INSO-ISO-IEC

27033-2

1st.Edition

Identical with
ISO/IEC 27033-2:2012
Feb.2014

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران-ایزو-آی ای سی

۲-۲۷۰۳۳

چاپ اول

اسفند ۱۳۹۲

فناوری اطلاعات- فنون امنیتی- امنیت شبکه

قسمت۲:

راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه

Information technology — Security techniques — Network security
Part 2:
Guidelines for the design and implementation of network security

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[۱] ،کمیسیون بین المللی الکتروتکنیک (IEC)[۲] و سازمان بین المللی اندازه شناسی قانونی (OIML)[۳] است و به عنوان تنها رابط[۴] کمیسیون کدکس غذایی (CAC)[۵] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها پایش می‌کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3 - International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- امنیت شبکه

قسمت۲:

راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه»

رئیس:	**سمت و/ یا نمایندگی**
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل اداره خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
آریا، بهناز (دکتری فناوری اطلاعات)	نماینده سازمان نظام صنفی رایانه‌ای کشور
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسئول سازمان فناوری اطلاعات ایران
خوشنویسان، نازنین (فوق لیسانسMBA)	پژوهش‌گر دانشگاه شهید بهشتی
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم

عباس نژاد، علی (دکتری مدیریت فناوری اطلاعات)	رئیس هیات مدیره شرکت کهکشان نور
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
کیامهر، بیتا (لیسانس الکترونیک)	رییس اداره هماهنگی فعالیت‌های مطالعاتی
ناظمی، اسلام (دکتری کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
یوسف زاده، سمیرا (فوق لیسانس مهندسی کامپیوتر نرم‌افزار)	پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت۲: راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و نوزدهمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۲/۱۱/۱۹ مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه‌شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهدگرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 27033-2:2012, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security.

فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت۲: راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه

۱ هدف و دامنه کاربرد

هدف از تدوین این قسمت از سری استاندارد ملی، ارائه راهنماهایی برای سازمان‌ها به منظور برنامه‌ریزی، طراحی، پیاده‌سازی و مستندسازی امنیت شبکه است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد،اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده- است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 7498 (all parts), Information technology — Open Systems Interconnection — Basic Reference Model[1]

۲-۲ استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، فناوری اطلاعات - فنون امنیتی - سامانه های مدیریت امنیت اطلاعات - مرور کلی و واژگان

۲-۳ استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - سامانه های مدیریت امنیت اطلاعات - الزامات

۲-۴ استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات

۲-۵ استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات - فنون امنیتی - مدیریت مخاطرات امنیت اطلاعات

2-6 ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts[2]

۱- معادل کنونی این سری استانداردها، استانداردهای ملی ایران شماره ۱۶۲۷۴(تمامی قسمت‌ها)، فناوری اطلاعات -اتصال متقابل سامانه های باز مدل مرجع پایه بوده که همگی مصوب ۱۳۹۱ هستند.

۲- معادل کنونی این استاندارد، استاندارد ملی ایران شماره ۱-۱۴۸۶۶، فناوری اطلاعات -فنون امنیتی -امنیت شبکه -قسمت ۱- مرور کلی و مفاهیم مصوب ۱۳۹۱ است.

۳ اصطلاحات و تعاریف

برای اهداف این استاندارد ملی تعاریف و استانداردهای آورده شده در استاندارد ملی ایران شماره ۱۶۲۷۴(تمامی قسمت‌ها)، استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، استاندارد ملی ایران شماره ۲۷۰۰۲: سال۱۳۸۷، استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲ و استاندارد ملی ایران شماره ۱-۱۴۸۶۶: سال ۱۳۹۱ مورد نظر قرار می‌گیرد.

۴ کوته‌نوشت‌ها

برای اهداف این استاندارد ملی کوته‌نوشت‌های مورد استفاده در استاندارد ملی ایران شماره ۱-۱۴۸۶۶: سال ۱۳۹۱ و آنچه در زیر آمده است قابل اعمال هستند.

IDS	Intrusion Detection System	سامانه‌ی تشخیص نفوذ
IPS	Intrusion Prevention System	سامانه‌ی پیشگیری از نفوذ
POC	Proof of Concept	اثبات مفهوم
RADIUS	Remote Authentication Dial-In User Service	خدمت احراز هویت راه‌دور کاربر شماره‌گیر
RAS	Remote Access Service	خدمت دسترسی راه‌دور
SMS	Simple Message Service	خدمت پیام ساده
SMTP	Simple Mail Transfer Protocol	پروتکل ساده نامه‌رسانی
TACACS	Terminal Access Controller Access Control System	سامانه کنترل دسترسی به کنترل‌کننده پایانه دسترسی
TFTP	Trivial File Transfer Protocol	پروتکل انتقال پرونده جزئی
TLS	Transport Layer Security	امنیت لایه انتقال

۵ ساختار سند

ساختار این استاندارد ملی شامل موارد زیر است:

- آماده‌سازی برای طراحی امنیت شبکه
  - مقدمه
  - شناسایی دارایی‌ها
  - گردآوری الزامات
  - بازنگری الزامات
  - بازنگری طراحی‌ها و پیاده‌سازی‌های موجود
- طراحی امنیت شبکه
  - مقدمه
  - اصول طراحی

- نهایی‌سازی[1] طراحی
- پیاده‌سازی
- مقدمه
- معیار برای انتخاب اجزای شبکه
- معیار برای انتخاب محصول یا فروشنده
- مدیریت شبکه
- رویدادنگاری، پایش و رویارویی با پیشامدها[2]
- مستندسازی
- برنامه‌های آزمون و انجام آزمون
- نهایی‌سازی

۶ آماده‌سازی برای طراحی امنیت شبکه

۶-۱ مقدمه

اهداف امنیت شبکه، توان‌مندسازی جریان‌های اطلاعاتی است که فرآیندهای کسب و کار سازمان را ارتقا می‌دهند و از جریان‌های اطلاعاتی که فرآیندهای کسب‌وکار سازمان را تنزل می‌دهند، پیشگیری می‌کنند. کار آماده‌سازی برای طراحی و پیاده‌سازی امنیت شبکه شامل مراحل زیر است:

- شناسایی دارایی‌ها
- گردآوری الزامات
- بازنگری الزامات
- ارزشیابی گزینه‌های فنی و محدودیت‌ها
- ارزشیابی طراحی‌ها و پیاده‌سازی‌های موجود

این مراحل بهتر است منجر به مستندسازی زودهنگامی شوند که شامل تمامی ورودی‌ها[3] برای دنبال‌کردن گام-های طراحی و پیاده‌سازی باشد.

۶-۲ شناسایی دارایی‌ها

شناسایی دارایی‌ها اولین گام حیاتی برای تعیین مخاطرات امنیت اطلاعات هر شبکه‌ای است. دارایی‌هایی که باید محافظت شوند آنهایی هستند که افشای نامناسب، دست‌کاری یا خارج از دسترس کردن آن‌ها منجر به تنزل فرآیندهای کسب‌وکار سازمان‌ها می‌شوند. این دارایی‌ها شامل دارایی‌های فیزیکی(کارسازها[4]، سوده‌ها[5]،

1- Sign-off
2- Incident Response
3- Inputs
4- Servers
5- Switches

مسیریاب‌ها[1] و غیره) و دارایی‌های منطقی(تنظیمات پیکربندی،کد قابل‌اجرا، داده و غیره) هستند. این ثبت دارایی‌ها بهتر است به عنوان بخشی از تحلیل مخاطره‌ی برنامه‌ریزی تداوم[2]/ بازیابی پس از سانحه[3] وجود داشته‌باشد. سؤال‌هایی که باید پاسخ داده شوند از قرار زیر هستند:

- انواع مختلف تجهیزات شبکه و گروه‌بندی‌های امکاناتی[4] که نیاز به حفاظت دارند چه هستند؟
- انواع مختلف فعالیت‌های شبکه که نیاز به حفاظت دارند چه هستند؟
- چه دارایی‌های اطلاعاتی و توانایی‌های پردازش اطلاعاتی نیاز به حفاظت دارند؟
- دارایی‌های اطلاعاتی در کجای معماری سامانه‌های اطلاعاتی قرار گرفته‌اند؟

دارایی‌های قابل شناسایی شامل موارد موردنیازی است که بتواند به صورت امن از مدیریت، کنترل و ترافیک کاربر و ویژگی‌های[5] مورد نیاز کارکردی زیرساخت شبکه، خدمات و برنامه‌های کاربردی پشتیبانی کنند. این‌ها شامل افزاره‌هایی[6] مانند میزبان‌ها، مسیریاب‌ها، دیوارهای آتش و مانند آن، واسط‌های[7] کاربری (داخلی و خارجی)، اطلاعات ذخیره‌شده/پردازش شده و پروتکل‌های مورد استفاده هستند.
حفاظت از دارایی‌های زیرساختی تنها بخشی از هدف طراحی امنیت شبکه است. هدف اصلی حفاظت از دارایی-های کسب‌وکار، مانند اطلاعات و فرآیندهای کسب‌وکار است.

۶-۳ گردآوری الزامات

۶-۳-۱ الزامات قانونی و مقرراتی

الزامات قانونی و مقرراتی مربوط به موقعیت و کارکرد شبکه بهتر است جمع‌آوری و بازنگری شوند تا اطمینان حاصل‌شود که این الزامات در طراحی شبکه منظور شده‌اند. در جایی که اطلاعات در مرزهای قانونی[8] و مقرراتی جریان دارد، بهتر است ملاحظات خاص در نظر گرفته شوند. در چنین مواردی الزامات دو طرف مرز باید ثبت شوند.

۶-۳-۲ الزامات کسب‌وکار

فرایندهای کسب‌وکار سازمان‌ها و انواع رده‌بندی داده، الزامات دسترسی به آنها را تعیین می‌کند. شبکه بهتراست به گونه‌ای پیکربندی شود تا این دسترسی به/از دارایی‌های اطلاعاتی برای کاربران مجاز مقتضی را فعال و از

1- Routers
2- Continuity
3- Disaster Recovery
4- Facility Groupings
5- Features
6 -Devices
7 - Interfaces
8- Jurisdictional

دیگر دسترسی‌ها پیشگیری کند. دسترسی به اطلاعات، اغلب مربوط به درگاه‌های[1] باز (برای مثال پروتکل انتقال ابرمتن (HTTP)[2] روی پروتکل کنترل انتقال (TCP)[3] درگاه 80)، میزبان‌های مشخص (مانندwww.example.com در آدرس پروتکل اینترنتی (IP)[4] شماره 10.11.12.13)، گروه‌های خاصی از میزبان‌ها (برای مثال زیر شبکه 172.128.97.64/24) یا افزاره‌های واسط شبکه خاص (مانند واسطی با آدرس کنترل دسترسی رسانه (MAC)[5] شماره 10:00:00:01:02:03) است. نیاز است تا سازمان خدماتی را که برای دیگران فراهم می‌کند، خدماتی که از دیگران دریافت می‌کند و خدمات داخلی خود را شناسایی کند.

۶-۳-۳ الزامات عملکردی

برای اینکه بتوان پیکربندی‌های خطوط ارتباطی، کارسازها و دروازه‌های[6] امنیتی/دیوارهای آتش، به‌گونه‌ای مستندسازی شوند، که در پیاده‌سازی، مطابق با انتظارات کاربر، سطح خوبی از خدمات، بدون «پیکربندی بیش از حد» و هزینه‌های غیرضروری مرتبط، فراهم شود، به ترافیک داده نیاز است.

