INSO

14866-1

1st. Edition
Feb.2013

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

استاندارد ملی ایران
۱-۱۴۸۶۶
چاپ اول
بهمن ۱۳۹۱

فناوری اطلاعات-فنون امنیتی- امنیت شبکه- قسمت ۱ : مرور کلی و مفاهیم

Information technology — Security techniques — Network security — Part 1: Overview and concepts

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 حوزه های 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 می شود .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 می شود .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)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] 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 بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها 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 می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. 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- قسمت ۱: مرور کلی و مفاهیم »

رئیس:	**سمت و/ یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق- مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (فوق لیسانس مهندسی کامپیوتر- نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضاء: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
عسگرزاده، مجید (فوق لیسانس مهندسی کامپیوتر)	مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات
طی‌نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

فیاضی، مهدی (لیسانس مهندسی الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات،)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
معروف، سینا (لیسانس مهندسی کامپیوتر سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استاندارد ها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

پیش‌گفتار

استاندارد « فناوری اطلاعات-فنون امنیتی- امنیت شبکه- قسمت ۱ : مرور کلی و مفاهیم » که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویست و بیست و دومین اجلاس کمیته‌ی ملی استاندارد رایانه و فراوری داده‌ها مورخ ۱۳۹۱/۹/۱۱مورد تصویب قرارگرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

این استاندارد ملی برمبنای استاندارد بین‌المللی زیر تدوین شده و معادل آن به زبان فارسی است:

1- ISO/IEC 27033-1:2009, Information technology - Security techniques Network Security- Part 1- Overview and concepts

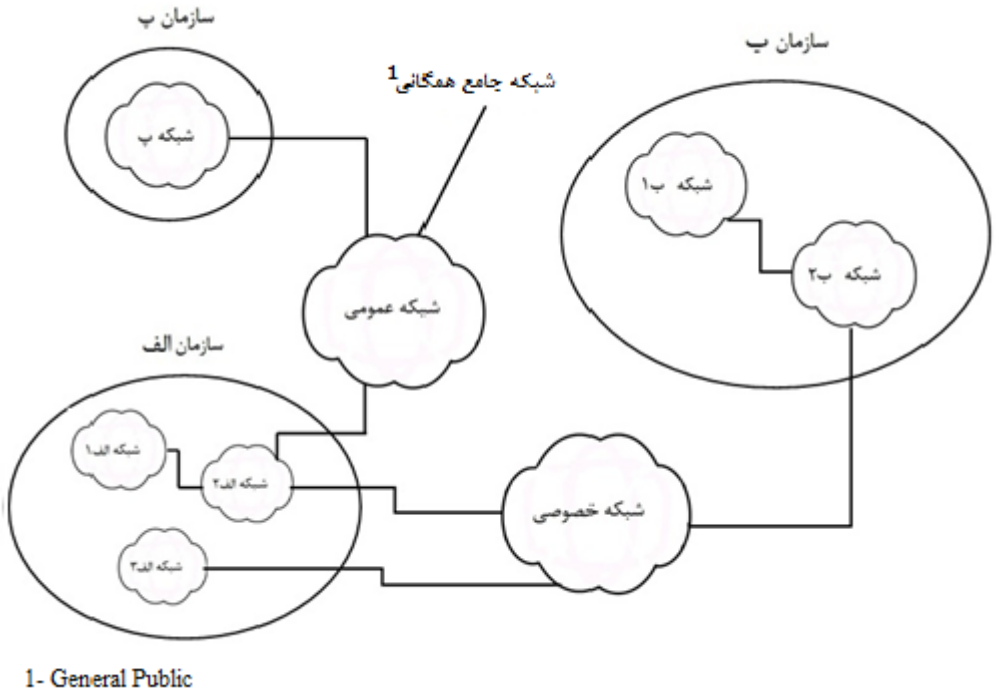
مقدمه

نظر به این‌که در دنیای امروز، سامانه‌های اطلاعاتی بیشتر سازمان‌های تجاری و دولتی توسط شبکه‌ها (مطابق شکل ۱)، وصل شده‌اند، اتصال شبکه‌ها یکی از حالت‌های زیر می‌باشد:

ـــ درون سازمان

ـــ بین سازمان‌های مختلف

ـــ بین سازمان و شبکه‌ی عمومی



شکل ۱ – انواع کلی اتصال شبکه‌ای

به‌علاوه با گسترش سریع فناوری شبکه‌ی عمومی در دسترس (به‌ویژه با اینترنت)، ارائه‌ی فرصت‌های کسب و کار مهم، سازمان‌ها را به‌طور فزاینده‌ای به سوی کسب و کار الکترونیکی بر روی یک مقیاس جهانی و ارائه‌ی خدمات برخط[1] عمومی سوق داده‌است. فرصت‌ها شامل فراهم‌کردن ارتباطات داده‌ی کم هزینه‌تر، استفاده از اینترنت، به‌عنوان رسانه‌ی ارتباط جهانی، ازطریق ارائه‌ی خدمات پیچیده‌تر توسط فراهم کنندگان خدمات اینترنت (ISP)[2] هستند. این می‌تواند به معنای استفاده از نقاط اتصال محلی به‌طور نسبی کم هزینه در هر دو انتهای مدار برای تجارت الکترونیکی برخط و سامانه‌های تحویل خدمت در مقیاس کامل، با استفاده از برنامه‌های کاربردی و خدمات تحت وب باشد. علاوه بر این فناوری جدید(شامل یکپارچگی داده، صدا و

1 - Online
2 - Internet Service Provider

تصویر) فرصت‌ها را برای کار از راه دور (که به عنوان «دورکاری» یا «ارتباط از دور» نیز شناخته‌می‌شود) که کارکنان را به ادامه‌ی فعالیت‌های مبتنی بر کار در خانه‌هایشان در دوره زمانی قابل‌توجهی قادر می‌سازد. آنها قادر به برقراری تماس با استفاده از امکانات راه دور برای دسترسی به سازمان و شبکه‌های عمومی و کسب و کار مرتبط که خدمات و اطلاعات را پشتیبانی می‌کنند، هستند.

به‌هرحال گرچه این محیط به سودآوری سازمان کمک قابل توجهی می‌کند، اما مخاطرات امنیت جدیدی هستند که باید مدیریت شوند. با تکیه‌ی شدید سازمان‌ها به استفاده از اطلاعات و شبکه‌های مرتبط برای پیشبرد کسب و کارشان، از دست دادن محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات و خدمات می‌تواند اثر مخرب شدیدی روی عملیات کسب و کار داشته باشد. بنابراین الزام اساسی برای محافظت درست شبکه‌ها و سامانه‌های اطلاعاتی و اطلاعات مرتبطشان وجود دارد. به‌عبارت دیگر: پیاده‌سازی و نگهداری مناسب امنیت شبکه، برای موفقیت در عملیات کسب و کار هر سازمانی کاملاً حیاتی است.

در این زمینه، صنایع فناوری اطلاعات و مخابرات، به دنبال راه‌حل امنیت جامع مقرون به صرفه‌ای با هدف محافظت از شبکه در برابر حملات مخرب و اقدامات نادرست غیرعمدی و برآوردن الزامات کسب و کار برای محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات و خدمات هستند. امن‌سازی شبکه هم‌چنین برای حفظ دقت در صدور صورتحساب یا استفاده‌ی مناسب از اطلاعات ضروری است. قابلیت‌های امنیتی در محصولات برای کل امنیت شبکه حیاتی هستند (شامل برنامه‌های کاربردی و خدمات). با این حال هم‌چنان‌که محصولات بیشتری برای ارائه‌ی راه‌حل‌های جامع با هم ترکیب می‌شوند، قابلیت همکاری با دیگر محصولات یا عدم آن، موفقیت راه‌حل را مشخص خواهدکرد. امنیت نه تنها باید موضوع نگرانی برای هر محصول یا خدمت باشد، بلکه باید به شیوه‌ای گسترش داده‌شود تا ترکیب قابلیت‌های امنیت را در راه‌حل کلان امنیت، ارتقا دهد.

هدف از از این استاندارد ملی، ارائه‌ی راهنمای دقیق جنبه‌های امنیتی مدیریت، اجرا و استفاده از شبکه‌های سامانه‌ی اطلاعات و اتصالات داخلی آنها است. افرادی داخل سازمان که مسؤولیت امنیت اطلاعات به‌طور کلی و امنیت شبکه به‌طور خاص را دارند، باید قادر به وفق‌دادن مواد داخل این استاندارد ملی، برای رفع الزامات خاص خود باشند. موضوعات اصلی آن در زیر هستند:

ـــ استاندارد ملی ISO/IEC 27033-1، *مرور و مفاهیم*، برای تعریف و توصیف مفاهیم مرتبط با امنیت شبکه و ارائه‌ی راهنمای مدیریت آن است. این قسمت شامل ارائه‌ی مروری کلی بر امنیت شبکه و تعاریف مرتبط، و راهنمایی برای چگونگی شناسایی و تحلیل مخاطرات امنیت شبکه و سپس تعریف الزامات امنیت شبکه است. این قسمت هم‌چنین چگونگی بدست آوردن معماری‌های فنی امنیتی باکیفیت و مخاطره، طراحی و جنبه‌های کنترلی مرتبط با سناریوهای شبکه نوعی و زمینه‌های «فناوری» شبکه را (که با جزییات قسمت‌های بعدی این استاندارد ملی، سروکار دارد) معرفی می‌کند.

ـــ استاندارد ISO/IEC 27033-2، *راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه*، برای تعریف اینکه چگونه سازمان‌ها باید معماری‌ها، طراحی‌ها و پیاده‌سازی‌های فنی امنیت شبکه، با کیفیت انجام دهند که از امنیت شبکه‌ی متناسب با محیط‌های کسب و کارشان، با استفاده از روشی منسجم برای برنامه‌ریزی، طراحی و پیاده‌سازی امنیت شبکه و مرتبط به کمک استفاده از مدل‌ها/ چارچوب‌ها (در این

متن، مدل/چارچوب برای ترسیم بازنمود یا توصیف نمایش ساختار و کارکردن سطح بالای نوعی از معماری/طراحی فنی امنیت استفاده شده‌است) و مرتبط با همه‌ی کارکنانی که در برنامه‌ریزی، طراحی و پیاده‌سازی معماری امنیت شبکه دخیل هستند، اطمینان حاصل کنند (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

ـــ استاندارد ISO/IEC 27033-3، *مخاطرات، فنون طراحی و مسایل کنترلی برای سناریوهای شبکه‌ی مرجع*، برای تعریف مخاطرات مشخص، فنون طراحی و مسایل کنترلی مرتبط با سناریوهای شبکه‌ی نوعی است. این قسمت دربرگیرنده‌ی همه‌ی کارکنان در برنامه‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیت شبکه می‌شود (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

پیشنهاد شده است که قسمت‌های بعدی خانواده استاندارد ISO/IEC 27033 موضوعات زیر را نشان دهند:

ـــ استاندارد ISO/IEC 27033-4، *مخاطرات، فنون طراحی و مسایل کنترلی برای امن‌کردن ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیت*، برای تعریف مخاطرات مشخص، فنون طراحی و مسایل کنترلی برای امن‌کردن اطلاعات در گردش بین شبکه‌ها با استفاده از دروازه‌های امنیت. این مربوط به همه‌ی کارکنانی می‌شود که در جریان جزییات طرح‌ریزی، طراحی و پیاده‌سازی دروازه‌های امنیت، هستند (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

ـــ استاندارد ISO/IEC 27033-5، *مخاطرات، فنون طراحی و مسایل کنترلی برای امن‌کردن شبکه‌های خصوصی مجازی (VPN)*[1]، برای تعریف مخاطرات مشخص، فنون طراحی و مسایل کنترلی برای امن‌کردن اتصالاتی که با استفاده از شبکه‌های خصوصی مجازی، برقرارشده‌اند. این مربوط به همه‌ی کارکنانی می‌شود که در جریان جزییات طرح‌ریزی، طراحی و پیاده‌سازی امنیت VPN، هستند (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

ـــ استاندارد ISO/IEC 27033-6، *همگرایی پروتکل اینترنتی*[2] ، برای تعریف مخاطرات مشخص، فنون طراحی و مسایل کنترلی برای امن‌کردن همگرایی IP شبکه‌ها، یعنی آنهایی که همگرایی داده، صدا و تصویر دارند. این مربوط به همه‌ی کارکنانی می‌شود که در جریان جزییات طرح‌ریزی، طراحی و پیاده‌سازی امنیت برای همگراییIP شبکه‌ها، هستند (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

ـــ استاندارد ISO/IEC 27033-7، *ارتباطات بی‌سیم*، برای تعریف مخاطرات مشخص، فنون طراحی و مسایل کنترلی برای امن‌کردن شبکه‌های بی‌سیم و رادیویی. این مربوط به همه‌ی کارکنانی می‌شود که در جریان جزییات طرح‌ریزی، طراحی و پیاده‌سازی امنیت برای شبکه‌های بی‌سیم و رادیو، هستند(برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

1 -Virtual Private Network(VPN)
2 -IP

تاکید شده‌است که این استاندارد ملی، جزییات بیشتر راهنمایی پیاده‌سازی کنترل‌های امنیت شبکه را فراهم کند که در سطح استانداردسازی شده‌ی پایه، در ISO/IECE 27002، توصیف شده‌اند.

اگر قسمت‌های دیگری در آینده وجود داشته باشند، مرتبط با همه‌ی کارکنانی می‌شود که در جریان جزییات برنامه‌ریزی، طراحی و پیاده‌سازی جنبه‌های شبکه که توسط آن قسمت‌ها پوشش داده میشود، هستند (برای مثال معماران و طراحان شبکه، مدیران شبکه و مسوولان امنیت شبکه).

باید توجه شود که این استاندارد ملی مرجع یا سند الزام‌آوری برای قوانین و مقررات الزامات امنیت نیست. اگرچه به اهمیت تاثیرات این استاندارد، تاکیدشده است، اما نمی‌توان آنها را به‌طور قطعی بیان کرد، چون وابسته به کشور، نوع کسب وکار و غیره هستند.

مگر در مواردی که بیان شود، در سراسر این قسمت از این استاندارد ملی، راهنمای اشاره شده برای شبکه‌های موجود و/یا طرح‌ریزی‌شده کاربردپذیر است، اما تنها به «شبکه‌ها» یا «شبکه» اشاره خواهدشد.

فناوری اطلاعات-فنون امنیتی- امنیت شبکه- قسمت ۱ : مرور و مفاهیم

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، مرور امنیت شبکه و تعاریف مرتبط با آن است. این استاندارد مفاهیم مرتبط با امنیت شبکه را تعریف و توصیف می‌کند و راهنمای مدیریتی برای امنیت شبکه فراهم می‌آورد.
(امنیت شبکه شامل امنیت دستگاه، امنیت فعالیت‌های مدیریت مربوط به دستگاه، برنامه‌های کاربردی/خدمات و کاربران نهایی به علاوه امنیت اطلاعاتی که بر روی پیوندهای ارتباطی در حال انتقال هستند.)

این قسمت مربوط به هرکسی می‌شود که مالک شبکه است، آن‌را نگهداری می‌کند یا از آن استفاده می‌کند. این امر شامل مدیران ارشد و دیگر مدیران غیرفنی و یا کاربران، علاوه بر مدیران و سرپرستانی که مسؤولیت مشخص امنیت اطلاعات و/یا امنیت شبکه را دارند می‌شود و به‌کارگیری کسانی که به‌طور کلی مسئول برنامه های امنیتی و توسعه‌ی خط‌مشی امنیتی یک سازمان هستند. هم‌چنین این استاندارد مرتبط با هر کسی است که درگیر برنامه‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیت شبکه می‌شود.

هم‌چنین، این مجموعه استاندارد ملی

راهنمایی در مورد نحوه شناسایی و تحلیل مخاطرات امنیتی شبکه و تعریف نیازمندی‌های امنیتی شبکه را بر اساس این تحلیل‌ها فراهم می‌کند.

ـــ یک مرور کلی از کنترل‌هایی که معماران فنی امنیت شبکه و کنترل‌های فنی وابسته به آن را پشتیبانی می‌کند و هم‌چنین آن کنترل‌های غیرفنی و فنی را که دقیقاً برای شبکه قابل اجرا نیستند، فراهم می‌کند.

ـــ چگونگی انجام خوب و با کیفیت معماری فنی امنیت شبکه، مخاطره، طراحی و جنبه‌های کنترلی مرتبط با سناریوهای شبکه نوعی و زمینه‌های « فناوری» شبکه را معرفی می‌کند(که با جزییات قسمت‌های بعدی خانواده استاندارد ISO/IEC 27033 سروکار دارد)، و

ـــ به‌طور خلاصه راجع به مسائل مرتبط با پیاده‌سازی و راه‌اندازی کنترل‌های امنیتی شبکه و پایش و بازبینی مداوم آن صحبت می‌کند.

به‌طور کلی این استاندارد نگرش کلی بر خانواده استاندارد ISO/IEC 27033 و «نقشه راه» برای تمام قسمت‌های دیگر این استاندارد فراهم می‌کند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها 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 نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ 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*

۲-۲ استاندارد ملی ایران به شماره ۲۷۰۰۰: سال *۱۳۹۱، فناوری اطلاعات- تکنیک های امنیتی- سامانه‌های مدیریت امنیت اطلاعات- قسمت بررسی و واژگان*

۲-۳ استاندارد ملی ایران به شماره ۲۷۰۰۱ : سال۱۳۸۷، *فناوری اطلاعات- تکنیک های امنیتی- سامانه‌های مدیریت امنیت اطلاعات- قسمت نیازها*

۲- ۴ استاندارد ملی ایران به شماره ۲۷۰۰۲ : سال ۱۳۸۷، *فناوری اطلاعات-تکنیک های امنیتی- نظام نامه شیوه مدیریت امنیت اطلاعات*

۲-۵ استاندارد ملی ایران به شماره ۲۷۰۰۵ : سال ۱۳۸۸، *فناوری اطلاعات- تکنیک های امنیتی- مدیریت مخاطره امنیت اطلاعات*

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود:

۳-۱
هشدار[1]

نشانه «فوری» که یک سامانه اطلاعات و شبکه ممکن است تحت حمله یا در خطر باشد که علت آن حادثه، خرابی یا خطای انسانی است.

۳-۲
معماری[2]

سازمان اساسی یک سامانه دربرگیرنده اجزای آن، ارتباط آنها با یکدیگر و با محیط و اصولی که راهنمای طراحی و تکمیل آن است.

1- Alert
2 - Architecture

۳-۳

حمله‌گر[1]

فردی که آگاهانه از آسیب‌پذیری‌های فنی و غیرفنی موجود در کنترل‌های امنیتی، به‌منظور سرقت یا به خطرانداختن سامانه‌های اطلاعات و شبکه یا به خطرانداختن دسترسی کاربران مجاز منابع سامانه‌های اطلاعات و شبکه بهره‌جویی می‌کند.

۴-۳

ثبت ممیزی[2]

عمل ضبط داده‌ها در مورد رویدادهای امنیت اطلاعات به منظور بازنگری و تحلیل و پایش مداوم آن‌هاست.

۵-۳

ابزار ممیزی[3]

ابزار خودکار برای کمک به تحلیل محتویات وقایع ممیزی هستند.

۶-۳

مرجع صدور گواهی(CA)[4]

مرجع مورد اعتماد یک یا چند کاربر برای ایجاد و نسبت دادن گواهی‌های کلید عمومی است.

یادآوری۱- در صورت تمایل، مرجع صدور گواهی می‌تواند کلید کاربران را ایجاد کند.

یادآوری۲- نقش مرجع صدور گواهی در این فرآیند، تضمین‌کننده‌ی این است که فرد مجاز، دارای گواهی‌نامه‌ی منحصر به‌فردی است، در واقع، کسی که ادعا می‌کند، هست. به طور معمول به‌این معناست که CA با نهادی که برای آن اطلاعاتی برای تایید هویت ادعا شده‌ی فرد، فراهم می‌کند، قرارداد دارد. مراجع صدور گواهی اجزای حیاتی در امنیت اطلاعات و تجارت الکترونیک هستند، زیرا آنها ضمانت می‌کنند که دو طرفی که اطلاعات را تبادل می نمایند، همان‌هایی هستند که ادعا می‌کنند.

1 - Attacker
2 - Audit logging
3 - Audit tools
4 - Certification authority

۷-۳

خط‌مشی امنیت اطلاعات شرکتی[1]

سندی که جهت‌گیری مدیریت و پشتیبانی از امنیت اطلاعات را مطابق با الزامات کسب و کار و قوانین و مقررات مربوطه توصیف می‌کند.

یادآوری- این سند سطح بالایی از نیازمندی‌های امنیت اطلاعات را توصیف می‌کند که باید درکل سازمان دنبال شود.

۸-۳

منطقه‌ی بی‌طرف(DMZ)[2]

محیط شبکه‌ای(به عنوان زیرشبکه‌ی در معرض نمایش هم شناخته می‌شود) که به عنوان یک «منطقه بی‌طرف» قرارداده شده‌است.

۹-۳

انکار خدمت(DOS)[3]

جلوگیری از دسترسی مجاز به منابع سامانه و یا به تاخیر انداختن عملیات سامانه و کارکرد آن در نتیجه‌ی نبود دسترس‌پذیری برای کاربران مجاز است.

۱۰-۳

برون‌نت[4]

گسترش درون‌نت‌های[5] سازمانی به‌ویژه بر روی زیرساخت‌های شبکه‌ی عمومی، به اشتراک‌گذاری منابع را بین سازمان و سازمان‌های دیگر و افراد قادر می‌سازد تا دسترسی محدودی به درون‌نت خود فراهم کنند.

یادآوری- برای مثال برای مشتریان یک سازمان که می‌توانند دسترسی به قسمتی از درون‌نت سازمان داشته‌باشند،یک برون‌نت فراهم می‌آورند، اما این مشتریان از دید امنیتی«مورد اعتماد»تلقی نمی‌شوند.

۱۱-۳

پالایش[6]

فرآیند پذیرش یا ردّ جریان داده‌ی از طریق شبکه مطابق با معیارهای مشخص است.

---

1 - Corporate information security policy
2 - Demilitarized zone
3 - Denial of Service
4 - Extranet
5 - Intranet
6 - Filter

۱۲-۳

دیواره‌ی آتش[1]

نوعی مانع امنیتی که در محیط بین شبکه‌ای قرارداده می‌شود- متشکل از یک افزاره‌ی خاص و یاترکیبی از چندین جزء و فن - که از طریق آن همه ترافیک از محیط یک شبکه به شبکه دیگر و بالعکس عبور می‌کند و تنها ترافیک مجاز که در خط‌مشی امنیتی محلی تعریف شده است، اجازه گذر دارد.

۱۳-۳

ناف[2]

افزاره شبکه‌ای که در لایه‌ی ۱ از مدل مرجع سامانه‌های اتصال متقابل باز (OSI)[3] کار می‌کند.

یادآوری- در نافهای شبکه، هوشمندی به معنای واقعی وجود ندارد و آنها تنها نقطه اتصال فیزیکی برای سامانه‌های شبکه‌شده و منابع هستند.

۱۴-۳

اینترنت جهانی[4]

سامانه جهانی که از شبکه‌های متصل به‌هم در محدوده‌ی عمومی تشکیل شده‌است.

۱۵-۳

اینترنت[5]

مجموعه‌ای از شبکه‌های متصل به‌هم هستند که بین شبکه‌ای یا به اختصار اینترنت نامیده می‌شوند.

۱۶-۳

درون‌نت

شبکه کامپیوتری خصوصی که از قراردادهای اینترنت و اتصالات شبکه برای اشتراک امن بخشی از اطلاعات سازمان یا تعامل با کارکنانش استفاده می‌کند.

1 - Firewall
2 - Hub
3 - Open Systems Interconnection
4 - The Internet
5 - Internet

۱۷-۳

نفوذ[1]

دسترسی غیرمجاز به شبکه یا سامانه‌ی متصل به شبکه، یعنی دسترسی غیرمجاز آگاهانه یا ناآگاهانه به یک سامانه اطلاعات که فعالیت‌های مخرب ضد یک سامانه‌ی اطلاعات یا استفاده غیرمجاز از منابع داخل یک سامانه اطلاعات را در برمی‌گیرد.

۱۸-۳

تشخیص نفوذ[2]

فرآیند رسمی تشخیص نفوذها که معمولاً با جمع‌آوری دانش درباره استفاده غیرعادی الگوها ، به‌علاوه اینکه چه آسیب‌پذیری، چگونه و کجا مورد بهره‌جویی قرار گرفته است و چگونه و کجا واقع شده است، توصیف می‌شود.

۱۹-۳

سامانه‌ی تشخیص نفوذ (IDS)[3]

سامانه‌ی فنی برای شناسایی یک نفوذ تلاش شده، یا در حال رخ دادن یا رخ داده و شاید هم پاسخ به نفوذ، که در سامانه‌های اطلاعاتی و شبکه‌ها استفاده می‌شود.

۲۰-۳

پیشگیری از نفوذ[4]

فرآیند رسمی پاسخگویی فعال برای جلوگیری از نفوذها است.

۲۱-۳

سامانه پیشگیری از نفوذ (IPS)[5]

نوعی از سامانه‌های تشخیص نفوذ که به‌طورخاص طراحی شده‌اند تا قابلیت پاسخگویی فعال را فراهم کنند.

1 - Intrusion
2 - Intrusion Detection
3 - Intrusion Detection System
4 - Intrusion Prevention
5 - Intrusion Prevention System

۲۲-۳

بدافزار[1]

نرم‌افزارهای مخربی که به‌طور خاص برای تخریب یا اختلال در یک سامانه، حمله به محرمانگی، یکپارچگی و/یا دسترس‌پذیری طراحی شده‌اند.

یادآوری- ویروس‌ها و تروجان‌ها[2] مثالهایی از یک بدافزار هستند.

۲۳-۳

سودهی برچسب چندپروتکلی(MPLS)[3]

فنی که برای استفاده در مسیریابی بین‌شبکه‌ای توسعه داده‌شده است و بوسیله‌ی آن برچسب‌ها به مسیرهای داده یا جریان داده‌ها با استفاده از اتصالات سوده[4] در زیر به‌علاوه سازوکار قرارداد مسیریابی عادی اختصاص داده‌شده‌اند.

یادآوری- سوییچینگ[5] برچسب می‌تواند به عنوان روشی برای ایجاد تونل‌ها مورد استفاده قرار گیرد.

۲۴-۳

سرپرستی شبکه[6]

عملکرد و مدیریت روز به روز فرآیندهای شبکه و دارایی‌های استفاده‌کننده از شبکه‌ها است.

۲۵-۳

تحلیل‌گر شبکه[7]

افزاره یا نرم‌افزاری که برای نظارت و تحلیل اطلاعات جاری در شبکه‌ها مورد استفاده قرار می‌گیرد.

یادآوری- قبل از تحلیل جریان اطلاعات، باید با روش خاصی مانند استفاده از یک اسنیفر شبکه[8]، اطلاعات گردآوری شوند.

۲۶-۳

عنصر[9] **شبکه**

سامانه اطلاعاتی که به یک شبکه متصل شده‌است.

---

1 - Malware
2 -Trojans
3 - Multi Protocol Label Switching
4 - Switch
5 - Switching
6 - Network Administration
7 - Network Analyzer
8 - Network Sniffer
9 - Element

۲۷-۳
مدیریت شبکه
فرآیند برنامه‌ریزی، طراحی، پیاده‌سازی، عملکرد، پایش و نگهداری شبکه است.

۲۸-۳
پایش[1] شبکه
فرآیند نظارت پیوسته و بازنگری داده‌های ضبط شده از فعالیت‌ها و عملکردهای شبکه که شامل ثبت ممیزی‌ها و هشدارها و تحلیل‌های مرتبط می‌شود.

۲۹-۳
خط‌مشی امنیت[2] شبکه
مجموعه‌ای از احکام، قواعد و تجربیاتی که رویکرد یک سازمان را در استفاده از منابع شبکه‌ای آن توضیح می‌دهد و مشخص می‌کند که چگونه زیرساخت‌های شبکه‌ای و خدمات آن باید محافظت شوند.

۳۰-۳
اسنیفر شبکه
افزاره یا نرم‌افزاری که برای گرفتن[3] جریان اطلاعات در شبکه استفاده می‌شود.

۳۱-۳
درگاه[4]
نقطه‌ی پایانی[5] یک اتصال است.

یادآوری- در مفهوم پروتکل اینترنت، یک درگاه یک نقطه پایانی کانال منطقی از یک اتصال پروتکل کنترل انتقال(TCP)[6]یا پروتکل داده‌گرام کاربر(UDP)[7] است. به پروتکلهای برنامه‌های کاربردی که بر اساس TCP یا UDP هستند، به‌طور عموم شماره‌های درگاه پیش‌فرضی اختصاص داده‌شده‌است، به‌طور مثال شماره درگاه ۸۰ برای پروتکل انتقال ابرمتن(HTTP)[8]

1 - Monitoring
2 - Security Policy
3 - Capture
4 - Port
5 - Endpoint
6 - Transfer Control Protocol
7 - User Datagram Protocol
8 - Hypertext Transfer Protocol

۳۲-۳

دسترسی از راه دور[1]

فرآیند دسترسی به منابع شبکه از شبکه‌ی دیگر یا از یک افزاره‌ی پایانه‌ای که دایمی متصل نشده‌است و به‌طور فیزیکی یا منطقی به شبکه دسترسی دارد.

۳۳-۳

کاربر راه دور[2]

کاربری که در یک پایگاه به غیر از پایگاهی که در آن، منابع شبکه مورد استفاده قرار گرفته‌اند، واقع شده‌است.

۳۴-۳

مسیریاب[3]

افزاره شبکه‌ای که با انتخاب مسیرها و یا مسیریابی بر اساس سازوکار[4] و الگوریتم‌های پروتکل مسیریابی، برای برقراری و کنترل جریان داده بین شبکه‌های متفاوت استفاده می‌شود.

یادآوری۱- شبکه‌ها خود می‌توانند براساس پروتکل‌های متفاوت باشند.

یادآوری۲- اطلاعات مسیریابی در جدول مسیریابی نگهداری می‌شوند.

۳۵-۳

دامنه‌ی امنیت[5]

مجموعه‌ای از دارایی‌ها و منابعی که تحت یک خط‌مشی امنیتی مشترک هستند.

۳۶-۳

دروازه امنیتی[6]

نقطه‌ی اتصال بین شبکه‌ها یا بین زیرگروه‌های داخل شبکه‌ها یا بین نرم‌افزارهای کاربردی داخل دامنه‌های امنیتی متفاوت که برای محافظت یک شبکه بنابر خط‌مشی امنیتی داده‌شده، در نظر گرفته شده‌است.

---

1 - Remote Access
2 - Remote User
3 - Router
4 - Mechanism
5 - Security Domain
6 - Security Gateway

۳-۳۷
هرزنامه[1]

نامه‌های الکترونیکی ناخواسته که می‌توانند حامل محتویات مخرب و/یا پیام‌های فریب‌کارانه باشند.

۳-۳۸
کلاهبرداری[2]

جعل هویت یک منبع قانونی یا یک کاربر است.

۳-۳۹
سوییچ

افزاره‌ای که اتصال بین دستگاه‌های شبکه را با مفهوم سازوکارهای سودهی داخلی فراهم می‌آورد. فناوری سودهی عموماً در لایه‌ی ۲ یا لایه‌ی ۳ مدل OSI پیاده‌سازی می‌شود.

یادآوری- سوده‌ها از سایر افزاره‌های اتصال درونی شبکه‌های محلی (به‌طور مثال یک ناف) متفاوت هستند چنان‌که فناوری مورد استفاده در سوده‌ها، اتصالات پایه‌ای نقطه به نقطه را برقرار می‌کنند.

۳-۴۰
تونل[3]

مسیر داده بین افزاره‌های شبکه که از طریق زیرساخت شبکه‌ی موجود ایجاد می‌شود.

یادآوری- تونل‌ها می‌توانند با استفاده از فنونی مانند کپسوله‌سازی[4] سودهی برچسب یا مدارهای مجازی برقرارشوند.

۳-۴۱
شبکه محلی مجازی(VLAN)[5]

شبکه‌ی مستقلی از نقطه نظر منطقی که داخل یک شبکه‌ی فیزیکی ایجاد شده‌است.

۴ کوته‌نوشت‌ها

یادآوری- کوته‌نوشت‌های زیر در تمام قسمت‌های خانواده استاندارد ISO/IEC 27033 استفاده می‌شوند.

1 - Spam
2 - Spoofing
3 - Tunnel
4 - Encapsulation
5 - Virtual Local Area Network

AAA	authentication, authorization and accounting	احرازهویت، مجوزسنجی، پاسخگویی
ACL	access control list	سیاههی کنترل دسترسی
ADSL	asymmetric digital subscriber line	خط رقمی مشترک نامتقارن
AES	advanced encryption standard	استاندارد رمزگذاری پیشرفته
ATM	asynchronous transfer mode	حالت انتقال ناهمگام
BPL	broadband power line	خطوط نیروی پهنباند
CA	certification authority	مرجع گواهی
CDPD	cellular digital packet data	بسته دادهی رقمی سلولی
CDMA	code division multiple access	دسترسی چندتایی تقسیم کد
CLID	calling line identifier	شناساگر خط تماس
CLNP	connectionless network protocol	پروتکل شبکهی بدون اتصال
CoS	class of service	ردهی خدمت
CRM	customer relationship management	مدیریت ارتباط با مشتری
DEL	direct exchange line	خط تبادل مستقیم
DES	data encryption standard	استاندارد رمزگذاری داده
DMZ	demilitarized zone	منطقهی بیطرف
DNS	domain name service	خدمت نام دامنه
DPNSS	digital private network signaling system	سامانهی سیگنالدهی شبکهی خصوصی رقمی
DoS	denial of service	انکار خدمت
DSL	digital subscriber line	خط مشترک رقمی
EDGE	enhanced data-rates for GSM evolution	نرخ دادهی ارتقایافته برای تکامل GSM
EDI	electronic data interchange	تبادل دادهی الکترونیکی
EGPRS	enhanced general packet radio service	خدمت رادیویی بسته عمومی ارتقایافته
EIS	enterprise information system	سامانهی اطلاعات بنگاهی
FiOS	fiber optic service	خدمت فیبرنوری
FTP	file transfer protocol	پروتکل انتقال پرونده
FTTH	fiber to the home	فیبر مشترک
GPRS	general packet radio service	خدمت بسته عمومی رادیویی
GSM	global system for mobile communications	سامانهی سراسری برای ارتباطات موبایل
HIDS	host based intrusion detection system	سامانهی تشخیص نفوذ مبتنی بر میزبان
HTTP	hypertext transfer protocol	پروتکل انتقال ابرمتن
IDS	intrusion detection system	سامانهی تشخیص نفوذ
IG	Implementation Guidance	راهنمای پیادهسازی
IP	Internet protocol	پروتکل اینترنت
IPS	intrusion prevention system	سامانهی پیشگیری از نفوذ
ISP	Internet service provider	فراهمکنندهی خدمت اینترنت
IT	information technology	فناوری اطلاعات

LAN	local area network	شبکه‌ی محلی
MPLS	multi-protocol label switching	برچسب سودهی چند پروتکلی
MRP	manufacturing resource planning	طرح‌ریزی منابع ساخت
NAT	network address translation	ترجمه‌ی آدرس شبکه
NIDS	network intrusion detection system	سامانه‌ی تشخیص نفوذ شبکه
NTP	network time protocol	پروتکل زمان شبکه
OOB	out of band	خارج از باند
PABX	private automated branch (telephone) exchange	تبادل شاخه‌ی خودکار خصوصی
PC	personal computer	رایانه‌ی شخصی
PDA	personal data assistant	کمک داده‌ای شخصی
PIN	personal identification number	شماره شناسایی شخصی
PKI	public key infrastructure	زیرساخت کلید عمومی
PSTN	public switched telephone network	شبکه‌ی عمومی تلفن
QoS	quality of service	کیفیت خدمت
RAID	redundant array of inexpensive disks	آرایه‌ی افزونه‌ای از دیسک‌های ارزان
RAS	remote access service	خدمت دسترسی از راه دور
RTP	real time protocol	پروتکل به‌هنگام
SDSL	symmetric digital subscriber line	خط رقمی مشترک متقارن
SecOPs	security operating procedures	روال‌های بهره‌برداری امنیت
SIM	subscriber identity module	پودمان شناسایی مشترک
SNMP	simple network management protocol	پروتکل مدیریت ساده‌ی شبکه
SPIT	spam over IP telephony	هرزنامه بر روی تلفن اینترنتی
SSH	secure shell	پوسته‌ی امن
TCP	transmission control protocol	پروتکل کنترل انتقال
TDMA	time division multiple access	دسترسی چندگانه‌ی مبتنی برتقسیم زمانی
TETRA	terrestrial trunked radio	رادیوی طیف مشترک زمینی
TKIP	temporal key integrity protocol	پروتکل یکپارچگی کلید زمانی
UDP	user datagram protocol	پروتکل داده‌گرام کاربر
UMTS	universal mobile telecommunications system	سامانه‌ی ارتباط راه دور موبایل عمومی
UPS	uninterruptible power supply	منبع تغذیه‌ی وقفه‌ناپذیر
USB	universal serial bus	گذرگاه سریال جهانی
VHF	very high frequency	فرکانس خیلی بالا
VoIP	voice over IP	صدا روی اینترنت
VLAN	virtual local area network	شبکه محلی مجازی
VPN	virtual private network	شبکه خصوصی مجازی
WAN	wide area network	شبکه گسترده
WAP	wireless application protocol	پروتکل برنامه‌کاربردی بی‌سیم
WEP	wired equivalent privacy	حریم هم‌ارز سیمی

WLAN	wireless local area network	شبکه محلی بی‌سیم
WORM	write once read many	یکبار نوشتنی چندبار خواندنی
WPA	Wi-Fi protected access	دسترسی محافظت شده‌ی Wi-Fi
3G	third generation mobile telephone system	سامانه‌ی تلفن همراه نسل سوم

۵ ساختار

ساختار خانواده استاندارد ISO/IEC 27033 به صورت دیاگرامی یا «نقشه راه» در شکل ۲ زیر نشان داده شده است.

