان طراحی و پیاده سازی آن مرکز داده، باید با توجه به ملاحظات سطح بالا و میانی که در سند بالا دستی بیان شده است، با نظارت سازمان پدافند غیر عامل تعیین و اجرا گردند.

ضرورت تحقیق

با توجه به نقش، اهمیت و حساسیت مراکز داده در کشور لازم بود این موضوع به صورت ریشه ای و اصولی و از ابعاد مختلف مورد بررسی قرار می گرفت. از سویی تهدیدات متصور در این حوزه در حال حاضر برای کشور ما بسیار زیاد است و ابعاد مختلفی نیز دارد. لذا با نگاهی فراتر از یک نگاه سازمانی، بلکه با نگاهی ملی باید به این موضوع نگریسته می شده و ابعاد مختلف تهدیدات بررسی و راهکارهای عملی و اجرایی متناسب ارائه می گردید.

در این تحقیق سعی گردیده ضمن ارائه مدلی بئمی، راهکارهای لازم متناسب با سطح و اهمیت هر مرکز داده ارائه گردد.

هدف تحقیق

هدف از انجام این تحقیق ارائه مدلی بومی به منظور لحاظ نمودن ملاحظات پدافند غیر عامل در طراحی و ساخت مراکز داده در کشور می باشد.

سوال تحقیق

آیا در طراحی و پیاده سازی مراکز داده کشور کلیه ملاحظات پدافند غیر عامل و امنیت در نظر گرفته می شود و رعایت می گردند؟

روش تحقیق

روش تحقیق حاضر از نوع توصیفی-اکتشافی است و برای تحلیل اطلاعات جمع آوری شده از روش تحلیل فرآیند محیطی بهره گیری شده است.

تعاریف

مرکز داده:

مرکز داده مکانی است:با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی و جهانی، با خدمات تمام وقت و در دسترس.

- دارای انواع تجهیزات سخت‌افزاری(رایانه‌ها، سوییچ ها، مودم‌ها، مسیر یاب‌ها[1]و...) و نرم‌افزاری(پایگاه های داده، سامانه های عامل و ...) پیشرفته که از پشتیبانی و نگهداری حرفه‌ای و تمام وقت برخوردار است.

- به پشتیبانی و ارائه انواع خدمات مرتبط با اطلاعات و داده‌ها از قبیل خدمات ذخیره، نگهداری و بازیابی داده‌ها، ERP، میزبانی خدمات اینترنتی (ISP)، میزبانی خدمات کاربردی (ASP)، میزبانی برون‌سپاری[2] خدمات و غیره برای کلیه اشخاص حقوقی و حقیقی دولتی و غیر دولتی می‌پردازد(IDC Org-۲۰۰۷-۱).

مراکز حیاتی[1] مراکزی هستند که انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری در سراسر کشور گردد.

مراکز حساس[2] مراکزی هستند که انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل‌توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی

---

[1] Routers

[2] Outsourcing

تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیر گذاری منطقه‌ای در بخشی از کشور گردد.

مراکز مهم[3] مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیر گذاری محلی در کشور وارد می‌گردد.

مزایای مراکز داده

- امنیت فیزیکی بالا
- امنیت الکترونیکی بالا
- مقابله با افزونگی و تکرار اطلاعات
- ارائهٔ بالاترین سرعت پردازش در یک مکان
- ارائهٔ بالاترین سرعت انتقال اطلاعات
- خرید تنها یک نسخه از نرم‌افزارها
- پشتیبانی متمرکز

معیارهای طراحی مراکز داده

معیارهای طراحی برای هرکدام از سرویس های ارائه شده در مرکز داده عبارتند از(Tippu-۲۰۰۷-۱):

- قابلیت دسترسی بالا
- توسعه پذیری
- امنیت
- قابلیت مدیریت

---

[1] Vital Centers
[2] Critical Centers
[3] Important Centers

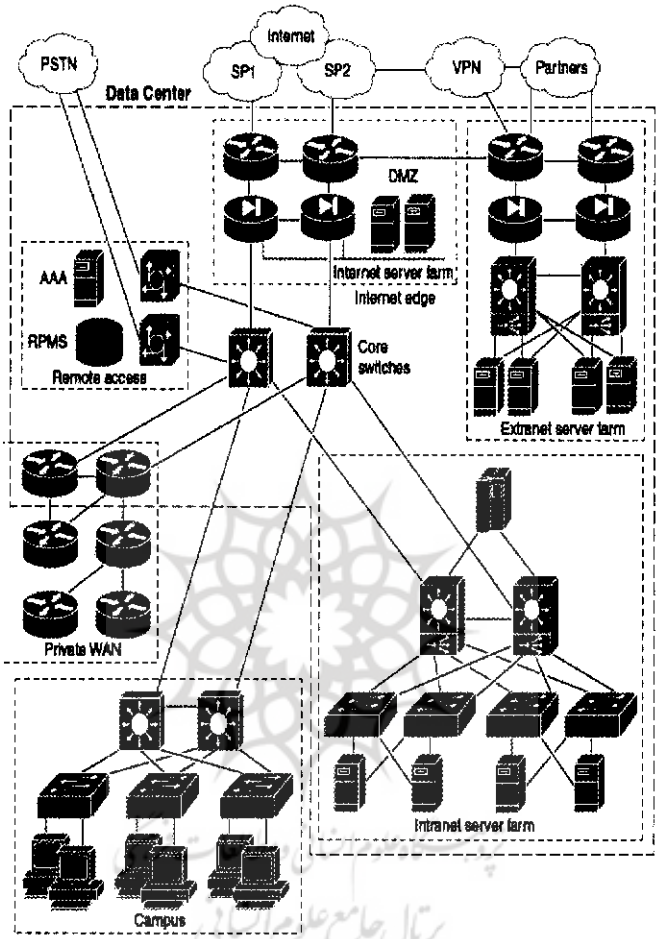
ادبیات نظری تحقیق

هر مرکز داده شامل اجزایی است که هر کدام متناسب با وظایفشان از ساختار خاصی برخوردار می‌باشند. از جمله این اجزا که در یک مرکز داده متعارف قابل مشاهده است، می توان به شبکه‌های Campus، شبکه‌های گسترده خصوصی (Private WAN)، دسترسی از راه دور و انواع Server Farm ها اشاره نمود. برای ارائه خدمات به هریک از این اجزا لازم است یک زیر ساخت ارتباطی ایجاد گردد تا به واسطه آن بتوان بین این اجزا ارتباط برقرار نمود.

