

# هائبرد

دنیای تجارت بدون مرز  
**SHIBERD**  
 شرکت تجارت الکترونیک هائبرد  
 www.hiberd.com  
 ۸۸۹۳۶۹۵۸

طراحی وب سایت، فروشگاه اینترنتی، CMS

چگونه اطلاعات را در عصر فناوری اطلاعات محافظت کنیم؟!  
 نقش فرهنگ سازمانی در مدیریت امنیت اطلاعات  
 بررسی جنبه های مختلف اعتماد در تجارت الکترونیک  
 سیستم مدیریت امنیت اطلاعات ISMS  
 امنیت اطلاعات در ایران و جهان  
 و چندین مقاله دیگر

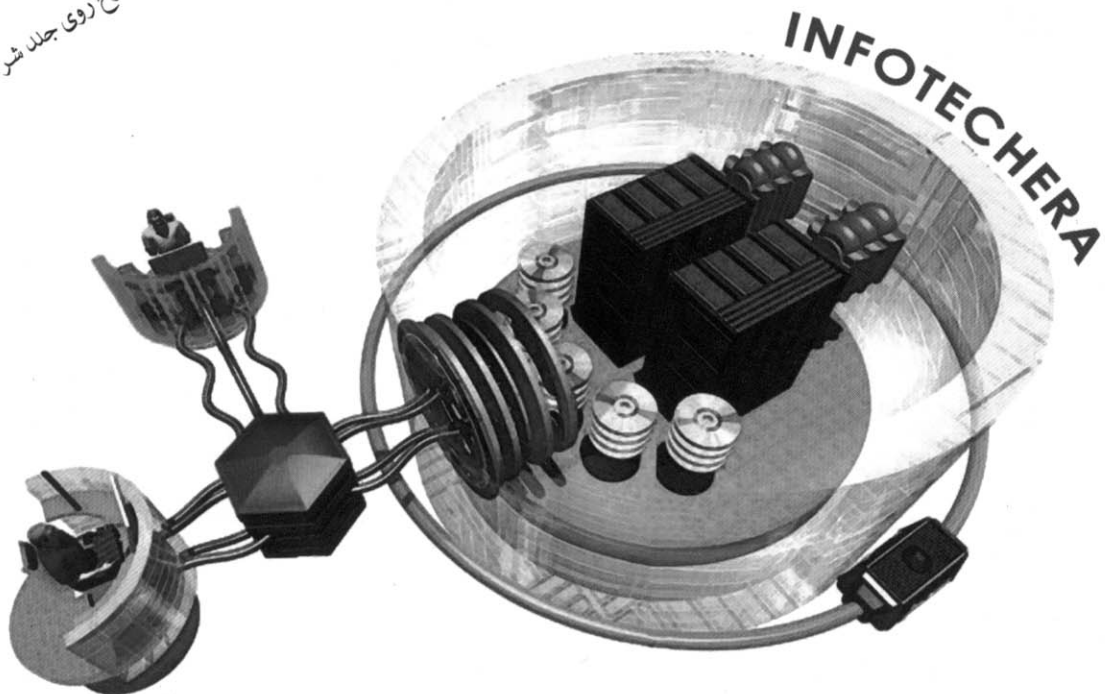
# فناوری اطلاعات

اولین ماهنامه تخصصی IT در ایران

سال چهارم، شماره ۳۶، مهر ماه ۱۳۸۷، ۱۰۰۰ تومان

ITE Magazine, Vol.4, No.36, October 2008  
 www.infotechera.com

در مسابقه تفسیر طرح روی جلد شرکت کنید



هشت ساعت دسترسی رایگان  
 به اینترنت برای مشترکین تهران

آواکستر  
 شبکه  
 www.azavastar.net

24x7

All Networking Accessories  
 That You Imagine

WARRANTY  
 1  
 YEAR

ALL N.W.P.® PRODUCTS ARE

**N.W.P.®**  
 HEADING FOR THE TOP 10!

# فناوری اطلاعات

خبری، تحلیلی، پژوهشی، آموزشی و اطلاع رسانی  
ماهنامه فنی مهندسی، سال چهارم، شماره ۳۶، مهرماه ۱۳۸۷، صفحه ۱۶۸۰

صاحب امتیاز و مدیر مسئول: مهندس احمد عدالت

جانشین مدیر مسئول: مهندس حسن اعتمادی

سردبیر: دکتر امیرحامد رضایی

مدیر هنری و اجرایی: پژمان جلالی

سازمان آگهی: هدیه کلبادی و مازیار اعتمادی  
تلفن: ۸۸۹۱۴۴۶۹

مدیر روابط عمومی و اشتراک: هدیه کلبادی  
مسئول تدارکات: علیرضا سرشار

## اعضای هیات علمی:

دکتر مسعود یقینی، دکتر محمد فتحیان، دکتر احمدعلی یزدان پناه  
دکتر مسعود حامدی، دکتر احمد ماکویی، دکتر کورش احراری، دکتر علی جهانگیری  
دکتر حجت احمدی، مهندس علیرضا عسگری، مهندس عشرت عدالت  
مهندس سامان نیکوکار، مهندس رضا زندیه، مهندس فرنود حسینی  
مهندس علی کسرای، مهندس علیرضا مقدسی

## اعضای هیات داوری:

دکتر مسعود یقینی: عضو هیات علمی دانشگاه علم و صنعت  
دکتر محمد فتحیان: عضو هیات علمی دانشگاه علم و صنعت و الزهرا  
دکتر احمدعلی یزدان پناه: عضو هیات علمی دانشگاه بهشتی  
دکتر کورش احراری: عضو هیات علمی و شورای مدیریت فرا منطقه ای WCIT سوییس  
دکتر احمد ماکویی: عضو هیات علمی دانشگاه علم و صنعت  
دکتر حجت احمدی: عضو هیات علمی دانشگاه تهران

## همکاران این شماره:

سید اصغر ابن الرسول، جواد دربان فولادی، مهدی ترابی، محمد امیر نیکجو  
لیلا اخوی زادگان، طیبه امیری، امیر مولا طلب، محمد علی اعلم  
مریم احمدی، معصومه آدینه، آذین بهزادیان، لیلا عظیمی  
محمد شهرتی فر، محمد رضا خانعلی پور  
قاسم سترک و همایون رحیمی

- ۳۶ سخن سردبیر
- ۳۷ دیدگاه
- ۳۹ خبر

## فاوا

- مدیریت فناوری اطلاعات
- ۵۰ سیستم های اطلاعات کسب و کار
- ۵۶ نقش فرهنگ سازمانی در مدیریت امنیت اطلاعات
- برنامه ریزی فناوری اطلاعات
- ۵۸ اجرای پروژه انتخاب ERP در وزارت بازرگانی
- تجارت الکترونیک
- ۶۴ بررسی جنبه های مختلف اعتماد در تجارت الکترونیکی
- اینترنت و شبکه
- ۷۹ چندین نکته برای افزایش تعداد بیننده های سایت...
- ۸۴ بررسی ساختار و عملکرد پروتکل مسیریابی...

لیتوگرافی: رحیمی ۷۷۵۳۲۵۰۵ چاپ: تحریر ۷۷۸۱۸۰۰۶ صحافی: یاران ۷۷۳۳۸۲۰۸  
نشانی چاپخانه: تهران - خیابان دماوند - روبروی ایستگاه قاسم آباد - خیابان کیایی  
کوچه فتحیان - شماره ۴ کد پستی چاپخانه: ۱۴۴۱۸۳۷۵۱۱

نشانی دفتر ماهنامه: تهران، خیابان سمیه، نرسیده به حافظ، بن بست درخشان، شماره ۲۷۸، طبقه اول، واحد ۱  
تلفن دفتر ماهنامه: ۷۰-۸۸۹۱۴۴۶۹ فاکس: ۸۸۹۱۴۴۷۰  
صندوق پستی ۱۴۱۵۵/۱۹۹۵

نشانی وب سایت: [www.InfoTechEra.com](http://www.InfoTechEra.com)  
پست الکترونیک: [Editor@InfoTechEra.com](mailto:Editor@InfoTechEra.com)  
اجرای وب سایت: نرم افزار برسیں شرکت ایمن کاوان کیهان

# Fava Nameh فاوانامه

## سیستم مدیریت امنیت اطلاعات ISMS به بهانه‌ی معرفی دیتاسنتر و بررسی مقوله استقرار ISMS در آن

مهندس علی کسرائی<sup>(۱)</sup>

واژه‌های کلیدی

ISMS، Data Center (مرکز داده)، چالش‌های استقرار ISMS در سازمان‌های کشور

چکیده:

شکی نیست که نگارنده‌ی این سطور، به جهت معرفی و تحلیل مقوله (ISMS)، بر مطالعه اسناد مبتنی بر استانداردهای (ISO 27001) و (ISO 27002) همت گمارده و به ترجمه‌ی قسمت‌های اساسی اسناد مذکور پرداخته است. اما از آن‌جا که ایشان را اعتقاد بر آن است تا از نتیجه‌ی پژوهش‌های دیگران نیز مطلع باشد، مطالعه‌ی ترجمه‌ها و نکته‌نظرات بسیاری از علمای فن را در دستور کار خود قرار داده است. پس ذکر این سطور بدان منظور است که ابتدا به ساکن مقاله‌ی حاضر را (تحقیق شخصی، گردآوری، همراه با ترجمه‌ی پاره‌ای از متون) بدانند و بدین سان، بر خود می‌دانند تا خالصانه، نکته‌ای را به خواننده‌ی گرامی یادآور شود: در خصوص ISMS، مقالات فارسی زبان و دارای ارزش علمی، به ندرت یافت می‌شود. با این وجود به پژوهش‌هایی دست یافتیم که به حق جان کلام را بیان کرده و در ترجمه‌ی قسمت‌هایی از استانداردها و مقالات زبان اصلی، به تکامل، اهتمام ورزیده بودند. با توجه به این که در متون ترجمه‌شده همه چیز را یافتیم و ضمن تطابق علمی آنان به جد، ذهنیاتی را رصد کردیم که حاصل نبوغ مترجمان و نویسندگان بود، صلاح خود بر آن دیدیم که ضمن اشاره به این مطلب، با ذکر نام این عزیزان در بخش منابع، به نوعی قدردانی ویژه خود را نشان‌دهنده‌ی نابشان سازیم. همچنین اعلام می‌دارد که در شمارگان آینده‌ی این ماهنامه سلسله مقالاتی در خصوص امنیت اطلاعات و مبانی شناخت امنیت ارایه می‌شود که همگام با آموزش مباحث امنیتی، خواننده‌ی گرامی را بر این مقوله، به وقوف کامل رهنمون می‌سازد.

