پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات

راهنمای کامل اخذ گواهینامه ISO 27000

مرجعی برای دروس مدیریت امنیت اطلاعات، معماری امنیت اطلاعات
مدل‌ها و استانداردهای امنیت اطلاعات

مؤلف:

دکتر محمدعلی ترکمانی

سرشناسه	:	ترکمانی، محمدعلی، ۱۳۵۴-
عنوان و نام پدیدآور	:	پیاده‌سازی سیستم های مدیریت امنیت اطلاعات : راهنمای کامل اخذ گواهینامه ISO 27000
مشخصات نشر	:	مشهد: ارسطو، ۱۳۹۴ .
مشخصات ظاهری	:	۲۷۲ص.: مصور، جدول، نمودار .؛ ۱۷×۲۴س‌م.
شابک	:	978-600-7558-50-8
وضعیت فهرست نویسی	:	فیپای مختصر
یادداشت	:	این مدرک در آدرس http://opac.nlai.ir قابل دسترسی است.
شماره کتابشناسی ملی	:	۳۷۶۶۴۴۰

نام کتاب : پیاده‌سازی سیستم‌های مدیریت امنیت اطلاعات

مؤلف : دکتر محمدعلی ترکمانی

ناشر : ارسطو (با همکاری سامانه اطلاع‌رسانی چاپ و نشر ایران)

صفحه‌آرایی ، تنظیم و طرح جلد : محمدعلی ترکمانی و علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : ششم – ۱۳۹۸

تعداد صفحات: ۲۶۱ صفحه

چاپ : مدیران

قیمت : ۵۳۰۰۰ تومان

شابک : ۸ – ۵۰– ۷۵۵۸ –۶۰۰ – ۹۷۸

تلفن‌های مرکز پخش : ۰۹۱۷۷۱۶۴۹۴۰ – ۵۰۹۶۱۴۶ – ۰۵۱۱

فهرست مطالب

مقدمه:

علیرغم پیشرفت تکنیک‌ها و مکانیزم‌های امنیتی، بازهم شاهد انتشار اخبار نفوذ مهاجمین به شبکه‌های رایانه‌ای سازمان‌ها هستیم. ظاهراً هم‌زمان با پیشرفت‌های امنیت شبکه مهاجمین نیز از تکنیک‌های جدیدی برای حمله سیستم‌های رایانه‌ای استفاده می‌کنند. این موضوع باعث شده است که حفظ محرمانگی، صحت اطلاعات حیاتی سازمان‌ها و جلوگیری از قطع سرویس‌های ارائه‌شده توسط سازمان‌ها به یک چالش اساسی برای مدیران تبدیل شود. برای مقابله با این چالش سازمان‌ها باید به‌صورت نظام‌مند و سیستماتیک با مسئله امنیت اطلاعات برخورد کنند. راه‌حلی که برای این مسئله ارائه‌شده است، استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان و دریافت گواهینامه مربوط به آن است. در حال حاضر محبوب‌ترین استاندارد در حوزه امنیت اطلاعات، استانداردهای خانواده ISO 27000 است که در کشور ما نیز به‌شدت در حال گسترش است. در این کتاب مجموعه استانداردهای امنیتی ISO 27000 موردبررسی قرار می‌گیرد. در کنار این استاندارد می‌توان استانداردهای دیگری را نیز به کاربرد که متخصصین به این کار اجرای موازی استانداردها در سازمان می‌گویند. لذا در این کتاب برخی از استانداردهای دیگر نظیر استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد ISO/IEC 17799، گزارش فنی ISO/IEC TR 13335، استاندارد BS25999 منتشرشده توسط موسسه استاندارد انگلستان (BSI) و همچنین برخی از مستندات مهم در حوزه امنیت اطلاعات نظیر مستندات NIST SP 800-30، NIST SP800-61 و NIST SP800- 50 بررسی‌شده است. این کتاب راهنمای مناسبی برای اخذ گواهینامه ISO 27000 بوده و مرجعی برای متقاضیان شرکت در آزمون‌های مرتبط خواهد بود.