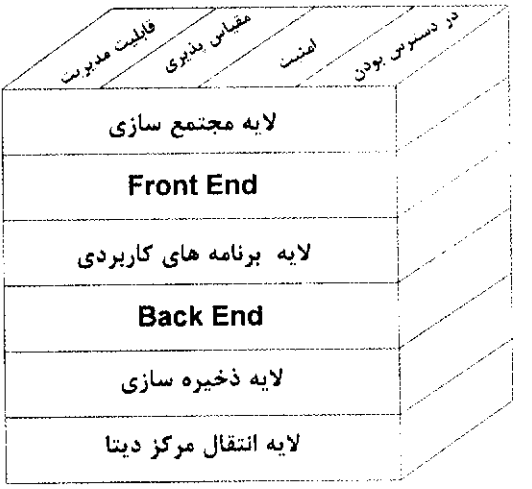
شکل ۱ نمونه ای از زیرساخت شبکه فراگیر و جایگاه مرکز داده را به همراه مولفه‌های آن نشان می‌دهد.

تعیین ساختار مرکز داده وابستگی شدیدی به نوع برنامه های کاربردی و بار ترافیک آن دارد. اما نکته مهم در تعیین ساختار تبدیل نیازها به اهداف تعریف شده ای است که به واسطه آن بتوان طرح تفصیلی یک مرکز داده را تعیین نمود. با توجه به اهمیت یک مرکز داده لازم است ساختار آن به صورت لایه ای در نظر گرفته شود. در هریک از لایه ها مدل های مختلفی برای طراحی مطرح می‌باشد. در طراحی بهینه مرکز داده باید از امکانات هر مدل نهایت استفاده را نمود. به طور مثال در طراحی قسمت هایی از آن استفاده از مدل‌های چندلایه‌ای بهینه می‌باشد.

شکل ۲ نشان دهنده لایه‌های مختلف دسترسی در شبکه مرکز داده می باشد که لایه های این طراحی عبارتند از:



شکل ۱: زیرساخت شبکه فراگیر و جایگاه مرکز داده

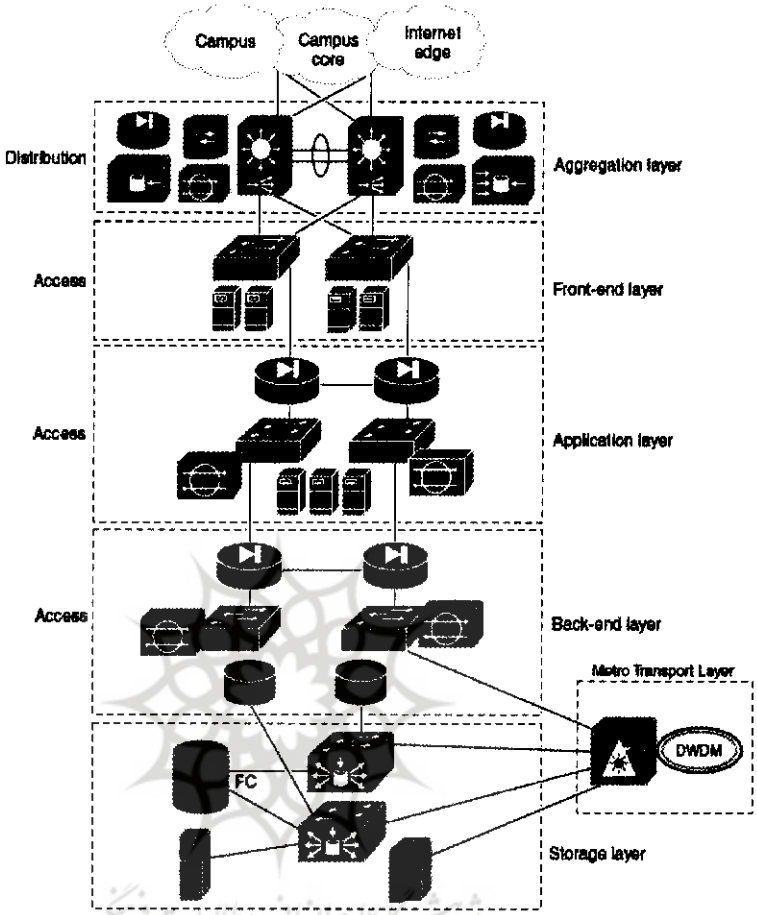


شکل ۲: لایه‌های مختلف دسترسی در شبکه مرکز داده

- لایه تجمیع[۱]
- لایه خط مقدم[۲]
- لایه کاربرد
- لایه عقبه[۳]
- لایه ذخیره سازی[۴]
- لایه انتقال شهری[۵]

اهداف طراحی و سرویس هایی که توسط مرکز داده ارائه می‌شوند ملزومات ساختمان شبکه مرکز را تعیین می‌کنند که در این خصوص شکل ۳ نمونه معماری مرکز داده را به عنوان مدلی برای استفاده مشخص می‌کند.

[۱] Back end
[۲] Storage
[۳] Back end
[۴] Storage
[۵] Metro Transport



شکل ۳: نمونه معماری مرکز داده

لایه تجمیع

وظیفه مهم این لایه برقرای ارتباط بین حوزه سرویس دهنده‌ها و بقیه شبکه مرکز داده بر مبنای مدل ارائه شده می‌باشد. همچنین ایجاد ارتباط بین تجهیزات مرکز داده و پشتیبانی از فعالیت های لایه ۲ و ۳ از دیگر وظایف این لایه می‌باشد و در مجموع، فعالیت های این لایه از مدل معماری ارائه شده شامل موارد ذیل می‌باشد:

- سوییچ های اصلی
- دیوارهای آتش
- سامانه‌های تشخیص تهاجم

- موتورهای اصلی سامانه
- ارتباطات SSL

لایه خط مقدم

این لایه ارتباط با رده اول سرویس دهنده‌ها در بخش سرویس دهنده‌ها را برقرار نموده و سرویس دهنده مربوطه در این لایه شامل سرویس‌های ذیر می‌باشد:

- FTP
- Telnet
- SMTP
- Web Servers
- و دیگر سرویس‌های مربوط به برنامه‌های کاربردی

موارد دیگر مثل QoS بستگی به سرویس دهنده‌ها و نوع عملکردهای آنها دارد. به طور مثال اگر Voice Over IP فعال گردد سرویس QoS نیز برقرار می‌شود.

لایه کاربرد

فعالیت‌های این لایه گذشته از سرویس دهی در خصوص برنامه‌های کاربردی، ارتباط منطقی بین لایه خط مقدم و عقبه را نیز شامل می‌شود. سرویس دهنده‌های این لایه درخواستهای کاربران را برای اعمال فرامین مربوطه به سرویس دهنده‌های لایه عقبه ترجمه می‌کنند.