گر خطا گفتیم اصلاحش تو کن مصلحی تو ای تو سلطان سخن

## مقدمه: (با هدف ایجاد ذهنیت اولیه از استانداردهای امنیتی)

(مدیریت امنیت اطلاعات)، برای اشخاصی دانسته است که در حوزه‌های طراحی، پیاده‌سازی و پشتیبانی موارد امنیتی دارای مسئولیتی هستند. از بررسی این سند، نتیجه این‌گونه حاصل شد که این استاندارد، شامل ۳۵ هدف امنیتی و ۱۲۷ اقدام بازدارنده برای تأمین امنیت می‌باشد که به هیچ عنوان به جزئیات خاصی اشاره ندارد، بلکه کلیات موضوع را بیان می‌کند. چراکه طراحان این استاندارد، معتقدند که ممکن است بسیاری از راهکارهای ارائه شده در این اسناد، برای همه سازمان‌ها، قابل استفاده نباشد و یا نیاز به گونه‌ای خاص از کنترل‌ها باشد. در سال (۲۰۰۰)، بخش اول استاندارد (2-BS7799) توسط موسسه بین‌المللی استاندارد به عنوان استاندارد (17799 ISO/IEC) انتشار یافت که شامل فصول ۱۰ گانه زیر می‌باشد:

- (۱) تدوین سیاست‌های امنیتی اطلاعات سازمان‌ها
- (۲) امنیت سازمانی
- (۳) طبقه‌بندی سرمایه‌ها و ارایه‌ی کنترل‌های لازم
- (۴) امنیت پرسنل
- (۵) امنیت فیزیکی و محیطی
- (۶) مدیریت ارتباطات و عملیات
- (۷) کنترل دسترسی
- (۸) امنیت سیستم‌های اطلاعاتی (سیستم‌های پشتیبان و ارتقای آن‌ها)
- (۹) مدیریت تداوم فعالیت‌های سازمان
- (۱۰) سازگاری با موارد قانونی

در نهایت، این استاندارد، مجدداً در سال (۲۰۰۲) میلادی بازنویسی شد و در سال (۲۰۰۵) با دو نام (BS ISO/IEC 17799:2005) و (17799-1:2005) اقدام (BS) در یک سند، منتشر شد، که شامل ۳۹ هدف امنیتی و ۱۳۴ اقدام بازدارنده می‌باشد. نتیجه آن که سازمان‌هایی که پس از مشاوره با متخصصان امر، موفق به ارائه برنامه‌ریزی مدون، مبتنی بر ایجاد فضای امن در تبادل اطلاعات سازمانی خود شده‌اند، پس از ممیزی بازرسان ویژه، موفق به اخذ گواهی نامه‌ای خواهند شد که نشان از وجود این استاندارد در آن حوزه دارد. بد نیست بدانید که تا تاریخ (May 2006) تعداد سازمان‌هایی که موفق به اخذ گواهی نامه‌ی مذکور شده‌اند، (۲۵۴۶) عدد می‌باشند که به علت اهمیت مباحث امنیت سازمان در جهان، روز به روز در حال افزایش است. در این وادی این سوال مطرح است که چرا نام کشور ایران، در میان فهرست ارائه شده، وجود ندارد؟ بر طبق آمارها، کشور ژاپن، بیشترین آمار اخذ گواهی نامه‌ی استاندارد امنیت را در سطوح سازمانی به خود اختصاص داده است و سپس انگلستان. حتی در این فهرست کشورهای چون قطر، مصر، عربستان و... نیز دیده می‌شوند. ریشه‌ی این چالش کجا است، الله اعلم...؟؟!! البته جدیدترین آمار ثبت کشورهای جهان در خصوص اخذ گواهی نامه ISMS2008 در خاتمه‌ی مقاله جهت هر گونه استفاده‌ی علمی ارائه خواهد شد.

## اشارتی گذرا بر راهنمای فنی (ISO/IEC TR13335)

## موسسه بین‌المللی استاندارد

این گزارش فنی در قالب ۵ فصل مجزا، در فواصل سال‌های ۱۹۹۶ تا ۲۰۰۱ توسط موسسه بین‌المللی استاندارد منتشر شد. شایان ذکر است که این گزارش، هیچ‌گاه به عنوان استاندارد ISO منتشر نشده و عنوان (Report Technical) بدان اطلاق شده است؛ اما تنها سند فنی معتبری است که

شکی نیست که شما نیز معتقدید که حفظ حیات سازمان‌ها، و همچنین وجهه‌ی آنان از دید ارباب رجوع، کارمندان، مدیران و... و در این وادی امنیت آن‌ها، تنها با دسته‌بندی بی‌اساس اسناد، جدا سازی اتاق‌ها، ایجاد محدودیت‌های عبور و مرور در برخی امکانه‌ها و داشتن کلمه عبور برای دسترسی به رایانه‌ها، به دست نمی‌آید. به منظور استقرار امنیت در سازمان‌ها و حفاظت از سرمایه‌های مختلفه آنان، باید فعالیت‌هایی را توأم با برنامه ریزی مدون، در دستور کار داشت که در ابتدایی‌ترین حالت، عبارتند از:

- (۱) آموزش و ارایه‌ی آگاهی‌های لازم به کلیه پرسنل در تمامی سطوح
- (۲) پیاده‌سازی کنترل‌های مورد نیاز برای حفظ سرمایه‌ها
- (۳) ایجاد پست‌ها و مسئولیت‌هایی در ارتباط با پیاده‌سازی ایمنی
- (۴) بازبینی و بهینه‌سازی دوره‌ای تمامی کنش‌ها
- (۵) بررسی شرایط پی‌گیری مستمر سازمان‌ها در اجرای برنامه‌های ارایه شده

بنابراین در صورت وجود چنین عملکردی می‌توان گفت که این سازمان، دارای برنامه‌ریزی، برای حفظ منابع خود می‌باشد. همچنین شکی نیست که به دلیل توسعه روز افزون دو فناوری (ارتباطات) و (اطلاعات) و ظهور اینترنت به عنوان نقطه عطف آن‌ها، شاهد آن هستیم که عصر حاضر، به عصر اطلاعات بدل شده است و هر آن‌گاه که خاطره‌ی به اشتراک گذاشتن داده‌ها به ذهن متبادر می‌شود، خواه ناخواه، ذهن پویا به دنبال راهکارهای ایجاد امنیت در فضای تبادل داده‌ها خواهد شد، و این فضای امن، به عوامل بسیاری وابسته است که اقدامات در سطح ملی را می‌طلبد. با ذکر این نکته که هر روز، شاهد گزارش‌هایی از حملات هکرها و خرابکاران رایانه‌ای در جهان هستیم، باید به ایجاد زیر ساخت‌های امنیتی در سطح ملی مانند:

- (۱) سیستم تأیید هویت الکترونیکی
  - (۲) سیستم‌های تشخیص نفوذ و راه‌های مقابله با تهدیدات
  - (۳) ایجاد دیتاسترها و استفاده از مزایای ناب آن‌ها و...
- اهتمام واجب ورزید. پس این جا است که سخن از نیاز به تدوین یک سیستم ویژه به عنوان استاندارد جهانی در تبادل امن داده‌ها رخ می‌نماید.

## استاندارد مدیریت امنیت اطلاعات چیست؟

ISO (International Organization for Standardization) و IEC (International Electro technical Commission) همان سیستم‌های ویژه به عنوان استانداردهای جهانی می‌باشند. در زمینه امنیت اطلاعات، ISO و IEC، یک کمیته‌ی مشترک به نام (ISO/IEC JTC1) تشکیل داده‌اند که پس از بررسی نظرات سازمان‌های ملی عضو، به تأیید استاندارد بین‌المللی (ISO/IEC 17799) که توسط انیستیتی استاندارد انگلیس، تحت عنوان (BS7799) ارائه شده بود، نایل شدند.

## استاندارد (BS7799) و تاریخچه آن:

موسسه استاندارد انگلیس، نسخه‌ی اول این استاندارد (BS7799 - 1) را در سال (۱۹۹۵) که شامل یک بخش تحت عنوان: (management information security Code of practice) بود، منتشر ساخت. دیری نپایید که نسخه دوم آن (BS7799 - 2) در سال (۱۹۹۹) ارائه شد که علاوه بر تصحیح مواردی از بخش اول مذکور، دارای ۲ بخش مجزا بود. در این نسخه، هدف از انتشار این استاندارد را ارایه‌ی راهکارهایی در زمینه



۴- امنیت پرسنلی: در این قسمت، ضمن اشاره به ضرورت رعایت ملاحظات امنیتی در به کارگیری پرسنل، ضرورت آموزش پرسنل در زمینه امنیت اطلاعات و ارتباطات، مطرح شده و لیستی از مسوولیت های پرسنل در پروسه تامین امنیت اطلاعات و ارتباطات سازمان، ارائه شده است.

