ISIRI
11210-1
1st. edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱ - ۱۱۲۱۰
چاپ اول

فناوری اطلاعات - فنون امنیتی - امنیت شبکه فناوری اطلاعات قسمت ۱: مدیریت امنیت شبکه

Information technology - Security techniques - IT network security Part 1:Network security management

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱)
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه : www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱) ، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۱۱۰۰۰ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Price: 11000 Rls.

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* 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 ذیصلاح 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 شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بینالمللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه 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 سا زمانها 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 ، مؤسسهٔ استاندارد 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 آنها 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 مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International Organization For Standardization
2- International Electro Technical Commission
3- International Organization For Legal Metrology (Organization International De Metrology Legal)
4- Contact Point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

" فناوری اطلاعات - فنون امنیتی - امنیت شبکه فناوری اطلاعات، قسمت ۱: مدیریت امنیت شبکه "

رئیس:	**سمت و/یا نمایندگی**
صلاحی، احمد (دکتری کامپیوتر)	مدیر گروه فناوری امنیت شبکه مرکز تحقیقات مخابرات ایران
دبیر:	
برزگر، مریم (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس مرکز تحقیقات مخابرات ایران
اعضاء:	
بحری، پیمان (کارشناسی ارشد مهندسی کامپیوتر- سخت‌افزار)	کارشناس مرکز تحقیقات مخابرات ایران
پیلتن، علیرضا (کارشناسی مهندسی کامپیوتر)	کارشناس شرکت امن‌افزار گستر شریف
تدین، محمد حسام (دکتری ریاضی)	هیات علمی پژوهشکده امنیت مرکز تحقیقات مخابرات ایران
حبیبی، هاشم (کارشناسی ارشد مهندسی کامپیوتر)	سازمان هوا فضا
حقیقی، صیاد (کارشناسی‌ارشد مهندسی برق- مخابرات/ امن)	دانشگاه خواجه نصیرالدین طوسی
خسروی، رامین (کارشناسی‌ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
خلاش قزل‌احمد، سمیه (کارشناسی ارشد ریاضی)	کارشناس مرکز تحقیقات مخابرات ایران
رستم‌پور، سهراب (کارشناسی مهندسی برق)	کارشناس مسئول شبکه شرکت ارتباطات سیار

رنجکش، نازی (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
سهی‌زاده ابیانه، محمدرضا (کارشناسی ارشد مهندسی برق- مخابرات/ امن)	کارشناس صنایع الکترونیک زعیم
سیفی، مهرداد (کارشناسی ارشد مدیریت صنعتی)	کارشناس و مسئول تدوین استانداردهای امنیت شبکه شرکت ارتباطات سیار
صابری، جواد (کارشناسی ارشد مهندسی برق- مخابرات/ امن)	مرکز تحقیقات مخابرات امن
طباطبائی، سید امیر حسین (کارشناسی ارشد ریاضی)	کارشناس صنایع الکترونیک زعیم
عظیمی، پدرام (کارشناسی ارشد مهندسی برق- مخابرات)	کارشناس دفتر تدوین شرکت مخابرات ایران
عنایتی، علیرضا (کارشناسی‌ارشد مهندسی برق- مخابرات/ سیستم)	کارشناس مرکز تحقیقات مخابرات ایران
کاظمی، سمیه (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
میراسکندری، سیدمحمدرضا (کارشناسی مهندسی برق)	مدیر کل شرکت فناوری اطلاعات
میرقدری، عبدالرسول (دکتری آمار)	هیات علمی دانشگاه امام حسین
نوروزی، سعید (کارشناسی کامپیوتر/ نرم‌افزار)	رئیس اداره شبکه شرکت ارتباطات سیار
یادگاری، امیرمنصور (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	هیات علمی پژوهشکده امنیت مرکز تحقیقات مخابرات ایران

فهرست مندرجات

ادامه فهرست مندرجات

ادامه فهرست مندرجات

پیش گفتار

این استاندارد تحت عنوان " فناوری اطلاعات - فنون امنیتی - امنیت شبکه فناوری اطلاعات، قسمت۱: مدیریت امنیت شبکه " که پیش نویس آن درکمیسیون‌های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران و مرکز تحقیقات مخابرات ایران تهیه و تدوین شده و در شصت و پنجمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۱۱/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی 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 تجدیدنظر استانداردهای ملی استفاده کرد.

منابع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 18028-1:2006, Information technology – Security techniques – IT network security – Part 1: Network security management

مقدمه

صنایع مربوط به IT و ارتباطات راه دور، به‌دنبال راه‌حل‌های امنیتی فراگیر و مقرون به صرفه هستند. یک شبکه امن بایستی در برابر حملات مخرب و ناخواسته، حفاظت شود و الزامات کسب‌وکار را از لحاظ محرمانگی، یکپارچگی، دسترسی‌پذیری، انکارناپذیری، پاسخگوئی، اعتبار و قابلیت اطمینان اطلاعات و سرویس‌ها، برآورده سازد. امن‌سازی یک شبکه به‌منظور حفظ دقت در صدور صورت‌حساب‌ها یا استفاده از اطلاعات مناسب نیز ضروری است. قابلیت‌های امنیتی محصولات، در امنیت کلی شبکه (شامل کاربردها و سرویس‌ها) حیاتی است. از طرفی هر میزان که محصولات بیشتری به‌منظور فراهم نمودن راه‌حل‌های جامع با هم ترکیب شوند، قابلیت همکاری این محصولات یا فقدان آن‌ها، میزان موفقیت راه‌حل را تعیین خواهد نمود. امنیت تنها نباید برای هر محصول یا سرویس درنظر گرفته شود، بلکه باید به‌گونه‌ای توسعه یابد که قابلیت ترکیب توانایی‌های امنیتی را در کلیه راه‌حل‌های انتها به انتها ارتقاء بخشد. بنابراین هدف استانداردهای ISO/IEC 18028 ارایه راهنمائی‌های دقیق در زمینه جنبه‌های مدیریتی، عملکردی و کاربردی شبکه‌های IT و اتصالات متقابل آنها است. توصیه می‌شود اشخاصی که درون یک سازمان مسوول امنیت IT به‌طور کلی و امنیت شبکه‌های IT به‌طور خاص هستند، بایستی قادر باشند به‌منظور برآوردن نیازمندی‌های خاص خود، مفاد مطرح‌شده در این استاندارد را برآورده سازند. اهداف اصلی این استاندارد عبارتند از:

- در این استاندارد تعریف و توصیف مفاهیم مرتبط با امنیت شبکه و راهنمائی‌های مدیریتی آن، شامل چگونگی شناسایی و تحلیل عوامل مرتبط با ارتباطات که به‌منظور ایجاد الزامات امنیتی شبکه درنظر گرفته می‌شوند، به انضمام ارایه مقدمه‌ای بر حیطه‌های ممکن کنترلی و حیطه‌های فنی خاص (که در قسمت‌های بعدی استاندارد ISO/IEC 18028 بررسی می‌شوند)،
- در قسمت دوم این استاندارد تعریف یک معماری امنیتی استاندارد که چارچوبی سازگار برای پشتیبانی از برنامه‌ریزی، طراحی و پیاده‌سازی امنیت شبکه است،
- در استاندارد ISO/IEC 18028-3، تعریف فنون ایمن‌سازی جریان‌های اطلاعات بین شبکه‌ها با استفاده از دروازه‌های امنیتی،
- در استاندارد ISO/IEC 18028-4، تعریف فنون ایمن‌سازی دسترسی راه دور،
- در استاندارد ISO/IEC 18028-5، تعریف فنون ایمن‌سازی اتصالات بین شبکه‌ای که توسط VPN[1]ها ایجاد می‌شوند.

این استاندارد مربوط به کسانی است که مالک، اپراتور و یا استفاده‌کننده از یک شبکه هستند. این افراد علاوه بر مدیران و مجریانی که مسوولیت‌های خاصی در زمینه امنیت اطلاعات و/یا امنیت و عملیات شبکه برعهده دارند و یا اشخاصی که مسوول برنامه امنیتی کلی سازمان و تدوین خطی‌مشی امنیتی هستند، شامل مدیران ارشد و یا دیگر مدیران و کاربران غیرفنی نیز می‌باشند.

[1] Virtual Private Networks

قسمت دوم این استاندارد مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیت شبکه، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-3 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزئی دروازه‌های امنیتی، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-4 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزئی امنیت دسترسی راه دور، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-5 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزئی VPNها، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات –
قسمت ۱ : مدیریت امنیت شبکه

۱- هدف و دامنه کاربرد

هدف از تدوین این استاندارد ارائه دستورالعملی برای ارتباطات و شبکه‌ها است که شامل جنبه‌های امنیتی اتصال بین شبکه‌های سامانه اطلاعاتی و اتصال کاربران راه دور به شبکه‌ها است. این امر متوجه مسوولان مدیریت امنیت اطلاعات به‌طور کلی و امنیت شبکه به‌طور خاص است. این دستورالعمل از تحلیل و شناسایی عوامل مرتبط با ارتباطات که بهتر است برای ایجاد الزامات امنیت شبکه لحاظ شوند، پشتیبانی می‌نماید و مقدمه‌ای بر چگونگی شناخت حیطه‌های کنترلی مناسب، همراه با جنبه‌های امنیتی مرتبط با اتصالات به شبکه‌های ارتباطی ارایه می‌کند و نیز به ارایه یک رویکرد از حیطه‌های کنترلی ممکن می‌پردازد. این حیطه‌ها شامل موضوعات طراحی و پیاده‌سازی فنی هستند که به تفصیل در استانداردهای ISO/IEC 18028-2 تا ISO/IEC 18028-5 شرح داده شده‌اند.

۲- مراجع الزامی

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

در صورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع الزامی زیر برای کاربرد این استاندارد الزامی است.

۲-۱- ISO/IEC 18028-2:2005، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – قسمت ۲ : معماری امنیتی شبکه

۲-۲- ISO/IEC 18028-3:2005، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – قسمت ۳ : ایمن سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی

۲-۳- ISO/IEC 18028-4:2005، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – قسمت ۴ : ایمن سازی دسترسی راه دور

۲-۴- ISO/IEC 18028-5:2006، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – قسمت ۵ : ایمن سازی ارتباطات بین شبکه‌ها با استفاده از VPNها

۲-۵- ISO/IEC 13335-1:2004، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – قسمت ۱ : مفاهیم و مدل‌ها برای مدیریت امنیت فناوری اطلاعات و ارتباطات

۲-۶- ISO/IEC 17799:2005، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – آیین کار امنیت اطلاعات

۲-۷- ISO/IEC 18044:2004، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – مدیریت حوادث امنیت اطلاعات

۲-۸- ISO/IEC 18043:2006، فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات – گزینش، استقرار و عملیات سامانه‌های تشخیص نفوذ

۳- اصطلاحات و تعاریف

۳-۱- اصطلاحات تعریف‌شده در سایر استانداردهای بین‌المللی

در این استاندارد، اصطلاحات و تعاریف ارایه‌شده در استاندارد ISO/IEC 7498 (همه‌ی قسمت‌ها) و اصطلاحات زیر که در استانداردهای ISO/IEC 17799 و ISO/IEC 13335-1 تعریف شده‌اند، مورد استفاده قرار گرفته است:

مسئولیت‌پذیری، دارایی، اعتبار، دسترس‌پذیری، کنترل‌های پایه، محرمانگی، یکپارچگی داده، پیامد، یکپارچگی، خط‌مشی امنیتی، انکارناپذیری، قابلیت اطمینان، مخاطره، تحلیل مخاطره، ارزیابی مخاطره، مدیریت مخاطره، کنترل، تهدید و آسیب‌پذیری.

۳-۲- اصطلاحات تعریف‌شده در این استاندارد

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار برده می‌شود:

۳-۲-۱-
هشدار[1]

نشانگری "لحظه‌ای" است که نشان می‌دهد یک سامانه اطلاعاتی و شبکه ممکن است به علت حادثه، خرابی یا خطای افراد تحت حمله یا در خطر حمله باشد.

۳-۲-۲-
مهاجم[2]

هر شخصی که بخواهد به‌طور عمدی، به‌منظور دزدیدن یا به‌خطر انداختن شبکه‌ها و سامانه‌های اطلاعاتی، یا به‌خطر انداختن دسترس‌پذیری برای کاربران مجاز سامانه‌های اطلاعاتی و منابع شبکه، از آسیب‌پذیری‌های موجود در کنترل‌های امنیتی فنی و غیرفنی سواستفاده کند.

۳-۲-۳-
ممیزی[3]

پرسش و امتحان رسمی یا تصدیق وقایع در برابر انتظارات، به‌منظور مطابقت و انطباق و برآوردن انتظارات.

۳-۲-۴-
ثبت ممیزی[4]

جمع‌آوری داده‌های مرتبط با رویداد امنیت اطلاعات به‌منظور بازنگری، تحلیل و پایش مداوم.

۳-۲-۵-
ابزارهای ممیزی[5]

ابزارهای خودکاری که برای تحلیل محتوای ثبت‌های ممیزی کمک می‌کنند.

---

[1] Alert
[2] Attacker
[3] Audit
[4] Audit Logging
[5] Audit Tolls

۳-۲-۶-

مدیریت تداوم کسب وکار[1]

فرایندی برای حصول اطمینان از بازیابی عملیات، در صورت بروز رخداد ناخواسته یا غیرمنتظره‌ای که توانایی اثرگذاری منفی بر تداوم عملکردهای اصلی کسب‌وکار و اجزای پشتیبان را دارد.

یادآوری توصیه می‌شود این فرایند اطمینان دهد که بازیابی در اولویت‌ها و مقیاس‌های زمانی مورد نیاز انجام می‌گیرد و متعاقباً تمام کارکردهای کسب‌وکار و اجزای پشتیبانی به وضع عادی بازگردانده می‌شوند. علاوه بر این توصیه می‌شود اجزای کلیدی این فرایند اطمینان دهد که طرح‌ها و تسهیلات ضروری در جای خود قرار گرفته‌اند و آزمون می‌شوند و این اجزای کلیدی شامل اطلاعات، فرایندهای کسب‌وکار، سرویس‌ها و سامانه‌های اطلاعاتی، ارتباطات داده‌ای و صوتی، تسهیلات فیزیکی و انسانی هستند.

۳-۲-۷-

Comp128-1

الگوریتمی اختصاصی که درابتدا به‌طور پیش‌فرض در سیم‌کارت‌ها استفاده می‌شد.

۳-۲-۸-

محدوده بی‌طرف[2]

شبکه محیطی (به‌عنوان زیرشبکه غربال‌شده نیز شناخته می‌شود) به عنوان یک "محدوده بی‌طرف" بین شبکه‌ها قرار می‌گیرد.

یادآوری محدوده بی‌طرف، یک محدوده بافر امنیتی را تشکیل می‌دهد.

۳-۲-۹-

انسداد سرویس‌دهی[3]

پیش‌گیری از دسترسی مجاز به یک منبع سامانه یا به‌تاخیر انداختن عملیات و عملکردهای سامانه.

۳-۲-۱۰-

شبکه خارجی [4]

گسترش شبکه داخلی یک سازمان به‌ویژه بر روی زیرساخت شبکه عمومی، به‌طوری‌که امکان به اشتراک گذاشتن منابع بین این سازمان و سایر سازمان‌ها و افراد را از طریق دسترسی محدود به شبکه داخلی آن سازمان فراهم می‌کند.

---

[1] Business Continuity Managment
[2] Demilitarized Zone, DMZ
[3] Denial Of Service, Dos
[4] Extranet

۳-۲-۱۱-

پالایش[1]

فرایند پذیرش یا رد جریان‌های داده در شبکه با استفاده از معیارهای مشخص.

۳-۲-۱۲-

دیواره آتش[2]

نوعی مانع امنیتی – تشکیل‌شده از یک دستگاه اختصاصی یا ترکیبی از چندین مولفه و روش – که بین محیط‌های شبکه‌ای قرار می‌گیرد و همه ترافیک را از یک محیط شبکه به دیگری و بالعکس منتقل می‌کند و با توجه به خط‌مشی امنیتی محلی تنها به ترافیک مجاز اجازه عبور می‌دهد.

۳-۲-۱۳-

هاب[3]

یک وسیله شبکه‌ای که در لایه یک از مدل مرجع OSI[4] (استاندارد ISO/IEC 7498-1) عمل می‌کند.

یادآوری هاب‌های شبکه، هوشمند نیستند، این دستگاه‌ها تنها نقاط الصاق فیزیکی را برای منابع یا سامانه‌های تحت شبکه فراهم می‌کنند.

۳-۲-۱۴-

رویداد امنیت اطلاعات[5]

رویداد معینی در یک سامانه، سرویس یا وضعیت شبکه که بیانگر یک نقض احتمالی خط‌مشی امنیت اطلاعات یا خرابی در کنترل‌ها و یا یک وضعیت ناشناخته قبلی مرتبط با امنیت است.

یادآوری به استاندارد ISO/IEC 18044 مراجعه شود.

۳-۲-۱۵-

رخداد امنیت اطلاعات[6]

یک یا مجموعه‌ای از رویدادهای ناخواسته یا غیرمنتظره امنیتی اطلاعات که احتمال بالایی در به‌خطر انداختن عملیات کسب‌وکار و تهدید کردن امنیت اطلاعات دارند.

یادآوری به استاندارد ISO/IEC 18044 مراجعه شود.

---

[1] Filtering
[2] Firewall
[3] Hub
[4] Open System Interconnection
[5] Information Security Event
[6] Information Security Incident

۳-۲-۱۶-

مدیریت رخداد امنیت اطلاعات[1]

فرآیند رسمی پاسخ‌گوئی و رسیدگی به رویدادها و رخدادهای امنیت اطلاعات.

یادآوری به استاندارد ISO/IEC 18044 مراجعه شود.

۳-۲-۱۷-

اینترنت[2]

سامانه‌ای جهانی از شبکه‌های به‌هم پیوسته در یک حوزه عمومی.

۳-۲-۱۸-

شبکه داخلی[3]

شبکه خصوصی که در داخل یک سازمان ایجاد می‌شود.

۳-۲-۱۹-

نفوذ[4]

دسترسی غیرمجاز به یک شبکه یا یک سامانه متصل به شبکه، به‌عبارتی دسترسی غیرمجاز عمدی یا تصادفی به یک سامانه اطلاعاتی به‌منظور انجام یک فعالیت مخرب در یک سامانه اطلاعاتی یا استفاده غیرمجاز از منابع آن.

۳-۲-۲۰-

تشخیص نفوذ[5]

فرایند رسمی آشکارسازی نفوذ که معمولاً از طریق جمع‌آوری دانش درباره الگوهای استفاده غیرعادی مشخص می‌شود، از قبیل اینکه چه آسیب‌پذیری‌هایی، چگونه و چه زمانی مورد سواستفاده واقع شده‌اند.

یادآوری به استاندارد ISO/IEC 18043 مراجعه شود.

---

[1] Information Security Incident Managment
[2] Internet
[3] Intranet
[4] Intrusion
[5] Intrusion Detection

۳-۲-۲۱-

سامانه تشخیص نفوذ[1]

سامانه‌ای فنی که برای شناسایی هر نوع تلاش برای نفوذ یا شناسایی نفوذی که در حال وقوع است یا رخ داده است، مورد استفاده قرار می‌گیرد و ممکن است در برابر نفوذ در سامانه‌های اطلاعاتی و شبکه‌ها واکنش نشان دهد.

یادآوری به استاندارد ISO/IEC 18043 مراجعه شود.

۳-۲-۲۲-

سامانه پیش‌گیری از نفوذ[2]

نوعی از سامانه‌های تشخیص نفوذ است، که به‌طور خاص به‌منظور تامین قابلیت پاسخ‌گویی فعال طراحی شده‌اند.

یادآوری به استاندارد ISO/IEC 18043 مراجعه شود.

۳-۲-۲۳-

لغزش[3]

یک نوع اعوجاج خطی است که در زمان انحراف سیگنال مخابره شده از مرجع، رخ می‌دهد.

۳-۲-۲۴-

بدافزار[4]

نرم‌افزار مخربی مانند ویروس یا اسب تروا است که به‌طورخاص برای تخریب یا ازهم گسیختن سامانه طراحی شده است.

۳-۲-۲۵-

سودهی برچسب چندپروتکلی[5]

فنی که به‌منظور استفاده در مسیریابی بین شبکه‌ای توسعه یافته است و برچسب‌هایی را برای مسیرها یا جریان‌های داده منفرد اختصاص می‌دهد. این برچسب‌ها علاوه بر سازوکارهای پروتکل مسیریابی طبیعی، برای سودهی اتصالات نیز مورد استفاده قرار می‌گیرند.

---

[1] Intrusion Detection System, IDS
[2] Intrusion Prevention System, IPS
[3] Jitter
[4] Malicious Software, Malware
[5] Multi Protocol Lable Switching, MPLS

یادآوری سودهی برچسب می‌تواند به عنوان یک روش برای ایجاد تونل‌ها استفاده می‌شود.

۳-۲-۲۶-

اداره کردن شبکه[1]

عملیات و مدیریت روزبه‌روز فرایندها و کاربران شبکه.

۳-۲-۲۷-

تحلیل‌گر شبکه[2]

دستگاهی که برای ضبط جریان اطلاعات در شبکه‌ها و رمزگشایی آنها، مورد استفاده قرار می‌گیرد.

۳-۲-۲۸-

عنصر شبکه[3]

سامانه اطلاعاتی که به یک شبکه متصل است.

یادآوری توصیف تفصیلی عنصر امنیتی در بخش دوم این استاندارد ارایه شده است.

۳-۲-۲۹-

مدیریت شبکه[4]

فرایند برنامه‌ریزی، طراحی، پیاده‌سازی، عملیاتی کردن، پایش و پشتیبانی از شبکه.

۳-۲-۳۰-

پایش شبکه[5]

فرایند مشاهده و بازنگری پیوسته داده ثبت‌شده در فعالیت و عملیات شبکه که شامل ممیزی وقایع ثبت‌شده و هشدارها و تحلیل‌های مربوط است.

---

[1] Network Administration
[2] Network Analyzer
[3] Network Element
[4] Network Managment
[5] Network Monitorig

۳-۲-۳۱-

خط‌مشی امنیتی شبکه[1]

مجموعه‌ای از بیانیه‌ها، قواعد و تجربه‌هایی که رویکرد سازمان را برای استفاده از منابع شرح می‌دهد و چگونگی حفاظت از زیرساخت و سرویس‌های شبکه را مشخص می‌نماید.

۳-۲-۳۲-

درگاه[2]

نقطه انتهایی یک اتصال.

یادآوری در پروتکل‌های اینترنتی، یک درگاه، نقطه انتهایی یک کانال منطقی اتصال TCP یا UDP است. در پروتکل‌های کاربردی که مبتنی بر TCP یا UDP هستند، معمولاً به درگاه‌ها شماره پیش‌فرضی نسبت داده شده است، به‌عنوان مثال درگاه ۸۰ برای پروتکل HTTP.

۳-۲-۳۳-

حریم خصوصی[3]

حق هر فرد از نظر محرمانه بودن زندگی شخصی و خانوادگی، خانه و مسایل مربوط.

یادآوری هیچ مرجع دارای اختیاری اجازه پایمال کردن این حق را نخواهد داشت، مگر با اجازه قانون و درصورت لزوم، برای تامین امنیت ملی در جامعه مردم‌سالار، ایمنی عمومی یا بهبود اقتصاد یک کشور، پیش‌گیری از جرایم یا اختلال، حفاظت از سلامت یا اخلاق یا حفاظت از حقوق و آزادی دیگران.

۳-۲-۳۴-

دسترسی راه دور[4]

فرایند دسترسی به منابع شبکه از شبکه‌ای دیگر یا از یک پایانه که به‌طور دایم و به صورت فیزیکی یا منطقی به شبکه‌ای که به آن دسترسی صورت می‌گیرد، متصل نیست.

۳-۲-۳۵-

کاربر راه دور[5]

کاربر در سایتی به غیر از سایتی که منابع شبکه مورد استفاده در آن قرار گرفته است.

---

[1] Network Security Policy
[2] Port
[3] Privacy
[4] Remote Access
[5] Remote User

۳-۲-۳۶-

مسیریاب[1]

وسیله شبکه‌ای که به‌منظور ایجاد و کنترل جریان داده بین شبکه‌های مختلف، با انتخاب مسیرهایی براساس الگوریتم‌ها و سازوکارهای پروتکل مسیریابی، مورد استفاده قرار می‌گیرد. این شبکه‌ها می‌توانند مبتنی بر پروتکل‌های مختلف شبکه باشند. اطلاعات مسیریابی در جداول مسیریابی نگهداری می‌شود.

۳-۲-۳۷-

بعد امنیتی[2]

مجموعه‌ای از کنترل‌های امنیتی که برای پرداختن به جنبه خاصی از امنیت شبکه طراحی شده‌اند.

یادآوری توصیف تفصیلی ابعاد امنیتی در بخش دوم این استاندارد ارایه شده است.

۳-۲-۳۸-

حوزه امنیتی[3]

مجموعه‌ای از منابع و دارایی‌ها که تحت خط‌مشی امنیتی مشترکی قرار دارند.

۳-۲-۳۹-

دروازه امنیتی[4]

نقطه اتصال بین شبکه‌ها، یا بین زیرگروه‌های شبکه، یا بین کاربردهای نرم‌افزاری در حیطه‌های امنیتی مختلف که باتوجه به خط‌مشی امنیتی معین، حفاظت از شبکه را برعهده دارد.

یادآوری توصیف تفصیلی دروازه امنیتی در استاندارد ISO/IEC 18028-3 ارایه شده است.

۳-۲-۴۰-

لایه‌های امنیتی[5]

لایه‌های امنیتی بیانگر سلسله مراتبی از تجهیزات و تسهیلات گروه‌بندی شده شبکه هستند که توسط ابعاد امنیتی حفاظت می‌شوند.

یادآوری توصیف تفصیلی لایه‌های امنیتی در بخش دوم این استاندارد ارایه شده است.

---

[1] Router
[2] Security Dimension
[3] Security Domain
[4] Security Gateway
[5] Security Layers

۳-۲-۴۱-

سطح امنیتی[1]

سطح امنیتی بیانگر نوع خاصی از فعالیت شبکه‌ای است که توسط ابعاد امنیتی حفاظت می‌شود.

یادآوری توصیف تفصیلی سطح امنیتی در استاندارد ISO/IEC 18028-2 ارایه شده است.

۳-۲-۴۲-

ارسال انبوه هرزنامه[2]

ارسال انبوهی از پیغام‌های غیردرخواستی که در دریافت منجر به تاثیرات مخرب شدید بر دسترس‌پذیری منابع سامانه‌های اطلاعاتی خواهد شد.

۳-۲-۴۳-

جعل کردن[3]

جعل هویت منبع یا کاربر قانونی.

۳-۲-۴۴-

سوده[4]

وسیله‌ای که اتصال بین سایر دستگاه‌های شبکه‌ای را با استفاده از سازوکارهای سودهی داخلی فراهم می‌کند.

یادآوری سوده‌ها از سایر وسایل بین شبکه‌ای محلی (مانند هاب‌ها)، مجزا هستند، زیرا فناوری به‌کارگرفته شده در سوده‌ها، برقراری اتصالات را به‌صورت نقطه به نقطه امکان‌پذیر می‌سازد. این عمل اطمینان می‌دهد که ترافیک شبکه فقط توسط وسایل خاص شبکه، قابل رویت است، همچنین ایجاد چندین اتصال را به‌طور همزمان ممکن می‌سازد. فناوری سودهی معمولاً می‌تواند در لایه۲ یا ۳ از مدل مرجع OSI (استاندارد ISO/IEC 7498-1)، پیاده‌سازی شود.

۳-۲-۴۵-

تونل[5]

مسیر داده‌ای بین وسایل شبکه‌ای که در عرض زیرساخت شبکه موجود، ایجاد می‌شود. در ایجاد این مسیر، از فنونی چون محفظه‌بندی پروتکل، سودهی برچسب و مدارات مجازی استفاده می‌شود.

