چالش‌های کنترلی و امنیت فیزیکی در مراکز داده‌ی استاندارد

محمدجمال رازقی*
فرشاد عرب مارکده**

تاریخ دریافت: ۹۵/۰۷/۲۵
تاریخ پذیرش: ۹۶/۰۳/۱۷

چکیده:

مراکز داده جدید از لایه‌هایی از فضای تکنیکی (فنی)، پشتیبانی و نیروی اجرایی پشتیبان اتاق رایانه با قابلیت پردازش بسیار بالا و ذخیره‌سازی تشکیل شده‌اند. بسته به نوع و اندازه مرکز داده، جهت تأمین امنیت فیزیکی ممکن است که به تمامی نیازمندی‌های امنیتی ساختمانی، اتاق، ناحیه اطراف و کل سایت نیاز باشد. در این مقاله مهم‌ترین چالش‌های کنترلی و امنیت فیزیکی در مراکز داده استاندارد که مهندسین طراح با آن‌ها سروکار دارند، به‌اختصار مورد بحث و تحلیل قرارگرفته‌اند.

واژگان کلیدی:

مرکز داده، امنیت فیزیکی، کنترل، استانداردسازی، مرکز داده استاندارد

۱. مقدمه

پیش از طراحی هرگونه طرح امنیتی، طراحان مرکز داده باید آنالیز ریسک دقیقی از جایگاه فعلی و آینده‌ی سایت تهیه کنند و این طرح را با توجه به تمامی ریسک‌های شناخته‌شده در آنالیز خود، تهیه نمایند. پیش از طراحی هر مرکز داده در حین ساخت آن، بررسی و تحلیل امنیتی کاملی از اوضاع نیاز است و می‌بایست پس از راه‌اندازی و قرار دادن تجهیزات، سالانه این کار را انجام دهند. مسئولین، مهندسین و معماران امنیتی باید موارد زیر را ارزیابی کرده و توصیه‌های خود را به‌صورت مکتوب ارایه دهند.

هدف از این مقاله، بررسی چالش‌های اصلی کنترل و تأمین امنیت فیزیکی و راه‌کارهای موردنیاز برای حفظ محرمانگی[1]، صحت[2] و در دسترس بودن مرکز داده است. در حال حاضر شرکت‌های زیادی در حال ایجاد اتاق‌ها یا ساختمان‌های اختصاصی مرکز داده، با مجوز خصوصی یا نیمه‌خصوصی هستند که امکان کنترل بیشتر اپراتور بر امنیت فیزیکی ساختار، تجهیزات و افرادی که در آن کار می‌کنند، فراهم می‌شود.

۲ طرح امنیت فیزیکی

طرح امنیت فیزیکی باید هم برای مرکز داده و هم ساختمانی که مرکز داده در آن قرار دارد، تهیه و اجرا شود.

لازم به ذکر است که هیچ ضمانتی برای امنیت کامل وجود ندارد، ولی هماهنگی و اجرای الزامات استاندارد، بالاترین سطح قابل قبول از امنیت را فراهم می‌کند. به‌طور خلاصه بخش‌های زیر در زمینه امنیت فیزیکی مراکز داده دیده باید لحاظ شوند:

- امنیت کارمندان،
- تجهیزات IT،
- شبکه،
- تجهیزات ارتباطی،
- سایت و ساختمانی که شامل این امکانات است.

واضح است که هیچ راه‌کاری به تنهایی نمی‌تواند امنیت مؤثری را ارایه نماید. تمامی پارامترهای امنیتی معماری، عملیاتی و فیزیکی که در تصویر فهرست شده‌اند (شکل ۱)، یک یا چند مورد از کارهای زیر را با هم یا به تنهایی انجام می‌دهند:

- به تأخیر انداختن،
- مانع شدن،
- تشخیص،

1. Confidentiality
2. Integrity

* دکتری مدیریت صنعتی
** دانشجوی کارشناسی ارشد، مهندس کنترل و ابزاردقیق، دانشگاه شهید بهشتی

- تصمیم‌گیری،
- عکس‌العمل.

شکل (۱) پارامترهایی که باید در هر کدام از حوزه‌های امنیت فیزیکی در نظر داشت را مشخص کرده است.

شکل ۱: پارامترهای امنیتی

۲-۱ امنیت فیزیکی در مرکز داده

مراکز داده جدید از لایه‌هایی از فضای تکنیکی (فنی)، پشتیبانی و نیروی اجرایی پشتیبان اتاق رایانه با قابلیت پردازش بسیار بالا و ذخیره‌سازی تشکیل شده‌اند. بسته به نوع و اندازه مرکز داده‌ای که می‌خواهید امنیت فیزیکی داشته باشد، ممکن است که به تمامی نیازمندی‌های امنیتی ساختمانی، اتاق ، ناحیه اطراف و کل سایت نیاز داشته باشید. این نیازمندی‌ها عبارتند از:

- تجهیزات کنترل دسترسی،
- معماری،
- موانع ورودی برای سایت،
- تجهیزات تشخیص و اعلام خطر،
- خدمات استحفاظی/ نگهبانی،
- نظارت بر سایت.

۲-۲ امنیت فیزیکی و IT

با توجه به پیچیدگی تهدیدهای موجود برای مرکز داده کارمندان باید هم برای حفظ امنیت تجهیزات IT، و هم برای امنیت فیزیکی آموزش ببینند و نمی‌توانند تحلیل امنیت IT را جدای از امنیت فیزکی انجام دهند.

۲-۳ طراحی امنیت در حوزه IT یا Cyber

طراحی امنیت در حوزه IT یا Cyber، امنیت داده‌های ذخیره‌شده و داده‌های در حال انتقال در شبکه را تأمین کرده و آن‌ها را در مقابل حملات و تهدیدهایی که الزامات محرمانگی ، صحت و در دسترس بودن را نقض می‌کنند، محافظت می‌کند. برنامه‌ریزی برای امنیت IT از محدوده این بخش خارج است و در بخش سیستم امنیت اطلاعات مرکز داده مورد بررسی قرار می‌گیرد.

۲-۴ طرح امنیتی برای مرکز داده[3]

طرح امنیتی باید جامع، ولی شفاف و ساده باشد، تا به سادگی خوانده‌شده و قابل فهم باشد. این طرح را باید طبق برنامه‌ی زیر، بازبینی و به روزرسانی کرد:

- سالانه یک‌بار،
- بعد از هرگونه ساخت و یا تغییر اساسی در مرکز داده، و فضاهای مرتبط با آن،

3. Data Center Security Plan

• بعد از هرگونه ساخت و یا تغییر اساسی در مرکز داده، هنگامی که مرکز داده در یک زمین یا ساختمان چند منظوره مستقر شده است،
• بعد از هرگونه اختلال امنیتی یا خرابی واردشده به سیستم ،
• هنگامی که تغییر امنیتی در سطوح محلی، منطقه‌ای و یا ملی این الزام را ایجاد کند.

پیش از طراحی هرگونه طرح امنیتی، طراحان مرکز داده باید آنالیز ریسک دقیقی از جایگاه فعلی و آینده‌ی سایت تهیه کنند و این طرح را با توجه به تمامی ریسک‌های شناخته‌شده در آنالیز خود، تهیه نمایند. طرح امنیتی مرکز داده باید وظایف دپارتمانی هر جز را مشخص کند ، از جمله:

• مدیریت،
• امنیت IT،
• تجهیزات،
• امور مالی،
• منابع انسانی،
• فناوری اطلاعات،
• امنیت فیزیکی،
• خریدها،
• عملیات.

در طرح امنیتی نقش و وظایفی که امنیت IT یا شبکه می‌تواند در حمایت از امنیت فیزیکی انجام دهد باید مشخص شود. پلان امنیت مرکز داده باید جزئیات راه‌کارهای مقابله با خطرات برای محافظت از هریک از موارد زیر را در خود گنجانده باشد:

• محافظت از جان نیروهای مرکز داده،
• محافظت از اموال فیزیکی،
• محافظت از اموال الکترونیکی.

کارکنان باید در موارد امنیتی مرتبط به آنان، آموزش ببینند. این آموزش باید در طول اجرای طرح، انجام‌شده و در زمان‌های مختلف، تجدید شود.

سرویس‌دهندگان امنیتی، هنگام کار بر روی تجهیزات اعلام خطر، باید کنترل شوند. در این طرح بهتر است که جزئیات دستور کار سرویس لازم روی این سیستم‌ها بیان شود تا از انجام عملیات غیرمجاز روی این سیستم‌ها، جلوگیری شود.