۵- امنیت فیزیکی و پیرامونی: در این قسمت، اهمیت و ابعاد امنیت فیزیکی، جزئیات محافظت از تجهیزات و کنترل های مورد نیاز برای این منظور، ارائه شده است.

۶- مدیریت ارتباطات: در این قسمت، ضرورت و جزئیات روال های اجرایی مورد نیاز، به منظور تعیین مسوولیت هر یک از پرسنل، روال های مربوط به سفارش، خرید، تست و آموزش سیستم ها، محافظت در مقابل نرم افزارهای مخرب، اقدامات مورد نیاز در خصوص ثبت وقایع و پشتیبان گیری از اطلاعات، مدیریت شبکه، محافظت از رسانه ها و روال ها و مسوولیت های مربوط به درخواست، تحویل، تست و سایر موارد تغییر نرم افزارها ارائه شده است.

۷- کنترل دسترسی: در این قسمت، نیازمندی های کنترل دسترسی، نحوه مدیریت دسترسی پرسنل، مسوولیت های کاربران، ابزارها و مکانیزم های کنترل دسترسی در شبکه، کنترل دسترسی در سیستم عامل ها و نرم افزارهای کاربردی، استفاده از سیستم های ماینتورینگ و کنترل دسترسی در ارتباط از راه دور به شبکه ارائه شده است.

۸- نگهداری و توسعه سیستم ها: در این قسمت، ضرورت تعیین نیازمندی های امنیتی سیستم ها، امنیت در سیستم های کاربردی، کنترل های رمزنگاری، محافظت از فایل های سیستم و ملاحظات امنیتی مورد نیاز در توسعه و پشتیبانی سیستم ها، ارائه شده است.

۹- مدیریت تداوم فعالیت سازمان: در این قسمت، رویه های مدیریت تداوم فعالیت، نقش تحلیل ضربه در تداوم فعالیت، طراحی و تدوین طرح های تداوم فعالیت، قالب پیشنهادی برای طرح تداوم فعالیت سازمان و طرح های تست، پشتیبانی و ارزیابی مجدد تداوم فعالیت سازمان، ارائه شده است.

۱۰- پاسخ گویی به نیازهای امنیتی: در این قسمت، مقررات مورد نیاز در خصوص پاسخ گویی به نیازهای امنیتی، سیاست های امنیتی مورد نیاز و ابزارها و مکانیزم های بازرسی امنیتی سیستم ها، ارائه شده است.

#### بخش دوم

در این بخش از استاندارد برای تامین امنیت اطلاعات و ارتباطات سازمان، مطابق شکل (۱) یک چرخه ایمن سازی شامل ۴ مرحله طراحی، پیاده سازی، تست و اصلاح ارائه شده و جزئیات هر یک از مراحل به همراه لیست و محتوای مستندات مورد نیاز جهت ایجاد سیستم مدیریت امنیت اطلاعات سازمان، ارائه شده است.

استاندارد ISO/IEC 17799 موسسه بین المللی استاندارد: در سال 2000، بخش اول استاندارد BS7799:2 بدون هیچ گونه تغییری توسط موسسه بین المللی استاندارد به عنوان استاندارد ISO/IEC 17799 منتشر شد.

جزئیات و تکنیک های مورد نیاز در مراحل استقرار امنیت در حوزه ی اطلاعات و ارتباطات در آن درج شده است. پس می توان نتیجه گرفت که به نوعی، مکمل استانداردهای مدیریتی (BS7799) و (ISO/IEC 17799) می باشد.

#### مشروح ارکان پیشنهادی مندرج در گزارش فنی (TR 13335)

ذهنیت به خصوصی در آرایه ی این بخش لحاظ است و آن چیزی نیست جز بخشنامه ی شماره (۱۳۷۱۱-۸۶ / م / ۳۸۵۰۵) مورخ (۱۳۸۶/۸/۱۰) معاون اول محترم رییس جمهور، که در آن، به صراحت، سازمان ها، بر تهیه طرح مدیریت امنیت اطلاعات، تا پایان سال ۱۳۸۶، مکلف شده اند. با ذکر این مطلب که این خبر توسط جناب مهندس حیدرعلی کورنگی در سمینار (ISMS) شبکه علمی کشور به اطلاع شرکت کنندگان رسید؛ نگارنده را بر آن داشت، شرح خلاصه شده ی به نسبت کاملی را جهت آگاهی خوانندگان و مدیران، ارائه کند. البته لازم به ذکر است که این سطور به عینه در گزارشی تحت عنوان ( راهنمای پیاده سازی سیستم مدیریت امنیت اطلاعات)، توسط دبیرخانه ی شورای عالی امنیت فضای تبادل اطلاعات کشور، ارائه شده است که فرازهایی از آن را می خوانید: استانداردهای مدیریتی ارائه شده در خصوص امنیت اطلاعات و ارتباطات سازمان ها، عبارتند از: استانداردهای مدیریتی BS7799 موسسه استاندارد انگلیس - استاندارد مدیریتی 17799 ISO/IEC موسسه بین المللی استاندارد - گزارش فنی TR 13335 ISO/IEC موسسه بین المللی استاندارد

#### استاندارد BS7799 موسسه استاندارد انگلیس

استاندارد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که نسخه اول آن (BS7799:1) در سال 1995 منتشر شد. نسخه دوم این استاندارد (BS7799:2) که در سال 1999 ارائه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش ارائه شد. آخرین نسخه این استاندارد، (BS7799:2002) نیز از سال 2002 تا 2005 در دو بخش منتشر شد.

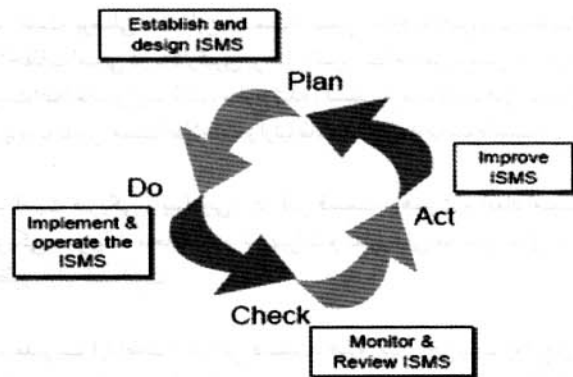
#### بخش اول

در این بخش از استاندارد، مجموعه کنترل های امنیتی مورد نیاز سیستم های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته بندی کلی شامل موارد زیر، ارائه شده است:

۱- تدوین سیاست امنیتی سازمان: در این قسمت، به ضرورت تدوین و انتشار سیاست های امنیتی اطلاعات و ارتباطات سازمان، به نحوی که کلیه مخاطبین سیاست ها در جریان جزئیات آن قرار گیرند، تاکید شده است. همچنین جزئیات و نحوه نگارش سیاست های امنیتی اطلاعات و ارتباطات سازمان، ارائه شده است.

۲- ایجاد تشکیلات تامین امنیت سازمان: در این قسمت، ضمن تشریح ضرورت ایجاد تشکیلات امنیت اطلاعات و ارتباطات سازمان، جزئیات این تشکیلات در سطوح سیاست گذاری، اجرایی و فنی به همراه مسوولیت های هر یک از سطوح، ارائه شده است.

۳- دسته بندی سرمایه ها و تعیین کنترل های لازم: در این قسمت، ضمن تشریح ضرورت دسته بندی اطلاعات سازمان، به جزئیات تدوین راهنمای دسته بندی اطلاعات سازمان پرداخته و محورهای دسته بندی اطلاعات را ارائه کرده است.



شکل (۱): مراحل ایمن سازی بر اساس استاندارد BS7799:2002

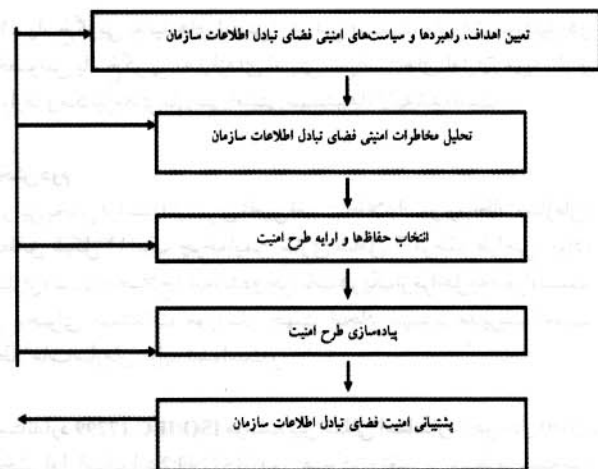
راهنمای فنی ISO/IEC TR13335 موسسه بین‌المللی استاندارد: این گزارش فنی در قالب ۵ بخش مستقل در فواصل سال‌های ۱۹۹۶ تا ۲۰۰۱ توسط موسسه بین‌المللی استاندارد منتشر شده است. اگر چه این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان Technical Report بر آن نهاده شد، اما تنها مستندات فنی معتبری است که جزئیات و تکنیک‌های مورد نیاز مراحل ایمن سازی اطلاعات و ارتباطات را تشریح کرده و در واقع مکمل استانداردهای مدیریتی BS7799 و ISO/IEC 17799 می‌باشد.

#### بخش اول

در این بخش که در سال ۱۹۹۶ منتشر شد، مفاهیم کلی امنیت اطلاعات از قبیل سرمایه، تهدید، آسیب پذیری، ریسک، ضربه و ...، روابط بین این مفاهیم و مدل مدیریت مخاطرات امنیتی، ارائه شده است.