در این خصوص بهتر است اطلاعاتی جمع آوری شوند، به طور مثال: سرعت خطوط ارتباطی موجود، پیکربندی/ظرفیت مسیریاب‌ها در هر مکان متعلق به طرف سوم، تعداد کاربرانی که مجاز به دسترسی از طریق هر پیوند هستند (دسترسی هم‌زمان و تعداد کاربران مجاز به دسترسی)، کمینه، میانگین و بیشینه‌ی زمان موردنیاز برای اتصال کاربر، هویت کاربران مجاز که از طریق پیوند دسترسی دارند، تعداد دفعات مورد نیاز بازدید از صفحات وب، دفعات موردنیاز دسترسی به پایگاه داده[7] رشد مورد انتظار یک ساله و سه/پنج ساله یا آیا ثبت ورود به ویندوز نیاز است. برای یافتن تعداد مناسب درگاه‌ها و کانال‌های مورد نیاز به خصوص در اتصال‌های شماره‌گیری می‌توان از نظریه جدول مخابراتی (صف‌بندی[8]) سود جست. این الزامات کارآیی بهتر است بازنگری شوند، پرس‌وجوها پاسخ داده‌شوند و معیار کارآیی مورد نیاز توسط معماری فنی و معماری فنی امنیتی مرتبط و مورد توافق رسمی، برآورده شوند.

۶-۴ الزامات بازنگری

بازنگری توانمندی‌های کنونی و هر تغییر برنامه‌ریزی شده در معماری شبکه نیاز است که انجام شوند و با معماری امنیت فنی در حال توسعه مقایسه شود تا هر ناسازگاری یادآوری شود. هر ناسازگاری نیاز است که بازنگری شود و معماری‌های متناسب با آن اصلاح شود[9].

اطلاعاتی که در طول بازنگری جمع‌آوری می‌شوند بهتر است، شامل کمینه موارد زیر باشند:

- شناسایی نوع(انواع) اتصال(اتصالات) شبکه که استفاده می‌شوند،

---

1 - Ports
2 - Hyper text transfer protocol
3 - Transmission control protocol
4 - Internet Protocol
5 - Media access control
6 - Gateways
7 - Database
8- Queuing
9- Modified

- تعیین مخاطرات امنیتی،
- توسعه فهرست معماری امنیت فنی و کنترل‌های امنیتی مورد نیاز،
- پروتکل‌های شبکه‌ای که استفاده می‌شوند،
- برنامه‌های کاربردی تحت شبکه که در جنبه‌های مختلف شبکه استفاده می‌شوند

اطلاعات گردآوری شده بهتر است در زمینه توانایی‌های شبکه باشند. جزئیات بهتر است از معماری شبکه مرتبط به‌دست آیند و این جزئیات باید برای فراهم آوردن درک لازم و ایجاد زمینه مناسب برای گام‌های فرآیندی بعدی بازنگری شوند. با روشن شدن این جوانب در مرحله‌ی اولیه‌ی ممکن، فرآیند شناسایی «معیار شناسایی الزامات امنیتی مرتبط»، شناسایی نواحی[1] کنترل و بازنگری گزینه‌های معماری امنیتی فنی و تصمیم‌گیری در مورد این که کدام یک بهتر است، اتخاذ شود، کارآمدتر می‌شوند و درنهایت نتیجه‌ای قابل اعمال در راه‌حل امنیتی می‌دهند.. برای مثال ممکن است به خاطر موقعیت مکانی فقط یک مجرا برای اتصالات شبکه وجود داشته باشد بنابراین حتی با این‌که کنترل امنیتی ممکن است مجراهای متفاوتی برای اتصالات افزونه[2] داشته باشد، اما بر اساس موقعیت مکانی انتخاب‌شده، این امر امکان‌پذیر نیست. کنترل‌های دیگر مجاز هستند تعیین‌شوند تا بهترین راه برای حفاظت از اتصالات شبکه پیداشود.

با در نظر گرفتن جنبه‌های معماری شبکه و برنامه کاربردی در مرحله اولیه بهتر است فرصتی داد که اگر به صورت واقع‌بینانه با معماری کنونی به راه‌حل امنیتی قابل قبولی، نتوان دست یافت، آن معماری‌ها بازنگری و احتمالاً تجدید نظر شوند.

۶-۵ بازنگری طراحی‌ها و پیاده‌سازی‌های موجود

بازنگری کنترل‌های امنیتی موجود باید در پرتو نتایج حاصل از بازنگری مدیریت و ارزیابی مخاطره‌ی امنیت انجام‌گیرد(جزئیات مدیریت مخاطره را می‌توان در استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲ یافت). نتایج ازریابی مخاطره امنیت ممکن است نشان دهند که کدام کنترل‌های امنیتی متناسب با تهدیدهای ارزیابی شده مورد نیاز است. تحلیل شکاف باید بر اساس معماری امنیت شبکه‌ی فعلی تکمیل شود تا معین گردد به چه چیزی در معماری امنیت شبکه‌ی موجود مورد اشاره نشده است.

توصیه می‌شود معماری امنیت شبکه دربرگیرنده‌ی کنترل‌های امنیت موجود، درنظر گرفته نشده و جدید باشد.

۷ طراحی امنیت شبکه

۷-۱ مقدمه

دلیل وجود معماری امنیت شبکه محدود کردن جریان ترافیک بین دامنه‌های مورد اعتماد[3] مختلف است . واضح‌ترین مرز بین دامنه‌های اعتماد رابط بین شبکه داخلی یک سازمان و دنیای خارج است. همچنین سازمانی با اندازه قابل توجه، مرزهایی بین دامنه‌های اعتماد داخلی دارد که باید شناسایی و کنترل شوند. معماری امنیت

1- Areas
2- Redundant
3- Trust Domains

شبکه شامل توصیفی[1] از واسطهای بین شبکه‌ی داخلی یک سازمان/انجمن و دنیای بیرونی است. این معماری بازتابی از الزامات ذکر شده در بند ۶-۴ است و چگونگی محافظت از سازمان در برابر تهدیدات و آسیب پذیری-های عمومی را نشان می‌دهد، آنچنان که در استاندارد ملی ایران شماره ۱-۱۴۸۶۶، توصیف شده است.
رهنمود[2]در مورد بهروش‌های[3] طراحی در بند ۷-۲ در زیر آمده است و رهنمود در مورد جنبه‌های معماری امنیت شبکه که مربوط به فناوری شبکه‌بندی[4] مشخص برای نشان دادن الزامات امروز و آینده‌ی نزدیک است، در استاندارد ISO/IEC 27033-4 آمده است و الی آخر. اشاره دارد. رهنمود برای فرانامه‌های[5] مشخصی که برای یک سازمان امکان‌پذیر است، در استاندارد ISO/IEC 27033-3 پوشش داده شده است.
فرضیات فنی ایجادشده در طی جمع‌آوری الزامات بهتراست مستندسازی شوند، به‌طور مثال:

- توصیه می‌شود فقط ارتباطات IP مجاز[6] اجازه برقراری داشته‌باشند (دیوارهای آتش به طور عادی فقط از ارتباطات IP پشتیبانی می‌کنند و اگر هر پروتکل دیگری اجازه فعالیت داشته باشد ممکن است مدیریت آن-ها با مشکل باشد)؛
- اگر به پروتکل‌های فاقد IP نیاز باشد توصیه می‌شود یا با خارج از معماری امنیت سر وکار داشته باشند یا پروتکل را تونل‌زنی[7] کند.

معماری امنیت شبکه به صورت عادی خدمات زیر را دربرمی‌گیرد اما محدود به این موارد نیست:

- شناسایی و احراز هویت (گذرواژه‌ها، نشان‌افزارها[8]، کارت‌های هوشمند،گواهی‌نامه‌ها، TACACS+/RADIUS/RAS[9] و غیره)؛
- کنترل‌های دسترسی منطقی (ورود[10] تکی، کنترل دسترسی مبتنی بر نقش[11]، پایگاه‌های داده مورداعتماد، کنترل‌های برنامه کاربردی، دیواری آتش، افزاره‌های پیشکار[12] و غیره)؛
- ممیزی و حسابرسی امنیتی (رویدادنگار[13]های ممیزی، تسهیلات تحلیل رویدادنگارهای ممیزی، تسهیلات تشخیص نفوذ، افزاره‌های یک بار نوشتن و چندبارخواندن (WORM[14]) و غیره)؛
- پاک‌سازی مطمئن انبارش[15]/ حذف امن[16] (تسهیلات «زدایش[17]» اثبات‌پذیر[1])؛

1- Description
2- Guidance
3- Best Practices
4- Networking
5-Scenario
6- Authorized
7- Tunneling
8- Tokens
9- Terminal Access Controller Access Control System Plus
10- Sign on
11 -Role
12- Proxy
13- Log
14- Write Once Read Many
15- Assured storage clearance
16- Secure deletion
17- Wipe

- آزمون امنیت(پویش آسیب‌پذیری، دیده‌بانی[2] شبکه، آزمون نفوذ[3] و غیره)؛
- محیط[4] توسعه امن(محیط‌های توسعه و آزمون جداگانه، بدون مترجم[5] و غیره)؛
- کنترل تغییر نرم‌افزار(نرم‌افزار مدیریت پیکربندی، کنترل نسخه و غیره)؛
- توزیع نرم‌افزار امن (امضای رقمی، TLS،SSL (RFC 5246) و غیره)؛
- نگهداری و دسترس‌پذیری امن (تسهیلات پشتیبان‌گیری/بازگردانی[6]خوب، برگشت‌پذیری[7]، خوشه‌بندی[8]، حفاظ‌های داده[9]، ارتباطات متنوع و غیره)؛
- امنیت انتقال (استفاده از رمزگذاری انتقال، فناوری طیف گسترده[10]، LAN[11]های بی‌سیم (WLAN)[12]، شبکه‌های خصوصی مجازی(VPN)[13]/برون‌نت‌ها[14]).

۷-۲ اصول طراحی

۷-۲-۱ مقدمه

محدوده مخاطرات رایج مربوط به معماری‌های امنیت شبکه‌بندی، همان خطاهای طراحی هستند. این خطاها به سبب طراحی ضعیف و/یا نبود ملاحظات مناسب برای برنامه‌ریزی تداوم کسب‌وکار یا عدم تطابق طراحی با سطح تهدید مورد انتظار به‌وجود می‌آیند. عناصر بنیادینی برای توسعه معماری‌های امنیتی شبکه مورد نیاز هستند تا این معماری‌ها بتوانند تمامی کنترل‌های امنیتی و الزامات کسب‌وکار شناسایی شده را پوشش‌دهند. بیشتر این عناصر را می‌توان با بهترین روش‌های طراحی امنیت شبکه پوشش داد. استاندارد ISO/IEC 27033-4 و استانداردهای بعدی، طراحی و پیاده‌سازی به‌روش‌های معماری امنیت فنی شبکه را به همراه جزئیات در برخی جنبه‌ها در برمی‌گیرند. رهنمود با جزئیات بیشتر در مورد بهترین روش‌های پیاده‌سازی را می‌توان در نشریات دیگر یافت.

بندهای زیر رهنمودی عمومی پیرامون بهترین روش‌های طراحی فراهم می‌آورد که باید به هنگام ساخت معماری امنیت شبکه دنبال شود.

1- Provable wipe facilities
2- Sniffing
3- Penetration
4- Environment
5- Compiler
6- Restore
7- Resilience
8- Clustering
9- Data vaults
10- Spread spectrum
11- Local Area Networks
12- Wireless
13-Virtual private networks
14- Extranets

۷-۲-۲ دفاع عمقی[1]

سازمان‌ها نیاز است مسئله امنیت را نه تنها از یک منظر[2]، بلکه با رویکردی لایه‌ای فراگیر[3] ببینند. امنیت باید در تمام لایه‌های شبکه، جامع[4] باشد. اتخاذ رویکردی لایه‌ای با عنوان «دفاع عمقی» شناخته می‌شود. مؤلفه‌های امنیت ترکیبی از خط‌مشی، طراحی، مدیریت و فناوری هستند. هر سازمان باید نیازهای خود را تعیین و دفاع عمقی را بر اساس همان نیازها طراحی کند.