لایه عقبه

وظیفه اصلی این لایه برقراری ارتباط با سرویس‌های بانک اطلاعاتی می‌باشد و تا حدودی همانند لایه کاربردی عمل می‌کند و ارتباط خود با لایه بالاتر (سرویس دهنده‌های لایه کاربردی) را با استفاده از سامانه‌هایی مثل دیوار آتش تحت کنترل امنیتی دارد.

همچنین سرویس دهنده‌های بانک‌های اطلاعاتی در این لایه می‌توانند از طریق سوییچ های لایه ۲ با تجهیزات لایه بالاتر تبادل اطلاعات نمایند.

لایه ذخیره سازی

در این لایه عملیات مربوط به ارتباطات سامانه‌ها در شبکه ذخیره سازی، توسط

کانال‌هایی مثل فیبر نوری به عمل می‌آید و این ارتباطات به کمک سوییچ هایی که دارای اتصال‌های فیبر نوری هستند از سرویس دهنده‌های دارای امکانات فیبر نوری به سامانه‌های ذخیره ساز مثل واحدهای نوارمغناطیسی برقرار می‌شود.

لایه انتقال شهری

وظیفه اصلی این لایه انجام عملیات در خصوص برقراری ارتباط پر سرعت بین مراکز داده توزیع شده می‌باشد و به عبارتی این لایه ارتباط سریع campus-to-campus را برقرار می‌نماید. این مراکز داده توزیع شده از تکنولوژی Metro-Optical برای ارتباط بین بانک های اطلاعاتی و سامانه‌های ذخیره سازی استفاده می‌کنند. اتصالات پرسرعت برای ارتباطات همزمان و غیر همزمان استفاده می‌شوند.

استانداردهای مهم مراکز داده

استاندارد TIA/TR ۹۴۲

اولین استاندارد مطرح که موارد زیادی از ملزومات مرکز داده را تحت پوشش قرار می‌دهد در اکتبر سال ۲۰۰۴ میلادی منتشر شد. این استاندارد با نام TIA/TR ۹۴۲ نام گرفت. نسخه بعدی این استانداردکه تکمیل شده آن بود بعدها به نام استاندارد TIP ارائه شد (CSC Standard-۲۰۰۷-۱).

این استاندارد که نام کامل آن ANSI/TIA/EIA-۹۴۲ است، به عنوان یک استاندارد ارتباطی برای مراکز داده مطرح می‌باشد که همیشه در حال تکمیل و به روز شدن است به طوری که موارد مهم طراحی را در مراکز داده کوچک تا مراکز داده بزرگ شامل می‌شود و به طور کلی این استاندارد شامل توصیه‌هایی در خصوص عملیات کابل کشی، طراحی شبکه و دیگر ملزومات می‌باشد.

عناوین کلی این استاندارد عبارتند از:

- تجهیزات مکانی (زمین و سامانه‌های تهویه و ...)
- پیکر بندی مسیرهای ارتباطی شبکه داده
- پیکر بندی مسیرهای خطوط برق
- سامانه‌های پشتیبان اطلاعات
- سامانه‌های پشتیبان تغذیه برق
- سامانه‌های سخت‌افزار

در این استاندارد چهار مدل زیر ساخت برای طراحی و پیکر بندی مراکز داده در خصوص سامانه توزیع برق و تهویه پیشنهاد می‌گردد که عبارتند از:

- لایه ۱: در این لایه تنها یک مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان نمی شود که در این حالت درصد دسترس پذیری به میزان ۹۹,۶۷۱٪ می‌باشد.
- لایه ۲: در این لایه تنها یک مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان می‌شود که در این حالت درصد دسترس پذیری به میزان ۹۹,۷۴۱٪ می‌باشد.
- لایه ۳: در این لایه چندین مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان و یک مسیر پشتیبان انتقال داده می‌شود که در این حالت درصد دسترس پذیری به میزان ۹۹,۹۸۲٪ می‌باشد.
- لایه ۴: در این لایه چندین مسیر برای توزیع برق و تهویه در نظر گرفته می‌شود و شامل تجهیزات پشتیبان و چند مسیر پشتیبان انتقال داده می‌شود که در این حالت درصد دسترس پذیری به میزان ۹۹,۹۹۵٪ می‌باشد.

استاندارد EN ۵۰۱۷۳-۴

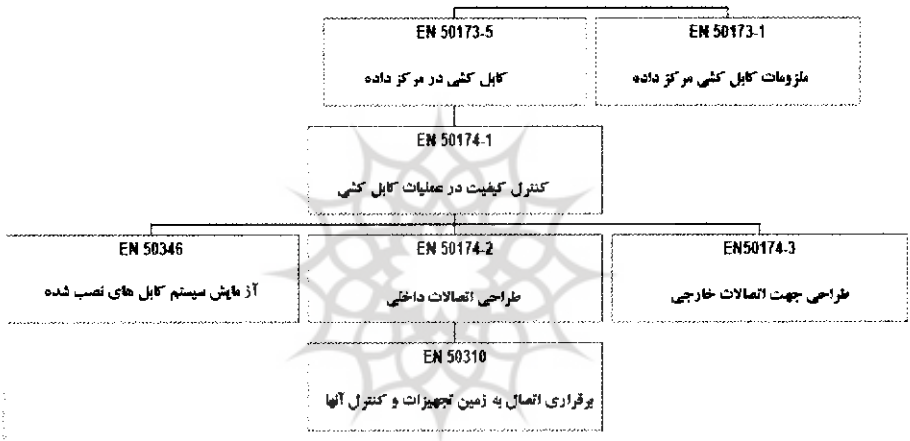
در این استاندارد تغییرات اساسی در حوزه زیر ساخت فیزیکی مرکز داده با توجه به موارد ذیل در نظر گرفته می‌شوند:

- تجهیزات پشتیبان با دسترسی راه دور
- ترسیم راه کار فنی مرکز
- سامانه اعلام و اطفاء حریق
- سامانه‌های پشتیبان تجهیزات برق، آب و ...
- در نظر داشتن لایه‌های امنیتی مختلف

استاندارد EN ۵۰۱۷۳-۵

این استاندارد که در حقیقت بخش اتصالات از استاندارد TIA ۹۴۲ را شامل می‌شود به طور عمده در مورد ملزومات طراحی مرکز داده در حوزه اتصال کابل ها، سامانه‌ها، منابع تغذیه و .... می‌باشد. (شکل ۴)

همچنین در مورد سامانه‌های پشتیبان، امنیت لایه‌ای، کابل کشی استاندارد، انعطاف پذیری در طراحی و دیگر موارد مرتبط راهنمایی‌های لازم را ارائه می‌نماید.