#### بخش دوم

این بخش که در سال ۱۹۹۷ منتشر شد، مراحل ایمن سازی و ساختار تشکیلات تامین امنیت اطلاعات سازمان ارائه شده است. بر اساس این گزارش فنی، چرخه ایمن سازی مطابق شکل (۲) به ۵ مرحله شامل تدوین سیاست امنیتی سازمان، تحلیل مخاطرات امنیتی، تعیین حفاظها و ارائه طرح امنیت، پیاده سازی طرح امنیت و پشتیبانی امنیت اطلاعات، تفکیک شده است.



شکل (۲): مراحل ایمن سازی بر اساس گزارش فنی ISO/IEC 13335

#### بخش سوم

در این بخش که در سال ۱۹۹۸ منتشر شد، تکنیک‌های طراحی، پیاده سازی و پشتیبانی امنیت اطلاعات از جمله محورها و جزئیات سیاست‌های امنیتی سازمان، تکنیک‌های تحلیل مخاطرات امنیتی، محتوای طرح امنیتی، جزئیات پیاده سازی طرح امنیتی و پشتیبانی امنیت اطلاعات، ارائه شده است.

#### بخش چهارم

در این بخش که در سال ۲۰۰۰ منتشر شد، ضمن تشریح حفاظ‌های فیزیکی، سازمانی و حفاظ‌های خاص سیستم‌های اطلاعاتی، نحوه انتخاب حفاظ‌های مورد نیاز برای تامین هریک از مولفه‌های امنیت اطلاعات، ارائه شده است.

#### بخش پنجم

در این بخش که در سال ۲۰۰۱ منتشر شد، ضمن افزودن مقوله ارتباطات و مروری بر بخش‌های دوم تا چهارم این گزارش فنی، تکنیک‌های تامین امنیت ارتباطات از قبیل شبکه‌های خصوصی مجازی، امنیت در گذرگاه‌ها، تشخیص تهاجم و کدهای مخرب، ارائه شده است.

#### مستندات ISMS دستگاه

بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر دستگاه (سازمان) باید مجموعه مستندات مدیریت امنیت اطلاعات و ارتباطات را به شرح زیر، برای خود تدوین کند:

- اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه
- طرح تحلیل مخاطرات امنیتی فضای تبادل اطلاعات دستگاه
- طرح امنیت فضای تبادل اطلاعات دستگاه
- طرح مقابله با حوادث امنیتی و ترمیم خرابی‌های فضای تبادل اطلاعات دستگاه

- برنامه آگاهی رسانی امنیتی به پرسنل دستگاه
- برنامه آموزش امنیتی پرسنل تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه

**اهداف، راهبردها و سیاست‌های امنیتی:** اولین بخش از مستندات ISMS دستگاه، شامل اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه می‌باشد. در این مستندات، لازم است موارد زیر، گنجانیده شوند:

**اهداف امنیت فضای تبادل اطلاعات دستگاه:** در این بخش از مستندات، ابتدا، سرمایه‌های فضای تبادل اطلاعات دستگاه، در قالب سخت‌افزارها، نرم‌افزارها، اطلاعات، ارتباطات، سرویس‌ها و کاربران، تفکیک و دسته‌بندی شده و سپس اهداف کوتاه مدت و میان مدت تامین امنیت هریک از سرمایه‌ها، تعیین خواهد شد. نمونه‌ای از این اهداف، عبارتند از:

نمونه‌هایی از اهداف کوتاه مدت امنیت:

- جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه سرمایه‌های فضای تبادل اطلاعات دستگاه
- مهار خسارت‌های ناشی از ناامنی موجود در فضای تبادل اطلاعات دستگاه

آورد. در این مرحله، ضمن کسب شناخت نسبت به اطلاعات، ارتباطات، تجهیزات، سرویس ها و ساختار شبکه ارتباطی دستگاه، ضعف های امنیتی موجود در بخش های مختلف، شناسایی خواهند شد تا در مراحل بعدی، راه کارهای لازم به منظور رفع این ضعف ها و مقابله با تهدیدها، ارایه شوند. روش تحلیل مخاطرات امنیتی، باید در مجموعه راهبردهای امنیتی فضای تبادل اطلاعات دستگاه، مشخص شده باشد. در تحلیل مخاطرات امنیتی، به مواردی پرداخته می شود که به صورت به قوه، امکان دسترسی غیر مجاز، نفوذ و حمله کاربران مجاز یا غیر مجاز فضای تبادل اطلاعات دستگاه، به منابع (سرمایه های) فضای تبادل اطلاعات دستگاه و منابع کاربران این فضا را فراهم می کنند. در این مستند، لازم است مخاطرات امنیتی فضای تبادل اطلاعات، حداقل در محورهای "معماری شبکه"، "تجهیزات شبکه"، "سرویس دهنده های شبکه"، "مدیریت و نگهداری شبکه" و "تشکیلات و روش های مدیریت امنیت شبکه"، بررسی شوند.

**معماری شبکه ارتباطی:** در این بخش، لازم است معماری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- ساختار شبکه ارتباطی
- ساختار آدرس دهی و مسیریابی
- ساختار دسترسی به شبکه ارتباطی

**تجهیزات شبکه ارتباطی:** در این بخش، لازم است تجهیزات شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- محافظت فیزیکی
- نسخه و آسیب پذیری های نرم افزار
- مدیریت محلی و از راه دور
- تصدیق هویت، تعیین اختیارات و ثبت عملکرد سیستم، بویژه در دسترسی های مدیریتی
- ثبت وقایع
- نگهداری و به روز کردن پیکربندی
- مقابله با حملات علیه خود سیستم، بویژه حملات ممانعت از سرویس

**مدیریت و نگهداری شبکه ارتباطی:** در این بخش، لازم است مدیریت و نگهداری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- تشکیلات و روش های مدیریت و نگهداری شبکه ارتباطی
- ابزارها و مکانیزم های مدیریت و نگهداری شبکه ارتباطی

**سرویس های شبکه ارتباطی:** در این بخش، لازم است سرویس های شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- سیستم عامل سرویس دهنده
- سخت افزار سرویس دهنده، به ویژه رعایت افزونگی در سطح ماحول و سیستم
- نرم افزار سرویس
- استفاده از ابزارها و مکانیزم های امنیتی روی سرویس دهنده ها

**تشکیلات و روش های تامین امنیت شبکه ارتباطی:** در این بخش، لازم است تشکیلات و روش های امنیت شبکه ارتباطی دستگاه، حداقل در محورهای

• کاهش رخنه پذیری های سرمایه های فضای تبادل اطلاعات دستگاه

**نمونه هایی از اهداف میان مدت امنیت:**

- تامین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت افزارها، متناسب با حساسیت آن ها.
- تامین صحت عملکرد و قابلیت دسترسی برای نرم افزارها، متناسب با حساسیت آن ها.
- تامین محرمانگی، صحت و قابلیت دسترسی برای اطلاعات، متناسب با طبقه بندی اطلاعات از حیث محرمانگی.
- تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، متناسب با طبقه بندی اطلاعات از حیث محرمانگی و حساسیت ارتباطات.
- تامین قابلیت تشخیص هویت، حدود اختیارات و پاسخ گویی، حریم خصوصی و آگاهی رسانی امنیتی برای کاربران شبکه، متناسب با طبقه بندی اطلاعات قابل دسترس و نوع کاربران.

**راهبردهای امنیت فضای تبادل اطلاعات دستگاه:** راهبردهای امنیت فضای تبادل اطلاعات دستگاه، بیانگر اقداماتی است که به منظور تامین اهداف امنیت دستگاه، باید انجام گیرد. نمونه ای از راهبردهای کوتاه مدت و میان مدت امنیت فضای تبادل اطلاعات دستگاه، عبارتند از:

**نمونه هایی از راهبردهای کوتاه مدت امنیت:**

- شناسایی و رفع ضعف های امنیتی فضای تبادل اطلاعات دستگاه
- آگاهی رسانی به کاربران فضای تبادل اطلاعات دستگاه
- کنترل و اعمال محدودیت در ارتباطات شبکه داخلی دستگاه

**نمونه هایی از راهبردهای میان مدت امنیت:**

- رعایت استانداردهای مدیریت امنیت اطلاعات
- تهیه طرح ها و برنامه های امنیتی فضای تبادل اطلاعات دستگاه، بر اساس استانداردهای فوق
- ایجاد و آماده سازی تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه
- اجرای طرح ها و برنامه های امنیتی فضای تبادل اطلاعات دستگاه

**سیاست های امنیتی فضای تبادل اطلاعات دستگاه:** سیاست های امنیتی فضای تبادل اطلاعات دستگاه، متناسب با دسته بندی انجام شده روی سرمایه های فضای تبادل اطلاعات دستگاه، عبارتند از:

- سیاست های امنیتی سرویس های فضای تبادل اطلاعات دستگاه
- سیاست های امنیتی سخت افزارهای فضای تبادل اطلاعات دستگاه
- سیاست های امنیتی نرم افزارهای فضای تبادل اطلاعات دستگاه
- سیاست های امنیتی اطلاعات فضای تبادل اطلاعات دستگاه
- سیاست های امنیتی ارتباطات فضای تبادل اطلاعات دستگاه
- سیاست های امنیتی کاربران فضای تبادل اطلاعات دستگاه

**طرح تحلیل مخاطرات امنیتی:**

پس از تدوین اهداف، راهبردها و سیاست های امنیتی فضای تبادل اطلاعات دستگاه و قبل از طراحی امنیت فضای تبادل اطلاعات، لازم است شناخت دقیقی از مجموعه فضای تبادل اطلاعات موجود دستگاه به دست

زیر مورد تجزیه و تحلیل قرار گیرد:

- طرح‌ها، برنامه‌ها و سایر مستندات امنیتی
- تشکیلات امنیت، روال‌های اجرایی و شرح وظایف پرسنل امنیت