ساختار این کتاب به شرح ذیل است:

فصل اول کتاب اصول و مفاهیم پایه موردنیاز را بررسی می‌کند. در پایان این فصل حوزه‌های کنترلی ISO27001:2013 معرفی می‌گردد.

فصل‌های دوم تا شانزدهم کتاب به بررسی ۱۴ حوزه کنترلی استاندارد ISO27001:2013 اختصاص دارد.

ازآنجاکه مدیریت ریسک‌های امنیت اطلاعات اهمیت زیادی در تأمین امنیت اطلاعات سازمان و اخذ گواهی‌نامه دارد، فصل هفدهم کتاب نیز به مدیریت ریسک اختصاص داده‌شده است.

در فصل هجدهم کتاب نمونه سیاست‌های امنیتی ارائه گردیده است. شکل و محتوای سیاست امنیتی ممکن است از سازمانی به سازمان دیگر متفاوت باشد و به فاکتورهای زیادی از قبیل اندازه سازمان، اهداف سازمان، میزان حساسیت اطلاعات سازمان، تعداد و انواع سیستم‌های محاسباتی و اطلاعاتی که مورداستفاده قرار می‌گیرند، بستگی دارد. بررسی در نمونه سیاست‌های امنیتی از پیش آماده و تهیه‌شده توسط سایر مراکز موفق، در ایجاد دید کلی از سیاست‌های امنیتی و موارد مربوط به آن‌ها کمک زیادی خواهد کرد. در نوشتن یک سیاست امنیتی می‌توان از نمونه سیاست‌های موجود استفاده کرد ولی باید همواره توجه کرد که عوامل تأثیرگذار و مرتبط سازمان باسیاست امنیتی را هم مدنظر قرار دهیم.

در فصل نوزدهم کتاب متن کامل استاندارد ISO27001:2013 ارائه گردید است.

همچنین در پیوست ۱، چک‌لیست کاربردی ممیزی بر اساس الزامات و اهداف کنترلی استاندارد ISO27001 آورده شده است.

از این کتاب می‌توان به‌عنوان مرجع دروس معماری امنیت اطلاعات و مدیریت امنیت اطلاعات در رشته‌های فناوری اطلاعات و کامپیوتر استفاده نمود. در پایان هر فصل تعدادی سؤال تشریحی و چهارگزینه‌ای آورده شده است تا خوانندگان بهتر بتوانند خود را برای آزمون‌هایی که در پیش رودارند آماده نمایند. امید است این اثر موردتوجه اساتید، دانشجویان، سازمان‌های متقاضی دریافت استاندارد و همچنین ممیزین ISO 27000 قرار گیرد. از خوانندگان عزیز تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشالله در ویرایش‌های بعدی اشکالات یا کاستی‌های احتمالی کتاب مورد تجدیدنظر قرار گیرد. در پایان از زحمات آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین از مدیریت انتشارت ارسطو جناب آقای حسین قنبری تشکر و قدردانی نماییم.

محمدعلی ترکمانی

تابستان ۱۳۹۵

فصل اول

تعاریف و اصول پایه

۱-۱- تعریف امنیت اطلاعات و سیستم امن

امنیت اطلاعات عبارت است از حفاظت اطلاعات و به حداقل رساندن دسترسی غیرمجاز به اطلاعات، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات. سایر ویژگی‌های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می‌تواند مشمول این حفاظت باشند.

۱-۱-۱- سیستم امن

یک سیستم امن سیستمی است که اگر حمله‌کننده به آن ورودی بد بدهد، سیستم خراب نشود. خصوصیات اصلی یک سیستم امن عبارتند از:

- **محرمانگی**:[1] محرمانگی یعنی اطلاعات تنها توسط افرادی که تائید صلاحیت شده‌اند، قابل دیدن باشد. به‌عنوان‌مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند.
- **صحت**:[2] صحت یعنی داده‌ها نباید به‌صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند.

[1] Confidentiality
[2] Integrity

- **دسترسی‌پذیری**[1]: هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به‌عبارت‌دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های موردنظر را ارائه دهد.