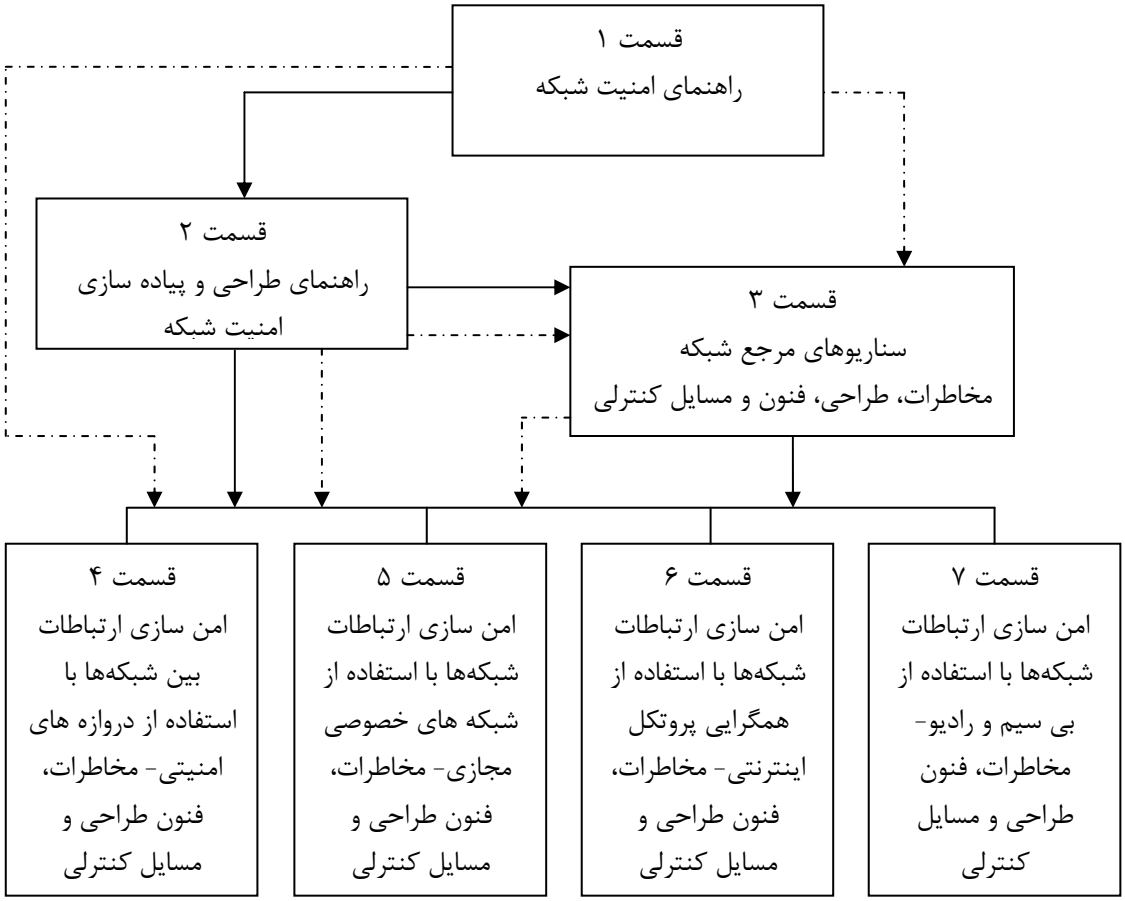
باید توجه داشت که در شکل ۲، خطوط ممتد، شکل سلسله مراتبی معمولی قسمت های خانواده استاندارد ISO/IEC 27033 را نشان می‌دهند. خطوط نقطه چین نشان می‌دهند که در دنباله فرایندهای شرح داده شده در (الف) قسمت ۱– قسمت‌های ۶،۵،۴،۳ و ۷ ممکن است در خصوص اطلاعات در مورد مخاطرات امنیتی مورد استفاده قرارگیرند و (ب) قسمت ۲، قسمت های ۶،۵،۴،۳ و۷ ممکن است برای اطلاعات در خصوص فنون طراحی و مسایل کنترلی استفاده شوند. علاوه براین، در قسمت ۳ اشاره هایی به جنبه های ویژه‌ی پوشش داده شده در قسمت های ۶،۵،۴ و۷ برای پیشگیری از دوباره کاری داده‌شده‌است (یعنی در استفاده از قسمت ۳، ممکن است نیاز به کمک گرفتن از قسمتهای ۶،۵،۴ و۷ باشد).

بنابراین برای هر سازمان، با شروع از ابتدا یا انجام بازنگری کلی بر شبکه(ها)ی موجود، بهتراست اول محتویات قسمت۱و سپس قسمت ۲ استفاده شوند، اما کمک گرفتن برای اطلاعاتی در مورد مخاطرات امنیتی، فنون طراحی و مسایل کنترلی هم که در قسمت های ۳ تا ۷ واقع شده اند، ضروری و مناسب است.

برای مثال، سازمانی که در نظر دارد محیط شبکه‌ی جدیدی را پیاده‌سازی کند که شامل استفاده از همگرایی آدرس‌های IP، دروازه‌های امنیتی و برخی استفاده‌های بی‌سیمی به علاوه‌ی استفاده از میزبانی وب و اینترنت باشد (به طور مثال، برای نامه الکترونیکی و دسترسی خارجی برخط).

در استفاده از فرآیندهای توصیف شده در قسمت ۱، برای تعیین مخاطرات امنیتی شبکه جدید، سازمان باید از اطلاعات مرتبط با مخاطره‌ی سایر قسمت‌های مربوط از خانواده استاندارد ISO/IEC 27033 کمک بگیرد، یعنی آن قسمت هایی که مخاطرات امنیتی مشخصی (به علاوه فنون طراحی و مسایل کنترلی) مربوط به همگرایی آدرس‌های IP، دروازه‌های امنیتی و برخی استفاده‌های بی‌سیمی را به علاوه‌ی استفاده از میزبانی وب و اینترنت (به طور مثال، برای نامه الکترونیکی و دسترسی خارجی برخط) تعریف می‌کند.

در استفاده از قسمت ۲ برای تعیین معماری فنی امنیت شبکه‌ی موردنیاز، سازمان باید از اطلاعات فنون طراحی و مسایل کنترلی از دیگر قسمت های خانواده استاندارد ISO/IEC 27033 کمک بگیرد، یعنی آنهایی که فنون طراحی و مسایل کنترلی مشخصی (به علاوه ی مخاطرات امنیتی) مربوط به همگرایی آدرس‌های IP، دروازه‌های امنیتی و برخی استفاده‌های بی‌سیمی را به علاوه‌ی استفاده از میزبانی وب و اینترنت (به طور مثال، برای نامه الکترونیکی و دسترسی خارجی برخط) تعریف می‌کند.



شکل ۲ – «نقشه راه » خانواده استاندارد **۲۷۰۳۳**

در آینده ممکن است قسمت‌های دیگری برای خانواده استاندارد ISO/IEC 27033 بوجود بیاید. مثال‌هایی از موضوعات احتمالی که با قسمت‌های آینده باید پوشش داده شوند، شامل شبکه‌های محلی، شبکه‌های گسترده، شبکه‌های پهن‌باند، میزبانی وب، نامه الکترونیکی اینترنتی، و دسترسی مسیریابی‌شده به سازمان‌های طرف‌سوم هستند.

بندهای اصلی تمام این قسمت‌ها باید دربرگرفته شوند، اما محدود به سه اسم مخاطرات تخصیص، فنون طراحی و مسایل کنترلی نیستند.

ساختار این استاندارد ملی موارد زیر را در بر می‌گیرد:

- مرور کلی بر رویکرد امنیت شبکه (مطابق با بند ۶)
- خلاصه‌ای از فرآیندهایی برای شناسایی مخاطرات مرتبط با شبکه و آماده‌سازی شناسایی کنترل‌های امنیتی، یعنی برقراری الزامات امنیت شبکه (مطابق با بند ۷)
- مرور کلی کنترل‌هایی که معماری فنی امنیت شبکه و کنترل‌های فنی مرتبط را پشتیبانی می‌کند، یعنی کنترل‌های دیگر(غیرفنی و فنی) که تنها برای شبکه کاربردی نیستند(مطابق با بند ۸). مراجعی برای محتوای مربوط به ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 فراهم‌شده‌اند.
- مقدمه‌ای برای دست‌یابی به معماری‌های کیفی فنی امنیت که این اطمینان را ایجاد می‌کند که امنیت شبکه‌ی متناسب با محیط کسب وکار سازمان را با استفاده از رویکردی منسجم برای برنامه‌ریزی و

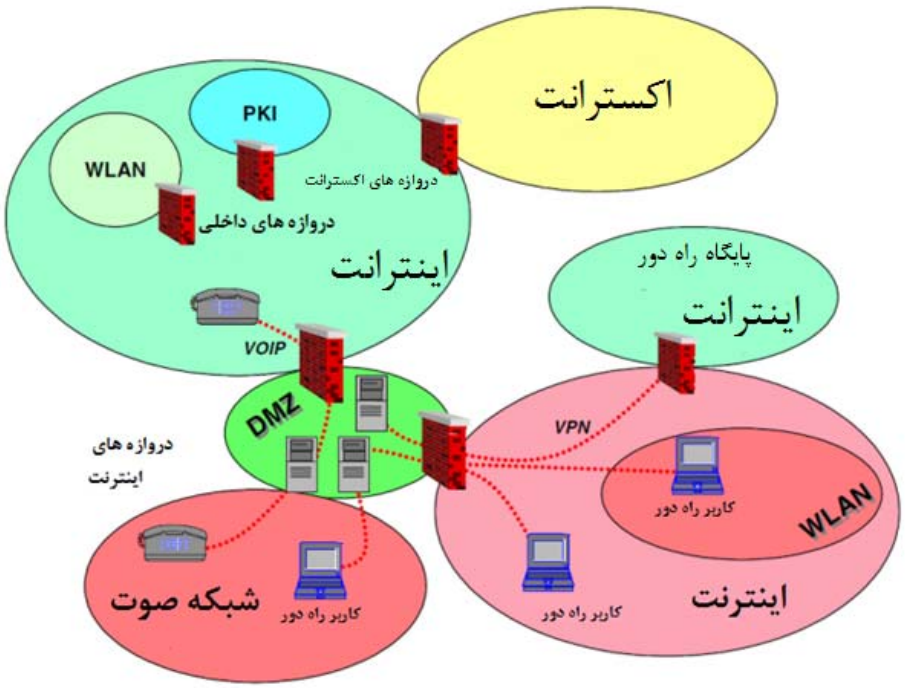
طراحی امنیت شبکه، به کمک استفاده از مدل‌ها/چارچوب‌ها فراهم شده‌است. (یعنی مقدمه‌ای بر محتویات ISO/IEC 27033-2) (مطابق با بند ۹)

- مقدمه‌ای بر مخاطرات مشخص، طراحی، فنون و مسایل کنترلی وابسته به سناریوهای مرجع شبکه(یعنی مقدمه‌ای بر محتویات ISO/IEC 27033-3) (مطابق با بند ۱۰)
- مقدمه‌ای بر مخاطرات مشخص، فنون طراحی و مسایل کنترلی برای موضوعات «فناوری» شبکه،(یعنی مقدمه‌ای بر محتویات ISO/IEC 27033-4، ISO/IEC 27033-5، ISO/IEC 27033-6، ISO/IEC 27033-7و قسمت‌های احتمالی آینده) (مطابق با بند ۱۱و پیوست الف)
- خلاصه‌ای از مسایل مرتبط با توسعه، پیاده‌سازی و آزمایش راه‌حل امنیت شبکه(مطابق با بند۱۲)، بهره برداری از راه حل امنیت شبکه(مطابق با بند ۱۳)، و پایش مداوم و بازنگری پیاده‌سازی امنیت شبکه (مطابق با بند۱۴)، و
- جدولی که ارجاع متقابل بین ISO/IEC 27001/27002 کنترلهای مربوط به امنیت شبکه و ISO/IEC 27033-4 و بندهای این استانداردهای ملی قید شده در پیوست ب را نشان می‌دهد.

۶ مرور کلی

۶-۱ پس‌زمینه

مثالی از یک محیط شبکه که امروزه می‌توان در بسیاری از سازمان‌ها دید، در شکل ۳ زیر نشان‌داده شده‌است. (هدف از شکل ۳ در این مرور کلی تنها توضیح دادن است وهدف دیگری مورد نظر نیست)



شکل ۳ – نمونه محیط شبکه

درون‌نت، شبکه‌ی داخلی سازمان را تعریف می‌کند که به آن اعتماد دارد و آن‌را به صورت داخلی نگهداری می‌کند. معمولاً تنها افرادی که برای سازمان کار می‌کنند، دسترسی مستقیم فیزیکی به این شبکه دارند و از آن جایی که شبکه در مکان داخلی متعلق به سازمان واقع شده است، سطح حفاظت فیزیکی آن به راحتی می‌تواند پیاده‌سازی‌شود. در بیشتر موارد، درون‌نت با فن‌آوری‌های استفاده‌شده و الزامات امنیتی، همساز[1] نیست؛از سوی دیگر زیرساخت‌هایی می‌توانند وجود داشته‌باشند که نیاز به سطح بالاتری از محافظتی دارند که توسط خود درون‌نت فراهم‌شده است. چنین زیرساخت‌هایی، به طور مثال، قسمت‌های ضروری محیط PKI[2] می‌توانند در قطعه‌ی[3] خاصی از درون‌نت، عملیاتی شوند. از سویی دیگر، فناوری‌های خاصی(به طور مثال زیرساختهای شبکه محلی بی سیم) به خاطر مخاطرات اضافی که ایجاد می‌کنند، نیازمند جداسازی و احرازهویت هستند. برای هر دو مورد، دروازه‌های امنیتی داخلی، می‌توانند برای پیاده‌سازی این قطعه‌بندی[4] به‌کاررروند.

امروزه نیاز کسب وکار بیشتر سازمان‌ها، ارتباطات ضروری و تبادل داده با شرکای خارجی و سایر سازمان‌هاست. مهم ترین شرکای کسب وکار، اغلب به به طوری مستقیم به هم متصل هستند که درون‌نت را به شبکه‌ی سازمان شریک بسط می‌دهند، اصطلاح اکسترانت معمولاً برای چنین روشی استفاده می‌شود. چون اعتماد به سازمان شریک متصل شده، در بیشتر موارد کمتر از خود سازمان هست،دروازه‌های امنیتی برون‌نت، مخاطرات ایجاد شده توسط این اتصالات را پوشش می‌دهند.

شبکه‌های عمومی که اینترنت عمومی‌ترین نمونه‌ی آن است، امروزه بیشتر برای بهینه‌سازی هزینه‌های ارتباط و تسهیل تبادل داده‌ها با شرکای تجاری، مشتریان و عموم استفاده می‌شوند و شکل‌های متفاوتی از گسترش درون‌نت ارائه می‌دهند. به علت سطح پایین امنیت در شبکه های عمومی، به خصوص اینترنت، دروازه‌های امنیتی حرفه‌ای برای کمک به مدیریت مخاطرات مربوط، نیاز است. این دروازه‌های امنیتی دربرگیرنده‌ی اجزای خاصی برای نشان دادن الزامات شکل‌های متفاوت بسط درون‌نت و اتصالات شرکای تجاری و مشتریان هستند.

کاربران راه دور می‌توانند از طریق فناوری شبکه‌های خصوصی مجازی متصل شده‌باشند و ممکن است از اتصالات بی‌سیم و امکاناتی شبیه نقاط دسترسی عمومی شبکه‌های محلی بی‌سیم برای دسترسی به اینترنت، استفاده کنند. به‌طور متناوب کاربران راه دور می‌توانند از شبکه تلفن برای برقراری اتصالات شماره‌گیری به یک خدمت‌گزار[5] دسترسی از راه دور که اغلب در محیط منطقه‌ی بی‌طرف[6] از دیواره‌ی آتش اینترنت واقع شده‌است، استفاده کنند.

1 - Homogenous
2 - Public Key Infrastructure
3 - Segment
4 - Segmentation
5 - Server
6 - DMZ

وقتی سازمانی تصمیم به استفاده از فناوری‌های صدا بر روی IP[1] برای پیاده‌سازی شبکه‌ی داخلی تلفن می‌گیرد، دروازه‌های امنیتی مناسب، برای شبکه تلفن معمولاً خوب عمل می‌کنند.
فرصت‌های کسب وکار فراهم شده توسط محیط‌های شبکه‌ای جدید باید در برابر مخاطرات ناشی از فناوری‌های جدید، متوازن شوند. به‌طور مثال اینترنت ویژگی‌های فنی متعددی دارد که از نقطه‌نظر امنیتی باعث نگرانی می‌شود، چون از ابتدا به عنوان اولویت، بر اصل انعطاف‌پذیری و نه امنیت طراحی شده‌بود و بسیاری از پروتکل‌های اساسی در استفاده‌های رایج، به‌طور ذاتی امن نیستند. افراد زیادی در دنیا هستند که ظرفیت، دانش و تمایل دسترسی به سازوکارهای اساسی، پروتکل‌ها وخلق رخدادهای امنیتی، از دسترسی‌های غیرمجاز گرفته تا انکار خدمت به‌طور کامل مخرب را دارند.

۲-۶ برنامه‌ریزی و مدیریت امنیت شبکه

با در نظرگرفتن تمام اتصالات شبکه، همه‌ی افرادی که در سازمان، مسؤولیتی در قبال اتصالات دارند،باید در مورد الزامات کسب وکار ومنافع آن، مخاطرات امنیتی مرتبط و جنبه‌های فنی معماری امنیت مربوط/فنون طراحی و زمینه‌های کنترل امنیت،توجیه شده باشند. الزامات کسب وکار و منافع آن، بسیاری از تصمیمات و اقدامات صورت‌گرفته در فرآیند در نظر گرفتن اتصالات شبکه، شناسایی جنبه‌های فنی معماری امنیت/فنون طراحی و زمینه‌های کنترل امنیتی بالقوه، و در نهایت انتخاب طراحی،پیاده‌سازی و نگهداری شبکه‌های امن را تحت تاثیر قرار خواهند داد.
فرآیند کلی دستیابی و نگهداری امنیت مورد نیاز شبکه به شرح زیر خلاصه شده‌است:
الف- تعیین دامنه/زمینه و سپس ارزیابی مخاطرات امنیتی
۱- جمع‌آوری اطلاعات شبکه‌ی در حال کار و/یا طراحی شده
الف- بازنگری خط‌مشی امنیت اطلاعات شرکتی برای بیانیه‌هایی در مورد مخاطرات مرتبط با شبکه که همیشه به عنوان درجه بالا لحاظ می‌شوند و برای کنترل‌های امنیتی شبکه که در رابطه با مخاطرات ارزیابی شده، نیاز به پیاده‌سازی خواهند داشت.

یادآوری- این خط‌مشی هم‌چنین بهتر است جایگاه سازمان را در(۱) الزامات نظارتی و قانونی مرتبط با اتصالات شبکه آن‌طور که توسط نهادهای نظارتی و قانونی مربوط تعریف شده است (شامل دستگاه‌های دولتی ملی)، و (۲) حساسیت داده‌هایی که باید در شبکه ذخیره شوند یا انتقال یابند، دربرگیرد.

ب- جمع‌آوری و بازنگری اطلاعات در شبکه(ها)ی موجود و/یا طرح‌ریزی‌شده– معماری(ها)، برنامه‌های کاربردی، خدمات، انواع اتصالات و سایر مشخصه‌ها– این امر برای شناسایی و ارزیابی مخاطرات و تعیین کردن آنچه که در شرایط معماری/طراحی فنی امنیت شبکه، امکان‌پذیر است، نقطه اتکایی خواهد بود.

1 - VoIP

ج- جمع‌آوری سایر اطلاعات تا بتوان اثرات نامطلوب بالقوه‌ی کسب و کار، تهدیدها و آسیب‌پذیری‌ها را ارزیابی کرد. (این شامل ارزش‌دهی به عملیات کسب و کار اطلاعات که با اتصالات شبکه منتقل‌شده‌باشند، خواهدشد، هرگونه اطلاعات که بالقوه قابل دسترسی از روشی غیرمجاز از طریق این اتصالات، و خدمات فراهم شده) باشند.

۲- شناسایی و ارزیابی مخاطرات امنیت شبکه و حوزه‌های کنترل بالقوه‌ی مناسب

الف- انجام ارزیابی مخاطرات امنیت شبکه و بازنگری مدیریت با استفاده از اطلاعات مخاطره مربوطه به سناریوها و موضوعات فناوری موردنیاز شبکه (مطابق با بند ۱۰و۱۱) -تعریف الزامات امنیت. (توجه داشته باشید که این شامل (۱) ارزیابی مخاطرات وابسته به خلاءهای بالقوه مربوط به نظارت و قانونگذاری در ارتباط با اتصالات شبکه، هم‌چنان‌که توسط نهادهای نظارتی و قانونی مربوط تعریف شده است (شامل دستگاه‌های دولتی ملی)، و (۲) استفاده از اثرات بالقوه مضر کسب و کار، تایید حساسیت/طبقه‌بندی داده‌هایی که باید در شبکه ذخیره شوند یا انتقال یابند)،

ب- شناسایی کنترل‌های امنیتی پشتیبانی- غیرفنی و فنی که تنها بر روی شبکه اعمال نمی‌شوند(مطابق با بند ۸)،

ج- بازنگری گزینه‌های معماری/طراحی فنی امنیت ، با در نظر گرفتن سناریوها و موضوعات «فناوری» و گزینش و مستندسازی معماری/طراحی فنی امنیت و کنترل‌های امنیت مربوط(مطابق با بند ۹و۱۱ و پیوست A)[توجه داشته‌باشید که این امر شامل کنترل‌های مورد نیاز برای مطابقت با مقررات و قوانین مربوط با اتصالات شبکه، آن‌چنان‌که توسط نهادهای نظارتی و قانونی مربوط تعریف شده است، خواهد بود. (شامل دستگاه‌های دولتی ملی)]

د) توسعه و آزمون راه‌حل امنیتی(مطابق با بند ۱۲)،

ه) پیاده‌سازی و اجرای کنترل‌های امنیتی (مطابق با بند ۱۳)،

و)پایش و بازنگری پیاده‌سازی(مطابق با بند ۱۴). توجه داشته‌باشید که این شامل پایش و بازنگری کنترل‌های مورد نیاز برای مطابقت با مقررات و قوانین مربوط با اتصالات شبکه، هم‌چنان‌که توسط نهادهای نظارتی و قانونی مربوط تعریف شده است، خواهد بود. (شامل دستگاه‌های دولتی ملی) :

۱- بازنگری‌ها باید به‌صورت دوره‌ای انجام‌شوند و در مورد تغییرات بزرگ (در نیازمندی‌های کسب و کار، فناوری، راه‌حل‌های امنیتی و غیره) و به عنوان ضرورت، نتایج مراحل پیشین که خلاصه آنها در بالا تهیه شد، بهتر است بازبینی و به‌هنگام شده باشند.

مرور کلی برنامه‌ریزی امنیت شبکه و مدیریت فرآیندها به صورت دیاگرام در شکل زیر نشان داده شده است.

شکل ۴ – برنامه‌ریزی امنیت شبکه و مدیریت فرآیندها

یادآوری- مطابق با ISO/IEC 27001، ISO/IEC 27002، ISO/IEC 27003، ISO/IEC 27004 و ISO/IEC 27005

این تاکید شده‌است که سرتاسر این فرآیند مرجع باید برای ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 به‌طور مناسب پیاده‌سازی‌شود تا راهنمای عمومی برای شناسایی کنترل‌های امنیت را دربرگیرد. . این استاندارد ملی مکمل این استانداردها است و مقدمه‌ای بر چگونگی شناسایی کنترل‌های مناسب امنیت شبکه و پس از آن برای ISO/IEC 27033-2 تا ISO/IEC 27033-7 فراهم می‌کند.

۷ شناسایی مخاطرات و آماده‌سازی برای شناسایی کنترل‌های امنیت

۷-۱ معرفی

هم چنان که در بند ۶ بالا اشاره شد، اولین مرحله در شناسایی و ارزیابی مخاطرات مرتبط با شبکه، آماده‌سازی برای شناسایی کنترل‌های امنیت، جمع‌آوری اطلاعات شبکه‌ی موجود و/یا طرح‌ریزی شده‌است. بند ۷-۲ زیر، راهنمایی برای آن فراهم‌می‌کند. مرحله‌ی بعد شناسایی و ارزیابی مخاطرات امنیت شبکه و زمینه‌های کنترلی بالقوه‌ی مناسب برای آن است. بند ۷-۳ زیر، راهنمایی برای آن فراهم می‌کند.

۷-۲ اطلاعات شبکه‌ی موجود و/یا طرح‌ریزی شده

۷-۲-۱ الزامات امنیتی در خط‌مشی امنیت شبکه‌ی شرکت

خط‌مشی امنیت اطلاعات یکپارچه‌ی سازمان(انجمن) می‌تواند دربرگیرنده‌ی بیانیه‌هایی برای نیازهای محرمانگی، یکپارچگی، انکار ناپذیری و دسترس‌پذیری باشد، به علاوه‌ی مروری بر انواع تهدید و مخاطره و کنترل‌های امنیتی شبکه که در رابطه با مخاطرات ارزیابی شده ، نیاز به پیاده‌سازی دارند. بنابراین بهتر است اولین قدم، بازنگری خط‌مشی امنیت اطلاعات شرکت برای جزییات مخاطرات مربوط به هر شبکه‌ای که همیشه به عنوان اهمیت بالا، لحاظ می‌شوند و کنترل‌های امنیت شبکه‌ای که باید پیاده‌سازی شوند، باشد.
به‌طور مثال چنین خط‌مشیی می‌تواند اظهار کند که:

- دسترس‌پذیری انواع خاصی از اطلاعات یا خدمات یک نگرانی اساسی است.
- هرگونه اتصالات شماره‌گیری مجاز نیستند.
- تمام اتصالات به اینترنت باید ازطریق دروازه امنیتی انجام شوند.
- نوع خاصی از دروازه‌ی امنیتی باید استفاده شود.
- دستورالعمل پرداخت بدون امضای دیجیتال مجاز نیست.

چنین الزاماتی بهتر است برای انجام ارزیابی مخاطره و بازنگری مدیریت و شناسایی جنبه‌های معماری/طراحی فنی امنیت و کنترل‌های بالقوه‌ی امنیتی لحاظ شوند. هرگونه از این الزامات باید در فهرست پیش‌نویس زمینه‌های کنترلی بالقوه، مستندسازی شوند و در صورت نیاز در گزینه‌های معماری/طراحی فنی امنیت، منعکس شوند.
راهنمای خط‌مشی امنیت اطلاعات در ISO/IEC 27002 و ISO/IEC 27005 آورده شده است.

۷-۲-۲ اطلاعات شبکه‌ی موجود/طرح‌ریزی شده

۷-۲-۲-۱ معرفی

گام بعدی، باید جمع‌آوری و بازنگری اطلاعات شبکه‌ی موجود و/یا شبکه(ها)ی طرح‌ریزی‌شده باشد. - معماری(ها)، برنامه‌های کاربردی، خدمات، انواع اتصالات و سایر مشخصه‌ها- این نقطه اتکایی برای شناسایی و ارزیابی مخاطرات و تعیین آن‌چه که در شرایط معماری/طراحی فنی امنیت شبکه امکانپذیر است، خواهدبود. این جنبه‌ها در زیر توصیف شده‌اند.

۷-۲-۲-۲ معماری شبکه، برنامه‌های کاربردی و خدمات

جزییات باید از معماری شبکه‌ی موجود و/یا طرح‌ریزی شده، برنامه‌های کاربردی و خدمات، به‌دست آمده و برای فراهم کردن درک و زمینه‌ی لازم در ارزیابی مخاطره‌ی امنیتی و بازنگری مدیریت و سپس با توجه به گزینه‌های معماری فنی امنیت شبکه، بازنگری شوند. با روشن شدن این جنبه‌ها در اولین مراحل ممکن، فرآیند شناسایی و ارزیابی مخاطرات امنیتی و کنترل‌های امنیتی مرتبط و گزینه‌های معماری فنی امنیت شبکه و تصمیم‌گیری در مورد اینکه کدام‌یک باید تصویب شود، باید کارآمدتر شوند و در نهایت منجر به یک راه‌حل امنیتی عملی‌تر بشود.

علاوه بر این، با توجه به معماری شبکه‌ی موجود و/یا طرح‌ریزی شده، جنبه‌های برنامه‌های کاربردی و خدمات، در مراحل اولیه باید زمان کافی اختصاص داد تا این جنبه‌ها بازنگری شوند و اگر واقعاً راه حل امنیتی قابل قبولی برای محیط شبکه‌ی موجود/طرح‌ریزی شده حاصل نشد، احتمال تجدیدنظر وجود داشته باشد.

بسته به ناحیه‌ی پوشش، شبکه‌ها می‌توانند به صورت گسترده‌ای طبقه‌بندی شوند:

- مجموعه‌ی LANها که برای به‌هم وصل‌کردن سامانه‌ها بصورت محلی استفاده می‌شوند و
- مجموعه‌ی WAN که برای به‌هم وصل‌کردن سامانه‌ها تا حد پوشش گسترده‌ی جهانی استفاده می‌شوند.

(برخی منابع عبارت شبکه‌ی ناحیه‌ی شهری(MAN) را برای WAN محدودشده استفاده می‌کنند،به‌طور مثال داخل شهر. به‌هرحال امروزه همان فن‌آوری‌ها برای WAN استفاده می‌شوند و بنابراین تفاوت چشمگیری بین MAN و WAN وجود ندارد. به علاوه در راستای اهداف این استاندارد، شبکه‌های ناحیه شخصی(PAN)[1] در رده LAN قرار می‌گیرند. عبارت دیگری که امروزه استفاده می‌شود، شبکه ناحیه‌ی جهانی(GAN)[2] است، یعنی یک WAN جهانی. توجه داشته باشید که امروزه عباراتی هم برای شبکه‌های

1 - Personal Area Networks
2 - Global Area Network

مربوط به ذخیره‌سازی، مانند شبکه‌ی ناحیه‌ی ذخیره‌سازی(SAN) و ذخیره‌ساز متصل به‌شبکه(NAS) وجود دارند، اما در حوزه‌ی پوشش ISO 27033 نیستند.)

پروتکل‌های مختلف، مشخصه‌های امنیتی متفاوتی دارند و توجه ویژه‌ای هم نیازدارند. برای مثال:

- پروتکل‌های رسانه‌ای به اشتراک‌گذاشته‌شده به شکل عمومی در LANها استفاده‌شده‌اند و سازوکارهایی برای تنظیم استفاده از رسانه‌ی به اشتراک گذاشته‌شده‌ی بین سامانه‌های متصل شده، فراهم می‌کنند. هم‌چنان‌که یک رسانه‌ی به‌اشتراک گذاشته‌شده استفاده می‌شود، تمام اطلاعات شبکه، به‌طور فیزیکی توسط همه‌ی سامانه‌های متصل‌شده قابل دسترسی هستند. هاب اترنت مثالی برای این هست.
- پروتکل‌های کنترل دسترسی که برای اجازه‌ی ورود به شبکه طراحی شده‌اند. مثال‌های آن IEEE 802. 1x و WPA هستند.
- پروتکل‌های مسیریابی استفاده‌شده برای تعریف مسیر از طریق گره‌های مختلفی که اطلاعات را از قسمت‌های شبکه هم LAN هم WAN عبور می‌دهند. اطلاعات در طول مسیر به‌طور فیزیکی برای همه‌ی سامانه‌ها قابل دسترسی است و مسیریابی می‌تواند چه عمدی و چه سهوی تغییرکند.
- پروتکل‌های MPLS که مبنای بسیاری از شبکه‌های انتقال اطلاعات هستند، اجازه‌ی اشتراک گذاری به هسته‌ی شبکه‌ی انتقال با شبکه‌های چندتایی خصوصی را می‌دهند، بدون اینکه هیچ عضوی از شبکه خصوصی از این اشتراک‌گذاری اگاه شود.کاربرد اصلی، پیاده‌سازی VPNها است، به‌طوری که برچسب‌های مختلفی برای شناسایی و جداسازی ترافیک متعلق به VPNهای مختلف استفاده‌شوند. (MPLS مبتنی بر VPN مبتنی بر ساز و کارهای رمزگذاری داده نیست.)این مشتریان شرکت را قادر می‌سازد تا شبکه‌ی داخلی‌شان را به یک فراهم‌کننده‌ی خدمت، برونسپاری کنند و بنابراین از گسترش ومدیریت کردن هسته‌ی IP شبکه دوری می‌کنند. مزیت کلیدی، توانایی همگراکردن خدمات شبکه، مانند صدا و داده روی یک شبکه با استفاده از سازوکارهای کیفیت خدمات[1] برای حصول اطمینان از بازدهی زمان واقعی[2] است.

بسیاری از پروتکل‌های استفاده‌شده در شبکه امنیتی را پیاده‌سازی نمی‌کنند، برای مثال ابزارهایی برای به‌دست‌آوردن گذرواژه از ترافیک شبکه توسط حمله‌گرها، به‌طور عادی استفاده می‌شوند. این ابزار پروتکل‌هایی مثل Telnet را که گذرواژه‌های رمزنشده را روی شبکه‌ی عمومی ارسال می‌کند، بسیار آسیب‌پذیر می‌کند.

یادآوری- Telnet برنامه‌ی شبیه‌ساز پایانه‌ای برای کارکردن برخط روی رایانه‌ی راه دور است

بسیاری از پروتکل‌ها در ترکیب با هم‌بندی‌های مختلف شبکه و رسانه و با استفاده از فن‌آوری‌های با سیم و بی‌سیم می‌توانند استفاده شوند. در بسیاری موارد این اثر بیشتری بر مشخصه‌های امنیتی دارد.

نوع برنامه‌ی کاربردی استفاده شده در شبکه باید در محتوای امنیت درنظر گرفته‌شود. انواع آن می‌توانند شامل:

1- Quality Of Service
2 - Real Time

- برنامه‌های کاربردی تین کلاینت
- برنامه‌های کاربردی رومیزی[1]
- برنامه‌های کاربردی مبتنی بر شبیه‌ساز پایانه[2]
- زیرساخت پیام‌رسانی و برنامه‌های کاربردی
- برنامه‌های کاربردی مبتنی بر ذخیره و ارسال یا برنامه‌ی ردیف‌گر[3]
- برنامه‌های کاربردی مشتری-خدمت‌گزار[4]

مثال‌های زیر نشان می‌دهند که چگونه مشخصه‌های برنامه‌های کاربردی بر روی الزامات امنیتی محیط شبکه‌های که آنها ممکن است استفاده کنند، تاثیر می‌گذارند:

- برنامه‌های کاربردی پیام‌رسان(که رمزنگاری و امضای دیجیتالی را برای پیام‌ها فراهم می‌کنند) می‌توانند کنترل سطح امنیتی کافی را بدون پیاده‌سازی کنترل‌های امنیتی اختصاص داده شده، روی شبکه ارائه دهند.
- برنامه‌های کاربردی تین کلاینت، ممکن است برای عملکرد مناسب، لازم باشد تا کد سیار بارگیری[5] کنند. در حالی که محرمانگی ممکن است مساله ای مهم در این زمینه باشد، اما یکپارچگی مهم است و شبکه باید سازوکارهای مناسب را برای آن فراهم کند. به‌طور متناوب اگر الزامات مهم‌تر نیاز به برآورده‌شدن داشته‌باشند، امضای دیجیتال کدهای سیار، یکپارچگی و احرازهویت اضافی را ارائه می‌کند. اغلب این کار با چارچوب برنامه‌ی خودش انجام می‌شود و برای همین ممکن است به فراهم‌آوردن این خدمات در شبکه نیاز نباشد.
- برنامه‌های کاربردی مبتنی بر ذخیره و ارسال یا برنامه‌ی ردیف‌گر، معمولاً داده‌های مهم را در گره‌های میانی برای پردازش آنی، به‌طور موقت ذخیره‌می‌کنند. اگر الزامات یکپارچگی و محرمانگی وجود دشته باشند، کنترل‌های مناسب برای حفاظت داده‌ها در انتقال روی شبکه مورد نیاز خواهد بود. با این‌حال با توجه به ذخیره‌سازی موقت داده‌ها در میزبان‌های واسط، این کنترل‌ها ممکن است کافی نباشند. بنابراین ممکن است اعمال کنترل‌های اضافی برای محافظت داده‌های ذخیره‌شده در گره‌های میانی نیاز باشد.
  نوع خدمات (سامانه نام دامنه[6]، پست الکترونیکی،صدا) استفاده شده در شبکه نیز از لحاظ امنیت، باید مورد توجه قرار گیرند.