شکل۴: حوزه استانداردهای EN ۵۰۱۷۳

بررسی تاریخی ادبیات تحقیق

مراکز داده در آمریکا

کشور آمریکا به علت پیشرو بودن در فن‌آوری اطلاعات، و نیز به سبب حاکمیت بر بستر اصلی اینترنت، از نخستین کشورهای دارای مرکز داده بوده و در حال حاضر نیز بیشترین و بزرگترین مراکز داده در این کشور قرار دارد.

دولت آمریکا به منظور ارتقای ضریب ایمنی مراکز اطلاعاتی خود بانک‌های اطلاعاتی و کارگزاران شبکه خود را در مکان های با ضریب امنیتی بالا نگهداری می‌کند. بعضی از این اماکن محوطه‌های وسیعی در اعماق کوه های راکی، در نقاط پنهانی از اعماق صحراهای نوادا وآریزونا، در زیر یخچال‌های آلاسکا و در اعماق اقیانوس‌ها می‌باشند.

مراکز داده در ایران

برخی اقدامات انجام شده در کشور به شرح ذیر می‌باشند (کریم بیگی-۱۳۸۴-۱)(امیری-۱۳۸۵-۱):

- سال ۱۳۸۱ : ضوابط صدور مجوز ایجاد مجتمع خدمات اینترنت IDC به بخش خصوصی، که این اقدام شامل تعریف ، مقررات مربوط به واگذاری مجوز مجتمع خدمات اینترنتی و مدارک لازم جهت ایجاد مجتمع خدمات اینترنت به بخش خصوصی می‌باشد.

- سال ۱۳۸۳: دبیرخانه شورای عالی اطلاع‌رسانی با همکاری پارک فن‌آوری پردیس همایش نقش مراکز داده در توسعه فن‌آوری اطلاعات و ارتباطات را در دی ماه در تهران برگزار کرد که در پایان همایش، سند راهبردی مراکز داده کشور و همچنین آیین نامه مرکز خدمات داده اینترنتی نیز منتشر شده که خود گویای یک اقدام جدی در این حوزه بوده است.

- سال ۱۳۸۴ : اعطای مجوز تاسیس و راه اندازی مرکز داده به سه شرکت خصوصی: داده پردازی ایران ، کنسرسیوم فن آوا – پتسا و پارس آنلاین

- سال ۱۳۸۵ : در شهریور ماه این سال همایش چشم انداز مراکز داده در ایران در مرکز تحقیقات مخابرات برگزار گردید.

- سال ۱۳۸۶: برگزاری مناقصه بین شبکه علمی فاز تهران و مترو اترنت کرمان و قم به ترتیب با اعتباری حدود ۴۰ میلیارد ریال و ۱۳۵ میلیارد ریال به عنوان بخشی از پروژه شبکه ملی.

- سال ۱۳۸۶: اختصاص ۳۰۰ میلیارد ریال اعتبار از سوی وزارت ICT در فاز اول و طرح شبکه ملی دیتا به مبلغ ۳۵۰۰ میلیارد ریال که مقرر گردید که شرکت فن‌آوری اطلاعات به عنوان مجری طرح آنرا اجرا نماید که بعدها بنا به ایجاد تغییرات در وظایف این شرکت، مجری طرح شرکت ارتباطات زیرساخت اعلام گردید.

- بهار ۱۳۸۷: مکلف شدن بانک مرکزی برای راه‌اندازی مرکز داده‌ای

جهت نگهداری داده‌های تراکنش بانکی مشتریان و عملکرد کلیه پایانه‌های بانک .

- خردادماه ۱۳۸۷: نشست تخصصی مرکز تحقیقات راهبردی مجمع تشخیص مصلحت نظام با استادان و کارشناسان دانشگاه با عنوان زیرساخت‌های فن آوری اطلاعات.
- خردادماه ۱۳۸۷: راه‌اندازی آزمایشی مرکز داده مرکز تحقیقات مخابرات
- آبان ماه ۱۳۸۷: برگزاری همایش مدیریت فن آوری اطلاعات و ارتباطات با محوریت مدیریت سرویس‌های یکپارچه در شبکه های نسل آینده در هتل المپیک تهران

بررسی محیطی تحقیق

همه مراکز داده در یک درجه از اهمیت قرار ندارند، و بسته به نقش آنها، خدمات ارائه شده، گستره آنها و دیگر پارامترها در رده‌های گوناگون اهمیت قرار دارند که ملزومات پدافند غیر عامل و امنیتی هر یک نیز متفاوت از دیگری است (mit-۲۰۰۷-۱). از طرف دیگر همیشه برقراری ملزومات پدافند غیر عامل امنیت هزینه بالایی می‌طلبد. از این رو لازم است مطابق نیازمندی‌های واقعی پدافند غیر عامل و امنیتی یک مرکز داده، تدابیر لازم اتخاذ شود تا از صرف هزینه های زیادی جلوگیری شود.

از همین رو باید مراکز داده را از نظر حساسیت امنیتی طبقه‌بندی نمود. این طبقه‌بندی باید حتی‌الامکان نزدیک به سطح واقعی امنیت مورد نیاز باشد تا از یک طرف از نقض احتمالی امنیت به علت مسامحه در برقرار امنیت مورد نیاز جلوگیری شود و از سویی دیگر از صرف هزینه‌های گزاف به علت افراط در تعیین سطح امنیتی پیشگیری بعمل آید (ngdc-۲۰۰۷-۱).

با توجه به لزوم توسعه مراکز داده در کشور، از سویی اهمیت و حساسیت این مراکز، تهیه سند بالادستی در حوزه ملاحظات پدافند غیر عامل و امنیت در این مراکز بسیار ضروری بوده است. لذا با توجه به اهداف و رویکردهای سازمان پدافند غیر عامل که تکیه بر ۳ اصل امنیت، ایمنی و پایداری دارد، تهدیدات متصور برای این مراکز در ۳ دسته

تهدیدات ناشی از ۱- جنگ و مخاصمات بین المللی، ۲- تهدیدات امنیتی و ۳- تهدیدات محیطی و طبیعی برای مکان های مهم، حساس و حیاتی باید متناسب با شرایط مراکز داده در کشور و با رویکرد بومی بررسی می گردید؛ برای این منظور ابتدا مراکز داده به ۳ دسته مهم، حساس و حیاتی تقسیم بندی گردیده است. در ادامه مصادیق رده بندی یک مرکز داده به منظور تعیین طبقه بندی آن نیز بیان شده است. لذا با استفاده از این مصادیق، می توان در زمان تصمیم گیری برای طراحی و پیاده سازی یک مرکز داده خاص، سطح آن مرکز داده (مهم، حساس یا حیاتی) را مشخص نمود. در نهایت ملاحظات پدافند غیر عامل در خصوص هر سطح مرکز داده به تفکیک بصورت کنترل های سطح میانی در حوزه های مختلف می گردید. لازم به ذکر است که اقدامات گفته شده انجام گردیده و چکیده آن در ادامه این مقاله بیان می گردد.