طرح امنیتی، می‌تواند شامل موارد زیر باشد:

• روش‌های مجاز برای ازبین‌بردن اسناد چاپ‌شده، مغناطیسی و سایر مدیاها،
• بسته‌های رسیده در کجا و توسط چه کسانی باید باز و جابه‌جا شوند،
• دسترسی و جابه‌جایی مدیاهای قابل انتقال مانند دیسک‌های نوری و هاردهای قابل انتقال،
• کنترل، جابه‌جایی، انبار و نگهداری از فیلم‌های ذخیره‌شده‌ی دوربین‌های CCTV،
• راهنمای مکتوب برای پاسخ به اعلام خطرهای مرتبط با CCTVها،
• برنامه‌ی دقیق به‌همراه جزئیات برای اعلام، پاسخ عملیات، هنگام رویدادهای فوری در کنار مشخص کردن خطرات طبیعی (مانند سیل، زلزله، برف، یخ، سونامی، طوفان، گرما/ سرمای شدید، طوفان خاک و شن، رعدوبرق و ...)، فنی (مانند انفجار، آتش، فروریختن ساختمان، اختلالات ارتباطی و ...) و انسانی (مانند اقتصادی، تروریستی و ...)،
• استفاده از سیستم‌ها و فرایندهایی که پیش از حادثه می‌توان انجام داد تا مرکز داده برای این گونه حوادث آماده شود و بتواند در مقابل آنان مقاومت کند و پس از حادثه، به‌کار خود ادامه دهد،
• قسمت بازسازی سانحه (DR[4]) و عملیات پس از آن، باید سالی یک‌بار و پس از هر کدام از موارد زیر بازبینی شود:

• تشخیص حوادث جدید،
• تغییر قوانین،
• تغییر ساختارها،
• تغییرات اساسی در سایت، کمپ و یا ساختمان.

همچنین هر مرکز داده باید پیش از طراحی و در حین آن، بررسی و تحلیل امنیتی کاملی از اوضاع خود را داشته باشد و پس از راه‌اندازی و قرار دادن تجهیزات، سالانه این کار را انجام دهد. مسئولین، مهندسین و معماران امنیتی باید موارد زیر را ارزیابی کرده و توصیه‌های خود را به‌صورت مکتوب ارایه دهند عناوین این گزارش باید شامل موارد زیر باشد:

4. Disaster Recovery

- مشخص کردن امکانات ، تجهیزات و نیروهای مرکز داده،
- استخراج تهدیدات طبیعی ، فناوری و انسانی،
- احتمال ریسک،
- خرابی‌های گذشته و احتمالی آینده ساختمان،
- اثرات بالقوه این خرابی‌ها و ریسک آنان،
- راه‌کارهای احتمالی،
- آنالیز فایده/ هزینه این کارها.

۳ الزامات قانونی

محافظت از داده‌ها و تجهیزات رایانه‌ای که داده‌ها در آن قرار دارند و یا در آن پردازش می‌شوند، از الزامات قانونی به‌شمار می‌رود. بسته به اندازه سازمان و وابستگی آن به IT، سازگاری آن با قوانین دولتی باید در مدیریت اسناد و منابع شما، اثر مثبتی داشته باشد.

۳-۱ مقررات یا قانون‌های مؤثر امنیتی

قوانین و الزامات در کشورها و مناطق مختلف متفاوت است. طراحان باید از این قوانین که به حفظ محرمانگی داده‌ها، خروج تصادفی یا عمده داده‌های مالی، پزشکی، شخصی و امنیت ملی مرتبط می‌شود، آگاه باشند. برخی از این پارامترها که در طراحی مرکز داده تأثیرگذار است را می‌توان این‌گونه نام برد:

- Sabanes- Oxley،
- استانداردهای مخصوص برخی از صنایع ویژه(مانند صنایع نظامی)،
- استاندارد پردازشی فدرالی[5] آمریکا،
- (HIPAA) بیمه سلامت و رفتار جوابگویی[6]،
- استانداردهای حریم خصوصی اروپا[7].

هدف اصلی این قوانین، حفظ سرمایه‌گذاران، کارمندان و عموم کارمندان از تهدیداتی مثل انتشار اطلاعات شخصی تا فروریختن کل سازمان است. طراحان و مهندسین امنیت مرکز داده، نباید دید مکانیکی و چک‌لیستی به این قوانین داشته باشند. باید به آنان از نگاه آنالیز ریسک از بالا به پایین نگاه کرد.

۴ افزایش امنیت با استفاده از طراحی طبیعی

موانع طبیعی و یا احساس دیده‌شدن ناخوداگاه در محیط، خود از پارامترهایی است که به افزایش امنیت کمک می‌کند. در طول طراحی و یا بازسازی مرکز داده، به‌کارگیری راهبردها و پیشنهادات افزایش امنیت از طریق طراحی محیطی (CPTED[8]) ، کمک بسیاری به امنیت مرکز داده می‌کند. سه اصلی که در ادامه می‌آیند، اصول طراحی براساس CPTED است.

۴-۱ کنترل دسترسی طبیعی

معماران یا طراحان امنیت مرکز داده، باید از مزیت‌های کنترل دسترسی طبیعی برای هدایت عابران هنگام ورود و خروج به سایت، ساختمان، اتاق و یا هر محیط مرتبط با مرکز داده استفاده کنند؛ مانند قراردادن درها در محل‌های خاص، استفاده از موانعی که مسیرهای عبوری را محدود می‌کند.

هرکدام از نواحی مرکز داده، با توجه به حساسیت تجهیزات و امکانات موجود در آن، باید به سطوح حفاظتی تقسیم‌بندی شوند. در واقع، تمامی نواحی از جمله اتاق‌های پشتیبانی، اتاق‌های اداری، لابی‌ها، نواحی اختصاص‌یافته به سرویس دهندگان، اتاق تجهیزات و ...

۴-۲ نظارت طبیعی

مفهوم نظارت طبیعی، به این معناست که با استفاده از ویژگی‌های محیطی و فیزیکی، مانند قراردادن مسیرهای عبوری، فضاهای باز، الگوی رفت‌وآمد عابران و مناطق کاری به‌صورت‌های خاص، فعالیت داخل محیط را توسط بیرونی‌ها و فعالیت بیرون را توسط افراد داخل سایت، قابل دیدن کنیم. بدین صورت که احساس دیده‌شدن در تمامی این نواحی ایجاد شود. طراحی اتاق‌ها، مسیرهای عبوری، فضاها و سایت‌ها، باید به‌گونه‌ای باشد که راه‌های زیادی برای کنترل رفتار و یا رفت‌وآمدهای غیرمجاز، وجد داشته باشد. تا حد امکان، کارکنان مرکز داده، باید احساس امنیت و راحتی در محیط خود داشته باشند.

۴-۳ ایجاد احساس مالکیت

مفهموم ایجاد احساس مالکیت، بدین معناست که فضایی ایجاد شود تا کارکنان آن محیط، احساس تعلق و یا عضویت داشته باشند. به‌صورتی‌که اگر

5. Federal Processing Standrd
6. Health Insurance and Accoutability Act
7. European Privacy Standards
8. Crime Prevention Through Enviromental Design (CPTED)

فـردی غیرمجـاز، اتفاقـی و یـا عمـدی وارد آن محیـط شـد، احسـاس قرارداشـتن در جـای نامناسـب، برایـش ایجادشـده و کامـلا قابـل تشـخیص باشـد. ایـن کار باعـث می‌شـود کـه افـراد غیرمجـازی کـه قصـد ورود آنـان بـه نواحـی محـدود شـود. بـرای نمونـه، می‌تـوان بـا قـراردادن علائـم و مرزهایـی مشـخص، نواحـی کنترل‌شـده و عمومـی را از یکدیگـر جـدا کـرد، به‌گونـه‌ای کـه اگـر کسـی وارد ناحیـه دسترسـی محـدود شـود، افـراد مجـاز زیـادی او را ببیننـد.

۵ کنترل دسترسی

تمامـی سیسـتم‌های کنتـرل دسترسـی، بایـد اجـازه‌ی خـروج اضطـراری تجهیـزات را تـا جایـی کـه بـا قوانیـن قابـل اعمـال سـاختمان مطابـق اسـت، در اختیـار قـرار دهنـد. طـراح مرکـز داده، بایـد بـا تمامـی قوانیـن AHJ[۹] سـازگار باشـد.

تمامـی نقـاط دسترسـی شـامل ورودی‌هـای پشـتیبانی، درهـای ورود تجهیـزات و خروجی‌هـای اضطـراری، بایـد از نوعـی کنتـرل دسترسـی اسـتفاده کننـد.