---

[1] Security Plane
[2] Spamming
[3] Spoofing
[4] Switch
[5] Tunnel

۳-۲-۴۶-

شبکه خصوصی مجازی[1]

شبکه منطقی رایانه‌ای با استفاده محدود که از منابع سامانه یک شبکه فیزیکی ساخته می‌شود، به‌عنوان مثال با استفاده از رمزنگاری و/یا با تونل زدن پیوندهای شبکه مجازی در عرض شبکه واقعی.

[1] Virtual Private Network

۴- کوته‌واژگان

یادآوری اصطلاحات اختصاری زیر در کلیه بخش‌های استاندارد ISO/IEC 18028 استفاده شده است.

واژه اختصاری	عبارت کامل انگلیسی	عبارت کامل فارسی
3G	Third Generation mobile telephone system	سامانه تلفن سیار نسل سوم
AAA	Authentication, Authorization and Accounting	احراز اصالت، مجوزدهی و قابلیت حسابرسی
ACL	Access Control List	فهرست کنترل دسترسی
ADSL	Asymmetric Digital Subscriber Line	خط دیجیتالی نامتقارن مشترکین
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
ATM	Asynchronous Transfer Mode	حالت انتقال ناهمزمان
CDPD	Cellular Digital Packet Data	داده بسته‌ای دیجیتالی سلولی
CDMA	Code Division Multiple Access	دسترسی چندگانه تقسیم کد
CLID	Calling Line Identifier	شناسه تماس‌گیرنده
CLNP	Connectionless Network Protocol	پروتکل شبکه غیراتصال‌گرا
CoS	Class of Service	دسته سرویس
CRM	Customer Relationship Management	مدیریت روابط مشتری
DEL	Direct Exchange Line	خط تبادل مستقیم
DES	Data Encryption Standard	استاندارد رمزگذاری داده
DMZ	Demilitarized Zone	محدوده بی‌طرف
DNS	Domain Name Service	سرویس نام‌دهی حوزه
DoS	Denial of Service	انسداد سرویس‌دهی
DSL	Digital Subscriber Line	خط دیجیتالی مشترکین
EDGE	Enhanced Data-Rates for GSM Evolution	نرخ داده ارتقاءیافته برای تکامل سامانه جهانی ارتباطات سیار
EDI	Electronic Data Interchange	تبادل الکترونیکی داده
EGPRS	Enhanced General Packet Radio Service	سرویس رادیویی بسته‌ای عمومی ارتقاءیافته
EIS	Enterprise Information System	سامانه اطلاعاتی بنگاه‌های اقتصادی
FTP	File Transfer Protocol	پروتکل انتقال فایل
GPRS	General Packet Radio Service	سرویس رادیویی بسته‌ای عمومی
GSM	Global System for Mobile	سامانه جهانی ارتباطات سیار

	communications	
HIDS	Host based Intrusion Detection System	سامانه تشخیص نفوذ مبتنی بر میزبان
HTTP	Hypertext Transfer Protocol	پروتکل انتقال ابرمتن
IDS	Intrusion Detection System	سامانه تشخیص نفوذ
IP	Internet Protocol	پروتکل اینترنت
ISP	Internet Service Provider	ارایه‌کننده سرویس اینترنت
IT	Information Technology	فناوری اطلاعات
LAN	Local Area Network	شبکه محلی
MPLS	Multi-Protocol Label Switching	سودهی برچسب چند پروتکلی
MRP	Manufacturing Resource Planning	برنامه‌ریزی منابع ساخت
NAT	Network Address Translation	ترجمه آدرس شبکه
NIDS	Network Intrusion Detection System	سامانه تشخیص نفوذ شبکه
NTP	Network Time Protocol	پروتکل زمانی شبکه
OOB	‘Out of Band’	خارج از باند
PC	Personal Computer	رایانه شخصی
PDA	Personal Data Assistant	دست‌یار داده شخصی
PIN	Personal Identification Number	شماره شناسه شخصی
PKI	Public Key Infrastructure	زیرساخت کلید عمومی
PSTN	Public Switched Telephone Network	شبکه تلفن سوده عمومی
QoS	Quality of Service	کیفیت سرویس‌دهی
RAID	Redundant Array of Inexpensive Disks	آرایه افزونه دیسک‌های ارزان
RAS	Remote Access Service	سرویس دسترسی راه دور
RTP	Real Time Protocol	پروتکل بلادرنگ
SDSL	Symmetric Digital Subscriber Line	خط دیجیتالی متقارن مشترکین
SecOPs	Security Operating Procedures	رویه‌های عملیاتی امنیتی

SIM	Subscriber Identity Module	ماژول شناسه مشترکین
SNMP	Simple Network Management Protocol	پروتکل مدیریتی شبکه ساده
SSH	Secure Shell	پوسته امن
TCP	Transmission Control Protocol	پروتکل کنترل ارسال
TDMA	Time Division Multiple Access	دسترسی چندگانه تقسیم زمانی
Telnet	Terminal emulation program to work on-line on a remote computer	برنامه شبیه‌ساز پایانه برای کارکردن برخط بر روی رایانه‌های راه دور
TETRA	TErrestial Trunked RAdio	رادیو کابلی زمینی
TKIP	Temporal Key Integrity Protocol	پروتکل یکپارچگی کلید موقت
UDP	User Datagram Protocol	پروتکل بسته داده کاربر
UMTS	Universal Mobile Telecommunications System	سامانه مخابراتی سیار جهانی
UPS	Uninterruptible Power Supply	منبع تغذیه بی‌وقفه
USB	Universal Serial Bus	گذرگاه سریال جهانی
VHF	Very High Frequency	فرکانس بسیار بالا
VoIP	Voice over IP	صدا بر روی IP
VPN	Virtual Private Network	شبکه خصوصی مجازی
WAN	Wide Area Network	شبکه گسترده
WAP	Wireless Application Protocol	پروتکل کاربردی بی‌سیم
WEP	Wired Equivalent Privacy	حریم خصوصی هم‌ارزی باسیم
WLAN	Wireless Local Area Network	شبکه محلی بی‌سیم
WORM	Write Once Read Many	یک‌بار نوشتن چندبار خواندن

۵- ساختار

رویکرد اتخاذ شده در این استاندارد به صورت زیر است:

- ابتدا خلاصه‌سازی فرایند کلی شناسایی و تحلیل عوامل مرتبط با ارتباطات که لازم است برای ایجاد الزامات امنیتی شبکه درنظر گرفته شوند، و
- سپس ارایه تعریفی از حیطه‌های کنترلی بالقوه، همراه با ملاحظه امنیت مرتبط با اتصالات به و بین شبکه‌های ارتباطی. در انجام این امر، شاخص‌هایی برای تعیین اینکه در چه مواردی ممکن است استانداردهای ISO/IEC 13335 و ISO/IEC 17799، به‌کار گرفته شوند، ارایه شده است. همچنین موضوعات مربوط به طراحی فنی و پیاده‌سازی، معرفی شده و در صورت لزوم به استانداردهای ISO/IEC 18028-2 تا ISO/IEC 18028-5، که به‌طور تفصیلی به این موضوعات پرداخته‌اند، ارجاع داده شده است.

سه معیار ساده برای کمک به افراد مسوول در امر امنیت اطلاعات و به‌منظور شناسایی حیطه‌های کنترلی بالقوه ارایه می‌شود. این معیارها برای شناسایی موارد زیر به‌کار می‌روند:

- انواع مختلف اتصالات شبکه
- مشخصات مختلف شبکه‌بندی و روابط اعتماد مربوطه و
- انواع مخاطرات امنیتی بالقوه مرتبط با اتصالات شبکه (و استفاده از سرویس‌هایی که به‌واسطه این اتصالات فراهم می‌شوند).

نتایج حاصل از ترکیب این معیارها، برای تعیین حیطه‌های کنترلی بالقوه مورد استفاده قرار می‌گیرد. متعاقباً به‌طور مختصر توضیحاتی در مورد حیطه‌های کنترلی بالقوه، با اشاره به منابعی که با جزییات بیشتر به این مساله پرداخته‌اند، ارایه می‌شود.

حیطه‌های کنترلی بالقوه عبارتند از:

- معماری امنیتی شبکه، که موارد زیر را پوشش می‌دهد:
  - شبکه‌بندی محلی،
  - شبکه‌بندی گسترده،
  - شبکه‌های بی‌سیم،
  - شبکه‌های رادیویی،
  - شبکه‌بندی پهن‌باند،
  - دروازه‌های امنیتی (به استاندارد ISO/IEC 18028-3 مراجعه شود)،
  - سرویس‌های دسترسی راه دور (به استاندارد ISO/IEC 18028-4 مراجعه شود)،
  - VPNها (به استاندارد ISO/IEC 18028-5 مراجعه شود)،
  - همگرایی IP (داده، صوت و تصویر)،
  - فعال‌کردن دسترسی به سرویس‌ها که توسط شبکه‌های خارج (از سازمان) فراهم می‌شود،

- معماری‌های میزبان وب،

(برای جزییات بیشتر در مورد معماری امنیتی شبکه به استاندارد ISO/IEC 18028-2 مراجعه شود)

- چارچوب مدیریت سرویس امن،
- مدیریت امنیت شبکه،
- مدیریت فنی آسیب‌پذیری،
- احراز اصالت داده و شناسایی،
- پایش و ثبت ممیزی شبکه،
- تشخیص نفوذ،
- حفاظت در برابر کد مخرب،
- سرویس‌های مبتنی بر رمزنگاری زیرساختی مشترک،
- و مدیریت تداوم کسب‌وکار[1].

در ادامه پیاده‌سازی و اجرای کنترل‌های امنیتی، پایش و بازنگری پیاده‌سازی، بررسی می‌شود.

۶- هدف

هدف این استاندارد ارایه موارد زیر است:

- دستورالعملی برای شناسایی و تحلیل عوامل مرتبط با ارتباطات که بایستی برای تعیین الزامات امنیتی شبکه در نظر گرفته شوند و
- ارایه یک تعریف برای حیطه‌های کنترلی بالقوه که شامل حیطه‌هایی که در استانداردهای ISO/IEC 18028-2 تا ISO/IEC 18028-5 به تفصیل شرح داده شده‌اند.

۷- دید کلی

۷-۱- پس‌زمینه

با توجه به گسترش روزافزون جریان کسب‌وکار الکترونیکی در جهان، هر روزه میزان بیشتری از سامانه‌های اطلاعاتی سازمان‌های دولتی و کسب و کار توسط شبکه‌ها به‌هم متصل می‌شوند. این اتصالات شبکه می‌تواند درون‌سازمانی، بین سازمان‌های مختلف و بین سازمان‌ها و مراکز عمومی باشد.

درحقیقت توسعه سریع فناوری شبکه قابل‌دسترس عمومی، به‌ویژه اینترنت و وب جهانی[2]، فرصت‌های بسیاری را برای کسب‌وکار و ارایه سرویس‌های عمومی برخط ایجاد نموده است. این فرصت‌ها از ارایه ارتباطات داده‌ای با هزینه پایین‌تر که از اینترنت به عنوان یک ابزار جهانی برای ایجاد اتصال استفاده

---

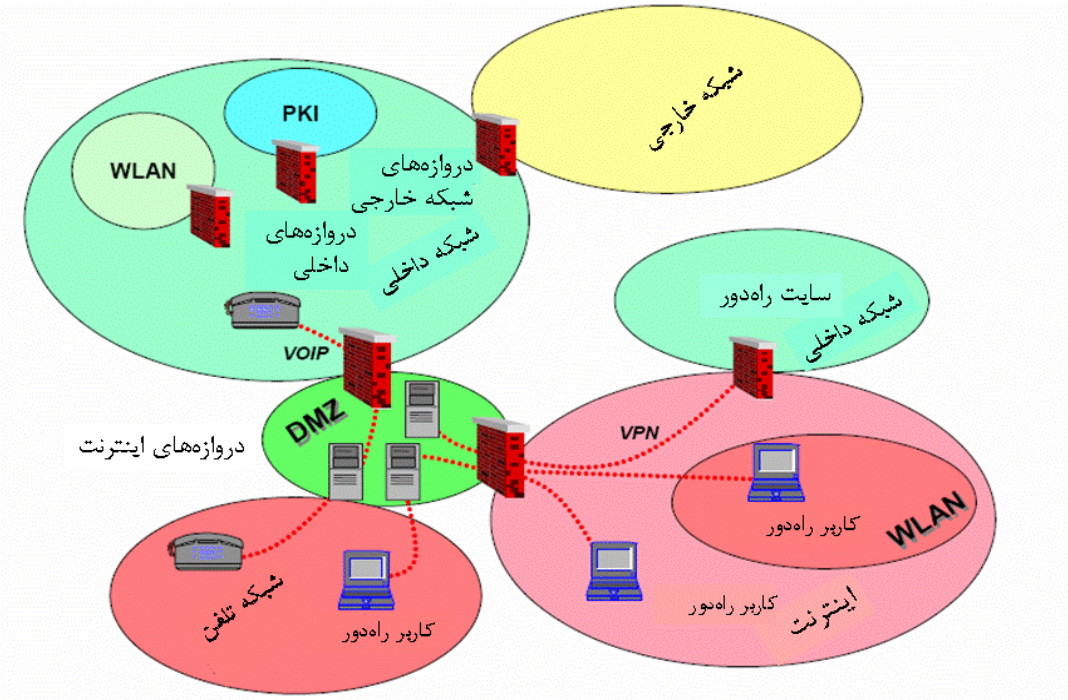
[1] این امر شامل طرح‌ریزی بازیابی در صورت بروز حادثه IT می‌شود

[2] World Wide Web

می‌کنند، تا سرویس‌های بسیار پیچیده توسط ISP، گسترده هستند. بدین مفهوم که استفاده از نقاط اتصال محلی نسبتاً کم‌هزینه در هر نقطه انتهایی مدار برای ارایه خدماتی نظیر تجارت الکترونیکی بر خط در مقیاس زیاد و سامانه‌های تحویل سرویس، با استفاده از برنامه‌های کاربردی و سرویس‌های تحت وب امکان‌پذیر است. به‌علاوه فناوری‌های جدید که شامل یکپارچه‌سازی صوت و داده هستند، فرصت‌های بیشتری را برای ایجاد مدل‌های کسب‌وکار از نوع ارتباطات راه دور فراهم می‌کنند. این موضوع در اغلب مواقع به کارمندان این امکان را می‌دهد که دور از محل کار، با استفاده از تسهیلات راه دور مانند شماره‌گیری[1] یا اتصالات شبکه محلی بی‌سیم، به برقراری ارتباط بین شبکه‌های شرکتی بپردازند و به اطلاعات و سرویس‌های پشتیبان کسب‌وکار ، دست یابند.

با وجود اینکه چنین محیطی مزایای کسب‌وکار بسیاری را به‌دنبال خواهد داشت، اما مخاطرات امنیتی جدیدی را به‌وجود می‌آورد که بایستی مدیریت شوند. بدین ترتیب در سازمان‌هایی که بسیار متکی به استفاده از اطلاعات برای انجام فعالیت‌های کسب‌وکار خود هستند، از دست رفتن هر یک از ابعاد امنیتی محرمانگی، یکپارچگی، دسترس‌پذیری، انکارناپذیری، مسئولیت‌پذیری، اعتبار و قابلیت اطمینان اطلاعات و سرویس‌ها، پیامدهایی منفی بر عملیات کسب‌وکار آنها می‌گذارد. درنتیجه نیازی اساسی به حفاظت از اطلاعات و مدیریت امنیت سامانه‌های اطلاعاتی در سازمان‌ها وجود دارد.

نمونه‌ای از یک سناریوی شبکه‌بندی معمول که در اغلب سازمان‌های امروزی مشاهده می‌شود، در شکل ۱ شرح داده شده است.



شکل ۱- یک محیط شبکه‌بندی معمول

[1] Dial-In

شبکه داخلی بیانگر شبکه‌ای است که یک سازمان بر آن متکی است و به‌طور داخلی پشتیبانی می‌شود. نوعاً تنها افرادی که برای سازمان کار می‌کنند، دسترسی فیزیکی مستقیم به شبکه را دارند و از آنجایی که شبکه در محدوده متعلق به سازمان واقع شده است، سطحی از حفاظت فیزیکی به آسانی قابل دستیابی است. در اغلب حالات، این شبکه‌ها از نظر فناوری‌های به‌کارگرفته شده و الزامات امنیتی، همگن نیستند و ممکن است زیرساخت‌هایی وجود داشته باشند که به سطح حفاظت بالاتری نسبت به آنچه که توسط خود شبکه داخلی برآورده می‌شود، نیاز داشته باشند. چنین زیرساخت‌هایی، نظیر بخش‌های ضروری یک محیط PKI، ممکن است در یک بخش اختصاصی از شبکه داخلی اجرا شوند. از طرف دیگر، فناوری‌های خاص نظیر زیرساخت‌های WLAN، ممکن است به‌دلیل مواجهه با مخاطرات اضافی، نیاز به جداسازی داشته باشند. در هر دو حالت ممکن است دروازه‌های امنیتی شبکه داخلی، به‌منظور پیاده‌سازی این جداسازی مورد استفاده قرارگیرند.

نیازهای کسب‌وکار اکثر سازمان‌های امروزی، ضرورت ارتباطات و تبادل داده‌ای با شرکای خارجی و دیگر سازمان‌ها را ایجاب کرده است. اغلب، بیشتر شرکای مهم کسب‌وکار از طریق گسترش مستقیم شبکه داخلی به شبکه سازمان شریک، متصل می‌شوند، معمولاً عبارت "شبکه خارجی" برای چنین گسترش‌هایی استفاده می‌شود. از آنجا که اعتماد به سازمان‌های شریک متصل‌شده در بیشتر مواقع کمتر از اعتماد در درون سازمان است، به‌منظور پوشش مخاطراتی که از طریق این اتصالات ایجاد می‌شود، از دروازه‌های امنیتی خارجی استفاده می‌شود.

امروزه اغلب از شبکه‌های عمومی و اساساً شبکه‌های داخلی، برای ارایه ارتباطات با هزینه بهینه و تسهیلات تبادل داده‌ای با شرکا و مشتریان (جامعه عمومی) و به‌منظور ارایه انواع گسترش شبکه‌های داخلی استفاده می‌شود. با توجه به سطح پایین اعتماد در شبکه‌های عمومی به‌ویژه اینترنت، نیاز به استفاده از دروازه‌های امنیتی پیچیده برای کمک به مدیریت چنین مخاطراتی است. این دروازه‌های امنیتی، شامل مولفه‌های خاصی برای تعیین الزامات انواع مختلف گسترش‌های شبکه‌های داخلی نظیر اتصالات شرکاء و مشتری هستند.

کاربران راه دور ممکن است با استفاده از فناوری VPN، اتصال برقرار کنند و بیشتر از تسهیلات اتصال بی‌سیم مانند نقاط پرازدحام[1] WLAN عمومی، برای دسترسی به اینترنت استفاده نمایند. به‌روش جایگزین ممکن است کاربران راه دور از شبکه تلفنی برای برقراری اتصالات مستقیم از طریق شماره‌گیری[2] به یک سرویس‌دهنده راه دور که معمولاً در DMZ دیواره آتش اینترنت قرار دارند، استفاده کنند.

هنگامی‌که سازمانی برای پیاده‌سازی شبکه تلفنی داخلی، تصمیم به استفاده از فناوری‌های VoIP می‌گیرد، در این صورت از دروازه‌های امنیتی مناسب برای شبکه تلفنی استفاده می‌شود.

با وجود اینکه در اغلب جنبه‌ها، فناوری‌هایی که برای یک سناریوی شبکه‌بندی معمول استفاده می‌شوند، فرصت‌ها و مزایای بسیاری را برای کسب‌وکار به‌دنبال خواهند داشت به عنوان مثال کاهش دادن یا بهینه کردن هزینه‌ها، ولی استفاده از این فناوری‌ها موجب پیچیده‌تر شدن محیط‌ها می‌شود و مخاطرات

[1] Hotspot
[2] Dial-Up

امنیت اطلاعات جدیدی را به‌وجود می‌آورد. بنابراین، توصیه می‌شود مخاطراتی که در این محیط‌ها مطرح می‌شود، به‌طورصحیح ارزیابی شوند که در این صورت با پیاده‌سازی کنترل‌های امنیتی مناسب، مخاطرات ارزیابی‌شده کاهش می‌یابند.

به بیان دیگر، توصیه می‌شود فرصت‌های کسب‌وکار فراهم‌شده توسط این محیط‌های جدید، در برابر مخاطراتی که به‌واسطه فناوری‌های جدیدتر به‌وجود می‌آید، متعادل شوند. به عنوان مثال، اینترنت دارای مشخصات فنی است که از نقطه‌نظر امنیتی حایز اهمیت هستند. اینترنت اساساً به صورت جهشی و بدون درنظرگرفتن اولویت‌های امنیتی طراحی شده است و بسیاری از پروتکل‌های به‌کار رفته در آن برای استفاده‌های رایج، ماهیتاً امن نیستند. قدرت اصلی اینترنت در این است که یک سامانه بسیار باز است و در ابتدا توسط کمیته تحقیقاتی دانشگاهی در پاسخ به نیازمندی‌های پروژه دولت امریکا به‌وجود آمد و با انتشار گسترده نتایج و توزیع رایگان نرم‌افزار و ملزومات آن همراه بود. موارد فوق موجب عمومیت و رشد سریع اینترنت گردید. با این حال، عمومیت زیاد و باز بودن اینترنت، آسیب‌پذیری‌های امنیتی مهمی را به‌دنبال داشته است. تعداد زیادی از مردم در جهان که دارای ظرفیت، دانش و تمایل به دسترسی به سازوکارها و پروتکل‌های به‌کارگرفته شده در اینترنت هستند، مشکلات امنیتی نظیر دسترسی‌های غیرمجاز تا DoS ویران‌گر در مقیاس بالا را ایجاد می‌کنند.

به‌طور خلاصه میزان سوءاستفاده‌های کسب و کار و دولتی موفق از فرصت‌هایی که توسط شبکه‌بندی جدید ارائه می‌شود، به درجه کنترل و مدیریت مخاطرات عملیاتی در محیط باز وابسته است.

در بند ۷-۲ خلاصه‌ای از فرایند توصیه‌شده برای شناسایی و تحلیل عوامل مرتبط با ارتباطات که بایستی برای ایجاد الزامات امنیتی شبکه در نظر گرفته شوند و همچنین به‌منظور ارایه تعریفی از حیطه‌های نیازمندکنترل، بیان شده است.

۷-۲- فرایند شناسایی

هنگام درنظرگرفتن اتصالات شبکه، می‌بایست تمام افراد یک سازمان که به‌گونه‌ای دارای مسوولیتی مرتبط با اتصالات شبکه هستند، به‌طور کامل از الزامات و منافع کسب‌وکار آن سازمان آگاه باشند. به‌علاوه، این افراد بایستی از مخاطرات امنیتی اتصالات شبکه و حیطه‌های کنترلی مربوطه نیز مطلع باشند. الزامات و منافع کسب‌وکار احتمال دارد بسیاری از تصمیمات اتخاذشده و فعالیت‌های انجام‌شده در فرایند بررسی اتصالات شبکه، شناسایی حیطه‌های کنترلی تعیین‌کننده و در نهایت انتخاب، طراحی، پیاده‌سازی، حفظ و نگهداری از کنترل‌های امنیتی را تحت‌تاثیر قرار دهند. لذا می‌بایست الزامات و منافع کسب‌وکار در تمامی مراحل فرایند به‌طور کامل مدنظر قرار گیرند.

به‌منظور شناسایی و تعیین الزامات امنیتی و حیطه‌های کنترلی مناسب در شبکه، لازم است در ابتدا اقدامات زیر به‌طور کامل صورت گیرد (به استاندارد ISO/IEC 17799 مراجعه شود):

- بازنگری الزامات کلی امنیتی اتصالات شبکه، به همان صورت که در خط‌مشی امنیتی[1] مربوط به اطلاعات تشکیلاتی یک سازمان، تنظیم شده است (به بند ۸ مراجعه شود)،
- بازنگری معماری‌های شبکه و کاربردهای مرتبط با اتصالات شبکه، به‌منظور تامین زمینه لازم برای انجام فعالیت‌های بعدی (به بند ۹ مراجعه شود)،
- شناسایی نوع یا انواع اتصالات شبکه که بایستی در نظر گرفته شوند (به بند ۱۰ مراجعه شود)،
- بازنگری مشخصات شبکه‌بندی پیشنهادی (با استفاده از اطلاعات موجود در شبکه و معماری‌های کاربردی) و روابط اعتماد مربوطه. (به بند ۱۱ مراجعه شود)،
- تعیین انواع مخاطرات امنیتی مربوطه، در صورت امکان با استفاده از نتایج حاصل از بازنگری ارزیابی و مدیریت مخاطرات - شامل درنظر گرفتن ارزش اطلاعات منتقل‌شده از طریق اتصالات برای فعالیت‌های کسب‌وکار و نیز ارزش هر نوع دیگری از اطلاعات که به‌طور بالقوه به یک شیوه غیرمجاز از طریق این اتصالات قابل دسترسی باشند و ارزش سرویس‌های ارایه‌شده[2] (به بند ۱۲ مراجعه شود)،
- شناسایی حیطه‌های کنترلی مناسب و متناسب با نوع (انواع) اتصال شبکه، شناسایی مشخصات شبکه‌بندی و روابط اعتماد وابسته و نیز انواع مخاطرات امنیتی مشخص‌شده و به موازات آن مستندسازی و بازنگری گزینه‌های معماری امنیت و توافق بر روی گزینه‌های ارجح [3](به بند ۱۳ مراجعه شود)،
- پیاده‌سازی و اجرای کنترل‌های امنیتی (به بند ۱۴ مراجعه شود) و
- بازنگری و پایش پیاده‌سازی کنترل‌های امنیتی به‌طور مداوم و پیوسته[4] (به بند ۱۵ مراجعه شود).

لازم به ذکر است که توصیه‌های کلی در زمینه شناسایی کنترل‌ها، در استاندارد ISO/IEC17799 عنوان شده است و در استاندارد ISO/IEC 13335-2 نیز پس از انتشار موجود خواهد بود. در این استاندارد تکمیل‌کننده دو استاندارد فوق است و به معرفی چگونگی شناسایی حیطه‌های کنترل مناسب، با توجه به امنیت مرتبط با اتصالات به شبکه‌های ارتباطی پرداخته است و به‌همین دلیل مکمل قسمت دوم این استاندارد و استانداردهای ISO/IEC 18028-3 تا ISO/IEC 18028-5 نیز است.