۲-۱-اصطلاحات امنیتی

۱-۲-۱-آسیب‌پذیری[2]

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند دریکی از موارد زیر باشد:

- طراحی سیستم: به‌عنوان‌مثال طراحی پروتکل TCP/IP درست انجام‌نشده و بسته های TCP/IP به‌صورت متن ساده[3](رمز نشده) هستند.
- پیاده‌سازی: به‌عنوان‌مثال در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است.
- ایراد در عملیات سیستم: فرآیندها درست انجام نمی‌شود. به‌عنوان‌مثال یک فرم پرشده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آن را ببیند.

۲-۲-۱-حمله[4]

حمله عبارت است از بهره‌برداری از آسیب‌پذیری‌های یک سیستم.

۳-۲-۱-تهدید[5]

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

---

1 Availability
2 Vulnerability
3 Clear Text
4 Attack
5 Threat

۴-۲-۱-مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- Authentication: تائید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت(مانند یک شخص یا یک سرویس‌دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلال‌گر ثالث است که خود را به‌جای طرف واقعی جا زده است.
- Authorization: اجازه[۸]مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احرازشده، مجوز انجام چه‌کارها و عملیاتی را در سیستم دارد.
- Accounting: حسابداری مکانیزمی است که مشخص می‌کند فرد موردنظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به‌عنوان‌مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهم‌ترین مرحله Authentication است که تأمین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به‌عنوان‌مثال وقتی فردی می‌خواهد به سیستم دسترسی پیدا کند، ما می‌خواهیم بدانیم آیا همان فرد موردنظر است یا خیر، تائید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به‌عنوان‌مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تائید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر کارکنان دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تائید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تائید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین

8Authorization

Authorization نیز با موفقیت انجام می‌شود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۳-۱-سرویس‌های امنیتی

سرویس امنیتی سرویسی است که برای ارتقاء امنیت داده مورداستفاده قرار می‌گیرد. تحقق سرویس‌های امنیتی، با استفاده از یک یا چند مکانیزم امکان‌پذیر است. سرویس‌های امنیتی سیاست‌های امنیتی[۹] را ارائه کرده و توسط مکانیزم‌های امنیتی اجرا می‌شوند. RFC 2196 سیاست امنیتی را به این شکل تعریف می‌کند:

سیاست‌های امنیتی قوانینی است که باید توسط افرادی که به فناوری‌ها و دارایی‌های اطلاعاتی سازمان شما دسترسی دارند، رعایت شود.

دو نوع سرویس امنیتی متداول وجود دارد که عبارتند از:

- سرویس امنیتی RFC2828
- سرویس امنیتی X.800

برخی از سرویس‌های امنیتی X.800 عبارتند از: احراز هویت ، کنترل دسترسی، محرمانگی، جامعیت داده، عدم انکار و قابلیت دسترسی.

۴-۱-مکانیزم‌های امنیتی

مکانیزم‌های امنیتی، روش‌ها و راهکارهایی برای تشخیص و جلوگیری از حمله‌های امنیتی هستند. همان‌طور که ذکر شد سرویس‌های امنیتی توسط مکانیزم‌های امنیتی اجرا می‌شوند. برخی از مکانیزم‌های امنیتی عبارتند از:

۱.رمزنگاری :[۱۰] رمزنگاری نقشی کلیدی در امنیت دارد. بسیاری از نیازهای امنیتی و سرویس‌های امنیتی نظیر تائید هویت، محرمانگی به‌وسیله رمزنگاری تأمین می‌شوند.