بسیاری از افزاره‌های سیار دارای اتصال[5] همه‌گذر(USB)[6]، اتصال شبکه و همچنین قابلیت بی‌سیم هستند. این افزاره‌ها می‌توانند به شبکه داخلی یا سامانه‌های روی آن متصل شوند که این اتصال به صورت موردی[7] است که بهتر است از طریق اتصال افزاره‌های سیار به صورت باز و ناامن صورت پذیرد، این افزاره‌ها به عنوان یک نقطه دسترسی بی‌سیم قلابی[8] روی شبکه داخلی عمل کرده، می‌توانند کنترل های پیرامونی را دور بزنند. برای محدود کردن اتصال ناامن افزاره‌های سیار به شبکه بهتر است خط‌مشی‌های سخت‌گیرانه‌ای وضع شوند و پویش‌های روال‌مندی باید بر روی کانال‌های بی‌سیم انجام شوند تا تمام نقطه‌های دسترسی قلابی را بیابند.

توصیه می‌شود تمام نقطه‌های دسترسی بی‌سیم درون یک منطقه‌ی بی‌طرف(DMZ)[9] قرار داشته باشند. نقاط دسترسی که درشبکه‌ی داخلی قرار گرفته‌اند بهتر است تنظیمات سخت‌گیرانه‌ای داشته باشند: قوی‌ترین پروتکل امنیتی(جایی که قابلیت آن وجود دارد WPA2[10]) و پالایش آدرس‌های MAC به‌منظور محدود کردن افزاره-های متصل به افزاره‌های مجاز. استاندارد ISO/IEC 27033-3 جزئیات بیشتری را در مورد تهدیداتی که توسط فناوری ارتباطات سیار و کنترل‌های مربوط ارائه شده‌اند، فراهم می‌آورد.

اصل دفاع عمقی نحوه استفاده از کنترل‌های امنیتی چندگانه یا فنون امنیتی را بیان می‌کند تا به کاهش مخاطره‌ی مؤلفه‌های دفاعی که افشا[11] یا دور زده[12] می‌شوند، کمک کند. یک مثال می تواند نصب نرم‌افزار ضدویروس بر روی ایستگاه‌های کاری جداگانه باشد درحالی که ویژگی حفاظت از ویروس در دیواری آتش و کارسازهای همان محیط وجود دارد. این مجاز است که محصولات امنیتی متفاوتی از فروشندگان متعدد مورد استفاده قرار گیرند تا از خط سیرهای[13] بالقوه مختلفی در درون شبکه دفاع شود و کمک کند که از هرگونه کمبودی در دفاع که منجر به شکست گسترده‌تری می‌شود پیشگیری شود. این رویکرد به «رویکرد لایه‌ای» شهرت دارد.

1- Defence in depth
2- Perspective
3- Pervasive
4- Comprehensive
5- Connectivity
6- Universal serial bus
7- Ad-hoc
8- Rogue
9- Demilitarized zone
10- Wi-Fi protected Access
11- Compromise
12- Circumvented
13- Vector

شکل ۱نشان می‌دهد که امنیت پیرامونی[1] چگونه است، اهمیت امنیت زیرساخت، ذره‌ای کم‌تر است و اهمیت امنیت میزبان هم اندکی کمتر از قبلی است، سپس امنیت برنامه کاربردی و امنیت داده قراردارند. تمام لایه‌ها برای حفاظت از داده‌ها هستند.

شکل ۱- رویکرد دفاع عمقی

راه‌حل‌های امنیتی که بر اساس رویکرد لایه‌ای بوده انعطاف‌پذیر و مقیاس‌پذیر[2] هستند. راه‌حل این چنینی قابل-تطبیق با نیازهای امنیتی سازمان است.

۷-۲-۳ مناطق[3] شبکه

منطقه‌بندی شبکه از مفهومی استفاده می‌کند که در آن منابع سامانه با سطوح مختلف حساسیت(برای مثال مقدار رواداری[4] مخاطره‌ی متفاوت و آمادگی[5] برای تهدید) بهتر است در مناطق امنیتی جداگانه قرار داده‌شوند. این کار روشی ایجاد می‌کند که سامانه‌ها باید تنها داده‌هایی را در دسترس قرار دهند که برای انجام وظایف ضروری باشند(برای مثال فقط کارسازهایی که برای اینترنت خدمات فراهم می‌کنند در سامانه‌ی نام دامنه (DNS)[6] عمومی شوند).

مفهوم ساده‌ی برقراری جریان ترافیک شبکه به جایی که شما می‌خواهید و محدود کردن آن به جایی که شما نمی‌خواهید، دروازه امنیتی است: افزاره‌های اختصاصی دیوار آتش، توابع دیوار آتش در افزاره‌های IPS و فهرست‌های کنترل دسترسی در مسیریاب‌هاو سوده‌های شبکه.

1- Perimeter
2- Scalable
3- zones
4- Tolerance
5- Susceptibility
6- Domain name system

با جای‌گذاری[1] و پیکربندی مناسب دروازه‌ها به ساخت معماری‌های امن، تقسیم زیرساخت شبکه به مناطق امنیتی و کنترل ارتباطات مابین آنها کمک می‌شود. اطلاعات تکمیلی درمورد چگونگی گماردن و پیکربندی دروازه‌های امنیتی در استاندارد ISO/IEC 27033-4 آمده است.

اصل قسمت‌بندی[2]، قواعد طراحی امنیت شبکه‌ی زیر را شرح می‌دهد:

- شبکه‌هایی که سطوح حساسیت متفاوت دارند، بهتر است در مناطق امنیتی متفاوتی قرار داده‌شوند:
  - افزاره‌ها و سامانه‌های رایانه‌ای که برای شبکه‌های خارجی خدماتی فراهم می‌کنند(برای مثال اینترنت) بهتر است در منطقه دیگری(DMZ) نسبت به افزاره‌ها و سامانه‌های رایانه‌ای شبکه داخلی قرار بگیرند.
  - دارایی‌های راهبردی[3] بهتر است در مناطق امنیتی اختصاصی[4] قرار داده‌شوند.
  - توصیه می‌شود افزاره‌ها و سامانه‌های رایانه‌ای با سطح اعتماد کم مانند کارسازهای دسترسی از راه دور و نقاط دسترسی شبکه بی‌سیم در مناطق امنیتی اختصاصی قرار بگیرند.
- انواع متفاوت شبکه بهتر است در مناطق امنیتی جداگانه قرار بگیرند:
  - ایستگاه‌های کاری کاربر بهتر است در مناطق امنیتی جدا نسبت به کارسازها قرار گیرند.
  - سامانه‌های مدیریت شبکه و امنیت بهتر است در مناطق امنیتی اختصاصی قرار داده‌شوند.
  - سامانه‌های در مرحله توسعه بهتر است در مناطق دیگری نسبت به سامانه‌های محصول قرار بگیرند.

۷-۲-۴ طراحی برگشت‌پذیر

طراحی امنیت شبکه باید لایه‌های متعددی از افزونگی[5]را ترکیب کند تا مواردی را که نقطه تکی شکست[6] هستند از بین ببرد و قابلیت دسترسی زیرساخت شبکه را بیشینه سازد. این امر شامل استفاده از واسط‌های افزونه، پودمان‌های[7] پشتیبان، افزاره‌های آماده‌به‌کار[8]و مسیرهای افزونه‌ی هم‌بندی[9] می‌شود. به علاوه، طراحی‌ها از مجموعه گسترده‌ای از ویژگی[10]ها سود می‌برند با این هدف که شبکه برگشت‌پذیری بیشتری در مقابل حملات و شکست‌ها داشته باشد.

1- Placement
2 -Compartmentalization
3- Strategic assets
4- Dedicated
5- Redundancy
6- Single point of failures
7- Modules
8- Standby
9- Topology
10- Feature

۷-۲-۵ فرانامه‌ها

محیط شبکه‌ای تحت بازنگری را می‌توان با فرانامه(های) شبکه‌ای خاص و موضوع(های) فناوری که مرتبط با تهدیدهای خوب تعریف شده، ملاحظات طراحی و مسائل کنترلی هستند، مشخص‌کرد. چنین اطلاعاتی هنگام بازنگری گزینه‌های طراحی/معماری فنی امنیت و انتخاب و مستندسازی طراحی/معماری فنی امنیت منتخب و کنترل‌های امنیتی مربوطه بسیار مفید هستند.

مرجع چنین فرانامه‌هایی استاندارد ISO/IEC 27033-3 است. این استاندارد برای هر فرانامه رهنمودی با جزئیات در مورد تهدیدهای امنیتی و فنون طراحی امنیتی و کنترل‌های مورد نیاز برای تقابل با آن تهدیدها را آورده است.

۷-۲-۶ مدل‌ها و چارچوب‌ها

به طور سنتی هرمؤلفه از مهندسی سامانه امنیتی شامل انتخاب، استفاده یا توسعه یک مدل یا چارچوب امنیتی است.

مدل امنیتی برای توصیف هستارها[1] (مفاهیمی که توسط خط مشی امنیتی سازمان اداره می‌شود) و تعریف قواعد دسترسی لازم برای معرفی خط مشی ذکر شده، استفاده می‌شود. مدل امنیتی به‌طور عادی هم بر روی محرمانگی از طریق کنترل‌های دسترسی و هم بر روی یکپارچگی اطلاعات تمرکز دارد؛ بعضی به صورت رسمی و بقیه به صورت غیر رسمی تعریف شده‌اند.

چارچوب‌های امنیتی راهی را برای تدوین طرحی کلی[2] از چگونگی شکل‌دهی سامانه امن، برای سازمان‌ها فراهم می‌آورند. استاندارد ITU-T X.805 می‌تواند مثالی برای چارچوب باشد. این چارچوب فراگیری برای استاندارد-های سری ITU-T 800 است که توصیه‌هایی در مورد فراهم‌آوری امنیت شبکه سرتاسری[3] دارد. برای این منظور استاندارد X.805 مفهوم ابعاد امنیت را تعریف می‌کند. این ابعاد دربرگیرنده‌ی[4] ابزارها، فناوری‌ها، استانداردها، مقررات[5]، روال‌ها[6] و غیره هستند که تمام جنبه‌های امنیت را پوشش می‌دهد. استاندارد X.805 تصدیق می‌کند که می‌توان از سازوکارهای امنیتی افزون، به‌وسیله شناسایی قابلیت‌های امنیتی درون یک لایه که از لایه دیگر محافظت می‌کند، دوری کرد. به همین دلیل از هزینه کلی راه‌حل امنیتی کاسته می‌شود. استاندارد X.805 یک چارچوب امنیتی کلی است و به همین دلیل مشخصاتی برای هیچ سامانه یا مؤلفه اطلاعاتی خاص فراهم نمی-آورد. بلکه اصول امنیتی را مشخص می‌کند و به قابلیت‌های امنیتی که امنیت شبکه سرتاسری را تسهیل کرده-اند، می‌پردازد. برای یافتن مثالی ازچگونگی اعمال ITU-T 805 برای پشتیبانی از کنترل‌های استاندارد ملی ایران به شماره ۲۷۰۰۱ سال ۱۳۸۷، به پیوست پ مراجعه شود.

1- Entities
2- Outline
3- End to end
4- Container
5- Regulations
6- procedures

۷-۳ نهایی‌سازی طراحی

نهایی‌سازی طراحی امنیت شبکه کامل شده بهتر است با امضای سطوح مناسب مدیریتی انجام گیرد.

۸ پیاده‌سازی

۸-۱ مقدمه

پیاده‌سازی امنیت شبکه بهتر است بر اساس طراحی امنیت شبکه معرفی شده در بند ۷ صورت پذیرد.