---

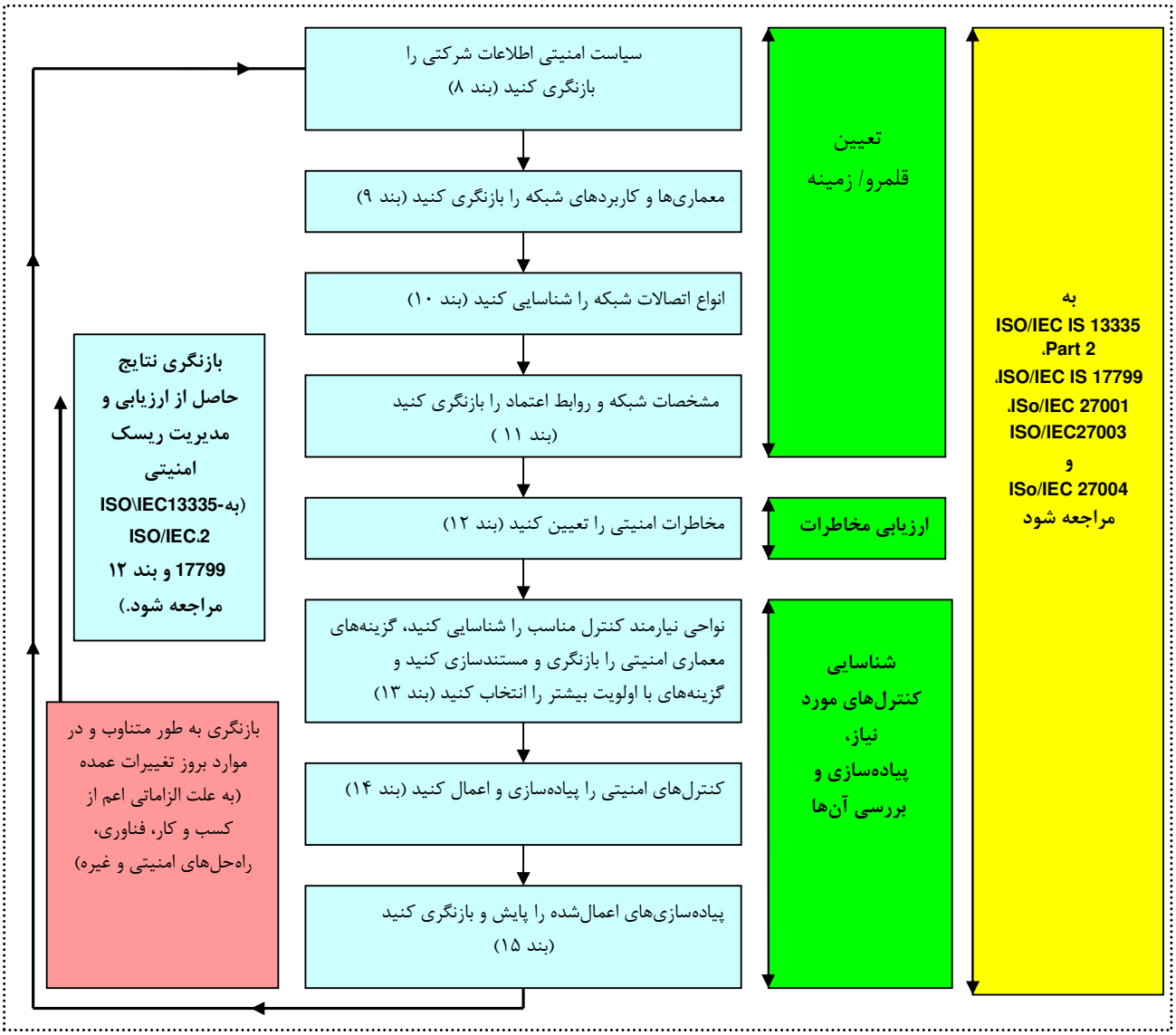
[1] این امر شامل وضعیت خطی‌مشی در زمینه‌های (۱) الزامات قانونی و مقررات مربوط به اتصالات شبکه به همان‌صورت که توسط نهادهای تنظیم کننده و قانون‌گذار مربوطه (نظیر آژانس‌های ملی دولتی) تعریف شده است، (۲) طبقه‌بندی داده‌هایی که لازم است در شبکه ذخیره شوند یا از طریق آن منتقل شوند، است.

[2] این امر شامل (۱) ارزیابی مخاطرات مربوط به نقض بالقوه قوانین و مقررات مرتبط با اتصالات شبکه می‌باشد، به همان‌صورت که توسط موسسه‌های تنظیم‌کننده و قانون‌گذار مربوطه تعریف شده است (نظیر آژانس‌های ملی دولتی) و (۲) استفاده از تاثیرات بالقوه مخرب کسب و کار توافق شده، تایید دسته‌بندی داده‌هایی که لازم است در شبکه ذخیره شوند یا از طریق آن منتقل شوند.

[3] این امر شامل کنترل‌های مورد نیاز جهت تطبیق با قوانین و مقررات مربوط به اتصالات شبکه می‌باشد، به همان صورت که توسط موسسه‌های تنظیم‌کننده و قانون‌گذار تعریف شده است (نظیر آژانس‌های ملی دولتی).

[4] این امر شامل پایش و بازنگری کنترل‌های مورد نیاز جهت تطبیق با قوانین و مقررات مربوط به اتصالات شبکه می‌باشد، به همان صورت که توسط موسسه‌های تنظیم‌کننده و قانون‌گذار تعریف شده است (نظیر آژانس‌های ملی دولتی).

شکل۲ به تشریح فرایند کلی شناسایی و تحلیل عوامل مربوط به ارتباطات که لازم است برای تعیین الزامات امنیت شبکه به‌کار گرفته شوند و نیز ارایه شاخص‌هایی از حیطه‌های کنترلی بالقوه، پرداخته است. هر مرحله در این فرآیند، در بندهایی که پس از این شکل آمده، به‌تفصیل توصیف شده است.



شکل ۲- فرآیند مدیریت در زمینه امنیت شبکه

در شکل۲ خطوط مشکی پررنگ، بیانگر مسیر اصلی فرآیند مدیریت است و خط مشکی نقطه‌چین بیانگر مکانی است که انواع مخاطرات امنیتی می‌توانند با استفاده از نتایج حاصل از بازنگری ارزیابی و مدیریت مخاطرات امنیتی تعیین شوند.

علاوه بر مسیر اصلی فرآیند، در برخی مراحل خاص نیاز است نتایج مراحل قبلی به‌منظور حصول اطمینان از سازگار بودن مراحل مختلف، مجدداً بازدید شوند، به‌ویژه مراحل "بازنگری خط‌مشی امنیتی اطلاعات شرکتی" و "بازنگری معماری‌ها و کاربردها" به‌عنوان مثال،

- پس از تعیین انواع مخاطرات امنیتی، ممکن است نیاز به بازنگری خط مشی امنیتی اطلاعات شرکتی باشد، زیرا ممکن است عاملی ظاهر شده باشد که در آن سطح از خط‌مشی تحت پوشش قرار نگرفته است.
- در شناسایی حیطه‌های کنترلی بالقوه، لازم است خط‌مشی امنیت در زمینه اطلاعات شرکتی درنظر گرفته شود، زیرا به‌عنوان مثال ممکن است خط‌مشی امنیتی تعیین کند که در یک سازمان، یک کنترل خاص باید بدون در نظر گرفتن مخاطرات اعمال شود، و
- در بازنگری گزینه‌های معماری امنیت بایستی به‌منظور حصول اطمینان از سازگار بودن، معماری‌ها و کاربردهای شبکه در نظر گرفته شوند.

۸- ملاحظه الزامات خط‌مشی امنیتی اطلاعات شرکتی

خط‌مشی امنیت اطلاعات شرکتی یک سازمان، ممکن است شامل بیانیه‌هایی در زمینه ضرورت نیاز به محرمانگی، یکپارچگی، دسترس‌پذیری، انکارناپذیری، مسئولیت‌پذیری، اعتبار، قابلیت اطمینان و همچنین دیدگاه‌هایی در مورد انواع تهدیدات و الزامات کنترلی که به‌طور مستقیم مربوط به اتصالات شبکه هستند، باشد.

به‌عنوان مثال یک چنین خط‌مشی امنیتی می‌تواند موارد زیر را به‌طور صریح عنوان کند:

- دسترس‌پذیری انواع خاصی از اطلاعات یا سرویس‌ها، بسیار حایز اهمیت است،
- هیچ‌گونه اتصالی از طریق خطوط تلفن[1] مجاز نیست،
- هرگونه اتصالی به اینترنت بایستی از طریق دروازه امنیتی صورت گیرد،
- یک نوع خاص دروازه امنیتی بایستی مورد استفاده قرار گیرد،
- هیچ‌گونه دستورالعمل پرداختی بدون امضای دیجیتالی معتبر نیست.

چنین بیانیه‌ها، نگرش‌ها و الزاماتی که قابل اجرا در یک سازمان یا گستره اجتماع هستند، بایستی در تعیین انواع مخاطرات امنیتی (به بند ۱۲ در زیر مراجعه شود) و شناسایی حیطه‌های کنترلی بالقوه برای اتصالات شبکه (به بند۱۳ در زیر مراجعه شود)، مورد توجه قرار گیرند. در صورت وجود چنین الزامات امنیتی، لازم است این الزامات در فهرست پیش‌نویس حیطه‌های کنترلی بالقوه، ثبت و مستندسازی شوند و در صورت لزوم در گزینه‌های معماری امنیت نیز منعکس گردند. در زمینه جایگاه سند خط‌مشی امنیتی اطلاعات شرکتی در رویکرد یک سازمان به امر امنیت اطلاعات، همچنین در زمینه محتویات این استاندارد و چگونگی ارتباط آن با سایر اسناد امنیتی، رهنمودهایی در استانداردهای ISO/IEC 13335-1 و ISO/IEC 177799 عنوان شده است و در استاندارد ISO/IEC 13335-2 پس از انتشار موجود خواهد بود.

[1] Dial-Up Lines

۹- بازنگری معماری‌ها و کاربردهای شبکه

۹-۱- پس‌زمینه

همان‌گونه که پیش از این عنوان شد، مراحل لازم برای حصول اطمینان از درنظر گرفتن تمامی کنترل‌های بالقوه مورد نیاز، به‌منظور برقراری امنیت در شبکه، به صورت زیر هستند:

- شناسایی نوع (انواع) اتصالات شبکه که مورد استفاده قرار می‌گیرد،
- شناسایی مشخصات شبکه‌بندی و روابط اعتماد وابسته به آن،
- تعیین مخاطرات امنیتی،
- تهیه فهرستی از حیطه‌های کنترلی مورد نیاز[۱] و طراحی‌های مربوطه.

توصیه می‌شود متابعت از این مراحل در زمینه معماری شبکه و کاربردهایی که موجودند و یا برنامه‌ریزی می‌شوند، صورت گیرد.

از این‌رو بایستی جزییات لازم از معماری شبکه مربوطه و کاربردهای آن استخراج شود و به‌منظور ایجاد زمینه و درک لازم از مراحل مختلف فرآیند، بازنگری شود.

با تشریح این جنبه‌ها در نخستین مرحله ممکن، بایستی فرایند تعیین معیارهای مربوط به شناسایی الزامات امنیتی، شناسایی حیطه‌های کنترلی و بازنگری گزینه‌های فنی معماری امنیت و تصمیم‌گیری در مورد اینکه کدام‌یک بایستی اتخاذ شود، کارآمدتر گردد و در نهایت منجر به راه‌حل امنیتی کاراتر شود.

ملاحظه جنبه‌های وابسته به معماری شبکه و کاربردها در مراحل اولیه، بایستی این امکان را برای معماری‌هایی که یک راه‌حل امنیتی مقبول در آنها به‌صورت واقع‌گرایانه وجود ندارد، فراهم نماید تا مورد بازنگری و اصلاح قرار گیرند.

حیطه‌های مختلفی که باید در نظر گرفته شوند، شامل موارد زیر هستند:

- انواع شبکه،
- پروتکل‌های شبکه،
- کاربردهای شبکه،
- فناوری‌های به‌کار گرفته شده برای پیاده‌سازی شبکه‌ها.

برخی از موارد مربوط به بازنگری هر یک از این حیطه‌ها، در بندهای ۹-۲ تا ۹-۶، مورد بحث قرار گرفته‌اند. بند ۱۰ راهنمایی‌هایی در زمینه نحوه شناسایی انواع اتصالات شبکه، بند ۱۱ راهنمایی‌هایی در زمینه نحوه تعیین مشخصات شبکه‌بندی و روابط اعتماد مربوط به آن و بند ۱۲ راهنمایی‌هایی در رابطه با شناسایی مخاطرات امنیتی ارایه می‌دهد (راهنمایی‌های عمومی در مورد معماری‌ها و کاربردهای شبکه در استاندارد ISO/IEC 7498 موجود است).

---

[۱] شامل حیطه‌های کنترلی مرتبط با استفاده از رمزنگاری برای مواردی نظیر محرمانگی، یکپارچگی و احراز اصالت.

۹-۲- انواع شبکه

شبکه‌ها با توجه به ناحیه‌ای که تحت پوشش قرار می‌دهند، به صورت زیر دسته‌بندی می‌شوند:

- شبکه‌های LAN که برای اتصال سامانه‌ها به طور محلی مورد استفاده قرار می‌گیرند، و
- شبکه‌های WAN که برای اتصال سامانه‌ها در سطح وسیع و حتی جهانی مورد استفاده قرار می‌گیرند.

(برخی منابع به تعریف "شبکه‌های شهری"[1] پرداخته‌اند که به شبکه‌های وسیع و محدودشده به یک ناحیه خاص همچون یک شهر، اطلاق می‌شود. از آنجا که امروزه فناوری به‌کارگرفته شده در شبکه‌های شهری و شبکه‌های WAN یکسان است، لذا تفاوت عمده‌ای بین شبکه‌های شهری و شبکه‌های WAN وجود ندارد، همچنین در این استاندارد "شبکه‌های شخصی"[2] در دسته شبکه‌های LAN قرار می‌گیرد).

۹-۳- پروتکل‌های شبکه

پروتکل‌های مختلف دارای مشخصات امنیتی متفاوتی هستند، لذا بایستی به‌طور خاص تحت بررسی قرار گیرند. به‌عنوان مثال:

- پروتکل‌های رسانه‌ی به اشتراک گذاشته که به‌طور عمده در شبکه‌های LAN مورد استفاده قرار می‌گیرند و سازوکارهایی در زمینه تنظیم استفاده از رسانه‌ی به اشتراک گذاشته، در سامانه‌های به‌هم متصل فراهم می‌کنند. هنگامی‌که یک رسانه به اشتراک گذاشته‌شده، مورد استفاده قرار می‌گیرد، تمام اطلاعات موجود در شبکه از طریق کلیه سامانه‌های به‌هم متصل در طول مسیر، به‌طور فیزیکی قابل دستیابی است.
- پروتکل‌های مسیریابی برای تعیین مسیر انتقال اطلاعات بین گره‌های مختلف در شبکه‌های WAN، مورد استفاده قرار می‌گیرند. اطلاعات در طول مسیر به‌طور فیزیکی برای تمام سامانه‌ها قابل دستیابی است، به‌علاوه مسیریابی به‌طور تصادفی یا عمدی قابل تغییر است، و
- پروتکل‌های MPLS که اغلب شبکه‌های حامل مبتنی بر آنها هستند، این امکان را برای "شبکه هسته حامل"[3] فراهم می‌کنند که توسط VPNهای متعددی به اشتراک گذاشته شود، بدون اینکه هیچ‌یک از این VPNها از وجود VPN دیگری که شبکه هسته را به اشتراک گذاشته است، مطلع شود. کاربرد عمده این پروتکل‌ها در پیاده‌سازی VPNها است که با استفاده از برچسب‌های مختلف به شناسایی و جداسازی ترافیک VPNهای مختلف پرداخته می‌شود (VPN که مبتنی بر MPLS باشد، بر پایه سازوکارهای رمزنگاری داده نیست). در این حالت این امکان برای مشتریان شرکتی فراهم می‌شود که شبکه داخلی خود را به یک ISP واگذار نمایند و به این ترتیب به استقرار و مدیریت شبکه هسته IP خود نیاز نخواهند داشت. مزیت

[1] Metropolitan Area Network, MAN
[2] Personal Area Network, PAN
[3] Carrier Core Network

اصلی این عمل، قابلیت همگرا کردن سرویس‌های شبکه همچون صوت و داده با استفاده از سازوکارهای کیفیت سرویس‌دهی و به‌منظور تضمین کارایی بلادرنگ است.

بسیاری از پروتکل‌های مورد استفاده در شبکه، هیچ امنیتی را فراهم نمی‌کنند. به‌عنوان مثال، ابزارهایی که با استفاده از آنها می‌توان کلمه‌های عبور را از ترافیک شبکه به‌دست آورد، عموماً توسط مهاجمان مورد استفاده قرار می‌گیرند که این موضوع ارسال کلمه‌های عبور رمزنگاری‌نشده در یک شبکه عمومی را بسیار آسیب‌پذیر می‌سازد.

بسیاری از پروتکل‌ها می‌توانند در همبندی‌ها و رسانه‌های مختلف شبکه و همچنین با فناوری‌های باسیم و یا بی‌سیم مورد استفاده قرار گیرند، که در بسیاری از حالات مشخصات امنیتی شبکه را تحت‌تاثیر قرار می‌دهند.

۹-۴- کاربردهای شبکه‌ای

لازم است در بحث امنیت، نوع کاربردی که در شبکه استفاده می‌شود، مدنظر قرار گیرد. انواع کاربردها شامل موارد زیر هستند:

- "کاربردهای سرویس‌گیرنده نازک "[1]،
- کاربردهای "میز کار"[2]،
- کاربردهای مبتنی بر "تقلید"[3] پایانه‌ها،
- زیرساخت‌ها و کاربردهای انتقال پیغام،
- کاربردهای مبتنی بر ذخیره‌سازی و ارسال به‌جلو یا مبتنی بر "برنامه ردیف‌گر"[4]، و
- کاربردهای مشتری- خدمتگزار.

مثال‌های زیر نشان می‌دهد که چگونه مشخصات یک برنامه کاربردی، الزامات امنیتی محیط‌های شبکه‌ای که از این برنامه‌ها استفاده کرده است را تحت‌تاثیر قرار می‌دهد:

- کاربردهای انتقال پیغام (همچون رمزنگاری و امضاهای دیجیتالی پیغام‌ها) بدون تخصیص کنترل‌های امنیتی خاص در شبکه، یک سطح امنیتی مناسب را ارایه می‌دهند.
- کاربردهای سرویس‌گیرنده نازک ممکن است به‌منظور عملکرد مناسب، نیاز به بارگیری کد سیار[5] داشته باشند. با وجود اینکه محرمانگی موضوع عمده در این زمینه نیست، ولی یکپارچگی داده حایز اهمیت است و بایستی در این راستا شبکه سازوکارهای مناسبی فراهم نماید. همچنین در صورتی‌که نیاز به برآوردن الزامات بیشتری باشد، امضاهای دیجیتالی کدهای سیار، یکپارچگی داده و احراز اصالت اضافه را فراهم می‌کنند. اغلب این عمل در چارچوب یک کاربرد صورت می‌گیرد و بنابرین ممکن است نیاز به ارایه این سرویس‌ها توسط شبکه نباشد.

---

[1] Thin Client Applications
[2] Desktop Applications
[3] Emulation
[4] Spooler
[5] Download Mobile Code

- معمولاً کاربردها مبتنی بر ذخیره‌سازی و ارسال به‌جلو[1] یا مبتنی بر برنامه ردیف‌گر[2]، به‌طور موقت و به‌منظور پردازش بیشتر، به ذخیره‌سازی داده‌های حایز اهمیت در گره‌های میانی می‌پردازند. در صورت نیاز به یکپارچگی داده و محرمانگی و به‌منظور حفاظت از داده‌های در حال انتقال، اعمال کنترل‌های مناسب در شبکه مورد نیاز است. با این وجود، به دلیل ذخیره‌سازی موقت داده‌ها در میزبان‌های میانی، ممکن است این کنترل‌ها کافی نباشند. از این‌رو ممکن است نیاز به اعمال کنترل‌های اضافه روی داده‌های ذخیره شده در گره‌های میانی باشد.

۹-۵- فناوری‌های مورد استفاده برای پیاده‌سازی شبکه‌ها

شبکه‌ها ممکن است به صورت‌های مختلفی ارایه شوند. معمول‌ترین ساختار آنها ارایه براساس نواحی جغرافیایی است که توسط یک شبکه تحت پوشش قرار می‌گیرد.

۹-۵-۱- شبکه‌های محلی

یک LAN، شبکه‌ای برای اتصال رایانه‌ها و سرویس‌دهندگان در یک ناحیه کوچک جغرافیایی است. اندازه یک شبکه محلی می‌تواند از تعداد محدودی سامانه به‌هم متصل که به‌عنوان مثال یک شبکه خانگی را تشکیل می‌دهند، تا چند هزار سامانه موجود در یک شبکه دانشگاهی[3]، متغیر باشد. سرویس‌های معمول پیاده‌سازی شده در این شبکه‌ها شامل به اشتراک گذاشتن منابع نظیر چاپگرها و به اشتراک گذاشتن فایل‌ها و برنامه‌های کاربردی هستند. شبکه‌های LAN، سرویس‌هایی مرکزی نظیر سرویس‌های انتقال پیغام یا سرویس‌های روزشمار (تقویمی) را نیز ارایه می‌دهند. در برخی موارد نیز شبکه‌های LAN به‌عنوان جایگزین کارکرد سنتی سایر شبکه‌ها مورد استفاده قرار می‌گیرند، به‌عنوان مثال می‌توان به پروتکل‌ها و سرویس‌هایVoIP که به‌عنوان جانشینی برای شبکه‌های تلفن مبتنی بر مرکز تلفن داخلی ارایه می‌شوند، اشاره نمود. شبکه‌های LAN کوچک عموماً با استفاده از فناوری‌های رسانه به اشتراک گذاشته‌شده پیاده‌سازی می‌شوند. پروتکل Ethernet یک فناوری استاندارد است که در این راستا مورد استفاده قرار می‌گیرد و به‌منظور ارایه پهنای باند بیشتر و نیز پشتیبانی از محیط‌های بی‌سیم، توسعه یافته است. از آنجایی که فناوری‌های رسانه به اشتراک گذاشته‌شده و به‌ویژه Ethernet، در شبکه‌های با اندازه بزرگ دارای محدودیت‌هایی هستند، فناوری‌های نوعی مورد استفاده در شبکه‌های WAN، نظیر پروتکل‌های مسیریابی، اغلب در شبکه‌های LAN نیز مورد استفاده قرار می‌گیرد. یک شبکه محلی می‌تواند با سیم و یا بی‌سیم باشد.

---

[1] Forward
[2] Spooler
[3] Campus Network

۹-۵-۱-۱ شبکه محلی باسیم

شبکه محلی باسیم، معمولاً از گره‌هایی تشکیل شده است که در یک شبکه از طریق یک سوده یا هاب و با استفاده از کابل‌های شبکه‌بندی به هم متصل هستند و به‌این ترتیب یک شبکه داده با سرعت بالا را به‌وجود می‌آورند. فناوری‌های شناخته شده‌ای که در LANهای باسیم مورد استفاده قرار می‌گیرد، شامل Ethernet (IEEE 802.3) و Token Ring (IEEE 802.5) هستند.

۹-۵-۱-۲ شبکه محلی بی‌سیم

WLAN، با استفاده از امواج رادیویی فرکانس بالا، به ارسال بسته‌های شبکه از طریق هوا می‌پردازد. انعطاف‌پذیری این شبکه‌ها به دلیل عدم نیاز به کابل‌کشی در ایجاد شبکه است. فناوری‌های معروف به‌کار گرفته شده در WLANها، پیاده‌سازی‌های ارایه‌شده در IEEE 802.11 و همچنین Bluetooth هستند.

۹-۵-۲- شبکه‌های گسترده

شبکه‌های WAN برای اتصال مکان‌های دور و اتصال شبکه‌های LAN آنها مورد استفاده قرار می‌گیرند. یک WAN می‌تواند با استفاده از کابل‌ها و مدارها از یک سرویس‌دهنده و یا از طریق اجاره یک سرویس از یک ارایه‌دهنده سرویس‌های ارتباطات راه دور ایجاد شود. فناوری‌های به‌کار گرفته شده در شبکه‌های WAN امکان ارسال و مسیریابی ترافیک شبکه در یک مسیر طولانی را فراهم می‌کنند و معمولاً تسهیلات وسیع مسیریابی برای هدایت بسته‌های شبکه به سمت شبکه محلی مقصد را فراهم می‌کند. نوعاً زیرساخت شبکه‌بندی فیزیکی عمومی، برای اتصال بین شبکه‌های LAN مورد استفاده قرار می‌گیرد به‌عنوان مثال می‌توان به خطوط اجاره‌ای ارتباطات ماهواره‌ای یا فیبرهای نوری اشاره نمود. یک WAN می‌تواند باسیم و یا بی‌سیم باشد.

۹-۵-۲-۱ شبکه‌های گسترده باسیم

WAN باسیم معمولاً از دستگاه‌های مسیریابی (مانند مسیریاب‌ها) تشکیل شده است که از طریق سیم‌های مخابراتی به یک شبکه خصوصی یا عمومی متصل شده‌اند. معروف‌ترین فناوری‌های باسیم به‌کارگرفته شده در شبکه‌های ATM WAN، Frame Relay و X.25 هستند.

۹-۵-۲-۲ شبکه‌های گسترده بی‌سیم

WAN بی‌سیم، معمولاً با استفاده از امواج رادیویی به ارسال بسته‌های شبکه از طریق هوا در یک مسافت طولانی می‌پردازد که این مسافت می‌تواند تا ده کیلومتر و یا بیشتر نیز باشد. فناوری‌های معروف به‌کار گرفته‌شده در شبکه‌های WAN شامل TDMA، CDMA، GSM و IEEE802.16 هستند.

۹-۶- سایر ملاحظات

در هنگام بازنگری معماری شبکه و کاربردهای آن لازم است اتصالات شبکه موجود در درون سازمان، به آن سازمان و یا از آن سازمان و همچنین شبکه‌ای که یک اتصال به آن صورت گرفته است، درنظر گرفته شوند. اتصالاتی که در سازمان موجود هستند، ممکن است اتصالات جدید را به دلایلی همچون توافق‌نامه‌ها یا قراردادها محدود کنند و یا از برقراری آنها جلوگیری نمایند. وجود سایر اتصالات به شبکه و یا از شبکه‌ای که یک اتصال از آن مورد نیاز است، می‌تواند آسیب‌پذیری‌های اضافی و در نتیجه مخاطرات بیشتری را موجب شود و احتمالاً نیاز به تضمین قوی‌تر و/یا کنترل‌های اضافه باشد.

۱۰- شناسایی انواع اتصالات شبکه

انواع کلی مختلفی از اتصالات شبکه وجود دارد که یک سازمان یا اجتماع می‌تواند از آنها استفاده کند. برخی از این اتصالات، از طریق VPNها (که دسترسی به آنها محدود به یک اجتماع شناخته‌شده است) و برخی از طریق شبکه‌های عمومی (که دسترسی به آنها به‌طور بالقوه برای هر فرد و سازمان امکان‌پذیر است) ایجاد می‌شود. به‌علاوه انواع مختلف اتصالات شبکه می‌توانند برای سرویس‌های متنوعی همچون پست الکترونیکی یا EDI داده مورد استفاده قرارگیرند و همچنین می‌توانند شامل استفاده ازتسهیلات اینترنت، شبکه داخلی (اینترانت) یا شبکه خارجی (اکسترانت) باشند که هر یک دارای ملاحظات امنیتی جداگانه است. هر نوع از اتصالات شبکه دارای آسیب‌پذیری‌های متفاوت و مخاطرات امنیتی خاص خود است و در نتیجه نیازمند مجموعه متفاوتی از کنترل‌ها است. (به استاندارد ISO/IEC 177799 مراجعه شود).

جدول ۱، یک روش برای دسته‌بندی انواع کلی اتصالات شبکه که ممکن است برای مدیریت کسب‌وکار مورد نیاز باشند، به همراه یک مثال توصیفی برای هر نوع را نشان می‌دهد.

با توجه به معماری‌ها و کاربردهای شبکه مربوطه، لازم است یک یا بیش از یک نوع ارایه‌شده در جدول ۱، برای اتصال (اتصالات) شبکه مورد نظر، به‌طور مناسب انتخاب شود.

قابل ذکر است که انواع کلی اتصالات شبکه توصیف‌شده در این استاندارد، بیشتر از نقطه‌نظر کسب‌وکار دسته‌بندی و سازماندهی شده‌اند تا از نقطه‌نظر فنی، بدین معنا که دو نوع متفاوت اتصالات شبکه ممکن است گاهی با فنون فنی یکسان پیاده‌سازی شوند که در این حالت، در برخی موارد ممکن است کنترل‌های اعمال‌شده یکسان باشد، در حالی‌که در موارد دیگر، ممکن است این کنترل‌ها متفاوت باشند.