وقتی که معماری شبکه، برنامه‌های کاربردی و خدمات بازنگری می‌شوند، به اتصالات درون شبکه‌ای موجود، به یا از سازمان/انجمن و به شبکه‌ای که اتصال را پیشنهاد کرده است، باید توجه داده‌شود. مثلاً به خاطر یک موافقت‌نامه یا قرارداد اتصالات موجود در سازمان/انجمن می‌توانند محدود شود یا از ایجاد اتصالات جدید پیشگیری کنند. وجود اتصالات دیگر به یا از شبکه‌ای که به اتصال نیاز دارد، می‌تواند آسیب‌پذیری‌های اضافی

1 - Desktop
2- Terminal Emulation
3- Spooler
4 - Client Server
5 - Download
6 - Domain Name System

و بنابراین مخاطرات مهم‌تری را معرفی و به‌طور احتمالی نیاز به کنترل‌های قوی‌تر و/یا اضافه‌تری را می‌تواند تضمین کند.
(راهنمای کلی شبکه و معماری‌های برنامه‌های کاربردی در ISO/IEC 7498 پیدا می‌شوند.)

۷-۲-۲-۳ انواع اتصالات شبکه

بسیاری از انواع اتصالات شبکه‌ای کلی وجود دارند که سازمان/انجمن ممکن است نیاز به استفاده‌ی از آن داشته باشند. بعضی از این نوع اتصالات می‌توانند از طریق شیکه‌های خصوصی ساخته‌شوند(با دسترسی که محدود به یک گروه شناخته‌شده است) و بعضی از آنها می‌توانند از طریق شبکه‌های عمومی (با دسترسی بالقوه‌ی قابل استفاده برای هر سازمان یا شخص). علاوه بر این انواع اتصالات شبکه‌ای می‌توانند برای طیفی از خدمات مانند پست الکترونیکی استفاده شوند و می‌توانند استفاده‌ی از امکانات اینترنت،درون‌نت یا اکسترانت را، هر کدام با تفاوت در ملاحظات امنیتی، دربرگیرند. هر کدام از انواع اتصال می‌توانند آسیب‌پذیری متفاوتی داشته‌باشند و بنابراین مخاطرات امنیتی مرتبط و در نهایت به مجموعه‌ی مختلفی ازکنترل‌ها نیاز است.
یک روش برای دسته‌بندی انواع کلی اتصالات شبکه‌ای که ممکن است برای انجام کسب و کار مورد نیاز باشد، در زیر آمده است:
- اتصال داخلی بین قسمت‌های مختلف همان سازمان درون همان مکان کنترل‌شده یعنی ساختمان کنترل‌شده یا پایگاه تکی،
- اتصال داخلی بین قسمت‌های جغرافیایی مختلف یک سازمان، به‌طور مثال اتصال دفترهای منطقه‌ای با پایگاه دفتر مرکزی از طریق WAN. اغلب اگرچه همه‌ی کاربران قادر به دسترسی به سامانه‌های دسترس‌پذیر از طریق شبکه نیستند، اما کاربران داخل سازمان هم نباید برای دستیابی به همه برنامه‌ها یا اطلاعات اجازه داشته‌باشند.
- اتصال بین پایگاه یک سازمان و کارکنانی که در محل‌های دور از سازمان کار می‌کنند یا برقراری پیوندهای راه دور به سامانه‌های محاسباتی سازمان توسط کارمندانی که از خانه یا پایگاه‌های راه دور دیگر کار می‌کنند و از طریق شبکه‌ای که سازمان آن را نگهداری می‌کند، وصل نشده‌اند.
- اتصال بین سازمان‌ها داخل یک گروه محدود، به طور مثال به دلیل وضعیت قراردادی یا قانون لازم‌الاجرا یا منافع مشابه تجاری بطور مثال بانکداری یا بیمه. چنین اتصالاتی نباید دسترسی به تمام بازه برنامه‌های کاربردی را که بوسیله هر کدام از سازمان‌های شرکت کننده استفاده می‌شوند، فراهم کنند.
- اتصال با سایر سازمان‌ها، به‌طورمثال برای دستیابی به بانک داده‌هایی که سازمان دیگر نگهداری می‌کند. در این نوع از اتصال شبکه‌ای، همه کاربران که شامل کاربران سازمان متصل‌شونده هستند، به‌طورجداگانه توسط سازمان بیرونی که اطلاعاتش دستیابی می‌شوند، از قبل مجوز داده شوند.
- اتصالات به دامنه عمومی کلی با دسترسی تعریف شده برای کاربران سازمان به بانک داده دسترسی عمومی، پایگاه وب و/ یا تسهیلات پیام الکترونیکی (به‌طور مثال با اینترنت)

- اتصال به شبکه عمومی تلفن از محیط IP، با دسترسی تعریف شده به PSTN از یک تلفن در شبکه‌ی IP .
چنین اتصالاتی همچون تماسهایی که می‌توانند از هر نقطه دنیا دریافت شوند، غیرقابل‌کنترل هستند.
تمام معانی که از این دسته‌بندی‌ها استفاده می‌شود، انواع مختلف اتصال در محیط شبکه‌ی موجود و/یا طرح‌ریزی شده باید برای مفاهیم امنیتی‌شان، بازنگری شوند و اطلاعات به‌دست‌آمده باید در فرآیند شناسایی و ارزیابی مخاطرات امنیتی و کنترل‌های امنیتی وابسته و گزینه های معماری فنی امنیت شبکه استفاده شوند و تصمیم‌گیری شود که کدام‌یک باید پذیرفته شوند.

۷-۲-۲-۴ سایر مشخصه‌های شبکه

سایر مشخصه‌های شبکه(ها)ی موجود و/یا طرح‌ریزی شده، باید بازنگری شوند- این خصوصاً از این جهت مهم است که تعیین شود آیا شبکه‌ی مورد استفاده/ در آینده استفاده شونده، یک شبکه‌ی عمومی است- شبکه‌ای که به‌وسیله‌ی هرکسی قابل دسترسی است، یا شبکه‌ی خصوصی، به‌طور مثال شبکه‌ای شامل خطوط شخصی یا استیجاری، باید خیلی امن‌تر درنظر گرفته‌شود تا یک شبکه‌ی عمومی. هم‌چنین دانستن نوع داده‌ای که روی شبکه منتقل می‌شود مهم است، به‌طور مثال یک:

- شبکه داده‌ای- شبکه‌ای برای انتقال داده‌ها و اجبارکردن به استفاده از پروتکل‌های داده‌ای
- شبکه صدا – یک شبکه به هدف استفاده‌ی تلفن اما قابل استفاده برای داده یا
- شبکه ترکیبی دربرگیرنده‌ی هم داده و هم صدا و شاید هم تصویر

سایر اطلاعات مرتبط مانند:

- اینکه شبکه، بسته‌ای است یا سوییچینگ یا MPLS است
- اینکه از کیفیت خدمات پشتیبانی می‌کند، به عنوان مثال در یک شبکه‌یMPLS (کیفیت خدمات مربوط می‌شود به کارایی پایدار ، قابلیت اطمینان و دسترسی پذیری . خدمات شبکه باید طوری تحویل شوند که کمترین سطح بازدهی قابل استفاده باشد. برای مثال اگر پهنای باند ناکافی باشد خدمات صدا بریده بریده و مقطّع خواهند بود. کیفیت خدمات بر قابلیتهای سامانه شبکه ای اشاره دارد که خدمت ارائه داده شده را در کمترین سطح بازدهی یا بالاتر از بازدهی مورد نیاز پایدار نگه دارد.)،

به‌علاوه، این اتصال خواه اتصال دایمی خواه اتصال در زمان مورد نیاز، باید برقرارشده باشد.
وقتی این مشخصه‌های شبکه‌ی موجود و/یا طرح‌ریزی‌شده، شناسایی و دست کم برقرار شده بودند، اگر شبکه عمومی یا خصوصی بود، آن‌وقت توجه برای پیگیری ورود به بازنگری مدیریت و ارزیابی مخاطرات امنیت شبکه ارزش دارد. تقریباً شبکه به چیزهایی مشابه دسته بندی می‌شوند.
شبکه با:

- گروه ناشناخته‌ی کاربران
- گروه شناخته شده‌ای از کاربران و مرتبط با یک کسب و کار (از بیش از یک سازمان)
- گروه شناخته شده‌ای از کاربران منحصراً داخل سازمان

سپس به مفهوم دسته‌بندی درشبکه‌ی استفاده شده/ درحال استفاده، خواه یک شبکه عمومی‌باشد خواه خصوصی توجه کنید و بیشتر دسته بندی شود مانند:

- گروه ناشناخته‌ای از کاربران و استفاده از شبکه‌ی عمومی
- گروه شناخته شده‌ی کاربران مرتبط با یک کسب و کار و استفاده از شبکه‌ی عمومی
- گروه شناخته شده‌ی کاربران منحصرا درون سازمان و استفاده از شبکه‌ی عمومی
- گروه ناشناخته‌ای از کاربران و استفاده از شبکه‌ی خصوصی
- گروه شناخته شده‌ی کاربران مرتبط با یک کسب و کار و استفاده از شبکه‌ی خصوصی

به هر روشی که بازنگری انجام شود، باید توجه داشت که ترکیبات خاصی نسبت به بقیه حالت‌ها سطح پایین‌تری از خطر خواهند داشت. اطلاعات بدست آمده باید در فرآیند شناسایی و ارزیابی مخاطرات امنیتی و کنترل‌های امنیتی وابسته و گزینه‌های معماری فنی امنیت شبکه استفاده‌شوند و تصمیم‌گیری شود که کدام‌یک باید پذیرفته‌شوند.

۷-۲-۲-۵ سایر اطلاعات

در نهایت، اطلاعات دیگر باید جمع‌آوری شوند تا به درستی برای بازنگری مدیریت و ارزیابی مخاطرات امنیتی شبکه‌ی سازگار با ISO/IEC 27001 و27002 آماده‌شوند که شامل تعریف دقیق بازنگری مرز/دامنه می‌شود. انجام این کار در فرصتهای اولیه از ابهام بعدی و کار اضافی جلوگیری خواهدکرد و تمرکز و اثر بخشی بازنگری را بهبود خواهد داد. تعریف مرز/دامنه باید به روشنی نشان دهد کدام یک از موارد زیر موقعی که مدیریت و ارزیابی مخاطرات شبکه انجام می‌شود باید در نظر گرفته‌شوند.

- انواع اطلاعات
- فرآیندهای کسب و کار
- اجزای واقعی یا بالقوه‌ای سخت افزار یا نرم افزار، خدمات، اتصالات و غیره. جزییات(اگر به طور مشخص در عبارات کلی شناخته نشده اند)
- محیط های واقعی یا بالقوه (بطور مثال مکانها، امکانات)
- فعالیتها (عملکردها)

این اطلاعات ، به همراه آنچه که در تطابق با بند ۷. ۲ بالا جمع آوری شد، باید در بازنگری مدیریت و ارزیابی مخاطرات امنیت شبکه استفاده شوند، فعالیتهای هر کدام در بند ۷. ۳ زیر خلاصه شده است.

۷-۳ مخاطرات امنیت اطلاعات و نواحی کنترل بالقوه

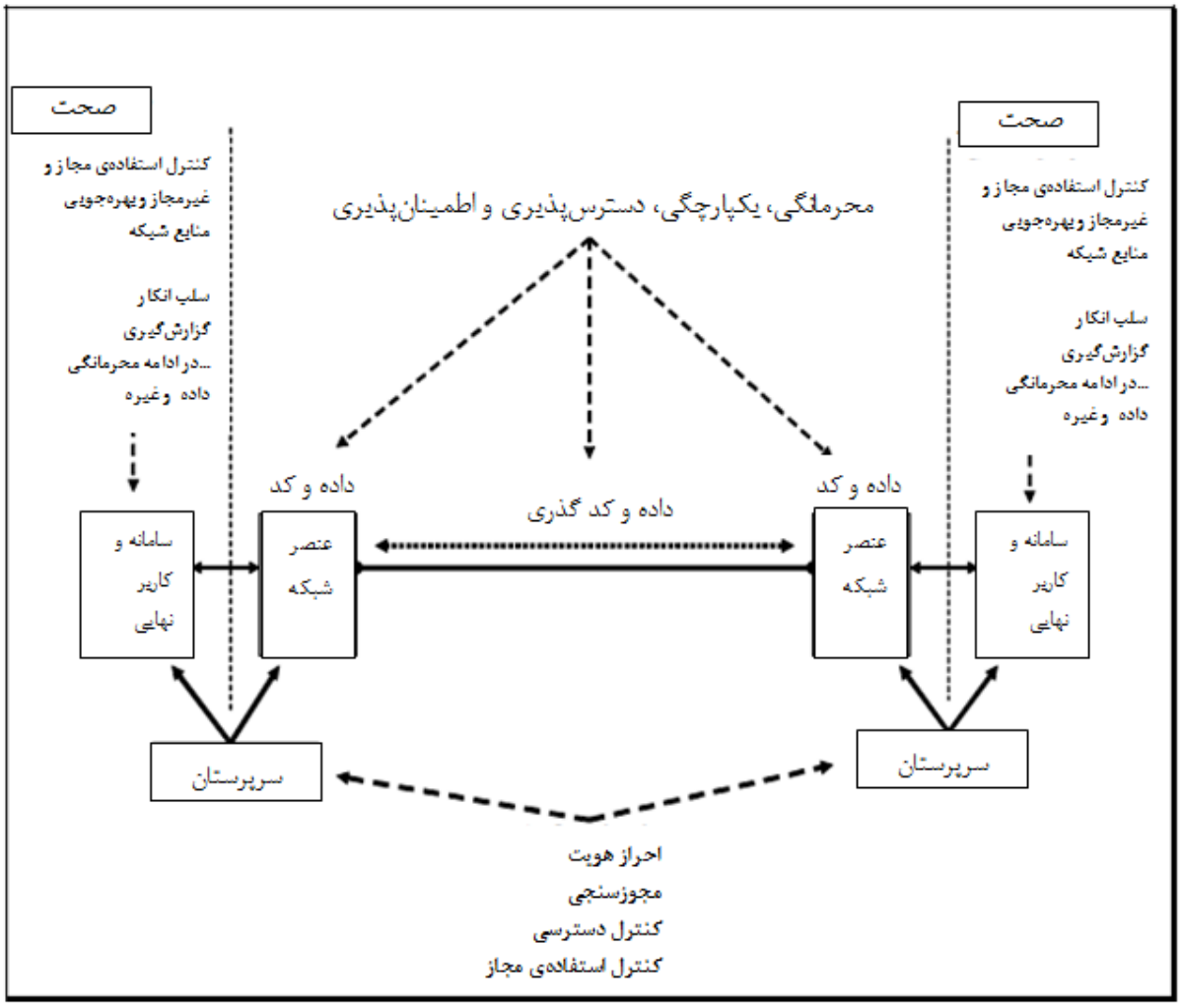
همان‌طور که پیشتر گفته‌شد، بیشتر سازمان‌ها امروز وابسته به استفاده از شبکه و سامانه‌های اطلاعات مرتبط و اطلاعات برای پشتیبانی از عملکردهای کسب و کارشان هستند. بعلاوه در بسیاری موارد، الزامات کسب و کار روشنی برای استفاده از شبکه‌ها، بین سامانه‌های اطلاعاتی در محل هر سازمان و به دیگر مکانها هم درون و هم بیرون از سازمان، دربرگیرنده‌ی کلیات عمومی وجود دارد. وقتی که اتصالی به شبکه دیگر برقرار شود مراقبت قابل توجهی باید صورت گیرد تا اطمینان حاصل شود که سازمان متصل‌شده در معرض مخاطرات مضاعفی قرار نگرفته باشد (از تهدیدهای بالقوه بهره‌جویی آسیب‌پذیری). این مخاطرات می‌توانند به‌طور مثال نتیجه‌ی اتصال خود شبکه یا از اتصالات شبکه‌ی دیگرسو باشند.

بعضی از این مخاطرات می‌توانند مربوط به حصول اطمینان از پایبندی به قوانین و مقررات مربوط باشد. (مخصوصا باید به قانون حفاظت از داده‌ها و حریم خصوصی توجه کرد. بسیاری از کشورها قوانین کنترلی برای جمع‌آوری خصوصی پردازش و انتقال داده‌های شخصی وضع‌کرده‌اند ، یعنی داده‌ای که می‌تواند مربوط به فرد یا افرادی خاص باشد . بسته به قوانین ملی مربوط ، چنین کنترل‌هایی می‌توانند وظایفی را برای جمع‌آوری ، پردازش و انتشار اطلاعات شخصی از طریق شبکه‌ها اعمال‌کنند و حتی می‌توانند توانایی انتقال داده به سایر کشورها هم که نتیجه‌اش اضافه‌شدن نگرانی‌های مهم امنیتی است، محدود کنند. برخی تجهیزات سخت افزاری و برخی آدرس‌های IP، نمونه‌های داده‌ای مبهم‌تری هستند که می‌توانند موضوع چنین قوانینی باشند).

بنابراین مخاطرات پیش‌رو می‌توانند مربوط به نگرانی درباره دسترسی غیر مجاز به اطلاعات، ارسال غیر مجاز اطلاعات، معرفی کدهای مخرب، انکار دریافت یا انکار مبدا اطلاعات، انکار خدمات اتصال و عدم دسترسی به اطلاعات و خدمات باشند. این مخاطرات می‌توانند مربوط به از دست دادن موارد زیر باشند.

- محرمانگی کد و اطلاعات (در شبکه‌ها و سامانه‌های متصل به شبکه‌ها)
- یکپارچگی کد و اطلاعات (در شبکه‌ها و سامانه‌های متصل به شبکه‌ها)
- دسترس‌پذیری اطلاعات و خدمات شبکه (و رسانه‌های متصل به شبکه‌ها)
- انکارناپذیری تراکنش های شبکه (الزامات)
- پاسخگویی تراکنش های شبکه
- اعتبار اطلاعات (و البته کاربران و مدیران شبکه)
- قابلیت اطمینان اطلاعات و کد (در شبکه‌ها و رسانه های متصل به شبکه‌ها)
- توانایی کنترل استفاده‌ی غیرمجاز و بهره‌برداری از منابع شبکه، از جمله در زمینه خط‌مشی سازمان (به‌طور مثال فروش و یا استفاده از پهنای باند برای منافع شخصی) و مسئولیت نسبت به قوانین و مقررات (بطور مثال ذخیره سازی هرزه نگاری درباره کودکان)
- توانایی برای کنترل سوء استفاده از دسترسی‌های مجاز.

مدل مفهومی از نمایش امنیت شبکه که در آن انواع مخاطرات امنیتی که ممکن است رخ دهد در شکل ۵ زیر نشان داده شده است .



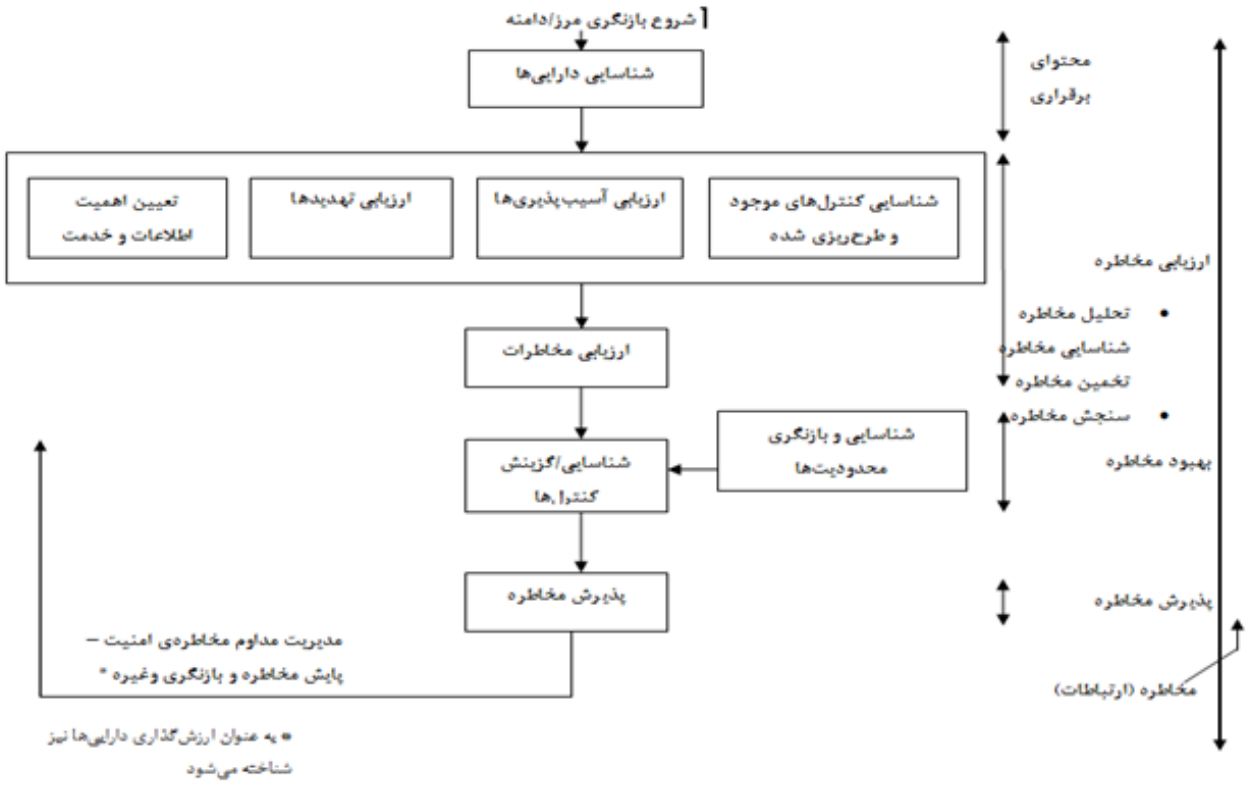
شکل ۵ – مدل مفهومی حوزه‌ی مخاطره‌ی امنیت شبکه

بنابراین، بازنگری مدیریت و ارزیابی مخاطره‌ی امنیت شبکه باید برای شناسایی و تایید کنترل‌های فنی امنیت و جنبه‌های معماری/طراحی فنی امنیت و پشتیبانی کنترل‌های غیرفنی امنیتی و بعد از آن، تجربیات خوب امنیتی شناخته شده، مانند آن‌چه در ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 آورده‌شده‌است، انجام شود. این شامل این پنج فعالیت می‌شود:

- تعیین معیارهای اهمیت اطلاعات و خدمات که با عبارت‌های اثرات نامطلوب بالقوه بر روی عملکردهای کسب و کار، موقعی که رخدادهای ناخواسته، واقع می‌شوند، بیان شده‌است. (گاهی اوقات به نام ارزیابی دارایی نامیده‌می‌شود.)این‌کار ارزش عملکردهای کسب و کار اطلاعات را که از طریق شبکه باید منتقل شوند، هرگونه اطلاعات بالقوه در دسترس به‌طور غیرمجاز از طریق شبکه و خدمات ارائه شده را دربر می‌گیرد.
- شناسایی وارزیابی احتمال کلی یا سطوح تهدید در برابر اطلاعات و خدمات

- شناسایی وارزیابی درجه‌ی جدیت یا سطوح آسیب‌پذیری‌هایی که می‌تواند به‌سیله‌ی تهدیدهای شناخته‌شده، مورد بهره‌برداری قرارگیرند.
- ارزیابی مقادیر مخاطرات بر اساس معیارهای تعریف‌شده‌ی اثرات نامطلوب بالقوه روی عملکردهای کسب وکار و سطوح تهدید و آسیب‌پذیری‌ها
- شناسایی جنبه‌های معماری /طراحی امنیت فنی و حوزه‌های کنترل بالقوه‌ی امنیت که توجیه شده‌اند و بنابراین نیاز به حصول اطمینان از این‌که مخاطرات ارزیابی شده در سطوح قابل قبول باقی می‌مانند، است.

فرآیندهای اصلی ارزیابی و مدیریت مخاطره‌ی امنیت شبکه در شکل ۶ زیر نشان داده‌شده‌اند(این اثر بسط یافته‌ی جعبه‌ی شکل ۴ بالاست که « تعیین دامنه/محتوی و بعد ارزیابی مخاطرات» نام گرفته است و جعبه‌ی مربوط به آن«شناسایی مخاطرات مربوط به شبکه و آمادگی برای شناسایی کنترل‌های امنیتی.») در شکل ۶، دو ردیف اول جعبه که «برقراری بازنگری مرز/ دامنه» و «شناسایی دارایی‌ها» برچسب خورده‌اند، فعالیت‌های مقدماتی را نشان‌می‌دهند. دو ردیف بعدی جعبه‌ها، فعالیت‌های ارزیابی مخاطره را نشان‌می‌دهند و دو ردیف آخر، گزینش کنترل امنیت اطلاعات و (باقیمانده) فعالیت‌های پذیرش مخاطره را نشان‌می‌دهند.



شکل ۶- مدیریت فرآیندها و ارزیابی مخاطره‌ی امنیت شبکه

یادآوری- برای جزییات اطلاعات مربوط به شروع بازنگری ارزیابی و مدیریت مخاطره‌ی امنیت شبکه، به ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 رجوع شود.

در اجرای چنین بازنگری‌هایی تاکید می‌شوداز اطلاعات مخاطره‌ی(و کنترل امنیت) مرتبط با سناریوهای شبکه‌ی موردنیاز و موضوعات «فناوری»، هرجایی که کاربردپذیر باشد، استفاده شود – مطابق با بندهای ۱۰و۱۱ و پیوست الف، زیر و قسمت‌های ۳ تا ۷.

۸ کنترل‌های پشتیبانی

۸-۱ مقدمه

این بند، مرورکلی بر کنترل‌هایی را که معماری‌های فنی امنیت شبکه و کنترل‌های فنی مرتبط، پشتیبانی می‌کنند، فراهم می‌کند، یعنی سایر کنترل‌ها (غیرفنی و فنی) که کاربردپذیر هستند اما نه فقط برای شبکه‌ها. اطلاعات بسیاری از انواع این کنترل‌ها در استانداردهای ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 پیدا می‌شوند. کنترل‌هایی که به‌طور ویژه راجع به استفاده از شبکه‌ها مهم هستند، در بندهای ۸-۲ تا ۸-۹ زیر شرح داده‌شده‌اند، که مدیریت امنیت شبکه (فعالیت‌های مدیریت امنیت شبکه، مسؤولیتها و نقش‌های امنیت شبکه، پایش شبکه و ارزیابی امنیت شبکه)، مدیریت فنی آسیب‌پذیری، شناسایی و احرازهویت، ثبت ممیزی شبکه و پایش، تشخیص نفوذ، حفاظت در برابر کدهای مخرب، رمزنگاری[1] مبتنی بر خدمات و مدیریت تداوم کسب و کار را نشان می‌دهند. ، مراجعی مربوط به محتوای ISO/IEC 27001، ISO/IEC 27002 و ISO/IEC 27005 به عنوان موضوع مرتبط فراهم شده‌اند.

۸-۲ مدیریت امنیت شبکه

۸-۲-۱ پیش‌زمینه

مدیریت کلان امنیت شبکه باید با روشی امن انجام شود و با توجه به پروتکل‌های مختلف دسترس‌پذیر شبکه و خدمات امنیت مربوط، تکمیل شود. برای پیشبرد این هدف، سازمان باید تعدادی از کنترل‌های امنیت شبکه را درنظر بگیرد که بیشتر آنها می‌توانند از طریق استفاده از ISO/IEC 27002 وISO/IEC 27005 شناسایی شوند. آن قسمت‌هایی که نیاز به بسط محتوای امنیت شبکه دارند، در بندهای ۸-۲-۲ تا ۸-۲-۵ زیر، شرح داده‌شده‌اند.

1 - Cryptographic

۸-۲-۲ فعالیت‌های مدیریت امنیت شبکه

۸-۲-۲-۱ مقدمه

نیاز کلیدی هر شبکه، پشتیبانی آن توسط فعالیت‌های مدیریت امن است که وظیفه‌ی آغاز و کنترل پیاده‌سازی و اجرای امنیت را خواهدداشت. این فعالیت‌ها برای حصول اطمینان از امنیت سامانه‌های اطلاعات همه‌ی سازمان/انجمن باید انجام شوند. فعالیت‌های مدیریت امنیت شبکه باید شامل :

- تعریف تمام مسؤولیت‌های مربوط به امنیت شبکه و معرفی مدیر امنیت با مسؤولیتهای کلان
- خط‌مشی امنیت شبکه و معماری فنی امنیت مستند شده
- مستندات روال‌های بهره‌برداری امنیت[1] شبکه
- وارسی تطابق امنیت شامل آزمون امنیت برای حصول اطمینان از حفظ امنیت در سطح مورد نیاز
- شرایط امنیتی مستندشده برای اتصال به شبکه قبل از این‌که به اتصالی اجازه داده شود،باید رعایت شوند- آنچه که به سازمان‌ها یا افراد داخلی یا خارجی مربوط است.
- شرایط امنیتی مستندشده برای کاربران راه دور شبکه
- طرح مدیریت رخداد امنیت شبکه
- طرح مستندشده و آزمایش‌شده‌ی تداوم کسب و کار/بازیابی به هنگام بروز فاجعه

برای اطلاعات جزیی‌تر در مورد این موضوعات، باید اشاره‌ای به ISO/IEC 27002، ISO/IEC 27005 و ISO/IEC 27035 شود. تنها برای موضوعاتی از بالا که به‌ویژه راجع به استفاده از شبکه‌ها مهم هستند، راهنمایی بیشتری در بندهای زیر فراهم‌شده‌است.

۸-۲-۲-۲ خط‌مشی امنیت شبکه

خط‌مشی امنیت شبکه، مسؤولیت مدیریت برای پذیرش آشکار و پشتیبانی از خط‌مشی امنیت شبکه‌ی سازمان است(هم‌چنان‌که در ISO/IEC 27002 به آن اشاره شده‌است). این خط‌مشی باید از خط‌مشی امنیت اطلاعات سازمان، ناشی شود و با آن سازگار باشد. خط‌مشی امنیت باید قابلیت پیاده‌سازی، آمادگی دسترس‌پذیری به اعضای مجاز سازمان را داشته‌باشد و دربرگیرنده‌ی بیانیه‌های شفافی در موارد زیر باشد:

- موضع‌گیری سازمان نسبت به استفاده‌های قابل قبول شبکه
- قواعد روشن برای استفاده‌ی امن از منابع خاص شبکه، خدمات و برنامه‌های کاربردی
- پیامدهای ناشی از عدم تطابق با قواعد امنیتی
- نگرش سازمان نسبت به سوء استفاده از شبکه
- دلیل(های) منطقی برای این خط‌مشی و برای هرگونه قواعد امنیتی خاص

(در بعضی شرایط، این احکام روشن اگر برای سازمان راحت‌تر و برای کارکنان روشن‌تر است، می‌توانند در خط‌مشی امنیت اطلاعات گنجانده‌شوند.)

1 - SecOP

محتویات خط‌مشی امنیت شبکه معمولاً باید شامل خلاصه‌ای از نتایج بازنگری ارزیابی و مدیریت مخاطره‌ی امنیت شبکه باشد(که توجیهی برای صرف کنترل‌ها فراهم می‌کند)، و جزییات همه‌ی کنترل‌های امنیتی انتخاب‌شده‌ی متناسب با مخاطرات ارزیابی شده را دربرگیرد(مطابق با بند ۳.۷ بالا)

۸-۲-۲-۳ رویه‌های بهره‌برداری امنیت شبکه

در پشتیبانی از خط‌مشی امنیت شبکه، مستندات روال‌های بهره‌برداری امنیت باید توسعه‌داده و نگهداری شوند. این مستندات باید شامل جزییات رویه‌های بهره‌برداری روزبه‌روز مرتبط با امنیت شبکه باشند، و این‌که چه کسی مسؤول مدیریت و استفاده‌ی آنهاست. یک مثال الگو در پیوست پ نشان داده‌شده‌است.

۸-۲-۲-۴ وارسی پذیرش امنیت شبکه

برای تمام شبکه‌ها، بررسی پذیرش امنیت باید با یک چک‌لیست جامع تشکیل شده از کنترل‌های مشخص‌شده‌ی زیر صورت‌گیرد:

- خط‌مشی امنیت شبکه
- روال‌های بهره‌برداری امنیت مرتبط
- معماری فنی امنیت
- خط‌مشی (امنیت) دسترسی خدمت دروازه‌ی امنیت
- طرح(های) تداوم کسب وکار
- هرجا که مربوط به وضعیت امنیت اتصالات باشد

این‌کار باید شامل انجام آزمون امنیت برای استانداردهای شناخته‌شده با راهبرد آزمون امنیت و طرح‌های مرتبط تولیدشده‌ی قبل از تنظیم باشد، دقیقاً مانند آن‌چه در آزمون‌ها با چه چیز، کجا و چه‌وقت انجام می‌شوند. این‌کار باید ترکیبی از پویش آسیب‌پذیری و آزمون نفوذ را در برگیرد. قبل از آغاز چنین آزمونی، طرح آزمون باید برای حصول اطمینان از این‌که آزمون با شیوه‌ای کاملاً سازگار با قوانین مربوط انجام‌خواهدشد، بررسی شود. موقع انجام این بررسی، نباید فراموش کرد که یک شبکه، ممکن است فقط به یک کشور محدود نشده باشد-ممکن است در کشورهای مختلف با قوانین متفاوت گسترده شده‌باشد. در پیگیری آزمون‌ها، گزارش‌ها باید مشخصات آسیب‌پذیری‌های مواجه‌شده و اصلاحات موردنیاز و این را که در چه اولویتی قراردارند، نشان دهند.

۸-۲-۲-۵ شرایط امنیتی برای اتصالات شبکه‌ی چند سازمان

به‌جز در مواردی که شرایط امنیتی برای اتصال در یک مکان و یک قرارداد، مورد توافق هستند، سازمان، تحت تاثیر پذیرش مخاطرات مرتبط با اتصالات نقطه‌ی دیگر شبکه خارج از دامنه‌ی خود می‌باشد. چنین

مخاطراتی می‌توانند شامل آنهایی باشندکه مرتبط با محافظت داده/حریم شخصی هستند، در جایی‌که سمت انتهایی دیگر شبکه (خارج از دامنه‌ی سازمان)و در کشوری دیگر که قوانین آن ممکن است متفاوت باشند، قرار دارد.

در این روش، سازمان الف می‌تواند اطمینان حاصل‌کند که سازمان ب مخاطراتش را به روشی قابل قبول مدیریت می‌کند. در چنین مواردی الف باید شرایط امنیتی را برای سند اتصال طوری تولیدکند که کنترل‌هایی که باید در سمت ب ارائه شوند، با جزییات تعریف شوند. این‌کار باید توسط سازمان ب پیاده‌سازی شود، و پیگیری شود که آن سازمان بیانیه‌ی اتصال را که برای اثر و امنیت آن پشتیبانی خواهد کرد، امضا می‌کند. سازمان الف حق تصدی(کمیسیون) یا انجام بررسی انطباق سازمان ب را برای خود محفوظ می‌دارد.

هم‌چنین مواردی وجود خواهند داشت که سازمان‌ها در یک گروه بر سر سند«شرایط امنیت برای اتصال» توافق می‌کنند که تعهدات و مسؤولیت‌های هر قسمت را شامل بررسی انطباق متقابل ثبت کنند.

۸-۲-۲-۶ مستندات شرایط امنیت برای کاربران راه‌دور شبکه

کاربران مجاز برای کار از راه دور باید مدرک مستندشده‌ی «شرایط امنیت برای کاربران راه‌دور شبکه» داشته باشند. این مدرک مسؤولیت‌های کاربران را برای سخت‌افزار، نرم‌افزار و داده مرتبط با شبکه و امنیت آن شرح می‌دهد.

۸-۲-۲-۷ مدیریت رخداد امنیت شبکه

در جایی‌که شبکه‌ها در حال استفاده هستند(در مقابل جایی که شبکه ندارند)احتمال وقوع رخدادهای امنیت شبکه بسیار است و اثرات جدی مضر کسب و کار بیشتری از آن نتیجه‌می‌شوند. علاوه بر این با اتصال شبکه‌ها به سازمان‌های دیگر، به‌طور خاص مجازات‌های قانونی قابل توجهی می‌تواند در ارتباط با رخدادهای امنیت وجود داشته‌باشد.