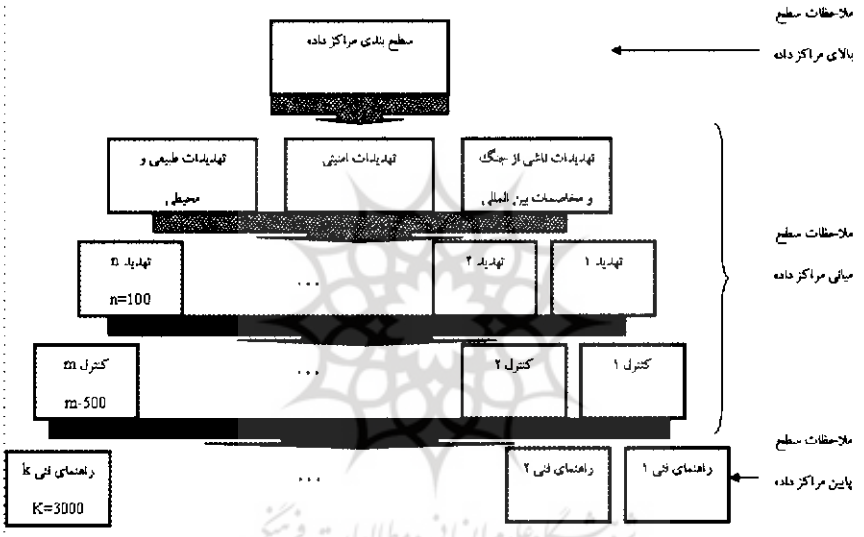
پس از تعیین سطح و مشخص شدن سطح مرکز داده، کافی است کنترل های تعیین شده برای آن سطح، مورد توجه قرار گرفته و لحاظ گردند. طبیعی است جنس این کنترل ها از نوع کنترل های فنی سطح بالا و سطح میانی بوده و لذا به موارد فنی سطح پایین که عموما مرتبط با محصولات مختلف و تکنولوژی های سطح پایین بوده و وابسته به زمان طراحی و پیاده سازی و متناسب با ابزارهای در دسترس پیاده ساز در زمان پیاده سازی می باشد و از سویی دائما در حال تغییر است، نمی پردازد. لازم به ذکر است که کنترل های سطح بالا و میانی به گونه ای انتخاب گردیده که در صورت رعایت نمودن و لحاظ نمودن این موارد، تمامی موارد مورد نظر پدافند غیر عامل در سطح پایین نیز لحاظ خواهد گردید.

لذا مدل و معماری به کار گرفته شده برای تدوین ملاحظات پدافند غیر عامل و امنیت مراکز داده، مدلی منحصر به فرد و بومی کشور می باشد. این مدل دارای ۵ لایه می باشد (شکل ۵).

در لایه اول، ملاحظات پدافند غیر عامل در مراکز داده در سطح بالا، در لایه های دوم، سوم و چهارم، این ملاحظات در سطح میانی و در نهایت در لایه پنجم، این ملاحظات در سطح پایین بیان گردیده است.

در سطح بالا، مطالب مربوط به رده بندی مراکز داده و مصادیق این رده بندی و چگونگی تعیین سطح یک مرکز داده و مشخص کردن نوع آن (مهم، حساس یا حیاتی) بیان گردیده است (لایه اول).

در سطح میانی، بدلیل گستردگی سطحی و عمقی مراکز داده (به عنوان قلب تپنده IT) و کاربرد اکثر مقوله های مطرح امروزی در حوزه IT در این مراکز، و به منظور پرداختن به تمامی کنترل های مربوط به این مقوله ها در مراکز داده، ابتدا ۳ حوزه اصلی تهدید با رویکرد پدافند غیر عامل مشخص، سپس کلیه تهدیدات متصور برای مراکز داده برای این ۳ حوزه، در حدود ۱۰۰ مقوله احصاء (لایه سوم) و در نهایت کنترل های مربوط به این تهدیدات در قالب حدود ۵۰۰ کنترل (لایه چهارم) مشخص می گردد.



شکل ۵: مدل و معماری ۵ لایه تدوین ملاحظات پدافند غیر عامل در مراکزداده

در سطح پایین نیز همان گونه که اشاره شد، از آنجا که این کنترل ها وابسته به محصولات و تکنولوژی های مرتبط با زمان پیاده سازی مرکز داده می باشد، بنابراین این موارد باید در زمان پیاده سازی و با توجه به کنترل های سطح میانی توسط کارشناسان خبره طراح مراکز داده در حوزه های مختلف، استخراج شده و لحاظ گردند.

در این مدل اولین سطح، ملاحظات سطح بالای پدافند غیر عامل است که در ادامه شرح داده می شود.

در ملاحظات سطح بالای مراکز داده کشور، این مراکز با توجه به ملاحظات پدافند غیر عامل کشور و همچنین مصادیق تعیین جایگاه یک مرکز داده، سطح بندی می گردند. توضیح اینکه، پس از بیان دسته بندی مراکز داده، مصادیقی ارائه گردیده که هر سازمانی که بخواهد اقدام به ایجاد مرکز داده نماید، با توجه به این مصادیق بتواند سطح مرکز داده مورد نیاز خود را احصاء نمایند، سپس ملاحظات پدافندی متناسب با سطح بدست آمده را اعمال نماید.

تجزیه و تحلیل یافته ها

با توجه به سطوح دسته بندی مراکز از دیدگاه سازمان پدافند غیر عامل، رده‌های زیر برای یک مرکز داده وجود خواهد داشت:

- **سطح III مرکز داده حیاتی**
- **سطح II مرکز داده حساس**
- **سطح I مرکز داده مهم**

با توجه به اصول پدافند غیر عامل یعنی ۳ اصل امنیت، ایمنی و پایداری، ساختار مراکز داده باید به گونه‌ای طراحی و پیاده سازی گردد که این سه اصل همواره مورد توجه قرار گرفته شده باشد. مقوله اول یعنی امنیت در ادامه شرح داده خواهد شد، مقوله دوم نیز در بخش امنیت محیطی و طبیعی مفصلا مورد توجه و تاکید قرار گرفته شده است و مقوله سوم یعنی پایداری نیز به عنوان یکی از اصول مهم پدافند غیرعامل، هم در موضوعات مرتبط به امنیت و هم در موضوعات مرتبط به تهدیدات ناشی از جنگ و مخاصمات بین المللی به آن پرداخته شده است.