روش‌هـای احـراز هویـت، بایـد شـامل یـک یـا چنـد مـورد از مـوارد زیـر باشـد:

- نـوع ۱: چیزهایـی کـه شـخص موردنظـر دارد (ماننـد کلیدهـا، کارت‌هـا و ...)،
- نـوع ۲: چیزهایـی کـه او می‌دانـد (ماننـد کلمـات عبـور، کدهـا و ...)،
- نـوع ۳: هویـت او (ماننـد تشـخیص توسـط نگهبـان، داده‌هـای بیومتریـک، اثـر انگشـت و ...).

در صـورت امـکان، اتـاق رایانـه و دیگـر مناطق حسـاس، باید از احـراز هویـت چندگانـه کـه یکـی از آنـان، ویژگی‌هـای بیومتریـک اسـت، اسـتفاده کنـد، مثـلا اسـتفاده از کارت الکترونیکـی اثـر انگشـت بـرای احـراز هویـت به‌منظـور ورود بـه اتـاق رایانـه.

توصیـه می‌شـود کـه فهرسـتی از کارکنـان و افـراد طـرف قـرارداد کـه بایـد بـه نواحـی خاصـی دسترسـی داشـته باشـند و کلیـد، کارت، کلمـات عبـور و ماننـد آن را در اختیـار دارنـد، تهیـه شـود و هـرگاه کـه دیگـر نیـازی بـه ادامـه‌ی دسترسـی آنـان وجـود نـدارد، دپارتمـان منابـع انسـانی بـا بخشـی کـه آن فـرد در آن شـاغل بـوده اسـت، به مسـئول سیسـتم‌های دسترسـی اطـلاع دهـد تـا تغییـرات لازم در سیسـتم، سـریعا اعمـال شـود.

در صـورت امـکان، علائـم هشـداردهنده‌ای نیـز از طـرف سیسـتم کنتـرل دسترسـی بـه جایـی دیگـر (محلی یـا دور) ارسـال شـود تـا پاسـخ‌های لازم نیـز از آنـان دریافـت شـود.

ایـن مکان‌هـا معمـولا شـامل مـوارد زیـر اسـت:

- شرکت دیده‌بانی دورافتاده‌ی طرف قرارداد،
- ایستگاه نگهبانی اصلی مجزا،
- ایستگاه نگهبانی در ساختمان دیگر،
- ایستگاه نگهبانی در همان ساختمان.

در طـرح امنیـت، طـرح DR و سیسـتم‌های کنتـرل دسترسـی، بایـد بـرای اعتصـاب احتمالـی کارگـران مرکـز هـم تمهیداتـی دیـده شـود، بـرای نمونـه، سیسـتم کنتـرل دسترسـی، محدودیت‌هایـی بـرای آن کارگـران ایجـاد نمایـد تـا اوضـاع بـه حالـت عـادی برگـردد.

۵-۱ مکانیسم‌های قفل

مکانیسـم‌های قفـل، بـه دو دسـته تقسـیم‌بندی می‌شـوند کـه هرکـدام، انـواع و سـطوح امنیتـی خـاص خـود را دارنـد:

- مکانیکی:

- دندانه‌دار،
- اهرمی،
- زبانه پینی،
- زبانه ویفری،
- رمزی از نوع شماره‌گیر،
- وسـایل مکانیکـی بـرای تجهیـز درگاه‌هـای ورودی[۱۰] و سـیم‌ها[۱۱]،

- ترکیبی- الکتریکی و مکانیکی

- قفل کلیدی الکتریکی،
- چفت الکتریکی،
- کوبه‌ی الکتریکی،
- پلکانی،
- مجموعه قفل الکتریکی،
- قفل الکترومغناطیسی،
- قفل تیغه‌ای.

طـرح امنیـت مرکـز داده بایـد قبـل از انتخـاب قفل‌هـای مناسـب بـرای هـر منطقـه، یـک ارزیابـی کامـل از میـزان

۹. سازمان یا ارگانی که قدرت قانون گذاری دارد، مثلا شهرداری که می‌تواند در طرح ساختمان‌ها قوانین خاصی را اعمال کند (Authority Having Jurisdiction)
10. Ports
11. Cords

ریسک و آسیب‌پذیری داشته باشد.

انتخاب نوع قفل‌ها در برنامه‌ریزی مرکز داده به پارامترهای متفاوتی وابسته است، مانند:

- تعداد کل قفل‌ها،
- دسته‌بندی فضاها،
- جمعیت‌شناسی و میزان تغییر در تعداد کارمندان و افراد طرف قرارداد،
- نوع امکانات و تجهیزات،
- آمار جرائم محلی،
- آنالیز ریسک،
- به‌کارگیری امکانات دیگر در امنیت فیزیکی.

مهارت لازم برای بازکردن قفل و اثر روانشناختی نوع قفل انتخابی، باید در نظر گرفته شود. برخی از آسیب‌پذیری‌های قفل‌های مکانیکی مانند فشار، جدا شدن خود درب از چهارچوب ، کپی از کلیدها و دزدیدن آن‌ها را باید هنگام انتخاب قفل در نظر داشت.

۵-۲ درها

مقررات زیر که توسط AHJ اصلاح‌شده و پذیرفته شده است، به‌طور کامل به کار خواهد رفت:

توصیه می شود که درهای مرکز داده و اتاق رایانه، شرایط زیر را برآورده کنند:

- نصب حسگری در سمت خروجی، در را برای عابری که به آن نزدیک می‌شود باز کند،
- سیستم قفل از نوع مقاومت به خرابی باشد،
- مداری مستقل باید وجود داشته داشته که در شرایط اضطرار، مانند آتش‌سوزی، بتواند در را باز کند،
- بازکننده‌ی دستی، در کنار در قرار دارد که هنگام درخواست بازشدن دستی در، مستقیما به مدار قفل دستور بازشدن داده و کمینه ۳۰ ثانیه در را باز نگه دارد،
- سیستم آلارم آتش باید بتواند درها را باز کرده و تا راه‌اندازی مجدد دستی سیستم، درها را باز نگه دارد؛ در مواردی که امنیت شدیدتری برای مرکز داده مورد نیاز است، تأخیر در بازشدن مجدد در، مفید خواهد بود (مثلا ۴۰ ثانیه بین هر بار بازشدن)،
- با شروع شرایط هشدار در سیستم هشدار آتش‌سوزی ساختمان یا فعال‌سازی سیستم آبپاشی ساختمان، در به‌طور خودکار باز می‌شود و تا زمانی که سیستم هشدار آتش به‌صورت دستی دوباره تنظیم نشود، در باز نگه داشته می‌شود،
- با شروع فرایند آزادسازی یک هشدار شنیداری و/ یا یک سیگنال دیداری در نزدیکی در فعال شود،
- بعد از آزادسازی، قفل‌شدن تنها به‌وسیله دست انجام شود،
- درهای خروجی باید با دوربین کنترل شوند تا در صورت هرگونه اتفاق، کارمندان امنیت بتوانند با بررسی فایل آرشیوشده، به بررسی و تحلیل آن حادثه بپردازند. زمان تأخیر، باید با توجه به زمان پاسخ‌گویی کارمندان حراست و اطفا محاسبه شود.

۵-۳ کنترل دسترسی الکترونیکی

سیستم‌های کنترل دسترسی الکترونیکی (EAC[12]) باید بتوانند حرکات را مستقلا از نقاط مختلف ردیابی کنند. هر یک از کارکنان، باید کد احراز هویت، کارت و یا هر وسیله احراز هویت فیزیکی یا الکترونیکی مخصوص به خود را داشته باشد تا سیستم کنترل دسترسی الکترونیکی خودکار بتواند موارد زیر را کنترل و ذخیره کند:

- ساعت ورود و خروج،
- هویت فرد واردشونده،
- مکانیسم اجازه‌ی دسترسی به افراد.

برای کنترل دسترسی می‌توان از سیستم‌های لمسی دیجیتال[13] (که برای بازشدن، کد ورودی می‌خواهند)، کارت الکترونیکی[14] و سیستم‌های بیومتریکی[15] (مانند اثر انگشت، تشخیص چهره و چشم) و یا ترکیبی از این‌ها، کمک گرفت.

۶ آلارم‌ها

حسگرهای صوتی معمولا در نواحی اطراف مرکز داده استفاده می‌شوند تا صداهای اطراف محل محافظت‌شده را تشخیص و ذخیره نمایند و صداهای اضافی ناشی از ترافیک و یا هوا را در اطراف مسیرهای ارتباطی، فیلتر کنند و درصورتی‌که تماس، برش و یا اثری دیگر بر روی این مسیرها تشخیص داده شد، اعلام خطر نمایند.