جدول ۱- انواع اتصالات شبکه

حرف ارجاع	نوع اتصالات شبکه	مثال توصیفی
A	اتصال درون منطقه کنترل شده منفرد از یک سازمان	اتصال بین بخش‌های مختلف یک سازمان، درون یک منطقه کنترل‌شده، به‌عنوان مثال یک ساختمان منفرد کنترل‌شده یا یک سایت.
B	اتصال بین بخش‌هایی از یک سازمان که از	اتصال بین ادارات منطقه‌ای (و/یا ادارات منطقه‌ای با سایت اداره مرکزی) درون یک سازمان منفرد از طریق یک

	نظر جغرافیایی مجزا و متفاوت هستند.	WAN. در این نوع اتصال، نه تنها تمام کاربران قادر به دسترسی به سامانه‌های اطلاعاتی که در شبکه موجود است، نیستند، بلکه تمام کاربران داخل سازمان نیز مجاز به دسترسی به تمام کاربردها و اطلاعات نیستند. (به‌عنوان مثال دسترسی هر کاربر، تنها مطابق امتیازات اعطاشده است). یک نوع دسترسی از بخش دیگر سازمان می‌تواند برای مقاصد پشتیبانی راه دور باشد. همچنین ممکن است برای این نوع کاربران و این نوع اتصالات، اختیارات ویژه دسترسی بیشتری نیز موجود باشد.
C	اتصالات بین سایت یک سازمان و کارکنانی که در محل‌هایی دور از آن سازمان کار می‌کنند.	استفاده از پایانه‌های داده‌ای سیار توسط کارمندان (به‌عنوان مثال فروشنده‌ای که از طریق یک سایت مشتری به بررسی موجودی می‌پردازد) یا برقراری پیوندهای راه دور به سامانه‌های محاسباتی یک سازمان، توسط کارمندانی که در خانه یا سایت‌های دور کار می‌کنند و از طریق شبکه آن سازمان به هم متصل نیستند.
D	اتصالات بین سازمان‌های مختلف درون یک اجتماع بسته، به عنوان مثال به دلایل مختلفی از جمله شرایط اجباری قراردادی یا قانونی یکسان یا ذی‌نفعان کسب‌وکار نظیر بانکداری یا بیمه.	اتصالات بین دو یا چند سازمان برای تسهیل تراکنش‌های الکترونیکی بین سازمانی به دلیل یک نیاز کسب‌وکار (به‌عنوان مثال انتقال سهام‌های الکترونیکی در صنعت بانکداری). این نوع از اتصال شبکه مشابه قسمت B است، به‌جز این‌که سایت‌هایی که به هم متصل می‌شوند، متعلق به دو یا چند سازمان هستند و هدف از ایجاد اتصال، فراهم ساختن امکان دسترسی به تمام کاربردهای مورد استفاده توسط هر یک از سازمان‌های شرکت‌کننده، نیست.
E	اتصالات به سایر سازمان‌ها	ممکن است دسترسی به پایگاه‌های داده راه دوری که توسط سایر سازمان‌ها نگهداری می‌شود، امکان‌پذیر باشد، (به‌عنوان مثال از طریق ارایه‌دهندگان سرویس). در این نوع از اتصالات شبکه، تمام کاربران از جمله کاربرانی که به سازمان متصل می‌شوند، به‌طور انفرادی توسط سازمان خارجی که امکان دسترسی به اطلاعاتش را فراهم کرده است، از قبل مجوزدهی می‌شوند. اگرچه در ابتدا تمام کاربران مجوزدهی می‌شوند ولی هیچ تمایزی بین کاربران برحسب توانایی آنها برای پرداخت هزینه سرویس ارایه‌شده، وجود ندارد. همچنین ممکن است دسترسی به کاربردها در سامانه‌هایی از سازمان که به ذخیره یا پردازش اطلاعات شرکتی می‌پردازند، برای کاربران خارج از سازمان امکان‌پذیر باشد. در این شرایط لازم است کاربران خارج سازمان، شناسایی و مجوزدهی شوند. یک نوع دسترسی از

		سازمان دیگر می‌تواند برای مقاصد پشتیبانی راه دور باشد. همچنین ممکن است برای این نوع کاربران و این نوع اتصالات، امتیازات دسترسی بیشتری نیز موجود باشد.
F	اتصالات به حوزه عمومی	دسترسی به پایگاه‌های داده قابل دسترسی عمومی، می‌تواند توسط کاربران سازمان صورت گیرد، وب سایت‌ها و/یا تسهیلات پست الکترونیکی (به‌عنوان مثال از طریق اینترنت)، که دسترسی به‌منظور بازیابی اطلاعات یا ارسال اطلاعات از/به افراد و/ یا مکان‌هایی صورت می‌گیرد که به‌طور خاص توسط سازمان، از قبل مجوزدهی نشده‌اند. در این نوع اتصال، کاربران سازمان از این امکان برای مقاصد سازمانی (حتی خصوصی) استفاده می‌کنند، هرچند سازمان ممکن است کنترل اندکی بر روی اطلاعات در حال انتقال داشته باشد. همچنین دسترسی می‌تواند توسط کاربران خارج سازمان به تسهیلات سازمانی صورت گیرد (به‌عنوان مثال از طریق اینترنت). در این نوع اتصال شبکه، دسترسی افراد خارج سازمان، صریحاً توسط سازمان مجوزدهی نشده است.
G	اتصالات به شبکه تلفن عمومی از یک محیط IP	دسترسی به PSTN از طریق یک تلفن در یک شبکه IP صورت می‌گیرد. این نوع اتصالات کنترل‌شده نیستند، به این دلیل‌که مکالمات می‌تواند از هر ناحیه‌ای در جهان دریافت شود.

۱۱- بازنگری مشخصات شبکه و روابط اعتماد مربوط

۱۱-۱- مشخصات شبکه

لازم است مشخصات شبکه موجود یا شبکه پیشنهادی تحت بازنگری قرار گیرد. به‌ویژه شناسایی اینکه شبکه ازکدام نوع زیر است، بسیار حایز اهمیت است:

- شبکه عمومی - شبکه قابل دسترسی توسط هر فرد، یا
- شبکه خصوصی، به‌عنوان مثال شبکه‌ای که شامل خطوط شخصی یا اجاره‌ای است، از این‌رو امن‌تر از یک شبکه عمومی در نظر گرفته می‌شود.

همچنین آگاهی از نوع داده منتقل‌شده توسط شبکه نیز دارای اهمیت است، به‌عنوان مثال:

- شبکه داده- شبکه‌ای که به انتقال داده‌های اصلی و استفاده از پروتکل‌های داده می‌پردازد،
- شبکه صوت- شبکه‌ای که برای ارایه سرویس تلفن ایجاد شده است، ولی قابل استفاده برای انتقال داده نیز است یا
- شبکه‌ای شامل داده و صوت و احتمالاً تصویر.

سایر اطلاعات، همچون اطلاعات زیر نیز مرتبط هستند:

- اینکه یک شبکه مبتنی بر بسته است یا سوده،
- آیا در یک شبکه، MPLS از کیفیت سرویس‌دهی پشتیبانی می‌کند،

(کیفیت سرویس‌دهی در ارتباط با عملکرد سازگار است. سرویس‌های شبکه باید به‌گونه‌ای ارایه شوند تا بتوانند کمترین سطح عملکرد قابل استفاده را فراهم کنند. به‌عنوان مثال در صورتی‌که پهنای باند کافی، وجود نداشته باشد، سرویس صوت به‌طور مکرر قطع و وصل و در نهایت به‌طورکلی قطع خواهد شد. کیفیت سرویس‌دهی به معنای قابلیت یک سامانه شبکه در حفظ سرویس ارایه‌شده در کمترین سطح عملکرد یا بالاتر از آن است).

به‌علاوه لازم است معلوم شود که یک اتصال دایمی است یا تنها در مواقع نیاز ایجاد می‌شود.

۱۱-۲- روابط اعتماد

پس ازاینکه مشخصات شبکه‌بندی موجود یا پیشنهادشده، شناسایی و در کمترین حد ممکن ایجاد گردید، در صورتی‌که شبکه، یک شبکه عمومی یا خصوصی باشد، بایستی روابط اعتماد مربوط شناسایی شوند. (به بند۱۱-۱ در بالا مراجعه شود)

در ابتدا لازم است محیط(های) اعتماد قابل کاربرد که مرتبط با اتصال (اتصالات) شبکه هستند با استفاده از فهرست زیر شناسایی شود:

- سطح اعتماد پایین، مانند شبکه‌ای با یک اجتماع ناشناخته از کاربران،
- سطح اعتماد متوسط، مانند شبکه‌ای با یک اجتماع شناخته‌شده از کاربران و در یک جامعه تجاری بسته (در اجتماعی با بیش از یک سازمان)،
- سطح اعتماد بالا، مانند شبکه‌ای با یک جامعه شناخته‌شده از کاربرانی که منحصراً در داخل سازمان هستند.

سپس لازم است محیط (محیط‌های) اعتماد مناسب (با سطح اعتماد پایین، متوسط و بالا) به مشخصات شبکه قابل کاربرد (عمومی یا خصوصی) و نوع (انواع) اتصالات شبکه که در آن موجود هستند، (از A تا G) نسبت داده شوند تا روابط اعتماد ایجاد شود. این عمل با استفاده از ماتریسی که در جدول ۲ در زیر نشان داده شده است، امکان‌پذیر است.

جدول ۲- شناسایی روابط اعتماد

انواع اتصالات شبکه (بند۱۰)		محیط‌های اعتماد		
		سطح پایین	سطح متوسط	سطح بالا
مشخصات شبکه	عمومی	F G	D E	B C
	خصوصی	E	D E	A B C

با استفاده از جدول ۲ لازم است دسته مرجع برای هر یک از روابط اعتماد مربوطه تعیین شود. تمام دسته‌های احتمالی موجود در جدول ۳ در زیر توصیف شده‌اند.

جدول ۳- مراجع روابط اعتماد

دسته روابط اعتماد	توصیف
پایین/ عمومی	اعتماد پایین و استفاده از یک شبکه عمومی.
متوسط/ عمومی	اعتماد متوسط و استفاده از یک شبکه عمومی.
بالا/ عمومی	اعتماد بالا و استفاده از یک شبکه عمومی.
پایین/ خصوصی	اعتماد پایین و استفاده از یک شبکه خصوصی.
متوسط/ خصوصی	اعتماد متوسط و استفاده از یک شبکه خصوصی.
بالا/ خصوصی	اعتماد بالا و استفاده از یک شبکه خصوصی.

لازم است این مراجع در بند۱۲، به‌منظور تایید انواع مخاطرات امنیتی و شناسایی حیطه‌های کنترلی بالقوه، مورد استفاده قرار گیرند.

این وظیفه در صورت‌نیاز می‌تواند از طریق اطلاعات موجود در معماری‌ها و کاربردهای شبکه صورت گیرد (همان‌گونه که با استفاده از بند۹ حاصل شد).

۱۲- شناسایی مخاطرات امنیت اطلاعات

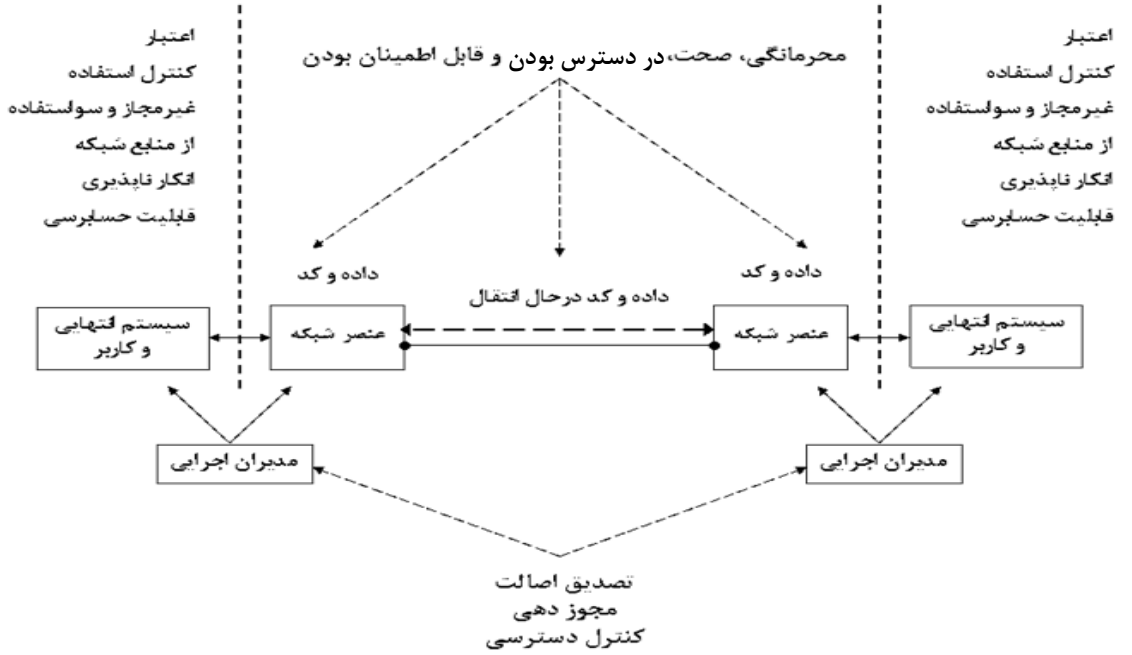
همان‌طورکه پیش از این نیز ذکر شد، امروزه اغلب سازمان‌ها، در انجام فعالیت‌های کسب‌وکار خود، وابسته به استفاده از سامانه‌ها و شبکه‌های اطلاعاتی هستند. علاوه بر این در بسیاری از موارد، یک نیاز کسب‌وکار معین به استفاده از اتصالات شبکه‌ای بین سامانه‌های اطلاعاتی، در هر مکان سازمان و به دیگر مکان‌های داخل یا خارج آن سازمان که شامل/از شبکه عمومی هستند، وجود دارد. در هنگام برقراری اتصال به یک شبکه بایستی دقت کافی مبذول گردد تا از در معرض خطر قرار نگرفتن سازمان در برابر مخاطرات اضافه (تهدیدات بالقوه‌ای که از آسیب‌پذیری‌ها استفاده می‌کنند)، اطمینان حاصل شود. به عنوان مثال این مخاطرات می‌توانند از اتصال به‌تنهایی و یا از اتصالات شبکه در طرف دیگر نتیجه شوند.

برخی از این مخاطرات ممکن است مربوط به الزامات متابعت از قوانین و مقررات باشند. (مقررات مربوط به حریم خصوصی و حفاظت از داده، بایستی مورد ملاحظه دقیق قرار گیرد. برخی از کشورها دارای قوانینی برای اعمال کنترل در زمینه‌های جمع‌آوری، پردازش و انتقال داده‌های شخصی - داده مربوط به یک فرد یا افراد خاص- هستند. بسته به قوانین ملی مربوطه در هرکشور، این قوانین کنترلی وظایفی بر عهده افرادی خاص قرار می‌دهند. این افراد کسانی هستند که از طریق شبکه‌ها به جمع‌آوری، پردازش و ارسال اطلاعات شخصی می‌پردازند و حتی ممکن است به‌منظور اتخاذ ملاحظات امنیتی بیشتر، ظرفیت ارسال داده به کشورهای معینی را محدود کنند. دو مثال نامشهود از داده‌هایی که تحت چنین قوانینی لحاظ می‌شوند، برخی آدرس‌های IP و سخت‌افزاری هستند.)

انواع مخاطراتی که در این بند ذکر شده‌اند، مربوط به دسترسی غیرمجاز به اطلاعات، ارسال غیرمجاز آنها، ورود کدهای مخرب، انسداد دریافت یا منشا، انسداد اتصال سرویس و دسترس‌ناپذیری اطلاعات و سرویس‌ها است. به این ترتیب انواع مخاطرات امنیتی که یک سازمان با آن مواجه خواهد بود، مربوط به از دست رفتن یکی از موارد زیر است:

- محرمانگی اطلاعات و کد (در شبکه‌ها و سامانه‌های متصل به شبکه‌ها)،
- یکپارچگی اطلاعات و کد (در شبکه‌ها و سامانه‌های متصل به شبکه‌ها)،
- دسترس‌پذیری اطلاعات و سرویس‌های شبکه (و سامانه‌های متصل به شبکه‌ها)،
- انکارناپذیری تراکنش‌های شبکه (الزامات)،
- مسئولیت‌پذیری تراکنش‌های شبکه،
- اعتبار اطلاعات (و نیز کاربران و مدیران اجرایی شبکه)،
- قابل اطمینان بودن اطلاعات و کد (در شبکه‌ها و سامانه‌های متصل به شبکه‌ها)،
- قابلیت کنترل استفاده غیرمجاز و سواستفاده از منابع شبکه، که در متون مربوط به خط‌مشی سازمان عنوان شده است (به عنوان مثال فروش پهنای باند و یا استفاده از آن برای مصالح شخصی) و همچنین قابلیت کنترل مسوولیت‌های مرتبط با وضع قوانین و مقررات (به‌عنوان مثال ذخیره تصاویر مستهجن از کودکان)

قابل ذکر است که لزوماً تمامی انواع مخاطرات امنیتی، در هر مکان یا در هر سازمانی وجود ندارند. ولی لازم است کلیه انواع آنها شناسایی شوند تا حیطه‌های کنترلی بالقوه تعیین شوند (و درنهایت کنترل‌ها انتخاب، طراحی، پیاده‌سازی و حفظ شوند). یک مدل مفهومی از امنیت شبکه همراه با مکان‌هایی که در آنها امکان وقوع مخاطرات امنیتی وجود دارد، در شکل زیر نشان داده شده است.



شکل ۳- مدلی مفهومی از نواحی مخاطرات امنیتی شبکه

لازم است اطلاعاتی در مورد عملکردهای کسب‌وکار مرتبط با انواع مخاطرات امنیتی ذکرشده فوق جمع‌آوری شود که این امر با ملاحظه دقیق میزان حساسیت یا ارزش اطلاعات درگیر (که به عنوان تاثیرات بالقوه مخرب کسب‌وکار بیان می‌شود) و نیز تهدیدات و آسیب‌پذیری‌های بالقوه مربوطه امکان‌پذیر خواهد بود. در صورتی‌که بیش از یک اثر مخرب بر عملکردهای کسب‌وکار سازمان وجود داشته باشد، بایستی به ماتریس جدول ۵ رجوع شود.

لازم به تاکید است که در تکمیل این مرحله، بایستی از نتایج حاصل از بازنگری(های)[1] ارزیابی و مدیریت مخاطرات امنیتی، که با ملاحظه اتصال(اتصالات) شبکه حاصل شده است، استفاده شود. این نتایج در هر سطحی از جزییات که بازنگری‌ها انجام شده باشند توجه را به سمت تاثیرات بالقوه مخرب کسب‌وکار و مرتبط با انواع مخاطرات امنیتی ذکرشده فوق و نیز تهدیدات، آسیب‌پذیری‌ها و در نتیجه مخاطرات متناظر جلب می‌کنند.

در هنگام ملاحظه آسیب‌پذیری‌های شبکه ممکن است درطی بازنگری مدیریت و ارزیابی مخاطرات امنیتی، ملاحظه تعدادی از وجوه شبکه به‌طور جداگانه ضروری باشد. در جدول ۴ انواع آسیب‌پذیری‌هایی که در هر وجه شبکه، قابل بهره‌برداری و سواستفاده هستند، فهرست شده است.

جدول ۴- انواع آسیب‌پذیری‌های بالقوه

وجوه شبکه	انواع آسیب‌پذیری‌ها امنیتی بالقوه شبکه				
	وقفه	شنود	تغییر	نفوذ	فریب
کاربران شبکه	ممکن است کاربران، متضرر از دست رفتن یا وقفه در سرویس شوند.	ممکن است تراکنش‌های کاربر و/یا فعالیت شبکه، پایش شود.	ممکن است جزییات کاربر و داده کاربر، تغییر داده‌شده یا خراب شود.	ممکن است کاربران برای دستیابی غیرمجاز به تسهیلات، جعل هویت شوند.	ممکن است هویت کاربران برای تراکنش‌های فریب‌کارانه ، جعل شود.
سامانه‌های انتهایی شبکه	ممکن است سامانه‌های انتهایی به‌طور موقت و یا دایم غیرقابل دسترس باشند.	ممکن است اشخاص غیرمجاز، داده و یا کدهای روی سامانه‌های انتهایی را بخوانند.	ممکن است داده یا کد، تغییرداده‌شده و یا خراب شود.	ممکن است سامانه‌های انتهایی به‌منظور دستیابی غیرمجاز به تسهیلات، جعل‌هویت شوند. اشخاص غیرمجاز می‌توانند به‌منظور اعمال حملات بیشتر، به حساب‌های شخصی دسترسی یافته و از آنها استفاده کنند.	ممکن است هویت سامانه‌های انتهایی برای تراکنش‌های فریب‌کارانه یا اعمال حملات بیشتر، جعل شود.
کاربردهای تحت شبکه	ممکن است کاربردها، به‌طور موقت و یا دایم غیرقابل دسترس باشند.	ممکن است داده و یا کد، توسط اشخاص غیرمجاز، در هنگام انتقال شنود شود و یا روی سرویس‌دهندگان خوانده‌شود.	ممکن است داده یا کد، تغییر داده‌شده و یا خراب شود.	اشخاص غیرمجاز می‌توانند به‌منظور اعمال حملات بیشتر، به حساب‌های سامانه دسترسی یافته و از آنها استفاده کنند.	اشخاص غیرمجاز می‌توانند به‌منظور اعمال حملات بیشتر، به حساب‌های شخصی دسترسی یافته و از آنها استفاده کنند.

[1] راهنمائی‌هایی در مورد دیدگاه‌های مربوط به ارزیابی و مدیریت مخاطرات امنیتی در استاندارد ISO/IEC 17799 ارایه شده است و نیز در استاندارد ISO/IEC 13335-2 پس از انتشار موجود خواهد بود.

سرویس‌های شبکه	ممکن است سرویس‌ها به‌طور موقت و یا دایم، غیرقابل دسترس باشند.	ممکن است داده و یا کد توسط اشخاص غیر مجاز، در هنگام انتقال شنود شود و یا روی سرویس‌دهندگان خوانده‌شود.	ممکن است داده یا کد، تغییر داده‌شده و یا خراب شود.	اشخاص غیرمجاز می‌توانند به‌منظور اعمال حملات بیشتر، به حساب‌های شخصی دسترسی یافته و از آنها استفاده کنند.	ممکن است سرویس‌دهندگان و دستگاه‌های شبکه، به‌منظور دسترسی غیر مجاز، شنود ترافیک شبکه یا قطع کردن سرویس‌های شبکه، جعل هویت شوند.
زیرساخت شبکه	ممکن است تسهیلات به‌طور موقت و یا دایم، غیرقابل دسترس باشند.			ممکن است اشخاص غیر مجاز، تسهیلات شبکه را تحت نفوذ قراردهند.	

با استفاده از نتایج حاصل از بازنگری ارزیابی و مدیریت مخاطرات امنیتی به عنوان یک اصل راهبردی و نیز با استفاده از بند ۱۱، بایستی مراجع روابط اعتماد مربوطه، تعیین شده و در قسمت بالای ماتریس جدول ۵ که در پایین ارائه شده است، جای گیرند. موارد تحت بررسی در قسمت راست جدول قرار می‌گیرد. علاوه بر این لازم است مراجع مرتبط با حیطه‌های کنترلی بالقوه معرفی‌شده در بند۱۳، در زیر و در بندهای مربوطه، ذکر شوند.

جدول ۵- انواع مخاطرات و مراجع امنیتی مرتبط با سطوح نیازمند کنترل

انواع مخاطرات	مراجع روابط اعتماد					
	پایین/ عمومی	متوسط/ عمومی	بالا/ عمومی	پایین/ خصوصی	متوسط/ خصوصی	بالا/ خصوصی
از دست رفتن محرمانگی	۱-۲-۱۳ [1]	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳
	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۸-۲-۱۳
	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۹-۲-۱۳
	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۲-۳-۱۳
	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۳-۳-۱۳
	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۴-۳-۱۳
	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۶-۳-۱۳
	۵-۳-۱۳	۵-۳-۱۳	۵-۳-۱۳	۵-۳-۱۳	۵-۳-۱۳	۷-۳-۱۳
	۶-۳-۱۳	۶-۳-۱۳	۶-۳-۱۳	۶-۳-۱۳	۶-۳-۱۳	۴-۱۳
	۷-۳-۱۳	۷-۳-۱۳	۷-۳-۱۳	۷-۳-۱۳	۷-۳-۱۳	۵-۱۳
	۴-۱۳	۴-۱۳	۴-۱۳	۴-۱۳	۴-۱۳	۲-۶-۱۳
	۵-۱۳	۵-۱۳	۵-۱۳	۵-۱۳	۵-۱۳	۳-۶-۱۳

[1] لازم است تمام ارجاعات به بند ۱۳-۲-۱.در این جدول مورد ملاحظه قرار گیرد. این بند به شیوه‌ای مناسب در سناریوی شبکه‌بندی مورد بحث قابل اعمال است.

	۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵	۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵	۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۶-۵ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵	۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۶-۵ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵	۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵	۱۳-۶-۴ ۱۳-۶-۵ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۲ ۱۳-۱۰-۵
از دست رفتن یکپارچگی	۱۳-۲-۱ ۱۳-۲-۷ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۵ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵	۱۳-۲-۱ ۱۳-۲-۷ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۵ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵	۱۳-۲-۱ ۱۳-۲-۷ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۶-۵ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵	۱۳-۲-۱ ۱۳-۲-۷ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۵ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵	۱۳-۲-۱ ۱۳-۲-۷ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۵ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵	۱۳-۲-۱ ۱۳-۲-۸ ۱۳-۲-۹ ۱۳-۳-۲ ۱۳-۳-۳ ۱۳-۳-۴ ۱۳-۳-۶ ۱۳-۳-۷ ۱۳-۴ ۱۳-۵ ۱۳-۶-۲ ۱۳-۶-۳ ۱۳-۶-۴ ۱۳-۷ ۱۳-۸ ۱۳-۹ ۱۳-۱۰-۳ ۱۳-۱۰-۵

از دست رفتن دسترسی پذیری	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳
	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳
	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳
	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳	۹-۲-۱۳
	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳
	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳
	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳
	۵-۳-۱۳	۵-۳-۱۳	۶-۳-۱۳	۵-۳-۱۳	۵-۳-۱۳	۶-۳-۱۳
	۶-۳-۱۳	۶-۳-۱۳	۷-۳-۱۳	۶-۳-۱۳	۶-۳-۱۳	۷-۳-۱۳
	۷-۳-۱۳	۷-۳-۱۳	۴-۱۳	۷-۳-۱۳	۷-۳-۱۳	۴-۱۳
	۴-۱۳	۴-۱۳	۵-۱۳	۴-۱۳	۴-۱۳	۵-۱۳
	۵-۱۳	۵-۱۳	۲-۶-۱۳	۵-۱۳	۵-۱۳	۲-۶-۱۳
	۲-۶-۱۳	۲-۶-۱۳	۳-۶-۱۳	۲-۶-۱۳	۲-۶-۱۳	۳-۶-۱۳
	۳-۶-۱۳	۳-۶-۱۳	۴-۶-۱۳	۳-۶-۱۳	۳-۶-۱۳	۴-۶-۱۳
	۴-۶-۱۳	۴-۶-۱۳	۵-۶-۱۳	۴-۶-۱۳	۴-۶-۱۳	۷-۱۳
	۷-۱۳	۷-۱۳	۷-۱۳	۷-۱۳	۷-۱۳	۸-۱۳
	۸-۱۳	۸-۱۳	۸-۱۳	۸-۱۳	۸-۱۳	۹-۱۳
	۹-۱۳	۹-۱۳	۹-۱۳	۹-۱۳	۹-۱۳	۱۱-۱۳
	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	
از دست رفتن انکارناپذیری	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳	۱-۲-۱۳
	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳	۷-۲-۱۳
	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳	۸-۲-۱۳
	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳	۲-۳-۱۳
	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳	۳-۳-۱۳
	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳	۴-۳-۱۳
	۵-۳-۱۳	۵-۳-۱۳	۶-۳-۱۳	۵-۳-۱۳	۵-۳-۱۳	۶-۳-۱۳
	۶-۳-۱۳	۶-۳-۱۳	۷-۳-۱۳	۶-۳-۱۳	۶-۳-۱۳	۷-۳-۱۳
	۷-۳-۱۳	۷-۳-۱۳	۴-۱۳	۷-۳-۱۳	۷-۳-۱۳	۴-۱۳
	۴-۱۳	۴-۱۳	۵-۱۳	۴-۱۳	۴-۱۳	۵-۱۳
	۵-۱۳	۵-۱۳	۲-۶-۱۳	۵-۱۳	۵-۱۳	۲-۶-۱۳
	۲-۶-۱۳	۲-۶-۱۳	۳-۶-۱۳	۲-۶-۱۳	۲-۶-۱۳	۳-۶-۱۳
	۳-۶-۱۳	۳-۶-۱۳	۴-۶-۱۳	۳-۶-۱۳	۳-۶-۱۳	۴-۶-۱۳
	۴-۶-۱۳	۴-۶-۱۳	۵-۶-۱۳	۴-۶-۱۳	۴-۶-۱۳	۷-۱۳
	۷-۱۳	۷-۱۳	۷-۱۳	۷-۱۳	۷-۱۳	۸-۱۳
	۸-۱۳	۸-۱۳	۸-۱۳	۸-۱۳	۸-۱۳	۹-۱۳
	۹-۱۳	۹-۱۳	۹-۱۳	۹-۱۳	۹-۱۳	۴-۱۰-۱۳
	۴-۱۰-۱۳	۴-۱۰-۱۳	۴-۱۰-۱۳	۴-۱۰-۱۳	۴-۱۰-۱۳	۱۰-۱۳,۵
	۱۰-۱۳,۵	۱۰-۱۳,۵	۱۰-۱۳,۵	۱۰-۱۳, ۵	۱۰-۱۳,۵	۱۱-۱۳
	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	۱۱-۱۳	

همان‌گونه که از جدول مشخص است، هرچه یک کاربر به میزان بیشتری، قابل اعتماد باشد، اعمال کنترل‌های بیشتری مورد نیاز خواهد بود. دو دلیل برای این موضوع وجود دارد که عبارتند از:

اولاً، تعدادی از فنون کنترلی در استاندارد ISO/IEC 17799 شرح داده شده‌اند (و پس از انتشار استاندارد ISO/IEC 13335-2، ارایه خواهند شد)، که به‌منظور حفاظت از تسهیلات میزبان انتخاب می‌شوند و شامل شناسایی، احراز اصالت و کنترل دسترسی منطقی هستند. در وضعیت‌های با سطح اعتماد پایین، لازم است شدت کنترل‌های مورد نیاز در زمینه‌های شناسایی، احراز اصالت و کنترل دسترسی، بیشتر از وضعیت‌های با سطح اعتماد بالا باشد. درصورتی‌که چنین سطح کنترلی قابل اعمال نباشد، بایستی کنترل‌های اضافی مرتبط با وضعیت، به‌کارگرفته‌شوند. از طرف دیگر در وضعیت‌های با سطح اعتماد پایین‌تر، بایستی تنظیم مجوزها (امتیازات)، به‌گونه‌ای باشد که اطمینان حاصل شود دسترسی تنها به منابع سازگار با مدل اعتماد و الزامات دسترسی مورد نظر، انجام می‌گیرد.

ثانیاً، کاربران قابل اعتماد اغلب مواقع، به اطلاعات و/یا کارکردهای بحرانی‌تر/مهم‌تر دسترسی دارند و این به‌معنای آن است که در چنین حالتی به‌دلیل ارزش منابع در دسترس، نیاز به کنترل‌های اضافه، خواهد بود و اعتماد به کاربران به‌تنهایی کافی نیست.

۱۳- شناسایی حیطه‌های کنترلی بالقوه مناسب

۱۳-۱- پس‌زمینه

لازم است بر اساس نتایج بازنگری ارزیابی و مدیریت مخاطرات و با بهره‌گیری از مراجع تعیین‌شده در بند۱۲، حیطه‌های کنترلی بالقوه از بند۱۳ (و همچنین با استفاده از استاندارد ISO/IEC 17799) تعیین و انتخاب شوند. در استاندارد ISO/IEC 13335-2 پس از انتشار، اطلاعاتی مربوط به این بند ارایه خواهد شد. بند۱۳-۲، جنبه‌های گوناگونی از معماری امنیتی شبکه و حیطه‌های کنترلی بالقوه مرتبط را بیان می‌نماید و در ادامه بندهای۱۳-۳ تا ۱۳-۱۰، دیگر حیطه‌های کنترلی بالقوه را معرفی می‌کنند. در حقیقت، یک راه‌حل امنیتی خاص ممکن است شامل تعدادی از حیطه‌های کنترلی بالقوه بیان‌شده در بندهای ۱۳-۲ تا ۱۳-۱۱ باشد.

تاکید می‌شود که تعدادی از کنترل‌های مرتبط به سامانه‌های اطلاعاتی، مستقل از اینکه این سامانه‌ها دارای اتصالات شبکه باشند، بایستی با استفاده از استاندارد ISO/IEC 17799 انتخاب شوند. استاندارد ISO/IEC13335-2 نیز پس از انتشار، اطلاعاتی را در این زمینه ارایه خواهد کرد.

فهرست کنترل‌های بالقوه‌ی شناخته‌شده در زمینه معماری‌ها و کاربردهای شبکه مربوطه، بایستی مورد بازنگری قرار گیرد و در صورت لزوم، تنظیم شود و به عنوان مبنایی در پیاده‌سازی کنترل‌های امنیتی مورد نیاز (بند۱۴) و نیز در پایش و بازنگری پیاده‌سازی‌ها، استفاده شود (بند ۱۵).

۱۳-۲- معماری امنیت شبکه

۱۳-۲-۱- مقدمه

مستندسازی گزینه‌های ممکن معماری امنیت، ابزاری برای آزمودن راه‌حل‌های مختلف و مبنایی برای ارزیابی بده-بستان[1] فراهم می‌نماید. همچنین راه‌حل موارد مرتبط با محدودیت‌های فنی و تضاد بین نیازهای کسب‌وکاری و امنیتی که در اغلب موارد رخ می‌دهد را تسهیل کند.

در مستندسازی این گزینه‌ها، بایستی هریک از الزامات خط‌مشی امنیتی اطلاعات شرکتی (به بند۸ مراجعه شود)، معماری و کاربردهای شبکه مربوطه (به بند۹ مراجعه شود) و فهرست حیطه‌های کنترلی بالقوه‌ی شناسایی‌شده برطبق بندهای ۱۲ و ۱۳، مورد بررسی دقیق قرار گیرند. در انجام این کار لازم است هریک از معماری‌های امنیتی موجود نیز مورد توجه قرار گیرد. هنگامی‌که این گزینه‌ها به عنوان بخشی از فرایند طراحی معماری فنی، مستندسازی و بازنگری شدند، لازم است یک معماری امنیت برتر، مورد توافق قرار گیرد و در یک سند با نام «مشخصات کنترلی طراحی معماری امنیت فنی» (در توافق با طراحی معماری فنی و برعکس) گردآوری شود. پس از آن ممکن است نیاز به تغییراتی در معماری‌ها و کاربردهای شبکه (برای حصول اطمینان از سازگاری با معماری امنیت برتر) و/یا در فهرست کنترل‌های بالقوه (به‌عنوان مثال، به دلیل توافق بر اینکه معماری امنیت بایستی به‌طور فنی با یک روش خاص، قابل پیاده‌سازی باشد، اعمال مکرر یک کنترل شناخته‌شده، ضروری است) باشد.

قابل ذکر است که استاندارد ISO/IEC 18028-2، یک معماری امنیت مرجع[2] بسیار مفید را توصیف می‌کند که می‌توان از آن به عنوان مبنایی، در هر یک از موارد زیر استفاده نمود:

- توصیف یک چارچوب محکم برای پشتیبانی از برنامه‌ریزی، طراحی و پیاده‌سازی امنیت شبکه،
- تعریف اجزای عمومی معماری‌گونه مرتبط با امنیت که در صورت استفاده درست، یک امنیت شبکه‌ای انتها به انتها را فراهم می‌کنند.

بر پایه این معماری امنیت مرجع، توصیفاتی از معماری‌های امنیتی فنی و متفاوت جهان واقع که برای بیان الزامات امروزی و نیز آینده نزدیک، مورد نیاز هستند، در این استاندارد ارایه شده است و با جزییات بیشتر در استانداردهای ISO/IEC 18028-3 تا ISO/IEC 18028-5، به آن پرداخته خواهد شد.

اصول شرح داده شده در معماری امنیت مرجع، برای هر نوع شبکه‌بندی جدید اعم از شبکه‌های داده، صوت و شبکه‌های همگرای بی‌سیم یا رادیو، قابل استفاده است و می‌تواند مستقل از فناوری شبکه و یا موقعیت در پشته پروتکل، به‌کار رود. این معماری، موارد کلیدی امنیتی مرتبط با مدیریت، کنترل و همچنین استفاده از زیرساخت، سرویس‌ها و کاربردهای شبکه را بیان می‌کند و یک چشم‌انداز انتها به انتها، بالا به پایین و جامع از امنیت شبکه را ارایه می‌نماید.

معماری امنیت "مرجع" دارای سه مولفه است:

---

[1] Trade Off

[2] در متن قسمت ۲، « مرجع» به عنوان یک مثال برای شرح این به کار می‌رود که چگونه معماری امنیت فنی در یک سطح خیلی بالا معرفی می‌شود. البته ممکن است مثال‌های دیگری نیز وجود داشته‌باشد.

- ابعاد امنیتی (با عنوان "گروه‌های کنترلی امنیت" نیز شناخته می‌شوند)،
- لایه‌های امنیتی (با عنوان "اجزاء امنیت شبکه" نیز شناخته می‌شوند)،
- سطوح امنیتی (با نام "حوزه‌های امنیتی" نیز شناخته می‌شوند).

ابعاد امنیتی مجموعه‌ای از کنترل‌های امنیتی هستند که هر کدام برای مشخص کردن جنبه خاصی از امنیت شبکه، طراحی شده‌اند. در مجموع هشت بعد امنیتی در معماری "مرجع" توصیف شده است که قابل توسعه به کاربردها و اطلاعات کاربر انتهایی است، به‌عنوان مثال:

- انکارناپذیری،
- محرمانگی داده،
- یکپارچگی داده،
- دسترس‌پذیری.

لازم است به‌منظور ارایه یک راه‌حل امنیتی انتها به انتها، ابعاد امنیتی به سلسله مراتبی از گروه‌های تجهیزات شبکه و گروه‌بندی تسهیلات شبکه اعمال شوند. این سلسله مراتب با عنوان "لایه‌های امنیتی"، شناخته می‌شوند که عبارتند از:

- لایه امنیتی زیرساخت،
- لایه امنیتی سرویس‌ها،
- لایه امنیتی کاربردها.

لایه‌های امنیتی بر روی یکدیگر بنا می‌شوند تا راه‌حل‌های مبتنی بر شبکه را ارایه دهند، بدین معنا که لایه زیرساخت، تسهیلاتی برای لایه امنیتی سرویس‌ها و لایه امنیتی سرویس‌ها، تسهیلاتی برای لایه امنیتی کاربرد فراهم می‌کند و با ارایه یک نمای ترتیبی از امنیت شبکه، بخش‌هایی از محصولات و راه‌حل‌ها را که برقراری امنیت در آنها مورد نیاز است، مشخص می‌نماید.

لایه امنیتی زیرساخت، شامل تسهیلات انتقال شبکه و نیز بخش‌های مجزای شبکه است که توسط سازوکارهای مربوط به ابعاد امنیتی، حفاظت می‌شوند. چند نمونه از مولفه‌های متعلق به لایه امنیتی زیرساخت شامل مسیریاب‌های مجزا، سوده‌ها و سرویس‌دهندگان و نیز پیوندهای ارتباطی بین مسیریاب‌های مجزا، سوده‌ها و سرویس‌دهندگان است.

لایه امنیتی سرویس‌ها بیانگر امنیت سرویس‌هایی است که ارایه‌دهندگان سرویس، برای مشتریان خود فراهم می‌کنند. این سرویس‌ها از سرویس‌های انتقال پایه و اتصال به فعال‌کنندگان سرویس‌ها مانند سرویس‌هایی که برای ایجاد دسترسی به اینترنت ضروری هستند (به عنوان مثال سرویس‌هایی اعم از سرویس‌های احراز اصالت، مجوزدهی و سرویس‌های مسئولیت‌پذیری، سرویس‌های پیکربندی پویای میزبان[1]، سرویس‌های پویای نام‌دهی حوزه) تا سرویس‌های ارزش افزوده اعم از سرویس تلفنی رایگان، کیفیت سرویس‌دهی، شبکه VPN را در برمی‌گیرند.

[1] Dynamic Host Configuration Sevices , DHCS

لایه امنیتی کاربردها، بر امنیت کاربردهای مبتنی بر شبکه که توسط مشتریان ارایه‌دهندگان سرویس قابل دسترسی هستند، متمرکز است. این کاربردها به وسیله سرویس‌های شبکه، فعال می‌شوند و شامل انتقال فایل اصلی (مانند FTP)، کاربردهای مرورگر وب، کاربردهای زیربنایی نظیر فهرست‌یار، پیام‌رسانی صوتی مبتنی بر شبکه و پست الکترونیکی و نیز کاربردهای پیشرفته اعم از مدیریت ارتباط با مشتری، کسب‌وکار سیار/الکترونیکی، آموزش مبتنی بر شبکه، تعامل تصویری هستند.

سطوح امنیتی در حقیقت انواع خاصی از فعالیت‌های شبکه‌اند که توسط سازوکارهای پیاده‌سازی شده برای ابعاد امنیتی، محافظت می‌شوند. معماری امنیت "مرجع"، سه سطح امنیتی را به‌منظور معرفی انواع فعالیت‌های حفاظت شده در یک شبکه، تعیین می‌کند. این سطوح عبارتند از:

- سطح مدیریت،
- سطح کنترل،
- سطح کاربر انتهایی.

سطوح امنیتی فوق به‌ترتیب، به الزامات خاص امنیتی مرتبط با فعالیت‌های مدیریتی شبکه، فعالیت‌های سیگنالینگ و کنترل شبکه و فعالیت‌های کاربر انتهایی اشاره می‌کنند. شبکه‌ها باید به گونه‌ای طراحی شوند، که رویدادهای مربوط به یک سطح امنیتی، تا حد ممکن و به طور مناسب از دیگر سطوح امنیتی مجزا باشد.

بندهای زیر، به ارایه یک معرفی از جنبه‌های فنی متفاوت معماری امنیت و واقعی مربوط به نواحی گوناگون شبکه‌بندی می‌پردازد.

تاکید می‌شود که برای هر پروژه بایستی معماری امنیت فنی، قبل از اتمام فهرست کنترل‌های لازم برای پیاده‌سازی، به طور کامل مستندسازی شده و مورد توافق قرار گیرد.

۱۳-۲-۲- شبکه‌بندی محلی

۱۳-۲-۲-۱ پس‌زمینه

هنگامی‌که شبکه‌های LAN، در نواحی حفاظت‌شده فیزیکی، به عنوان مثال، در ناحیه تحت تملک یک سازمان استفاده می‌شوند، مخاطرات به‌گونه‌ای هستند که تنها فنون کنترلی فنی پایه، مورد نیاز خواهد بود. درهرحال برای استفاده این شبکه‌ها در محیط‌های بزرگتر و نیز هنگامی‌که از فناوری‌های بی‌سیم، استفاده می‌شود (به بند۱۳-۲-۴ مراجعه شود)، لزوماً حفاظت فیزیکی، به‌تنهایی هیچ سطحی از امنیت را تضمین نمی‌کند. به‌علاوه، فناوری‌های رسانه به اشتراک گذاشته‌شده که به طورگسترده در شبکه‌های LAN به کار می‌روند، از هر سامانه‌ای‌که از رسانه مشترک استفاده می‌کند، اجازه دسترسی به تمام ترافیک شبکه را می‌دهند.

میزکار به‌دلیل اینکه واسط کاربر است، یک ناحیه آسیب‌پذیر به شمار می‌رود. اگر میزکار قفل نشده باشد، نصب نرم‌افزار غیرمجاز بر روی شبکه محلی توسط یک کاربر امکان‌پذیر خواهد بود. سامانه‌های سرویس‌دهنده‌ای که در یک شبکه سازمانی به‌کار می‌روند، چه سامانه‌های در معرض اینترنت و چه سرویس‌دهندگان داخلی که به‌طور مستقیم به اینترنت متصل نیستند، یک مخاطره امنیتی اصلی بالقوه

به‌حساب می‌آیند. با اینکه اغلب ادارات IT مدعی هستند که وصله‌های لازم را به محض دسترس‌پذیری، به کار خواهند برد، به دلیل این‌که حتی برخی از سازمان‌های بزرگ در اضافه نمودن وصله‌ها به تمام سرویس‌دهندگان شکست خورده‌اند و این امر موجب قطع ترافیک شبکه داخلی توسط کرم‌ها شده است، لازم است این مخاطره به‌طور جدی مورد توجه قرار گیرد.

۱۳-۲-۲-۲ مخاطرات امنیتی

مخاطرات امنیتی در یک شبکه محلی باسیم، از گره‌هایی که به طور فیزیکی به شبکه متصل هستند، ناشی می‌شود. در مجموع مخاطرات امنیتی کلیدی مربوط با شبکه‌های LAN شامل موارد زیر هستند:

- دسترسی و تغییرات غیرمجاز روی میزکار PCها، سرویس‌دهندگان و دیگر دستگاه‌های متصل به شبکه محلی،
- سرویس‌دهندگان فاقد وصله[1]،
- کلمه‌های عبور با کیفیت پایین،
- سرقت سخت‌افزار،
- خرابی منابع تغذیه،
- وارد کردن کد مخرب از طریق پست الکترونیکی و دسترسی به وب،
- خرابی در پشتیبان‌گیری دیسک‌های سخت محلی،
- خرابی سخت‌افزارهایی چون دیسک‌های سخت،
- اتصالات غیرمجاز به شبکه محلی (رایانه‌های دستی)،
- دسترسی غیرمجاز به محفظه‌های هاب‌ها و وصله‌ها،
- کلمه‌های عبور پیش‌فرض روی درگاه‌های مدیریتی هاب‌ها و سوده‌ها،
- امنیت فیزیکی ضعیف.

۱۳-۲-۲-۳ کنترل‌ها

امن نگهداشتن فضای شبکه محلی، مستلزم امن بودن مولفه‌های شبکه محلی و نیز دستگاه‌های متصل به آن است. کنترل‌های لازم به‌منظور امن کردن محیط یک شبکه محلی می‌تواند شامل موارد زیر باشد:

- فیزیکی و محیطی
  - استفاده از "سامانه‌های کابل فولادی"[2] برای حفاظت از CPU[3]ها، نمایشگرها و صفحات کلید در برابر سرقت،
  - استفاده از قفل‌های سخت‌افزاری روی دستگاه‌ها، برای پیش‌گیری از سرقت قسمت‌هایی همچون حافظه،

[1] Patches
[2] Steel Cable System
[3] Central Process Units

- استفاده از دستگاه‌های نگهدارنده[1] به‌منظور پیش‌گیری از برداشت غیرمجاز از سایت،
- حصول اطمینان از اینکه هاب‌ها و مسیریاب‌های شبکه محلی، در جعبه‌های امن فیزیکی و در فضاهای ارتباطی امن، نگهداری می‌شوند،
- استفاده از UPS با امکان خاموش شدن خودکار، برای دستگاه‌های مهم و PCهای کاربرانی که نمی‌خواهند استمرار فعالیت آنها دچار مشکل شود.

– سخت‌افزاری و نرم‌افزاری:

- پیکربندی دستگاه‌ها با آدرس‌های IP خصوصی،
- خط‌مشی رمزعبور قوی،
- الزام استفاده از حداقل یک جفت شناسه کاربر و رمزعبور، به‌منظور ورود در هر ایستگاه کاری،
- نصب نرم‌افزار ضدویروس و به‌روز کردن خودکار و منظم نرم‌افزار،
- اعمال تنظیمات رجیستری امن،
- غیرفعال کردن فلاپی دیسک، CD-ROM و درگاه‌های USB،
- آینه‌کردن درایوهای سرویس‌دهنده (یا استفاده از RAID) به‌منظور افزونگی،
- حذف نرم‌افزارهای غیرلازم.

– عملیاتی:

- مستندسازی نرم‌افزار و تنظیمات امنیتی به‌منظور استفاده‌های آتی در پیکربندی ایستگاه‌های کاری جدید،
- زمان‌بندی کردن بارگیری و نصب دوره‌ای وصله‌ها سیستم‌های عامل،
- ساختن و نگهداری آخرین دیسک‌های تعمیر اضطراری[2] و ذخیره آنها در یک محل کنترل‌شده،
- پیاده‌سازی سامانه ثبت برای ثبت مشکلات مربوط به پشتیبانی و سواستفاده از ایستگاه‌های کاری،
- بایگانی کردن تمام اسناد مربوط به ایستگاه‌های کاری (کاغذها/ راهنماها/ دیسک‌ها)، برای استفاده توسط متخصصان سرویس،
- حصول اطمینان از وجود یک نظام پشتیبان‌گیری،
- حصول اطمینان از اینکه هاب‌ها و سوده‌ها دارای قابلیت تغییر کلمه‌های عبور، به‌طور پیش‌فرض، هستند،
- اعمال رشته‌های گروه/ کلمه‌های عبور مناسب برای پروتکل مدیریت شبکه،
- پیکربندی صحیح ثبت‌های ممیزی، در صورت وجود و پیاده‌سازی فرایندهایی برای پایش ثبت‌های ممیزی،

---

[1] Proximity Devices
[2] Emergency Repair Disks

- زمان‌بندی کردن به‌روز رسانی‌های دوره‌ای سفت‌افزار[1]
- طبق جدول زمانی،
- مستندسازی تنظیمات مربوط به تجهیزات، برای استفاده در پیکربندی مجدد آنها؛ گرفتن کپی پشتیبان از فایل پیکربندی مسیریاب‌ها و ذخیره آن در یک محل امن،
- بررسی کلیه دستگاه‌های متصل به شبکه محلی، به‌منظور شناخت آسیب‌پذیری‌ها.

۱۳-۲-۳- شبکه گسترده

۱۳-۲-۳-۱ پس‌زمینه

شبکه WAN مرسوم، اساساً با استفاده از برقراری پیوندهای ثابت بین محل‌های اجاره‌شده از ارایه‌کنندگان سرویس به‌وجود آمد، به‌طوری‌که ارایه‌کننده سرویس دارای کمترین فعالیت مدیریتی بر روی این پیوندها بود، درعین‌حال عملیاتی بودن پیوندها را تضمین می‌کرد. درهرحال پیشرفت فناوری‌های به‌کار گرفته شده در WAN، موجب واگذاری مسولیت مدیریت به‌سوی ارایه‌کنندگان سرویس شده است، با این مزیت که از آن پس، یک سازمان ملزم به توسعه و مدیریت شبکه خود نبود. به این معنا که حصول اطمینان از امن بودن تسهیلات مدیریت شبکه، برعهده ارایه‌کنندگان سرویس است. علاوه بر این، با توجه به اینکه یک WAN به‌طورعمده، برای مسیریابی ترافیک شبکه در فواصل طولانی استفاده می‌شود، لازم است عمل مسیریابی به طور مناسب امن شود، به‌طوری‌که اطمینان حاصل شود، ترافیک شبکه به یک شبکه محلی نادرست، هدایت نخواهد شد. به‌این ترتیب، ترافیکی که در طول یک WAN حرکت می‌کند، برای تمام کسانی که به زیرساخت این شبکه دسترسی دارند، قابل شنود خواهد بود. از آنجایی‌که دسترس‌پذیری به زیرساخت در WAN نسبت به شبکه محلی بیشتر است، لازم است نسبت به رمزنگاری اطلاعات مهم و حساسی که در محیط یک WAN منتقل می‌شوند، دقت کافی مبذول گردد. همچنین بایستی ارایه‌کنندگان سرویس، ملزم به برآوردن سطح امنیتی مورد درخواست یک سازمان شود.

۱۳-۲-۳-۲ مخاطرات امنیتی

در حالی‌که یک WAN باسیم دارای مخاطرات امنیتی اولیه مشترکی با یک شبکه محلی باسیم است (به بند۱۳-۲-۲ مراجعه شود)، ولی با توجه به‌اینکه یک WAN در معرض ترافیک بیشتری است، با مخاطرات امنیتی بیشتری روبرو خواهد بود. بنابراین لازم است کنترل‌هایی، شامل کنترل روی دسترسی، اعمال شود به‌گونه‌ای که اطمینان حاصل شود، WAN باسیم، به آسانی در معرض مخاطراتی که موجب خرابی‌های وسیع می‌شود، قرار نمی‌گیرد. به طور مشابه، با این‌که یک WAN بی‌سیم دارای مخاطرات امنیتی اولیه مشترکی با WLAN است (به بند۱۳-۲-۲ مراجعه شود)، ولی به علت امکان تداخل در سامانه‌هایی که برای انتقال بسته‌های شبکه استفاده شده‌اند، میزان خرابی نیز بالاتر خواهدبود. به‌طورکلی مخاطرات کلیدی مرتبط با WAN، شامل موارد زیر است:

[1] Firmware

- نفوذ، هنگامی‌که اطلاعات فاش شوند یا یکپارچگی داده قابل تضمین نباشد،
- حملات DoS، زمانی است که منابع برای کاربران مجاز، غیر قابل دسترسی شوند،
- اتصال شخص ثالث و حساب‌های شماره‌گیری اینترنتی برای استفاده شخصی در خانه که اغلب مواقع به راحتی، امکان کنار زدن و خنثی کردن کنترل‌های پیاده‌سازی در سطح شبکه و سرویس‌دهنده وجود دارد و منجر به درمعرض قرارگرفتن شبکه سازمان دربرابر کرم‌ها، اسب‌های تراوا و ویروس‌ها می‌شود،
- تاخیر بیش از حد که سرویس‌های صوت مبتنی بر IP را تحت‌تاثیر قرار می‌دهد،
- لغزش روی شبکه که کیفیت صوت را تحت‌تاثیر قرار خواهد داد (لغزش به‌طورعمده از طریق استفاده از کابل‌های مسی‌که برای تحویل سرویس به‌کار می‌روند، ایجاد می‌شود)،
- خرابی دستگاه،
- خرابی کابل،
- دستگاه‌های فاقد وصله،
- از دست رفتن انرژی در یک سایت اصلی که قسمت‌های زیاد دیگری را تحت‌تاثیر قرار می‌دهد،
- تسهیلات مدیریتی شبکه ارایه‌کنندگان سرویس.