مصادیق طبقه‌بندی و رده بندی مراکز داده کشور

با وجود آنکه نمی توان فرمولی واحد و جامع را برای تعیین سطح یک مرکز داده ارائه نمود، بنابراین تلاش شده است تا با محور قرار دادن شاخصه هایی، تا حدی به این مهم دست پیدا نمود. بدیهی است تعیین سطح، در زمان ایجاد آن مرکز داده و با توجه به مصادیق بیان شده، توسط کارشناسان خبره این حوزه تعیین خواهد شد.

- طبقه‌بندی داده ها و اطلاعات و تعیین سطح ضربه بالقوه
- تجمیع داده‌ها

- کاربرد مراکز داده
- گستره کاربرد مراکز داده

ملاحظات پدافند غیر عامل سطح میانی مراکز داده

در این بخش تهدیدات مراکز داده با رویکرد پدافند غیر عامل در ۳ دسته کلی "تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین الملل"، "تهدیدات امنیتی" و "تهدیدات محیطی و طبیعی" دسته بندی شده اند (جدول ۱). در ادامه متناسب با سطح مراکز داده (مهم، حساس و حیاتی) راهکارهای لازم در قالب کنترل‌های فنی (حدود ۵۰۰ کنترل) سطح میانی (ISO/IEC۲۷۰۰۱-۲۰۰۵-۱) (NIST SP ۸۰۰-۶۰-۲۰۰۷-۱) با توجه به شرایط ملی و بومی کشور تدوین شده که به علت حجم بالا در این مقاله آورده نشده و فقط مثالی از آنها ذکر گردیده است(جدول ۲). لازم به ذکر است که سطوح بالاتر مراکز داده علاوه بر کنترل های ذکر شده برای آنها، کنترل های ذکر شده برای سطوح پایینتر را نیز شامل می شوند.

جدول ۱. تهدیدات مراکز داده با رویکرد پدافند غیر عامل

ردیف	نوع تهدید	حوزه
	اختلال الکترونیکی و الکتریکی	تهدیدات ناشی از جنگ (اطلاعات و فیزیکی) و مخاصمات بین المللی
	کدهای مخرب و بدافزارها (Malwares)	
	دسترسی غیر مجاز از راه دور	
	وقفه در کار	
	جاسوسی	
	حملات تروریستی سایبری (هکرها)	
	دسترسی غیرمجاز به اطلاعات	
	دسترسی غیرمجاز به شبکه	
	دسترسی غیرمجاز به سامانه	
	دسترسی غیرمجاز به برنامه‌های کاربردی	
	دسترسی غیر مجاز به اطلاعات یا سامانه‌ها حین مبادله با نهادهای خارج از مرکز داده	
	پردازش‌های اطلاعاتی غیر مجاز	
	تغییر غیرمجاز، از دست دادن یا سوءاستفاده از اطلاعات در برنامه‌های کاربردی	
	حمله فیزیکی	
	بمب گذاری یا انفجار	

	حوادث هسته ای و اتمی	
	حوادث شیمیایی	
	جنگ الکترومغناطیسی	
	ارگانیزم ها (ویروس، باکتری و...)	
	دسترسی غیر مجاز به سامانه ها، تجهیزات و منطقه فیزیکی	
	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	
	دسترسی فیزیکی غیر مجاز به بستر انتقال داده ها	
	عدم سازگاری با فن آوری های مدرن جنگ الکترونیک	
	تهدید ناشی از عدم سازگاری با سامانه های مدرن اطلاعات عملیات	
	تهدید ناشی از عدم سازگاری با فن آوری های مدرن جنگ متحرک	
	آسیب یا سرقت (الکترونیکی)	
	آسیب یا سرقت (فیزیکی)	
	اختلال در ارتباطات شبکه	
	اختلال در سامانه برق	
	قرار دادن کشور در موقعیت جنگ تمام عیار اطلاعاتی	
	تغییر سریع فن‌آوری (در حوزه جنگ سایبر)	
	جهانی شدن	
	زیر ساخت های عمده جهانی نظیر اینترنت	
	حملات مختل کننده خدمات	
	جنگ روانی دشمن	
	انکار سرویس	
	تغییر هویت اطلاعات در حال گذر	
	دسترسی غیر مجاز به اطلاعات	
	عدم استتار	
	عدم اختفا	
	نا آرامی های اجتماعی	
	ورود و خروج غیر مجازافراد	تهدیدات امنیتی
	دسترسی غیر مجاز به سامانه ها، تجهیزات و منطقه فیزیکی	
	دسترسی غیر مجاز به رسانه‌های ذخیره‌سازی اطلاعات	
	دسترسی فیزیکی غیر مجاز به بسترانتقال داده ها	
	عدم اصلاح و بازیابی پس از حوادث امنیتی	
	عدم رویکرد مداوم برای مدیریت حوادث امنیتی	
	ناامنی یا نادرستی در عملیات پردازش اطلاعات	
	عدم امنیت در تعامل با طرفهای ثالث	
	خطاهای سامانه	
	برون‌سپاری خدمات و پردازش اطلاعات	

	عدم به کارگیری نرم افزارهای کد باز	
	نقض صحت و دسترس‌پذیری اطلاعات و سامانه‌های پردازش اطلاعات	
	عدم حفاظت اطلاعات در شبکه‌ها	
	دسترسی غیر مجاز کاربر	
	عدم در نظر گرفتن امنیت در سامانه‌های اطلاعاتی به عنوان یک بخش اصلی	
	نقض محرمانگی یا صحت اطلاعات در اثر عدم استفاده یا استفاده نادرست از رمزنگاری	
	عدم اطمینان از امنیت فایل سامانه ها	
	نقض امنیت اطلاعات و نرم‌افزارهای کاربردی سامانه‌عامل	
	عدم مدیریت آسیب‌پذیری‌های فنی	
	عدم رعایت قوانین	
	عدم سازگاری با خط مشی‌ها	
	عدم وجود مدیریت یکپارچه امنیت اطلاعات	
	فقدان نظام مدیریت امنیت اطلاعات	
	استخدام یا به کارگماری افراد نامناسب.	
	عدم آگاهی نیروهای انسانی از مسؤلیت ها و تعهدات	
	تهدیدهای مربوط به تغییر شغل یا انفصال از خدمت کارکنان و پیمانکاران	
	دسترسی‌های غیر مجاز طرف های خارج مرکز داده	
	تهدید ناشی از تحریم فن آوری های پیشرفته خارجی	
	وابستگی به خارج از کشور در بخش تعمیر و نگهداری	
	وابستگی به تولیدات سخت افزاری و نرم افزاری خارجی	
	وضع مقررات جهانی و وجود ساختارهای بین المللی	
	عدم تجهیز به سامانه مدیریت بحران و شرایط اضطرار	
	فقدان یک سامانه هشداردهنده سریع و به موقع	
	عدم بکارگیری سازه های امن و پایدار	
	تولید اطلاعات غلط و نامطمئن	
	عدم بهره مندی از مراکز احتیاط (Backup) امن، ایمن و پایدار	
	عدم بکارگیری خطوط ارتباطی مطمئن و پایدار بومی شده (شبکه های مبتنی بر فیبر نوری)	
	اتصالات نا امن به شبکه های اینترنت و اینترانت و فیبر نوری	
	عدم پیش بینی برق پشتیبان (مانند UPS)	
	عدم وجود تخصص لازم	
	عدم وجود آموزش امنیتی کافی	