بنابراین سازمانی با اتصالات شبکه، باید نقشه‌ی مدیریت و زیرساخت مرتبط با رخداد امنیت اطلاعات پیاده‌سازی‌شده و مستندشده‌ی خوبی در مکانی داشته‌باشد تا قادر به پاسخگویی سریع به محض شناسایی رخدادهای امنیت باشد، اثر آنها کمینه شود و به‌خاطر پیشگیری از وقوع مجدد رخداد، از آن درس گرفته‌شود. این نقشه باید قادر به نشان دادن هم رویدادهای امنیت اطلاعات (رخدادهای شناسایی‌شده‌ی سامانه، خدمت یا وضعیت شبکه که امکان نقض خط‌مشی امنیت اطلاعات یا خرابی محافظت‌کنندگان امنیت، یا وضعیت ناشناخته‌ی قبلی که ممکن است مرتبط با امنیت باشد)، و هم رخدادهای امنیت اطلاعات (رویدادهای امنیت اطلاعات ناخواسته یا غیرقابل انتظار تکی یا سری رویدادهایی که احتمال بسیار زیاد به خطرافتادن کارکرد کسب و کار و تهدید امنیت اطلاعات را دارند). جزییات بیشتر در مورد مدیریت رخداد امنیت اطلاعات در ISO/IEC 27035 فراهم‌شده‌است.

۸-۲-۳ نقش‌ها و مسؤولیت‌های امنیت شبکه

نقش‌ها و مسؤولیت‌هایی که باید با مدیریت امنیت شبکه تعریف شوند، در ادامه آمده‌اند. (توجه داشته باشید که بسته به اندازه‌ی سازمان، این نقش‌ها می‌توانند ترکیب شوند.)

مدیریت ارشد

- تعریف اهداف امنیت سازمان
- آغاز، بهبود، انتشار و وضع‌کردن خط‌مشی امنیتی سازمان،رویه‌ها و نقش‌ها
- آغاز، بهبود، انتشار و وضع‌کردن خط‌مشی مورد قبول در حال استفاده
- حصول اطمینان از اینکه خط‌مشی‌های موردقبول در حال استفاده و امنیت اجرا شده‌اند

یادآوری- مدیریت ارشد، صاحبان کسب و کار را دربرمی‌گیرد.

مدیریت شبکه

- توسعه‌ی جزییات خط‌مشی امنیت شبکه
- پیاده‌سازی خط‌مشی امنیت شبکه
- پیاده‌سازی خط‌مشی مورد استفاده‌ی قابل قبول
- مدیریت واسط ذی‌نفعان خارجی / فراهم‌کنندگان خدمت خارجی برای حصول اطمینان از تطابق با خط‌مشی‌های امنیت شبکه‌ی داخلی و خارجی
- حصول اطمینان از این‌که در جای خود، مسوولیت عملیاتی شبکه‌ها جدا از مسوولیت عملیاتی رایانه‌هاست

تیم امنیت شبکه

- تعیین، توسعه، آزمون، بررسی و نگهداری ابزار و اجزای امنیت شبکه
- نگهداری ابزار و اجزای امنیت شبکه برای پیگیری متقابل تهدیدها(به‌طور مثال به‌هنگام‌سازی کدهای مخرب(شامل ویروس) پرونده‌های امضا)،
- به‌هنگام‌سازی پیکربندی‌های مربوط به امنیت شبکه (به‌طور مثال فهرست‌های کنترل دسترسی) بر حسب نیازهای در حال تغییر کسب و کار

سرپرستان شبکه

- نصب، به‌هنگام‌سازی، استفاده و حفاظت از خدمات و اجزای امنیت شبکه
- انجام وظایف روزانه‌ی مورد نیاز برای اعمال ویژگی‌های امنیت شبکه، قواعد و پارامترهای مورد نیاز معتبر توسط خط‌مشی‌های امنیت شبکه
- انجام اقدام مناسب برای اطمینان در مورد حفاظت از اجزای امنیت شبکه (مانند پشتیبان‌ها، پایش فعالیت‌های شبکه، پاسخگویی به رخدادهای امنیتی یا هشدارها وغیره)

کاربران شبکه

- گفتگو درباره‌ی الزامات امنیتی‌شان
- تطابق با خط‌مشی امنیت شرکت
- تطابق با خط‌مشی‌های استفاده‌ی قابل قبول از منابع شبکه
- گزارش کردن رویدادها و رخدادهای امنیتی شبکه
- فراهم‌کردن بازخورد اثربخشی امنیت شبکه

ممیزان (داخلی و/یا خارجی)

- بازنگری و ممیزی(به‌طور مثال آزمون دوره‌ای اثربخشی امنیت شبکه)
- وارسی تطابق با خط‌مشی امنیت شبکه
- وارسی و آزمون سازگاری عملکرد قواعد امنیت شبکه با الزامات کسب و کار جاری و محدودیت‌های قانونی(به‌طور مثال فهرست‌های مجاز برای دسترسی‌های شبکه)

۸-۲-۴ پایش شبکه

پایش شبکه قسمت بسیار مهمی از مدیریت امنیت شبکه است. این قسمت با بند ۸-۵ زیر مرتبط است.

۸-۲-۵ ارزیابی امنیت شبکه

امنیت شبکه مفهومی پویاست. کارکنان امنیت باید با گسترش در این زمینه به‌هنگام باشند و اطمینان یابند که شبکه‌ها با وصله‌های امنیتی در دسترس از طرف فروشندگان به کار خود ادامه‌می‌دهند.

این مراحل برای ممیزی کنترل‌های امنیتی موجود در کنار معیارهای آزمون امنیت، پویش آسیب‌پذیری و غیره باید به‌طور دوره‌ای انجام شوند. امنیت باید نقطه توجه اصلی در ارزیابی فناوری شبکه‌ی جدید و محیط شبکه باشد.

۸-۳ مدیریت فنی آسیب‌پذیری

محیط‌های شبکه‌ای مثل سایر سامانه‌های پیچیده، عاری از خطا نیستند. آسیب‌پذیری‌های فنی برای اجزای بیشتر مورد استفاده در شبکه ارائه و انتشار داده‌شده‌اند. بهره‌برداری از این آسیب‌پذیری‌های فنی می‌تواند پیامدهای سختی برای امنیت شبکه‌ها، که اغلب هم در زمینه‌ی دسترس‌پذیری و محرمانگی مشاهده‌می‌شود، داشته‌باشد. بنابراین مدیریت آسیب‌پذیری فنی باید برای پوشش تمام اجزای شبکه ارائه شود و شامل :

- بدست آوردن به‌هنگام اطلاعات درباره‌ی آسیب‌پذیری‌های فنی،
- ارزیابی نقاط ضعف شبکه‌ها در خصوص این آسیب‌پذیری‌ها،
- تعریف کنترل‌های امنیتی مناسب برای نشان‌دادن مخاطرات وابسته، و
- پیاده‌سازی و مقایسه‌ی کنترل‌های امنیتی تعریف‌شده

پیش‌نیاز مدیریت آسیب‌پذیری فنی باید فهرست کاملی از تمام اجزای شبکه‌ی موجود باشد که جزییات فنی حیاتی مثل نوع افزاره، فروشنده، شماره نسخه‌ی سخت‌افزار، ثابت‌افزار یا نرم‌افزار، و هم‌چنین اطلاعات سازمانی مثل افراد اداری مسؤول را فراهم می‌کند.
اگر سازمان، برنامه‌ی مدیریت آسیب‌پذیری فنی کلان را برپاکرده است، راه‌حل ارجح، اعمال مدیریت آسیب‌پذیری فنی شبکه به وظایف کلی سازمان است. (اطلاعات بیشتر در مورد مدیریت آسیب‌پذیری فنی، شامل راهنمای پیاده‌سازی در ISO/IEC 27002 یافت می‌شود.)

۸-۴ شناسایی و احرازهویت

محدود کردن دسترسی کارکنان مجاز از طریق اتصالات، مهم است (خواه داخل خواه خارج از سازمان). برای مثال دستیابی به خدمات مشخصی از شبکه و اطلاعات مربوط که یک خط‌مشی مشترک را لازم دارند، باید برای کارکنان مجاز محدود شود. این نوع الزامات، اختصاص به استفاده ازاتصالات شبکه ندارد و بنابراین جزییات متناسب برای استفاده از شبکه‌ها باید از ISO/IEC 27002 و ISO/IEC 27005 به‌دست‌آیند.
سه زمینه کنترل امنیت که می‌توانند به استفاده از شبکه‌ها و سامانه‌های اطلاعاتی مربوط شوند، در زیر آمده‌اند:
- *ورود از راه دور*- خواه کارکنان مجاز که دور از سازمان کار می‌کنند، خواه مهندسان نگهداری یا کارکنان دیگر سازمان‌ها که با خطوط شماره‌گیری وصل‌شده‌اند یا اتصالات اینترنتی، خطوط اختصاصی از سایر سازمان‌ها یا دسترسی به اشتراک‌گذاشته‌شده از طریق اینترنت. اینها اتصالاتی هستند که برحسب نیاز یا به‌وسیله‌ی سامانه‌های داخلی یا شرکای طرف قرارداد با استفاده از شبکه‌های عمومی برقرارشده‌اند.
هر نوع ورود از راه‌دور باید کنترل‌های امنیتی اضافی متناسب با ذات شبکه‌های متصل شده، داشته باشند. به‌طور مثال ندادن اجازه‌ی دسترسی مستقیم به سامانه‌ها و نرم‌افزار شبکه به حساب‌های کاربری[1] مورد استفاده برای دسترسی راه‌دور، جز در جاهایی که احرازهویت اضافی فراهم‌شده‌باشد. (مطابق با زیر)- و شاید رمزگذاری انتها-به-انتها و محافظت اطلاعات مربوط به نرم‌افزار پست‌الکترونیکی و داده‌های شاخه‌ی[2] ذخیره‌شده در رایانه‌های شخصی و رایانه‌های قابل‌حمل مورد استفاده در دفاتر خارج سازمان با کارکنانش از دسترسی غیر مجاز
- افزایش احرازهویت- در حالی که استفاده از جفت نام کاربری / گذر واژه یک راه ساده برای اصالت سنجی کاربران است اما آنها هم می‌توانند در معرض خطر قرار گیرند یا حدس زده شوند. بنابراین روشهای امن بیشتری برای احرازهویت کاربران باید مورد توجه قرار گیرند به ویژه برای کاربران راه دور و یا زمانی که احتمال زیادی وجود دارد که یک فرد غیر مجاز دسترسی به سامانه‌های مهم و محافظت شده را بدست آورد – مثلا چون که دسترسی ممکن است با استفاده از شبکه های عمومی راه اندازی شده باشد یا دسترسی به سامانه‌ها می‌تواند خارج از کنترل مستقیم سازمان صورت بگیرد (بطور مثال با یک لپ تاپ).

1 - Accounts
2 - Directory

مثال‌های ساده‌ای هستند که از شناساگر خط تماس (CLID[1])استفاده می‌کنند اما چون این برای کلاهبرداری آزاد است نباید به عنوان یک شناساگر(ID) تایید نشده بدون احرازهویت اضافی، مورد استفاده قرارگیرد و پیوندهای ارتباطات از طریق مودم وقتی در حال استفاده نیستند، تنها پس از درستی سنجی هویت تماس گیرنده متصل می‌شوند. مثالهای پیچیده‌تر اما امن‌تر – به ویژه در زمینه دسترسی از راه دور، از مفاهیم دیگر شناسایی برای پشتیبانی احرازهویت کاربران مانند نشانه های مقایسه شده راه دور و کارتهای هوشمند استفاده می‌کنند – و اطمینان حاصل می‌کنند که نشانه یا کارت تنها در ترکیب با کاربران حساب احرازهویت شده مجاز (و بهتر است که کاربران رایانه مخفی و مکان – نقطه دسترسی -)و برای مثال هرPIN یا نمایه زیست‌سنجی بطور کلی ، این احرازهویت قوی دو عاملی بیان شده است.

- *ورود تکی امن* – در جایی که شبکه‌ها کاربرانی دارند که احتمال مواجهه با بررسی چند باره شناسایی و احرازهویت است. در چنین شرایطی کاربران برای اتخاذ شیوه‌های ناامن مانند یادداشت کردن گذرواژه‌ها یا استفاده مجدد همان داده های احرازهویت وسوسه‌می‌شوند. ورود تکی امن، می‌تواند خطرات ناشی از چنین رفتاری را با کم کردن تعداد گذر واژه‌ها یی که کاربران باید به یاد داشته باشند را کاهش دهد.

علاوه بر کاهش خطرات ، بهروه وری کاربران ممکن است بهبود یابد و حجم کار پشتیبان سامانه‌ها[2] در رابطه با بازنشانی گذرواژه‌ها کاهش یابد.

با این حال توجه داشته باشید که پیامدهای شکست سامانه ورود تکی امن می‌تواند شدید باشد. زیرا تنها یک پیامد نیست بلکه بسیاری از سامانه‌ها و برنامه‌های کاربردی در معرض خطر و آزاد برای تشخیص رمز هستند. (گاهی این «شاه‌کلید» خطر، نامیده می‌شود.)

بنابراین سازوکار شناسایی یا اصالت‌سنجی قوی‌تر، از شناسایی و احرازهویت عادی می‌تواند ضروری‌تر باشد و این ممکن است برای حذف شناسایی و اصالت‌سنجی درکارکردهای بسیار ممتاز (در سطح سامانه) از یک روش ورود تکی امن مطلوب باشد.

۸-۵ ثبت ممیزی و پایش شبکه

حصول اطمینان از اثر بخشی امنیت شبکه از طریق ثبت ممیزی و پایش مداوم ، با تشخیص سریع ، بررسی و گزارش از رویدادهای امنیتی و سپس رخدادها و پاسخ به آنها بسیار مهم است. بدون این فعالیت، اطمینان از این‌که کنترل‌های امنیت شبکه همیشه اثر بخش باقی بمانند و رخدادهای امنیتی با اثرات مضر ناشی شده روی عملیات کسب و کار رخ ندهند ، ممکن نخواهد بود.

اطلاعات ثبت ممیزی کافی از وضعیتهای خطا و رویدادهای قابل قبول باید برای فراهم کردن امکان کامل بازنگری رخدادهای مشکوک و واقعی ثبت شوند. به‌هر حال باید تشخیص داد که ذخیره‌کردن حجم زیادی از

1 - Calling Line Identifier
2 - Helpdesk

ممیزی‌های مربوط به اطلاعات می‌تواند مدیریت تحلیل را مشکل‌ساز کند و روی بازدهی اثر بگذارد، بنابراین باید مراقب بود که چه چیزی واقعاً ثبت شده است.

برای شبکه، ثبت ممیزی‌هایی که باید نگهداری شوند شامل انواع رویدادهای زیر هستند:

- تلاش ناموفق برای ورود از راه‌دور به همراه تاریخ و زمان
- رویدادهای ناموفق احرازهویت مجدد(یا کاربرد نشانه[1])
- نفوذها در ترافیک دروازه‌های امنیتی
- تلاش‌های از راه‌دور برای دسترسی به ثبت ممیزی‌ها
- مدیریت هشدارها/آگاهی‌های سامانه به همراه مفاهیم امنیتی(به‌طور مثال تکرار آدرس IP، اختلالات مدار حامل).

در زمینه‌ی شبکه، ثبت ممیزی‌ها باید از تعدادی منابع مانند مسیریاب‌ها، دیواره‌های آتش، سامانه‌های تشخیص نفوذ استخراج شوند و به خدمت‌گزارهای ممیزی مرکزی برای یکپارچگی و تحلیل کامل ارسال شوند. همه‌ی ثبت ممیزی‌هاباید هم در زمان واقعی و هم برون‌خطی بررسی شوند. در زمان واقعی، ثبت‌های ممیزی می‌توانند روی صفحه‌ی غلتشی[2]نمایش داده‌شوند و برای هشدار حملات بالقوه استفاده شوند. تحلیل برون‌خطی چون اجازه می‌دهد تصویر کامل‌تری از روند تحلیل، ارائه شود، ضروری‌است. اولین نشانه‌های حمله می‌تواند این باشد که در ثبت وقایع دیواره‌ی آتش، رد بسته های قابل توجهی وجود داشته باشد که نشان می‌دهد فعالیت‌های کاوشگرانه‌ای علیه یک هدف بالقوه وجود دارد. سامانه‌ی تشخیص نفوذ نیز می‌تواند در زمان واقعی، الگوی حمله را تشخیص دهد.

این امر مورد تاکید است که باید به‌منظور تحلیل و بررسی، نرم‌افزار تحلیل و مدیریت ثبت ممیزی تایید شده‌ی مناسب، برای ثبت ذخیره و بازیابی، قابلیت ردیابی و گزارش‌گیری از ثبت ممیزی‌ها(برای کاربران خاص، برنامه های کاربردی و انواع اطلاعات و با دوره زمانی بویژه وقتی که برای اهداف بازرسی مورد نیاز است) و گزارش گیری با خروجی‌های سریع ، تمرکز یافته و قابل فهم، مورد استفاده قرارگیرد. گزارش‌های تحلیل ثبت ممیزی باید در یک مکان امن نگهداری شوند و برای یک دوره زمانی مورد توافق بایگانی شوند. علاوه برحفاظت شناسایی، اصالت‌سنجی و کنترل دسترسی، محافظتی هم باید برای خود ثبت ممیزی‌ها قرار داده‌شود. پایش مداوم باید در بر گیرنده پوشش موارد زیر باشد.

- ثبت ممیزی از دیواره‌های آتش ، مسیریابها ، خدمت‌گزارها و غیره
- هشدارهای آگاهی از قبیل ثبت ممیزی‌های از پیش پیکربندی شده برای اعلام انواع رویدادهای مشخص
- خروجی سامانه تشخیص نفوذ
- نتایج فعالیتهای پویش امنیت شبکه
- اطلاعات رویدادها و رخدادهای گزارش شده توسط کاربران و کارمندان پشتیبانی ، و
- نتایج بازنگری تطابق امنیت

1 - Token
2 - Scrolling

دنباله‌های[1] ممیزی باید به‌صورت برخط برای دوره‌ای مطابق با نیازهای سازمان با تمام مسیرهای ممیزی پشتیبان‌گیری شده و بایگانی شده به روشی که یکپارچگی و دسترس‌پذیری را تضمین کند، نگهداری شوند، به‌طور مثال با استفاده از رسانه‌های یک بار نوشتنی چندبار خواندنی [2] مانند لوح‌های فشرده[3].

علاوه بر این، ثبت ممیزی‌ها حاوی اطلاعات حساس یا اطلاعاتی هستند که مورد استفاده برای کسانی است که بخواهند از طریق اتصالات شبکه، به سامانه حمله کنند و در اختیارداشتن ثبت ممیزی‌ها می‌تواند در صورت بروز رویداد یک اختلاف، گواهی بر انتقال روی شبکه باشد- و بنابراین به‌ویژه در زمینه‌ی حصول اطمینان از یکپارچگی و سلب انکار ضروری هستند. بنابراین تمام ثبت ممیزی‌ها باید به‌طور مناسب محافظت شوند که شامل زمانی هم که لوح های فشرده‌ی بایگانی شده در زمان برنامه‌ریزی شده، خراب شده‌اند، می‌شود. دنباله‌های ممیزهای باید مطابق با الزامات سازمان و قوانین ملی، برای دوره‌ای به‌طور امن حفظ شوند و هم‌چنین مهم است که وقت هم‌زمان‌سازی به‌درستی برای تمام دنباله‌های ممیزی و خدمت‌گزارهای مربوط، نشان داده‌شود، به‌طور مثال استفاده از پروتکل زمانی شبکه(NTP)[4] ، بویژه برای دادگاه‌ها و احتمال استفاده از آن‌ها در پیگردهای قانونی.

این امر مورد تاکید است که پایش شبکه باید به روشی کاملاً سازگار با قوانین و مقررات ملی و بین‌المللی مربوط انجام شود. این شامل قانون برای محافظت داده‌ها و برای تنظیم قدرت‌های بازرسی است(که توسط قانون همه‌ی کاربران باید از هرگونه پایش، قبل از این‌که انجام شود، آگاه شوند).

در بیان کلی، پایش باید با مسوولیت انجام شود و نباید برای بازنگری رفتار کارکنان در کشورها و با قوانین حریم شخصی خیلی محدود استفاده شود. واضح است که فعالیت‌های انجام گرفته باید سازگار با خط‌مشی‌های حریم شخصی و امنیت سازمان/انجمن باشد و رویه‌ها با مسوولیت‌های مرتبط در جایی قرارداده‌شوند. ثبت ممیزی و پایش شبکه هم‌چنین باید اگر مدرک ثبت ممیزی بخواهد در پیگرد قانونی و کیفری استفاده‌شود با یک روش امن قانونی انجام شود.

بیشتر کنترل‌های مورد نیاز پایش و ثبت ممیزی در رابطه با استفاده از شبکه‌ها و سامانه‌های اطلاعاتی مربوط، می‌توانند با استفاده از ISO/IEC 27002 و ISO/IEC 27005 تعیین شوند.

۸-۶ تشخیص و پیشگیری نفوذ

هم‌چنان‌که استفاده از شبکه‌ها در حال افزایش است، پیدا کردن راه‌های مختلف برای نفوذ به سامانه‌های اطلاعاتی و شبکه‌ی سازمان‌ها یا انجمن آسان‌تر شده‌است. برای پنهان کردن نقطه‌ی آغازی دسترسی و برای دسترسی از طریق شبکه‌ها و سامانه‌های اطلاعات داخلی هدف. علاوه بر این نفوذگرها در حال پیچیده‌تر شدن هستند و روش‌های پیشرفته‌تر حمله و ابزارها به‌سادگی قابل دسترس در اینترنت یا نوشتجات آزاد

1 - Trail
2 - WORM (write once read many)
3 - CD
4 - Network Time Protocol

هستند. در واقع بسیاری از این ابزار به‌طور خودکار هستند و می‌توانند بسیار اثربخش و آسان برای استفاده و از جمله به‌وسیله‌ی افراد با تجربه‌ی محدود هستند.
از نظر اقتصادی برای بیشتر سازمان‌ها، پیشگیری از تمام نفوذهای بالقوه غیرممکن است، در نتیجه برخی نفوذها به احتمال زیاد رخ می‌دهند. مخاطرات مرتبط با بیشتر این نفوذها باید از طریق پیاده‌سازی شناسایی و احرازهویت خوب، کنترل دستیابی منطقی و پاسخگویی و کنترل‌های ممیزی و اگر توجیه داشت، قابلیت‌های تشخیص و پیشگیری نشان‌داده شوند. چنین قابلیت‌هایی وسیله‌ای فراهم می‌کنند که نفوذها را پیش‌بینی کنند. نفوذها را در زمان واقعی شناسایی کنند و هشدارهای مناسب را افزایش دهند و از نفوذها پیشگیری کنند. این‌کار هم‌چنین مجموعه اطلاعات محلی نفوذ و یکپارچگی بعدی و تحلیل را به علاوه‌ی تحلیل الگوهای رفتاری/کاربردسامانه‌ی اطلاعات معمولی سازمان، فراهم می‌سازد.
سامانه‌ی تشخیص نفوذ باید به تمام ترافیک ورودی شبکه‌های داخلی برای شناسایی این‌که قصد نفوذی انجام شده‌است، در حال رخدادن است یا رخداده‌است و نفوذها پاسخ دهد، علاوه بر این‌که به کارکنان هشدار دهد. دو نوع سامانه‌ی تشخیص نفوذ وجود دارد:

- NIDS(Network IDS) - که بسته‌های شبکه را پایش می‌کند و برای پوشش(تشخیص) دادن نفوذگر با تطبیق دادن الگوی حمله با بانک اطلاعاتی از الگوهای شناخته‌شده‌ی حمله، تلاش می‌کند. و
- HIDS(Host IDS) - که فعالیت‌های روی میزبان‌ها(خدمت‌گزارها) را توسط پایش ثبت رویدادهای امنیتی یا بررسی تغییرات روی سامانه مانند تغییرات روی پرونده‌های سامانه‌های حیاتی یا رجیستری سامانه پایش می‌کند.

سامانه‌ی پیشگیری از نفوذ، تمام ترافیک را قبل از این‌که به سمت شبکه‌ی داخلی گذرکند، بررسی می‌کند و به‌طور خودکار تمام حملات تشخیص داده‌شده را مسدود می‌کند، به‌عبارت دیگر و سامانه‌ی پیشگیری از نفوذ به‌طور مشخصی برای فراهم کردن قابلیت پاسخگویی فعال طراحی شده‌است.
جزییات راهنمایی برای تشخیص و پیشگیری از نفوذ در ISO/IEC 18043 آورده‌شده‌است.

۸-۷ محافظت در برابر کد مخرب

کدمخرب(ویروس، کرم‌ها، تروجان‌ها، جاسوس‌افزار و غیره که مجموعاً بدافزار نامیده‌می‌شوند) می‌تواند از طریق اتصالات شبکه وارد شود. کد مخرب می‌تواند باعث شود کامپیوتر کارکردهای غیرمجازی (به‌طور مثال بمباران هدفی مشخص با پیام‌ها در زمان و تاریخی مشخص) انجام‌دهد، یا در واقع منابع حیاتی را خراب کند(به‌طور مثال حذف پرونده‌ها) . بدافزار به محض اینکه کپی شود، سعی در یافتن میزبان‌های نفوذپذیر دیگر می‌کند. کد مخرب نمی‌تواند قبل از اینکه خرابی به بارآید، تشخیص داده‌شود، مگر اینکه کنترل‌های مناسب پیاده‌سازی شده‌باشند. کدمخرب ممکن است باعث به خطرافتادن(تشخیص رمز) کنترل‌های امنیتی (به‌طور مثال گرفتن و افشای گذرواژه)، افشای ناخواسته‌ی اطلاعات، تخریب اطلاعات، و/یا استفاده‌ی غیرمجاز از منابع سامانه باشد.

بعضی از قالب‌های کدمخرب باید توسط نرم‌افزار پویش مخصوص شناسایی و حذف شوند. پویشگرها برای دیواره‌های آتش، خدمت‌گزارهای پرونده[1]، خدمت‌گزارهای پیام‌رسان، و رایانه‌های شخصی[2]/ایستگاه‌های کاری برای برخی انواع کدهای مخرب دسترس‌پذیر هستند.

به‌علاوه برای توانایی تشخیص کدهای مخرب جدید، اطمینان از اینکه نرم‌افزار پویش همیشه از طریق به‌هنگام‌سازی روزانه، به هنگام نگه‌داشته‌شوند، خیلی مهم است. به‌هرحال کاربران و سرپرستان باید آگاه باشند که به پویشگرها نمی‌توان برای تشخیص تمام کدهای مخرب (یا نوع خاصی از کدهای مخرب) اتکاکرد، زیرا قالب‌های جدید کدهای مخرب به‌طور مداوم به‌وجود می‌آیند. به‌طور معمول قالب‌های دیگر از کنترل برای تشدید حفاظت فراهم‌شده توسط پویشگرها مورد نیاز است(جایی که وجود دارند)

به‌طور کلی این وظیفه‌ی نرم‌افزار ضد کدمخرب است که داده‌ها و برنامه‌ها را برای شناسایی الگوهای مشکوک مربوط به بدافزار پویش کند. کتابخانه‌ی الگوها برای اینکه به عنوان امضاها شناخته‌شده‌است، پویش می‌شود و باید در فاصله‌های زمانی منظم یا هر زمان امضاهای جدید برای هشدارهای بدافزار با خطر بالا دسترس‌پذیر شدند، به‌هنگام شوند. در زمینه‌ی دسترسی از راه‌دور، نرم افزار ضد کدمخرب باید در سامانه‌های راه‌دور و هم‌چنین خدمت‌گزارهای سامانه‌ی مرکزی- به‌ویژه ویندوز و خدمت‌گزارهای پست الکترونیکی[3].

کاربران شبکه و سرپرستان باید در رابطه با نرم‌افزار مشکوک موقعی که با طرف‌های خارجی و با پیوندهای بیرونی در دادوستد هستند، هوشیارباشند که خطراتی بزرگ‌تر از مخاطرات عادی مربوط به آن وجود دارند. راهنماهای کاربران و سرپرستان باید به‌صورت رویه‌های ترسیم‌شده وتجربیاتی برای کمینه‌کردن امکان به وجود آوردن کدهای مخرب توسعه داده‌شود.

کاربران و سرپرستان باید برای پیکربندی سامانه‌ها و برنامه‌های کاربردی مرتبط با اتصالات شبکه دقت ویژه کنند تا کارکردهایی را که در شرایط محیط ضروری نیستند، غیرفعال کنند، برای مثال برنامه‌های کاربردی رایانه‌ی شخصی میتوانند چنان پیکربندی شوند که ماکروها به‌طور پیش‌فرض غیرفعال باشند یا قبل از اجرای ماکروها، تایید کاربر لازم باشد. جزییات بیشتر در مورد محافظت در برابر کدهای مخرب در ISO/IEC 27002 و ISO/IEC 27005 آورده‌شده‌است.

یادآوری- ISO/IEC 11889، فناوری را که به‌طور وسیعی در رسانه‌های خدمت‌گزار و مشتری، توسعه‌داده‌شده و می‌تواند برای تشخیص و جداسازی کدهای مخرب یا منابع ناشناس استفاده شود، توصیف می‌کند.

1- File Servers
2 - PCs
3 - E-mail Servers

۸-۸ خدمات مبتنی بر رمزنگاری

جایی که حفظ محرمانگی مهم است، کنترل‌های رمزنگاری باید برای رمزکردن اطلاعات درحال عبور از شبکه‌ها مورد توجه قرارگیرند. جایی‌که حفظ یکپارچگی مهم است، امضاهای دیجیتال و/یا کنترل‌های پیام یکپارچگی باید برای محافظت اطلاعاتی که روی شبکه عبور می‌کنند، مورد توجه‌قرارگیرند.

کنترل‌های امضای دیجیتالی نه‌تنها می‌توانند حفاظت یکسانی از کنترل های پیام احرازهویت به‌عمل‌آورند، بلکه ویژگی‌هایی هم دارند که به آنها اجازه‌ی فعال‌سازی رویه‌های سلب انکار را می‌دهند.

در جایی‌که الزاماتی برای حصول اطمینان از اینکه دلیل اساسی می‌تواند ارائه شود که اطلاعات توسط شبکه منتقل شده باشند (سلب انکار) کنترل‌هایی مانند آن‌چه در پی می‌آیند، باید مورد توجه‌قرارگیرند:

- پروتکل‌های ارتباطی که تایید تحویل را فراهم‌کنند،
- پروتکل‌های کاربردی که نشانی‌های آغازکننده یا شناسایی‌کننده‌ای را نیاز دارند، فراهم باشد تا وجود این اطلاعات را بررسی کنند.
- دروازه‌هایی که قالب‌های آدرس فرستنده و گیرنده را برای صحت دستورات و سازگاری با اطلاعات در شاخه های مرتبط بررسی می‌کند.
- پروتکل هایی که تحویل از شبکه‌ها را تایید می‌کند و اجازه می‌دهند تا ترتیب اطلاعات تعیین شود.

این مهم است که اگر اعتراضی در مورد انتقال یا دریافت اطلاعات هست، بتوان اثبات نمود(قالب دیگری از انکارخدمت). اطمینان بیشتر باید از طریق استفاده از روش امضای دیجیتال استاندارد، فراهم شود. تصمیم برای استفاده از رمزنگاری، امضای دیجیتال، یکپارچگی پیام یا سایر کنترلهای مبتنی بر رمزنگاری باید بر اساس حساب‌های مربوط به قوانین دولتی و تنظیمات و هم چنین زیر ساخت کلید عمومی مناسب ، الزامات مدیریت کلید، مناسب بودن ساز و کارهای زیر بنایی مورد استفاده برای انواع شبکه دخیل و درجه حفاظت مورد نیاز وثبت نام قابل اعتماد و قابل اطمینان کاربران یا نهادهای مرتبط یا کلیدهای (گواهی شده در جای مربوط)مورد استفاده در پروتکل‌های امضای دیجیتال، گرفته‌شود.

ساز و کارهای رمزنگاری در ISO/IEC 18033 استانداردسازی شده‌اند. یک فن رمزنگاری مشترک که به‌طورمعمول استفاده می‌شود به عنوان رمز بلوک شناخته می‌شود و روشهای استفاده از رمزهای بلوک برای محافظت رمزنگاری به عنوان حالتهای عملیات[1] شناخته می‌شوند در ISO/IEC 10116 استاندارد سازی شده‌است. کنترل‌های یکپارچگی پیام ، به عنوان احراز هویت کدها شناخته می‌شوند (یا MAC ها) در ISO/IEC 9797 استاندارد سازی شده اند. فنون امضای دیجیتال در ISO/IEC 9796 وISO/IEC 14888 استانداردسازی شده‌اند. اطلاعات بیشتر در مورد عدم انکار در ISO/IEC 14516 و ISO/IEC 13888 آمده‌است. مدیریت کلید، به عنوان یک خدمت پایه برای تمام خدمات رمزنگاری دیگر اطمینان می‌دهد که تمام کلیدهای رمزنگاری در طول کامل شدن چرخه حیاتشان مدیریت شده‌اند و با یک روش امن

1 - Modes of Operation

استفاده‌شده‌اند. برای اطلاعات در مورد مدیریت کلید ، و موضوعات مرتبط مانندPKI یا موضوعات بیشتر شامل مدیریت شناسایی مرجع باید به سایر مستندات و استانداردهای زیر ارجاع شود.

- ISO/IEC 11770 (مدیریت کلید)
- ISO/IEC 9594-8 (دایرکتوری:کلید عمومی و چارچوب‌های گواهی صفت)
- ISO 11166-2 (بانکی، مدیریت کلید با استفاده از الگوریتم نامتقارن)
- ISO 11568 (بانکی‌ها – مدیریت کلید جزء)
- ISO 11649 (خدمات مالی – مرجع بستانکارساخت یافته برای اطلاعات پرداخت)
- ISO 13492 (اجزای داده ای مدیریت کلید خرد)
- ISO 21118 (زیرساخت کلید عمومی بانکی)

توجه داشته باشید که رمزنگاری باید هم‌چنین برای مدیریت افزاره‌های شبکه استفاده شود. به علاوه دسترسی و فایلهای ثبت مدیریت شبکه باید برای حفظ داده‌های حساس در جلسات رمزنگاری‌شده‌ی امن انتقال‌یابند.

۸-۹ مدیریت تداوم کسب و کار

این مهم است که کنترل‌ها در مکانی باشند که برای تداوم کارکرد کسب و کار در رویدادهای حوادث طبیعی توسط فراهم آوردن قابلیت بازیابی هر قسمت از کسب و کار پس از اختلال در یک چار چوب زمانی مناسب اطمینان دهند، بنابراین سازمان باید برنامه مدیریت تداوم کسب و کار را در مکانی با فرآیندهایی که مراحل تداوم کسب و کار را نیز بپوشاند داشته باشد – بازنگری تحلیل پیامد کسب و کار ،بازنگری ارزیابی مخاطره ، برقراری الزامات بازیابی کسب و کار ،تدوین راهکار تداوم کسب و کار ،تولید طرح تداوم کسب و کار،آزمون طرح تداوم کسب و کار حصول اطمینان از آگاهی تداوم کسب و کار برای تمام کارکنان نگهداری مداوم طرح تداوم کسب و کار و کاهش مخاطره.

تنها با پیگیری تمام مراحل زیر می‌توان اطمینان حاصل شود.

- اولویت‌های مورد نیاز کسب و کار و مقیاسهای زمانی در مسیر نیازهای کسب و کار هستند.
- گزینه‌های ارجح مشخص راهکار تداوم کسب و کار، مناسب با این اولویت‌ها و بازه‌های زمانی هستند و بنابراین
- طرح‌ها و امکانات صحیح و لازم درست در جای خود قرار داده شده‌اند، شامل اطلاعات، فرآیندهای کسب و کار سامانه‌های اطلاعاتی و خدمات ارتباطات صدا و داده‌ای ، مردم و امکانات فیزیکی

راهنمای مدیریت تداوم کسب و کار بطور کامل شامل توسعه یک راهکار تداوم کسب و کار و طرح‌های مربوط و آزمون بعدی می‌تواند از ISO/PAS 22399:2007 به‌دست آید.

از نقطه نظر شبکه این راهنما، برای نگهداری اتصالات شبکه، پیاده سازی اتصالات جایگزین با ظرفیت کافی و بازیابی اتصالات بعد از رویدادهای ناخواسته است. این جنبه‌ها و الزامات باید بر درجه اهمیت اتصالات به

کارکرد کسب و کار در طول زمان و اثرات مضر کسب و کار در رویداد اختلالات بنا نهاده شوند. در حالی که اتصال می‌تواند مزایای بسیاری برای سازمان به همراه داشته باشد، وقوع یک اختلال در انعطاف پذیری و بهره‌مندی از نظرات خلاق، می‌تواند نقاط آسیب پذیر و «نقاط تکی شکست » را که می‌تواند پیامدهای مخل عمده در سازمان داشته باشد بازنمایی کند.