12. Electronic Access Control (EAC)
13. Touchpads
14. Card Systems
15. Biometrics

حسگرهای خازنی برای کنترل میدان‌های الکترونیکی در نواحی خاصی از سایت مرکز داده استفاده می‌شوند تا تجهیزات حساس به این تغییرات، کنترل شوند. حسگرهای الکترومکانیکی مانند برخی کابل‌ها، فویل و صفحات فشاری و مغناطیسی، حرکت و فشار ناشی از حرکت را کنترل می‌کنند. حسگرهای شیشه نیز، که شکستگی شیشه‌ها را کنترل می‌کنند، باید نسبت به اختلالات الکترومغناطیسی ایمن باشند.

حسگرهای پسیو فروسرخ (PIR[16]) ، معمولا در جاهایی قرار می‌گیرند که عابران در مرکز داده، حتما در دید آنان قرار داشته باشند تا بتوانند رفت‌وآمدها را کنترل کنند. همچنین در جاده‌هایی که پیش از این تنها از حفاظ‌های فیزیکی استفاده می‌شد (حاشیه مراکز داده، حفره‌های کنترلی برای تجهیزات و مانند آن)، می توان از این حسگرها استفاده کرد. شرایطی که باعث ایجاد آلارم‌های ناخواسته می‌شوند عبارتند از:

- تغییرات ناگهانی دما،
- نور مستقیم خورشید،
- حشرات،
- اختلالات فرکانسی رادیویی.

حسگرهای فتوالکتریک در داخل و یا خارج مرکز داده، جایی که باید طیفی از نورهای نامرئی مانیتور شوند و شکستگی آنان کنترل شود استفاده می‌شوند. آلارم‌های ناخواسته با برخی شرایط محیطی مانند برف و باران شدید و یا عبور حیوانات ایجاد می‌شود. حسگرهای فراصوتی و ماکروویو، مانند PIRها عمل می‌کنند، با این تفاوت که نسبت به امواج صوتی حساس هستند.

حسگرهای لرزشی در جاهایی که امکان خرابی و یا نفوذ از دیوار و یا کف در اتاق‌های مهم وجود دارد، استفاده می‌شوند، مانند اتاق انبار.

۷ کنترل و نظارت

امنیت، از دو نوع نظارت بهره می‌گیرد، فیزیکی و فنی. نظارت فیزیکی اساسا توسط انسان‌ها انجام می‌شود که خارج از محدوده‌ی این استاندارد است. نظارت فنی از تجهیزات الکترونیکی استفاده می‌کند که عمدتا دوربین‌های CCTV هستند. دوربین‌های مدار بسته یا CCTV این امکان را فراهم می‌کنند که چند منطقه را به‌طور هم‌زمان کنترل کنیم. گزارشی از وقایع هنگام حوادث و یا بروز آلارم‌ها داشته باشیم و در موارد بروز هرگونه جرم، سندی قابل دفاع برای مرکز داده ارایه د هیم.

پارامترهایی چون مکان دوربین‌ها، تعداد فریم در ثانیه، شفافیت تصویر، نور محیط و موارد دیگر، باید با توجه به ارزیابی ریسک‌های ممکن و خطرات احتمالی مشخص شود. بهتر است که از یک مشاور امنیت در مورد تعیین مناطق حساس و ارزیابی پارامترهای محیطی، عملیاتی و فنی بهره گرفت و پس از آن، طرح دوربین‌های CCTV را تأیید کرد. نور محیط، به‌ویژه در محیط‌های باز، برای تشخیص چهره، اتومبیل‌ها و فعالیت‌های خاص، بسیار اهمیت دارد و در بهره‌گیری آینده از رکوردهای ثبت‌شده، بسیار تعیین‌کننده است. جانمایی دوربین‌ها نیز باید به‌گونه‌ای باشد که در مقابل سرقت و آسیب ایمن باشد. به درستی در جای خود محکم شود، از دسترس عابران و اتومبیل‌ها دور باشد، در محفظه ای امن قرار داده داشته و در مقابل سرما و گرما محافظت شود، در صورت لزوم، در موقعیت‌های با ریسک بالا از آلارم‌هایی مخصوص استفاده نموده و اگر از دوربین‌های IP استفاده می‌شود، پروتکل SNMP برای آنان فعال شود که در صورت جداشدن از شبکه معلوم شود.

در انتخاب دوربین نیز باید پارامترهای کارایی آن مانند شفافیت، نسبت سیگنال به نویز، اندازه فیزیکی، قابلیت‌های IP و PoE بررسی شود.

دوربین‌های ثابت، یک بار تنظیم‌شده و سپس محیط تعیین‌شده را کنترل می‌کنند. دوربین‌های PTZ[17]، قابلیت کنترل جهت و عدسی را دارند که در صورت لزوم، می‌توان نقاطی را که به کنترل بیشتری در زمان خاصی نیاز دارد، تحت پوشش در آورد. در مکان‌هایی که نور کافی ندارند، باید از دوربین‌های خاص این محیط‌ها استفاده کرد، برای نمونه، دوربین‌هایی که در روز تصویر رنگی و در شب، تصویر تک رنگ از محیط ارایه می‌کنند، دوربین‌های فروسرخ که با نوری که با

16. Passive Infrared
17. Pan – Tik - Zoom

چشم دیده نمی‌شود، تصویری واضح از محیط تاریک تهیه می‌کند.

برخی دوربین‌ها، آنالیزکننده‌ی شکل دارند که می‌توانند حرکاتی خاص را تشخیص دهند. می‌توان از این دوربین‌ها برای نواحی بسیار حساس، یا دارای ریسک بالا و یا مکان‌هایی که ثبت تمامی لحظات در ۲۴ ساعت روز و ۷ روز هفته لزومی ندارد، استفاده کرد. بهتر است که ترکیب نظارت CCTV با سیستم آلارم کنترل دسترسی، در پلان امنیت مرکز داده گنجانده شود. برای نمونه، فعال‌شدن و تمرکز دوربین PTZ در هنگام وقوع آلارم در مکانی خاص و یا هنگامی که دو نفر با یک کارت هویت وارد مرکز داده می‌شوند.

استفاده از SNMP شدیدا توصیه می‌شود، برای نمونه، در مواردی که دسترسی غیرمجاز به زیرساخت فیزیکی دوربین‌ها رخ داده و تلاشی در اضافه یا کم‌کردن زیرساخت فیزیکی شناسایی شود، به موقع اطلاع داده شود.

۸ موانع فیزیکی

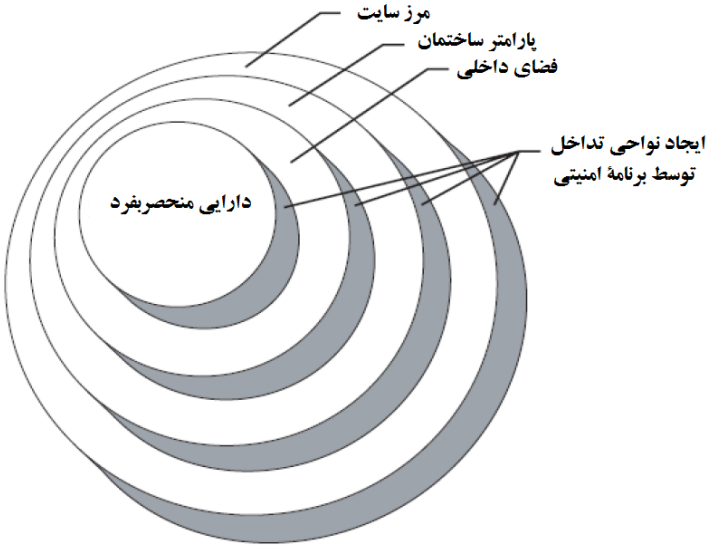
تعاریف مورد استفاده در مورد به‌کارگیری موانع به این ترتیب هستند:

مانع: یک مانع مصنوعی یا طبیعی که برای کنترل دسترسی به چیزی، یا کسی، اعم از حیوانات، وسایل نقلیه، یا هر شیء متحرک دیگر استفاده می‌شود.

منطقه‌ی شفاف‌سازی‌شده/ آزاد[18]: جداسازی منطقه‌ای، یک مانع در بیرون از ساختمان‌ها یا هر شکل از اختفای طبیعی یا مصنوعی.

بخش‌بندی‌کردن: جداسازی اموال و دارایی‌ها از خطرات احتمالی مربوط به طراحی ساختمان یا راه‌کارهایی دیگر، شامل موانع فیزیکی.