	اشتباهات و غفلت ها مانند عدم بکارگیری صحیح تجهیزات، عدم نصب صحیح نرم افزارها و برنامه های کاربردی، سهل انگاری	
	قوانین ضعیف و متناقض	
	عدم وجود کنترل روی قوانین	
	عدم وجود حمایت های لازم (دولتی و ...)	
	استفاده از سامانه های پایه غیر بومی	
	اتکا قابل ملاحظه به سامانه های ارتباطی بی سیم و ماهواره غیر امن	
	عدم سازگاری با سامانه های اطلاعات جغرافیایی(GIS)	
	عدم استفاده از ماهواره های امن جهت سنجش از راه دور	
	زلزله	تهدیدات محیطی و طبیعی
	آتش	
	طوفان و صاعقه	
	سیل	
	رطوبت و دما	
	دود	
	سقوط اجسام	
	تداخل الکترومغناطیسی امواج	
	مشکلات تأسیساتی (آب ،گاز، برق، تلفن)	
	مواد پرخطر	
	تشعشعات رادیواکتیو	
	گرد و غبار و مه	

جدول ۲. مثالی از کنترل های ذکر شده برای یکی از تهدیدات مراکز داده متناسب با سطح آنها[1]

[1] شماره های انتهای هر کنترل امنیتی، ارجاع به شماره کنترل در استاندارد ISO/IEC ۲۷۰۰۱:۲۰۰۵ می باشد. در برخی موارد از کنترل های استاندارد NIST SP-۸۰۰-۳۰ نیز استفاده شده که دراین صورت شماره مربوط ذکر شده است. سایر کنترل ها نیز توسط نگارنده تدوین گردیده است.

نوع تهدید	سطح مرکز داده	شرح کنترل
پردازش‌های اطلاعاتی غیر مجاز	مهم	• الزامات ممیزی و فعالیت های که شامل بررسی سامانه‌های عملیاتی است، برای کمینه کردن مخاطرات اختلال در فرایند کسب و کار، باید دقت طرح‌ریزی و تصویب شوند (A.۱۵,۳,۱) • رکوردهای ممیزی مربوط به فعالیت‌های کاربران، وقایع استثنایی، و رویدادهای امنیتی باید تولید و نگهداری شوند. این رکوردها برای کمک به تفحص های آتی و نظارت بر کنترل دسترسی کاربرد دارند. (A.۱۰,۱۰,۱) • فرایند اجرایی برای استفاده از مراقبت امکانات پردازش اطلاعات باید پایه ریزی شده و نتایج نظارت فعالیت ها باید به طور منظم بازنگری شوند. • امکانات ثبت کردن و ثبت اطلاعات باید در برابر دسترسی بدون مجوز و پنهانی حفاظت شود. • فعالیت های مدیر و اپراتور سامانه باید ثبت شوند. • خطاها باید ثبت و تحلیل شده و اقدامات مناسب صورت بگیرد. • ساعت سامانه های پردازش اطلاعات در سازمان یا حوزه امنیتی باید با زمان دقیق مرجع هماهنگ باشند.(A.۱۰,۱۰,۶) • در صورت بروز خطا در ثبت رکوردهای ممیزی یا پر شدن ظرفیت محل ذخیره، باید هشدار مناسب به مدیر فنی مربوط داده شده و اقدام مقتضی (توقف ثبت، خاموش کردن سامانه، یا بازنویسی روی رکوردهای قدیمی) انجام شود. (NIST AU-۵) • سامانه‌های اطلاعاتی باید مهر زمانی (timestamp) هر رویداد را مشخص نمایند. (NIST AU-۸) • سامانه‌های اطلاعاتی باید از اطلاعات ممیزی و ابزارهای ممیزی در مقابل دسترسی غیرمجاز، تغییر یا حذف محافظت کنند. (NIST AU-۹) (A.۱۵,۳,۲)

	حساس	• هر سامانه اطلاعاتی باید امکان ثبت وقایع بیشتر و جزئی‌تر در رکوردهای ممیزی به همراه نوع، محل، و عامل آن فراهم کنند. ((NIST AU-۳(۱) • در صورتی که حجم رکوردهای ممیزی به ۷۵٪ ظرفیت محل ذخیره رسید، باید سامانه اطلاعاتی هشداری به مدیر سامانه بدهد. ((NIST AU-۵(۱) • سامانه‌های اطلاعاتی باید قابلیت تحلیل و خلاصه‌سازی رکوردهای ممیزی و تولید گزارش‌های مفید و قابل پیکربندی بر اساس انتخاب رویدادهای خاص را داشته باشند. ((NIST AU-۷, AU-۷(۱)
	حیاتی	• هر سامانه اطلاعاتی باید قابلیت مدیریت مرکزی محتوای رکوردهای ممیزی تولید شده توسط مولفه‌های مختلف سامانه را داشته باشد. ((NIST AU-۳(۲) • مرکز داده باید از مکانیزم‌های خودکار برای هشدار فوری به پرسنل امنیتی درباره فعالیت‌های غیرمعمول، استفاده نماید ((NIST AU-۶(۲) • سامانه‌های اطلاعاتی باید اطلاعات ممیزی خود را روی رسانه‌های سخت‌افزاری با قابلیت یکبار-نوشتن _write-once) ثبت نمایند (مانند نوشتن روی CD یا چاپ روی کاغذ) (NIST AU-۹(۱))

ملاحظات پدافند غیر عامل سطح پایین مراکز داده

اصولاً ملاحظات سطح پایین مراکز داده، باید متناسب با هر مرکز داده خاص، و در زمان طراحی و پیاده سازی آن، با درنظر گرفتن مدل و ملاحظات امنیتی سطح بالا و میانی که بیان گردید، طراحی و پیاده سازی گردد. لیکن به منظور آشنایی با ماهیت ملاحظات این سطح، در ادامه به عنوان نمونه، یک مورد از ملاحظات فنی سطح پایین و اجرایی مراکز داده بیان شده است. بدیهی است جزئیات مربوط به این هر یک از این موارد برای هر مرکز داده به صورت خاص بوده و در زمان طراحی تعیین می‌گردد.