---

9 POLICY
10 Enchipherment

۲. امضای دیجیتال:[۱۱] این مکانیزم برای تائید اعتبار فرستنده و صحت اطلاعات فرستاده‌شده به کار می‌رود.
۳. کنترل دسترسی:[۱۲] اجازه دستیابی به اطلاعات (خواندن و نوشتن) را فقط به افراد مجاز می‌دهد.
۴. کنترل مسیر:[۱۳] مسیریابی امن از هر مسیر امکان عبور مقدار مشخصی از داده را ممکن می‌سازد. در غیر این صورت یک شکاف امنیتی رخ می‌دهد. به‌طورکلی وظیفه یک الگوریتم مسیریابی خوب فقط یافتن کوتاه‌ترین مسیر نیست، بلکه الگوریتم مسیریابی باید منصف باشد و بتواند ترافیک شبکه را روی مسیرهای مختلف توزیع نماید.
۵. کنترل ترافیک:[۱۴] در کانال‌های ارتباطی ناامن اطلاعات به‌صورت رمز شده ارسال می‌گردد تا چنانچه مهاجم پیام‌ها را شنود کند، نتواند پیام اصلی را از داخل آن استخراج نماید. اما حمله‌کننده می‌تواند اطلاعاتی از قبیل مبدأ، مقصد و اندازه پیام‌ها را تحلیل نموده و از آن‌ها برای یافتن برخی از پیام‌ها یا تعیین کلید رمزنگاری استفاده نماید. به‌عنوان‌مثال در یک سیستم نظامی ممکن است دشمن حجم داده‌های ارسالی را تحلیل کرده و چنانچه در یک روز خاص حجم اطلاعات بیش‌ازاندازه معمول باشد، حدس بزند که احتمالاً قرار است عملیاتی انجام گردد.
مکانیزم کنترل ترافیک در پیام ارسالی بیت‌هایی جاگذاری کرده تا تلاش تحلیل ترافیک را خنثی نماید.

۱-۵- خط‌مشی‌ها یا سیاست‌های امنیتی

عناصر دخیل در سیاست‌های امنیتی در RFC 2196 لیست و ارائه‌شده‌اند.
GIAC Security[۱۵] سیاست‌های امنیتی را به شرح ذیل تعریف می‌کند:
"یک سیاست امنیتی انجام اعمالی است که باید صورت بگیرد تا بتوان از اطلاعات ذخیره‌شده در کامپیوتر محافظت کرد". یک سیاست امنیتی مؤثر باعث ایجاد امنیت نسبی

11 Digital Signature
12 Access Control
13 Routing Control
14 Traffic Control
15 Global Information Assurance Certification

برای کاربران می‌شود و به کاربران اجازه می‌دهد تا بتوانند بدون ترس کارهای خود را انجام دهند. یک سیاست امنیتی چیزی جز یک راهبرد برای نگهداری اطلاعات و منابع شبکه نیست. در یک سازمان سیاست‌های امنیتی مختلفی تدوین می‌گردد که برخی از آن‌ها عبارتند از:

۱-سیاست‌های کلمه عبور

۲-سیاست‌های ایمیل

۶-سیاست‌های دستیابی به اینترنت

۷-سیاست‌های پشتیبان‌گیری

۸-سیاست‌های تشخیص نفوذ

۱-۵-۱- سیاست‌های کلمه عبور

سیاست‌های کلمه عبور یکی از مسائل مهم امنیت شبکه است. وجود یک سیاست امنیتی حساب شده برای پسوردها امری ضروری است. نمونه‌ای از این سیاست‌ها به شرح ذیل است:

۱-کلمات عبور نباید شامل لغات موجود در دیکشنری باشد.

۲-حتی‌الامکان اسم شخص یا چیزی نباشد (چون معمولاً اسم اشیاء در دیکشنری وجود دارد).

۳-نام مکان خاصی نباشد.

۴-ترکیب مشخصی از کلمات روی صفحه‌کلید نباشد(مانندALI123).

۵-شماره تلفن نباشد.

۶-نباید ترکیبی از موارد بالا به‌علاوه یک حرف یا رقم باشد.

۱-۵-۲-سیاست‌های اینترنتی

اینترنت مجموعه شگفت‌آوری از اطلاعات است که تنها با چند کلیک ساده می‌توان به این اطلاعات دسترسی پیدا کرد. در میان این اطلاعات ممکن است بعضی از آن‌ها حاوی مطالب غیراخلاقی باشند. لذا شما صریحاً محتاج به یک سیاست مخصوص برای استفاده از اینترنت هستید.