پیاده‌سازی امنیت شبکه شامل قطعه‌بندی و قسمت‌بندی است

- معیار برای انتخاب مؤلفه‌های شبکه؛
- معیار برای انتخاب محصول یا فروشنده؛
- مدیریت شبکه؛
- رویدادنگاری، پایش و رویارویی با پیشامدها؛
- مستندسازی؛
- برنامه‌های آزمون وانجام آزمون ؛
- نهایی‌سازی

۸-۲ معیار برای انتخاب مؤلفه‌های شبکه

برای همه طراحی‌های شبکه امن ترکیبی از مؤلفه‌های عمومی وجود دارد که می‌توان از آنها استفاده کرد. این مؤلفه‌ها در ترکیبی استفاده می‌شوند که یک طراحی فنی امنیت شبکه را به‌وجود می‌آورند. بند ۸ و استاندارد ISO/IEC 27033-3 و استانداردهای بعدی این سری، یادآور جزئیات فنی برخی از مؤلفه‌های فهرست‌شده در زیر است. این مؤلفه‌ها در بعضی از ترکیب‌ها برای تأمین الزاماتی که در بند ۶-۴ آمده‌اند استفاده شده‌است. برخی از این مؤلفه‌ها به شرح زیر هستند:

- قطعه‌بندی و قسمت‌بندی
- سامانه‌های مدیریت امنیت(برای مثال مدیریت پایش و پیکربندی)
- فناوری‌های امنیتی پایه مانند مدیریت هویت، رمزنگاری و غیره
- افزاره‌های کنترل پذیرش[1] شبکه
- فنون کاهش تهدید
- افزاره‌های پیرامونی
- پالایه‌های[2] شبکه مانند دیوارهای آتش و افزاره‌های دسترسی از راه دور خدمات بازرسی[3] محتوا[4]
- سامانه‌های تشخیص نفوذ/ سامانه‌های پیشگیری از نفوذ

1- Admission
2- Filters
3- Inspection
4- Content

- محافظت نقطه‌پایانی[1]
- مسیریاب‌ها و سوده‌ها
- اتصالات برون‌شبکه‌ای

۸-۳ معیار برای انتخاب محصول یا فروشنده

توصیه نمی‌شود که انتخاب محصولات جداگانه صورت گیرند، بلکه بهتر است به عنوان فرآیندی تکرارشونده که با طراحی معماری امنیتی شبکه مرتبط است انجام شوند.

مثال‌هایی از اینکه بهتر است انتخاب محصول بر چه اساسی باشد، شامل موارد زیر است:

- تناسب فنی و شایستگی محصول؛
- کارآیی[2]؛
- پشتیبانی پروتکل؛
- برگشت‌پذیری؛
- سازگاری؛
- توسعه‌پذیری[3]؛
- امکانات مدیریت شبکه؛
- قابلیت ممیزی؛
- انطباق[4]؛
- مستندسازی فنی؛
- نگهداری؛
- تسهیلات تشخیصی[5] راه دور؛
- امنیت منطقی؛
- تضمین قابلیت‌های امنیتی توسط طرح‌هایی[6] برای ارزشیابی مانند استاندارد ملی ایران به شماره۱۵۴۰۸(یا معادل آن)؛
- «مشخصات» فروشنده(توانایی، ردیابی[7]سابقه، تعهد به کیفیت، جایگاه بازار، اندازه، صلاحیت کلی از جمله برای محصولات موردنظر، ثبات سازمانی/مالی[8]، مراجع و امکانات آموزشی[9])؛
- زمان‌بندی تحویل؛

1- Endpoint
2- Performance
3- Extensibility
4- Compliance
5- Diagnostic
6- Schemes
7- Track record
8- Financial
9- Training Facilities

- هزینه‌ها.

۸-۴ مدیریت شبکه

مدیریت شبکه به فعالیت‌ها، روش‌ها، روال‌ها و ابزارهایی اطلاق می‌شود که متعلق به عملیات، سرپرستی[۱]، نگهداری و تأمین[۲] سامانه‌های شبکه‌ای شده است.

- عملیات با فعال نگه داشتن شبکه(و خدماتی که فراهم می‌آورد) و کارکرد بی‌مشکل آن سروکار دارد که شامل پایش شبکه برای یافتن مشکلات در اسرع وقت و قبل از تحت تأثیر قرار دادن کاربران است.
- سرپرستی شبکه با ردیابی منابع در آن وچگونگی اختصاص آنها سروکار دارد و شامل تمام اصول «سازمان‌دهی حفظ و نگهداری سوابق[۳]» برای تحت کنترل نگه داشتن شبکه است.
- عملیات نگهداری به انجام تعمیرات و ارتقا می‌پردازد- برای مثال وقتی که باید یکی از تجهیزات جایگزین شود یا هنگامی که یک مسیریاب برای تصویر سامانه‌ی عامل[۴] نیاز به یک وصله[۵] دارد یا وقتی که یک سوده‌ی جدید به شبکه وصل می‌شود. نگهداری، هم‌چنین سنجه‌های[۶] بازدارنده[۷] و تصحیح‌کننده[۸] با این هدف که شبکه مدیریت شده «بهتر» کار کند، نیز دارد. مانند تنظیم پارامترهای پیکربندی افزاره.

پیکربندی نادرست مؤلفه‌های مربوط به شبکه چه داخلی چه خارجی باعث مخاطرات قابل ملاحظه‌ای هم برای قابلیت دسترسی و هم برای یکپارچگی و محرمانگی در شبکه می‌شود.
بنابراین کنترل‌هایی برای نشان‌دادن این مخاطرات ضروری هستند. این کنترل‌ها را می‌توان با عنوان کنترل‌های سازمانی یا کنترل‌های فنی رده‌بندی[۹] کرد.
کنترل‌های سازمانی می‌توانند شامل اعطای حق مناسب به افراد اداری، اصول عملیاتی مانند اصل چهار چشم[۱۰]، جداسازی وظایف، روال‌ها و خط‌مشی‌ها به منظور جلوگیری از انتخاب گذر واژه‌های پیش‌فرض[۱۱] یا ضعیف باشند. کنترل‌های عملیاتی می‌توانند شامل کنترل پیکربندی و نسخه کنترل برای نشان دادن پیکربندی‌های ناقص بالقوه یا رهگیری تغییرات در پیکربندی افزاره‌ها باشند.

1- Administration
2- Provisioning
3- Housekeeping: عملیاتی ازقبیل حفظ و نگهداری سوابق در سازمان یا رایانه است که کار را ساماندهی می‌کند و لی به طور مستقیم عملکرد را تشکیل نمی‌دهد
4- Operating system Image
5- Patch
6- Measures
7- Preventive
8- Corrective
9- Categorized
۱۰- این اصل الزام می‌کند که پیش از انجام هر کنشی حداقل دو نفر آن را تأیید کنند.
11- Default

کنترل‌های فنی شامل استفاده از واسطهای سرپرستی و ابزارهایی است که کیفیت مناسب احراز هویت، مجوزسنجی[1] و محرمانگی را فراهم می‌آورند. برای تعدادی از مؤلفه‌هایی که از طریق شبکه به هم مرتبط‌هستند مدیریت فنی لازم است. دروازه‌های امنیتی را می‌توان هم به صورت محلی و هم به صورت راه‌دور مدیریت کرد اما مدیریت راه‌دور بهتر است از ابزاری استفاده کند که احراز هویت قوی یا دو-عاملی[2] را تضمین کند یا لااقل به طور فنی از گذرواژه‌های پیش‌فرض و ضعیف بپرهیزد، این ابزارها همچنین باید یکپارچگی و محرمانگی متناسب[3]را فراهم کنند و هرجا که ممکن است از کارکردهای محرمانگی استفاده کنند. برای مثال، استفاده از تونل‌های VPN رمزگذاری‌شده[4] که با سطوح مناسبی از رمزنگاری[5] یا با استفاده از شبیه‌سازی[6] پایانه‌ی پوسته‌ی امن(SSH)[7] پیکربندی شده‌اند. کارسازها را نیز می‌توان هم به صورت محلی و هم راه‌دور مدیریت کرد. جایی‌که کارسازها از اطلاعات حساسی پشتیبانی می‌کنند، مدیریت راه‌دور باید دوباره از ابزاری استفاده کند که احرازهویت قوی یا دو-عاملی را تضمین کند یا حداقل به طور فنی از گذرواژه‌های پیش‌فرض و ضعیف پرهیزکند؛ این ابزارها همچنین باید یکپارچگی و محرمانگی متناسب را فراهم و هرجا ممکن است از کارکردهای محرمانگی استفاده کنند.

مؤلفه‌های زیرساخت مانند سوده‌ها و مسیریاب‌ها را می‌توان به صورت محلی از طریق درگاه پیشانه[8]، به صورت راه‌دور از ایستگاه مدیریت مرکزی مدیریت کرد. این مورد با استفاده از برنامه کاربردی تبدیل پایانه به منظور کار برخط[9] از یک رایانه راه‌دور یا از یک سامانه مدیریت توزیع‌شده صورت می‌پذیرد. با این وجود روشن شده است که این پروتکل‌ها امن نیستند مگر این‌که بتوانند با روشی پیکربندی شوند که اتصال را کاملا رمزگذاری کند. مثالی برای اتصال امن راه‌دور SSH است که می‌تواند کاملا رمزگذاری شود و شامل امکانات انتقال پرونده است.دسترسی بیشتر به مؤلفه‌های زیرساخت بهتر است از طریق یک کارساز احراز هویت کنترل شود.

شبکه‌هایی که به یک تأمین‌کننده برون‌سپاری[10] می‌شوند معمولا سامانه‌های مدیریتی خودشان را دارند. با این حال بهتر است از یک ایستگاه مدیریت مرکزی با استفاده از روش‌های مدیریت راه‌دور امن مدیریت شوند. روش-های مدیریت راه‌دور بهتر است شامل رمزگذاری و احراز هویت با استفاده از رمزنگاری کلید عمومی باشند. مثال-هایی از روش‌های امن که می‌توانند استفاده شوند،Telnet و TFTP از طریق تونل VPNیا SSH با کنترل توسط کارساز احرازهویت هستند.

1- Authorization
2- Factor
3- Adequate
4- Encrypted
5- Encryption
6- Emulation
7- Secure shell
8- Console port
9- Online
10- Outsourced

سازمان‌های بسیاری از دریچه‌های[1] مدیریتی پروتکل مدیریت شبکه ساده(SNMP)[2] برای پایش مستقیم چنین شبکه‌هایی استفاده می‌کنند. در نسخه‌های یک و دو SNMP که امنیتی ضعیف داشتند یا بدون امنیت هستند مخاطرات قابل توجهی وجود دارند. بنابراین اگر سازمانی تصمیم به استفاده از SNMP دارد بهتر است از نسخه‌ی ۳ به همراه کنترل‌های امنیتی کامل استفاده کند.

۸-۵ رویدادنگاری، پایش و رویارویی با پیشامدها

کارساز ممیزی بهتر است به همراه تمام سامانه‌های دروازه امنیتی که درون یک DMZ واقع شده‌اند پیکربندی شود. امنیت DMZ بهتر است نسبت به داخل و خارج شبکه تأمین شده باشد. همچنین پیکربندی هرگونه افزاره مرتبط با امنیت که درون یا بیرون DMZ واقع شده، بهتر است این‌گونه صورت پذیرد. توصیه نمی‌شود کارساز ممیزی بخشی از دامنه‌ی شبکه‌ی داخلی باشد و بهتر است دسترسی به آن فقط به صورت مستقیم و توسط مأمور[3] امنیتی منتصب[4] به سامانه‌دروازه/دیواری آتش امنیتی صورت گیرد. بنابراین برای بارگذاری[5] رویدادنگار ممیزی نیاز به دسترسی نوشتن است. این بارگذاری توسط یک پروتکل امن(برای مثال پروتکل رونوشت امن[6] (SCP)) از مؤلفه‌های زیرساخت، کارسازها و دیوارهای آتش صورت می‌پذیرد. تمام دیوارهای آتش و رویدادنگار ممیزی مربوط بهتر است برای بازدید بعدی به‌وسیله کارکنان امنیتی به سمت کارساز ممیزی هدایت شوند. این بازدید با کمک نرم‌افزار تحلیل ممیزی فراهم شده برای بازنگری پرونده‌های رویدادنگار ممیزی انجام می‌شود.