**طرح امنیت:** پس از تحلیل مخاطرات امنیتی شبکه ارتباطی دستگاه و دسته‌بندی مخاطرات امنیتی این شبکه، در طرح امنیت، ابزارها و مکانیزم‌های موردنیاز به منظور رفع این ضعف‌ها و مقابله با تهدیدها، ارایه می‌شوند. در طرح امنیت، لازم است کلیه ابزارها و مکانیزم‌های امنیتی موجود، به کار گرفته شوند. نمونه‌ای از این ابزارها عبارتند از:

#### ۱- سیستم‌های کنترل جریان اطلاعات و تشکیل نواحی امنیتی

- فایروال‌ها
- سایر سیستم‌های تامین امنیت گذرگاه‌ها

#### ۲- سیستم‌های تشخیص و مقابله یا تشخیص و پیش‌گیری از حملات، شامل:

- سیستم‌های مبتنی بر ایستگاه
  - سیستم‌های مبتنی بر شبکه
  - ۳- سیستم فیلترینگ محتوا (به ویژه برای سرویس E-Mail)
  - ۴- نرم افزارهای تشخیص و مقابله با ویروس
  - ۵- سیستم‌های تشخیص هویت، تعیین حدود اختیارات و ثبت عملکرد کاربران
  - ۶- سیستم‌های ثبت و تحلیل رویدادنامه‌ها
  - ۷- سیستم‌های رمزنگاری اطلاعات
  - ۸- نرم افزارهای نظارت بر ترافیک شبکه
  - ۹- نرم افزارهای پوششگر امنیتی
  - ۱۰- نرم افزارهای مدیریت امنیت شبکه
- ویژگی‌های اصلی سیستم امنیتی شبکه ارتباطی دستگاه، عبارتند از:

- چندلایه بودن سیستم امنیتی
- توزیع شده بودن سیستم امنیتی
- تشکیل نواحی امنیتی جهت کنترل دقیق دسترسی به سرویس‌های شبکه
- یکپارچگی مکانیزم‌های امنیتی، به ویژه در گذرگاه‌های ارتباطی شبکه
- تفکیک زیرساختار مدیریت امنیت شبکه (حداقل بخش اصلی سیستم امنیتی شبکه)

• انتخاب اجزای سیستم امنیتی شبکه، از Brandهای مختلف، به نحوی که ضعف‌های امنیتی یکدیگر را پوشش داده و مخاطره باقی مانده را کاهش دهند

- انتخاب محصولات که دارای تاییدیه‌های معتبر، از موسسات ارزیابی بین‌المللی می‌باشند

**طرح مقابله با حوادث امنیتی و ترمیم خرابی‌ها:** طرح مقابله با حوادث امنیتی، با هدف پیش‌گیری، تشخیص و مقابله با حوادث امنیتی فضای تبادل اطلاعات، ارایه می‌شود. محتوای این طرح، حداقل شامل موارد زیر می‌باشد:

- ۱- دسته‌بندی حوادث
- ۲- سیاست‌های مربوط به هر یک از سرویس‌های مقابله با حوادث امنیتی
- ۳- ساختار و شرح وظایف مربوط به تیم مقابله با حوادث امنیتی دستگاه
- ۴- سرویس‌های پیش‌گیری و مقابله با حوادث که توسط تیم مقابله با

حوادث امنیتی دستگاه ارایه می‌شود

- ۵- روال‌های اجرایی مربوط به هر یک از سرویس‌ها
- ۶- متدولوژی مقابله با حوادث امنیتی
- آماده‌سازی تیم
- تشخیص و تحلیل حوادث
- محدودسازی، ترمیم و ریشه‌کنی حوادث
- فعالیت‌های بعد از حوادث
- چک لیست مقابله با حوادث
- ۷- الگوی مقابله با حوادث امنیتی

**برنامه آگاهی‌رسانی امنیتی:** برنامه آگاهی‌رسانی امنیتی، با هدف برنامه‌ریزی نحوه آگاهی‌رسانی به کاربران شبکه دستگاه ارایه می‌شود و باید حاوی موارد زیر باشد:

- ۱- اهداف آگاهی‌رسانی
- ۲- راهبردها
- ۳- برنامه اجرایی آگاهی‌رسانی
- ۴- مفاد دوره‌های آگاهی‌رسانی از قبیل:
- اعلام حیطه حریم خصوصی کاربران
- اعلام وظایف، مسئولیت‌ها و مواردی که کاربران باید پاسخ‌گو باشند
- اعلام مواردی که کاربران باید نسبت به آن حساسیت داشته باشند (از قبیل اعلام حوادث به تیم مقابله با حوادث)
- ارایه اطلاعات در زمینه آسیب‌پذیری سیستم‌ها و مواردی که کاربران باید دقت بیشتری لحاظ کنند

**برنامه آموزش پرسنل تشکیلات امنیت:** برنامه آموزش امنیتی، با هدف توانمندسازی پرسنل تشکیلات امنیت دستگاه ارایه می‌شود و باید حاوی موارد زیر باشد:

- ۱- اهداف آموزش
- ۲- راهبردها
- ۳- برنامه اجرایی آموزش
- ۴- مفاد دوره‌های آموزشی

#### تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه

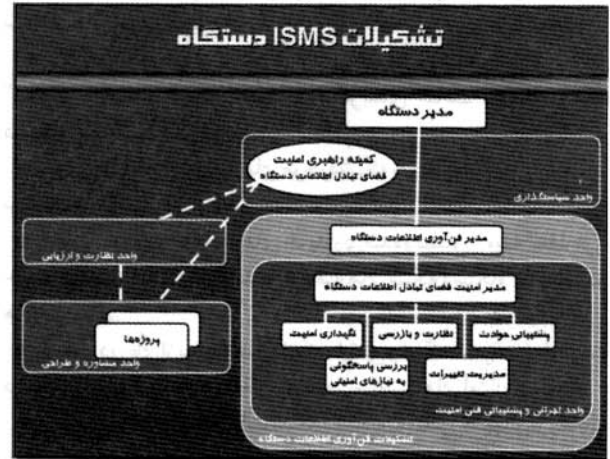
اجزا و ساختار تشکیلات امنیت: بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر دستگاه به منظور تامین امنیت اطلاعات و ارتباطات خود، لازم است تشکیلات تامین امنیت به شرح زیر، ایجاد کند.

**اجزای تشکیلات امنیت:** تشکیلات امنیت شبکه، متشکل از سه جز اصلی به شرح زیر می‌باشد:

- در سطح سیاست‌گذاری: کمیته راهبری امنیت فضای تبادل اطلاعات دستگاه
- در سطح مدیریت اجرایی: مدیر امنیت فضای تبادل اطلاعات دستگاه
- در سطح فنی: واحد پشتیبانی امنیت فضای تبادل اطلاعات دستگاه

علاوه بر موارد فوق، واحدهای "مشاوره و طراحی" و "نظارت و بازرسی" نیز لازم است. اما این واحدها به‌الزام در داخل دستگاه و چارت سازمانی، تشکیل نخواهند شد.





### ۱- اعضای کمیته راهبردی امنیت:

- مدیر دستگاه (رییس کمیته)
- نماینده ویژه مدیر دستگاه
- مدیر حراست دستگاه
- مدیر فناوری اطلاعات دستگاه
- مدیر امنیت شبکه دستگاه (دبیر کمیته)

### ۲- مدیر امنیت:

مدیریت واحد پشتیبانی امنیت شبکه را به عهده دارد و توسط مدیر فناوری اطلاعات دستگاه تعیین می شود.

### ۳- تیم های پشتیبانی امنیت:

شامل تیم های زیر بوده و اعضای آن مستقیم توسط مدیر امنیت شبکه دستگاه تعیین می شوند:

- تیم پشتیبانی حوادث
- تیم نظارت و بازرسی
- تیم نگهداری امنیت
- تیم مدیریت تغییرات
- تیم بررسی پاسخ گویی به نیازهای امنیتی

### شرح وظایف تشکیلات امنیت

#### شرح وظایف کمیته راهبردی امنیت:

- بررسی، تغییر و تصویب سیاست های امنیتی شبکه
- پی گیری اجرای سیاست های امنیتی از مدیر امنیت شبکه
- تایید طرح های و برنامه های امنیت شبکه دستگاه شامل:

- طرح تحلیل مخاطرات امنیتی
- طرح امنیت شبکه

- طرح مقابله با حوادث و ترمیم خرابی ها
- برنامه آگاهی رسانی امنیتی کاربران

- برنامه آموزش واحد پشتیبانی امنیت شبکه

- بررسی ضرورت تغییر سیاست های امنیتی شبکه

- بررسی، تغییر و تصویب تغییرات سیاست های امنیتی شبکه

#### شرح وظایف مدیر امنیت:

- تهیه پیش نویس سیاست های امنیتی شبکه و ارایه به کمیته راهبردی امنیت شبکه

- نظارت بر اجرای کامل سیاست های امنیتی شبکه توسط واحد پشتیبانی امنیت شبکه، کاربران شبکه، مدیران و کارشناسان ادارات و طراحان امنیت شبکه دستگاه

- تهیه طرح ها و برنامه های امنیت شبکه دستگاه با کمک واحد مشاوره و طراحی و ارایه آن ها به کمیته راهبردی

- مدیریت واحد پشتیبانی امنیت شبکه دستگاه و نظارت بر عملکرد اجزای این واحد

- تشخیص ضرورت و پیشنهاد بازنگری و اصلاح سیاست های امنیتی شبکه

- تهیه پیش نویس تغییرات سیاست های امنیتی شبکه

#### شرح وظایف واحد پشتیبانی امنیت

##### شرح وظایف پشتیبانی حوادث امنیتی شبکه:

- تشخیص و مقابله با تهاجم

- مرور روزانه Log فایروال ها، مسیریاب ها، تجهیزات گذرگاه های ارتباط با سایر شبکه ها و سرویس دهنده های شبکه داخلی و اینترنت دستگاه، به منظور تشخیص اقدامات خرابکارانه و تهاجم.