۹ راهنمایی هایی برای طراحی و پیاده سازی امنیت شبکه

۹-۱ پیش‌زمینه

این بند، جنبه‌های مختلف معماری/طراحی فنی امنیت شبکه و زمینه‌های کنترل بالقوه مرتبط را نشان می‌دهد. بند ۱۰ مخاطره، فنون طراحی و زمینه‌ی کنترل امنیت را برای سناریوهای مرجع شبکه معرفی می‌کند. بند ۱۱ مخاطره، فنون طراحی و مسایل کنترل امنیت، به‌ویژه «فناوری» را که موضع نگرانی سازمان‌های امروزی است، معرفی می‌کند. در واقع یک راه‌حل ویژه‌ی امنیت شبکه، می‌تواند شماری از موضوعات و زمینه‌های کنترل معرفی‌شده در بندهای ۱۰ و ۱۱ را دربرگیرد. جدولی در پیوست ب نشان داده شده‌است که ارجاع متقابل بین کنترل‌های مرتبط امنیت شبکه‌ی ISO/IEC 27001/27002 و این استاندارد ملی را نشان می‌دهد.

به‌دنبال بندهای ۸ تا ۱۱ (و پیوست الف) معماری/طراحی فنی امنیت پیشنهادی و فهرستی از کنترل‌های شناسایی شده باید به‌طور کامل در زمینه‌ی معماری‌ها و برنامه‌های کاربردی مربوط به شبکه، بازنگری شوند. معماری و فهرست کنترل‌ها سپس باید در صورت لزوم تنظیم شوند و پس از آن به‌عنوان پایه‌ای برای توسعه، پیاده‌سازی و آزمون راه‌حل‌های فنی امنیت استفاده‌شوند(مطابق با بند ۱۲ زیر). سپس، بعد از این‌که معماری فنی امنیت و در نتیجه پیاده‌سازی کنترل امنیت امضاشده بودند، باید عملیات برخط (مطابق با بند ۱۳زیر) با پایش مداوم و بازنگری پیاده‌سازی شروع شود. (مطابق با بند ۱۴ زیر)

۹-۲ معماری/طراحی فنی امنیت شبکه

مستندسازی معماری/طراحی فنی امنیت ممکن و گزینه‌های پیاده‌سازی ،روش‌هایی را برای آزمایش راه‌حل‌های مختلف و پایه‌ای برای تجزیه و تحلیل‌های تجاری فراهم می‌کند. این عمل تحلیل مسائل مربوط به محدودیت های فنی، و مجادلات بین الزامات کسب و کار و امنیت را، که اغلب بوجود می‌آیند، تسهیل می‌بخشد.

در مستند سازی گزینه‌ها، حساب کاربری باید برگرفته از الزامات خط‌مشی امنیت اطلاعات هر شرکت (مطابق با بند۷-۲-۱)، معماری مناسب شبکه، برنامه‌های کاربردی، سرویس ها، نوع اتصالات و خصوصیات دیگر (به بند ۷-۲-۲ مراجعه شود)، و فهرستی از کنترل های بالقوه شناسایی شده توسط ارزیابی مخاطرات امنیتی و بررسی مدیریت باشد(به بند ۷-۳ مراجعه شود). در اجرای این طرح، حساب کاربر باید برگرفته از معماری/طراحی فنی امنیت موجود باشد. زمانی‌که گزینه‌ها سندسازی و بازنگری می‌شوند، به عنوان قسمتی از فرآیند طراحی معماری فنی، معماری امنیتی برگزیده باید در سند کنترل مشخصات معماری/طراحی فنی

امنیت مستند شود. (این عمل با طراحی معماری فنی و برعکس سازگار است). درنتیجه، تغییراتی در معماری شبکه، نرم افزارهای کاربردی و سرویس‌ها می‌تواند صورت گیرد، (جهت اطمینان حاصل کردن از سازگاری با معماری/طراحی فنی امنیت برگزیده‌شده) و یا فهرستی از کنترل های بالقوه تهیه شود. (برای مثال: از آنجایی که توافق شده‌است که معماری/طراحی امنیتی تنها می‌تواند به صورت فنی و با یک روش خاص اجرا شود، نیازمند جایگزینی یک شناسه کنترلی دارد.)

توجه داشته باشید که ISO/IEC 27033-2 چگونگی دست‌یابی به کیفیت معماری‌ها/طراحی‌های فنی امنیت را برای سازمان‌ها تعریف می‌کند که از امنیت شبکه برای محیط های کسب وکارشان، با استفاده از یک رویکرد منسجم برای برنامه‌ریزی، طراحی و پیاده‌سازی امنیت شبکه اطمینان حاصل کنند.

ورودی فرآیند توسعه معماری/طراحی فنی امنیت شبکه، همان طور که در ISO/IEC 27033-2 تعریف شده است شامل:

- اسناد خدماتی مورد نیاز سازمان/ انجمن
- سند معماری ، طراحی و یا پیاده‌سازی موجود و یا برنامه ریزی شده
- خط‌مشی امنیت شبکه فعلی (و یا قسمت های مرتبط با اطلاعات خط‌مشی امنیتی سامانه)- که ترجیحاً بر اساس نتایج ارزیابی مخاطره امنیتی و نظارت مدیریت است)
- تعریف دارایی‌هایی که باید محافظت شوند
- الزامات عملکرد فعلی و برنامه ریزی شده، از جمله ترافیک مربوطه
- اطلاعات محصول فعلی

خروجی فرآیند طراحی شامل:

- سند معماری/طراحی فنی امنیت شبکه
- مستندات الزامات دسترسی خدمت (امنیت) ،برای هریک از سامانه‌های امنیتی دروازه/دیواره‌ی آتش (که شامل قانون یا قوانین پایه‌ای دیواره‌ی آتش است)
- روالهای عملیات امنیتی (SecOPs)
- مربوط به شرایط اتصالات امن شبکه برای طرف سوم
- مربوط به راهنماهای کاربر برای کاربران طرف سوم

سند معماری/طراحی امنیت شبکه با جزئیات در ISO/IEC 27033-2 توصیف شده است، که شامل الگوی نمونه‌ای برای اسناد مورد نیاز خدمات دسترسی (امنیت) در پیوست د (از ISO/IEC 27033-2)می‌باشد. اطلاعات بیشتر در مورد اسناد ارجاع داده شده را می توان در بند ۸-۲-۲ بالا و همچنین در ISO/IEC 27033-2 یافت.

(علاوه‌براین، زمانی‌که معماری/طراحی فنی امنیت شبکه مستندسازی و اجرا شد، سپس باید برنامه‌های آزمایشی امنیتی ساخته و آزمون های امنیتی اجرا شوند. زمانی‌که نتایج قابل قبولی از این آزمون‌ها با اعمال هرگونه تغییرات برای مشکلات کوچکی که در طول آزمایش پدید آمد، گردآوری شد سپس امضای رسمی مدیریتی برای معماری/طرح فنی امنیت شبکه و تکمیل عملیات اجرایی باید صورت‌گیرد. (مطابق با بند ۱۲) اطلاعات هر یک از عملیات زیر درISO/IEC 27033-2 ارائه شده‌اند. (در نتیجه در اینجا تکرار نمی‌شوند):

- آمادگی برای طراحی فنی و پیاده‌سازی امنیت شبکه:
  - شروع پروژه امنیت شبکه
  - تایید نیازمندی های شبکه وسیع سازمان/انجمن
  - بازنگری معماری فنی و پیاده‌سازی موجود و یا برنامه ریزی شده (تمام معماری‌ها و پیاده‌سازی های فنی موجود و یا برنامه ریزی شده باید توصیف و بررسی شوند که با الزامات و نیازهای عملی سازمان/انجمن مطابقت دارند یا خیر(-موارد قبلی مشاهده شود)
  - شناسایی و تایید دارایی ها
  - تایید ارزیابی مخاطرات امنیتی و نتایج مدیریتی، و بازنگری کنترل‌های امنیتی شبکه‌ی موجود و یا برنامه‌ریزی شده در چارچوب همان نتایج و انتخاب کنترل بالقوه امنیت.
  - بازنگری نیازمندی‌های عملکرد شبکه و تایید ضوابط(نیازمندی‌های عملکرد شبکه احتیاج به بازنگری و بررسی دارد و معیارهای عملکرد باید با معماری فنی و معماری/طراحی فنی امنیتی مربوطه به‌طور رسمی مطابق باشد.)
  - طرح فنی امنیت شبکه، شامل پوشش تمام مباحث فنی قابل اجرا می‌باشد (با عنوان‌های ISO/IEC 27001:2007 بررسی شود)، و:
  - استفاده از راهنمای «سناریو» و «فناوری» (که در ISO/IEC 27033-3 تا 27033-6 ارائه شده است) (همچنین بند ۱۰ و ۱۱ مشاهده گردد.)
  - استفاده از مدل‌ها/ چارچوب‌ها (شامل ITU-T X. 805 و غیره)
  - انتخاب محصول (که باید به عنوان یک فرآیند مکررمرتبط با طراحی معماری فنی امنیت شبکه اجرا شود و به‌طور مجزا انجام نشود، و باید بر اساس عوامل متعددی باشد(شامل سازگاری فنی، عملکرد، قابلیت توسعه، امکانات مدیریت، امنیت منطقی، و البته قابلیت فروشنده، پیگردی سوابق و غیره. . .)
  - اثبات مفاهیم(تعهد اثبات مفهوم در جایی که معماری فنی امنیت شبکه و مجموعه محصولات مربوط به آن در مکانی قرار نگرفته اند و یا مجموعه خدمات پیچیده ای پیش‌بینی شده است توصیه می‌شود. (اذعان به این که محصولات همیشه با داده‌های ارائه شده توسط فروشنده مطابقت ندارد!)
  - تکمیل معماری/طراحی فنی امنیت شبکه و اسناد مرتبط
- آماده شدن برای انجام آزمون (یک سند راهبردی آزمون امنیتی باید در حالی ساخته شود که رویکردی را که در آزمایش به منظور اثبات معماری فنی امنیت شبکه صورت گرفته است، توصیف می‌کند، در درجه اول برچگونگی آزمایش کلیدهای کنترل فنی امنیتی باید تمرکز کند. سپس طرح آزمون باید برای معماری فنی امنیت شبکه توسعه یابد، که شامل جزئیات بیشتری در مورد آزمون‌هایی که باید انجام شود، توسط چه کسی و در چه مکانی، می‌شود.
- امضای رسمی معماری فنی امنیت شبکه

اصول کلی طرح (مواردی که در بیشتر و نه همه موارد روی می‌دهد) در ISO/IEC 27033-2 ارائه شده‌است. علاوه بر این، باید به پیوست‌های ISO/IEC 27033-2 مانند مدل/چارچوب[1] (معماری «مرجع») برای امنیت شبکه، مدل/چارچوب مورد مطالعه، به الگو نمونه مستندات رجوع شود.
تاکید می‌شود که معماری/طراحی فنی امنیت برای هر پروژه باید قبل از نهایی نمودن فهرست کنترل‌های امنیتی برای پیاده‌سازی، به‌طورکامل مستندسازی و تایید شود.

۱۰ مرجع سناریوهای شبکه، مخاطرات، طراحی، فنون و مسائل کنترل

۱۰-۱ مقدمه

قسمت سوم از خانواده استاندارد ISO/IEC 27033 مخاطرات، طراحی ، فنون و مسائل مربوط به کنترل را همراه با مرجع طرح‌های شبکه توصیف می‌کند. نمونه هایی از این طرح‌ها در بند های ۲-۱۰ تا ۱۰-۱۰ در ادامه شرح داده شده است. قسمت سوم راهنمایی دقیقی بر روی مخاطرات امنیتی و فنون طراحی ایمن و کنترل‌های لازم برای کاهش این مخاطرات را در تمام حالات خاص بیان می‌کند.

۱۰-۲ خدمات دسترسی به اینترنت برای کارمندان

امروزه تقریبا همه سازمان‌ها خدمات دسترسی به اینترنت را برای کارمندان خود فراهم می‌کنند، و در ارائه این خدمات باید دسترسی را به منظور شناسایی دقیق مجوزها و نه به صورت دسترسی عمومی آزاد،در نظربگیرند. در یک خط‌مشی مشخص باید تعریف شود که کدام یک از سرویس‌ها و به چه اهدافی باید ارائه شوند. دسترسی به اینترنت معمولا برای اهداف تجاری اجازه داده می‌شود و با توجه به خط‌مشی، دسترسی به اینترنت سازمان برای اهداف خصوصی نیز (به طور معمول به صورت محدود) مجاز است. باید توجه شود که کدام یک از سرویس‌ها مجاز به استفاده هستند – آیا سرویس‌های پایه‌ای www (مانندhttp و https) هستند، آیا تنها بازیابی اطلاعات مجاز است و/یا کارمندان مجاز به شرکت در کانال‌های گپ‌زنی و انجمن‌ها و غیره می‌باشند، آیا خدمات همکاری پیشرفته مجاز هستند- اگر به این صورت باشد، آن‌ها مجموعه مخاطرات احتمالی خود را که مربوط به یک سناریوی خاص است، معرفی کرده‌اند.
مبانی اولیه باید تنها شامل سرویس‌هایی شود که در برگیرنده‌ی خدمات مجاز نیازهای تجاری می‌شود، اما معمولا عملیات تجاری نیازمند استفاده از سرویس‌هایی هستند که با مخاطرات امنیتی بیشتری همراه است. حتی زمانی که خط‌مشی محدودی به کارگرفته می‌شود، خدمات دسترسی به اینترنت برای کارمندان، مخاطرات امنیتی قابل توجهی را به همراه دارد.

---

۱ - (در متن استاندارد ISO/IEC 27033) برای ارائه یا توصیف نمایش ساختار و عملکرد سطح بالای یک معماری/طراحی فنی امنیت استفاده می‌شود.

۱۰-۳ خدمات همکاری پیشرفته

خدمات همکاری پیشرفته (مانند پیام های فوری - گپ زدن، کنفرانس ویدئویی و محیط های اشتراک گذاری مستندات) که ارتباطات متنوع و امکانات به اشتراک گذاری مستندات را در هم ادغام می‌کند، در محیط های تجاری امروز بیش از بیش اهمیت پیدا می‌کنند. چنین خدمات سازمانی معمولا تلفن ویدئویی، ارتباطات صوتی از طریق کانال های گپ زنی، سامانه‌های پست الکترونیکی و همچنین به اشتراک گذاری اسناد و محیط های همکاری مشترک بر خط را در هم ادغام می‌کنند. دو راه اصلی برای چگونگی استفاده از این خدمات برای یک سازمان وجود دارد :

از آن‌ها تنها به عنوان خدمات داخلی استفاده شود، اما با این مشکل که این خدمات غیر قابل استفاده با شرکای خارجی هستند.

از آنها به عنوان خدمات داخلی و خدمات خارجی به یک سازمان استفاده شود. این عمل فواید بیشتری از استفاده این نوع خدمات را ارائه می دهد، اما ضمنا مخاطرات امنیتی مرتبط بیشتری در مقایسه با استفاده داخلی دارد.

با توجه به پیاده‌سازی، خدمات می‌توانند به صورت خانگی، و یا فقط به عنوان یک سرویس خریداری شده از یک شخص سوم اجرا شوند. در خیلی از موارد که تنها خدمات خانگی استفاده می‌شوند، پیاده‌سازی به احتمال زیاد در داخل خانه خواهد بود. اگر خدمات به صورت داخلی و خارجی استفاده شوند، آنگاه خرید خدمات سازمانی از یک شخص سوم می‌تواند بهترین راهکار باشد. مخاطرات امنیتی و مشاوره در مورد تکنیک های طراحی امنیتی و کنترل کاهش آن مخاطرات در استفاده های داخلی،و داخلی و خارجی شرح داده می‌شوند.

۱۰-۴ خدمات کسب و کار به کسب و کار

کسب و کار سنتی در خدمات کسب و کار با استفاده از خطوط استیجاری اختصاصی یا قسمت‌هایی از شبکه اجرا شده است. اینترنت و فناوری‌های مشابه آن گزینه‌های بیشتری را فراهم می‌آورند، اما مخاطرات امنیتی جدید مرتبط با پیاده‌سازی این نوع خدمات را به همراه دارند. به طور معمول کسب و کار در خدمات تجاری نیازمندی های مخصوص خود را دارد. برای مثال،در دسترس بودن و قابل اعتماد بودن از نیازهای اساسی اکثر سازمان‌هایی است که کارشان به‌طور مستقیم وابسته به خدمات کسب و کار است.

زمانی که از اینترنت به عنوان شبکه ارتباطی اساسی برای اجرای کسب وکار در خدمات کسب و کار استفاده‌می‌شود، نیازهایی چون در دسترس بودن و قابل اعتماد بودن باید متفاوت از گذشته به کار گرفته شود. اقدامات ثابت شده مانند پیش‌فرض‌های کیفیت خدمات استفاده شده، برای مثال در رابطه با خطوط استیجاری، دیگر عملی نیستند. مخاطرات امنیتی جدید باید با فنون طراحی مناسب و کنترل‌ها کاهش‌یابند.

۱۰-۵ تجارت در خدمات مشتری

کسب و کار در خدمات مشتری شامل تجارت الکترونیکی و بانکداری الکترونیکی می‌شود. نیازمندی‌ها شامل محرمانه بودن (مخصوصا مرتبط با بانکداری الکترونیکی) احراز هویت (به چه روش هایی امروزه امکان‌پذیر است- برای مثال دو عامل، بر پایه گواهی‌نامه و غیره، رابطه بین هزینه‌های پیاده‌سازی- که معمولا در صورت

وجود مشتریان زیاد، بالا است و کاهش مخاطرات مرتبط مانند ضررهای مالی، از دست دادن شهرت/اعتبار در تجارت) درستی، و مقاومت در مقابل حملات پیچیده- مانند حملات « مردی در میان[1]»و «مردی در مرورگر[2] »

مشخصات عبارتند از :

- « امنیت» تنها بر روی جایگاه نهایی که معمولا تحت کنترل سازمانی که محیط مناسبی را برای پیاده‌سازی کنترل‌ها و حفظ سطح خوبی از جایگاه امنیتی فراهم می‌کند، تضمین شده است.
- امنیت در مقام کلاینت، که معمولا یک رایانه ضعیف است. در چنین محیط هایی اجرای کنترل‌ها دشوارتر است، درنتیجه سکوی مشتری مخاطرات قابل توجهی را در این طرح فراهم می‌کند. (بدون وجود مجموعه ای از «شرایطی برای اتصال امن» مورد نیاز در یک قرارداد، که تحمیل آن در چنین محیط‌هایی می‌تواند دشوار باشد.)

۱۰-۶ خدمات برون سپاری

با توجه به پیچیدگی محیط های فناوری امروزه خیلی از سازمان‌ها از خدمات پشتیبانی فناوری فراهم شده خارج سازمانی استفاده می‌کنند، یا برون سپاری کامل یا مقطعی، پشتیبانی زیرساخت‌های فناوری اطلاعات خود را دارند. خیلی از فروشندگان الزاماتی برای دسترسی مستقیم به محصولات در حال استفاده در سازمان‌ها ی مشتریان دارند، تا بتوانند به درستی پشتیبانی و یا موارد مدیریت حادثه را اداره کنند. در حالی که بسیاری از خدمات برون سپاری نیازمند حقوق دسترسی دائمی هستند، برای مثال برای پشتیبانی زیر ساخت، بقیه تنها به دسترسی موقتی نیازمندند. در بعضی از موارد خدمات برون سپاری به حقوق دسترسی بسیار بالایی به منظور انجام کارهای مورد نیاز، به خصوص در حالات مدیریت حادثه احتیاج دارند.

۱۰-۷ تقسیم بندی شبکه

قوانین خاص برای بسیاری از سازمان‌های کشور، به خصوص کشورهای چند ملیتی، اثر به‌سزایی در الزامات امنیتی اطلاعات دارد. سازمان‌های بین‌المللی معمولا با چندین کشور مختلف کار می‌کنند، و به همین دلیل تعهد دارند تا با قوانین خاص شرکت‌های مختلف تطابق داشته باشندکه علاوه بر این می‌تواند منجر به نیازهای امنیت اطلاعاتی مختلف برای هر کشور که سازمان در آن فعال است شود. برای مثال، قانون یک کشور خاص میتواند نیازمند حفاظت مخصوصی از داده مشتری/کاربر باشد و اجازه انتقال این گونه داده‌ها را به کشور دیگر ندهد. این عمل معمولا نیازمند کنترل‌های امنیت اطلاعات اضافی برای تضمین تطابق با چنین قانون‌هایی است.

برای پوشش الزامات امنیت اطلاعات مختلف برای کشورها یک سازمان بین المللی که کار تقسیم‌بندی یک شبکه را در واقع به موازات مرزهای کشور انجام می‌دهد، می‌تواند یک راه حل گسترده موثر باشد. در خیلی از

1- Man-in-the-middle attack
2- Man-in-the-browser

مواقع چنین راهکار وسیعی می‌تواند برای ساختن یک مانع مجزای دفاعی مورد استفاده قرارگیرد. برای مثال علاوه بر کنترل دسترسی سطح کاربردی.

۱۰-۸ ارتباطات تلفن همراه

این طرح شبکه مرجع در مورد دستگاه های ارتباطی تلفن همراه شخصی است. برای مثال، تلفن‌های هوشمند یا منشی های دیجیتالی شخصی (PDA) که بسیار محبوب گشته‌اند، (راهنمای جنبه های امنیتی برقرارارتباط به و از اینگونه دستگاه‌ها در ISO 27033-7 درتامین ارتباطات امن از طریق شبکه‌های بی سیم و رادیو ارائه شده است.

اگرچه محرک اصلی توسعه‌ی سریع ویژگی‌های جدید دستگاه های ارتباطی تلفن همراه شخصی از بازار مصرف کننده نشأت می‌گیرد، این ویژگی‌ها در محیط های کسب و کار نیز استفاده می‌شوند. همان طور که عنوان«شخصی» دلالت می‌کند، این گونه دستگاه‌ها جز متعلقات شخصی هستند و برای هردو منظور کسب و کار و شخصی استفاده می‌شوند. حتی دستگاه هایی که در بازار تجارت هدایت می‌شوندبه ویژگی های معرفی شده برای بازار مصرف نیاز دارند، فروشندگان میخواهند در بازارهای رقابتی تا جایی که ممکن است به تجارت دست یابند.

خیلی از ویژگی‌های جدید با چنین دستگاه‌هایی قابل دسترسی است، رشد قابلیت های حافظه دستگاه و ارتباطات همیشه برقرار از طریق اینترنت که بر روی همگان باز است، به معنای مخاطرات قابل توجه امنیت اطلاعاتی است- مخصوصا در شرایطی که شخص از یک دستگاه برای اهداف شخصی و کاری استفاده می‌کند. به علاوه، با محبوبیت بالای دستگاه های ارتباطی تلفن همراه شخصی و وضعیت آن‌ها به عنوان «ابزار شخصی» در خیلی از موارد خط‌مشی‌های محدودی که برای تنها استفاده از مجموعه ویژگی‌های محدود یا تنها به تعداد محدودی از دستگاه‌ها مجوز می دهد با شکست مواجه می‌شوند و یا دور زده می‌شوند و این به معنی محدودیت اثر امنیت اطلاعات است.

۱۰-۹ پشتیبانی شبکه برای کاربران در حال سفر

امروزه کاربرانی که درحال سفر هستند اتصالی را با کیفیت آنچه درمکان‌های ثابت استفاده می‌کنند، انتظاردارند، مانند شرکت اصلی خودشان. راه حل‌ها و پیشنهادها در این زمینه معمولا به جنبه کاربردی تمرکز دارد. از نظر امنیت اطلاعات، سطح های کاربردی پیشنهاد شده مخاطرات جدیدی را به همراه دارد، برای مثال با تحت تاثیر قرار دادن یا بی اعتبارکردن مفروضات در مورد امنیت اطلاعات. به عنوان مثال، یک فرض از حفظ اینترنتی که به درستی کنترل شده (از خارج) و حمایت شده ممکن است به طور مقابل ملاحظه ای مورد پرسش قرار گیرد اگر دسترسی کاربر در حال سفر به اینترنت با کنترل های مناسب اجرا نشده باشد.

۱۰-۱۰ پشتیبانی شبکه برای خانه و شرکتهای تجاری کوچک

خانه و شرکت‌های تجاری کوچک اغلب نیازمند گسترش شبکه داخلی یک سازمان به یک خانه یا مکانی کوچک برای کسب و کار هستند. هزینه‌های توسعه خانه و یا مکان هایی تجاری کوچک یک موضوع حیاتی

است، از این رو بازتاب های هزینه / سود معمولا به هزینه های اجرایی بالایی احتیاج ندارد. این به آن معنی است که محدودیت‌های هزینه‌ها در کنترل‌های امنیتی که برای این کردن چنین توسعه‌های شبکه استفاده می‌شود و معمولا مانع از استفاده ایجاد کنترل‌های امنیت درون شبکه‌ای که برای اتصال قسمت‌های بزرگتر شبکه استفاده می‌شود به کارمی‌رود. در خیلی از طرح‌های خانه یا تجارت‌های کوچک زیرساخت می‌تواند برای اهداف شخصی به اندازه اهداف تجاری مورد استفاده قرارگیرد. مخاطرات امنیتی تعریف شده و یا پیشنهاد شده در تکنیک‌های طراحی امنیت و کنترل برای کاهش مخاطرات بحث شده است.

۱۱ مباحث«فناوری» – مخاطرات، تکنیک های طراحی و مسائل مربوط به کنترل

جزئیات مخاطرات امنیتی، تکنیک های طراحی و مسائل مربوط به کنترل مرتبط با مباحث «فن آوری» در پیوست الف گنجانده شده است. مباحث پوشش داده شده عبارتند از:

- شبکه‌های محلی (به بند الف-۱ مراجعه شود)
- شبکه‌های گسترده (به بند الف-۲ مراجعه شود)
- شبکه‌های بی سیم (به بند الف-۳ مراجعه شود)
- شبکه‌های رادیویی (به بند الف- ۴ مراجعه شود)
- شبکه‌های باندپهن (به بند الف-۵ مراجعه شود)
- درگاه امنیتی (به بند الف-۶ مراجعه شود)
- شبکه‌های مجازی خصوصی (به بند الف-۷ مراجعه شود)
- شبکه‌های صدا (به بند الف-۸ مراجعه شود)
- همگرایی IP (به بند الف-۹ مراجعه شود)
- میزبانی وب (به بند الف-۱۰ مراجعه شود)
- پست الکترونیکی اینترنتی (به بند الف-۱۱ مراجعه شود)
- دسترسی مسیریابی شده به سازمان‌های طرف سوم (به بند الف-۱۲ مراجعه شود)
- مرکز داده‌ها (به بند الف-۱۳مراجعه شود)

۱۲ راه حل توسعه و آزمون امنیت

زمانی که معماری فنی امنیت به طورکامل سندسازی و تایید شد، به همراه طرح‌های مدیریت، سپس راه‌حل مورد نظر باید در « حالت آزمایشی » توسعه و اجرا شود و به درستی بررسی و تطابق‌ها درآن رسیدگی شود. آزمون عمومی« متناسب هدف » برای راه‌حل‌ها باید در ابتدا با اسناد راهبردی آزمون که تولید شده و روشی که باید در آزمایش برای اثبات رساندن راه‌حل و پس از آن نقشه آزمون را توصیف می‌کند، اجرا شود. ممکن است نیاز به اجرای تغییراتی که در نتیجه کاستی‌های این روش از آزمون شناسایی شده باشد و هر تعداد آزمون مجدد مورد نیاز، صورت گیرد.

زمانی که آزمون « متناسب هدف » به طور موفقیت آمیز پایان یافت و هرگونه تغییرات اعمال شد، پیاده‌سازی باید برای مطابقت با معماری فنی امنیت مستند شده وکنترل‌های مورد نیاز امنیتی که در اسناد زیر مشخص شده است، بازنگری شود:

- معماری امنیت فنی
- خط‌مشی امنیت شبکه
- SecOP های مرتبط
- خط‌مشی خدمات دسترسی درگاه امنیت
- طرح (های) تداوم کسب و کار
- نقاط مرتبط، شرایط امنیتی برای اتصال

بازنگری تطابق باید قبل از عملیات اجرایی صورت گیرد. بازنگری باید زمانی به اتمام برسد که کلیه کاستی‌ها شناسایی، ترمیم، و توسط مدیریت ارشد امضا شده باشد.

باید توجه‌کرد که آزمون‌های امنیتی مرتبط با استانداردهای شناخته شده بین المللی، دولتی، جامعه‌ای(در صورت عدم وجود استانداردهای بین‌المللی) با خط‌مشی آزمون امنیتی و برنامه‌های آزمایشی امنیتی مرتبط باید قبل از این که دقیقا مشخص شود آزمون‌ها با چه،کجا وچه زمانی صورت گیرند، اجرا شوند.

(یک مثال نمونه برای برنامه آزمون امنیتی در ISO/IEC 27033-2 ارائه شده است.) این عمل باید شامل ترکیبی از بررسی آسیب‌پذیری و بررسی نفوذپذیری باشد. قبل از شروع هرگونه آزمون، برنامه آزمون باید بررسی شود تا از اجرای آزمایش به روشی کاملا منطبق با قوانین و مقررات مربوطه، اطمینان حاصل کنند. هنگام انجام این بررسی، نباید فراموش کرد که یک شبکه ممکن است تنها محدود به یک کشور نباشد – بلکه می‌تواند از طریق کشورهای مختلف با قوانین مختلف گسترده شده باشد. پس از انجام آزمون، گزارش باید بیانگر جزئیات آسیب پذیری مواجه شده و نیازمندی های رفع آن و با تعیین الویت، و پیوست تایید شده که کلیه رفع اشکال‌ها صورت گرفته است، باشد. چنین گزارشی باید توسط مدیر ارشد امضا شود.

در آخر، زمانی که همه موارد رضایت بخش بود، پیاده‌سازی باید امضا و تائید شود- از جمله توسط مدیریت ارشد.

۱۳ راه حل اعمال امنیتی

« اعمال» به معنی اجرای روز به روز شبکه با راه‌حل‌های امنیتی تایید شده در محل، با آزمون‌های امنیتی انجام شده و کارهای از قبل به اتمام رسیده مربوط می‌باشد. به عبارتی دیگر زمانی که معماری فنی امنیت و در نتیجه پیاده‌سازی کنترلی امنیت امضا شد، سپس عملیات اجرایی باید آغاز شود. با گذشت زمان، و اگر تغییر قابل توجهی روی داد، پس از آن آزمون‌های اجرایی و بازنگری بار دیگر باید اجرا شود. (بند ۱۴ زیر مشاهده شود)

۱۴ راه‌حل نظارت و بازنگری اجرایی

پس از شروع عملیات واقعی، نظارت مستمر و انطباق فعالیت های بازنگری باید به موازات استانداردهای ملی، دولتی، جامعه ای (در صورت عدم وجود استانداردهای بین المللی) مرتبط شناخته شده اجرا شود. چنین فعالیت‌هایی باید قبل از نسخه جدید قابل ارائه مرتبط با تغییرات مهم درالزامات تجاری، فناوری ، راه کارهای امنیتی و غیره انجام گیرد. فعالیت‌ها در این زمینه باید از الگویی که در بند ۱۲ بالا توضیح داده شد پیروی کنند.

پیوست الف

(اطلاعاتی)

مباحث « فناوری»– مخاطرات، فنون طراحی و مسائل کنترلی

الف-۱ شبکه‌های محلی

الف-۱-۱ پس‌زمینه

یک شبکه محلی (LAN) شبکه‌ای است برای اتصال رایانه‌ها و خدمت‌گزارها در یک مکان جغرافیایی کوچک. اندازه‌ی محدوده‌ی آن از تعداد محدودی سامانه‌ی متصل به هم، مانند شبکه‌ی خانگی، تا چندین هزار سامانه می‌باشد، مانند شبکه‌ی دانشگاه. خدمات معمول اجرا شده شامل به اشتراک گذاشتن منابع مانند پرینترها و به اشتراک گذاشتن فایل‌ها و نرم افزارهای کاربردی است. شبکه‌های محلی معمولا خدمات مرکزی مانند ارسال پیام یا خدمات تقویمی را ارائه می‌دهند. در بعضی از موارد شبکه‌های محلی به عنوان جایگزینی برای عملیات سنتی دیگر شبکه‌ها به کار می‌روند. مانند زمانی که پروتکل های VoIP و خدمات آنان جایگزینی برای شبکه تلفنی سانترال شدند. شبکه محلی می‌تواند بر پایه سیم و یا بی سیم باشد.

شبکه محلی سیمی معمولا از اتصال گره هایی در شبکه از طریق یک سوئیچ شبکه با استفاده از کابل‌های شبکه تشکیل شده است، که قابلیت های شبکه داده پر سرعت را ارائه می‌دهد. معمول‌ترین فناوری شبکه محلی سیمی استفاده شده اترنت است. (IEEE 802.3)

یک شبکه‌ی محلی بی‌سیم (WAN) از امواج رادیویی با فرکانس بالا برای ارسال بسته‌ها از طریق هوا استفاده می‌کند. انعطاف پذیری آن بر اساس این حقیقت است که یک شبکه محلی می‌تواند بدون نیاز به سیم کشی شبکه به سرعت گسترش یابد. فناوری‌های شبکه محلی بی‌سیم که به خوبی شناخته شده‌اند شامل پیاده‌سازی‌های IEEE 802. 11 و بلوتوث می‌باشد.

وقتی شبکه‌های محلی در مناطق محافظت شده مورد استفاده قرار می‌گیرند، برای مثال فقط درون سازمان، به احتمال زیاد مخاطرات به گونه‌ای هستند که نیاز به کنترل‌های فنی پایه‌ای می‌باشد. اگرچه برای استفاده از محیط‌های بزرگتر، و همچنین زمانی که فناوری های بی سیم مورد استفاده قرارمی‌گیرد، محافظت‌های فیزیکی به تنهایی بعید است بتواند کلیه سطح های امنیتی را ضمانت کنند.

رایانه‌های رومیزی از آنجایی که رابط مورد استفاده کاربر هستند، یک منطقه‌ی آسیب پذیر هستند. اگر رایانه‌ی شخصی کاربر قفل نشده باشد کاربر این امکان را دارد که نرم‌افزاری شناسایی نشده را روی شبکه نصب کند. سامانه‌های خدمت‌گزار مورد استفاده در شبکه‌ی شرکت‌ها ، اعم ازآنهایی که در معرض اینترنت هستند و یا خدمت‌گزارهای داخلی که دسترسی مستقیمی به اینترنت ندارند، می‌توانند مخاطرات امنیتی زیادی را به همراه داشته‌باشند- که باید جدی گرفته‌شوند. برای مثال، در حالی که قسمت‌های فناوری اطلاعات ادعا می‌کنند که درمورد وصله‌های درخواست شده به محض آنکه در دسترس باشند کوشا هستند،

حتی سازمان‌های بزرگ نیز در اضافه کردن وصله‌ی کلیه خدمت‌گزارها به موقع ناکام می‌مانند - که منجر به اختلال ترافیک شبکه توسط کرم‌ها و ویروس‌ها می‌شود.

الف-۱-۲ مخاطرات امنیت

در شبکه‌ی سیمی، مخاطرات امنیتی از گره های فیزیکی که به شبکه وصل هستند ناشی می‌شود. به طور کلی، موارد اصلی مخاطرات امنیتی مرتبط با شبکه‌های محلی شامل مواردی است که مرتبطند با :

- دسترسی غیر مجاز و تغییرات رایانه‌های رومیزی، خدمت‌گزارها و سایر دستگاه‌های متصل به شبکه‌ی محلی
- دستگاه های غیر متصل
- سرقت سخت افزار
- خرابی منبع تولید برق
- اضافه کردن کدهای مخرب از طریق پست الکترونیکی و دسترسی وب
- عدم موفقیت در گرفتن نسخه های پشتیبان از دیسکت سخت های محلی
- خرابی سخت افزار مانند دیسکت سخت
- اتصالات غیر مجاز به زیرساخت های شبکه محلی، مانند سوده‌ها و کابینت های قطعات
- اتصالات غیر مجاز به دستگاه های انتهایی، مانند لپ تاپ‌ها
- استفاده از رمزهای معمول بر روی پورت‌های مدیریتی دستگاه های شبکه
- نفوذ، که در آن اطلاعات افشا می‌شود یا یکپارچگی ویا دسترسی داده‌ها قابل ضمانت نیستند
- حملات انکار خدمت که منابع برای کاربران مجاز غیر قابل دسترس می‌شود
- زمان های تاخیر طولانی، که خدماتی مانند VoIPرا تحت تاثیر قرار می‌دهد
- خرابی دستگاه
- خرابی کابل
- امنیت فیزیکی کم

مخاطرات امنیتی مرتبط با شبکه های محلی بی‌سیم در بند الف -۳-۲توضیح داده شده است.