طراحی لایه‌ای: به‌کاربردن لایه‌های متعدد جداکننده‌ها و موانع، دیگر راه‌کارها، یا ترکیبی از هر دو است تا ممانعت و تأخیر را به بیشترین حد برساند. شکل زیر، این لایه‌ها را نمایش می‌دهد (شکل ۲).



شکل ۲: لایه‌های امنیت

18. Clear Zone

مانع طبیعی: هر چیز طبیعی که مانع از دسترسی می‌شود، شامل کوه‌ها، دریاچه‌ها، بیابان‌ها، باتلاق‌ها.

مانع روانی: یک قطعه، مانع یا فقدان مانع که حضورش به تنهایی از دسترسی یا نفوذ غیرمجاز ممانعت می‌کند.

مانع ساختاری: چیزی که به‌صورت فیزیکی از دسترسی، فعالیت، تخریب، یا جابه‌جایی اموال مرکز داده جلوگیری می‌کند.

سه دسته‌ی کلی مانع را می‌توان به‌عنوان موانع فیزیکی نام برد:

- دیواره‌های بیرونی ساختمان،
- حصارها،
- سازه‌های سنگی.

موانع ساختاری غیر قابل نفوذ نیستند، اما عمدتا برای تأخیر در ورود به‌کار می‌روند، تا سیستم‌های دیگر بتوانند شناسایی انجام دهند و به کارکنان، نگهبانان، ایستگاه‌های کنترل، یا عوامل اجرای قانون اطلاع دهند. استفاده خوب از موانع، کمینه فرد مزاحم را مجبور به ترک مواضع نفوذ و رهاسازی هم‌زمان یک اقدام انسانی یا الکترونیکی می‌کند.

موانع محافظ برای محافظت در برابر انفجارهای عمدی و تصادفی به‌کار می‌رود. طراح امنیت مرکز داده باید در طراحی خود به مقاومت نسبی که موانع گوناگون در برابر انفجار و موج پس از آن از خود نشان می‌دهند نیز توجه کند. در فهرست زیر مقاوم‌ترین موانع در برابر انفجار آورده شده است:

- دیوارهای بتنی ضخیم تقویت‌شده،
- دیوارهای بتنی یا آجری ضخیم بدون اینکه تقویت شده باشد،
- دیوارهای بتنی تقویت‌شده،
- سنگرهای خشتی ضخیم،
- دیوارهای ساختمانی با چارچوب آهنی،
- دیوارهای چوبی محکم،
- دیوارهای آجری معمولی،
- شیشه‌های تقویت‌شده با سیم،
- شیشه‌های معمولی.

جدول (۱) ضخامت موردنیاز دیوار بتنی در مقابل اثرات ثانویه انفجار در فواصل مختلف را نشان می‌دهد:

جدول ۱: ضخامت دیوار بتنی برای محافظت در برابر انفجار[۱]

فاصله تا انفجار (m)	سرعت (m/s)	ضخامت دیوار بتنی (mm)
۳۰٫۵	۶۱۰	۳۰۵
۶۹	۶۱۰	۲۴۵
۱۵۲	۴۵۷	۱۷۸
۲۷۴	۳۰۵	۱۲۷
۷۱۶	۱۵۲	۶۴

موانع را باید به‌صورت لایه‌ای طراحی کرد و تجهیزات و سیستم‌هایی که محافظت شدید نیاز دارند، داخل لایه‌های متعددی قرار گیرند تا دسترسی به آنان تا حد ممکن با تأخیر باشد. این موانع باید نسبت به خروج تجهیزات یا جابه‌جایی غیرمجاز نیز عکس‌العمل نشان دهند و آن را به تأخیر اندازند و مانع شوند. موانع باید برای جلوگیری و تأخیر در دسترسی یا آسیب به سایت، ساختمان‌ها یا مناطق مرکز داده به‌کار رود.

همچنین این موانع می‌توانند از دسترسی بصری به ساختمان یا اموال جلوگیری کنند. موانع دسترسی بصری، متجاوز بالقوه را از شناسایی موقعیت اموال یا وجود آن، باز خواهد داشت. همچنین می‌توان از این موانع به‌گونه‌ای استفاده کرد که دسترسی بصری به مرکز داده را نیز محدود کند، به‌صورتی‌که دیگران از وجود مرکز داده در آن محل مطلع نشوند، مانند قراردادن مرکز داده در میان انباری قدیمی یا جنگلی انبوه که هیچ نشانی از مرکز داده و وجود آن نمایان نشود.

موانع باید سه نوع از نفوذ را به تأخیر اندازند یا جلوگیری کنند:

- اجباری،
- با فریب و پنهان‌کاری،
- تصادفی.

زمانی که موانع در بیرون از ساختمان به‌کار می‌روند، یک منطقه‌ی شفاف‌سازی‌شده که اختفا را از خود نشان می‌دهد، مانند درختان، علف‌های هرز، زباله،

ساختمان‌های کوچک یا وسایل نقلیه محافظت می‌شوند.

دستورالعمل‌های مناطق شفاف‌سازی‌شده اطراف موانع مورد استفاده در پارامترهای سایت مرکز داده شامل:

- مناطق شفاف‌سازی‌شده باید از هر دو طرف محافظت شوند،
- قسمت بیرونی مانع باید کمینه ۶ متر (۲۰فوت) دورتر از همه‌ی موانع بصری، مانند ساختمان‌ها، رودخانه‌ها، پارکینگ‌ها و اشیای طبیعی مانند درختان، صخره‌ها و تپه‌ها باشد،
- قسمت داخلی موانع مورد استفاده برای یک محدوده‌ی دفاعی، باید ناحیه‌ای را محافظت کند که کمینه ۱۵ متر (۵۰ فوت) دورتر از ساختمان‌ها یا دیگر اموال و دارایی‌ها باشد.

۸-۱ موانع وسیله‌ی نقلیه

طراح امنیت مرکز داده باید در طراحی خود افزایش استفاده از وسایل نقلیه و آسیب کلی وارده به ساختمان‌ها و اشخاص اعم از عمدی و سهوی را در نظر بگیرد.

موانعی که باید هنگام طراحی موانع حفاظتی برای ورودی‌ها و دیگر مناطق آسیب‌پذیر سایت مرکز داده و ساختمان‌ها در نظر گرفته شوند شامل موارد زیر است:

- حصارها[19]،
- میله‌های محافظ فلزی[20]،
- موانع نقلیه بتنی،
- موانع بتنی،
- تیرک‌های فلزی،
- ترکیبی از مواد مانند تایرها، تراورس‌های راه‌آهن و اتصالات زمین.

۸-۲ قسمت خارجی ساختمان

توانایی قسمت خارجی ساختمان در به تأخیر انداختن حملات احتمالی به مرکز داده باید ارزیابی شود. هنگام طراحی مرکز داده، باید عملکرد همه‌ی سطوح خارجی ساختمان به‌عنوان موانع امنیتی ارزیابی شود. در مورد ساختارهای موجود بازسازی‌شده به‌عنوان مرکز داده، باید یک بررسی دقیق از ساختار فیزیکی و نقشه‌های معماری موجود که در طول طراحی و ساخت اولیه ایجاد شده‌اند، انجام شود.

به‌منظور ارزیابی نقشه‌های معماری و بررسی فیزیکی کارایی هر دیوار، سقف، یا کف ساختمان، کمینه باید موارد زیر در نظر گرفته شوند:

- میزان فضای موجود بین دیوارها، سقف و کف اتاق‌ها،
- احتمال خطر شناخته‌شده توسط فضاهای تأمین هوای موجود یا مطابق با HVAC ،
- اصلاح و تعمیر دیوارها، سقف و کف اتاق‌های اصلی،
- ضعف‌های مشخص‌شده در طول بررسی فیزیکی،
- دسترسی به پشت‌بام از ساختارهای مجاور،
- دسترسی به موتورخانه از طریق تونل‌زدن،
- دسترسی به موتورخانه از طریق تونل‌های شبکه فاضلاب، مترو و دیگر راهروهای زیرزمینی.

به‌منظور افزایش مقاومت در برابر نفوذ، شش قسمت هر اتاق ساختمان مرکز داده (کف، سقف و چهار دیوار عمودی)، باید با بتن تقویت‌شده یا دیگر مواد بنایی تقویت‌کننده ترکیب شوند.