مدیریت اطلاعات امنیت شامل گردآوری و استانداردسازی اطلاعات گردآوری شده است؛ با این هدف که تصمیمات بر اساس آن اطلاعات گرفته‌شود. اطلاعات گردآوری شده ممکن است شامل رویدادنگاری‌های سامانه[7]، اطلاعاتSNMP، هشدارهای[8] IDS/IPS و جریان اطلاعات باشد.

هر جا که ممکن است، بهتر است کارساز ممیزی و/یا سامانه‌های IDS/IPS به گونه‌ای پیکربندی شوند که به مأمور امنیتی منتصب اخطار دهند. بر اساس اولویت سطح فعالیت غیرعادی تشخیص‌داده‌شده[9] این اخطار می‌تواند به صورت رایانامه[10]، پیامک[11] یا هردو باشد. بهتر است تمام فعالیت‌های غیرعادی آشکار شود چرا که ممکن است اقدامی برای حمله باشد. مأمور امنیتی مربوطه بهتر است بر اساس اولویت سطح اخطار، روال‌های رویارویی با پیشامدها را پیاده‌سازی کند. برای پوشش مدیریت پیشامد امنیت اطلاعات به استاندارد ملی ایران شماره ۲۷۰۳۵، سال:۱۳۹۲ مراجعه شود.

1- Traps
2- Simple Network Management Protocol
3- Officer
4- Assigned
5- Upload
6- Secure Copy Protocol
7- Syslogs
8- Alerts
9- Detected abnormal activity
10- Email
11- SMS

۸-۶ مستندسازی

سند معماری امنیت شبکه یکی از حیاتی‌ترین اسناد امنیتی فنی است و همانطور که پیش از این بیان شد این سند بهتر است با ارزیابی[۱] مخاطره امنیتی، نتایج بازنگری مدیریت مخاطره، شبکه‌بندی و خط‌مشی‌های امنیت اطلاعات سازمان/جامعه و دیگر خط‌مشی‌های مربوط سازگار باشد. این سند همانند هر سند حیاتی دیگر بهتر است برای تغییر، تحت کنترل باشد. یک الگوی[۲] مثال در پیوست ب بند ب-۱ آمده است. این سند بهتر است مرجعی را برای مستندسازی معماری فنی مربوط و دیگر مستندات امنیتی فنی فراهم کند. مستندات کلیدی مرتبط شامل موارد زیر هستند:

- مستندسازی الزامات امنیت اطلاعات برای تمام مؤلفه‌های شبکه‌ی مدیریت شده(مانند دروازه‌ها، دیوارهای-آتش، مسیریاب‌ها و غیره). این الزامات همچنین شامل الزامات امنیتی کارکردی[۳] مانند الزامات مبتنی بر قاعده‌ی[۴] دیواره آتش است. برای مثالی از الگو به بند ب-۲ پیوست ب مراجعه شود؛
- مستندسازی الزامات نرم‌افزار تحلیل رویدادنگار ممیزی؛
- گزارش‌های تحلیل محصول.

۸-۷ برنامه‌های آزمون و انجام آزمون

بهتر است سند راهبرد آزمون امنیتی توسعه داده شود تا رویکردی را که توسط آزمون باید صورت پذیرد تا معماری فنی امنیت شبکه‌بندی اثبات شود شرح دهد. توصیه می‌شود این سند بر روی اینکه چگونه کنترل‌های فنی امنیت کلیدی بهتر است مورد آزمون قرارگیرند، تمرکز کند تا اثبات شود که الزامات تعریف شده برآورده و خط‌مشی‌ها طبق طراحی پیاده‌سازی شده‌اند. توصیه می‌شود برای اثبات این دیدگاه‌ها، آزمون سامانه و وارسی‌های[۵] مبتنی بر بازبینه[۶] اجرا شود.

مستند راهبرد آزمون بهتر است حوزه‌هایی مانند زیر را در بر داشته باشد:

- سازوکارهای شناسایی و احراز هویت
- برگشت‌پذیری طراحی
- سازوکارهای مجوزسنجی
- پیاده‌سازی کنترل‌های خط‌مشی
- درستی‌سنجی[۷]سامانه‌های عامل مقاوم[۸]
- درستی‌سنجی راه‌حل رویدادنگار ممیزی

1- Assessment
2- Template
3- Functional
4- Rule base
5- Checks
6- Checklist
7- Verification
8- Hardened

راهبرد آزمون بهتر است شامل آزمون واحد[1] و کاربردپذیری نیز باشد تا از شایستگی طراحی، اطمینان حاصل شود.

توصیه می شود قبل از اجرای آزمون سامانه، طرح آزمونی آماده شود. طرح آزمون بهتر است شامل داده‌های آزمون همراه با فرانامه‌های آزمون برای مدرک[2] آن باشد. برنامه‌ی آزمون بهتر است شامل شرایط آزمون مناسب هم باشد. داده‌های آزمون بهتر است به دقت آماده شوند تا بتوانند کارکرد کنترل‌های فنی امنیت را آزمایش کنند[3].

۸-۸ نهایی‌سازی

توصیه می‌شود نهایی‌سازی پیاده‌کردن امنیت شبکه کامل شده، با سطوح مناسب مدیریتی نهایی‌سازی شود.

1- Unit
2- Evidence
3- Examine

پیوست الف

(اطلاعاتی)

ارجاعات مابین کنترل‌های مرتبط با امنیت شبکه استانداردهای ملی ایران به شماره‌های ۲۷۰۰۱، سال:۱۳۸۷ و ۲۷۰۰۲، سال:۱۳۸۷ و بندهای این استاندارد ملی ایران

بند استانداردهای ملی ایران ۲۷۰۰۱، سال: ۱۳۸۷ و ۲۷۰۰۲،سال ۱۳۸۷		بند این استاندارد ملی ایران
۱۰-۶-۱ کنترل‌های شبکه	شبکه‌ها بهتر است برای حفظ امنیت سامانه‌ها و برنامه‌های کاربردی شبکه که شامل گذر[1] اطلاعات می‌شود به‌طور متناسب مدیریت و کنترل شوند تا دربرابر تهدیدات درامان بمانند.	به موارد الف- تا ث- بند ۱۰-۶-۱ استاندارد ملی ایران شماره ۲۷۰۰۲/۲۷۰۰۱ مراجعه شود
۱۰-۶-۱ مورد الف	هرجا که مناسب بود بهتر است مسئولیت[2] عملیاتی[3] شبکه‌ها از عملیات رایانه‌ای جدا شود.	۸-۳ مدیریت شبکه
۱۰-۶-۱ مورد ت	برای فعال‌سازی ثبت[4]کنش‌های[5] مربوط به شبکه بهتر است رویدادنگاری و پایش مناسب اعمال گردد.	۸-۴ رویدادنگاری و پایش
۱۰-۶-۱ مورد ث	فعالیت‌های مدیریتی بهتر است هماهنگی[6] نزدیکی با دو زیر مورد داشته باشد. بهینه‌سازی[7] خدمت به سازمان و حصول اطمینان از اینکه کنترل‌ها پیوسته در سراسر زیرساخت پردازش[8] اطلاعات اعمال شده‌اند.	۸-۳ مدیریت شبکه
۱۰-۶-۲ امنیت خدمات شبکه	ویژگی‌های امنیت، سطوح خدمات و الزامات مدیریتی تمام خدمات شبکه بهتر است شناسایی و در تمام توافقات خدمات شبکه ذکر شوند. چه این خدمات در داخل فراهم شوند و چه برون-سپاری شوند.	۶-۳ گردآوری الزامات ۶-۴ بازنگری الزامات

1- Transit
2- Responsibility
3- Operational
4- Recording
5- Actions
6- Coordinate
7- Optimize
8- Processing

بند استانداردهای ملی ایران ۲۷۰۰۱، سال: ۱۳۸۷ و ۲۷۰۰۲،سال ۱۳۸۷		بند این استاندارد ملی ایران
۱۰-۸-۱ خط‌مشی‌ها و روال‌های تبادل اطلاعات	برای حفاظت از تبادل اطلاعات، بهتر است خط‌مشی‌ها، روال‌ها وکنترل‌های تبادل اطلاعات رسمی از طریق انواع امکانات ارتباطی در جای خود قرارگیرند	۸-۵ مستندسازی
۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه	کاربران بهتر است تنها به خدماتی دسترسی داشته باشند که به‌طور مشخص مجاز به استفاده از آن‌ها باشند.	۸-۳ مدیریت شبکه
۱۱-۴-۲ احراز هویت کاربر برای اتصالات بیرونی	بهتر است روش های احرازهویت مناسبی برای دسترسی کاربران راه دور استفاده شوند.	۸-۳ مدیریت شبکه

پیوست ب
(اطلاعاتی)
نمونه الگوهای مستندسازی

ب-۱ مثالی از الگوی سند معماری امنیت شبکه

ب-۱-۱ مقدمه

شامل بخش‌هایی مانند:

- هدف/منظور/ دامنه کاربرد[1]،
- هم فرضیات فنی و هم طور دیگر،
- وضعیت[2] سند،
- ساختار سند.

ب-۱-۲ الزامات مرتبط با کسب‌وکار

شامل بخش‌هایی مانند:

- مقدمه،
- متن،
- شبکه بندی و دیگر خدمات فناوری اطلاعات

ب-۱-۳ معماری فنی

شامل بخش‌هایی مانند:

- مقدمه،
- مرورکلی[3] فنی،
  - خلاصه،
  - دامنه اصلی ۱،
  - دامنه اصلی ۲،
  - دامنه اصلی ۳،
  - غیره،
  - کارسازها،
  - ایستگاه‌های کاری،

1- Scope
2- Status
3- Overview

  - رویدادنگاری،
  - مدیریت،
  - احراز هویت و کنترل دسترسی،
  - برگشت‌پذیری و پوشش[1] خدمت،
- محل‌های[2] سامانه،
- مؤلفه‌های سامانه،
- اتصالات متقابل[3]،
- مؤلفه ۱،
  - مرورکلی،
  - پیکربندی،
  - رویدادنگاری،
  - مدیریت،
- مؤلفه ۲،
  - مرورکلی،
  - پیکربندی،
  - رویدادنگاری،
  - مدیریت،
- مؤلفه ۳،
  - مرورکلی،
  - پیکربندی،
  - رویدادنگاری،
  - مدیریت،
- مؤلفه x و غیره،
- مدیریت کارساز،
  - مقدمه،
  - پایش خدمات،
  - سرپرستی سامانه گسترش‌یافته(XSA)[4]،
  - مدیر امنیت سازمان(ESM)[5]،

1- Coverage
2- Locations
3- Interconnection
4- Extended System Administration
5- Enterprise Security Manager

  - هر مدیر دیگر،
- دیوار آتش،
  - مقدمه،
  - مرورکلی،
  - پشتیبان پیکربندی دیوار آتش،
  - معیار طراحی و پیکربندی ،
  - مجموعه قواعد،
- مدیریت دیوار آتش،
  - پیکربندی،
  - هشدارهای دیوار آتش،
  - دسترسی راه‌دور،
- رویدادنگاری،
- سامانه پشتیبان،
  - مقدمه،
  - دیوارهای آتش،
  - کارسازها،
  - برنامه‌های کاربردی،
- ارتباطات شبکه،
  - شبکه‌های محلی مانند VLAN[1] و WLANها،
  - مسیریاب‌ها،
  - سوده‌ها،
  - آدرس‌دهی IP،
- مسئولیت‌های مدیریت،
  - کارسازها،
  - دیوارهای آتش،
  - زیرساخت‌ها،
  - مدیریت برنامه کاربردی.