الف-۱-۳ کنترل های امنیتی

برای امن کردن شبکه‌های محلی نیاز است که هم اجزای شبکه محلی و هم دستگاه های متصل امن باشند. بنابراین کنترل‌ها برای امن کردن محیط های شبکه های محلی می‌تواند شامل:

-فیزیکی و محیطی:

- استفاده از سامانه‌های کابل فولادی برای جلوگیری از سرقت CPU ها، مانیتورها و صفحه کلیدها
- استفاده از قفل‌ها بر روی دستگاه‌ها برای جلوگیری از سرقت قطعاتی مانند حافظه‌ها
- استفاده از دستگاه‌های مشابه برای جلوگیری از حذف غیر مجاز آنان از پایگاه

- اطمینان حاصل‌کردن از این که دستگاه‌های شبکه محلی، مانند سوده‌ها و مسیریاب‌ها، در یک محفظه فیزیکی امن در یک اتاق ارتباطات امن نگهداری می‌شوند
- استفاده از UPS و سامانه خاموشی خودکار برای دستگاه‌های حیاتی و برای رایانه‌ی کاربران، اگر نمی‌خواهند کاری را که در حال انجام آن هستند، از دست بدهند.

- سخت افزار و نرم افزار:

- تنظیم دستگاه‌ها با آدرس های خصوصی (مانند IP)
- خط‌مشی قوی رمزها
- نیاز به حداقل یک نام کاربری و یک رمز عبور برای آغاز به کار برای هر رایانه / ایستگاه کاری
- نشان دادن زمان آخرین ورود موفق
- عدم نمایش نام کاربری آخرین ورود موفق، ونه هر لیستی از نام های کاربری استفاده شده از قبل
- نصب نرم افزارهای کدهای ضد مخرب (مانند آنتی ویروس)، که به طور خودکار به روزرسانی می‌شوند
- پیاده سازی تنظیمات پیکربندی امن
- غیر فعال کردن رانه‌ی دیسک کوچک ، رانه‌ی لوح فشرده-فقط خواندنی ، و پورت‌های UPS
- انجام عملیات آینه‌کردن[1] بر روی رانه‌های[2] خدمت‌گزار (یا اجرای RAID) به جهت افزونگی
- پاک کردن نرم افزارهای غیرضروری
- حصول اطمینان از مدیریت خوب رایانه‌های رومیزی

- عملیاتی:

- مستندسازی نرم‌افزار و تنظیمات امنیتی برای استفاده در تنظیمات رایانه‌ها/ایستگاه‌های کاری جدید در آینده
- برنامه‌ریزی بارگیری ونصب تناوبی وصله‌های[3] سامانه عامل
- ایجاد وحفظ تعمیرات اضطراری دیسک‌ها در لحظه و ذخیره در یک محل کنترل شده
- اجرای ثبت وقایع برای ثبت مشکلات نگهداری و سوءاستفاده از رایانه‌های شخصی/ایستگاه‌های کاربر
- فایل مستندات کلیه‌ی رایانه‌ها/ ایستگاه‌های کاری (مقالات/کتابچه راهنما/دیسک) برای استفاده توسط فنورزهای[4] خدمات
- حصول اطمینان از روش پشتیبان‌گیری
- حصول اطمینان ازتغییر گذرواژه‌ی منظم کلیه دستگاه‌های شبکه

1 - Mirroring
2 - Drives
3 - Patches
4 - Technician

-تنظیم گذرواژه‌های پروتکل مدیریت شبکه/رشته‌های ارتباطات
-رمزگذاری ترافیک شبکه
-تنظیم ثبت وقایع ممیزی به درستی و اگر امکان داشت، پیاده سازی روش‌هایی برای نظارت بر ثبت وقایع ممیزی
- برنامه‌ریزی نصب به روز رسانی‌های سامانه عامل به طور دوره‌ای
- تنظیم اسناد تجهیزات برای استفاده در تنظیم مجدد آنان در آینده، گرفتن رونوشت پشتیبان از فایل تنطیمات مسیریاب، و نگهداری آن در مکانی امن
-آزمایش کلیه دستگاه های متصل به شبکه محلی برای یافتن آسیب پذیری ها

کنترل های امنیتی مرتبط با شبکه های محلی بی سیم در بند الف-۳-۳ توضیح داده شده است.

الف-۲ شبکه های گسترده

الف-۲-۱ پس‌زمینه

شبکه های گسترده برای اتصال مکان های دور و شبکه های محلی شان به یکدیگر به کار می‌روند. یک شبکه گسترده می‌تواند به گونه ای ساخته شود که از کابل ها، مدارهای یک ارائه کننده خدمت، یا با اجاره خدمات از یک ارائه کننده ارتباط از راه دور استفاده کند. فناوری های شبکه گسترده انتقال و مسیریابی ترافیک شبکه را به راه دور امکان پذیر می‌کند، و معمولا ویژگی های وسیعی از مسیریابی برای مسیردهی بستک های شبکه به مقصد صحیح شبکه محلی فراهم می‌کند. معمولا ساختار شبکه فیزیکی عمومی برای اتصال شبکه های محلی به کار می‌رود، برای مثال خطوط استیجاری، ارتباطات ماهواره ای یا فیبر نوری، یک شبکه گسترده می‌تواند براساس سیم و یا بی سیم پایه گذاری شود.

یک شبکه گسترده سیمی شامل دستگاه های مسیریابی است (مانند روترها) که به یک شبکه عمومی یا خصوصی از طریق سیم های ارتباطی متصل است. یک شبکه گسترده بی سیم معمولا از امواج رادیویی برای ارسال بسته های شبکه از طریق هوا به مسافت های طولانی استفاده می‌کند، که می‌تواند تا ده کیلومتر یا بیشتر باشد.

درحالی که شبکه های گسترده سنتی غالبا با استفاده از اتصال‌های ثابت اجارهای از ارائه‌کننده های خدمات که از حداقل فعالیت مدیریتی این اتصال‌ها برخوردار بودند. به جای تضمین کاربردی بودن آنان، استفاده می‌کردند. پیشرفت در فناوری شبکه های گسترده، تغییر در مسئولیت و مدیریت شرکت های ارائه کننده خدمات را به همراه داشت. با این فایده برای سازمان که مجبور نبودند خودشان شبکه را گسترده و مدیریت کنند. این به آن معناست که شرکت ارائه کننده خدمات متعهد می‌شود که امکانات مدیریت شبکه امن باشد. از آنجایی که شبکه های گسترده در اصل برای مسیریابی ترافیک شبکه در مسیر های طولانی مورد استفاده قرار می‌گیرند، عملیات مسیریابی باید امن باشد تا اطمینان حاصل کنند که مسیریابی به مقصد شبکه محلی به صورت اشتباه صورت نگیرد. بنابراین ترافیکی که از شبکه گسترده می‌گذرد مستعد رهگیری توسط افرادی است که به زیرساخت شبکه گسترده دسترسی دارند. از آنجایی که زیرساخت شبکه گسترده گرایش بیشتری

به قابل دسترس بودن دارد تا شبکه محلی، باید توجه شود که اطلاعات محرمانه در محیط‌های شبکه گسترده به صورت رمزگذاری منتقل شوند. شرکت ارائه دهنده خدمات باید متعهد شود تا سطح امنیتی مورد نیاز سازمان را تامین کند.

الف-۲- ۲ مخاطرات امنیتی

از آنجایی که شبکه گسترده سیمی مخاطرات امنیتی یکسانی با شبکه محلی سیمی دارد (بند الف-۱ در بالا مشاهده شود) و از آنجایی که شبکه های گسترده در معرض ترافیک شبکه بیشتری قرار دارد با مخاطرات امنیتی بیشتری مواجه است، به این معناست که کنترل ها، شامل دسترسی، باید صورت گیرد تا از عدم به خطر افتادن شبکه گسترده و در نتیجه ایجاد اختلالات گسترده اطمینان حاصل کند. به طور مشابه، از انجایی که شبکه گسترده بی سیم مخاطرات امنیتی اصلی یکسانی با شبکه محلی بی سیم دارد (بند الف-۳ زیر مشاهده شود) بیشتر مستعد ابتلا به اختلالات با توجه به توانایی مسدود کردن سامانه‌هایی که برای انتقال بسته های شبکه به کار می‌رود، است.

به طور کلی مخاطرات امنیتی اصلی مرتبط با شبکه های گسترده عبارتند از مواردی که مرتبطند با :

- نفوذ، که در آن اطلاعات فاش شده، یا یکپارچگی ویا دسترسی به داده ضمانت نشود.
- حملات انکار خدمت ، که منابع برای کاربران دارای مجوز غیر قابل دسترس شود.
- تاخیر زیاد، که بر روی خدماتی چون انتقال صدا بر بستر IP تاثیر می‌گذارد.
- لغزش بر روی شبکه، که می‌تواند بر روی مواردی مانند کیفیت صدا تاثیر داشته باشد. (عمدتا ناشی از استفاده از کابل های مسی برای ارائه خدمات است)
- خرابی دستگاه
- خرابی کابل
- دستگاه‌های غیرمتصل
- رفتن برق در مرکز انتقال که عملکرد دیگران را تحت تاثیر قرار می‌دهد
- امکانات مدیریت شبکه‌ی شرکت ارائه کننده‌ی خدمات

الف-۲-۳ کنترل های امنیتی

کنترل های امنیتی مورد نیاز ایجاد امنیت در شبکه های گسترده شامل:

- استفاده از پروتکل‌های مدیریت امنیت مانند SSH ، SCP و یا SNMPv3
- رمزگذاری اتصال‌های مدیریتی
- رمزگذاری ترافیک شبکه
- پیاده‌سازی شناسایی امن برای دسترسی به دستگاه‌های شبکه گسترده، با هشداردهنده مناسب دستگاه‌ها
- امن کردن تجهیزات فیزیکی شبکه گسترده در هر سایت، مانند استفاده از کمدهای قفل شده با دسترسی هشدار دهنده
- استفاده از UPS برای جلوگیری از اختلالات منبع تغذیه

-اتصال دوگانه سایت‌ها، با استفاده از مسیرهای گوناگون
- نمونه برداری فعال از دستگاه های شبکه گسترده
- نقشه برداری شبکه برای شناسایی دستگاه های غیر مجاز
- مدیریت قطعات
- پوشش رمزگذاری شده برای داده های حساس
- اخذ ضمانت خدمات از ارائه دهنده خدمت، مانند مواردی چون دسترسی، تاخیر و لغزش
- ایجاد مجوزها و حساب های کاربری برای دسترسی به دستگاه های شبکه گسترده
- استفاده از دیواره‌ی آتش که کلیه ترافیک های ناخواسته به سمت شبکه را از بین می‌برد
- اطمینان حاصل کردن از مخفی بودن زیر ساخت و آدرس ها
- قرار دادن آدرس هایی که نمی‌توانند در اینترنت مسیریابی شوند
- استفاده از نرم افزار برای جلوگیری از کدهای مخرب، مانند تروجان ، ویروس، جاسوس‌افزار[1] وکرم‌ها[2] از درگاه‌های باز امنیتی در داخل شبکه
- استفاده از IDS برای شناسایی ترافیک های مشکوک
- اطمینان حاصل کردن از امنیت منطقی سامانه‌های مدیریتی شبکه
- مدیریت شبکه خارج از محدوده
- اطمینان حاصل کردن از امنیت فیزیکی مکان‌های مدیریت شبکه

الف-۳ شبکه های بی سیم

الف-۳-۱ پیش زمینه

شبکه های بی سیم به شبکه هایی گفته می‌شود که محیط های کوچک از نظر جغرافیایی را پوشش می‌دهند و از ابزار ارتباطی بدون سیم مانند امواج رادیویی یا فروسرخ استفاده می‌کنند. معمولا شبکه های بی سیم برای اتصالات مشابه با شبکه های محلی استفاده می‌شوند. بنابراین به آن‌ها شبکه های محلی بی سیم (WLANs) نیز گفته می‌شود. فناوری اصلی استفاده شده در IEEE 802. 11 و بلوتوث استاندارد شده است. باید توجه داشته باشید که شبکه های بی سیم متشکل از دسته های مختلف شبکه از شبکه های رادیویی مانند GSM ، 3G ، VHF به عنوان ابزاری که از دکل های انتقال داده استفاده می‌کنند است. (بند الف. ۴ زیر) به علاوه، اتصالات مادون قرمز و سایر انواع اتصالات که اتصالات بی سیم را پشتیبانی می‌کنند، باید به عنوان قسمت جانبی از ملاحظات اتصالات شبکه در نظر گرفته شوند.

شبکه های محلی بی سیم از کلیه آسیب پذیری های شبکه های محلی سیمی رنج می‌برند. به علاوه یک سری از آسیب پذیری های مخصوص که مرتبط با خصوصیات اتصال‌های بی سیم است. بعضی از فناوری‌های مخصوص (بیشتر بر اساس رمزگذاری) برای شناسایی این آسیب پذیری های اضافی توسعه یافتند. اگرچه

1- Spyware
2 -Worms

نسخه های جدید این فناوری (مانند WEP) معماری ضعیفی دارد، بنابراین انتظارات مربوط به الزامات اعتماد را برآورده نمی‌کنند.

الف. ۲. ۳ مخاطرات امنیت

مخاطرات امنیتی اصلی مرتبط با استفاده از شبکه های محلی بی سیم شامل مواردی چون:

- استراق سمع
- دسترسی های غیر مجاز
- اختلال و پارازیت
- عدم تنظیمات
- حالت دسترسی امن به طور معمول در حالت خاموش باشد
- پروتکلهای رمزگذاری غیر امن
- استفاده از پروتکل های مدیریتی غیر امن برای مدیریت شبکه های محلی بی سیم
- همیشه امکان شناسایی کاربران شبکه های محلی بی سیم وجود ندارد
- دستگاه های فریب‌کار (مانند نقاط دسترسی)

الف-۳-۳ کنترل های امنیتی

کنترل های مورد نیاز شبکه های محلی بی سیم می‌تواند شامل :

- تنظیم زیرساخت با معیارهای تکنیکی امنیتی مناسب (محافظت از شبکه‌های گسترده در زیرساخت شرکت‌ها)
- محافظت از شبکه های محلی بی سیم از زیر ساخت های شرکت ها
- رمزگذاری ارتباطات و رد و بدل داده ها، برای مثال با اجرای VPN بر اساس IPsec بر روی شبکه های محلی بین کاربر و دیواره‌ی آتش محیطی
- اعمال توجهات به منظور توسعه امنیت هر دستگاه شبکه محلی بی سیم، با تنظیم دیواره‌ی آتش های شخصی و تشخیص نفوذ نرم افزارهای کدها ضد مخرب (شامل آنتی ویروس‌ها) بر روی دستگاه کاربر
- استفاده از احرازهویت
- کنترل سطح انتقال برای از بین بردن انتشار در خارج از حوزه فیزیکی سازمان
- تنظیمات SNMP تنها برای دسترسی خواندن
- مجموعه صورت عملیات ممیزی و تجزیه و تحلیل برای شناسایی هر اختلال و استفاده غیر مجاز
- مدیریت رمزگذاری خارجی، برای مثال با استفاده از SSH
- حفظ امنیت فیزیکی در نقاط دسترسی بی سیم

الف-۴ شبکه‌های رادیویی

الف-۴-۱ پس‌زمینه

شبکه‌های رادیویی به شبکه‌هایی گفته می‌شود که از امواج رادیویی به عنوان واسط‌های اتصال برای پوشش دادن یک منطقه جغرافیایی وسیع استفاده می‌کنند. نمونه های معمول شبکه‌های رادیویی شبکه‌های تلفن همراه است که از فناوری هایی مانند GSM یا UTM استفاده می‌کند و دسترسی عمومی خدمات صدا و داده را ارائه می‌کند.

باید توجه داشت که شبکه‌هایی که از امواج رادیویی برای پوشش مناطق کوچک استفاده می‌کنند در یک دسته بندی دیگری قرار می گیرند که مرتبط با بند الف-۳ بالا می‌شوند.

نمونه هایی از شبکه‌های رادیویی شامل :

- TETRA
- GSM
- 3G(شامل UMTS)
- GPRS
- CDPD
- CDMA

الف-۴-۲ مخاطرات امنیت

مخاطرات امنیت اصلی مرتبط با استفاده از شبکه‌های رادیویی به طورکلی شامل مواردی است که مرتبطند با :

- استراق سمع
- سرقت کانال ارتباطی
- جعل هویت
- تهدیدات سطح کاربردی، برای مثال تقلب
- محرومیت از خدمات

مخاطرات امنیتی مرتبط با GSM شامل مواردی است که مرتبطند با :

- ضعف الگوریتم A5/x و Comp 128-1

یادآوری - الگوریتم انحصاری است که در ابتدا به طور پیش فرض در سیم کارت مورد استفاده قرار گرفت.

- رمزگذاری عمومی GSM خاموش باشد
- سیم کارت شبیه سازی شده واقعی باشد

مخاطرات امنیتی مرتبط با 3G شامل مواردی است که مرتبطند با :

- تلفن‌ها مستعد حملات الکترونیکی هستند، از جمله وارد کردن کدهای مخرب، برای مثال ویروس ها
- شانس حملات بالا است چون تلفن‌ها اکثرا روشن هستند.
- خدمات می‌تواند عاملی برای استراق سمع باشد.
- شبکه رادیویی می‌تواند دچار پارازیت شود.
- امکان وارد کردن یک ایستگاه اصلی اشتباه وجود دارد.
- درگاه‌ها می‌توانند عاملی برای دسترسی غیر مجاز باشند.
- خدمات می‌تواند موضوعی برای حملات و دسترسی غیرمجاز از طریق اینترنت باشد.
- معرفی هرزنامه‌ها امکان پذیر است.
- سامانه‌های مدیریتی می‌تواند موضوعی برای دسترسی غیر مجاز از طریق RAS شود.
- خدمات می‌تواند از طریق تجهیزات پشتیبانی مهندسی دزدیده و یا گم شده مورد حمله قرار گیرد از جمله لپ تاپ.

UMTS عضو اصلی خانواده فناوری های تلفن همراه 3G است، که ظرفیت قابل توجه و قابلیت های پهنای باند برای پشتیبانی تعداد بسیار زیادی از کاربران صدا و داده را فراهم می‌کند، و از کانالی با عرض 5 MHz برای دریافت نرخ های بالاتری از داده و افزایش ظرفیت استفاده می‌کند، و استفاده بهینه از منابع رادیویی، به ویژه برای اپراتورهایی است که بلوک های بزرگ و پیوسته ای از طیف را برای کاهش هزینه توسعه شبکه‌های 3G ارائه می‌کنند- معمولا محدوده ای از 2×10 MHz تا 2×20 MHz است. GPRS اولین گام ضروری به سمت نسل سوم شبکه‌های تلفن همراه به همراه افزایش ویژگی های شبکه GSM است، که اجازه می دهد هر دو بسته سوییچ شده و ترافیک مدار سوییچ شده در زیر ساخت GSM وجود داشته باشند. GPRS تا هشت قطعه زمانی TDM 9. 05Kb یا 13. 4Kb برای پهنای باند کلی از 72. 4Kb یا 107. 2Kb استفاده می‌کند. GPRS هر دو ارتباط TCP/IP و X. 25 را پشتیبانی می‌کند. با فعال کردن EDGE شبکه‌های GSM قادر خواهند بود که EGPRS ، نسخه پیشرفته GPRS را اجرا کنند، که پهنای باند هر قطعه زمانی را تا 60Kb افزایش می دهد. GPRS یک ارتباط اینترنتی « همیشه برقرار » را که یک مشکل امنیتی بالقوه است را ایجاد می‌کند، یک ارائه کننده شبکه GPRS معمولا سعی دارد امنیت پیوند ارتباطی را با ایجاد یک دیواره آتش بین شبکه GPRS و اینترنت بالا ببرد، ولی باید به گونه ای تنظیم شود که به خدمات دارای مجوز اجازه کار دهد، در غیر این صورت می‌تواند توسط طرف سومی مورد سواستفاده قرارگیرد.

CDPD یک ویژگی برای پشتیبانی دسترسی بی سیم به اینترنت و شبکه‌های عمومی تعویض بسته‌ها بر روی شبکه تلفن همراه است. CDPD ، TCP/IP و CLNP را پشتیبانی می‌کند. CDPD ارائه رمزگذاری RC4 با کلیدهای ۴۰ بیتی برای رمزگذاری بهره می برد. CDPD در استاندارد IS-732 تعریف شده است. یک الگوریتم قوی نیست و با یک حمله نیروی مخرب می‌تواند رمزگشایی شود. CDMA یک فرم طیف گسترده، ازخانواده تکنیک های ارتباطی دیجیتالی است که برای سال‌ها مورد استفاده قرار گرفته است. مبانی اصلی طیف گسترده استفاده از امواج حامل پارازیتی است، که پهنای باند بسیار گسترده تر از پهنای باند مورد نیاز یک ارتباط نقطه به نقطه ساده برای نرخ داده ای یکسان، می‌باشد. فنآوری برنامه نویسی دیجیتالی

بهCDMA اجازه می دهدکه از استراق سمع، اعم از عمدی یا تصادفی جلوگیری کند. فناوری CDMA صدا را به بیت های کوچکتر که در طیف های گسترده ای از فرکانس‌ها عبور می‌کنند، تجزیه میکند. هر بیت کوچک از مکالمه (یا داده) به وسیله یک کد دیجیتالی که تنها توسط تلفن CDMA و ایستگاه اصلی قابل شناسایی است تعریف می‌شود. این به آن معناستکه به صورت مجازی دستگاه دیگر میتواند تماس را دریافت کند. از آنجایی که میلیون‌ها کد ترکیبی برای هر تماس وجود دارد، از استراق سمع جلوگیری می‌کند.

الف-۴-۳ کنترل های امنیت

چندین فنون کنترل امنیت فنی برای مدیریت مخاطرات تهدیدات شناخته شده برای شبکه‌های رادیویی وجود دارد، که شامل مواردی چون:

- احراز هویت ایمن
- رمزگذاری با الگوریتم‌های موثر
- ایستگاه‌های اصلی حفاظت شده
-دیواره‌های آتش
- حفاظت در مقابل کدهای مخرب (ویروس، تروجان و غیره)
- ضد هرزنامه‌ها

الف-۵ شبکه‌های باندپهن

الف-۵-۱ پس‌زمینه

شبکه‌های باندپهن می‌تواند گروهی از فناوری‌ها باشد که به مشترکین فردی امکان دسترسی با سرعت بالا را به اینترنت موجود بدهد. نمونه‌هایی از فناوری باندپهن شامل:

- 3G
- کابل (فیبر، بافه هم محور)
- ماهواره
- XDSL
- FiOS
- BPL
- FTTH

XDSL دو نوع است. یکی از انواع آن نامتقارن (ADSL) است که سرعت بارگذاری از سمت کاربر پایین‌تر است (یک چهارم تا نصف سرعت بارگیری) و دیگری متقارن (SDSL) که سرعت بارگذاری و بارگیری یکسان است. در هر حال، سرعت بارگیری معمولا از 128 Kbps تا 2-8 Mbps است، که بستگی به محصول دارد. فناوری‌های کابل وماهواره نیز محصولات مشابهی دارند.

اهداف اصلی انتخاب فناوری باندپهن این استکه دارای سرعت بالا، و در فناوری های موجود ارزان تر از راه های ارتباطی معمولی هستند، و می‌توانند باندپهن نرم افزارهای فشرده را پشتیبانی کنند. (برای مثال،

HDTV به 20 – 15مگابیت در فشرده‌سازی فعلی احتیاج دارد). کلیه فناوری‌ها اجازه دسترسی به اینترنت و گسترش به اماکن مشترک را از طریق اینترنت می‌دهند. استفاده از اینترنت به عنوان یک حامل جهانی امکان ایجاد پیوندهای ارتباطی با سرعت بالا و ارزان ، و یا شاید با گسترش VPNها برای راه‌های ارتباطی ایمن را با سایت‌ها می‌دهد.

الف-۵-۲ مخاطرات امنیتی

باندپهن یک پیوند ارتباطی ساده « همیشه برقرار» پر سرعت بین مشترکین و اینترنت است. این ویژگی‌ها براندازی سامانه اتصالی از طریق باندپهن را تبدیل به یک پیشنهاد ارزشمند برای هکرها می‌کند. مخاطرات امنیتی اصلی مرتبط در استفاده از باندپهن شامل مواردی است که مرتبطند با :

- افشا، اصلاح یا حذف اطلاعات در نتیجه دسترسی غیرمجاز از راه دور
- انتشارکد مخرب
- بارگذاری / بارگیری و اجرای کدهای غیر مجاز
- سرقت هویت
- از بین رفتن تنظیمات سامانه کاربر
- شناخت آسیب های نرم افزار
- تراکم شبکه
- انکار خدمت

الف-۵-۳ کنترل های امنیتی

چندین فن برای کنترل‌های امنیتی مدیریت مخاطرات تهدیدات شناخته شده ارتباطات باندپهن وجود دارد که شامل :

- دیواره آتش های شرکت های کوچک/ شرکت های خانگی (SOHO)
- رمزگذاری داده
- نرم افزارهای ضدکدهای مخرب (شامل آنتی ویروس)
- سامانه‌های تشخیص نفوذ ، از جمله سامانه‌ی پیشگیری از نفوذ
- شبکه‌های اختصاصی مجازی
- به روز رسانی/ و اضافه کردن قسمتی به نرم افزارها

الف-۶ درگاه های امنیتی

الف-۶-۱ پس‌زمینه

یک تنظیم مناسب درگاه امنیتی باید بر اساس اسناد خط‌مشی های دسترسی به خدمات ایمن درگاه‌ها از سامانه‌های داخلی سازمان محافظت کند و ترافیک عبوری از آن را کنترل و به صورت ایمن مدیریت کند. (بند الف-۶-۳ زیر مشاهده شود)

الف-۶-۲ مخاطرات امنیت

روزانه، هکرها به صورت پیچیده تری سعی می‌کنند تا در شبکه‌های تجاری نفوذ پیدا کنند و درگاه‌ها در مرکز این توجهات هستند. تلاش‌ها برای دسترسی غیرمجاز می‌تواند مخرب باشد، مانند مواردی که منجر به حملات انکار خدمت می‌شود، که می‌تواند شامل منابع مورد سواستفاده قرارگرفته، و یامی‌تواند به دست آوردن اطلاعات ارزشمند باشد. درگاه می بایست سازمان را از این نوع رسوخ های دنیای خارجی محافظت کند، مانند اینترنت و شبکه‌های دیگر.

عدم نظارت محتوا سازمان را از تبعیت مسائل قانونی دور می‌کند و پتانسیل از دست دادن مالکیت معنوی را به وجود می آورد. به علاوه، هرچه سازمان‌ها ی بیشتری برای رفع نیاز های خود به اینترنت متصل می‌شوند، با نیاز به کنترل دسترسی به وبگاه های نامناسب و ناشایست مواجه می‌شوند. بدون این کنترل، سازمان‌ها با توجه به وب گشتی های غیرمولد زیان های بهره وری، قرار گرفتن در معرض تعهدات و تخصیص پهنای باند را به مخاطره می اندازند. بنابراین مخاطرات امنیتی اصلی شامل مواردی است که مرتبطند با :

- عدم دسترسی به ارتباطات دنیای خارجی
- آسیب دیدن داده‌ها
- تبدیل دارایی‌های با ارزش شرکت به موضوعی برای افشای غیرمجاز
- قرار گرفتن داده‌ها بر روی پایگاه‌ها یا انتقال بدون توانایی در تحمیل مجازات‌های قانونی مانند تجارت درونی.

الف-۶-۳ کنترل های امنیت

یک درگاه امنیت باید :

- شبکه‌های منطقی را ازهم جدا کند
- محدودیت و عملیات تجزیه و تحلیل را بر روی اطلاعاتی که بین شبکه‌های منطقی می گذرند ارائه کند
- باید توسط سازمان به عنوان وسیله ای برای کنترل دسترسی به و از شبکه سازمان مورد استفاده قرار گیرد
- یک نقطه کنترل شده و قابل مدیریت ازکل شبکه به وجود آورد
- خط‌مشی های امنیتی سازمان را در رابطه با اتصالات شبکه اجرا کند
- تنها یک نقطه برای ورود به شبکه ایجاد کند

برای هر درگاه امنیتی یک سند مجزای خط‌مشی دسترسی (امنیتی) خدمات باید ایجاد شود و محتوای ایجاد شده باید اطمینان حاصل کندکه تنها ترافیک بامجوز اجازه عبور دارد. این سند باید شامل جزئیات قوانین باشد که درگاه و تنظیمات آن باید مدیریت شود. این امکان نیز وجود داردکه اتصالات مجاز را بر اساس پروتکل ارتباطی و سایرجزئیات جداگانه معرفی کند.

بنابراین، به منظور اطمینان پیداکردن از اینکه تنها کاربران معتبر به ترافیک دسترسی از اتصالات ارتباطات دسترسی دارند، خط‌مشیی باید تعریف شود و به جزئیات محدودیت‌ها و قوانین درخواست شده برای ترافیک عبوری به داخل و خارج از درگاه امنیتی و مواردی برای مدیریت وتنظیمات آن را ثبت کند.

با درگاه های امنیتی، استفاده کامل باید از طریق شناسایی های موجود و احراز هویت، کنترل دسترسی منطقی و امکانات حسابرسی صورت گیرد. به علاوه، باید به طور معمول برای نرم افزار و یاداده های غیرمجاز، که یافت می‌شوند، بررسی شوند. گزارش حوادث باید مطابق طرح مدیریتی حوادث امنیتی اطلاعات سازمان و یا شرکت تنظیم شود. (ISO/IEC 27035 مشاهده شود.)

باید توجه شود که اتصال به شبکه زمانی امکان‌پذیر است که درگاه امنیتی انتخاب شده بررسی شود که مناسب نیازهای سازمان و/یا شرکت باشد، و کلیه مخاطرات در نتیجه چنین اتصالی به طور ایمن مدیریت شوند. باید اطمینان پیدا کند که گذر از درگاه امنیتی امکان پذیر نیست.

دیواره آتش نمونه مناسبی از درگاه امنیتی است. دیواره آتش به طور معمول باید به سطح اطمینان مناسبی متناسب با مخاطرات ارزیابی شده دست یابند، با قوانین یک دیواره آتش استاندارد که معمولا با جلوگیری از کلیه دسترسی‌ها بین شبکه‌های داخلی و خارجی شروع می‌شود، و اضافه کردن قوانین صریح ، نیازهای طرح های ارتباطی برآورده می‌شود.

جزئیات بیشتر در امنیت درگاه‌ها در ISO/IEC 27033-4 ارائه شده است (همچنین ISO/IEC 27002 و ISO/IEC 27005)

توجه داشته باشد که درحالی که جنبه های امنیتی شبکه از دیواره آتش های شخصی ، یک نوع خاصی از دیواره‌های آتش، در ISO/IEC 27033-4 توضیح داده‌نشده است، اما باید در نظر گرفته‌شوند. برخلاف بیشتر سایت‌های مرکزی که توسط دیواره‌های آتش اختصاصی محافظت می‌شوند، سامانه‌های از راه دورممکن است هزینه و مهارت های مخصوص پشتیبانی این دستگاه‌ها را تضمین نکنند. در عوض، یک دیواره آتش شخصی می‌تواند استفاده شود، که جریان ارتباطات را به (و گاهی اوقات به خارج از) یک رایانه راه دور کنترل می‌کند. مدیریت قوانین (خط‌مشی‌ها) دیواره آتش می‌تواند از راه دورتوسط کارمندان سایت مرکزی صورت گیرد، به شرط آنکه کاربر سامانه از راه دور درک فنی از نیازهای سامانه داشته باشد. اما اگر این عمل امکان پذیر نیست باید ازتنظیمات موثر مراقبت شود، به خصوص در مواردی که در سایت از راه دور افراد، دانش فناوری اطلاعات ندارند. برخی از دیواره‌های آتش شخصی می‌تواند توانایی انتقال از طریق شبکه به برنامه‌های مجاز (یا حتی کتابخانه‌ها) را برای محدود کردن توانایی گسترش اسب تروآ، محدود کند.

الف-۷ شبکه‌های خصوصی مجازی

الف-۷-۱ پس‌زمینه

یک VPN یک شبکه خصوصی است که با استفاده از زیر ساخت شبکه‌های موجود پیاده‌سازی می‌شود. از دید کاربر VPN مانند یک شبکه خصوصی عمل می‌کند و عملیات وخدمات مشابهی را ارائه می‌کند. یک VPN می‌تواند در موقعیت های مختلف استفاده شود مانند:

- برقراری دسترسی از راه دور به یک سازمان از طریق تلفن همراه یا کارمندان خارج از سایت
- متصل کردن مکان‌های مختلف یک سازمان به یکدیگر، مانند پیوندهای دوگانه برای پیاده‌سازی زیرساخت بازیابی

- ایجاد ارتباطات به شبکه سازمان برای همکاران دیگر در سایر سازمان‌ها و شرکت ها

به عبارت دیگر، VPN برقراری ارتباط بین دو رایانه یا شبکه‌ها را از طریق بستر ارتباطی مانند اینترنت فراهم می‌کند. این گونه از ارتباطات به طور سنتی و با هزینه زیادتوسط خطوط استیجاری با رمزگذاری های ارتباطات صورت می گرفت. با این حال با ظهور ارتباطات اینترنت پر سرعت و تجهیزات پایانی مناسب در انتهای هر سو، ارتباطات قابل اطمینان بین پایگاه‌ها می‌تواند با استفاده از VPNها توسعه یابد.

الف-۷-۲ مخاطرات امنیت

مخاطره‌ی امنیت اصلی مرتبط با ارتباطات با بیش از یک شبکه ناامن آن است، که ارتباط با اطلاعات حساسی که به طور بالقوه توسط افراد غیرمجاز قابل دسترسی است برقرار شود – که منجر به افشای غیرمجاز و یا اصلاح آن می‌شود. علاوه بر مخاطرات امنیتی که معمولا مرتبط با شبکه‌های محلی و گسترده است (بندهای الف. ۱ و الف. ۲ بالا مشاهده شوند)، مخاطرات امنیت معمول مرتبط با VPNها شامل مواردی است که مرتبط هستند با :

- پیاده‌سازی ناامن از طریق:
- مجموعه رمزگذاری بررسی نشده یا خراب
- ضعف رمز به اشتراک گذاشته شده که به راحتی قابل حدس زدن است
- پیکربندی ضعیف شبکه
- عدم اطمینان به کاربر راه دور
- عدم اطمینان به احرازهویت کاربران
- عدم اطمینان به ارائه کننده خدمات زیربنایی
- کارایی و دسترسی ضعیف خدمات
- عدم انطباق با الزامات قانونی و تنظیم مقررات برای استفاده از رمزنگاری در بعضی از کشورها

الف-۷-۳ کنترل های امنیت

در VPN ها، معمولا تکنیک های رمزگذاری و یا پروتکل های کاربردی برای اجرای عملیات امنیتی و خدمات مورد استفاده قرار می گیرند، مخصوصا اگر شبکه مورد استفاده VPN یک شبکه عمومی باشد (مانند اینترنت). در بیشتر پیاده‌سازی‌ها پیوند های ارتباطی بین مشترکین برای اطمینان رمزگذاری می‌شوند، و پروتکل های احراز هویت به منظور بررسی هویت سامانه‌ها متصل به VPN استفاده می‌شوند. به طور معمول، اطلاعات رمزگذاری شده از یک « تونل» ایمن که به درگاه سازمان متصل است، با حفظ محرمانه بودن و یکپارچگی اطلاعات عبورمی‌کند. درگاه کاربر راه دور را شناسایی می‌کند و به کاربر اجازه دسترسی به اطلاعاتی را که مجوز دریافت آن را دارند، می دهد.

بنابراین، VPN مکانیزمی براساس استفاده از تونل و بهبود پروتکلی یک پروتکل کامل (پروتکل کاربر) به عنوان یک ارائه ساده از بیت‌ها و استفاده آن در خلال پروتکل دیگر (پروتکل حامل) است. به طورمعمول،

پروتکل حامل VPN امنیت (اعتماد و یکپارچگی) را برای پروتکل (های) کاربر ایجاد می‌کند. در استفاده ازVPN ها، جنبه های معماری که باید موردتوجه قرار گیرد شامل :

- امنیت نقاط نهایی
- امنیت نقاط خاتمه
- حفاظت درمقابل نرم افزارهای مخرب
- تشخیص هویت قوی
- تشخیص نفوذ
- درگاه‌های امنیتی (از جمله دیواره آتش‌ها)
- رمزگذاری داده
- طراحی شبکه
- اتصالات دیگر
- تقسیم تونل ها
- ورود به سامانه ممیزی و نظارت بر شبکه
- مدیریت آسیب پذیری فنی

جزییات بیشتر درمورد VPN ها، ازجمله مواردی در مورد هر یک از این جنبه‌های معماری در ISO/IEC 27033-5 ارائه شده است.