جدول۲: آسیب‌پذیری موانع گوناگون در برابر وسایل نقلیه

آزمایشات موانع	وسایل نقلیه	آسیب موانع	آسیب وسایل نقلیه	آسیب سرنشینان
نرده‌های زنجیره‌ای	کامیون پیکاب ۳٫۴ تنی	نفوذ زیاد	رنگ خراشیده شده	بدون آسیب
دروازه دو سمت بازشو	کامیون پیکاب ۳٫۴ تنی	نفوذ زیاد	فرورفتگی‌های اندک	بدون آسیب
نرده‌های زنجیره‌ای کابل W/19mm (0.75in)	کامیون پیکاب ۳٫۴ تنی	نفوذ زیاد/ ایست وسایل نقلیه	آسیب وسیع در قسمت جلو	خطر آسیب
مانع پوشش بتن	کامیون پیکاب ۳٫۴ تنی	بدون نفوذ	آسیب زیاد	خطر آسیب
لاستیک‌ها	کامیون پیکاب ۳٫۴ تنی	بدون نفوذ	آسیب زیاد	خطر آسیب

19. Fences
20. Metal Highway Guard Rails

۸-۳ دیوارهای بتنی

دیوارهای بتنی، موانعی بسیار مفید هستند که نفوذ فیزیکی را با تأخیر زیادی مواجه می‌کنند. کارایی این دیوارها، به ضخامت دیوار و موادی که برای تقویت بتن استفاده می‌شود، بستگی دارد. دستورالعمل‌های کلی برای دیوارهای بتنی در بخش‌های زیر آورده می‌شود.

دیوارهای بتنی یا بلوکی که برای محافظت بارهای وارد بر ساختمان به‌کار می‌روند لزوما برای ایجاد تأخیر کافی به‌عنوان یک مانع مؤثر و کارامد طراحی نشده‌اند. دیوارهای بتنی تقویت‌شده حفاظت کمی در برابر نفوذ از خود نشان می‌دهند. برای امنیت مرکز داده، همه‌ی دیوارهای بتنی باید با میله‌های آهنی تقویت شوند. جدول (۳) سرعت نفوذ در یک دیوار ۳۰ سانتی‌متری بتنی تقویت‌شده را نشان می‌دهد.

دیوارهای بتنی بلوکی که هیچ ماده تقویت‌کننده‌ای ندارند، تقریبا هیچ مقاومتی در برابر نفوذ با استفاده از ابزار دستی کوچک ندارند. هنگام ساخت مرکز داده، دیوارهای بلوکی بتنی مورد استفاده باید دارای چند نوع روش تقویتی باشند که عموما شامل پرکردن هسته‌های تو خالی با بتن یا ملاط، کارگذاری میله، یا هر دو هستند.

• دیوارهای بتنی تقویت‌شده ضخیم ۱۰۰ میلی‌متری (۴ اینچی) عمدتا برای دیوار اتاق به‌کار می‌روند و مقاومت کمی را در برابر نفوذ با ابزار دستی ایجاد می‌کنند.

• دیوارهای بتنی تقویت‌شده ضخیم ۱۵۰ میلی‌متری (۶ اینچی) تأخیر بیشتری را از خود نشان می‌دهند، اما هنوز در برابر ابزار دستی و انفجارهای کوچک آسیب‌پذیر هستند.

• دیوارهای بتنی تقویت‌شده ضخیم ۲۰۰ میلی‌متری (۸ اینچی) عموما به‌عنوان دیوارهای محافظ و تحمل‌کننده بار هستند و همچنین با استفاده از ابزار دستی می‌توان در آن‌ها حفره ایجاد کرد.

• دیوارهای بتنی بزرگ‌تر از ۲۰۰ میلی‌متر (۸ اینچی) معمولا تنها در احداث طاق‌ها یا انبارهای مهمات مقاوم در برابر انفجار یافت می‌شوند.

جدول ۳: سرعت نفوذ در دیوار بتنی

بیشینه زمان دقیقه	کمینه زمان دقیقه	وزن تجهیزات kg (lb)	نیاز تجهیزات	نیاز مردم
۸٫۴	۲٫۸	۲۲ (۴۸)	مواد منفجره، صفحه‌ی تامپر، هیدرولیک دستی	۲
۸٫۴	۲٫۸	۱۸ (۳۹)	مواد منفجره، هیدرولیک دستی، پیچ‌های قطع‌کننده	۲
۵٫۸۵	۱٫۹۵	۱۰۲ (۲۲۵)	مواد منفجره، پلاتر	۱
۴۵٫۰	۱۵٫۰	۷۳ (۱۶۱)	چکش روتو، ضربه‌گیر، قطع‌کننده پیچ با نیروی هیدرولیکی دستی، ژنراتور	۲
۴٫۲	۱٫۴	۶۹ (۱۵۳)	مواد منفجره، صفحه‌ی تامپر، قطع‌کننده پیچ با نیروی هیدرولیکی دستی	۲

۸-۴ ورودی‌های ساختمان

ورودی‌های ساختمان معمولا برای یکی از اهداف زیر تعبیه می شود:

• ورودی (انسان و اتومبیل)،

• خروجی (انسان و اتومبیل)،

• تأمین نور طبیعی،

• ایجاد جریان هوا،

• جابه‌جایی وسایل و تجهیزات،

• خروج آب و امثال آن.

هر ورودی ساختمان که کمتر از ۵٫۵ متر از زمین ارتفاع دارد و بزرگ‌تر از ۶۲۰۰۰ میلی‌متر مربع است باید با موانعی، محافظت‌شده و مانیتور شود. ورودی‌های ساختمان باید مانند دیوارها و سقف، به سختی قابل نفوذ باشند. جدول (۴) زمان لازم برای نفوذ به درهای صنعتی را نشان می‌دهد.

درها معمولا از یکی از مواد زیر و یا ترکیبی از آن‌ها

ساخته می‌شوند:

- چوب،
- شیشه،
- فلز.

هنگام طراحی درهای مرکز داده، باید به موارد زیر توجه داشت:

- لولا و پیچ‌های آن باید همیشه در سمت محافظت‌شده‌ی درها قرار گیرد.
- لولاها را باید پرچ نمود یا به‌صورتی پوشاند که دسترسی غیرمجاز به آن غیر ممکن شود.
- چارچوب در را باید به صورتی امن به دیوارها متصل نمود.

جدول ۴: زمان نفوذپذیری درهای صنعتی

زمان مورد نیاز (دقیقه)	منطقه اصابت	Boise dB	روش نفوذ
۱٫۵-۰٫۵	صفحهٔ در	-	مواد منفجره
۲٫۵-۱٫۵	صفحهٔ در	۷۶-۷۰	حرارتی (Oxy-Lance)
۶-۲	صفحهٔ در	۶۴-۶۰	حرارتی(Cutting torch)
۰٫۵	اهرم پانیک[21]	-	نیروی مته
۱٫۵-۰٫۵	اهرم پانیک	۱۱۰-۷۲	Axe به‌وسیله فلز
۰٫۵	اهرم پانیک	۱۰۰-۷۶	Axe به‌وسیله شیشه
۵-۰٫۲۵	قفل	-	انتخاب قفل
۰٫۵	قفل	-	آچار
۰/۵	قاب قفل شده	۷۶-۷۴	اهرم میله
۱٫۵-۰٫۵	لولا	۷۳-۶۰	حرارتی (Cutting torch)
۳-۱	لولا	۷۵-۷۲	چکش و ضربه
۲٫۵-۱	لولا	-	مواد منفجره
۲-۰٫۵	شبکه/ پنجره	۱۰۰-۶۰	اهرم

پنجره‌هایی که در دیواره خارجی مرکز داده تعبیه می‌شوند تا نور طبیعی، جریان هوای طبیعی و دسترسی بصری را تأمین کنند، نه تنها برای اتاق رایانه و اتاق‌های امن مرکز داده موردنیاز نیستند بلکه اصلا توصیه هم نمی‌شوند.

انواع پنجره‌های مورد استفاده در ساخت‌وسازهای جدید شامل موارد زیر هستند:

- پنجره‌های سایبانی،
- پنجره‌های تک لنگه،
- پنجره‌های کشویی افقی،
- پنجره‌های کرکره‌ای،
- پنجره‌های تصویری،
- پنجره‌های طرحدار.

پنجره‌های تصویری باید تنها در دیواره‌های خارجی چارچوب مرکز داده کار گذاشته شوند.

پنجره‌های خارجی، باید در آنالیز ریسک امنیتی در نظر گرفته شوند و مواد لازم برای تقویت و ایجاد ساختارهای مستحکم بر روی آنان بررسی شود تا نفوذ را تا حد امکان با تأخیر مواجه کنند.