ب-۱-۴ خدمات شبکه

شامل بخش‌هایی مانند:

1 -Virtual LAN

– مقدمه،
– خدمات در محل الف،
– خدمان در محل ب،

توصیه می‌شود فهرستی از تمام خدمات شبکه بر اساس مکان که شامل موارد زیر باشد وجود داشته باشد:

– خدمات KiloStream[۱]،
– خدمات MegaStream[۲]،
– خدمات رله قاب[۳]،
– خدمات ATM[۴]،
– خدمات MPLS/IP[۵]،
– خدمات پهن‌باند[۶]،
– خدمات WiFi/WiMax،
– خدمات اتصال LAN،
– خدمات GSM[۷]،
– نرخ اولیه ISDN[۸] (تا ۳۰ عدد کانال Kbps ۶۴ که توسط MegaStreamها تحویل می‌شوند)،
– واسط نرخ پایه (BRI)[۹] ISDN (کانال‌های Kbps ۶۴ × ۲)،
– خطوط تبادل مستقیم آنالوگ[۱۰] ([۱۱]DEL)،
– خدمات درون‌نت[۱۲]/برون‌نت،
– ISPها[۱۳]،

با ذکرتمام خطوط و خدمات.

اگر فهرست بزرگ است بهتر است در پیوست بیاید و از متن اصلی سند به آن ارجاع داده شود.

۱- خدمت اختصاصی مدار خصوصی دیجیتال است که انتقال داده یا انتقال صدا را ارائه می‌کند.

۲- خدمت MegaStream، مدار خصوصی سرعت بالای نقطه به نقطه و دائم متصلی را که مناسب برای هم صدا و هم داده‌های برنامه‌های کاربردی است، فراهم می کند.

3- Relay frame
4- Asynchronous Transfer Mode
5- Multiprotocol Label Switching
6- Broadband
7- Global System for Mobile
8- Integrated Services Digital Network
9- Basic Rate Interface
10- Analogue
11- Direct Exchange Line
12- Intranet
13- Internet service provider

ب-۱-۵ جانمایی[1] سخت‌افزاری/فیزیکی

شامل بخش‌هایی مانند:

- مقدمه،
- مکان

بهتر است فهرستی از تمام سخت‌افزارها با نقشه‌های طبقات و جانمایی اطاقک‌ها[2] براساس مکان تهیه شود. این فهرست بهتر است به‌طور مثال شامل کارسازها، دیوارهای آتش و دیگر تجهیزات ارتباطی باشد. همچنین تمام سخت‌افزارها باید برچسب[3] گذاری شوند.توصیه می‌شود برنامه برچسب‌گذاری به طور مستقیم ذکر یا به آن ارجاع داده شود.

جدول ب- ۱ مثالی از جدول فهرست سخت‌افزار را نشان می‌دهد. توصیه می‌شود برای هر نوع سخت‌افزار، جدولی تهیه شود. جدول مثال مربوط به مؤلفه‌های کارساز است.

جدول ب- ۱ نمونه جدول فهرست سخت‌افزار

مؤلفه کارساز	سخت‌افزار	نرم‌افزار	توضیحات
نام و تولیدکننده کارساز	شماره قطعه	نرم‌افزار و نسخه‌ی آن	توضیحات مشخصی چنان‌چه موردنیاز باشند, مانند درجه-بندی[4] عمودی یا خوشه‌بندی

ب-۱-۶ نرم‌افزار

شامل بخش‌هایی مانند:

- مقدمه،
- فهرستی از نرم‌افزار،
  - نرم‌افزار در مکان الف،
  - نرم‌افزار در مکان ب،
  - غیره.

1- Layout
2- Cabinet
3- Label

۴- در اینجا Scaled

فهرست نرم‌افزار شامل شماره نسخه آنها بهتر است حاوی موارد زیر باشد:

- نرم‌افزار Windows،
- دیوارهای‌آتش،
- RAS/RADIUS،
- نرم‌افزار مسیریاب،
- نرم‌افزار سوده،
- پیشکار،
- مدیریت ممیزی،
- کارسازهای نامه،
- رله نامه SMTP،
- مدیریت محتوی،
- نمایش‌دهی[1] Java/ActiveX،
- کارساز وب،
- کارساز پروتکل انتقال پرونده (FTP)[2]،
- کنترل‌کننده‌های دامنه،
- نرم‌افزار پشتیبان،
- دیگر نرم‌افزارها.

این فهرست بهتر است در پیوست بیاید که درمتن اصلی به آن ارجاع داده شود.

ب-۱-۷ عملکرد

جزئیات عملکرد مورد انتظار شامل جزئیات هر زیرسامانه بهتر است مانند زیر ذکر شوند:

- رایانه‌های رومیزی[3]،
- کارسازها،
- LAN،
- WAN،
- دروازه‌ها،
- خدمات خارجی.

1- Screening
2- File transfer protocol
3- Desktop

ب-۱-۸ مسائل شناخته شده

جزئیات مسائل شناخته‌شده شامل نواحی مورد نظر عدم-انطباق بهتر است تحت سرفصل‌هایی مانند فنی، فیزیکی و محیطی ذکر شوند که شامل بخشهایی مانند زیر هستند:

- مقدمه،
- نواحی عدم-انطباق.

ب-۱-۹ مراجع

بهتر است ارجاعات به تمام اسناد مرتبط ذکر شوند که شامل موارد زیر هستند:

- نتایج ارزیابی مخاطره و بازنگری مدیریت امنیت،
- خط‌مشی امنیت شبکه‌بندی،
- خط‌مشی امنیت اطلاعات،
- دیگر خط‌مشی‌های امنیتی مربوط،
- مستندسازی معماری فنی،
- مستندات الزامات (امنیتی) دسترسی خدمات برای هر سامانه‌ی دیوار آتش(که شامل مجموعه قواعد دیوار آتش هم هستند)،
- مستندسازی الزامات نرم‌افزار تحلیل رویدادنگار(ممیزی)،
- طرح‌واره مدیریت پیشامد امنیت اطلاعات،
- روال‌های بهره‌برداری امنیت (SecOP)[1]،
- شرایط اتصال امن برای طرف سوم،
- راهنمای کاربر برای کاربران طرف سوم.

ب-۱-۱۰ پیوست‌ها

شامل بخش‌هایی مانند زیر هستند:

- پیکربندی سخت‌افزار،
- پیکربندی کارساز/پیشانه،
- پیکربندی دیوار آتش،
- پیکربندی مسیریاب،
- پیکربندی نرم‌افزار،
- پیکربندی پایگاه داده،
- نقشه آدرس‌دهی IP،
- پیکربندی SNMP،

1- Security operating procedures

- رخنه‌های سامانه،
- رخنه‌های برنامه کاربردی،
- استانداردها.

ب-۱-۱۱ واژه‌نامه

ب-۲ مثالی از الگوی سند کارکرد الزامات امنیتی

یادآوری- بهتر است به ازای هر سامانه‌ی دیوار آتش سندی تهیه شود.

ب-۲-۱ مقدمه

شامل بخش‌هایی مانند زیر است:
- پس‌زمینه/دامنه کاربرد/ اهداف،
- نام سامانه دیوار آتش،
- محل دیوار آتش،
- نقش دیوار آتش،
- نام فرد/گروه مسئول عملیات دیوار آتش،
- سابقه‌ی تجدیدنظر محتویات سند،
- مراجع.

ب-۲-۲ پیکربندی دیوار آتش

شامل بخش‌هایی مانند زیر است:

- مقدمه،
- شناسایی پیوندهایی[1] که از طریق دیوار آتش برقرار می‌شوند،
- مرور کلی معماری دیوار آتش،
- جزئیات سامانه دیوار آتش:
  - سخت‌افزار،
  - نرم‌افزار،
  - معماری دیوار آتش،
  - خدمت دیوار آتش،
  - مدیریت دیوار آتش،

1- Links

- مسیریاب داخلی،
- مسیریاب خارجی،
- ناف[1] DMZ ،
- کارساز کد ضد-مخرب[2]،
- نامه‌ی SMTP،
- صفحات وب،
- کارساز نامه SMTP،
- کارساز رویدادنگاری(ممیزی)،
- منبع تغذیه وقفه‌ناپذیر(UPS)[3]،
- مؤلفه‌های دیگر،
- سایر کنترل‌های مورد نیاز،

- شرح پیوندها از دیگر سامانه‌ها و به دیگر سامانه‌ها،
- انواع اطلاعاتی که دربر می‌گیرد و حساسیت آنها،
- انواع کاربران و تعداد و غیره.

ب-۲-۴ مخاطرات امنیتی

در زمینه‌ی کاربرد دیوار آتش بخش‌های زیر را در برمی‌گیرند:

-مقدمه،

-اثرات[4] مغایرات[5] بالقوه‌ی کسب‌وکار(در بعضب مواقع با عنوان ارزش‌گذاری[6] دارایی‌ها شناخته‌می‌شود)،

-ارزیابی‌های تهدید،

-ارزیابی‌های آسیب‌پذیری[7]،

-ارزیابی‌های مخاطره،

ب-۲-۴ مدیریت امنیت

شامل بخش‌هایی در مورد مسئولیت به شرح زیر است:

- مأمور/ گروه امنیتی،
- افراد مسئول شبکه،

1- Hub
2- Anti-malicious code server
3- Uninterruptable power supply
4- Impact
5- Adverse
6- Valuation
7- Vulnerability

- پشتیبانان دیوار آتش،
- مدیریت شبکه،
- سایر مدیریت‌های فناوری اطلاعات،
- کاربران.

ب-۲-۵ سرپرستی امنیت

شامل بخش‌هایی مانند زیر است:

- SecOPها،
- بازنگری‌های انطباق امنیت،
- دسترس‌پذیری،
- نگهداری،
- کنترل پیکربندی،
- مدیریت ظرفیت[1]،
- مدیریت مشکل،
- مدیریت سطح خدمت،
- تاریخ انقضای سند.

ب-۲-۶ احراز هویت و کنترل دسترسی

شامل بخش‌هایی مانند زیر است:

- مقدمه،
- کنترل‌های دسترسی منطقی برای افرادی مانند سرپرستان دیوار آتش، کاربران داخلی و کاربران راه‌دور،
- سنجه‌های کنترل دسترسی خارجی برای مواردی مانند دسترسی شبکه به مجموعه قواعد دیوار آتش، سکوی[2] امن و کارسازهای پیشکار برنامه کاربردی،
- حفاظت سطح شبکه.

ب-۲-۷ رویدادنگاری(ممیزی)

شامل بخش‌هایی در مورد رویدادنگاری مانندزیر است:

- اطلاعاتی که باید ثبت شوند،
- تحلیلی که باید انجام شود و با چه ابزاری انجام شود،
- امنیت.

1- Capacity
2- Platform

ب-۲-۸ مدیریت پیشامد امنیت اطلاعات

شامل بخش‌هایی مانند بخشهای مرتبط با ثبت فعالیت‌ها است:

- مقدمه،
- گزارش پیشامد،
- ساماندهی[1] پیشامد،
- غیره.

ب-۲-۹ امنیت فیزیکی

شامل بخش‌هایی در مورد مسئولیت‌های دسترسی کنترل به شرح زیر است:

- سامانه دیوار آتش،
- بافه‌کشی[2](کابل‌کشی).

ب-۲-۱۰ امنیت افراد

شامل بخش‌هایی کاربردپذیر[3] در مورد افراد مرتبط با دیوار آتش است مانند:

- وارسی/آزمایش مربوط به استخدام،
- تعلیم و آگاهی امنیت.