- مرور تردهای انجام شده به سایت و Data Center و گزارش اقدامات انجام شده توسط کارشناسان و مدیران سرویس ها.

- مرور روزانه گزارش سیستم تشخیص تهاجم به منظور تشخیص تهاجم های احتمالی.

- انجام اقدامات لازم به منظور کنترل دامنه تهاجم جدید.

- ترمیم خرابی های ناشی از تهاجم جدید.

- مستندسازی و ارایه گزارش تهاجم تشخیص داده شده به تیم هماهنگی و آگاهی رسانی امنیتی.

- اعمال تغییرات لازم در سیستم امنیت شبکه، به منظور مقابله با تهاجم جدید.

- مطالعه و بررسی تهاجم های جدید و اعمال تنظیمات لازم در سیستم تشخیص تهاجم و سایر بخش های سیستم امنیت شبکه.

- ارایه پیشنهاد در خصوص تغییرات لازم در سیستم امنیتی شبکه به منظور مقابله با تهدیدهای جدید، به مدیر امنیت شبکه.

- آگاهی رسانی به کاربران شبکه در خصوص روش های جدید نفوذ به سیستم ها و روش های مقابله با آن، آسیب پذیری های جدید ارایه شده برای سیستم های مختلف و روش های برطرف کردن آن ها.

- تشخیص و مقابله با ویروس

- بررسی و در صورت نیاز، انتخاب، خرید و تست نرم افزار ضد ویروس مناسب برای ایستگاه های کاری و سرویس دهنده های شبکه دستگاه به-

صورت دوره‌ای (هر سال یکبار)

- نصب نرم‌افزار ضد ویروس روی ایستگاه‌های کاری مدیران و ارایه اطلاعات لازم به سایر کاربران، جهت نصب نرم‌افزار.
- نصب نرم‌افزار ضد ویروس روی کلیه سرویس دهنده‌های شبکه دستگاه.
- تهیه راهنمای نصب و Update کردن نرم‌افزار ضد ویروس ایستگاه‌های کاری و سرویس دهنده‌ها و ارایه آن به کاربران شبکه از طریق واحد هماهنگی و آگاهی‌رسانی امنیتی.
- مرور روزانه Log و گزارشات نرم‌افزارهای ضد ویروس.
- مطالعه و بررسی ویروس‌های جدید و روش‌های مقابله با آن.
- ارایه روش‌های مقابله با ویروس‌ها به تیم هماهنگی و آگاهی‌رسانی امنیتی، جهت اعلام به کاربران و انجام اقدامات لازم.
- انجام اقدامات پیش‌گیرانه لازم به منظور کنترل دامنه تاثیر ویروس‌های جدید.
- ترمیم خرابی‌های ناشی از ویروس‌های جدید.
- مستندسازی و ارایه گزارش‌های آماری از ویروس‌ها، مقابله با آن‌ها و خرابی‌های ناشی از ویروس‌ها در شبکه دستگاه، به تیم هماهنگی و آگاهی‌رسانی امنیتی.
- فراهم کردن امکان Update نرم‌افزار ضد ویروس، به صورت روزانه (به جز نرم‌افزار ضد ویروس کاربران شبکه که باید توسط خود کاربران Update شود).
- ارائه اطلاعات لازم جهت آگاهی‌رسانی به کاربران در خصوص ویروس‌های جدید، توسط تیم هماهنگی و آگاهی‌رسانی امنیتی.
- ارایه پیشنهاد در خصوص تغییرات لازم در نرم‌افزارهای ضد ویروس و سیستم امنیتی شبکه به منظور مقابله با ویروس‌های جدید، به مدیر امنیت شبکه.
- آگاهی‌رسانی به کاربران شبکه در خصوص ویروس‌های جدید و روش‌های مقابله با آن‌ها.
- تشخیص و مقابله با حوادث فیزیکی
- انتخاب ابزارهای مناسب جهت محافظت فیزیکی از تجهیزات و سرمایه‌های شبکه در مقابل حوادث فیزیکی و دسترسی‌های غیرمجاز.
- مرور روزانه رویدادنامه‌های دسترسی فیزیکی به سرمایه‌های شبکه، به ویژه در سایت.
- سرکشی دوره‌ای به سایت، تجهیزات مستقر در طبقات ساختمانها و مسیر عبور کابل‌ها به منظور اطمینان از تامین امنیت فیزیکی آن‌ها.
- مطالعه و بررسی حوادث فیزیکی جدید و روش‌های مقابله با آن.
- ارایه روش‌ها به تیم هماهنگی و آگاهی‌رسانی امنیت جهت اعلام به کاربران و انجام اقدامات لازم.
- انجام اقدامات لازم به منظور کنترل دامنه حوادث فیزیکی.
- ترمیم خرابی‌های ناشی از حوادث فیزیکی.
- مستندسازی و ارایه گزارش‌های آماری از حوادث فیزیکی، مقابله با این حوادث و خرابی‌های ناشی از آن‌ها به تیم هماهنگی و آگاهی‌رسانی امنیتی.
- ارایه پیشنهاد در خصوص Update تجهیزات و روشهای تامین امنیت فیزیکی به مدیر امنیت شبکه.
- ارایه اطلاعات لازم جهت آگاهی‌رسانی به کاربران در خصوص حوادث فیزیکی، توسط تیم هماهنگی و آگاهی‌رسانی امنیتی.

## • شرح وظایف نظارت و بازرسی امنیتی

- مانیتورینگ ترافیک شبکه (در حیطه مانیتورینگ مجاز)
- بازرسی دوره‌ای از ایستگاه‌های کاری، سرویس دهنده‌ها، تجهیزات شبکه و سایر سخت‌افزارهای موجود شبکه، به منظور اطمینان از رعایت سیاست‌های امنیتی مربوطه.
- بازرسی دوره‌ای از سخت‌افزارهای خریداری شده و تطبیق پروسه "سفارش، خرید، تست، نصب و پیکربندی سخت‌افزارهای شبکه دستگاه" با سیاست‌های مربوطه.
- بازرسی دوره‌ای از نرم‌افزارهای موجود شبکه به منظور اطمینان از رعایت سیاست‌های امنیتی مربوطه.
- بازرسی دوره‌ای از نرم‌افزارهای خریداری شده و تطبیق پروسه "سفارش، خرید، تست، نصب و پیکربندی نرم‌افزارهای شبکه دستگاه" با سیاست‌های مربوطه.
- بازرسی دوره‌ای از نحوه اتصال شبکه داخلی و شبکه دسترسی به اینترنت دستگاه، با سایر شبکه‌های مجاز، بر اساس سیاست‌های امنیتی مربوطه.
- بازرسی دوره‌ای از اطلاعات شبکه دستگاه به منظور اطمینان از رعایت سیاست‌های امنیتی مربوطه.
- بازرسی دوره‌ای از کاربران شبکه دستگاه به منظور اطمینان از آگاهی کاربران از حقوق و مسوولیت‌های خود و رعایت سیاست‌های امنیتی مرتبط با خود.
- بازرسی دوره‌ای از روند تهیه اطلاعات پشتیبان.
- بازرسی دوره‌ای از روند تشخیص و مقابله با حوادث امنیتی در شبکه دستگاه.
- بازرسی دوره‌ای از روند تشخیص و مقابله با ویروس در شبکه دستگاه.
- بازرسی دوره‌ای از روند تشخیص و مقابله با حوادث فیزیکی در شبکه دستگاه.
- بازرسی دوره‌ای از روند نگهداری سیستم امنیتی شبکه در شبکه دستگاه.
- بازرسی دوره‌ای از روند مدیریت تغییرات در شبکه دستگاه.
- بازرسی دوره‌ای از روند آگاهی‌رسانی امنیتی به کاربران شبکه دستگاه.
- بازرسی دوره‌ای از روند آموزش پرسنل واحد پشتیبانی امنیت شبکه دستگاه.
- بازرسی دوره‌ای از روند واگذاری فعالیت‌ها به پیمان‌کاران خارج از دستگاه.
- شرح وظایف مدیریت تغییرات
- بررسی درخواست خرید، ایجاد یا تغییر سخت‌افزارها، نرم‌افزارها، لینک‌های ارتباطی، سیستم عامل‌ها و سرویس‌های شبکه از دیدگاه امنیت شبکه، آسیب‌پذیری‌های سیستم یا سرویس مورد نظر، مشکلات امنیتی ناشی از به کارگیری آن بر سایر بخش‌های شبکه و در نهایت تصمیم‌گیری در خصوص تایید یا رد درخواست.
- بررسی آسیب‌پذیری‌های سخت‌افزارها، نرم‌افزارهای کاربردی، سیستم عامل‌ها، خطوط ارتباطی و سرویس‌های مرسوم شبکه و امنیت شبکه.
- آگاهی‌رسانی به طراحان شبکه و امنیت شبکه در خصوص آسیب‌پذیری فوق، به منظور لحاظ کردن در طراحی.
- ارایه گزارش بررسی‌ها به تیم هماهنگی و آگاهی‌رسانی امنیت شبکه.