اگر یک یا تعداد بیشتری از دیوارهای اتاق رایانه، دیوار خارجی محسوب می‌شود نباید پنجره‌ای روی آن وجود داشته باشد.

۸-۵ مقاوم‌سازی شیشه‌ها[22]

مقاوم‌سازی پنجره‌ها و شیشه‌های استفاده‌شده در ساختمان مرکز داده، باید در طراحی و امن‌سازی مرکز داده در نظر گرفته شود. مقاوم‌سازی شیشه‌ها عبارت است از نوسازی تعویض شیشه‌ها یا ورقه‌های روکش‌دار شیشه‌ای یا پلاستیکی به‌منظور افزایش سطح ساختمان (به‌ویژه پنجره‌ها و درها) و افزایش مقاومت آن در برابر انفجار و امواج ناشی از آن،

21. Panic
22. Glazing

آتش‌سوزی و دیگر خطرها.

هنگامی که برای پرکردن ورودی‌های سطح خارجی، یا ورودی‌های دیوارهای داخلی ساختمان مرکز داده از شیشه استفاده می‌شود، باید خطرات احتمالی برای ساکنان و تجهیزات، هنگامی که یک انفجار اتفاق می‌افتد در نظر گرفته شود. اگر شیشه‌های داخلی یا خارجی شکسته شوند، حوادث ناخوشایند زیر رخ می‌دهد:

- دسترسی غیرمجاز،
- خسارت فیزیکی و جانی ناشی از خرده شیشه‌های تیز، به‌ویژه هنگامی که در اثر انفجار در هوا پرتاب می‌شوند،
- خسارت مالی به تجهیزات مرکز داده ناشی از خرده شیشه‌های تیز پرتاب‌شده در هوا در اثر انفجار،
- خسارت مالی و جانی ناشی از خرده شیشه‌های ریخته‌شده.

مطابق و همگام با الزامات منطقه‌ای و مقررات امنیتی، همواره باید از شیشه‌های تقویت‌شده با گرما در پنجره‌ها و درهای مرکز داده استفاده کرد. شیشه‌های مقاوم‌شده ۳ تا ۵ بار قوی‌تر از شیشه‌های معمولی هستند و به‌دلیل اثرات فرایند مقاوم‌سازی ریسک آسیب‌رسانی و خطر خرده شیشه‌های ناشی از انفجار یا نفوذ را کم می‌کنند.

طراح باید استفاده از شیشه‌های بر پایه‌ی آکریلیک و پلی‌کربنات را در درها و پنجره‌ها، به‌دلیل قدرت همه جانبه و مقاومت آن‌ها در برابر شکستن در نظر گیرد. این مواد امنیت را بهبود می‌بخشند و در مقایسه با شیشه‌های ضخیم در برابر شکستن ۱۷ مرتبه مقاوم‌تر هستند .

۸-۶ شیشه‌های مقاوم در برابر گلوله یا تقویت‌شده

در مواردی که خطر شلیک گلوله نیز وجود دارد، شیشه‌های مقاوم در برابر گلوله باید در طراحی مرکز داده در نظر گرفته شود. آنچه اهمیت دارد، بررسی دقیق خطرات احتمالی و سپس انتخاب شیشه‌ی مناسب برای مرکز داده است تا قبل از ارزیابی درست، شیشه‌های مقاوم در برابر گلوله استفاده نشود.

از آنجایی که شیشه‌های مقاوم به گلوله در ضخامت‌های گوناگون از ۱۹ میلی‌متر (۳.۴ اینچ) تا ۱۱۹ میلی‌متر (۴.۷ اینچ) قابل دستیابی و قابل ساخت هستند، ارزیابی کامل نوع و ماهیت حملات حائز اهمیت است. گستره‌ی حملات می‌تواند از حمله‌ی افراد با سنگ یا چکش تا تفنگ‌های بسیار قوی، توپ‌ها، تانک‌ها یا موشک‌ها باشد. احتمال ارزیابی ریسک و خطر قبل از انتخاب شیشه‌ی مقاوم در برابر گلوله بسیار مهم است.

طراحان امنیتی باید هشت سطح از مقاومت تعریف‌شده در UL ۷۵۲ را در نظر بگیرند که در آن‌ها میزان مقاومت بر پایه‌ی مهمات مورد استفاده و تعیین موقعیت و قالب‌گیری گلوله تعیین می‌شوند:

- سطح ۱: دارای ضخامت ۴٫۸ میلی‌متر (۳٫۱۶ اینچ)، جامد، فولاد ... با قدرت کششی ۳۴۵۰۰۰ کیلوپاسکال (۵۰۰۰۰psi) یا ۹ میلی‌متری با پوسته تمام مسی و هسته سربی، ۱۲۴ گرینی در سرعت ۳۵۸ متر بر ثانیه (۱.۱۷۵ft/s)- سه گلوله‌ای،
- سطح ۲: مگنون صاف سربی ۰٫۳۵۸، ۱۵۸ گرینی در سرعت ۳۸۱ متر بر ثانیه (۱٫۲۵۰ft/s)- سه گلوله‌ای،
- سطح ۳: مگنون سربی ۰٫۴۴، دستگاه برش دو لایه‌ای، ۲۴۰ گرینی در سرعت ۴۱۱ متر بر ثانیه (۱٫۳۵۰ft/s)- سه گلوله‌ای،
- سطح ۴: تفنگ کالیبر ۰٫۳۰ با هسته سرب و سر صاف، ۱۸۰ گرینی در سرعت (۲٫۵۴۰ft/s)- یک گلوله‌ای
- سطح ۵: تفنگ ۷٫۶۲ میلی‌متری با هسته سرب و پوسته مس، ۱۵۰ گرینی، ۸۳۸ متر بر ثانیه (۲٫۷۵۰ft/s)- یک گلوله‌ای،
- سطح ۶: تفنگ ۹ میلی‌متری با هسته سرب و پوسته کاملا مسی، ۱۲۴ گرینی، ۴۲۷ متر بر ثانیه (۱٫۴۰۰ft/s)- پنج گلوله‌ای،
- سطح ۷: تفنگ ۵٫۵۶-۷ میلی‌متری با هسته سرب و پوسته کاملا مسی، ۵۵ گرینی، ۹۳۹ متر بر ثانیه (۳٫۰۸۰ft/s)- پنج گلوله‌ای،
- سطح ۸: تفنگ ۷٫۶۲-۸ میلی‌متری با هسته سرب و پوسته کاملا مسی، ۱۵۰ گرینی، ۸۳۸ متر بر ثانیه (۲٫۷۵۰ft/s)- پنج گلوله‌ای.

۸-۷ شیشه‌های مقاوم در برابر ورود غیرمجاز یا تقویت‌شده

وجود تجهیزات گران قیمت در مرکز داده، ریسک سرقت را نیز بالا می‌برد. از این جهت، مقاومت پنجره‌ها و دیگر ورودی‌های مرکز داده در برابر ورود با اعمال زور با ابزارهای متفاوت، نیز باید سنجیده شود. برخی از معیارهای مورد استفاده برای ارزیابی مقاومت شیشه در برابر ورود با اعمال زور شامل:

- آزمون اثر تک فوتی،
- آزمون اثر چند فوتی،
- آزمون اثر پرانرژی،
- آزمون کارایی.

طراح امنیت مرکز داده همچنین باید از پنج دسته از تعاریف محافظت ASTM F۱۲۳۳ مطلع باشد که روش‌های مقاوم‌سازی را از سه جهت ۱) حمله بالستیکی ۲) ورود با اعمال زور و ۳) ترکیبی از دو روش قبل ارزیابی و مقایسه می‌کنند.

۸-۸ حصارها و موانع فلزی

به‌کار گیری حصار در اطراف ساختمان مرکز داده، باید با تمهیداتی دیگر همچون به‌کارگیری آلارم‌ها همراه باشد. چرا که به تنهایی برای مانع‌شدن از ورود و خروج افراد غیرمجاز کافی نیستند.

طراحان باید در نظر داشته باشند که حصاری به ارتفاع ۲٫۴ متر با سه ردیف از سیم خاردار در کمتر از ۱۰ ثانیه نفوذپذیر است. علاوه بر آن، باید در نظر داشت که لزوما حصارهای به‌کار رفته برای اتومبیل‌ها، مانعی برای انسان‌ها نخواهد بود و برعکس. از حصارها، بیشتر برای نمایش حدود مالکیت، ممانعت از ورود حیوانات و اتومبیل، و ایجاد احساس محیط حفاظت‌شده استفاده می‌شود.