الف-۸ شبکه‌های صدا

الف-۸-۱ پس‌زمینه

امروزه PABXها برای پشتیبانی کانال‌های سنتی اتصال تلفن‌ها به PSTN وجود دارند. تنظیمات اطلاعات تماس با استفاده از DPNSS بین آنان رد و بدل می‌شود. (یک رابط استاندارد صنعتی بین PABX و شبکه‌ی موجود تعریف شده است). DPNSS به طور معمول امکاناتی را که تنها بین خروجی یک PABX به کلیه خروجی های روی PABX هایی که به یکدیگر در یک شبکه خصوصی متصل هستند، توسعه می‌بخشد. اگرچه در چند سال گذشته یک پروتکل جدید در کنار DPNSS برای هر دو ارتباط بین PABXها و بین PABX وPSTN تولید شد. این امر مربوط به معماری ISDN های خصوصی و یک پروتکل سیگنالی تبادلی براساس مفاهیم ISDN که در راهنمای ITU-T مشخص شده است، می‌باشد. پروتکل تبادلی Q .931 ، براساس راهنمای ITU-7، به عنوان QSIG شناخته شد. پروتکل های سیگنالی قوی هستند و مشکلات امنیتی به وجود نمی آورند، اما تعدادی از مخاطرات امنیتی مرتبط باسامانه‌های تلفن PABX سنتی وجود دارد.

الف-۸-۲ مخاطرات امنیت

مخاطرات امنیت مرتبط با سامانه‌های تلفنی سنتی شامل مواردی است چون:

- عدم کنترل پشتیبان‌گیری از اطلاعات مخصوص سایت، که می‌تواند دسترسی در شرایط خاص را تحت تاثیر قرار دهد.
- استراق سمع، در صورت دسترسی فیزیکی به کابل ها
- با مدیریت درگاه‌ها که مسئول نفوذهای غیر مجاز است که به طور ضعیفی محافظت می‌شوند، با یک سامانه ساده تماس برگشتی می‌تواند PABX رادوباره برنامه ریزی و یا برای استفاده مخرب و یا خاموشی آن اقدام کند.
- شماره گیری جعلی، چون جدول های محدودیت ارتباط راه دور داخلی به طور ضعیف نگهداری می‌شوند، بنابراین تماس‌ها به طور معمول مجاز به مسیریابی در شبکه هستند و به PSTN فرستاده می‌شوند (در بعضی از این مواقع این شرایط منجر به شماره گیری جعلی به شماره های مجاز بسیاری می‌شود – با زیان قابل توجه مالی
- جعل در ارتباط خاص از راه دور، اجازه تماس های انحرافی غیرمجاز و تنظیمات تماس را می دهد (با تقلب در استفاده از یک سامانه پیام صوتی مرتبط برای تغییر جهت دادن تماس‌ها خارج از PSTN)
- عدم انعطاف پذیری و /یا ظرفیت، که می‌تواند در دسترسی تاثیر داشته باشد.

الف-۸-۳ کنترل های امنیت

کنترلهای امنیت برای شبکه‌های صدا می‌تواند حصول اطمینان ازمواردی چون زیرباشد :
- امکان دسترسی فیزیکی به کابل ها،جعبه اتصال و قاب‌ها وجود ندارد.
- جدول های راه اصلی به طورمناسب برای جلوگیری مسیریابی تماس های بدون مجوز استفاده می‌شوند.
- دسترسی کاربر به کدهای مسیریابی وجود ندارد.
- به طور مکرر ازسامانه‌ها پشتیبان‌گیری می‌شود و در خارج سایت نگهداری می‌شود.
- چون PABXها با چندین پردازنده تنظیم شده‌اند، بنابراین سامانه تنها توسط یک نقطه معیوب نمی‌شود.
- باتری و منابع تغذیه UPS به کارمی روند.
- چندین مسیر مرتبط با خطوط تلفن آنالوگ پشتیبان برای کاربردهای اضطراری به PSTN به کار می رود.
- احراز هویت قوی در کلیه کانال های مدیریتی استفاده می‌شوند.(که ممکن است به معنای استفاده از تجهیزات اضافی طرف سومی باشد)
- شماره گیری های جعلی امکان پذیر نیست، و همچنین استفاده از مسیریابی غیرمجاز و یا از طریق سامانه پیام صوتی مرتبط امکان پذیر نیست.
- دستگاه های ضد کدهای مخرب
- سامانه تجزیه و تحلیل تماس نصب و هزینه تماس به طور منظم بررسی می‌شود.
- بازنگری تطابق و بررسی خدمات به طور منظم انجام می‌شود و نتایج پس ازآن عملی می‌شوند.

شایان ذکر است که سامانه‌های تلفنی PABX «سنتی» دیگر قدیمی شده‌اند، و تا حدی به سامانه‌های VoIP مهاجرت کرده اند و یا جایگزین شده‌اند (مطابق با بند ۱۱-۱۰)

الف-۹ همگرایی IP

الف-۹-۱ پس‌زمینه

از آنجایی که همگرایی IP (داده صدا و ویدئویی) محبوبیت یافت، مسائل امنیتی باید مشخص و بررسی شوند، اگرچه پیاده‌سازی های تلفنی در حال حاضر به کنترل های امنیتی برای جلوگیری از تخلفات جعلی و سایر حوادث امنیتی احتیاج دارند، این سامانه‌ها دریک شبکه داده منسجم فشرده نشده اند و در مقابل مخاطرات مشابه در شبکه‌های داده IP موضوعی نیستند. با همگرایی صدا و داده، کنترل های امنیتی برای کاهش مخاطرات مرتبط با حملات باید ارائه شوند.

یک نرم افزار کاربردی VoIP معمولا شامل یک نرم افزار مناسب میزبان بر روی یک سخت افزار و سامانه عامل موجود یا تجاری می‌باشد. تعداد خدمت گزارها بستگی به پیاده‌سازی ارائه شده و همچنین نحوه استقرار اصلی دارد. این اجزا از طریق IP بر روی اترنت ارتباط برقرار می‌کنند و در ارتباط تنگاتنگی از طریق سوئیچ و یا مسیریاب‌ها می باشند.

الف-۹-۲ مخاطرات امنیت

حوزه اصلی مخاطرات امنیت می‌تواند مرتبط با حملات بر پایه IP بر نرم افزار مخرب خاص ارائه کننده و یا سخت افزار و سامانه عامل میزبان نرم افزار کاربردی VoIP باشد. مخاطرات امنیت مرتبط با اجزای VoIP شامل مواردی است که مرتبط هستند با حملات بر پایه تجهیزات و نرم افزارهای شبکه، که می‌تواند توسط آسیب پذیری های طراحی و پیاده‌سازی راه حل های VoIP فعال شوند. مخاطرات امنیتی اصلی مرتبط با همگرایی IP شامل مواردی است که مرتبطند با :

- کیفیت خدمت – بدون وجود کیفیت خدمت، کیفیت ممکن است از بین برود، یا قطعی تماس‌ها در اثر از بین رفتن بسته‌ها و تاخیر در سراسر شبکه به وجود آید.
- عدم دسترسی خدمات بر اساس حملات انکار خدمت ، یا تغییر جدول مسیرها
- یکپارچگی و در دسترس بودن می‌تواند توسط کدهای مخرب (شامل ویروس‌ها) که می‌توانند ورود به شبکه را از طریق سامانه‌های ناامن VoIP مدیریت کنند و کاهش یا ازبین رفتن خدمات را در پی‌داشته‌باشند تاثیر پذیرد و می‌تواند در بین خدمت‌گزارهای شبکه پخش شود که منجر به خسارت حافظه‌ها می‌شود.
- هرزنامه از طریق تلفن IP (SPIT)
- نرم‌افزارهای تلفنی روی رایانه‌ها خطر قابل توجهی است که می‌توانند نقطه ورودی و رسوخ کدهای مخرب (شامل ویروس‌ها) باشند.
- خدمت‌گزارهای VoIP و سامانه‌های مدیریتی VoIP اگر در پشت دیواره‌های آتش محافظت نشوند، درمعرض خطر قرار دارند.
- امنیت شبکه داده با بازگذاشتن چندین درگاه بر روی دیواره‌های آتشبرای پشتیبانی VoIP می‌تواند کاهش یابد. یک ارتباط VoIP چندین پروتکل و شماره پورت های مرتبط دارد. H. 323 از چندین پروتکل برای

ارسال سیگنال‌ها استفاده می‌کند، و هر دوی H. 323 و SIP از RTP استفاده می‌کنند. نتایج نشان داده است که H. 323 تا یازده پورت مختلف را می‌تواند استفاده کند.

- فریب موضوع اصلی سامانه‌های تلفنی است، زمانیکه از VoIP استفاده می‌شود اگر امنیت لحاظ نشده باشد مخاطرات می‌توانند افزایش یابند. هکرها می‌توانند به دسترسی های غیر مجاز به سرویس های VoIP از طریق جعل ، حملات تکرار شونده، یا سرقت اتصال دست یابند.

- حقه تلفنی، یا تماس‌های غیرمجاز به شماره های زیاد، می‌تواند منجر به ضرر و زیان قابل توجهی شود.

- نقص های حفظ محرمانه بودن اطلاعات می‌تواند از طریق رهگیری ارتباطات، مانند«حمله غریبه‌ای در میان» در شبکه توسط کارمندان و سایر افرادی که به شبکه دسترسی دارند امکان پذیر است.

- استراق سمع تماس های صوتی

- از آنجایی که تلفن های IP به برق برای انجام عملیات نیاز دارند، شبکه تلفنی در صورت قطعی برق کاربردی ندارد

- احتمال خطای بیشتر در خدمات هم زمان صدا و داده به علت استفاده از اجزای مشترک وجود دارد، مانند یک شبکه محلی

الف-۹-۳ کنترل‌های امنیت

چندین کنترل امنیت فنی برای مدیریت مخاطرات از تهدیدات شناخته شده‌ی شبکه‌های همگرای IP وجود دارند که می‌توانند شامل :

- کیفیت خدمت باید در یک شبکه همگرا اجرا شود، در غیر این صورت احتمال کاهش کیفیت صدا وجود دارد. ارائه خدمات شبکه، و درجایی که امکان دارد، پیوند های IP باید از طریق فیبر به سایت تحویل داده شوند که ازکاهش لغزش (که بر کیفیت صدا تاثیر می گذارد) اطمینان حاصل کنند.

- کلیه خدمت گزارهای VoIP باحفاظت های نرم افزارهای مخرب تنظیم می‌شوند

- رایانه هایی که نرم افزارهای تلفنی را پشتیبانی می‌کنند باید با دیواره‌های آتش شخصی، نرم افزارهای بررسی و کدهای ضد مخرب (شامل آنتی ویروس) همراه باشند و به طور مکرر به روز رسانی شوند.

- خدمت‌گزارهای VoIP و سامانه‌های مدیریت VoIP باید در پشت دیواره آتش‌ها برای محفوظ ماندن از حملات حمایت شوند.

- استفاده از VLAN های اختصاصی برای هر یک از خدمات و رمزگذاری جریان داده های مختلف

- طراحان باید مطمئن شوند که تنها تعداد درگاه‌های محدودی در دیواره‌های آتش برای پشتیبانی خدمات VoIPباز می باشند.

- برای مبارزه با حقه‌ها کنترل های ضد جعل ، ضد بازگشتی باید برای جلوگیری از سرقت اتصال پیاده‌سازی شود.

- کلیه دسترسی‌ها به خدمت گزارهای مدیریتی باید تایید می‌شوند.

- IDS باید برای خدمت گزارهایی که خدمات VoIP را پشتیبانی می‌کنند در نظر گرفته شوند.

- رمزگذاری الگوی داده باید در جایی که اطلاعات حساس از طریق شبکه VoIP رد و بدل می‌شود در نظر گرفته شود.
- تلفن های IP باید توسط سوئیچ هایی که توسط UPSها پشتیبانی می‌شوند برق دریافت کنند.
- ممکن است احتیاج به ارائه خدمات همگرای صدا باشد، که یک منبع قدرت مستقل برای استفاده در مواقع اضطراری وجود دارد

الف-۱۰ میزبانی وب

الف-۱۰-۱ پس‌زمینه

میزبانی وب توسط تعداد زیادی از ارائه دهندگان خدمات شبکه در قالب خدمات استاندارد شده ارائه می‌شوند، که اغلب شامل امکانات پایگاه داده برای به کار بردن داده های پایدار و نیز یک محیط نرم افزاری اجرایی پایه می‌باشد. اگرچه بیشتر اجزای مورد نیاز پیاده‌سازی و آن هایی که خدمات میزبانی وب را ارائه می‌کنند در خارج محدوده این استاندارد قرار دارند (مانند خدمت‌گزار وب یا نرم افزار پایگاه داده)، بعضی از موارد قابل توجه در مورد کل خدمات که از نظر بسیاری از مردم میزبانی وب به عنوان قسمتی جدایی ناپذیر از ارائه یک شبکه می‌باشد، دراین جا مستند شده است.

سایت های میزبانی وب در خطر انواع تهدیدات قرار دارند، بخصوص در جاهایی که به اینترنت متصل هستند، برای مثال در جایی که سازمان‌ها ی برجسته درمعرض حملات گروه‌های حاشیه ای باشند. بنابراین، شناسایی تهدیدات بالقوه مهم است، و سپس کلیه آسیب پذیری هایی که می‌توانند توسط تهدیدات مورد سواستفاده قرار گیرند، مسدود شوند. این بهترین نتیجه توسط طراحی در مقابل موارد آسیب پذیر است. با پرداختن به این مسائل در مطابقت با راهنمایی های ارائه شده، طراحی وب سایتی ایمن، قابل اعتماد و با احتمال کم آسیب پذیری امکان پذیر است.

الف-۱۰-۲ مخاطرات امنیت

مخاطرات امنیت اصلی مرتبط با میزبانی وب شامل مواردی است که مرتبطند با :
- دسترسی مهاجم به نرم افزار کاربردی و داده با نقض یکی از موارد حفاظتی
- قرار گرفتن در معرض آسیب پذیری در اجزای زیر ساخت
- وجود چندین نقطه‌ی آسیب‌پذیر
- از دست دادن خدمات به دلیل خرابی سخت افزار
- عدم توانایی در قطع خدمات به منظور تعمیرات
- دسترسی ناخواسته توسط کاربران عمومی به مکان هایی که داده نگهداری می‌شود
- حملات درمقابل یکپارچگی داده (برای مثال خرابی های پایگاه‌های وب یا میزبانی محتوای غیرمجاز)
- نصب نرم افزارهای مخرب در سامانه
- سازش یک پایگاه وب با استفاده از عملیات سودهی
- عدم توانایی پشتیبان گیری بدون تحت تاثیر قرار دادن کارایی پایگاه

- افشای غیر مجاز حمله به امکانات برنامه آدرس دهی IP در پایگاه وب
- بهره برداری از ارتباط بین ایستگاه های مدیریت و پایگاه وب
- حملات نامحسوس
- مشکلات ردیابی نفوذ بین دستگاه ها
-عدم توانایی در بازیابی اطلاعات
- عدم توانایی به دسترسی الزامات توافق شده سطح خدمات
- عدم توانایی در حفظ تداوم خدمات
- استفاده غیرمجاز از خدمات وب، از جمله نقض خط‌مشی سازمان (مانند استفاده از خدمت گزار برای منافع شخصی) و عدم رعایت قوانین و مقررات (مانند نگهداری محتواهایی که حق کپی را نقض می‌کند و یا نگهداری عکس های نامناسب از کودکان)

الف-۱۰-۳ کنترل های امنیت

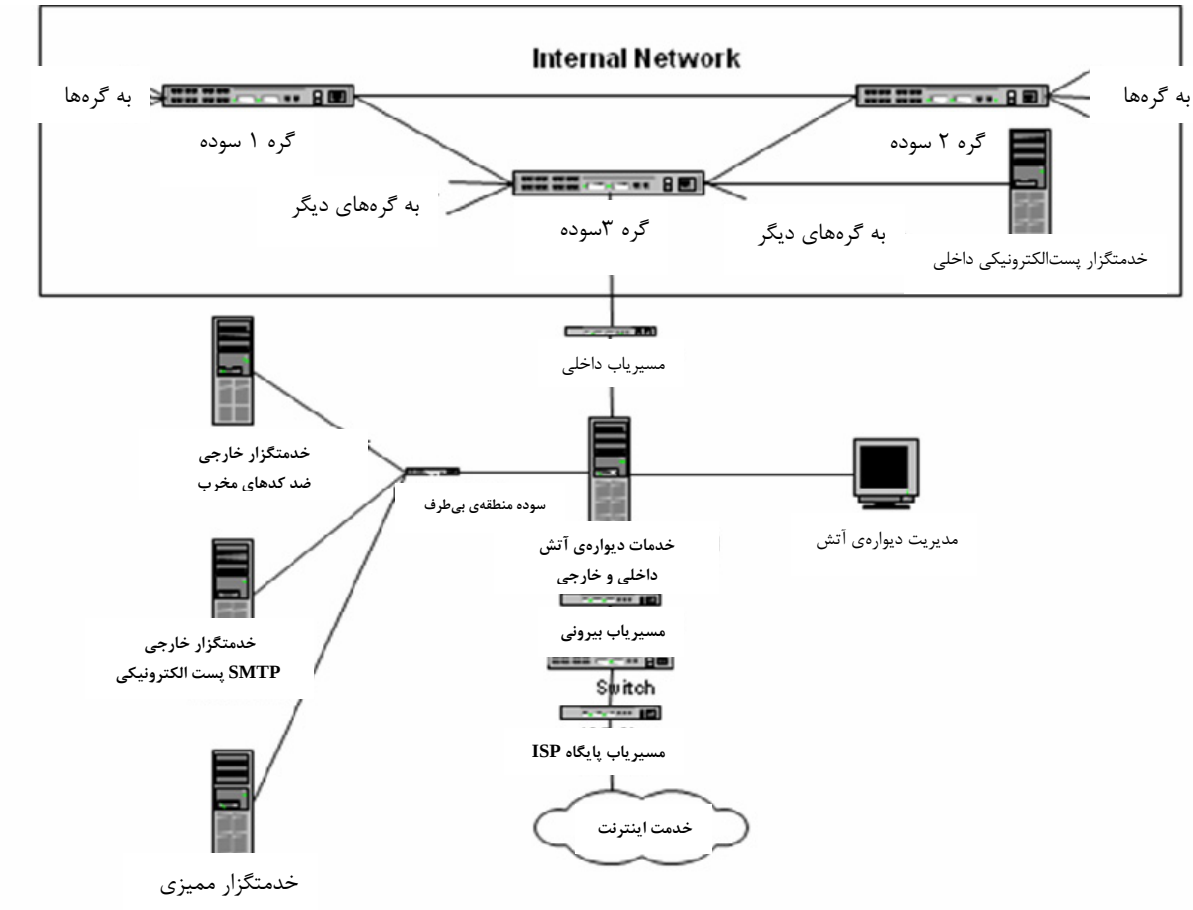
کنترل های فنی امنیت برای مدیریت مخاطرات تهدیدات شناسایی شده برای پایگاه‌های وب شامل :
- مقررات شدید امنیتی منطقه‌بندی و امنیت برای محدودکردن حملات موفق
- مشخصات انواع مختلف دیواره‌ی آتش برای مقابله با آسیب پذیری‌های دیواره‌ی آتش (اطلاعات بیشتر در مورد دیواره‌های آتش در بند الف-۶ بالا و ISO/IEC 27033-4 ارائه شده است)
- انعطاف پذیری، این طرح باید برای نقاط بالقوه‌ی شکست که باید محدود شوند آزمایش می‌شود.
-به اشتراک گذاری قطعی/بار برای محافظت در برابر خرابی تجهیزات
- استفاده از خوشه‌ها در جایی که دسترسی در محیط های ۲۴*۷ نیاز است
- خدمات خدمت‌گزار برای محدود کردن دسترسی به وب سایت و برای فعال کردن سطح بالایی از ورود به سامانه
- بررسی کامل مداوم برای تغییرات غیر مجاز داده
-کنترل‌های کد ضد مخرب (مانند آنتی ویروس) در ارسال‌ها برای جلوگیری از وارد شدن نرم‌افزارهای مخرب
- سودهی لایه ۲ به زور معمولاً در طراحی پایگاه وب استفاده می‌شود. سودهی لایه سه به غیر از الزامات مرتبط با کسب و کار نباید استفاده شود، برای مثال برای اشتراک‌گذاری ، به‌علاوه یک سوده یکسان نباید در هر دو سمت دیواره‌ی آتش استفاده شود. در طراحی سوده نقاط قابل بررسی باید در نظر گرفته شوند
شبکه‌های محلی مجازی بر اساس عملکردشان تقسیم بندی شده اند که به IDSها این امکان را بدهند که به راحتی با وجود حذف مجموعه ای از پروتکل‌ها در هر VLAN خود را وفق دهند. به علاوه اجرای پشتیبان گیری از VLAN به پشتیبان گیری این امکان را می‌دهدکه در هر زمانی از روز بدون اختلال کارایی سایت کار خود را انجام دهند

- با توجه به فعالیت های کسب و کار، نقشه آدرس دهی IP به منظور محدود کردن تعداد آدرس های عمومی به حداقل، با حفظ« اعتماد قوی» نقشه آدرس دهی IP با آگاهی آن‌که می‌تواند در پایگاه وب مورد حمله قرار می‌گیرد، به‌کار می‌رود.
- جایی که اتصال های مدیریتی در شبکه های عمومی به هم متصل می‌شوند، باید رمزگذاری شود (برای اطلاعات بیشتر در مورد دسترسی از راه دور ISO/IEC 27033-4 مشاهده شود) که شامل حداقل سامانه‌های هشدار/SNMP بر روی اتصالات پورت کنسول است.
- تمام تراکنشها و رویدادهای ثبت شده هر دستگاه در یک خدمت گزار ممیزی کپی می‌شوند، و در یک بستر پشتیبان‌گیری، مانند لوح‌فشرده کپی می‌شوند.
- زمان یکسان سازی خدمات ارائه شده به کلید اصلی برای تجزیه و تحلیل دسترسی های غیرمجاز و قابلیت ردیابی از طریق فایل های ثبت شده می‌باشد. این کار نیازمند آن است که زمان فایل های ثبت شده و همچنین خدمت گزارها به علاوه/منهای یک ثانیه یا کمتر باشد. (NTP مرتبط به این‌کار مربوط می‌شود، برای اطلاعات بیشتر بند ۱۰-۶ از ISO/IEC 27002 مشاهده شود)
-تجهیزات شبکه محلی برای کنترل تغییرات مدیریت نشده آدرس MAC تنظیم شوند.
- خدمات پشتیبان گیری مرکزی، ترجیح داده می‌شود که در زمان نیاز اجرا می‌شوند.
- پایگاه‌های وبی که احتیاج دارند در بیشتر مواقع ۲۴ ساعت در روز کار کنند، به سخت‌افزارهایی با کیفیت بالا که می‌توانند این شرایط را تحمل کنند نیاز دارند. زیرساخت خدمت گزار در پایگاه وب باید برای عملیات پشتیبانی« ۲۴*۷ »مشخص شود. سامانه عامل‌های پشتیبان باید قوی تر و کلیه خدمت گزارها و دیگر تجهیزات باید تحت آزمون‌های امنیتی قرار گیرند تا از قوی بودن کلیه تجهیزات اطمینان حاصل شود.
- پیاده‌سازی نرم‌افزارهای کاربردی قوی، که کدها در آن برای ساختار بررسی شده اند و به طور منطقی تصحیح شده اند، و از نرم افزار احرازهویت مورد تایید استفاده می‌کند.
- باید درنظر داشت که موارد مدیریتی تداوم کسب و کار به طور کامل در طراحی پایگاه‌های وب لحاظ نمی‌شوند. فعالیت های مدیریتی تجاری کاملا مداوم باید در رابطه با پایگاه وب اجرا شوند.

الف-۱۱ پست الکترونیکی اینترنتی

الف-۱۱-۱ پیش زمینه

استفاده از خدمات اینترنت در یک سازمان/شرکت برای دست یابی به الزامات قانونی تجارت با تهدیدات بسیاری همراه است که می‌تواند برای بهره برداری از سامانه‌های آسیب پذیر مورد استفاده قرار گیرد. بنابراین، پست الکترونیکی اینترنتی می‌تواند در معرض خطر انواع تهدیدات قرار گیرد، و هدف طراحی و اجرای راه حلی است که امن و قابل اعتماد باشد. شکل ۷ زیر نمونه راه حل بالقوه ای برای پست الکترونیکی اینترنتی است.



شکل ۷- مثالی برای راه‌حل پست الکترونیکی اینترنتی

سامانه‌های پست الکترونیکی (SMTP) برای همکاری با معماری فنی امنیت شبکه ساده هستند زیرا تنها باید نامه هایی را که دریافت می‌کنند بررسی و ارسال کنند. اطلاعاتی که جمع‌آوری می‌شوند باید شامل موارد زیر باشند :

- تعداد پیام‌های روزانه در هر سمت
- نوع و محتوای پیام هایی که اجازه داده می‌شوند
- تعداد و اندازه‌ی پیام‌های روزانه در هر سمت
- میانگین و حداکثر اندازه‌های پیام‌های اجازه داده‌شده
- جزییات سامانه نامه‌های داخلی
- جزییات رله نامه‌های داخلی، که با نامه‌های رله تعریف‌شده در معماری فنی امنیت ارتباط برقرار می‌کند
- جزییات سامانه (های) نامه های خارجی (که می‌تواند با / هر نامه رله در اینترنت، یا یکی از خدمت‌گزارهای نامه متعلق به ارائه دهنده خدمت باشد)
- جزییات الزامات احرازهویت خدمت‌گزار پست الکترونیکی برای ارتباطات داخلی و به ارتباطات پست الکترونیکی اینترنتی

- جزییات امکاناتDNS/WINS داخلی
- جزییات امکانات DNS برای اینترنت
- در صورت لزوم، مشخص شود چه دسترسی‌هایی به گروه‌های خبری نیاز است و اگر وجود دارد آیا مکان‌های محدودی که گروه‌های خبری به آن‌ها می‌توانند دسترسی داشته باشند، وجود دارد.
- آیا یکسان سازی زمان نامه/خدمت‌گزار برای اینترنت مورد نیاز است
- آیا بیش از یک مسیر به اینترنت وجود دارد
- الزامات بررسی کدهای مخرب (از جمله ویروس‌ها)

الف-۱۱-۲ مخاطرات امنیت

مخاطرات امنیت اصلی مرتبط با پست الکترونیکی اینترنتی شامل مواردی است که مرتبطند با :
- نفوذ غیر مجاز به شبکه سازمان‌ها / شرکت‌ها. تلاش در دسترسی غیرمجاز، از جمله شناسایی جعل هویت، که می‌تواند ۲۴ ساعته در روز صورت گیرد، بسیار پیچیده و خلاقانه شده‌است و می‌تواند برنامه های مخربی مانند پیش زمینه حملات انکار خدمت ، سو استفاده از منابع یا دست یابی اطلاعات با ارزش باشد.
- نصب کدهای مخرب، که می‌تواند شامل پیش زمینه‌ای از یک اسب تروآ که به جمع آوری اطلاعاتی مانند رمزها می‌پردازد و آن‌ها را به یک مکان خارجی ارسال می‌کند، باشد و یا امکاناتی برای از بین بردن کنترل دستگاه‌های راه‌دور. بنابراین، توجه خاصی به تهدیدات ترکیبی اخیر که کدهای مخرب شامل پایه‌بار[1] می‌باشند صورت گیرد.
- ارسال هرزنامه(هرزنامه یک تهدید قابل توجه خدمات پست الکترونیکی است- می‌تواند با استفاده از منابع شبکه برای مسیردهی هرزنامه‌ها و همچنین منابع سامانه برای درگاه های نامه ها، اثر منفی بر فعالیت های پست الکترونیکی داشته باشد، و می‌تواند برای انتشار نرم افزارهای مخرب مورد استفاده قرار گیرد
- رله هرزنامه (اگر خدمت گزار نامه‌ها به گونه‌ای تنظیم شده است که به رله نامه‌های ناشناس اجازه می‌دهد، می‌تواند توسط هرزفرست‌ها برای ارسال هرزنامه از طریق اینترنت با نام سازمان دارنده خدمت‌گزار پست‌الکترونیکی مورد استفاده قرار گیرد)
- جعل پست‌الکترونیکی (بسیار آسان است که هویت هر کاربر را به عنوان شخصی که در حال ارسال نامه است جا بزنیم)
- محتوای جعلی
- محتواهای نظارت نشده، سازمان را بدون آگاهی از اطلاعات امنیتی کارکنان نگه می‌دارد، که موارد قانونی و ضررهای بالقوه ای از مالکیت های معنوی را به همراه دارد.
- حمله مستقیم انکارخدمت به سامانه نامه‌ها

1 - Payload

- حمله انکارخدمت توزیع شده[1] که چندهزار پست‌الکترونیکی از چندین مکان برای نابودکردن خدمت‌گزارهای پست الکترونیکی ارسال می‌شوند.

الف-۱۱-۳ کنترل‌های امنیت

کنترل های امنیت برای پست الکترونیکی اینترنتی می‌تواند شامل :

- دیواره‌های آتش برای سطح اطمینان و مجموعه قوانین مناسب برای مخاطرات ارزیابی‌شده استفاده می‌شوند. برای بیشتر اهداف امنیتی، مجموعه قوانین اولیه باید از عبور تمام ترافیک عبوری از دیواره‌ی آتش جلوگیری کند. برای پست الکترونیکی، برای یک خدمت گزار پست الکترونیکی ارسال داده یه اینترنت و دریافت داده های ورودی از اینترنت کار معمولی است. همان طور که قبلا ذکر شد، پیشنهاد می‌شود که از دو دیواره‌ی آتش از شرکت های مختلف و یا سامانه عامل های مختلف استفاده شود.

- امکانات بایگانی و ممیزی با خدمات کامل یکسان سازی سازمان در کلیه اجزا، دیواره‌های آتش و خدمت گزارهای زیرساخت پشتیبانی می‌شوند. باید در طراحی به یکسان سازی زمان پرداخته شود، با توصیفی از ساعت اصلی و برنامه وراثتی برای خدمت گزارها و شبکه (ها). معمولا ساعت اصلی از طریق یک خدمت ماهواره ای موقعیت یابی جهانی (GPS) یا خدمات رادیویی زمان زمینی یکسان سازی می‌شود

- سامانه تبادل نامه اینترنتی (SMTP) به درستی برای تکمیل وظایف مرتبط با الزامات امنیتی توزیع شده است، از جمله ارائه‌ی رابط کاری با سازمان/ شرکت از اینترنت می‌باشد، و همچنین انتقال پست الکترونیکی از اینترنت به خدمت‌گزار پست‌الکترونیکی داخلی و برعکس. جلوگیری از رله پست الکترونیکی از اینترنت به آدرس های دیگر در اینترنت، و اطمینان پیدا کردن از آنکه نامه و پیوست هایش بدون درنظر گرفتن مسیر عاری از کدهای مخرب هستند.

- برای هر پست الکترونیکی دریافتی، به عنوان نتیجه جستجو در خدمت‌گزار DNS اینترنت، پیام‌ها به آدرس دیواره‌ی آتش سازمان هدایت می‌شوند، زمانی صورت می‌گیرد که توسط مسیریاب خارجی برای قسمت آدرس منبع خارج از محدوده آدرس های داخلی ، قبل از هدایت شدن به دیواره‌ی آتش، از اینترنت دریافت می‌شود. در دیواره‌ی آتش پیام باید برای یک قسمت آدرس خارج از فضای آدرس های داخلی و آدرس مقصد خدمت گزار نامه (که مسلما یک پست الکترونیکی بوده است) بررسی شود و سپس به خدمت‌گزار پست‌الکترونیکی SMTP هدایت شود. در خدمت‌گزار پست‌الکترونیکی SMTP ، پیام باید بررسی شود که از اینترنت بوده‌است، و سپس به خدمت‌گزار ضد کدهای مخرب برای بررسی ویروس‌ها و هر محتوای مخرب دیگر هدایت شود. در آخر، باید به خدمت‌گزار پست‌الکترونیکی داخلی برای توزیع توسط سامانه نامه داخلی ارسال شود. هر پیام دریافتی با آدرس نادرست باید حذف شود و در ثبت وقایع گنجانده شود. هر پیام دریافتی حاوی ویروس و یا سایر محتواهای مخرب باید قرنطینه شود و فرد یا گروه مناسب از آن اطلاع یابند.

- برای هر پست الکترونیکی ارسالی، پیام های فرستاده شده از طریق اینترنت ابتدا باید قبل از ارسال توسط خدمت‌گزار پست‌الکترونیکی SMTP خارجی برای هدایت شدن به اینترنت، توسط خدمت‌گزار

1- Distributed DoS

پست‌الکترونیکی داخلی به خدمت گزار ضد کدهای مخرب خارجی برای بررسی ویروس‌ها و هر محتوای مخرب دیگر ارسال شود. خدمت گزار نامه SMTP خارجی باید بررسی کند که آدرس خارج از محدوده آدرس داخلی است و برای دیگر مسیرهای پست الکترونیکی ارسال نشده است، سپس پیام را به اینترنت ارسال کند

- انتخاب یکی از دو گزینه ارسال پیام توسط نامه SMTP خارجی به تنها یک خدمت‌گزار پست‌الکترونیکی ISP برای مسیریابی بعدی یا هر آدرس نامه معتبر روی هر خدمت‌گزار پست‌الکترونیکی. گزینه اول باید امن‌تر باشد زیرا ISP (احتمالا کارشناس پست الکترونیکی) مسؤول سازمان‌دهی و پشتیبانی نامه‌های ارسالی است، اما می‌تواند تاخیر در تبادل پست الکترونیکی را به همراه داشته باشد. گزینه دوم قابل انعطاف تر است و تاخیر ناشی از ارسال به ISP را به همراه ندارد، اما اگر به درستی مدیریت نشود از امنیت کمتری برخوردار است- همچنین سازمان/شرکت باید پست الکترونیکی را به تعداد زیادی خدمت گزار نامه پشتیبانی کند و خطر حذف پست الکترونیکی را اگر رله پست الکترونیکی توسط خدمت‌گزار پست‌الکترونیکی راه دور تشخیص داده نشود، به همراه دارد. اگرچه می‌توان توسط روندهای احرازهویت بین خدمت گزارهای نامه مربوطه بر آن غلبه کرد. این که کدام گزینه انتخاب شود به ارزش های فنی راه حل و سطح تخصصی کسانی که پشتیبانی سامانه پست الکترونیکی را برعهده دارند بستگی دارد.

- معیارهای کنترل دسترسی باید براساس اصل حداقل امکانات پیاده سازی شوند.

- خدمت‌گزار پست‌الکترونیکی برای مسدودکردن یا حذف پست‌های الکترونیکی که شامل پیوست‌هایی هستند که معمولا کدهای مخرب را انتشار می‌دهند تنظیم شده اند، مانند :فایل های scr .،pif. ، . exe. vbs،bat .

- رایانه‌های آلوده برای جلوگیری از انتشارهای بیشتر باید به سرعت از شبکه حذف شوند و تجزیه و تحلیل ترمیمی قانونی اجرا و مرمت توسط بسترهای قابل اعتماد صورت گیرد.

- کارکنان باید آموزش ببینند که پیوست‌ها را به غیر از حالتی که خودشان در انتظار آن فایل هستند باز نکنند و نرم افزارهای نصب شده از طریق اینترنت را اجرا نکنند مگر اینکه برای یافتن کدهای مخرب بررسی شده باشد.

- فهرست‌های کنترل دسترسی در مسیریاب‌ها استفاده می‌شوند. فهرست‌های کنترل دسترسی مسیریاب مشخص می‌کنند چگونه با بسته‌ی IP ورودی با عملیات خاصی مانند ارسال مجدد، ثبت وقایع و یا حذف (یا جلوگیری) برخورد کنند، با ترکیب خط‌مشی های معمول مناسب مسیریاب (مانند حذف همه) ، امکان تعریف مجموعه قوانین برای یک مسیریاب که تا حد زیادی در حفظ امنیت شبکه موجود کمک می‌کند، وجود دارد.

- ضدفریب‌ها را فعال کنید. فریب به موقعیتی می‌گویند که منبع (منشا) آدرس پیام به گونه ای نشان داده‌شود که از طرف کسی یا جایی به غیر از منشا اصلی می‌آید. معیارهای ضدفریب به گونه ای پیام‌های اینترنتی را که ادعا می‌کنند از درون سازمان نشات گرفته‌اند، قبول نمی‌کنند، و برعکس (RFC 2827 فیلتر نفوذهای شبکه مشاهده شود: برای جزییات بیشتر، شکست محرومیت از خدمات)

- پیشکارهای[1] نامه الکترونیکی را فعال کنید. یک پیشکار، خدمت‌گزاری است که به عنوان واسط بین کاربر رایانه/ایستگاه کاری و اینترنت عمل می‌کند. بنابراین این اقدام مهم می‌تواند از خدمات امنیت، کنترل‌های مدیریتی و ذخیره اطمینان پیدا کند. امنیت به شرح زیر اجرا می‌شود:

- بررسی اطلاعات برای الگوهای شناخته شده (برای مثال، بررسی کلمات حساس برای اطمینان از انطباق)
- تبدیل بین آدرس های داخلی و خارجی
- ثبت وقایع از درخواست‌ها و درخواست کننده ها
- امکانات ضد کدهای مخرب براساس خدمت‌گزارها

خدمت‌گزارها می‌توانند محتوای مخرب را به وسیله پردازش ساده درخواست بررسی کنند. اگر درخواست مخرب باشد، احتمال این که خود خدمت‌گزار از کار بیافتد وجود دارد. از آنجایی که خدمت‌گزارها عموما در منطقه‌های بی‌طرف ارائه می‌شوند، یک منطقه‌ی نیمه مطمئن، به عنوان یک «فیوز» برای حمایت از درخواست کننده‌ی واقعی یا خدمت‌گزار رفتار می‌کند.