ب-۲-۱۱ پیوست‌ها

شامل مواردی درباره جزئیات پروتکل‌ها و خدمات است:

- دسترسی‌های بیرونی به داخل و از داخل به بیرون،
- مدیریت راه‌دور،
- مدیریت دیوار آتش،
- مدیریت کارساز DMZ،
- هرگونه جزئیات مرتبط با سایر پروتکل‌ها وخدمات.

ب-۲-۱۲ واژه‌نامه

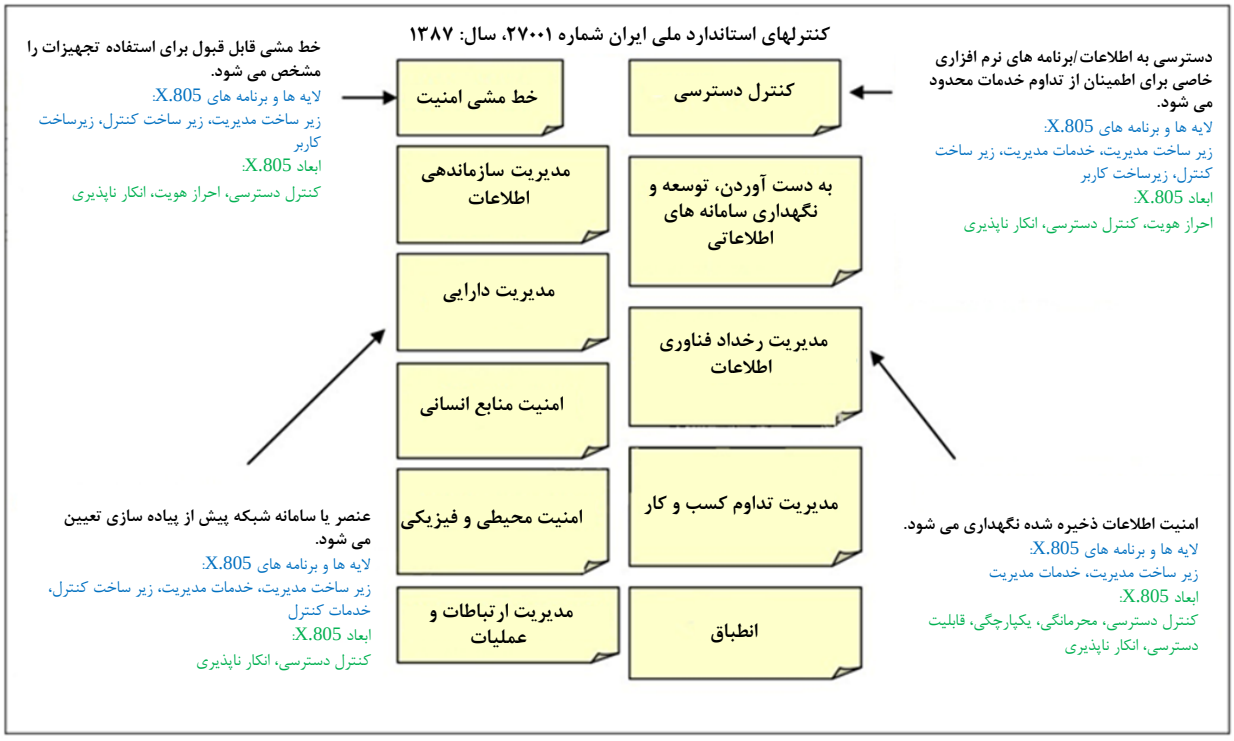
1- Handling
2- Cable
3- Applicable

پیوست پ

(اطلاعاتی)

چارچوب استاندارد ITU-T X.805 و نگاشت آن به کنترل‌های استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷

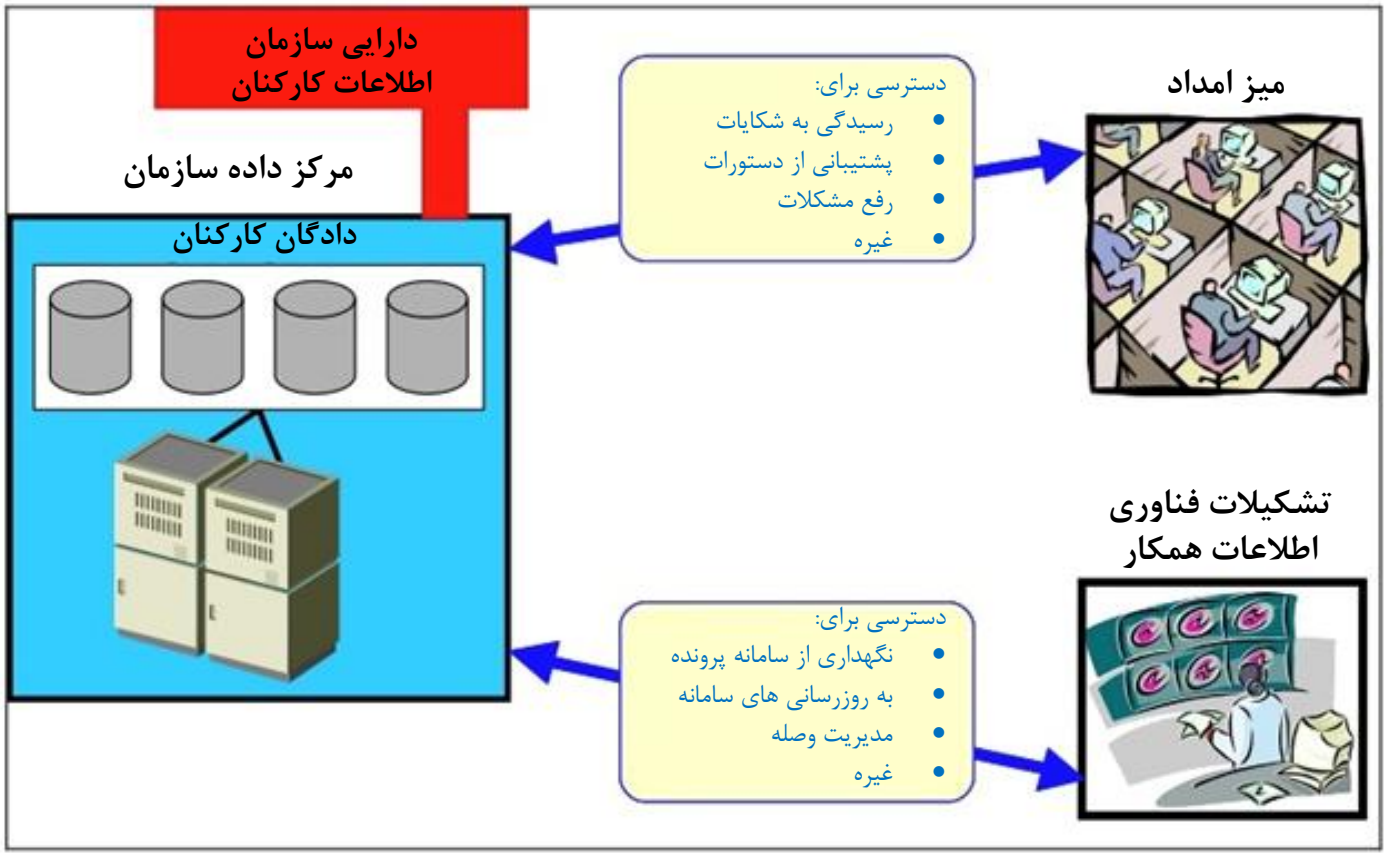
استاندارد ITU-T X.805 می‌تواند برای تقویت[1] بار فنی کنترل‌ها در استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷ استفاده شود. به طور خاص آنچنان که در شکل پ-۱ آمده است، استاندارد ITU-T X.805 می‌تواند چهار کنترل به استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷، اضافه‌کند. خط‌مشی امنیت، مدیریت دارایی، کنترل دسترسی و مدیریت پیشامد امنیت اطلاعات. لایه، برنامه‌ها و ابعاد مشخصی از استاندارد ITU-T X.805 که برای هر کدام از این کنترل‌ها کاربردپذیر[2] است در شکل به تصویر کشیده شده است. برای مثال برای مدیریت دارایی لایه‌های زیرساخت و خدمات و کنترل و سطوح مدیریت بیشترین کاربردپذیری را دارند و کنترل دسترسی و ابعاد قابلیت دسترسی برجسته‌ترین نگرانی‌های ما خواهندبود.



شکل پ-۱: تقویت استاندارد ITU-T X.805 برای کنترل‌های استانداردملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷

1- Augmentation
2- Applicable

به عنوان مثال تقویت می‌تواند برای ارزیابی و طراحی امنیت نظام‌مند مرکز داده‌ی سازمان‌ها مورد استفاده قرارگیرد. این مرکز داده، اطلاعات کارکنان سازمان و مخصوصا اطلاعات شخصی را ذخیره می‌کند و دسترسی به آن بهتر است محدود به کاربران مجاز باشد. سازمان‌های پشتیبانی که توسط خود سازمان به‌کار گرفته شده‌اند به اطلاعات کارکنان دسترسی دارند. یکی از آنها میز امداد[1] است. علاوه بر این، مرکز داده و سامانه‌های درون آن توسط تشکیلات فناوری اطلاعات همکار[2] نگهداری می‌شود. همان طور که در شکل پ-۲ دیده می‌شود، میز امداد به منظور رسیدگی به شکایات، پشتیبانی از سفارشات برای خدمات IT جدید، برای رفع مشکلاتی که کارکنان با خدمات IT دارند (مانند دسترسی راه‌دور) و غیره، به اطلاعات کارکنان دسترسی دارد. به علاوه تشکیلات فناوری اطلاعات همکار، به عنوان بخشی از فعالیت‌های نگهداری در خصوص نگهداری سامانه‌ی پرونده، به‌روز رسانی‌های سامانه، مدیریت وصله و غیره به اطلاعات کارکنان دسترسی دارد.

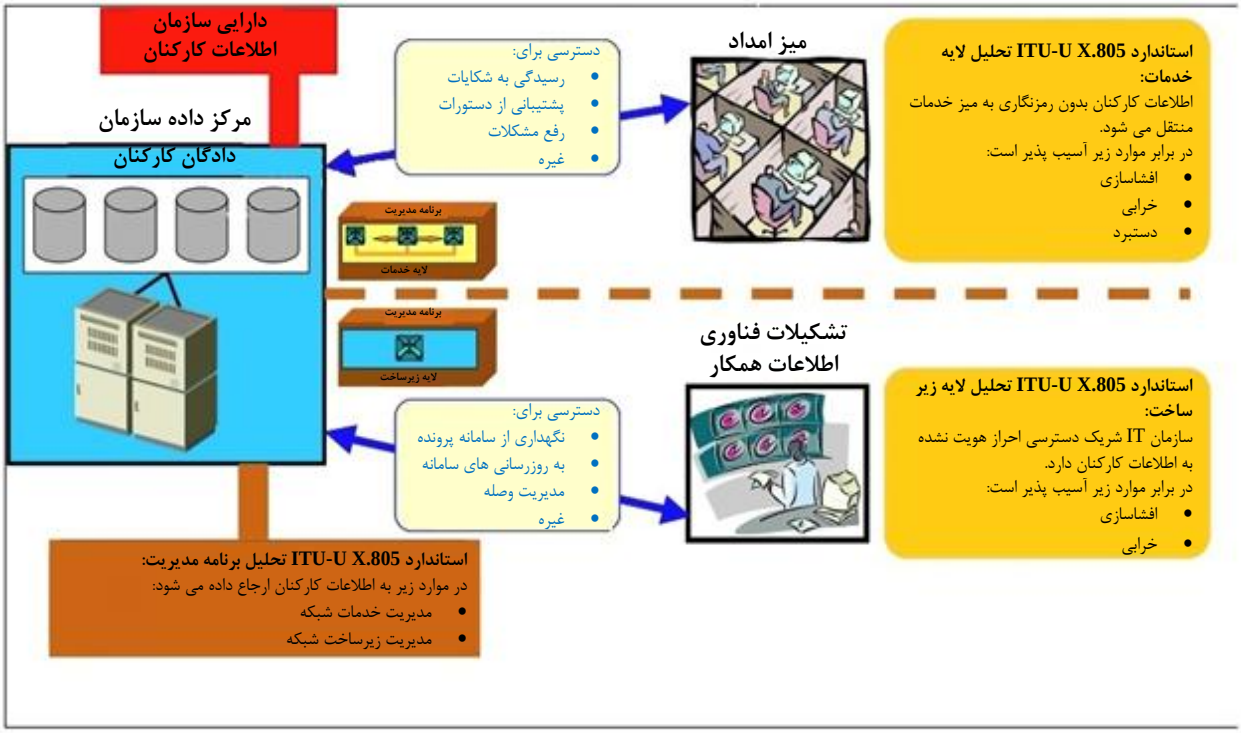


شکل پ-۲: فرانامه‌ی دسترسی برای دارایی سازمان

یک تحلیل تهدید/آسیب‌پذیری استاندارد ITU-T X.805 نشان می‌دهد که اعضای تشکیلات فناوری اطلاعات همکار قادر هستند اطلاعات کارکنان را ببینند و دستکاری کنند. از این رو باعث آسیب‌پذیری آن در مقابل افشا شدن و خرابی در لایه زیرساخت می‌شوند (به شکل پ- ۳مراجعه شود). به علاوه به عنوان بخشی از رفع مشکلات اجرایی، اطلاعات کارکنان بین مرکز داده و میز امداد، بدون رمزگذاری فرستاده می‌شوند. به همین