ورودی‌های مرکز داده نیز نباید بیشتر از حد لزوم باشد که مشکلات عملیاتی همچون باز ماندن درها و قفل‌نشدن را به‌همراه خواهد داشت.

۹ نتیجه‌گیری و جمع‌بندی

مراکز داده مکان‌های امنی برای پردازش و نگهداری اطلاعات با قابلیت اطمینان و دسترسی بالا هستند. استفاده از این مراکز باعث می‌شود که تشکیلات اقتصادی و سازمان‌های مهم بتوانند با اطمینان از حفظ امنیت داده‌های خود در برابر دسترسی‌های غیرمجاز و سایر حوادث غیرمترقبه، امکان ارایه‌ی بی‌وقفه سرویس‌های خود به مشتریان را داشته باشند. لذا باید بیشینه امنیت فیزیکی در طراحی آن‌ها در نظر گرفته شود. برخی از مراکز داده هیچ پنجره و منفذی به بیرون ندارند و برخی از مراکز داده حساس از جداره‌ها و پارتیشن‌های شیشه‌ای ضدگلوله استفاده می‌کنند و برخی نیز برای محافظت، از دیوارهای دوجداره استفاده می‌کنند. دوربین‌های مدار بسته و قفل‌های امنیتی چند لایه نیز در آن‌ها به وفور استفاده می‌شود. همچنین با توجه به لزوم قابلیت دسترسی و بازدهی بالا و کمینه زمان از کارافتادگی، علاوه‌بر استفاده از فناوری‌های روز برای تجهیزات مرکز داده، افزونگی[۲۳] و پشتیبانی نیز درنظر گرفته می‌شود.

۱۰ منابع

۱ مقررات دارایی‌ها، ASIS جهانی

۲ استاندارد ANSI/BICSI 002-2011

3 Alliance for Telecommunication Industry Solutions (ATIS)

• ATIS 0600336, Engineering Requirements for a Universal Telecommunications Framework (2003)

4 American Society of Heating, Refrigerating, and Air-Conditioning Engineer (ASHRAE)

• ASHRAE 62.1, Ventilation for Acceptable Indoor Air Quality (2007);

• ASHRAE Best practices for Datacom Facility Energy Efficiency (2009);

• ASHRAE Datacom Equipment Power Trends and Cooling Applications (2005);

• ASHRAE Design Considerations for Data and Communications Equipment Centers (2009);

• ASHRAE Gaseous and Particulate Contamination Guidelines for Data Centers (2009);

• ASHRAE Structural and Vibration Guidelines for Datacom Equipment Centers (2008);

• ASHRAE Thermal Guidelines for Data Processing Environments (2009);

5 Consumer Electronics Association (CEA)

• CEA-310-E, Cabinets, Racks, Panels, and Associated Equipment (2005);

23. Redundancy

6 European Committee for Electrotechnical Standardization (CENELEC)

• CENELEC EN 50173-1, Information technology - Generic Cabling Systems – Part 1: General Requirements (2007);

• CENELEC EN 50173-5, Information technology - Generic Cabling Systems - Part 5 Data Centres (2007);

• CENELEC EN 50174-2, Information technology - Cabling installation - Installation planning and practices inside buildings (2009);

7 European Telecommunications Standards Institute (ETSI)

• ETSI EN 300-019, Equipment Engineering (EE) - Environmental conditions and environmental tests for telecommunications equipment

8- Institute of Electrical and Electronics Engineers (IEEE)

• IEEE 142-2007 (The IEEE Green Book), Recommended Practice for Grounding for Industrial and Commercial Buildings;

• IEEE 450-2002, IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented LeadAcid Batteries for Stationary Application;

• IEEE 484-2002, IEEE Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications;

• IEEE 493-2007 (The IEEE Gold Book), Recommended Practice for Design of Reliable and Commercial Power Systems;

• IEEE 1100-2005 (The IEEE Emerald Book), Recommended Practice for Powering and Grounding Electronic Equipment;

• IEEE 1106-2005, IEEE Recommended Practice for Maintenance, Testing and eplacement of NickelCadmium Batteries for Stationary Applications;

• IEEE 1115-2000, IEEE Recommended Practice for Sizing Nickel-Cadmium Batteries for Stationary Applications;

• IEEE 1184-2006, IEEE Guide for the Selection and Sizing of Batteries for Uninterruptible Power Systems;

• IEEE 1187-2002, IEEE Recommend Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications;

• IEEE 1188-2005, IEEE Recommended Practice for Maintenance, Testing and Replacement of Valve Regulated Lead-Acid Batteries (VRLA) for Stationary Applications;

• IEEE 1189-2007, IEEE Guide for the Selection of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications;

• IEEE 1491-2005, IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications;

• IEEE 1578-2007, IEEE Recommended Practice for Stationary Battery Electrolyte Spill Containment and Management;

9- International Electrotechnical Commission (IEC)

• IEC 61280-4-1:2009(E), Fibre-optic communication subsystem test procedures - Part 4-1: Installed cable plant - Multimode attenuation measurement;

• IEC 61280-4-2:1999, Fibre Optic Communication Subsystem Basic Test Procedures - Part 4-2: Fibre Optic Cable Plant - Single-Mode Fibre Optic Cable Plant Attenuation;

• IEC 61935-1:2005, Generic cabling systems-Communication cabling in accordance with ISO/IEC 11801- Part 1: Installed cabling;

• IEC 62305-3: 2006, Protection against lightning - Part 3: Physical damage to structures and life hazard;

10- International Organization for Standardization (ISO)

• ISO/IEC 11801:2002, Information technology - Generic cabling for customer premises;

• ISO/IEC TR 14763-2:2000, Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation of copper cabling;

• ISO/IEC 14763-3:2006, Information technology— Implementation and operation of ustomer premises cabling-Part 3: Testing of optical fibre cabling;

• ISO/IEC 24764:2010, Information technology - Generic cabling systems for data centres;

National Electrical Contractors Association (NECA)

• ANSI/NECA/BICSI 607, Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings (2010);

11- National Fire Protection Association (NFPA)

• NFPA 12, Carbon Dioxide Fire Extinguishing Systems (2008);

• NFPA 12A, Halon 1301 Fire Extinguishing Systems (2009);

• NFPA 13, Standard for the Installation of Sprinkler Systems (2010);

• NFPA 20, Installation of Stationary Pumps for Fire Protection (2010);

• NFPA 70, The National Electrical Code® (NEC®) (2008);

• NFPA 70E, Standard for Electrical Safety in the Workplace (2004);

• NFPA 72, National Fire Alarm Code (1999);

• NFPA 75, Standard for the Protection of Information Technology Equipment (2009);
• NFPA 76, Recommended Practice for the Fire Protection of Telecommunications Facilities (2009)
• NFPA 1600, Standard on Disaster/Emergency Management Business Continuity Programs (2007);
• NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems (2008);
• NFPA Fire Protection Handbook (2003);Telcordia
• Telcordia GR-63-CORE, NEBS Requirements: Physical Protection (2006);
• Telcordia GR-139, Generic Requirements for Central Office Coaxial Cable (1996);
• Telcordia GR-3028-CORE (2001), Thermal Management in Telecommunications Central Offices: Thermal GR-3028-CORE;
12- Telecommunication Industry Association (TIA)
• ANSI/TIA TSB-155-A, Guidelines for the Assessment and Mitigation of Installed Category 6 Cabling to Support 10GBASE-T (2010);
• ANSI/TIA-526-14-A OFSTP-14 Optical Power Loss Measurement of Installed Multimode Fiber Cable Plant (1998);
• TIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces (2004).
• ANSI/TIA/EIA-606-A, Administration Standard for Commercial Telecommunications Infrastructure (2002);
• ANSI-J-STD-607-A, Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (2002);
• ANSI/TIA-862, Building Automation Cabling Standard for Commercial Buildings (2002);
• ANSI/TIA-942, Telecommunications Infrastructure Standard for Data Centers (2005);
Underwriters Laboratories (UL)
• ANSI/UL 497-2001, Standard for Safety Protectors for Paired-Conductor Communications Circuits;
• UL 60950-1 2003, Information Technology Equipment - Safety - Part 1: General equirements;
13- Other Standards and Documents
• Americans with Disabilities Act (ADA) (1990);
• EU Code of Conduct on Data Centres Energy Efficiency, Version 1.0 (2008);
• EU Best practices for EU Code of Conduct on Data Centres, version 1.0 (2008);
• International Building Code (IBC), 2009;
• International Fuel Gas Code (IFGC), 2009;
• International Mechanical Code (IMC), 2009;
• International Plumbing Code (IPC), 2009;