- کنترل‌های کد ضدمخرب بر روی خدمت‌گزار پست الکترونیکی اجرا می‌شوند. زمانی که سیستم‌های اطلاعاتی از کدهای مخرب عاری شدند (ازجمله ویروس‌ها)، تنها مسیر برای کد مخرب معرفی می‌شود توسط معرفی آن به عنوان داده (یا برنامه) است. بنابراین امکانات پست الکترونیکی، اولین انتخاب برای انتقال کدهای مخرب است ، و نقاط اولیه برای پیاده‌سازی کنترل‌های کد ضد مخرب را ارائه می‌کند. به‌طور معمول کنترل‌ها شامل امکاناتی برای قرنطینه‌ی فایل‌های مشکوک(برای مثال، بر اساس نوع محتوا) و غربالگری آدرس‌های پست‌الکترونیکی درخواست شده در مقابل لیست سیاه است. علاوه بر این، برای مقابله با تهدیدات ترکیبی اخیر، که کد مخرب شامل محتوای با ارزش، مسدود کردن پیوست‌های مخصوص شامل کدهای اجرایی باید مورد توجه قرار گیرد.

- فناوری‌های ضدهرزنامه ارائه شده است و کاربران برای حفاظت از آدرس‌های پست‌الکترونیکی در زمان دسترسی به سایت‌ها آموزش دیده‌اند.

- ضدرله بر روی خدمت‌گزارهای پست الکترونیکی و جستجوی معکوس DNS اجرا می‌شوند. یکی از راه‌های ممکن که خدمت‌گزار پست‌الکترونیکی می‌تواند از اینترنت مورد استفاده قرارگیرد این است که به آن یک پیامی که در حقیقت به طرف سومی مسیردهی شده، ارسال شود. سپس اگر خدمت‌گزار پست الکترونیکی پیام را قبول کرد به طرف سوم ارسال می‌شود، ظاهرا از سازمان/ شرکت به جای منشا اصلی. چنین مکانیزمی می‌تواند توسط «هرز فرست‌ها » یا نابودکردن شبکه‌ی سومی توسط حملات انکار خدمت مورد استفاده قرارگیرد. کنترل های ضدرله تشخیص می‌دهند که پست الکترونیکی دریافتی برای سازمان/شرکت است یا خیر. اگر نباشد، پست الکترونیکی ثبت(یا قرنطینه) می‌شود و خدمت‌گزار پست الکترونیکی کار دیگری انجام نمی‌دهد.

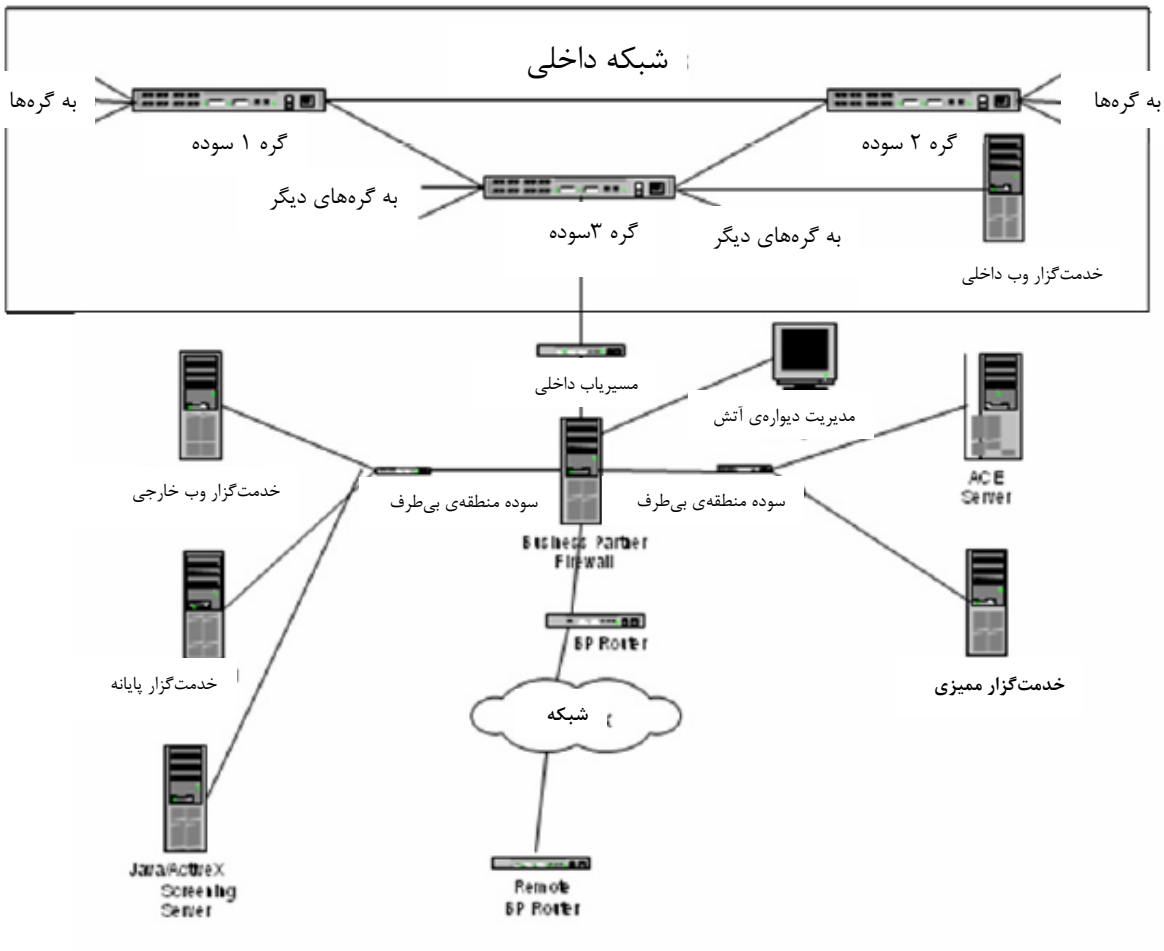
1 - Proxy

- هشدارها و درگاه‌های SNMPv3 را فعال کنید. SNMP می‌تواند برای کنترل از راه دور تجهیزات شبکه به‌کار رود و برای دستگاه که پیام‌هایی (یا درگاه‌هایی) را جهت آگاهی ایستگاه نظارت از شرایط دستگاه ارسال کند. این پروتکل نسبتا ناامن است و ترجیحاً برای اهداف کنترلی دستگاه استفاده نمی‌شود. اگرچه، درگاه‌های SNMP به طور گسترده استفاده می‌شوند و از طریق شبکه برای آگاهی محل مرکزی آمارها و شرایط خطا ارسال می‌شوند.
- مدیریت ممیزی اجرا شود. کلیه وقایع ثبت شده مربوط به پست الکترونیکی باید در خدمت‌گزار ممیزی نگهداری شوند و روزانه برای فعالیت های معمولی بررسی شوند. این وقایع ثبت شده شامل وقایع دیواره‌ی آتش و خدمت‌گزار پست الکترونیکی SMTP می‌شوند. این موارد ثبت شده باید با استفاده از کیفیت رویداد ارتباط و ابزار تجزیه و تحلیل بررسی شوند
- مدیریت دیواره‌ی آتش خارج از محدوده (OOB) نهادینه شود. این امر به آن اشاره دارد که از شبکه های مختلف برای داده و مدیریت استفاده شود تا اطمینان حاصل شود که افراد حمله کننده قادر به برقراری ارتباط با تجهیزات مورد هدفشان (در این مورد، دیواره‌ی آتش) نیستند. روش های زیادی برای مدیریت OOB وجود دارد:
- مدیریت تنها با دسترسی فیزیکی
- شبکه مدیریتی جداگانه
- استفاده از VLANها برای ایجاد کانال های جداگانه در شبکه داده، که امکان جداسازی ترافیک داده و مدیریتی را می‌دهد
در غیر این صورت مدیریت تنها با دسترسی فیزیکی صورت می‌گیرد.

الف-۱۲ دسترسی مسیریابی شده به طرف سوم

الف-۱۲-۱ پیش زمینه

از آنجایی که سازمان‌ها گرایش به کار گروهی پیدا کرده‌اند، ارتباطات طرف سوم با سایر سازمان‌ها افزایش یافته است، که احتیاج به یک اتصال مستقیم و امکانات درگاه بین سازمان‌ها دارد. شکل ۸ زیر نمونه‌ای از راه‌حل فنی امنیتی برای دسترسی مسیریابی شده با سازمان‌های طرف سوم است.



شکل ۸ – مثالی از یک دسترسی مسیریابی شده برای راه‌حل سازمان طرف‌سوم

دسترسی مسیریابی شده به سایر سازمان‌ها می‌تواند با فناوری‌های شبکه های گسترده یا پهنای باند صورت گیرد، و به دلایل زیادی مورد نیاز می‌شود، برای مثال دسترسی می‌تواند نیازمند پایگاه داده نرم افزار کاربردی در هر دو سمت باشد- که در این صورت یا کد غیرمجاز می‌تواند مطرح شود یا دسترسی غیرمجاز کاربران شبکه به شبکه‌ی دیگر می‌تواند صورت گیرد. اطلاعات جمع آوری شده باید موارد زیر را دربرگیرند :

- کدام برنامه های کاربردی باید از طریق اتصال‌های مسیریابی پشتیبانی شوند.
- جزییات خدمت‌گزارهای ارتباطی و مکان هایی که در آن قرار گرفته اند.
- جزییات رایانه های کاربر و این که در کجا قرار گرفته اند.
- جزییات مسیریاب سازمان دیگر در صورت وجود (از جمله آدرس IP ، روش های شناسایی، برای مثال، گواهی نامه‌ها ، رازهای مشترک، RADIUS ، +TACACS)
- نوع و سرعت اتصال‌های ارتباطی، برای مثال VPN از طریق پهنای باند، frame-relay ، اتصال سیمی مخصوص، شماره‌گیری و ISDN

منطقی است که برای هر دسترسی از سوی طرف سوم ، در صورت عدم وجود یک سند پیکربندی تهیه شود، که شامل دیدی کلی از الزامات، پیکربندی شبکه ، اطلاعات پیکربندی وجزییات آدرس دهی IP و شناسایی باشد. (وقتی دسترسی مسیریابی شده به سازمان‌های طرف سوم را درنظر می‌گیرید به طور معمول به راهنمای ISO/IEC TR 14516:1999 برای استفاده در مدیریت خدمات طرف سوم مراجعه کنید.)

الف-۱۲-۲ مخاطرات امنیت

مخاطرات امنیت اصلی مرتبط با دسترسی به سازمان‌های طرف سوم در اصل مرتبط با این اصل است که هر سازمان یک دامنه امنیتی جداگانه با خط‌مشی‌های خودش می‌باشد- و ممکن است به امنی سازمان شما نباشد. بنابراین، مخاطرات امنیتی اصلی مرتبط با دسترسی مسیریابی شده به سازمان‌های طرف سوم شامل مواردی است که مرتبطند با :

- دسترسی غیرمجاز به شبکه شما و «سامانه‌ها»ها و اطلاعات مربوط به آن
- وارد کردن کدهای مخرب از طریق درگاه‌های قابل اعتماد همیشگی
- حمله انکار خدمت از طریق سازمان طرف‌سوم
- باور این‌که شبکه‌ی طرف‌سوم از امنیت بالاتری نسبت به اینترنت برخوردار است

الف-۱۲-۳ کنترل های امنیت

کنترل های امنیت برای دسترسی مسیریابی شده به سازمان‌های سوم شامل :

- همه اتصالات سوم با دیواره‌ی آتش های مختلف جداسازی شده باشند که برای اینترنت و دسته بندی‌های دیگری از ارتباطات خارجی استفاده می‌شود
- وجود نرم افزارهای ضدکدهای مخرب، از جمله آنهایی که با دیواره‌ی آتش‌ها کارمی‌کنند که برای کدهای جاوا و ActiveX بررسی می‌شوند (همان طور که اشاره شد، چنین کدهایی با نرم افزارهای کدهای ضد مخرب معمولی (از جمله آنتی ویروس) به عنوان ویروس تشخیص داده نمی‌شوند. بنابراین نمی‌توانند تشخیص داده شوند و امکان بررسی معتبر بودن آنان وجود ندارد)
- یک نشانه‌ی قوی یا شناسایی کارتی اعمال شود، از طریق گواهی نامه های دیجیتالی با کلیدهای fob یا کارت های هوشمند، یا با دوعامل شناسایی توسط نشانه‌ها
- اگر ارتباطات از طریق دسترسی مسیریابی شده ISDN است، CLID به عنوان روش شناسایی اضافه استفاده شود.
- مسیریاب‌ها، از جمله در نقاط پایانی اتصالات، توسط یک خدمت گزار احرازهویت (مانند +TACACS) شناسایی شوند. اگرچه به هیچ روش شناسایی که مورد توافق سازمان سوم باشد دست نخواهید یافت، بنابراین رازهای به اشتراک گذاشته شده در پیاده سازی های کوچک می‌توانند استفاده شوند، که تبادل رمزهای عبور می‌باشد. برای اتصالات زیاد، گواهی نامه های دیجیتالی که به طور منظم تغییر می‌کنند باید استفاده شوند.

- مسیریاب سازمان طرف سوم باید از روش شناسایی یکسانی استفاده کند. برای مثال، گواهی نامه های دیجیتالی، رازهای به اشتراک گذاشته شده، RADIUS ، +TACACS .
- مسیریاب‌ها در دوسر اتصال از نظر فیزیکی امن باشند.
کلیه اتصالات طرف سوم توسط شرایطی برای اسناد اتصال امن پوشش داده شوند که توسط هر سازمان طرف سوم قبل از اجازه اتصال تایید شده باشند.
- استفاده از IDS/IPS لحاظ شود.
- ممیزی و حسابرسی اجرا شود.
- برای هر دسترسی طرف سوم، یک سند تنظیمات تهیه و تایید شود که شامل الزامات کلی، پیکربندی شبکه، اطلاعات تنظیمات و جزییات آدرس دهی IP و روش های شناسایی باشد. .

الف-۱۳ مرکز داده درون‌نت

الف-۱۳-۱ پیش زمینه

مراکز داده درون‌نت حیاتی ترین برنامه های کاربردی و داده را برای سازمان‌ها نگهداری می‌کنند. مرکز داده می‌تواند حیاتی ترین قسمت زیرساخت سازمان باشد و نگرانی های خاص خود را از جنبه های دیگری که در این ضمیمه شبکه را پوشش می‌دهددارد. اگرچه ذخیره سازی (SANها) و جنبه های میزبانی تکی در مراکز داده خارج از محدوده این استاندارد می‌باشند (مانند محافظت خدمت گزارها و پایگاه های داده) برخی از ملاحظات درباره امنیت کلی مرکز داده در اینجا مستند شده است.
تهدیداتی که مدیران امنیت فناوری با آن مواجه هستند از تلاش های نسبتا بی اهمیتی برای انتقام های ویران کننده در شبکه‌ها تا حملات پیچیده با هدف سود و سرقت داده های حساس شرکت رشد کرد. پیاده سازی امکانات قوی امنیت مرکز داده برای حفاظت برنامه های کاربردی حساس عملیات حیاتی و داده دلیل اصلی تلاش برای امنیت شبکه های سازمانی است.
از آنجایی که مسئولیت اصلی امنیت مرکز داده برای حفظ دسترسی خدمات است، روش هایی که امنیت بر جریان ترافیک، مقیاس پذیری و شکست تاثیر دارد باید لحاظ شود.

الف-۱-۳-۲ مخاطرات امنیت

روش‌های حملات به سطح بالایی برای از بین بردن حفاظت شبکه‌ها و با هدف دسترسی مستقیم به برنامه‌های کاربردی جهش پیداکرده است. حملات بر پایه HTTP ، XML و SQL از جمله تلاش‌های موثر حمله کننده‌ها هستند زیرا این پروتکل‌ها به طور معمول اجازه دارند به شبکه سازمان‌ها راه یابند و به اینترنت مرکز داده وارد شوند.
در ادامه چندین روش تهدیدآمیز که درون‌نت مرکز داده را تحت تاثیر قرار می‌دهند، آورده شده است:
- دسترسی غیرمجاز به داده
- دسترسی غیرمجاز به برنامه کاربردی
- دسترسی غیرمجاز به تجهیزات

- قطع خدمات حیاتی از طریق حملات انکار خدمت
- حملات تشخیص داده نشده
- از دست دادن داده
- عدم قابلیت بازگرداندن داده
- حملات هدفمند برای تغییر داده
- اضافه کردن امتیاز و مجوزها
- نصب کدهای مخرب
- استفاده از خدمت‌ها به طور غیرمجاز ، از جمله نقض خط‌مشی های سازمان

الف-۱۳-۳ کنترل های امنیت

کنترل های فنی امنیت برای مراکز داده می‌توانند شامل :

- درگاه های امنیتی برای کنترل دسترسی به مرکز داده
- استفاده از IPS/IDS در مرکز داده
- کنترل های کد ضد مخرب (شامل آنتی ویروس) برای میزبان‌ها
- مدیریت امن تجهیزات زیرساخت
- قابلیت‌های ورود به سامانه و ممیزی پشتیبانی شده توسط خدمات یکسان‌سازی کامل زمان در کلیه اجزای مرکز داده
- طرح تداوم کسب وکار برای خرابی ها
- طراحی انعطاف پذیر
- بررسی‌های منظم تغییرات غیرمجاز در داده ها
- استفاده از VLANها در تقسیم بندی خدمات در مرکز داده برای حفاظت از خدمات حساس
- تنظیم تجهیزات شبکه محلی برای کنترل تغییرات غیر مدیریت شده در آدرس های MAC
- استفاده از پروتکل های مدیریتی امن

پیوست ب

(اطلاعاتی)

مراجع مشابه بین کنترل های مرتبط با امنیت شبکه بـین ISO/IEC 27001 و ISO/IEC 27002 و بنـدهای داخل این قسمت از ISO/IEC 27033

جدول ب-۱ - مراجع مشابه بین کنترل های مرتبط با امنیت شبکه بین ISO/IEC 27001 و ISO/IEC 27002 و بندهای داخل این قسمت از ISO/IEC 27033

بند ISO/IEC 27001 و ISO/IEC 27002	مقررات	بند ISO/IEC 27033-1
۱۰-۴-۱ کنترل در برابر کدهای مخرب	تشخیص، پیشگیری و بهبود کنترل برای محافظت در برابر کدهای مخرب و روش های مناسب آگاهی کاربر باید اجرا شود	۸-۷ حفاظت در برابر کد مخرب
۱۰-۴-۲ کنترل در برابر کدهای تلفن همراه	جایی که استفاده از کد تلفن همراه مجاز است، باید اطمینان حاصل شود که تنظیمات کد تلفن همراه مجاز با توجه به خط‌مشی امنیتی که به روشنی تعریف شده عمل کند، و باید از اجرای کد های تلفن همراه غیر مجاز جلوگیری شود	۷-۲-۲-۲ معماری، نرم افزار کاربردی و خدمات شبکه
۱۰-۶-۱ کنترل های شبکه	شبکه‌ها باید به منظور محافظت در مقابل تهدیدات ، و برای حفظ امنیت سیستم‌ها و برنامه های کاربردی مورد استفاده در شبکه، از جمله اطلاعات تبادلی به درستی مدیریت و کنترل شوند.	توضیحات مقابل بندهای ۱۰-۶-۱ IG الف) تا ث) از ISO/IEC 27001/27002 مشاهده شود
۱۰-۶-۱ IG الف)	مسئولیت های عملیاتی برای شبکه‌ها در جاهای مناسب از عملیات کامپیوترها باید جدا شود	۸-۲ مدیریت امنیت شبکه
۱۰-۶-۱ IG ب)	مسئولیت‌ها و روش های مدیریت تجهیزات از راه دور، از جمله تجهیزات در مناطق کاربر، باید توزیع شوند	۷-۱۱ خدمات دسترسی از راه دور (برای جزییات بیشتر به ISO/IEC 27033-5 مراجعه شود)
۱۰-۶-۱ IG پ)	کنترل های ویژه باید به منظور حفظ محرمانه بودن و تمامیت داده‌ها هنگام عبور از روی شبکه های عمومی و یا از شبکه های بی سیم لحاظ شود، و برای	کلیه کنترل‌ها در ۱۱ مباحث «فناوری » مخاطرات، تکنیک های طراحی و مسائل مربوط به کنترل

	حفاظت از سامانه‌های متصل شده و برنامه های کاربردی(بندهای۴-۱۱ و ۱۲-۳ مشاهده شود) کنترل های ویژه ای نیز ممکن است برای حفظ در دسترس بودن خدمات شبکه و کامپیوترهای متصل مورد نیاز شوند.	
۱۰-۶-۱ IG ت)	ورود مناسب و نظارت باید اعمال شود تا ضبط اقدامات امنیتی مربوطه را امکان پذیر کند.	۸-۵ محاسبات ورود و مدیریت شبکه
۱۰-۶-۱ IG ث)	فعالیت های مدیریتی باید هم بهینه سازی خدمت به سازمان و هم اطمینان پیدا کردن از کنترل به طور مداوم سراسر زیرساخت های پردازش اطلاعات را هماهنگ کند	۸-۲ مدیریت امنیت شبکه
۱۰-۶-۲ امنیت خدمات شبکه	باید ویژگی های امنیتی، سطح خدمات و مدیریت مورد نیاز همه خدمات شبکه شناخته شود و در هر توافقنامه خدمات شبکه گنجانده شود، که آیا این خدمات ارائه شده درونی یا برون سپاری است.	۸-۲ مدیریت امنیت شبکه (و مرتبط با بندهای دیگر ۸ زیربند و بندهای ۹ تا ۱۱)
۱۰-۸-۱خط‌مشی های تبادل اطلاعات و روندها	خط‌مشی های تبادل رسمی، روندها باید برای حفاظت تبادل اطلاعات از طریق استفاده از انواع امکانات ارتباطی لحاظ شود	۶-۲ طراحی و مدیریت امنیت شبکه
۱۰-۸-۴ پیام های الکترونیکی	اطلاعات پیام‌های الکترونیکی باید محافظت شود	الف-۱۱ پست الکترونیکی اینترنتی
۱۰-۹-۱ تجارت الکترونیکی	اطلاعات تجارت الکترونیکی که از شبکه های عمومی عبور می‌کند باید از فعالیت های مخرب، اختلاف قرارداد و افشای غیر مجاز و اصلاح محافظت شود	۱۰-۴ تجارت درخدمات کسب و کار ۱۰-۵ تجارت درخدمات مشتری
۱۰-۹-۲ معامله بر خط	اطلاعات مربوط در معاملات روی خط باید برای جلوگیری از انتقال ناقص، گم کردن مسیر، تغییر پیام های غیر مجاز، افشای غیر مجاز، تکرار پیام های غیر مجاز و یا پاسخ محافظت شوند.	۱۰- ۵ تجارت درخدمات مشتری
۱۰-۹-۳ اطلاعات در دسترس عمومی	یکپارچگی اطلاعات موجود در سامانه‌های عمومی در دسترس ، باید برای جلوگیری از تغییر غیرمجاز محافظت شود.	الف-۱۰ میزبانی وب

۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه	کاربران تنها باید به خدماتی که مجاز به دسترسی به آنها هستند دستیابی داشته باشند	۸-۲-۲-۲ خط‌مشی امنیت شبکه
۱۱-۴-۲ شناسایی کاربر برای اتصالات خارجی	روش‌های شناسایی مناسب باید برای کنترل دسترسی کاربران از راه دور استفاده شوند	۸-۴ شناسایی و تصدیق هویت
۱۱-۴-۳ شناسایی تجهیزات در شبکه	شناسایی خودکار تجهیزات باید به عنوان وسیله‌ای برای تأیید هویت اتصالات از مکان‌های خاص و تجهیزات در نظر گرفته شود.	
۱۱-۴-۴ حفاظت از پورت تشخیصی و پیکربندی از راه دور	دسترسی به پورت‌های تشخیصی و پیکربندی فیزیکی و منطقی باید کنترل شود	
۱۱-۴-۵ تبعیض در شبکه ها	گروه های خدمات اطلاعات، کاربران و سامانه‌های اطلاعاتی باید در شبکه جدا باشند.	
۱۱-۴-۶ کنترل اتصالات شبکه	برای شبکه های به اشتراک گذاشته شده، به ویژه کسانی که در سراسر مرزهای این سازمان گسترش پیدا کرده‌اند، قابلیت کاربران برای اتصال به شبکه باید در راستای خط‌مشی‌های کنترل دسترسی و نیازهای برنامه‌های کاربردی کسب و کار محدود باشد.	۱۱- مباحث «فناوری» مخاطرات، تکنیک های طراحی و مسائل مربوط به کنترل
۱۱-۴-۷ کنترل مسیریابی شبکه	کنترل مسیریابی باید برای شبکه های اجرا شود تا اطمینان حاصل شود که قابلیت اتصال به کامپیوتر و جریان اطلاعات، خط‌مشی کنترل دسترسی برنامه های کاربردی کسب و کار را نقض نکرده است.	الف-۶ درگاه های امنیتی

جدول ب-۲ مراجع مشابه بین بندهای این قسمت از خانواده استاندارد ISO/IEC 27033 و ISO/IEC 27001 و ISO/IEC 27002

بند ISO/IEC 27033-1	مقررات	بند ISO/IEC 27001 و ISO/IEC 27002
۶	مرور کلی	
۶-۲	طراحی ومدیریت امنیت شبکه	۱۰-۸-۱ اطلاعات خط‌مشی های تبادل و روندها
۷	شناسایی مخاطرات و آماده شدن برای شناسایی کنترل های امنیتی	
۷-۲	اطلاعات شبکه فعلی و/یا در نظر گرفته شده	
۷-۲-۱	نیازمندی های امنیتی در اطلاعات خط‌مشی امنیتی شرکت	
۷-۲-۲	اطلاعات شبکه فعلی/ در نظر گرفته شده	
۷-۲-۲-۲	معماری، نرم افزار کاربردی و خدمات شبکه	۱۰-۴-۲ کنترل در برابر کد تلفن همراه
۷-۲-۲-۳	انواع اتصالات شبکه	
۷-۲-۲-۴	مشخصات دیگر شبکه	
۷-۲-۲-۵	اطلاعات دیگر	
۷-۳	اطلاعات مخاطرات امنیتی و پتانسیل مناطق کنترلی	
۸-۲	مدیریت امنیت شبکه	۱۰-۶-۱ کنترل های شبکه
۸-۲-۲	فعالیت های مدیریت امنیت شبکه	
۸-۲-۲-۲	خط‌مشی امنیت شبکه	۵-۱ خط‌مشی امنیت اطلاعات
		۱۱-۴-۱ خط‌مشی استفاده از خدمات شبکه
۸-۲-۲-۳	روندهای عملیاتی امنیت شبکه	
۸-۲-۲-۴	بررسی پذیرش امنیت شبکه	
۸-۲-۲-۵	شرایط امنیتی برای اتصالات شبکه	
۸-۲-۲-۶	شرایط امنیتی مستند شده برای کاربران راه دور	
۸-۲-۲-۷	مدیریت حادثه امنیت شبکه	۱۳ مدیریت حادثه امنیت اطلاعات

۸-۲-۳	قوانین امنیت شبکه و مسئولیت ها	۸-۱-۱ نقش‌ها و مسئولیت ها
۸-۲-۴	نظارت شبکه	۱۰-۱۰ نظارت
۸-۲-۵	ارزیابی امنیت شبکه	
۸-۳	مدیریت آسیب پذیری فنی	۱۲-۶ مدیریت آسیب پذیری فنی
۸-۴	شناسایی و تصدیق هویت	۱۱-۴-۲ شناسایی کاربر برای اتصالات خارجی
		۱۱-۵-۲ احرازهویت و شناسایی کاربر
۸-۵	محاسبات ورود و نظارت شبکه	۱۰-۶-۱ کنترل های شبکه
		۱۰-۱۰-۱ حسابرسی ورود
۸-۶	تشخیص نفوذ و پیشگیری	
۸-۷	حفاظت در برار کدهای مخرب	۱۰-۴ حفاظت در برابر کدهای مخرب و تلفن همراه
۸-۸	خدمات بر اساس رمزگذاری	۱۲-۳ کنترل های رمزگذاری
۸-۹	مدیریت تداوم کسب و کار	۱۴ مدیریت تداوم کسب و کار
۹	راهنمای طراحی و پیاده سازی شبکه	
۹-۲	طراحی/معماری امنیت فنی شبکه	
۱۰	طرح‌های مرجع شبکه – مخاطرات، طراحی، روش‌ها و موضوعات کنترلی	
۱۰-۲	دسترسی به اینترنت برای کارمندان	
۱۰-۳	خدمات همکاری پیشرفته	
۱۰-۴	تجارت در خدمات تجاری	۱۰-۹-۱ تجارت الکترونیکی
۱۰-۵	تجارت درخدمات مشتری	۱۰-۹-۱ تجارت الکترونیکی
		۱۰-۹-۲ تبادلات بر خط
۱۰-۶	خدمات برون سپاری	
۱۰-۷	تقسیم بندی شبکه	
۱۰-۸	ارتباطات تلفن همراه	
۱۰-۹	پشتیبانی شبکه برای کاربران در حال سفر	
۱۰-۱۰	پشتیبانی شبکه برای شرکت های خانگی و تجاری کوچک	
۱۱	مباحث «فناوری» – مخاطرات،	۱۰-۶-۱ کنترل های شبکه

	تکنیک‌های طراحی و مسائل مربوط به کنترل	
		۱۱-۴-۶ کنترل اتصالات شبکه
۱۲	اجرا و بررسی راه‌حل‌های امنیت	
۱۳	اجرای راه‌حل امنیتی	
۱۴	نظارت و بازنگری راه‌حل‌های پیاده‌سازی	
پیوست الف	مباحث «فناوری» – مخاطرات، تکنیک‌های طراحی و مسائل مربوط به کنترل	
الف-۱	شبکه‌های محلی	
الف-۲	شبکه‌های گسترده	
الف-۳	شبکه‌های بی سیم	
الف-۴	شبکه‌های رادیویی	
الف-۵	شبکه‌های پهنای باند	
الف-۶	درگاه‌های امنیتی	۱۱-۴-۷ کنترل مسیریابی شبکه
الف-۷	شبکه‌های خصوصی مجازی	
الف-۸	شبکه های صدا	
الف-۹	همگرایی IP	
الف-۱۰	میزبانی وب	۱۰-۹-۳ اطلاعات در دسترس عمومی
الف-۱۱	پست الکترونیکی اینترنتی	۱۰-۸-۴ پیام های الکترونیکی
الف-۱۲	دسترسی مسیریابی شده به سازمان طرف سوم	

پیوست ج

(اطلاعاتی)

الگوی نمونه برای اسناد روال‌های بهره‌برداری امنیت

۱ مقدمه

۱-۱ پیش‌زمینه

۱-۲ ساختار سند

۲ محدوده

۲-۱ مکانها

۲-۲ زیرساخت فنی

۲-۲-۱محیطهای فناوری اطلاعات

۲-۲-۲ معماری شبکه

۲-۲-۳ مکان ۱

۲-۲-۴ مکان ۲

۲-۲-۵ مکان ۳

۲-۲-۶ اتصالات خارجی

۳ خط‌مشی امنیتی

۴ امنیت اطلاعات سازمان

۴-۱ مقدمه

۴-۲ ساختار مدیریت امنیت و مسئولیت ها

۴-۲-۱ افسر امنیتی سازمان

۴-۲-۲ معاون افسر امنیتی سازمان

۴-۲-۳ افسر امنیتی اطلاعات در سازمان

۴-۲-۵ تیم پشتیبانی فناوری اطلاعات (مربوطه)

۴-۲-۶ مدیران کسب و کار منطقه

۴-۲-۷ کارکنان

۴-۲-۸ انجمن مدیریت سازمان

۴-۳ گزارش‌های نقاط ضعف و رخداد امنیت اطلاعات

۴-۴ توزیع روال‌های بهره‌برداری امنیت

۴-۵ ارزیابی مخاطرات مرتبط با احزاب خارجی

۴-۶ توافق نامه دسترسی خارجی (سوم)

۴-۷ برون سپاری

۵ مدیریت دارایی
۵-۱ موجودی دارایی
۵-۲ استفاده قابل قبول از اطلاعات و دارایی های دیگر
۵-۳ اطلاعات طبقه بندی
۶ امنیت منابع انسانی
۶-۱ حداقل امنیت کارکنان، از جمله ترخیص کالا، الزامات
۶-۲ شرایط و ضوابط
۶-۳ آگاهی امنیت اطلاعات و آموزش
۶-۴ فرآیند انضباطی
۶-۵ نظارت بر کارکنان
۶-۶ فسخ اشتغال
۶-۷ امنیت دسترسی به کارت / جواز عبور ساختمان
۶-۸ دسترسی فیزیکی به سامانه‌های فناوری اطلاعات و شبکه
۷ امنیت فیزیکی و محیطی
۷-۱پیاده سازی کنترل امنیت فیزیکی و محیطی
۷-۲ موارد امنیت فیزیکی
۷-۳ کنترل ورودی فیزیکی
۷-۴ کار در اتاق کلید / مناطق
۷-۵ محل قرار گرفتن تجهیزات
۷-۶ کلید و ترکیب
۷-۷ تشخیص هشدار دهنده اینترودر
۷-۸ حفاظت از تجهیزات در مقابل سرقت
۷-۹ حذف تجهیزات
۷-۱۰کنترل های دسترسی سخت افزار
۷-۱۱ تشخیص رشوه دادن
۷-۱۲ نگهداری و تعمیرات
۷-۱۳ امنیت قدرت
۷-۱۴ امنیت آتش
۷-۱۵ امنیت آب / مایع
۷-۱۶ آژیرهای امنیتی
۷-۱۷ امنیت رایانه

کتاب‌نامه

[1] ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic ReferenceModel: The Basic Model*

[2] ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — BasicReference Model — Security Architecture*

[3] ISO/IEC 7498-3:1997, *Information technology — Open Systems Interconnection — Basic ReferenceModel: Naming and Addressing*

[4] ISO/IEC 7498-4:1989, *Information processing systems — Open Systems Interconnection — BasicReference Model — Management Framework*

[5] ISO/IEC 9595-8, *Information technology — Open Systems Interconnection — The Directory: Publickeyand attribute certificate frameworks*

[6] ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Securityframeworks for open systems: Overview*

[7] ISO 11166-2, *Banking — Key management by means of asymmetric algorithms — Part 2: Approvedalgorithms using the RSA cryptosystem*

[8] ISO 11568 (all parts), *Banking — Key management (retail)*

[9] ISO 11649, *Financial services — Core banking — Structured creditor reference to remittanceinformation*

[10] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[11] ISO/IEC 11889-1, *Information technology — Trusted Platform Module — Part 1: Overview*

[12] ISO/IEC 11889-2, *Information technology — Trusted Platform Module — Part 2: Design principles*

[13] ISO/IEC 11889-3, *Information technology — Trusted Platform Module — Part 3: Structures*

[14] ISO/IEC 11889-4, *Information technology — Trusted Platform Module — Part 4: Commands*

[15] ISO 13492, *Financial services — Key management related data element — Application and usage ofISO 8583 data elements 53 and 96*

[16] ISO/IEC 13888:2004 (all parts), *Information technology — Security techniques — Non-repudiation*

[17] ISO/IEC 14516:1999, *Information technology — Security techniques — Guidelines for the use andManagement of Trusted Third Party services*

[18] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

[19] ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment andoperations of intrusion detection systems (IDS)*

[20] ISO/IEC TR 18044:20042), *Information technology — Security techniques — Information securityincident management*

[21] ISO 21118, *Information to be included in specification sheets — Data projectors*

[22] ISO/PAS 22399:2007, *Societal security — Guidelines for incident preparedness and operationalcontinuity management*

[23] ISO/IEC 27003, *Information technology — Security techniques — Information security managementsystems implementation guidance*

[24] ISO/IEC 27004, *Information technology — Security techniques — Information security management —Measurement*

[25] IETF *Site Security Handbook* (RFC 2196), September 1997

[26] IETF *IP Security Document Roadmap* (RFC 2411), November 1998

[27] IETF *Security Architecture for the Internet Protocol* (RFC 2401), November 1998

[28] IETF *Address Allocation for Private Internets* (RFC 1918), February 1996

[29] IETF *SNMP Security Protocols* (RFC 1352), July 1992

[30] IETF *Internet Security Glossary* (RFC 2828), May 2000

[31] IETF *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source AddressSpoofing* (RFC 2827), May 2000

[32] NIST Special Publications (800 series) on *Computer Security*

[33] NIST Special Publication 800-10: *Keeping Your Site Comfortably Secure: An Introduction to InternetFirewalls,* December 1994