1- Help desk
2- Corporate IT organization

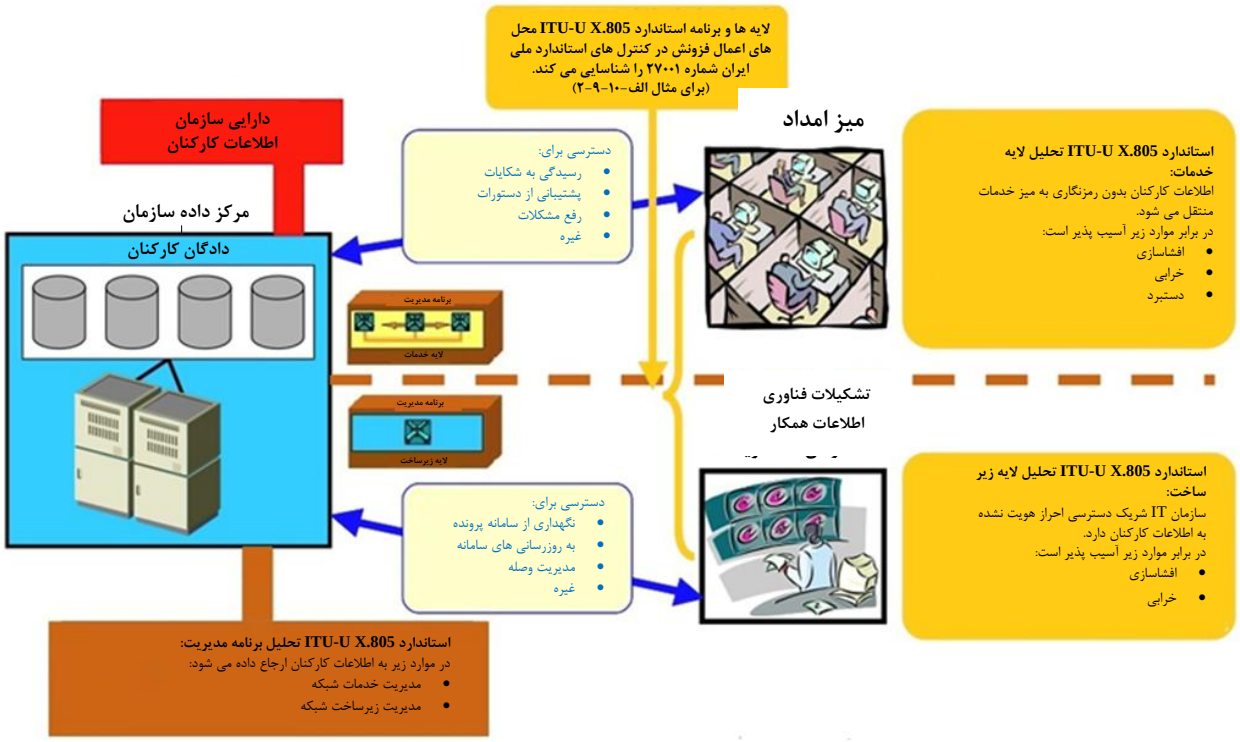
دلیل باعث آسیب‌پذیری آن در برابر افشا شدن، خرابی و شنود[1] می‌شوند. بنابراین برای حفاظت از اطلاعات کارکنان در مقابل تهدیدات و آسیب‌پذیری‌ها باید کنترل‌هایی در سطح مدیریت زیرساخت و لایه‌های خدمات آن شناسایی و انتخاب شوند. لازم به ذکر است که تحلیل گام به گام استاندارد ITU-T X.805 در این استاندارد ملی ذکر نشده است. فقط به اجمال، نتایج تحلیل ذکر شده در نظر گرفته شده‌اند.



شکل پ- ۳: نتایج تحلیل تهدید و آسیب‌پذیری استاندارد ITU-T X.805 برای دارایی سازمان

کنترل بند الف-۱۰-۹-۲ استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷به عنوان نیازی برای حفاظت از مدیریت اطلاعات کارکنان در لایه‌های خدمات و زیرساخت انتخاب شده است. این حفاظت در مقابل آسیب-پذیری‌ها و تهدیداتی است که توسط تحلیل‌های استاندارد ITU-T X.805 شناسایی شده‌اند(شکل پ- ۴). کنترل بند الف-۱۰-۹-۲ استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷ بیان می‌کند که اطلاعات درگیر در تراکنش‌های برخط باید حمایت شوند. این حمایت برای جلوگیری از انتقال ناتمام، مسیریابی نادرست، تغییر غیرمجاز پیام ، افشاسازی[2] غیرمجاز و تکثیر[3] و پاسخ به پیام غیرمجاز است.

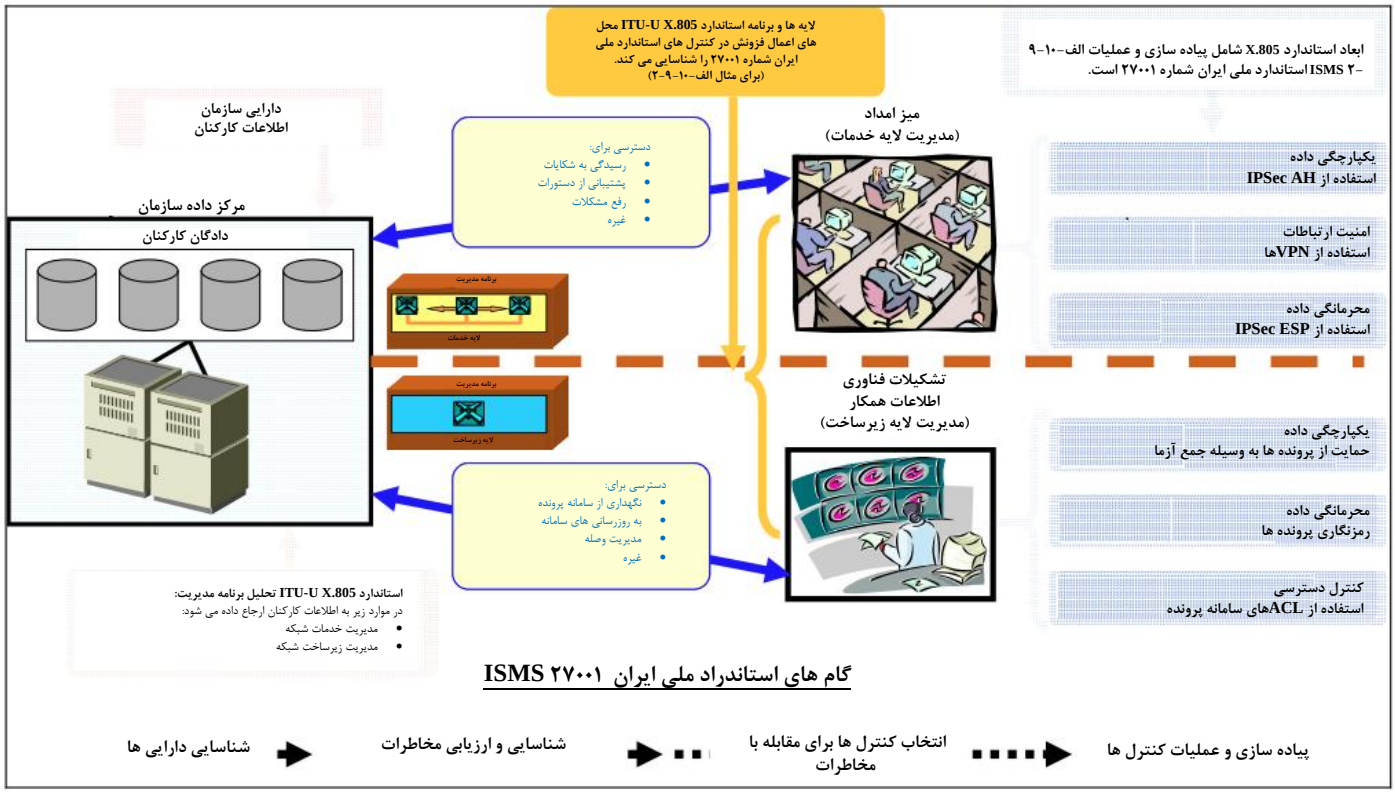
1- Interception
2- Disclosure
3- Duplication



شکل پ- ۴:کنترل‌های استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷

ابعاد استاندارد ITU-T X.805 جزئیات عملیات و پیاده‌سازی کنترل بند الف-۱۰-۹-۲ را فراهم می‌کند. این کنترل در لایه‌های زیرساخت و خدمات برای دارایی اطلاعاتی کارکنان است. در لایه خدمات، بعد امنیتی ارتباطات برای VPNها برای جلوگیری از مسیریابی نادرست فراهم شده است. بعد یکپارچگی داده، برای استفاده از IPSec AH[1] به منظور جلوگیری از انتقال ناتمام، تغییر، تکثیر و پاسخ به پیام غیرمجاز فراهم شده است. بعد محرمانگی داده، برای استفاده از IPSec ESP[2] به منظور جلوگیری از افشاسازی غیرمجاز فراهم شده است. در لایه زیرساخت، بعد یکپارچگی داده، برای استفاده از جمع‌آزماهای[3] پرونده به منظور جلوگیری از تغییر غیرمجاز فراهم شده است. بعد محرمانگی داده، برای رمزگذاری پرونده به منظور جلوگیری از افشاسازی غیرمجاز فراهم-شده‌است. بعد کنترل دسترسی برای استفاده از فهرست‌های کنترل دسترسی (ACL)[4] پرونده به منظور جلوگیری از نسخه برداری غیرمجاز فراهم شده‌است. در شکل پ- ۵ نشان می‌دهد که ابعاد استاندارد ITU-T X.805 برای پیاده‌سازی و عملیات بند الف-۱۰-۹-۲ به منظور حمایت از دارایی اطلاعاتی کارکنان فراهم شده-است.

1 - Internet Protocol Security Authentication Header
2 - Internet Protocol Security Encapsulating Security Payload
3- Checksums
4- Access control list



شکل پ- ۵: استاندارد ITU-T X.805 برای پیاده‌سازی استاندارد ملی ایران شماره ۲۷۰۰۱، سال: ۱۳۸۷

کتاب‌نامه

[1] ITU-T X.805, Security architecture for systems providing end-to-end communications
[2] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, IETF, August 2008