۱۳-۲-۳-۳ کنترل‌ها

کنترل‌های امنیتی کلیدی مورد نیاز برای امن کردن یک WAN، شامل موارد زیر است:

- جایگزینی پروتکل‌هایی که ذاتاً ناامن هستند مثل Telnet و FTP با پروتکل‌های امن نظیر SSH و SCP،
- رمزنگاری ارتباطات مدیریتی،
- پیاده‌سازی احراز اصالت امن به‌منظور دسترسی به دستگاه‌های WAN، همراه با هشداردهی مناسب دستگاه‌ها، با استفاده از گزارش‌دهی SNMP،
- امن کردن تجهیزات فیزیکی WAN در هر سایت، نظیر استفاده از محفظه‌های قفل‌شده با امکان هشداردهی دسترسی،
- استفاده از UPS برای حصول اطمینان در مقابل بروز وقفه منابع تغذیه،
- سایت‌های اتصال دوگانه که از مسیرهای متفاوت استفاده می‌کنند،
- سرکشی فعالانه از دستگاه‌های WAN،
- نگاشت دستگاه‌های شبکه به‌منظور شناسایی دستگاه‌های غیرمجاز،
- تسهیلات مدیریت وصله،
- استفاده از پوشش رمزنگاری برای داده‌های حساس،
- اخذ تضمین سرویس از ارایه‌کنندگان سرویس، برای مواردی همچون تاخیر و لرزش،
- پیاده‌سازی ممیزی و حسابرسی برای دسترسی به دستگاه‌های WAN،
- استفاده از دیواره‌های آتش که ترافیک‌های غیرمنتظره به داخل شبکه را دور بیندازند،

- حصول اطمینان از مخفی بودن ساختار MPLS و آدرس‌ها،
- اختصاص آدرس‌های IP غیرقابل مسیریابی در اینترنت،
- استفاده از ترجمه آدرس‌های شبکه که آدرس‌های داخلی IP را مخفی می‌کند، ولی به دستگاه‌های با آدرس‌های غیر قابل مسیریابی اجازه درخواست از اینترنت را می‌دهد،
- استفاده از نرم‌افزارهای ضد ویروس به‌منظور ممانعت از اینکه کدهای مخرب، نظیر اسب‌های تراوا، ویروس‌ها و کرم‌ها، روزنه‌های امنیتی را از داخل یک شبکه باز کنند،
- استفاده از IDS برای شناسایی ترافیک مشکوک،
- حصول اطمینان از اینکه سامانه‌های مدیریتی شبکه به‌طور منطقی امن شده‌اند،
- حصول اطمینان از اینکه مکان‌های مدیریتی شبکه به‌طور فیزیکی امن شده‌اند،
- حصول اطمینان از اینکه دستگاه‌ها پشتیبان‌گیری شده‌اند،
- بررسی قابلیت اطمینان کارمندان مدیریت شبکه.

۱۳-۲-۴- شبکه‌های بی‌سیم

۱۳-۲-۴-۱ پس‌زمینه

شبکه‌های بی‌سیم شبکه‌هایی هستند که نواحی جغرافیایی کوچک را تحت پوشش قرار می‌دهند و از ابزارهای ارتباطی بی‌سیم، نظیر امواج رادیویی یا مادون قرمز، استفاده می‌کنند. نوعاً شبکه‌های بی‌سیم به‌منظور پیاده‌سازی اتصالات معادل که در شبکه‌های LAN وجود دارند، استفاده می‌شوند و به همین دلیل WLAN نامیده می‌شوند. فناوری‌های اصلی به‌کار گرفته شده در این شبکه‌ها، استاندارد IEEE 802.11 و Bluetooth می‌باشند. تاکید می‌شود که شبکه‌های بی‌سیم، دسته متفاوتی از شبکه‌های رادیویی را همچون GSM، 3G و VHF تشکیل می‌دهند که این شبکه‌ها از دکل‌های آنتن هوایی برای انتقال استفاده می‌کنند، (به بند۱۳-۲-۵ مراجعه شود).

WLANها متحمل انواع آسیب‌پذیری‌های خاص مرتبط با LANهای باسیم و به‌علاوه آسیب‌پذیری‌های خاص مرتبط با مشخصات ارتباط بی‌سیم هستند. برخی از فناوری‌های خاص (که عمدتاً مبتنی بر رمزنگاری هستند)، به‌منظور تشخیص این آسیب‌پذیری‌های اضافی، توسعه یافته‌اند، اگرچه نسخه‌های قبلی این فناوری‌ها (مانند WEP) دارای ضعف‌های معماری‌گونه هستند و قادر به برآوردن انتظارات موجود در زمینه محرمانگی نیستند.

۱۳-۲-۴-۲ مخاطرات امنیتی

نواحی کلیدی مخاطرات امنیتی که مربوط به استفاده از WLANها هستند، شامل موارد زیر می باشند:

- شنود،
- دسترسی غیرمجاز،

- تداخل[1] و اختلال[2]،
- پیکربندی نادرست،
- غیرفعال‌کردن حالت دسترسی امن به‌طور پیش‌فرض،
- نسخه معیوبWEP یا TKIP،
- استفاده از نسخه معیوب SNMP برای مدیریت WLAN،
- عدم امکان مشاهده همیشگی استفاده‌کنندگان از WLAN.

۱۳-۲-۴-۳ کنترل‌ها

کنترل‌های مورد نیاز در WLANها شامل موارد زیر است:

- به‌کارگیری دیواره‌آتش بین WLAN و زیرساخت سازمان،
- پیاده‌سازی یک VPN مبتنی بر IPsec بر روی WLAN، بین سرویس‌گیرنده و یک دیواره‌آتش محیطی،
- ارتقای امنیت هر دستگاه در WLAN، از طریق پیکربندی دیواره‌های آتش شخصی، تشخیص نفوذ و نرم‌افزار ضد ویروس روی دستگاه سرویس‌گیرنده،
- کنترل سطوح انتقال به‌منظور حذف هرگونه انتشار به خارج از حوزه فیزیکی سازمان،
- پیکربندی SNMP به‌صورت دسترسی فقط خواندنی،
- مدیریت رمزنگاری خارج از محدوده[3]، به عنوان مثال استفاده از SSH،
- حفظ امنیت فیزیکی در نقاط دسترسی بی‌سیم،
- مقاوم‌سازی کلیه اجزاء سرویس‌دهنده،
- آزمایش سامانه،
- توسعه یک IDS بین شبکه سازمانی و شبکه بی‌سیم.

۱۳-۲-۵- شبکه‌های رادیویی

۱۳-۲-۵-۱ پس‌زمینه

شبکه‌های رادیویی، شبکه‌هایی هستند که از امواج رادیویی به عنوان یک واسط برای پوشش جغرافیایی نواحی وسیع استفاده می‌کنند. نمونه‌های نوعی از این شبکه‌ها، شبکه‌های تلفن سیار هستند که از فناوری‌هایی نظیر GSM یا UMTS استفاده می‌کنند و سرویس‌های داده و صوت قابل دسترس عمومی را ارایه می‌نمایند.

تاکید می‌شود که شبکه‌هایی که از امواج رادیویی برای پوشش نواحی کوچک استفاده می‌کنند، در دسته‌ای متفاوت مورد بحث قرار می‌گیرند و در بند۱۳-۲-۴ شرح داده می‌شوند.

---

[1] Interference
[2] Jamming
[3] Out Of Band

نمونه‌هایی از شبکه‌های رادیویی به‌صورت زیر هستند:

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

۱۳-۲-۵-۲ مخاطرات امنیتی

سناریوهای تهدید امنیتی عمومی که می‌توانند منجر به اعمال مخاطرات روی شبکه‌های رادیویی شوند، شامل موارد زیر هستند:

- استراق سمع،
- ربایش جلسه،
- جعل هویت،
- تهدیدات سطح کاربرد، به‌عنوان مثال تقلب[1]،
- DoS.

مثال‌هایی از مخاطرات مرتبط با برخی از انواع شبکه‌های رادیویی در پاراگراف‌های زیر ارایه شده است.

مخاطرات امنیتی متناظر با GSM حقایق زیر را دربرمی‌گیرد:

- الگوریتم‌های A5/x و Comp128-1 ضعیف هستند،
- عموماً رمزنگاری GSM غیرفعال است،
- همانندسازی SIM، یک واقعیت است.

مخاطرات امنیتی مرتبط با شبکه‌های سیار 3G، شامل این واقعیت‌ها هستند که:

- تلفن‌ها در معرض حملات الکترونیکی، شامل درج کدهای مخرب، نظیر ویروس‌ها هستند،
- فرصت‌های وقوع حملات بالا است به این دلیل که تلفن‌ها اغلب فعال هستند،
- سرویس‌ها می‌توانند مورد استراق سمع قرار گیرند،
- شبکه‌های رادیویی می‌توانند دچار ازدحام شوند،
- تعبیه ایستگاه‌های پایه قلابی امکان‌پذیر است،
- دروازه‌ها می‌توانند هدف دسترسی غیرمجاز باشند،
- سرویس می‌تواند هدف حمله و دسترسی غیرمجاز از طریق اینترنت قرار بگیرد،
- نفوذ هرزنامه امکان‌پذیر است،
- سامانه‌های مدیریتی می‌توانند هدف دسترسی غیرمجاز از طریق RAS باشند،

[1] Fraud

- سرویس می‌تواند به‌واسطه از دست‌دادن یا سرقت تجهیزات پشتیبانی مهندسی شامل رایانه‌های دستی، مورد حمله قرار گیرد.

شبکه UMTS یک عضو اصلی خانواده جهانی فناوری سیار 3G محسوب می‌شود و ظرفیت قابل توجه و قابلیت‌های باند وسیعی را به منظور پشتیبانی تعداد بیشتری از مشتریان داده و صوت، ارایه می‌دهد. این سامانه از پهنای کانال حامل ۵ MHz برای ارایه نرخ‌های ارسال داده بالاتر و ظرفیت افزوده استفاده می‌کند، که موجب فراهم شدن استفاده بهینه از منابع رادیویی، به‌ویژه برای اپراتورهایی که صاحب‌امتیاز بلوک‌های پیوسته و بزرگی از طیف هستند- بطور معمول در محدوده‌ای از 2×10 MHz تا 2×20 MHz- به‌منظور کاهش هزینه گسترش شبکه‌های 3G می‌شود.

GPRS با ارتقاء قابلیت کارکردهای شبکه GSM، یک گام اولیه ضروری برای تحقق شبکه‌های سیار 3G محسوب می‌شود. GPRS یک مشخصه برای انتقال داده روی شبکه‌های GSM به شمار می‌آید که به هر دو ترافیک سودهی مداری و بسته‌ای، اجازه حضور در زیرساخت GSM را می‌دهد. GPRS، تا هشت عدد شیار زمانی TDMA، 9.05Kb یا 13.4Kb را برای پهنای باند کلی 72.4Kb یا 107.2Kb مورد استفاده قرار می‌دهد. شبکه GPRS از هر دو نوع ارتباطات TCP/IP و X. 25، پشتیبانی می‌کند. شبکه‌های EDGE قادر به پیاده‌سازی EGPRS، که پهنای باند هر شیار زمانی را به 60Kb افزایش می‌دهد، هستند. شبکه GPRS، یک اتصال اینترنتی "همیشه فعال" را برقرار می‌کند که این امر یک مساله امنیتی بالقوه است. یک تامین‌کننده شبکه GPRS، معمولاً تلاش می‌کند که با تامین دیواره‌های آتش بین شبکه GPRS و اینترنت، سطح امنیتی اتصال را ارتقاء دهد، اما پیکربندی دیواره آتش می‌بایست به‌گونه‌ای باشد که به سرویس‌های معتبر اجازه کار دهد و بنابراین ممکن است توسط اشخاص ثالث مورد سواستفاده قرار گیرد.

CDPD، یک مشخصه برای پشتیبانی دسترسی بی‌سیم به اینترنت و شبکه‌های سودهی بسته عمومی دیگر روی شبکه‌های تلفنی سلولی، محسوب می‌شود. CDPD، TCP/IP و پروتکل شبکه بی‌سیم را پشتیبانی می‌کند. CDPD، از رمز دنباله‌ای RC4 با کلیدهای۴۰ بیتی برای رمزنگاری استفاده می‌کند. CDPD، در استاندارد IS-732 بیان شده است. الگوریتم مورد استفاده قوی نیست و می‌تواند توسط یک حمله جستجوی جامع[1] شود.

CDMA، شکلی از طیف گسترده، خانواده‌ای از فناوری‌های ارتباطی دیجیتال است که در طول سال‌ها مورد استفاده قرار گرفته‌است. اصل اساسی طیف‌گسترده بر مبنای استفاده از امواج حامل شبه‌نویز استوار است، که پهنای باندی بسیار وسیع‌تر از آنچه که برای ارتباطات نقطه به نقطه و برای همان نرخ داده مورد نیاز است، دارد. فناوری کدینگ دیجیتال، به CDMA، اجازه ممانعت از استراق سمع، در هر دو حالت عمدی و سهوی را می‌دهد. فناوری CDMA، صوت را به قطعات کوچک می‌شکند که روی طیف گسترده‌ای از فرکانس‌ها سیر می‌کند. هر قطعه کوچک مکالمه (یا داده) با یک کد دیجیتال که تنها برای تلفن‌های CDMA و ایستگاه پایه معلوم است، شناسایی می‌شود. این بدین معنا است که به‌طور مجازی هیچ دستگاه

[1] Brute Force

دیگری قادر به دریافت مکالمه نیست. از آنجا که میلیون‌ها ترکیب کد برای هر مکالمه‌ای در دسترس است، این خاصیت می‌تواند از استراق سمع جلوگیری کند.

۱۳-۲-۵-۳ کنترل‌های امنیتی

تعدادی کنترل امنیتی فنی برای مدیریت مخاطرات ناشی از تهدیدهای شناخته‌شده شبکه‌های رادیویی وجود دارند، که شامل موارد زیر می‌باشند:

- احراز اصالت امن،
- رمزنگاری با استفاده از الگوریتم‌های موثر،
- ایستگاه‌های پایه حفاظت شده،
- دیواره‌های آتش،
- حفاظت در مقابل کدهای مخرب (ویروس، اسب تراوا و غیره)،
- ضد هرزنامه.

۱۳-۲-۶- شبکه‌بندی پهن‌باند

۱۳-۲-۶-۱ پس‌زمینه

شبکه‌بندی پهن‌باند گروهی از فناوری‌ها است که به تک‌تک مشترکین امکان دسترسی پرسرعت به نقطه دست‌یابی به اینترنت[1] را فراهم می‌کند. در حال حاضر چهار فناوری اصلی موجود هستند:

- 3G،
- کابل،
- ماهواره،
- DSL.

دو نوع اصلی DSL وجود دارند: نوع غیرمتقارن که در آن سرعت بارگذاری فایل از کاربر، کمتر است (بین یک‌چهارم تا نصف سرعت بارگیری فایل) و نوع متقارن که در آن سرعت‌های بارگیری و بارگذاری فایل یکسان هستند. در هر دو مورد سرعت بارگیری فایل، به طور معمول بین ۱۲۸ Kb/s تا ۸-۲ Mb/s ، بر حسب محصول تغییر می‌کند. فناوری‌های کابل و ماهواره نیز محصولات مشابهی را دارند.

دلیل اصلی اتخاذ فناوری‌های پهن‌باند، سرعت بالا و دسترسی‌پذیری دایمی و ارزان آنها در مقایسه با ارتباطات مرسوم است. تمام فناوری‌ها اجازه دسترسی به اینترنت را می‌دهند و بنابراین بین اینترنت و ناحیه تعهدشده توسط مشترکین قرار می‌گیرند. استفاده از اینترنت به عنوان یک حامل جهانی، اجازه ایجاد ارتباط سریع و ارزان به سایت‌های دیگر را فراهم می‌کند. این اتصال ممکن است از طریق گسترش VPN به عنوان نوعی از اتصالات امن صورت پذیرد.

[1] Point Of Presence

۱۳-۲-۶-۲ مخاطرات امنیتی

به بیان ساده، شبکه پهن‌باند یک اتصال پرسرعت و همیشه فعال بین یک مشترک و اینترنت است. این خصوصیات منجر می‌شود که تخریب یک سامانه متصل به شبکه پهن‌باند به عنوان هدفی ارزشمند برای هکرها محسوب شود و به‌طور مستقیم منجر به مخاطرات زیر شود:

- افشا، تغییر یا حذف اطلاعات، به‌عنوان نتیجه‌دسترسی از راه‌دور غیرمجاز،
- انتشار کدهای مخرب،
- بارگذاری/بارگیری[1] و اجرای کدهای غیرمجاز،
- سرقت شناسه،
- پیکربندی نادرست سامانه‌های سرویس‌گیرنده،
- معرفی آسیب‌پذیری‌های نرم‌افزاری،
- تراکم در شبکه،
- DoS.

۱۳-۲-۶-۳ کنترل‌های امنیتی

تعدادی کنترل‌های امنیتی فنی، به‌منظور مدیریت مخاطرات ناشی از تهدیدات شناخته‌شده در ارتباطات پهن‌باند وجود دارند که شامل موارد زیر هستند:

- دیواره‌های آتش دفترکار کوچک/خانگی[2]،
- نرم‌افزار ضد کدهای مخرب (شامل ویروس‌ها)،
- سامانه تشخیص نفوذ شامل سامانه پیش‌گیری از نفوذ،
- VPNها،
- به‌روز رسانی نرم‌افزار/ افزودن وصله‌ها به نرم‌افزار.

۱۳-۲-۷- دروازه‌های امنیتی

۱۳-۲-۷-۱ پس‌زمینه

آرایش دروازه امنیتی یک سازمان بایستی به‌گونه‌ای باشد که به‌طور مناسب از سامانه‌های داخلی آن سازمان، حفاظت کند و برطبق یک خط‌مشی دسترسی سرویس دروازه امنیتی مستندسازی شده، جریان ترافیک عبوری را به‌طور امن، مدیریت و کنترل نماید.

---

[1] Upload/Download
[2] Small Office/Home Office , SOHO

۱۳-۲-۷-۲ مخاطرات امنیتی

هر روزه هکرها از فنون پیچیده‌تری به‌منظور رخنه در شبکه‌های کسب‌وکار استفاده می‌کنند و در این راستا دروازه به‌عنوان یک مرکز موردتوجه به‌شمار می‌آید. تلاش‌ها برای دسترسی غیرمجاز می‌تواند مخرب باشد، نظیر مواردی که منجر به یک حمله DoS می‌شود. این امر می‌تواند موجب سواستفاده از منابع یا دست‌یابی به اطلاعات ارزشمند شود. یک دروازه می‌بایست سازمان را در برابر چنین نفوذهایی از دنیای خارج همچون اینترنت و یا شبکه‌های شخص ثالث حفاظت کند. محتوی پایش‌نشده‌ای که از یک سازمان خارج می‌شود، منجر به پی‌آمدهای قانونی و از دست‌رفتن بالقوه دارایی‌های فکری سازمان می‌شود. علاوه بر این، هنگامی‌که سازمان‌های بیشتری برای برآوردن الزامات سازمانی خود به اینترنت متصل می‌شوند، نیاز به کنترل دسترسی دربرابر وب‌سایت‌های نامناسب و مورد اعتراض خواهند داشت. در صورت عدم اعمال چنین کنترل‌هایی، به‌دلیل استفاده غیربهره‌ور بدون فیلتر از سایت‌ها، سازمان‌ها با مخاطراتی نظیر از دست رفتن بهره‌وری، درمعرض قرار گرفتن اسناد، تخصیص نادرست پهنای باند مواجه خواهند شد. در صورتی‌که این تهدیدات مورد توجه قرار نگیرند، این خطر وجود خواهد داشت که اتصال به دنیای خارج دسترسی‌ناپذیر شود، داده‌ها تخریب شوند یا دارایی‌های با ارزش شرکت مورد افشای غیرمجاز قرار گیرند. ممکن است داده‌هایی که بدون اعتبار مناسب در وب‌سایت‌ها وجود دارند یا منتقل می‌شوند، موجب اعمال جریمه‌های قانونی همچون جریمه برای فروش غیرمجاز داخلی اطلاعات شوند.

۱۳-۲-۷-۳ کنترل‌های امنیتی

یک دوازه امنیتی بایستی:

- شبکه‌های منطقی را از هم مجزا کند،
- انجام عملیات محدودکننده و تحلیل‌گر روی اطلاعات عبوری بین شبکه‌های منطقی اعمال نماید،
- توسط یک سازمان به عنوان ابزاری برای کنترل دسترسی به و از شبکه متعلق به آن سازمان مورد استفاده قرار گیرد،
- یک نقطه منفرد کنترل‌شده و قابل مدیریت برای ورود به یک شبکه تامین کند،
- خط‌مشی امنیتی سازمان را با توجه به اتصالات شبکه، اعمال نماید،
- یک نقطه منفرد به منظور واقعه‌نگاری تامین نماید.

به‌ازای هر دروازه امنیتی بایستی یک سند جداگانه خط‌مشی (امنیتی) دسترسی سرویس ایجاد شود و محتوای آن به منظور اطمینان از اینکه تنها ترافیک مجاز حق عبور دارد، پیاده‌سازی شود. لازم است در این سند، کلیه جزییات مربوط به مجموعه قوانینی که دروازه ملزم به اجرای آنها است و نیز پیکربندی دروازه ذکر شود. امکان تعریف اتصالات مجاز بایستی به‌صورت جداگانه، برطبق پروتکل‌های ارتباطاتی و جزییات دیگر فراهم باشد. بنابراین لازم است این خط مشی، به‌منظور حصول اطمینان از اینکه تنها کاربران و ترافیک معتبر به اتصالات ارتباطاتی دسترسی می‌یابند، محدودیت‌ها و قوانین به‌کاررفته برای عبور ترافیک به داخل و

خارج از دروازه امنیتی و همچنین پارامترهای مرتبط با مدیریت و پیکربندی دروازه امنیتی را به‌طور تفصیلی تعریف و ثبت کند.

لازم است تمامی دروازه‌های امنیتی از کلیه فنون شناسایی و احراز اصالت، کنترل دسترسی منطقی و امکانات ممیزی موجود، استفاده کامل کنند. به‌علاوه، دروازه‌ها بایستی به‌طور منظم به‌منظور کشف وجود احتمالی نرم‌افزارها و/یا داده‌های غیرمجاز، بررسی شوند و چنانچه موردی یافت شود، لازم است مطابق با طرح مدیریت حادثه امنیتی اطلاعات سازمان و/یا جامعه، گزارشی از حادثه ارایه شود (به استاندارد ISO/IEC 18044 مراجعه شود).

تاکید می‌شود که بایستی اتصال به یک شبکه تنها پس از بررسی اینکه دروازه امنیتی انتخابی با نیازمندی‌های سازمان و/یا جامعه منطبق است و اینکه تمامی مخاطرات حاصل از چنین اتصالی به‌طور امن قابل مدیریت هستند، برقرار گردد. همچنین لازم است اطمینان حاصل شود که کنار زدن دروازه امنیتی امکان‌پذیر نخواهدبود.

یک دیواره آتش نمونه خوبی از یک دروازه امنیتی است. دیواره‌های آتش به‌طور معمول بایستی به سطح اطمینان قابل قبولی در برابر مخاطرات ارزیابی‌شده، رسیده باشند. مجموعه قوانین استانداردی که معمولاً در دیواره‌های آتش به‌کار می‌روند، با رد تمام دسترسی‌ها بین شبکه‌های داخلی و شبکه‌های خارجی شروع می‌شوند و قوانین صریح برای تامین مسیرهای ارتباطی مورد نیاز به آن اضافه می‌شوند.

جزییات بیشتر در مورد دروازه‌های امنیتی در استاندارد ISO/IEC 18028-3 (و نیز استاندارد ISO/IEC 17799) آورده شده است و در استاندارد ISO/IEC 13335-2 پس از انتشار موجود خواهد بود.

قابل ذکر است که اگرچه در بند۳، به جنبه‌های مرتبط با امنیت دیواره‌های آتش شخصی که نوع خاصی از دیواره‌های آتش هستند، پرداخته نشده است، ولی لازم است آنها نیز مدنظر قرار گیرند. برخلاف اکثر سایت‌های مرکزی که توسط دیواره‌های آتش اختصاصی حفاظت می‌شوند، ممکن است سامانه‌های راه دور هزینه و مهارت‌های تخصصی لازم به‌منظور پشتیبانی از این دیواره‌ها را تعیین نکنند. در عوض می‌توان از یک دیواره آتش شخصی که جریان ارتباطات را به (و گاهی خارج از) رایانه راه دور کنترل می‌نماید، استفاده نمود. ممکن است مدیریت اجرای قوانین (خط‌مشی‌های) مربوط به دیواره آتش توسط کارکنان سایت مرکزی، راه دور انجام گیرد که این امر موجب بی‌نیازی کاربر سامانه راه دور از درک فنی سامانه خواهد شد. به‌هرحال در صورتی‌که این امر امکان‌پذیر نباشد، برای اطمینان از پیکربندی موثر، به‌ویژه هنگامی‌که افراد حاضر در سایت راه دور دانش IT را ندارند، بایستی دقت کافی مبذول گردد. برخی دیواره‌های آتش شخصی می‌توانند قابلیت انتقال از طریق شبکه را تنها به برنامه‌های مجاز (یا حتی کتابخانه‌ها) محدود کنند که این عمل منجر به محدود شدن امکان پخش نرم‌افزارهای مخرب می‌شود.

۱۳-۲-۸- سرویس‌های دسترسی راه دور

۱۳-۲-۸-۱ پس‌زمینه

هدف از RAS، فراهم شدن امکان تبادل داده‌ها بین یک سایت راه دور و سرویس مرکزی است. راه حل‌های زیادی برای این منظور وجود دارند که شامل موارد زیر هستند:

- ارتباطات از طریق اینترنت،
- سرویس IP شماره‌گیری.

ارتباطات از طریق اینترنت به‌طور روزافزون، به‌منظور فراهم نمودن پهنای باند بالا از سایت مرکزی و پهنای باند کمتر از راه‌دور به سایت مرکزی، از اتصالات ADSL تامین‌شده توسط ISPها استفاده می‌کند. غیر از مواردی که داده‌ها دارای کمترین میزان حساسیت هستند، لازم است نوعی از VPN (به بند ۱۳-۹-۲ مراجعه شود) به‌منظور تامین امنیت جریان‌های داده‌های تبادل‌شده، مورد استفاده قرار گیرد.

سرویس‌های IP شماره‌گیری به یک سایت راه دور (به‌طور معمول یک کاربر منفرد) اجازه شماره‌گیری به یک بانک مودم در یک مکان مرکزی را می‌دهند. پس از احراز اصالت، اتصال بین سایت راه دور و سرویس مرکزی باز خواهد شد. به‌جز در مواردی که برنامه کاربردی یک پروتکل امنیتی را پیاده‌سازی می‌کند، این حالت ارتباطی به‌گونه‌ای است که در حالت آماده دریافت خواهد بود. ممکن است دسترسی از طریق RAS، توسط "شبکه دیجیتالی سرویس‌های مجتمع"[1] و یا خطوط آنالوگ انجام گیرد. در هر دو حالت، کاربر به یک نقطه مرکزی که سطحی از احراز اصالت در آن صورت می‌پذیرد، شماره‌گیری می‌کند. RAS، تنها امکان انتقال داده‌های رمزنشده را فراهم می‌کند.

۱۳-۲-۸-۲ مخاطرات امنیتی

تعدادی مخاطرات امنیتی وجود دارند که ممکن است مرتبط با RAS باشند. این مخاطرات شامل موارد زیر هستند:

- دسترسی غیرمجاز به سامانه‌ها، سرویس‌ها و اطلاعات یک سازمان (با روش‌هایی همچون استراق سمع) که منجر به افشا، تغییرات غیرمجاز و یا تخریب اطلاعات و/یا سرویس می‌شود،
- ورود کدهای مخرب به سامانه‌ها، سرویس‌ها و اطلاعات یک سازمان که منجر به تغییر، عدم دسترسی‌پذیری و تخریب می‌شود،
- یک حمله DoS بر سرویس‌های یک سازمان.

[1] Integrated Services Digital Network, ISDN

۱۳-۲-۸-۳ کنترل‌های امنیتی

در موارد دسترسی از راه‌دور لازم است سرویس‌های مرکزی خود را در برابر دسترسی‌های غیرمجاز، امن گردانند. علاوه بر این، انتظار می‌رود که خود سامانه‌های راه دور، دارای فنونی حفاظتی در برابر برخی از تهدیدات امنیتی باشند. کنترل‌هایی که ممکن است مورد نیاز باشند، شامل موارد زیر هستند:

- دیواره‌های آتش (شامل دیواره‌های آتش شخصی)،
- ACLهای مسیریاب،
- رمزنگاری پیوندهای دسترسی اینترنت،
- CLID،
- احراز اصالت قوی،
- نرم‌افزار ضد ویروس،
- مدیریت ممیزی.

جزییات بیشتر در زمینه امنیت سرویس‌های دسترسی از راه‌دور در استاندارد ISO/IEC 18028-4 ارایه شده است.