نمونه ای از ملاحظات سطح پایین مراکز داده

نظر به لزوم ایجاد امنیت بالا در مراکز داده، و بر اساس مدل های امنیتی Multi Layer Security و Defence In Depth طرح امنیتی ۵ لایه‌ای متناسب با موارد زیر پیشنهاد می‌گردد:

۱- امنیت فیزیکی و محیطی
۲- امنیت لایه شبکه
۳- امنیت لایه کاربرد
۴- امنیت لایه میزبان
۵- امنیت داده

به منظور ایجاد امنیت لازم در هر لایه، از ابزارهای امنیتی خاص آن لایه استفاده می‌گردد. برای این منظور از ابزارهایی نظیر فایروال، سامانه تشخیص و جلوگیری از نفوذ، سامانه پایش شبکه، سامانه‌های کنترل دسترسی، سامانه‌های ضد بد افزار، سامانه‌های تشخیص و رفع آسیب پذیری ها، سامانه‌های رمز کننده لایه‌های شبکه و بسیاری ابزارهای امنیتی دیگر متناسب با نوع و ماهیت شبکه یک مرکز داده بهره جسته می‌شود. اما از آنجا که فرآیند امن سازی و به تبع آن امن سازی لایه‌های شبکه، فقط به استفاده از یک سری ابزارهای امنیتی امکان پذیر نمی‌باشد، بلکه فعالیت هایی نظیر "پیکربندی امن کلیه تجهیزات و ابزارهای به کار گرفته شده در ایجاد و توسعه شبکه" و "رویه‌ها و روال های امنیتی مرتبط با امنیت" نیز باید طراحی و اجرا گردند، لازم است در کنار استفاده از تجهیزات امنیتی در هر لایه شبکه، به دو مقوله اشاره شده نیز توجه گردد.

نتیجه گیری

با عنایت به عدم لحاظ تمامی ملاحظات پدافند غیر عامل و امنیت در حال حاضر در مراکز داده کشور، در مدل ارائه شده در این تحقیق و نوع نگاه این مدل به ملاحظات پدافند غیر عامل و امنیت در طراحی و پیاده سازی مراکز داده در سطوح مختلف (مهم، حساس و حیاتی) می توان راهکار جامع مقابله با تهدیدات را به کارگیری روش هایی در سطوح بالا و میانی و نگاه بالا به پایین دانست.

ملاحظات سطح بالا مربوط به تعیین سطح مراکز داده با توجه به مصادیق ذکر شده می باشد. در ملاحظات سطح میانی ابتدا تهدیدات مراکز داده با رویکرد پدافند غیر عامل بررسی شده و دسته تهدیدات (در ۱۰۲ حوزه) استخراج گردیده است. سپس

کنترل های سطح میانی متناسب با هر دسته تهدید و همچنین متناسب با هر سطح مرکز داده (حدود ۵۰۰ کنترل) ارائه گردیده است.

ملاحظات سطح پایین نیز، وابسته به نوع محصولات، ابزارها و تکنولوژی به کار رفته برای طراحی و تجهیز مراکز داده بوده و بنابراین باید در زمان پیاده سازی و با توجه به ملاحظات سطح بالا و میانی تعیین گردند.

تمامی سازمان های دولتی، غیردولتی که به نوعی درصدد به کارگیری و استفاده از مراکز داده به منظور بهره مندی کاربران و احتمالاً خود سازمان از خدمات ارائه شده می باشند می باید ضمن توجه به این راهکارها، کنترل های لازم را در طراحی مراکز داده را مورد توجه قرار دهند.

منابع و مآخذ

[۱]عابدینی محسن ، حامد حاج حسین زاده - نقش پدافند غیرعامل در پروژه از دیدگاه الگوی تعاملی (PMIT) سامانه مدیریت پروژه دفاعی ایران(IDPMS) - سومین کنفرانس بین المللی مدیریت پروژه - ۱۳۸۶

[۲]جلالی محمد– پدافند غیر عامل – نشریه مهندسی اسوه شماره های ۷ و ۸

[۳] "Internet Data Center", http://idc.nic.in/

[۴] "Data Center & Networks", http://www.idcworks.com.my/data_centre_networks.htm

[۵] Word Data Center System Roster, http://www.ngdc.noaa.gov/wdc/list.shtml

[۶] بی نا- گزارش مرکز پژوهشهای مجلس – تهیه شده در گروه ارتباطات و فن‌آوریهای نوین

[۷]کریم بیگی آرش – گزارش مورخه ۱۳۸۴/۲/۳۰ منتشر شده در سایت http://www.ICTna.ir

[۸]http://www.iTanalayze.ir

[۹]امیری بهار -مرکز دادههای ایرانی - گزارش مورخه ۱۳۸۵/۷/۱ – بزرگراه فن‌آوری

[۱۰] http://www.ITNA.ir

]

tejarat.com/News/Cat۱۸/News۱۰۴۷۰.html

[۱۳] Sufia Tippu, "Google likely to set up □۱ billion datacenter in India", http://www.itwire.com.au/content/view/۵۲۵۴/۹۴۵/

[۱۴] "MyLoca Data Center", http://www.exabytes.com.my/about/datacenters/myloca.html

[۱۵] "GUIDELINES FOR IMPLEMENTATION OF THE COMMON SERVICES CENTERS (CSC) SCHEME IN STATES ", http://www.mit.gov.in/

[۱۶] "Department of Information Technology", http://www.mit.gov.in/

[۱۷] National Geophysical Data Center, http://www.ngdc.noaa.gov

[۱۸] ISO/IEC ۲۷۰۰۱: Information Technology – Security Techniques –Infromation Security Management Systems – Requirements, ۲۰۰۵.

[۱۹] ISO/IEC ۱۷۷۹۹: Information Technology – Security Techniques - Code of Practicfe for Infromation Security Management (۲nd edition), Feburary ۲۰۰۵.

[۲۰] Federal Information Processing Standards Publication, FIPS PUB ۱۹۹: Standards for Security Categorization of Federal Information and Information Systems, February ۲۰۰۴.

[۲۱] Federal Information Processing Standards Publication, FIPS PUB ۲۰۰: Minimum Security Requirements for Federal Information and Information Systems, March ۲۰۰۶.

[۲۲] National Institute of Standards and Technology, NIST SP ۸۰۰-۶۰: Guide for Mapping Types of Information and Information Systems to Security Categories, Draft Revision November ۲۰۰۷.

[۲۳] National Institute of Standards and Technology, NIST SP ۸۰۰-۵۳: Recommended Security Controls for Federal Information Systems, Revision ۱, December ۲۰۰۶.