- کلیه ی تجهیزات امنیتی مانند، IDS ها، IPS ها، فایروال ها، آنتی ویروس ها و ترمینال های امنیتی
- سیستم های کشف شنود شبکه ای
- سرورها
- تجهیزات غیرفعال در شبکه

#### ۳) ساختار برنامه های کاربردی:

- سیستم های مدیریت بانک های اطلاعاتی
- سیستم های امنیت اطلاعات
- سیستم های حفظ امنیت نرم افزار
- سیستم های بهینه سازی اطلاعات
- فایل سرورها، پایگاه های داده
- مکانیزم ذخیره و بازیابی اطلاعات

#### عوامل موثر در طراحی بهینه ی یک مرکز داده:

- ۱) سادگی (Simplicity)
- ۲) مقیاس پذیری (Scalability)
- ۳) ماژولار بودن (Modularity)
- ۴) منطقی بودن (Sanity)
- ۵) قابلیت انعطاف (Flexibility)

#### توضیحات ای پیرامون (Data center):

پُر واضح است که تا قبل از دهه (۱۹۹۰)، استفاده از اینترنت برای مردم عادی به آسانی امکان پذیر نبود، چرا که با توجه به خط فرمانی بودن محیط نرم افزارهای مربوطه، استفاده از اینترنت، نیاز به دانش خاصی داشت و اما از اوایل دهه (۱۹۹۰)، بعد از تولد مفهوم وب در اینترنت (۱۹۹۳) و اختراع و تکمیل پروتکل (HTTP)، استعمال اینترنت همه گیر شده و توانمندی در به اشتراک گذاشتن داده ها، به تعداد کاربران افزوده و حجم بالای ترافیک در سایت ها را موجب شد و سابورت این حجم ترافیک، به سرورهای قدرتمند همراه با اتصال های پرسرعت نیاز داشت، که هم هزینه ی بالایی را در بر داشته و به نوعی هم عملی نبود. در این وادی ناگهان تنها راه حلی که برای رفع این معضل به ذهن متخصصان رسید، ایجاد مراکز خاصی تحت عنوان (Data center) بود که با در اختیار داشتن اتصالات پرسرعت اینترنت و سرورهای قوی، امکان ارایه و راه اندازی سرورهای وب را برای استفاده عموم، هموار می ساخت. بدین معنی که مردم و شرکت های تجاری کوچک می توانستند با پرداخت اجاره بهای اندک، سایت های وب خود را عرضه کنند و شرکت های بزرگ نیز با در اختیار گرفتن یکی از سرورهای این مرکز داده، به استفاده از آن در سطوح مختلفی کاری خود بپردازند. بزرگترین دست آورد این فناوری کاربردی، در ابتدای امر، دسترسی به داده ها در سرعت های بالا با نرخ ارزان اتصال می باشد. به طوری که بعضی از مراکز داده، از طریق خطوط فیبرنوری، پهنای باندی بیش از (4 Gbps) را در اختیار دارند و تعداد سرورهای این مراکز، گاه تا بیش از (۱۰۰۰) سرور، گزارش شده است. نگارنده انتظار دارد تا خواننده گرامی تا این جا با مفهوم مراکز داده و اهمیت آن، آشنایی لازم را پیدا کرده باشد. در این خصوص اعتقاد داریم که در این سطور، به اشارتی عمومی، پیرامون (Data center) پرداختیم و لازم است تا برای اخذ اطلاعات بیشتر به منابع تخصصی رجوع شود. در ادامه ضمن بررسی مزایای راه اندازی مرکز داده در ایران و نگاهی گذرا به همین موضوع از زاویه ی آینده نگری، به ارایه ی بخشی پیرامون تعمیم (ISMS) در یک

- بررسی موارد مربوط به جابه جایی کاربران شبکه و پرسنل تشکیلات امنیت شبکه به منظور تغییر در دسترسی و حدود اختیارات آن ها در دسترسی به سرمایه های شبکه.
- بررسی نیازمندی های امنیتی و روش های ایمن سازی سیستم عامل ها، سرویس دهنده های شبکه، خطوط ارتباطی، نرم افزارها، تجهیزات شبکه و امنیت شبکه جدید که به کارگیری آن ها در شبکه، مورد تایید قرار گرفته است.
- ارایه دستور عمل های ایمن سازی و پیکربندی امن برای هر یک از موارد فوق.

#### • شرح وظایف نگه داری امنیت شبکه

- بررسی وضعیت عملکرد سیستم امنیتی شبکه، شامل:
- عملکرد صحیح فایروال ها.
- عملکرد صحیح سیستم تشخیص تهاجم.
- عملکرد صحیح سیستم ثبت وقایع.
- عملکرد صحیح سیستم تهیه نسخه پشتیبان.
- ارایه گزارشات روزانه در خصوص عملکرد سیستم امنیتی شبکه.
- ارایه گزارشات آماری از وضعیت سیستم امنیتی شبکه.
- رفع اشکالات تشخیص داده شده در عملکرد سیستم امنیتی شبکه.

#### مرکز داده (Data Center)

مرکز داده، در واقع مکانی است که سیستم های رایانه ای و کلیه ی تجهیزات جانبی مربوط به آن ها، مانند سیستم های ذخیره سازی و ارتباطی، در آن قرار گرفته است که البته بر اساس خاص بودنش، معماری ساختمانی خاص خود را خواهان است. یک دیتاستر به طور معمول شامل قسمت های زیر است:

- ۱) سیستم های UPS
- ۲) سیستم های پشتیبان
- ۳) کنترلرهای محیطی
- ۴) دستگاه های تهویه هوا
- ۵) سیستم های کنترل حریق
- ۶) ابزارهای کنترل دسترسی افراد

بررسی ساختار مراکز داده: مراکز داده را به لحاظ ساختار می توان به قسمت های زیر تقسیم بندی کرد که البته این تقسیمات به نوع مرکز داده نیز می تواند دست خوش تغییر شود:

#### ۱) ساختار فیزیکی:

- سیستم های کنترل حریق
- سیستم های تهویه هوا و ارزیابی رطوبت محیط
- سیستم های UPS و کنترل برق
- سیستم های کنترل دسترسی
- سیستم های پشتیبان

#### ۲) ساختار شبکه ای:

- کلیه ی تجهیزات شبکه مانند، روترها و سویچ ها و ...

دیتا سنتر از لحاظ فیزیکی (می پردازیم، تا درک، مفاهیم عمومی (ISMS) را برای خواننده کم اطلاع، هموارتر سازد.

### مزایای راه اندازی (Data center) در ایران

از مهم ترین مزیت های این پدیده، می توان به پایین آمدن ترافیک (Gateway) های شرکت مخابرات ایران، اشاره کرد. بر طبق آمار، در حال حاضر، بیش از (۳۰) سرور در کشورهای غربی (کانادا، آمریکا، انگلیس) در اجاره شرکت های ایرانی قرار دارد. ترافیک ماهانه هر سرور به طور متوسط (400 GB) می باشد که در مجموع، بیش از (12000 GB)، ترافیک به (Gateway) های شبکه می داده های ایران وارد می کند که خود باعث بالا رفتن ترافیک (Gateway) های شرکت مخابرات شده و هم زمان دسترسی را برای کاربران، بیشتر می کند.

نتیجه آن که با ایجاد مرکز داده در کشور، علاوه بر آن که در عمل، هیچ گونه مشکل ترافیکی وجود نخواهد داشت، به هنگام بروز مشکلاتی در (Gateway) های اصلی مخابرات (مانند قطع شدن لینک Flag در خرداد ماه سال جاری)، حداقل، امکان مشاهده سایت های فارسی و ایرانی، برای کاربران، فراهم خواهد بود. با عنایت به این که شرکت مخابرات ایران، سرمایه گذاری بهینه ای در بخش دیتا و اینترنت، انجام داده است که با توجه به مسیر خطوط فیبر نوری که در سراسر تهران و ایران، نصب شده است، پهنای باند بی نظیر، حاصل این حرکت ملی است. همچنین بر اساس آمار منتشره، در تهران یک حلقه، با پهنای باند بیش از (622 Mb) بین (8) مرکز اصلی مخابرات، وجود دارد که در عمل با این پهنای باند، می توان، یک مرکز داده با استانداردهای جهانی، راه اندازی کرد.

### مزایای (Data center) ها در آینده ایران

بر اساس آمار موثق، پس از اجرای کامل پروژه ی (Flag)، ایران از طریق (Bone Back) های پر قدرت، به پهنای باند (10 Gbps) متصل خواهد شد و این پهنای باند، معادل پهنای باندی است که در اختیار کشورهای پیشرفته ی اروپا و آمریکایی قرار دارد و با توجه به اینکه کشورهای منطقه، نیاز به ارتباط با کشورمان دارند، در عمل ایران، در آینده، به چهار راه ارتباطی خاورمیانه بدل خواهد شد. در صورت اجرای موفق این پروژه، کشور ایران، اولین کشوری است که در خاورمیانه، دارای مرکز داده خواهد بود. در این وادی، ضمن نیاز کشورهای عربی در خصوص بازار رو به رشد استفاده از اینترنت، در کشورشان، ایران می تواند با هزینه های متعادل اقدام به ورود (ارز) به مملکت کند و همچنین این مورد باعث ارتقای دانش فنی و عملی ایران در زمینه ی وب سرورها می شود.

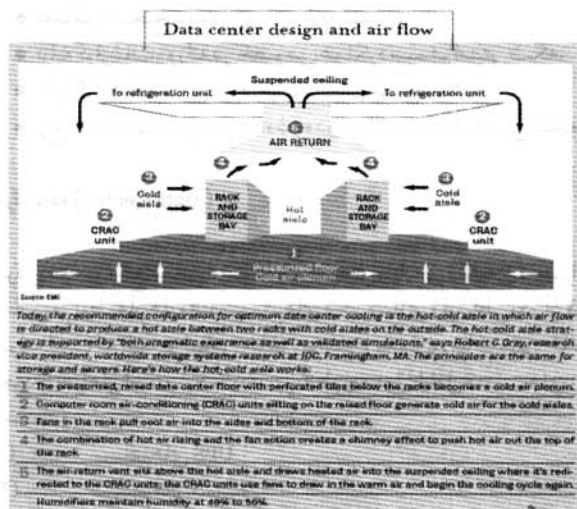
### روش های پیاده سازی امنیت فیزیکی مرکز داده

(تعمیم عمومی و گذرای ISMS بر بخش فیزیکی مراکز داده): مراکز داده ها باید در مقابل حوادث طبیعی، جرایم و ... امن شوند. پس به ذکر گذرای عناوین موارد مذکور به منظور آشنایی مقدماتی خوانندگان بسنده می شود.