۱۳-۲-۹- شبکه‌های خصوصی مجازی

۱۳-۲-۹-۱ پس‌زمینه

یک VPN، شبکه‌ای خصوصی است که با استفاده از زیرساخت شبکه‌های موجود پیاده‌سازی می‌شود. از نقطه نظر یک کاربر، VPN همانند یک شبکه خصوصی عمل می‌نماید و عملکردها و سرویس‌های مشابهی را ارایه می‌دهد. یک VPN می‌تواند در وضعیت‌های مختلفی مورد استفاده قرار گیرد، به عنوان مثال برای:

- پیاده‌سازی دسترسی راه دور به یک سازمان از طریق کارمندان سیار یا خارج از محوطه،
- متصل کردن محل‌های مختلف یک سازمان به یکدیگر، شامل اتصالات اضافه، برای پیاده‌سازی یک زیرساخت پشتیبان،
- برقراری اتصالات به شبکه یک سازمان برای سایر شرکای کسب و کار/سازمان‌ها،

به بیان دیگر VPNها برای دو رایانه یا دو شبکه، امکان برقراری ارتباط امن از طریق یک رسانه ناامن (به عنوان مثال اینترنت) را فراهم می‌کنند. این ارتباط قبلاً با صرف هزینه‌های بالا و از طریق خطوط اجاره‌ای، با استفاده از رمزکننده‌های پیوندی صورت می‌پذیرفت. در حال حاضر با ظهور اتصالات اینترنتی پرسرعت و تجهیزات پایانه‌ای مناسب در هر انتها، امکان برقرای ارتباطات امن و قابل اعتماد بین سایت‌ها از طریق VPNها فراهم شده است.

۱۳-۲-۹-۲ مخاطرات امنیتی

مخاطره امنیتی کلیدی در ارتباطات از طریق یک شبکه ناامن، امکان دسترس‌پذیر بودن اطلاعات حساس، برای اشخاص غیرمجاز است که این امر افشا و/یا تغییر غیرمجاز اطلاعات را به‌دنبال خواهد داشت.

علاوه بر مخاطراتی که نوعاً در ارتباط با شبکه‌بندی محلی و گسترده هستند (به بندهای۱۳-۲-۲-۲ و ۱۳-۲-۳-۲ مراجعه شود)، مخاطرات معمول دیگری در ارتباط با VPNها وجود دارند که شامل موارد زیر هستند:

- پیاده‌سازی ناامن به‌واسطه:
  - بخش رمزکننده آزمایش‌نشده یا معیوب،
  - یک رمز به اشترک گذاشته شده ضعیف که به آسانی قابل حدس زدن است،
  - همبندی ضعیف شبکه،
  - عدم قطعیت در مورد امنیت سرویس‌گیرنده از راه‌دور،
  - عدم قطعیت در مورد احراز اصالت کاربران،
- عدم قطعیت در مورد امنیت ارایه‌کننده سرویس،
- عملکرد ضعیف یا دسترسی‌پذیری سرویس،
- عدم سازگاری با نیازمندی‌های مربوط به قانون و مقررات در موارد استفاده از رمزنگاری در کشورهای خاص.

۱۳-۲-۹-۳ کنترل‌های امنیتی

در شبکه‌بندی و/یا پروتکل‌های مربوط به برنامه‌های کاربردی VPNها، برای پیاده‌سازی سرویس‌ها و کارکردهای امنیتی، به‌طور معمول از فنون رمزنگاری، استفاده می‌شود، به‌ویژه هنگامی‌که شبکه‌ای که شبکه خصوصی روی آن بنا می‌شود، یک شبکه عمومی (نظیر اینترنت) باشد. در اغلب پیاده‌سازی‌ها، پیوندهای ارتباطی بین شرکت‌کنندگان، به‌منظور حصول اطمینان از محرمانگی رمز می‌شوند و از پروتکل‌های احراز اصالت برای تصدیق شناسه سامانه‌های متصل به VPN استفاده می‌شود. اطلاعات رمزشده معمولاً، از طریق تونل امنی که به یک دروازه سازمان متصل می‌شود، منتقل می‌شوند و در عین‌حال از محرمانگی و یکپارچگی آنها نیز پشتیبانی می‌شود. دروازه پس از این مرحله کاربر راه دور را شناسایی می‌کند و به کاربر، تنها اجازه دسترسی به اطلاعاتی را می‌دهد که مجاز برای دریافت هستند.

بنابراین یک VPN مکانیزمی مبتنی بر تونل زدن پروتکل - فرض یک پروتکل کامل (پروتکل سرویس‌گیرنده) به عنوان رشته ساده‌ای از بیت‌ها و پوشاندن آن در پروتکل دیگر (پروتکل حامل) - است. به‌طور معمول پروتکل حامل VPN، تامین‌کننده امنیت (یکپارچگی و محرمانگی) برای پروتکل (پروتکل‌های) سرویس‌گیرنده است. با توجه به موارد استفاده از VPNها، لازم است برخی جنبه‌های معماری مورد لحاظ قرار گیرند. این جنبه‌ها عبارتند از:

- امنیت نقطه انتهایی،
- امنیت پایانه‌ای،
- حفاظت در برابر نرم‌افزارهای مخرب،
- احراز اصالت،
- تشخیص نفوذ،
- دروازه‌های امنیتی (شامل دیواره‌های آتش)،

- طراحی شبکه،
- اتصالات دیگر،
- شکستن تونل[1]،
- واقعه‌نگاری ممیزی و پایش شبکه،
- مدیریت آسیب‌پذیری‌های فنی،

توصیف تفصیلی در مورد VPNها مشتمل بر هر یک از جنبه‌های معماری مذکور، در استاندارد ISO/IEC 18028-5 ارایه شده است.

۱۳-۲-۱۰- همگرایی IP (داده، صوت، تصویر)

۱۳-۲-۱۰-۱ پس‌زمینه

هم‌چنان‌که همگرایی صوت و داده عمومیت می‌یابد، می‌بایستی پیامدهای امنیتی آن شناسایی و بیان شوند. گرچه پیاده‌سازی‌های تلفنی فعلی، برای پیش‌گیری از تقلب‌های مالیاتی و پست صوتی و سایر نقض‌های امنیتی نیاز به کنترل‌های امنیتی دارند ولی این سامانه‌ها با شبکه‌های داده شرکتی، یکپارچه نمی‌شوند و مواجه با مخاطراتی یکسان با شبکه‌های داده IP نیز نیستند. با همگرا کردن صوت و داده بایستی کنترل‌های امنیتی به‌منظور کاهش مخاطرات ناشی از حملات پیاده‌سازی شوند.

یک برنامه کاربردی VoIP معمولاً از نرم‌افزار اختصاصی نصب‌شده روی سخت‌افزاری باز یا از نظر کسب‌وکار قابل دسترس و نیز سیستم‌های عامل، تشکیل شده است. تعداد سرویس‌دهندگان بستگی به پیاده‌سازی فروشنده و نیز گسترش واقعی عمل دارد. این مولفه‌ها از طریق IP روی Ethernet، ارتباط برقرار می‌کنند و از طریق سوده‌ها و/یا مسیریاب‌ها به هم متصل می‌شوند.

۱۳-۲-۱۰-۲ مخاطرات امنیتی

نواحی اصلی مخاطره‌آمیز، می‌توانند مربوط به حملات مبتنی بر IP بر روی آسیب‌پذیری‌های نرم‌افزاری فروشنده‌ای خاص و سخت‌افزار یا بستر سیستم عاملی که میزبان برنامه کاربردی VoIP است، باشند. مخاطرات مرتبط با مولفه‌های VoIP، شامل حملات روی دستگاه‌ها و برنامه‌های کاربردی مبتنی بر شبکه هستند و ممکن است از طریق آسیب‌پذیری‌ها در طراحی یا پیاده‌سازی راه‌حل VoIP، فعال یا تسهیل شوند. نواحی مخاطره‌آمیزی که بایستی مورد توجه قرار گیرند، شامل موارد زیر هستند:

- کیفیت سرویس دهی – ممکن است عدم وجود کیفیت سرویس دهی کلی، موجب از دست دادن کیفیت، یا قطع شدن مکالمات در اثر گم شدن بسته‌ها و انتشار تأخیر در طول شبکه شود.
- عدم دسترسی‌پذیری سرویس در اثر حملات DoS، یا تغییرات در جداول مسیریابی،

[1] Split Tunneling

- یکپارچگی و دسترسی‌پذیری ممکن است، توسط ویروس‌هایی که سعی می‌کنند از طریق سامانه‌های VoIP ناامن به شبکه وارد شوند، تحت‌تاثیر قرار گیرند. این ویروس‌ها ممکن است موجب پایین آمدن سرویس و یا حتی از دست رفتن آن شوند. به‌علاوه ممکن است در سرویس‌دهندگان شبکه نیز انتشار یابند و بدین ترتیب موجب تخریب داده‌های ذخیره‌ای شوند،
- تلفن‌های نرم‌افزاری روی رایانه‌های شخصی سرویس‌گیرنده، یک مخاطره اساسی به حساب می‌آیند به این دلیل که می‌توانند نقطه‌ای برای ورود ویروس‌ها و اعمال نفوذ باشند،
- سرویس‌دهندگان و سامانه‌های مدیریت VoIP، در صورت عدم حفاظت توسط دیواره‌های آتش، در خطر خواهند بود،
- امنیت شبکه داده می‌تواند به‌علت اینکه چندین درگاه به‌منظور پشتیبانی VoIP روی دیواره‌های آتش باز می‌شوند، دچار تنزل شود. یک جلسه VoIP دارای پروتکل‌ها و شماره درگاه‌های مربوطه متعددی است. H .323 از پروتکل‌های متعددی به‌منظور سیگنالینگ استفاده می‌کند و H .323 و SIP از RTP استفاده می‌نمایند. در نتیجه ممکن است یک جلسه H .323 تا یازده درگاه مختلف را به‌کار گیرد.
- تقلب یک مساله اصلی در تلفن محسوب می‌شود و چنانچه ملاحظات امنیتی مورد توجه قرار نگیرد، VoIP موجب افزایش این قبیل مخاطرات می‌شود. هکرها می‌توانند از طریق جعل هویت، انجام حملات تکرار یا ربودن اتصال به سرویس VoIP دسترسی غیرمجاز پیدا کنند که در این صورت تقلب درعوارض یا فراخوانی نرخ‌های غیرمجاز عوارض، موجب خسارات قابل توجهی خواهد شد،
- ممکن است به‌دلیل شنود ارتباطات، محرمانگی از بین برود نظیر حمله "واسطه‌گرانه"[1] که درون شبکه‌ها توسط کارمندان و کسانی که دسترسی به شبکه دارند، قابل وقوع است.
- استراق سمع مکالمات صوتی،
- از آنجا که تلفن‌های IP برای کار به منبع تغذیه احتیاج دارند، شبکه تلفنی ممکن است در صورت خرابی منبع، قادر به کار نباشد،
- خرابی در سرویس‌های داده و صوت خطر بزرگتری است که به‌دلیل استفاده از مولفه‌های مشترک نظیر یک شبکه محلی، رخ می‌دهد.

۱۳-۲-۱۰-۳ کنترل‌های امنیتی

تعدادی کنترل‌های امنیتی فنی به‌منظور مدیریت مخاطرات ناشی از تهدیدات شناخته‌شده مربوط به شبکه‌های IP همگراشده، وجود دارند که شامل موارد زیر هستند:

- تسهیلات کیفیت سرویس در یک شبکه همگرا بایستی پیاده‌سازی شوند، در غیر این صورت ممکن است کیفیت صوت دست‌خوش تنزل شود. همچنین تحویل سرویس شبکه و در صورت

[1] Man-In-The-Middle

امکان اتصالاتIP بایستی از طریق فیبر به یک سایت انجام شود تا اطمینان حاصل شود که لغزش (که کیفیت صوت را تحت تأثیر قرار می‌دهد)، به کمترین حد خود رسیده است،

- کلیه سرویس‌دهندگان VoIP می‌بایست به‌منظور حفاظت در برابر نرم‌افزارهای مخرب، پیکربندی شوند،
- لازم است رایانه‌های شخصی که از تلفن‌های نرم‌افزاری پشتیبانی می‌کنند با دیواره‌های آتش شخصی مجهز شوند و همچنین می‌بایست نرم‌افزار بررسی ویروس مرتباً به‌روز شود،
- لازم است سرویس‌دهندگان VoIP و سامانه‌های مدیریت VoIP به دیواره‌های آتش مجهز شوند تا از آنها در مقابل حملات حفاظت کنند،
- طراحان می‌بایست اطمینان حاصل کنند که کمترین تعداد از درگاه‌ها روی دیواره‌های آتش به‌منظور حمایت از سرویس‌های VoIP باز هستند،
- برای مقابله با تقلب در عوارض لازم است کنترل‌های ضد جعل هویت و ضد تکرار پیاده‌سازی شوند تا از سرقت اتصال پیش‌گیری کنند،
- بایستی تمام دسترسی‌ها به سرویس‌دهندگان مدیریت، احراز اصالت شوند،
- سرویس‌های صوت و داده در مواقع ممکن بایستی مجزا شوند،
- بایستی IDS به‌منظور پشتیبانی از سرویس‌دهندگانی که سرویس‌های VoIP را تامین می‌کنند، در نظر گرفته شود،
- رمزنگاری مسیر داده بایستی هنگامی‌که اطلاعات حساس از طریق شبکه VoIP منتقل می‌شوند، در نظر گرفته شود،
- تغذیه تلفن‌های IP بایستی ازطریق هاب‌های Ethernet که توسط UPSها پشتیبانی می‌شوند، تامین شود،
- ممکن است در مواقع ضروری، نیاز به ارایه یک سرویس صوتی قراردادی با منبع تغذیه مستقل باشد.

۱۳-۲-۱۱- فعال‌کردن دسترسی به سرویس‌های ارایه‌شده توسط شبکه‌هایی که (نسبت به سازمان) بیرونی هستند

۱۳-۲-۱۱-۱ پس‌زمینه

ایجاد سرویس‌های پست الکترونیکی و اینترنت در یک سازمان به منظور برآورده کردن نیازمندی‌های قانونی، تهدیدات مختلفی را به‌دنبال می‌آورد. این تهدیدات موجب سواستفاده از سامانه‌های آسیب‌پذیر خواهند شد و جز در مواردی که سرویس‌ها به‌نحو درست طراحی و اجرا شده باشند، مخاطرات قابل ملاحظه‌ای را بر سازمان تحمیل خواهند کرد. به عنوان نمونه برخلاف وجود موانعی که فرستندگان هرزنامه در ارسال در محل کار مواجه می‌شوند، هرزنامه مشکل بزرگی برای بنگاه‌های کسب‌وکار و کارکنان آنها محسوب می‌شود. به‌دلیل اینکه فرستندگان هرزنامه تلاش می‌کنند تا اسامی کارکنان را به‌دست آورند، اغلب

سرمایه‌گذاران نیاز به استفاده از فناوری‌های ضد هرزنامه و آموزش فنون حفاظت از آدرس‌های پست الکترونیکی به کاربران، خواهند داشت. علاوه بر این در صورت اتصال به اینترنت ممکن است کاربران به حفاظت در برابر ورود نرم‌افزارهای مخرب نظیر اسب‌های تراوا به درون سازمان نیاز داشته باشند. این نرم‌افزارها می‌توانند منجر به آسیب‌های پرهزینه برای سامانه‌های اطلاعاتی و اعتبار یک سازمان شوند. نکته کلیدی که همواره بایستی مدنظر قرار گیرد این است که اینترنت همواره یک محیط غیرقابل اعتماد است.

۱۳-۲-۱۱-۲ مخاطرات امنیتی

نواحی مخاطره‌آمیز کلیدی که مربوط به فعال کردن دسترسی به سرویس‌های ارایه‌شده توسط شبکه‌های خارج سازمان هستند و همچنین مناطقی که در آنها آسیب‌پذیری‌های اینترنت و سرویس‌های پست الکترونیکی می‌توانند مورد سواستفاده قرار گیرند، شامل موارد زیر هستند:

- ورود بالقوه نرم‌افزارهای مخرب آسیب‌رسان، نظیر اسب‌های تراوا،
- دریافت انبوه هرزنامه،
- از دست دادن اطلاعات سازمان،
- مخدوش شدن یکپارچگی یا از دست رفتن اطلاعات،
- حملات DoS،
- استفاده غیرمجاز از اینترنت و سرویس‌های پست الکترونیکی شامل عدم مطابقت با خط‌مشی سازمان (به عنوان مثال استفاده ازسرویس‌ها برای منافع شخصی) و نیز موارد ناسازگار با قانون و مقررات (به‌عنوان مثال ارسال پست‌های الکترونیکی تهدیدآمیز).

۱۳-۲-۱۱-۳ کنترل‌های امنیتی

کنترل‌های امنیتی فنی برای مدیریت مخاطرات ناشی از تهدیدات شناخته‌شده در اینترنت/پست الکترونیکی شامل موارد زیر هستند:

- استفاده از دیواره‌های آتش با سطوح اطمینان متناسب با مخاطرات ارزیابی‌شده و مجموعه قوانین مرتبط با دیواره‌های آتش که موارد زیر را پوشش می‌دهند:
  - خط‌مشی پیش‌فرض "رد کردن تمام"،
  - فقط وب فرستنده (به عنوان مثال، http/https)
  - پست الکترونیکی دو جهته[1]،
- استفاده از ACLها و مترجم‌های آدرس شبکه روی مسیریاب‌ها، به‌منظور محدود ساختن و مخفی کردن ساختار آدرس‌دهی IP،

[1] Both Ways

- فعال‌سازی کنترل‌های ضد جعل برای پیش‌گیری از حملات بیرونی. این کنترل‌ها، یک پیغام بیرون از سازمان را (به‌عنوان مثال از اینترنت) را در صورتی‌که مدعی این باشد که از داخل سازمان منشا شده است، نمی‌پذیرند و بالعکس.
- فعال‌سازی وب و حایل‌های[1] پست الکترونیک به‌گونه‌ای که به عنوان یک واسطه بین کاربر در یک ایستگاه کاری و اینترنت عمل کنند. در این صورت سرمایه‌گذار می‌تواند از امنیت، کنترل مدیریت اجرایی و سرویس تسریع‌کننده[2] اطمینان حاصل کند. امنیت از طریق مقایسه URL تقاضاشده در برابر فهرست‌های سیاه و سفید (برای دسترسی به اینترنت)، پویش داده برای الگوهای شناخته شده، ترجمه بین آدرس‌های داخلی و خارجی، ایجاد یک ثبت ممیزی از تقاضاها و تقاضا دهنده‌ها و مجهز شدن به امکانات ضد ویروس در حایل‌ها اعمال می‌شود.
- کنترل‌های ضدویروس روی وب و حایل‌های پست الکترونیکی. کنترل‌های معمول شامل تسهیلاتی برای قرنطینه کردن فایل‌های مشکوک (به عنوان مثال از طریق نوع محتوی) و پنهان کردن URLهای تقاضا شده و آدرس‌های پست الکترونیکی در مقابل یک فهرست سیاه است. (لازم به ذکر است که فهرست‌های سیاه مصون از خطا نیستند، به‌ویژه هنگامی‌که از دیگر فهرست‌ها به‌دست می‌آیند. در این صورت احتمال خطر تشخیص اشتباه وجود خواهد داشت). اطلاعات بیشتر در زمینه کنترل‌های ضد ویروس در بند۱۳-۹ ارایه شده است،
- ضد بازپخش[3] روی سرویس‌دهندگان پست الکترونیکی و نیز بر روی جستجوهای معکوس در سرویس نام‌دهی حوزه. کنترل‌های ضد بازپخش بررسی می‌کنند که آیا پست الکترونیکی ورودی از طرف یک سازمان فرستنده صحیح است یا خیر. در صورت صحیح نبودن، پست الکترونیکی ثبت (یا قرنطینه) می‌شود و پس از آن سرویس‌دهنده پست الکترونیکی، اقدام دیگری انجام نمی‌دهد،
- فعال کردن هشدارها و تله‌های SNMP. SNMP می‌تواند برای کنترل راه دور یک دستگاه شبکه‌ای و نیز ارسال پیغام‌ها (یا "تله‌ها") توسط دستگاه به‌منظور آگاه کردن یک ایستگاه پایشی از شرایط آن دستگاه، مورد استفاده قرار گیرد،
- واقعه‌نگاری ممیزی شبکه و پایش (به بند ۱۳-۷ مراجعه شود)،
- دایر کردن مدیریت خارج از محدوده سازمانی که مربوط است به فرایند استفاده از شبکه‌های مختلف برای داده است و نیز مدیریت به‌منظور حصول اطمینان از این‌که برای یک مهاجم امکان اتصال به دستگاه هدف وجود ندارد،
- حصول اطمینان از اینکه آسیب‌پذیری‌های موجود در نرم‌افزار سرویس‌گیرنده که برای دسترسی به سرویس‌های اینترنت (به عنوان مثال مرورگر وب) مورد استفاده قرار می‌گیرند، به‌طور مناسبی با فرآیندهای مدیریت وصله‌ها و آسیب‌پذیری‌ها مربوط شده‌اند.

---

[1] Proxy
[2] Caching Service
[3] Anti-Relay

۱۳-۲-۱۲- معماری میزبانی وب

۱۳-۲-۱۲-۱ پس‌زمینه

سرویس‌های میزبان وب توسط بسیاری از ارایه‌کنندگان سرویس شبکه به شکل یک سرویس استاندارد که اغلب شامل تسهیلات پایگاه داده برای اداره داده‌های ماندگار و نیز یک محیط زمان اجرای برنامه کاربردی پایه است، ارایه می‌شوند. گرچه اغلب مولفه‌های مورد نیاز برای پیاده‌سازی و ارایه سرویس‌های میزبان وب خارج از دامنه کاربرد این استاندارد هستند (نظیر سرویس‌دهندگان وب یا نرم‌افزار پایگاه داده)، ولی به این دلیل که اغلب افراد، معماری میزبان وب را به عنوان بخشی جدایی‌ناپذیر از شبکه پیشنهادی، در نظر می‌گیرند، در اینجا ملاحظات چندی در مورد کلیت سرویس بیان می‌شود.

سایت‌های میزبان وب مواجه با تهدیدهای بسیاری هستند، به‌ویژه هنگامی‌که به اینترنت متصل می‌شوند، به‌عنوان مثال در مکان‌هایی که سازمان‌های مهم از جانب گروه‌های حاشیه‌ای تحت حمله هستند. بنابراین شناسایی کلیه تهدیدهای بالقوه و پس از آن مسدود شدن تمام آسیب‌پذیری‌هایی که می‌توانند توسط این تهدیدها مورد سوءاستفاده قرار گیرند، حایز اهمیت خواهد بود. بهترین راه برای نایل شدن به این هدف، حذف آسیب‌پذیری‌ها در طراحی معماری خواهد بود. با بیان این آسیب‌پذیری‌ها مطابق با یک راهبرد در این زمینه، امکان طراحی یک وب‌سایت امن، قابل اعتماد و با احتمال خطر پایین وجود خواهد داشت.

۱۳-۲-۱۲-۲ مخاطرات امنیتی

نواحی مخاطره‌آمیز کلیدی مربوط به این زمینه شامل موارد زیر هستند:

- دسترسی مهاجم به برنامه‌های کاربردی و داده از طریق وجود یک نقض در حفاظت از پیرامون،
- در معرض گذاشتن آسیب‌پذیری‌ها در مولفه‌های زیر ساخت،
- چندین نقطه خرابی،
- از دست رفتن سرویس به علت خرابی سخت‌افزار،
- عدم توانایی ارایه سرویس در هنگام تعمیر،
- دسترسی غیر عمدی توسط کاربران عمومی به نواحی ذخیره داده،
- نرم‌افزار مخرب که در سامانه بارگذاری می‌شود،
- در معرض خطر بودن با یک وب‌سایت به‌دلیل تغییر عملکرد،
- عدم توانایی در گرفتن فایل‌های پشتیبانی بدون تحت تأثیر قرار دادن عملکرد وب‌سایت،
- افشای غیرمجاز یک طرح آدرس‌دهی IP که موجب تسهیل کردن حمله به وب‌سایت می‌شود،
- سواستفاده از اتصالات بین ایستگاه‌های مدیریت و وب سایت،
- حمله کشف‌نشده،
- دشواری ردیابی نفوذهای بین دستگاهی،
- عدم توانایی در بازیابی داده،
- عدم توانایی در برآوردن الزامات توافق سطح سرویس،

- عدم توانایی در حفظ پیوستگی سرویس،
- استفاده غیرمجاز از سرویس‌های وب شامل تخلف از خط‌مشی‌های سازمان (به عنوان مثال استفاده از سرویس‌دهندگان برای منافع شخصی) و عدم تطابق با قانون و مقررات (به عنوان مثال ذخیره اطلاعاتی که حق کپی‌برداری را نقض می‌کند یا ذخیره موارد مستهجن).

۱۳-۲-۱۲-۳ کنترل‌های امنیتی

کنترل‌های امنیتی فنی به‌منظور مدیریت مخاطرات ناشی از تهدیدهای شناخته‌شده برای وب‌سایت‌ها، شامل این موارد هستند:

- تدارک ناحیه‌بندی و امنیت کامل به‌منظور محدود نمودن تاثیر یک حمله موفق،
- تعیین انواع مختلف دیواره‌های آتش به‌منظور مقابله با آسیب‌پذیری‌های احتمالی دیواره آتش. (اطلاعات بیشتر در زمینه دیواره‌های آتش در بند ۱۳-۲-۷ این استاندارد و نیز در استاندارد ISO/IEC 18028-3 ارایه شده است)،
- انعطاف‌پذیری؛ طراحی ارائه شده در برابر نقاط خرابی بالقوه بایستی امتحان شود و موارد خرابی نیز بایستی حذف گردند.
- افزودگی/تسهیم بار به‌منظور مقابله با خرابی تجهیزات،
- دسته‌بندی در موارد دسترسی بالا در یک محیط ۷ × ۲۴، یک نیازمندی محسوب می‌شود،
- حایل نمودن سرویس‌ها برای محدود نمودن دسترسی به یک وب‌سایت و همچنین فعال‌سازی یک واقعه‌نگاری با درجه بالا،
- کنترل‌های ضد ویروس روی بارگذاری‌ها برای پیش‌گیری از وارد کردن نرم‌افزار مخرب. (اطلاعات بیشتر در زمینه کنترل‌های مربوط به پیش‌گیری از کدهای مخرب در بند ۹-۱۳ ارایه شده است)،
- به‌طور معمول سودهی لایه ۲ در طراحی یک وب‌سایت مورد استفاده قرار می‌گیرد. سودهی لایه ۳ غیر از مواردی‌که مرتبط با نیازمندی‌های کسب و کار باشد، مورد استفاده قرار نمی‌گیرد، به‌عنوان مثال برای تسهیم بار. به‌علاوه نبایستی در هر دو طرف یک دیواره آتش از سوده‌های فیزیکی یکسانی استفاده کرد. نقاط مورد آزمایش نیز بایستی در طراحی سوئیچ درنظر گرفته‌شود.
- VPNها با توجه به کارکردشان تفکیک می‌شوند تا IDS را قادر سازند که راحت‌تر تنظیم شود، به‌گونه‌ای که در هر VPN، مجموعه پروتکل‌ها کاهش یابد. علاوه بر این، پیاده‌سازی یک VPN پشتیبان، به پشتیبان‌ها اجازه می‌دهد که بدون در خطر افتادن عملکرد سایت در هر زمانی از روز کار کنند،
- استفاده از طرح آدرس‌دهی IP به‌منظور محدود نمودن تعداد آدرس‌های عمومی به کمترین حد، با حفظ طرح آدرس‌دهی "در بیشترین حد اعتماد"، به‌گونه‌ای که آگاهی از آن بتواند برای غالب شدن بر یک حمله روی وب‌سایت، مورد استفاده قرار بگیرد.