۳-۵-۱-پشتیبان‌گیری و احیای اطلاعات

در این سیاست باید موارد زیر را مدنظر قرار دهید:
۱-برنامه پشتیبان گیری چه زمانی باید اجرا شود و هرچند وقت یک‌بار اجرا شود
۲-چه نوع پشتیبانی باید گرفته شود (کامل ، تفاضلی، افزایشی، ترکیبی)
۳-از چه رسانه‌ای برای ذخیره‌سازی اطلاعات باید استفاده شود(CD یا نوار مغناطیسی)

۶-۱-مفهوم سیستم مدیریت امنیت اطلاعات

ISMS یا سیستم مدیریت امنیت اطلاعات استانداردهایی را برای ایمن‌سازی فضای تبادل اطلاعات در سازمان‌ها ارائه می‌دهد. این استانداردها شامل مجموعه‌ای از دستورالعمل‌هایی است تا بتواند فضای تبادل اطلاعات یک سازمان را با اجرای یک طرح مخصوص به آن سازمان ایمن نماید. امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه‌ی رویکرد مخاطرات کسب‌وکار قرار داشته و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی و بهبود امنیت اطلاعات است.

۷-۱-استانداردهای مدیریتی ارائه‌شده در خصوص امنیت اطلاعات

بر اساس نگرش سیستماتیک ISMS، تأمین امنیت فضای تبادل اطلاعات سازمان‌ها، به‌یک‌باره مقدور نیست و لازم است این امر به‌صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد. به این منظور استانداردهای مختلفی ارائه‌شده است که متداول‌ترین و معروف رین آن‌ها عبارتند از:

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- استانداردهای مدیریتی سری ۲۷۰۰۰ موسسه بین‌المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد
- استاندارد ISO 31000 برای مدیریت ریسک

۸-۱-استانداردهای خانواده ISO27000

در سال ۲۰۰۵ موسسه بین‌المللی استاندارد به این نتیجه رسید که یک استاندارد واحد جوابگوی نیاز جامعه جهانی برای برقراری امنیت اطلاعات در حوزه‌های مختلف نیست. ازاین‌رو اقدام به تشکیل خانواده استاندارد ISO27000 نمود که جنبه‌های مختلف این امر را پوشش می‌دهد. جدول۱-۱ استانداردهای خانواده ISO 27000 این استانداردها را نشان میدهد.

جدول۱-۱: استانداردهای خانواده ISO 27000

شماره استاندارد	شرح
۲۷۰۰۰	مقدمه و مروری بر استانداردهای خانواده ISMS به همراه تعریف واژگان رایج مورداستفاده.
۲۷۰۰۱	ارائه الزامات استاندارد به‌منظور احراز صلاحیت سازمان‌ها جهت اخذ گواهینامه.
۲۷۰۰۲	مجموعه‌ای از تجربیات موفق در زمینه ISMS و راهنمای تمرین اجرای ISMS
۲۷۰۰۳	راهنمای پیاده‌سازی سیستم مدیریت امنیت اطلاعات(ISMS)
۲۷۰۰۴	استاندارد اندازه‌گیری و تعیین سطح مدیریت امنیت اطلاعات.
۲۷۰۰۵	استاندارد مدیریت ریسک در امنیت اطلاعات.
۲۷۰۰۶	راهنمای مراحل دریافت گواهینامه.
۲۷۰۰۷	راهنمای بازرسی و نظارت بر ISMS
۲۷۰۱۱	راهنمای پیاده‌سازی ISMSدر صنعت مخابرات.
۲۷۷۹۹	راهنمای پیاده‌سازی ISMS در حوزه سلامت.

۹-۱-گزارش فنی ISO/IEC TR ۱۳۳۳۵

گزارش فنی ISO/IEC TR ۱۳۳۳۵ در قالب ۵ بخش مستقل در فواصل سال‌های ۱۹۹۶ تا ۲۰۰۱ توسط موسسه بین‌المللی استاندارد (ISO) منتشرشده است.