- (۱) مکان ساختمان مراکز داده:

  - مرکز داده باید در مکانی باشد که ریسک ناشی از حوادث طبیعی دارای آمار قابل قبولی باشد.
  - از ساخت مراکز داده در مراکز شهرها، جلوگیری می شود.
  - دوری مکان مرکز داده از مراکز حادثه زای ساخت دست بشر مثل، مجاورت فرودگاه، راه آهن، زندان، پالایشگاه و ...

- به کارگیری الگوریتمی با برنامه ریزی علمی در ساخت ساختمان مرکز داده، تا در آینده، نیاز به اصلاح نداشته باشد.
- ایجاد فاصله ی ساختمان مرکز داده ی پشتیبان از مرکز داده ی اصلی حداقل حدود (۳۰) تا (۵۰) مایل.
- (۲) تسهیلات پشتیبان
- منابع تسهیلاتی آب و برق، براساس استانداردهای موجود، باید از دو منبع مجزا تامین شوند.
- (۳) تهیه منابع تغذیه برق و الکتریسیته مورد استفاده مراکز داده.
- (۴) جنس دیوارها و بررسی ضخامت آن ها:
- استفاده از بتن به ضخامت یک فوت توصیه شده است
- (۵) در مراکز داده، استفاده از پنجره ممنوع شده و یا باید آن را به حداقل رساند و باید تمهیدات امنیتی مخصوص را اعمال کرد.
- (۶) از نصب و اطلاع رسانی محل مراکز داده پرهیز می شود. چراکه هر رهگذری نباید به سادگی از محل آن مطلع شود.
- (۷) بحث خنک سازی و تهویه هوا و کنترل رطوبت نیز از مهم ترین



### ارکان حفاظتی به شمار می آید.

- (۸) کنترل و پیش گیری از نشت آب در ساختمان مرکز داده.
- (۹) تشخیص و پیش گیری از حریق.
- (۱۰) استفاده از درختان، تخته سنگ ها و گیاهان، جهت مخفی سازی ساختمان مرکز داده ها از دید اشخاص متفرقه.
- (۱۱) به حداقل رساندن راه های ورودی به ساختمان مرکز داده.
- (۱۲) پرهیز از قرار دادن مراکز داده در مجاورت پارکینگ ها.
- (۱۳) تعبیه ی درب های خروج اضطراری به هنگام آتش سوزی.
- (۱۴) استفاده از سیستم حفاظتی مانند دوربین های مدار بسته و ...
- (۱۵) استفاده از قاب کف کاذب به منظور سهولت در امر کابل کشی و هدایت کانال های تهویه ی هوا.
- (۱۶) حفاظت از ماشین آلات بیرونی مراکز داده از خطر دزدی.
- (۱۷) استفاده از امنیت فیزیکی لایه ای، بدین مفهوم که برای مثال جهت ورود به ساختمان مراکز داده، تمهیدات امنیتی ایجاد شود تا برای گذر از دیگر مکان های درونی سازمان، احتیاج به تایید و تصدیق هویت از مکان های حفاظتی قبلی باشد.



سخن آخر (نتیجه گیری به بهانه‌ی آرایه سال ۲۰۰۸):

در آخرین آمار آرایه شده از سوی موسسه بین المللی ثبت سازمانهای موفق به اخذ گواهینامه ها، شرکت فناوری اطلاعات سهلان ( فاس ) موفق به دریافت گواهی نامه پیاده سازی ISMS از موسسه ISACA با همکاری شرکت 7Secure شده است. ضمن تبریک به تیم کاری آن موسسه، تقاضا دارد، به آمار سازمانی کشورهای ژاپن، هند و انگلیس توجه کنید. البته آمار کشور مالزی هم خالی از تعمق نیست.

و نگارنده، معتقد است که نتیجه گیری را که پر واضح است، به عهده ی خواننده و نهاده و فقط متذکر شود که باید فعالیت های مدیریتی و اطلاعاتی به نحوی همگرا شوند که خدایی ناکرده مصداق شعر زیر واقع نشویم که فرمود:

بدون هدف در هیچستانی سرگردانیم که هیچ

نمی خواهیم، هیچ نمی فهمیم و هیچ نمی یابیم

و همواره برنامه ریزی را قبل از پیاده سازی مرام طی طریقت آبادانی مملکت مان قرار دهیم.

مراجع:

- 1) Vistorm, D. 2000 Companies aim to build security awareness computer world.
- 2) Mason, P. 2000 Info security is an issue for all. Computer weekly
- 3) Von Solms, R. 1997. Driving safely on the information superhighway
- 4) Andrew T. Robinson, A process for measuring Information Security Risk, December 2001
- 5) Elizabeth B. Lennon, The metrics Development Process, Information Technology Library
- 6) Martins, JHP Eloff, Measuring Information Security, Department of computer science, Rand Afrikaans University
- 7) Avinash Kadam, Implementation Methodology for Information Security System to comply with BS7799 Requirements, August 2002

و تشکر ویژه از پژوهش گران و موسساتی که نظرات شان روشن بخش راهمان شد:

- موسسه بین المللی ثبت گواهی نامه های ISMS
- موسسه توسعه و تبادل دانش فناوری اطلاعات - فرنود حسنی
- خبرگزاری مهر
- ماهنامه تحلیل گران عصر اطلاعات - هدی رضایی
- وزارت نیرو - منوچهر بسحاق
- شرکت پیشتاز پردازش پارس
- مهدی جعفری نژاد
- محمود عبادی
- افسانه کربلایی
- محسن میرزایی و محمد علی گورکانی
- شورای پژوهش های علمی کشور
- کیانوش مرادیان
- شبکه علمی غرب آسیا - سمینارهای ISMS
- یادداشت های مهندس حیدر علی کورنگی

۱۸) تعیین خط مشی امنیت فیزیکی که ریشه در همان برنامه ریزی دارد، در ابتدای مقاله، شرح آن گذشت.

۱۹) آگاه سازی پرسنل از برنامه های امنیتی فیزیکی مرکز داده.

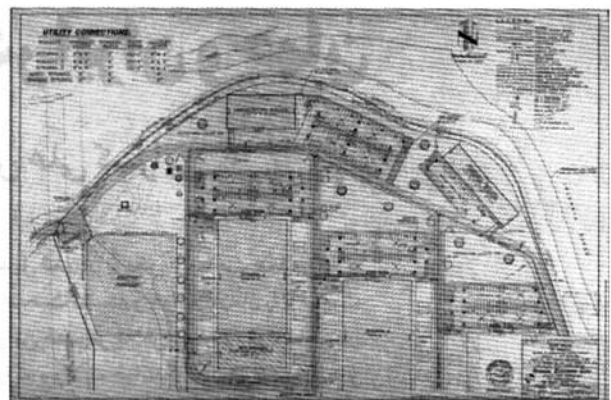
۲۰) از ورود مواد غذایی به مراکز داده جلوگیری به عمل آید.

۲۱) عملیات تمیز سازی محیط سایت باید مرتب انجام شده چرا که گرد و غبار به عملکرد سیستم ها صدمه می زند.

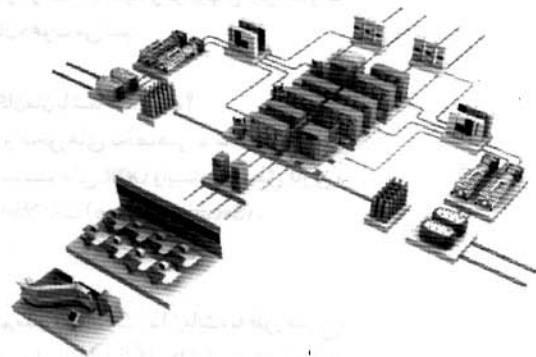
۲۲) پاک سازی رسانه ها و اسناد مکتوب مربوط به مراکز داده باید قبل از انهدام آن ها صورت گیرد. چرا که برای مثال هنگام حذف یک داده از روی هارد دیسک، به وسیله ی نرم افزارهای مخصوص، دوباره می توان آن را باز یابی کرد و بدان دسترسی داشت. در این خصوص اطلاع یافتیم که دکتر (Gutmann Peter)، استاد دانشگاه (اوکلند) موفق به پیشنهاد الگوهایی شده است که عملیات باز نویسی داده ها را تا ۳۵ مرتبه انجام می دهد. لازم به ذکر است که بر این اساس، نرم افزارهایی آرایه شده است که نسخه ی ویندوز آن (Sweep Pro-M) و نسخه ی لینوکس آن (Secure Hard disk Eraser) نام دارد.

۲۳) نگهداری از نسخه های پشتیبان در مکان های امن.

۲۴) کنترل دسترسی فیزیکی و استفاده از سیستم های حفاظتی پیشرفته مانند: اثر انگشت، عنبیه چشم، صدا، چهره و DNA و ... اشاره تصویری ۱) پلان جدیدترین دیتا سنتر گوگل (فقط جهت مطالعه، بدون شرح):



اشاره تصویری ۲) تصویری کامل از دیتا سنتری با اشل انترپرایز:



نکته) شکی نیست که ایجاد امنیت در محیط مراکز داده ها به همین مختصر اکتفا نمی کند. این سطور، با ذهنیت قوانین مندرج در گزارش فنی (TR 1335) به منظور آشنایی مقدماتی خوانندگان کم اطلاع در زمینه پیاده سازی (ISMS) در محیط فیزیکی مراکز داده، آرایه شده است. باشد تا مقبول افتد.