- اتصالات مدیریتی هنگامی‌که بر روی شبکه‌های عمومی برقرار می‌شوند، بایستی رمز شوند (برای اطلاعات بیشتر در زمینه کنترل راه دور به استاندارد ISO/IEC 18028-4 مراجعه شود). این امر حداقل شامل استفاده از اخطارها/ تله‌های SNMP، بر روی اتصالات درگاه میز فرمان است.
- تمام ثبت‌های مربوط به تراکنش‌ها و رویدادهای هر دستگاه، روی یک سرویس‌گیرنده ممیزی و سپس روی یک واسط پشتیبان نظیر لوح فشرده، کپی می‌شوند. (اطلاعات بیشتر در مورد واقعه‌نگاری و پایش ممیزی شبکه، در بند ۷-۱۳ ارایه شده است)،
- یک سرویس همزمانی به‌عنوان راهکار کلیدی برای تحلیل دسترسی‌های غیرمجاز و توانایی دنبال کردن وقایع از طریق فایل‌های ثبت، پیاده‌سازی می‌شود. این امر مستلزم این است که زمان‌بندی تمام فایل‌های ثبت و بنابراین سرویس‌دهنده‌ها، با اختلاف یک ثانیه بیشتر یا کمتر، همزمان شوند. (NTP نیز مرتبط با این زمینه است، برای اطلاعات بیشتر، به استاندارد ISO/IEC 17799، بند ۶-۱۰ مراجعه شود)،
- یک سرویس پشتیبان مرکزی به‌دلیل قابل اجرا بودن بیشتر در مواقع نیاز، ارجحیت دارد،
- وب سایت‌هایی که در بیشتر موارد می‌بایست ۲۴ ساعت در روز کار کنند، نیاز به سخت‌افزار با کیفیت بالا دارند که بتواند در برابر شرایط محیط اطراف ایستادگی کند. توصیه می‌شود زیرساخت سرویس‌دهنده در یک وب سایت، برای پشتیبانی ۷ × ۲۴ عملکرد، تخصیص یابد. سیستم‌های عامل پشتیبان نیز می‌بایست سخت‌سازی شود و تمام سرویس‌دهنده‌ها و دستگاه‌های دیگر می‌بایست تحت آزمایش امنیتی قرار گیرند تا اطمینان حاصل شود که تمام دستگاه‌ها به‌طور کامل سخت‌سازی شده‌اند،
- نرم‌افزارهای کاربردی قوی پیاده‌سازی شده بطوری‌که در آن‌ها کد ازنظر ساختاری بررسی شده است یعنی ازنظر منطقی صحیح باشد و از نرم‌افزارهای احراز اصالت تاییدشده استفاده می‌کند،

همچنین لازم به ذکر است که معمولاً مقوله‌های مربوط به مدیریت تداوم کسب‌وکار، در زمان طراحی وب سایت‌ها به‌طور کامل در نظر گرفته نمی‌شوند. لازم است فعالیت‌های کامل مدیریت تداوم کسب‌وکار، در ارتباط با وب سایت‌ها انجام پذیرند. (برای اطلاعات بیشتر در زمینه مدیریت تداوم کسب‌وکار به بند ۱۱-۱۳ مراجعه شود).

۱۳-۳- چارچوب مدیریت سرویس امن

۱۳-۳-۱- فعالیت‌های مدیریتی

یک نیازمندی امنیتی اصلی برای هر شبکه‌بندی، پشتیبانی شدن توسط فعالیت‌های مدیریت سرویس امن است که پیاده‌سازی و اجرای امنیتی را راه‌اندازی و کنترل می‌نماید. این فعالیت‌ها بایستی برای اطمینان از امنیت تمامی سامانه‌های اطلاعاتی یک سازمان یا جامعه انجام گیرند. با توجه به اتصالات شبکه بایستی فعالیت‌های مدیریتی شامل موارد زیر باشند:

- تعریف کلیه مسوولیت‌های مرتبط با امنیت شبکه‌بندی و تخصیص یک مدیر امنیتی با مسوولیت‌های کلی،
- مستندسازی خط‌مشی امنیت شبکه‌بندی به ضمیمه معماری امنیتی فنی مستندسازی شده،
- رویه‌های عملیاتی امنیتی مستندسازی شده،
- انجام بررسی تطابق امنیتی، شامل انجام آزمون امنیتی برای حصول اطمینان از این‌که امنیت در سطح مورد نیاز حفظ می‌شود،
- شرایط امنیتی مستندسازی شده برای اتصال به‌گونه‌ای که توافق در مورد آنها قبل از آن‌که اتصال توسط سازمان‌ها یا مردم خارجی مجاز شمرده شود، صورت می‌گیرد،
- شرایط امنیتی مستندسازی شده برای کاربران سرویس‌های شبکه،
- یک طرح مدیریت رخداد امنیتی،
- طرح‌های بازیابی حوادث ناگوار/ تداوم کسب‌وکار آزمایش شده و مستندسازی شده،

قابل ذکر است که این بند روی جنبه‌های توضیح داده شده در استاندارد ISO/IEC 17799 و آنچه که در استاندارد ISO/IEC 13335-2 پس از انتشار بیان خواهد شد، بنا شده است. از عنوان‌های فوق، تنها مواردی که از نظر شبکه‌بندی دارای اهمیت ویژه هستند، در این استاندارد به‌طور تفصیلی شرح داده شده‌اند. اطلاعات بیشتر، به‌عنوان مثال در زمینه محتوای خط‌مشی امنیت شبکه‌بندی و رویه‌های عملیاتی امنیتی و نیز مباحثی که به‌طور مشروح در این استاندارد مورد بررسی قرار نگرفته‌اند، در استاندارد ISO/IEC 17799 و همچنین استاندارد ISO/IEC 13335-2 پس از انتشار، ارایه شده است.

۱۳-۳-۲- خط‌مشی امنیت شبکه‌بندی

پذیرش و پشتیبانی مشهود خط‌مشی امنیتی شبکه‌بندی سازمان، (که در استاندارد ISO/IEC 17799 بیان شده است)، وظیفه مدیریت است. خط‌مشی امنیت شبکه بایستی از خط‌مشی امنیت اطلاعات سازمان منشا گرفته و با آن سازگار باشد. همچنین بایستی این خط‌مشی قابلیت پیاده‌سازی داشته، برای خواندن اعضای مجاز سازمان، به آسانی در دسترس باشد و در موارد زیر، حاوی بیانیه‌های روشن باشد:

- موضع سازمان در ارتباط با استفاده از شبکه مورد پذیرش،
- قوانین صریح برای استفاده امن از منابع، سرویس‌ها و برنامه‌های کاربردی خاص شبکه،
- پیامدهای خرابی برای تطبیق با قوانین امنیتی،
- نگرش سازمان در مواجهه با سواستفاده از شبکه،
- دلیل(دلایل) برای خط‌مشی و هر قانون امنیتی ویژه،

(در برخی شرایط محیطی این بیانیه‌های واضح می‌توانند در صورتی‌که برای سازمان مناسب‌تر باشد و/یا برای کارکنان آن روشن‌تر باشد، در متن خط‌مشی امنیت اطلاعات قرار داده‌شوند).

به‌طور معمول بایستی محتوای خط‌مشی امنیت شبکه شامل خلاصه‌ای از نتایج حاصل از ارزیابی و مدیریت مخاطرات امنیتی (که توجیهی برای به‌کارگیری کنترل‌ها فراهم می‌کند)، همراه با جزییات تمام کنترل‌های امنیتی انتخابی بر حسب مخاطرات برآورد شده، باشد (به بند ۱۲ مراجعه شود).

۱۳-۳-۳- رویه‌های عملیاتی امنیتی

در پشتیبانی از خط‌مشی‌های امنیتی شبکه، بایستی سندهای رویه‌های عملیاتی امنیتی که پوشش‌دهنده هر اتصال شبکه به‌طور مناسب هستند، باید تدوین و حفظ شوند. این سندها باید شامل جزییات روزبه‌روز رویه‌های عملیاتی مرتبط با امنیت و اینکه چه کسی مسوول استفاده و مدیریت آنها است، باشند.

۱۳-۳-۴- بررسی مطابقت امنیت

برای تمام اتصالات شبکه، بررسی مطابقت امنیت بایستی مطابق یک بازبینی جامع متشکل از چک‌لیست‌های مشخص که در موارد زیر تعریف شده‌اند، صورت پذیرد:

- خط‌مشی امنیتی شبکه،
- رویه‌های عملیاتی امنیتی مرتبط،
- معماری امنیتی فنی،
- خط‌مشی (امن) دسترسی سرویس دروازه امنیتی،
- طرح(های) تداوم کسب‌وکار،
- در موارد مربوط، شرایط امنیتی اتصال.

این امر بایستی قبل از عملیات جاری اتصالات شبکه ، قبل از انتشار یک نسخه جدید اصلی (مرتبط با تغییرات مهم مرتبط با کسب‌وکار یا شبکه) محقق شود و در غیر این‌صورت سالانه اتفاق بیفتد.

این امر می‌بایست شامل اجرای آزمون‌های امنیتی مطابق استانداردهای شناخته‌شده با یک راهبرد آزمون امنیتی و طرح‌های مرتبط از پیش تولید شده باشدکه بیانگر دقیق آزمون‌های مورد نیاز و اینکه همراه با چه آزمون‌های دیگری، کجا و چه موقع انجام پذیرند، باشند. به‌طور معمول این امر بایستی ترکیبی از پویش آسیب‌پذیری و آزمون‌های نفوذ را در برگیرد. قبل از آغاز چنین آزمون‌هایی، طرح آزمون بایستی امتحان شود تا اطمینان حاصل شود که آزمون به طریقی که کاملا منطبق با قانون‌گذاری مربوطه است، انجام می‌شود. در هنگام انجام چنین آزمون‌هایی نباید فراموش شود که یک شبکه ممکن است تنها به یک کشور محدود نشود – بلکه ممکن است در میان کشورهای مختلف با قانون‌گذاری‌های مختلف توزیع شود. با دنبال نمودن این آزمون‌ها، گزارشات می‌بایست خصوصیات آسیب‌پذیری‌های مواجه شده و تعمیرات مورد نیاز و اولویت آنها را بیان کنند.

۱۳-۳-۵- شرایط امنیتی اتصال

تا زمانی‌که شرایط امنیتی اتصال محقق نشود و به صورت قراردادی منعقد نگردد، یک سازمان در معرض پذیرش مخاطرات مربوط به انتهای دیگر یک اتصال شبکه‌ای خارج از حوزه خود می‌باشد. چنین مخاطراتی می‌توانند شامل موارد مرتبط با حفاظت حریم خصوصی/ داده باشند. هنگامی‌که یک اتصال ممکن است برای تبادل داده‌های شخصی بسته به قانون ملی در یک و یا هر دو انتها مورد استفاده قرار بگیرد و نیز هنگامی‌که

انتهای دیگر یک اتصال شبکه (خارج از حوزه یک سازمان) در کشور دیگر قرار دارد، قانون‌گذاری می‌تواند متفاوت باشد.

به عنوان یک مثال سازمان A ممکن است بخواهد که قبل از اتصال سازمان B به سامانه‌هایش از طریق یک اتصال شبکه‌ای، B سطح مشخصی از امنیت را بایستی برای سامانه درگیر در آن اتصال برقرار و ثابت نماید. در این راستا A می‌تواند مطمئن باشد که B مخاطراتش را از روشی قابل قبول مدیریت می‌کند. در چنین مواردی A می‌بایست یک سند شرایط امنیتی برای اتصال را که کنترل‌های موجود در انتهای B را به‌تفصیل شرح می‌دهد، ایجاد نماید. این شرایط امنیتی بایستی باید توسط B پیاده‌سازی شوند و سپس سازمان یک بیانیه الزام آور را امضاء می‌کند که سازمان را به آن سند متعهد کرده و امنیت حفظ خواهد شد. A حق فرمان دادن و اجرای یک بررسی تطابق بر روی B را برای خود حفظ خواهد کرد.

همچنین مواردی وجود دارد که سازمان‌های یک جامعه به طور متقابل روی یک سند "شرایط امنیتی برای اتصال" توافق می‌کنندکه این سند تعهدات و مسوولیت‌های تمام اشخاص، شامل پذیرش بررسی مطابقت را ثبت می‌کند.

۱۳-۳-۶- شرایط امنیتی مستند شده برای کاربران سرویس‌های شبکه

به کاربرانی که مجاز به کار از راه دور هستند، بایستی یک سند "شرایط امنیتی برای کاربران سرویس‌های شبکه" داده شود. این سند مسوولیت‌های کاربران برای سخت‌افزار، نرم‌افزار و داده در ارتباط با شبکه و امنیت آن را بیان می‌کند.

۱۳-۳-۷- مدیریت حادثه

حوادث امنیت اطلاعات احتمال وقوع بالاتری دارند و در نتیجه پیامدهای کسب و کار منفی جدی‌تری را، جایی‌که اتصالات شبکه وجود دارند (در مقابل جایی‌که اتصالی وجود ندارد)، بدنبال دارند. به‌علاوه با اتصالات شبکه به سازمان‌های دیگر بویژه مسایل قانونی بسیار مهمی در ارتباط با حوادث، امکان بروز دارند.

بنابراین، یک سازمان با اتصالات شبکه بایستی مجهز به یک طرح مدیریت حادثه امنیت اطلاعات مستندشده و پیاده‌سازی شده و در زیرساخت متناظر محقق شده باشد تا بتواند بمحض شناسایی حوادث سریعا پاسخ دهد، اثر آنها را کمینه کند و مواردی بیاموزد تا از وقوع مجدد آنها جلوگیری نماید. این طرح می‌بایست قادر باشد تا هر دوی رویدادهای امنیت اطلاعات (رویدادهای شناخته شده یک سامانه، سرویس یا حالت شبکه که بیانگر یک نقض ممکن در خط‌مشی امنیت اطلاعات یا خرابی حفاظ، یا یک وضعیت ناشناخته قبلی مرتبط با امنیت) و رخدادهای امنیت اطلاعات (یک یا یک سری از از رویدادهای غیرمنتظره یا ناخواسته امنیت اطلاعات که احتمال زیادی در به خطر انداختن عملیات کسب‌وکار و تهدید امنیت اطلاعات دارد) را مشخص نماید.

جزییات بیشتر در زمینه مدیریت حوادث امنیت اطلاعات در استاندارد ISO/IEC 18044 شرح داده شده است.

۱۳-۴- مدیریت امنیت شبکه

۱۳-۴-۱- مقدمه

مدیریت هر شبکه بایستی به طریقی امن صورت پذیرد و در حقیقت پشتیبانی از مدیریت کلان امنیت شبکه را فراهم کند. این امر می‌بایست از طریق ملاحظه پروتکل‌های مختلف موجود شبکه و سرویس‌های امنیتی مرتبط انجام گیرد.

در پیشبرد این امر، یک سازمان بایستی تعدادی از کنترل‌ها را مدنظر قرار دهد که عمده این کنترل‌ها با استفاده از استانداردهای ISO/IEC 17799، و ISO/IEC 13335-2 پس از انتشار، قابل شناسایی است. به‌علاوه، درگاه‌های عیب‌یابی راه دور، مجازی یا فیزیکی، بایستی در مقابل دسترسی غیرمجاز حفاظت شوند.

۱۳-۴-۲- جنبه‌های شبکه‌بندی

جنبه‌های مختلف شبکه‌بندی می‌توانند به صورت زیر دسته‌بندی شوند:

کاربران شبکه – کارکنانی که کاربران و/یا مدیران اجرایی شبکه هستند. طیف کاربران از افرادی که به منابع راه دور از طریق اینترنت، اتصالات شماره‌گیر یا بی‌سیم دسترسی دارند، تا افرادی که از ایستگاه‌های کاری یا رایانه‌های شخصی متصل به یک شبکه محلی استفاده می‌کنند، تغییر می‌کند. کاربران متصل به شبکه‌های محلی نیز از طریق اتصالات بین شبکه‌ای که ممکن است بین شبکه‌های محلی آنها و شبکه های دیگر وجود داشته باشند، به منابع راه دور متصل شوند. چنین اتصالاتی ممکن است برای کاربر، شفاف باشند.

سامانه‌های انتهایی – رایانه‌ها، ایستگاه‌های کاری و وسایل سیار (به عنوان مثال، تلفن‌های هوشمند و دستیارهای داده‌های شخصی) که به شبکه‌ها متصل هستند، شامل دستگاه‌های استفاده‌شده برای دسترسی به تسهیلات شبکه‌شده (به عنوان مثال سامانه‌های سرویس گیرنده) و دستگاه‌های استفاده‌شده برای ارایه سرویس‌ها (به عنوان مثال سرویس‌دهنده‌ها، سامانه‌های رایانه میزبان). این دسته دربرگیرنده سخت‌افزار، نرم‌افزار سیستم عامل، و هر نرم‌افزار برنامه‌های کاربردی محلی شامل نرم‌افزارهای مورد استفاده برای دسترسی به شبکه می باشد.

برنامه‌های کاربردی تحت شبکه – نرم‌افزارهای برنامه کاربردی که روی سرویس‌دهنده‌های شبکه و یا سامانه‌های میزبان اجرا می‌شوند و از طریق اتصالات شبکه‌ای کامپیوتری برای فراهم نمودن موارد زیر در دسترس قرار می‌گیرند، به عنوان مثال:

- سرویس‌های تراکنش مالی،
- سرویس‌های نرم‌افزاری بنگاه‌ها (به عنوان مثال CRM، EIS، MRP، غیره)،
- سرویس‌های مبتنی بر وب،
- سرویس‌های پایگاه داده بر خط،
- تسهیلات ذخیره بر خط،

سرویس‌های شبکه – سرویس‌های ارایه شده توسط شبکه، معمولا در نرم‌افزار بر روی میزبان انتهایی یا سامانه‌های سرویس‌دهنده‌ای که بخشی از زیرساخت شبکه را تشکیل می‌دهند، پیاده‌سازی می‌شوند، به‌عنوان مثال:

- اتصال‌پذیری،
- پست الکترونیکی،
- انتقال فایل،
- سرویس‌های فهرست‌یار[1].

سرویس‌های شبکه ممکن است:

- تحت مالکیت و عملکرد سازمان باشند،
- تحت مالکیت سازمان ولی تحت عملکرد آژانس‌های خارجی تحت قرارداد باشند،
- اجاره شده از آژانس‌های خارجی باشند،
- خریداری شده به‌طور موردی از تامین‌کنندگان خارجی باشند،
- ترکیبی از موارد بالا باشند.

زیرساخت شبکه – تسهیلات سخت‌افزاری و نرم‌افزاری درگیر، به عنوان مثال:

- مقدمات،
- کابل‌کشی،
- تسهیلات بدون سیم،
- وسایل شبکه (به عنوان مثال مسیریاب‌ها، سوده‌ها، مودم‌ها و غیره).

همان‌گونه که در بند ۱۲ بیان شد، این جنبه‌های امنیت شبکه بایستی به عنوان وجوه شبکه در نظر گرفته شوند. این وجوه بر روی یک‌دیگر بنا می‌شوند تا یک چارچوب مدیریت امنیت شبکه را همانند شکل زیر تشکیل دهند:

کاربران شبکه
سامانه‌های انتهایی شبکه
کاربردهای وابسته به شبکه
سرویس‌های شبکه
زیرساخت شبکه

شکل ۴- عناصر با ارزش در چارچوب مدیریت امنیت شبکه.

وجود برخی همپوشانی‌ها در بعضی سیستم‌ها که نقش‌های متعددی را در هر سناریوی شبکه واقعی بر عهده دارند، اجتناب ناپذیر است. به‌هرحال، این وجوه مفهومی کارکرد بایستی رویه‌های اصولی ضروری از ارزیابی را که به‌منظور تعیین نمودن مخاطرات امنیتی موجود در سناریو هر شبکه خاص، ضروری هستند،

[1] Directory

یاری نمایند. هر وجه با ارزش در این چارچوب امنیتی مفهومی می‌بایست به صورت مجزا مدیریت شود و تمام این وجوه بایستی به صورت جمعی نیز مدیریت شوند تا اطمینان حاصل شود که اهداف کلی یک شبکه امن حاصل شده است.

۱۳-۴-۳- نقش‌ها و مسولیت‌ها

نقش‌ها و مسولیت‌هایی که بایستی در ارتباط با مدیریت امنیت شبکه ایجاد شود به صورت زیر است (لازم به ذکر است که، با توجه به اندازه سازمان، ممکن است این نقش‌ها با یکدیگر ترکیب شوند).

مدیریت ارشد:

- تعریف اهداف امنیت سازمان،
- راه‌اندازی، تصویب، انتشار و اعمالِ خط‌مشی امنیتی سازمان، روش‌ها و قوانین،
- راه‌اندازی، تصویب، انتشار، و اعمال خط‌مشی کاربردی قابل پذیرش سازمان،
- حصول اطمینان از اینکه امنیت و خط مشی‌های کاربردی قابل پذیرش، اعمال می‌شوند،
- مدیریت شبکه:
- تدوین خط‌مشی امنیتی شبکه بتفصیل،
- پیاده‌سازی خط‌مشی امنیتی شبکه،
- پیاده‌سازی خط‌مشی کاربردی قابل پذیرش،
- مدیریت روابط واسط با ذی‌نفعان/ ارایه‌کنندگان سرویس خارجی، به‌منظور حصول اطمینان ار انطباق با خط مشی‌های امنیتی داخلی و خارجی شبکه،

گروه امنیت شبکه:

- تعیین، تدوین، آزمون، بررسی، حفظ و پشتیبانی از مؤلفه‌ها و ابزارهای امنیتی،
- پشتیبانی از ابزارها و مؤلفه‌های امنیتی به‌منظور پیگیری سیر تکاملی تهدیدات به‌طور دقیق، (به‌عنوان مثال به‌روزرسانی فایل‌های امضای ویروسی)،
- به‌روزآمدی پیکربندی‌های امنیتی (به‌عنوان مثال فایل‌های کنترل دسترسی) مطابق با تغییرات الزامات کسب‌وکار ،

مدیران اجرایی شبکه:

- نصب، به‌روزرسانی، استفاده و حفاظت از سرویس‌های امنیتی شبکه و مؤلفه‌های آن،
- انجام وظایف روزانه لازم، برای اعمال مشخصات، قوانین و پارامترهای امنیتی موردنیاز خط مشی‌های امنیتی در حال اجرا،
- به‌کارگیری تمهیدات مناسب، به‌منظور حصول اطمینان از حفاظت از مولفه‌های امنیت شبکه (به‌عنوان مثال اعم از تهیه فایل‌های پشتیبان، پایش فعالیت‌های شبکه، واکنش در برابر حوادث و اخطارها)

کاربران شبکه:

- اعلام الزامات امنیتی خود،

- مطابقت با خط‌مشی امنیتی سازمان،
- مطابقت با خط مشی‌های کاربردی قابل پذیرش سازمانی که مرتبط با منابع شبکه هستند،
- گزارش حوادث امنیتی شبکه،
- ارایه بازخورد از تاثیرات امنیتی شبکه،

ممیزان (داخلی و/ یا خارجی):

- بازنگری و ممیزی (به‌عنوان مثال آزمودن اثربخشی امنیت شبکه به‌طور دوره‌ای)،
- بررسی مطابقت سامانه‌ها با خط‌مشی امنیتی شبکه،
- بررسی و آزمودن سازگاری قوانین امنیتی اجرایی با الزامات رایج کسب‌وکار و محدودیت‌های قانونی (به‌عنوان مثال فهرست‌های مربوط به دسترسی‌های مجاز شبکه).

۱۳-۴-۴- پایش شبکه

پایش شبکه بخش بسیار مهمی از مدیریت امنیت شبکه است. این مطلب در بند ۱۳-۷ در زیر، به‌تفصیل بیان شده است.

۱۳-۴-۵- ارزیابی امنیت شبکه

امنیت شبکه یک مفهوم پویا است. لذا کارمندان بخش امنیت بایستی همواره به پیشرفت‌های صورت گرفته در زمینه امنیت توجه داشته باشند و اطمینان حاصل نمایند که هر شبکه با رایج‌ترین وصله‌ها و اصلاحات امنیتی که توسط فروشندگان فراهم می‌شود، به‌کار خود ادامه می‌دهد. همچنین بایستی اقداماتی برای ممیزی کنترل‌های امنیتی موجود با استفاده از معیارهای ارزیابی به‌طور دوره‌ای، صورت گیرد. این اقدامات شامل انجام آزمایشات امنیتی- پویش آسیب‌پذیری و غیره- هستند. توصیه می‌شود امنیت به‌عنوان یک ملاحظه اولیه در ارزیابی فناوری شبکه مورد توجه قرار گیرد.

۱۳-۵- مدیریت آسیب‌پذیری فنی

محیط‌های شبکه، همچون سایر سامانه‌های پیچیده، مصون از خطا نیستند. آسیب‌پذیری‌های فنی در مؤلفه‌هایی که به‌طور مکرر درشبکه مورد استفاده قرار می‌گیرند، موجود هستند و انتشار می‌یابند. سوءاستفاده از این آسیب‌پذیری‌های فنی، می‌تواند تاثیر منفی شدیدی در امنیت شبکه داشته باشد، که اغلب در حیطه‌های دسترسی پذیری و محرمانگی قابل مشاهده است. مدیریت آسیب‌پذیری فنی، بایستی کلیه مؤلفه‌های یک شبکه را تحت پوشش قرار دهد، و شامل موارد زیر باشد:

- به‌دست آوردن اطلاعات به‌موقع درمورد آسیب‌پذیری‌های فنی،
- ارزیابی میزان در معرض خطر بودن شبکه در برابر چنین آسیب‌پذیری‌ها،
- تعریف کنترل‌های مناسب برای آدرس‌دهی مخاطرات مربوطه، و
- پیاده‌سازی و تصدیق کنترل‌های تعریف شده.

لازمه مدیریت آسیب‌پذیری فنی، وجود یک فهرست کامل از کلیه مؤلفه‌های موجود در شبکه است، به‌گونه‌ای که با استفاده از آن اطلاعات فنی ضروری، مانند نوع وسیله، مشتری، شماره مدل سخت‌افزار، سفت‌افزار[1] یا نرم‌افزار، و همچنین اطلاعات شرکتی، نظیر مدیران اجرایی مسوول، فراهم شود.

اگر سازمانی یک برنامه کلی برای مدیریت آسیب‌پذیری تکنیکی تنظیم کرده‌باشد، لازم است یکپارچه‌سازی مدیریت آسیب‌پذیری تکنیکی مؤلفه‌های شبکه در قالب یک وظیفه کلی، به‌عنوان یک راه‌حل، در اولویت قرار گیرد. (اطلاعات بیشتر در زمینه مدیریت آسیب‌پذیری فنی، شامل راهنمایی‌هایی در زمینه پیاده‌سازی، در استاندارد ISO/IEC 17799 موجود است.)

۱۳-۶- شناسایی و احراز اصالت

۱۳-۶-۱- پس‌زمینه

حصول اطمینان از حفظ امنیت یک سرویس ارایه شده توسط شبکه و اطلاعات مربوط به آن، با محدود کردن دسترسی از طریق اتصالات به کارکنان مجاز (اتصالات به خارج سازمان یا داخل سازمان)، حایز اهمیت است. البته لازمه حفظ امنیت منحصراً، محدود کردن دسترسی به اتصالات شبکه نیست، و جزییات بیشتر در زمینه استفاده از اتصالات شبکه در استاندارد ISO/IEC 17799 موجود است و دراستاندارد ISO/IEC 13335-2 نیز پس از انتشار ارایه خواهد شد.

چهار ناحیه کنترلی که مربوط به استفاده از اتصالات شبکه هستند، و نیز سامانه‌های اطلاعاتی مرتبط با چنین اتصالاتی به‌طور مستقیم، در بندهای ۱۳-۶-۲ تا ۱۳-۶-۵ در زیر معرفی شده‌اند.

۱۳-۶-۲- ورود از راه دور

ورود به سامانه از راه دور، چه توسط کارکنانی که دور از سازمان کار می‌کنند و چه مهندسان بخش نگهداری راه دور یا کارکنان سایر سازمان‌ها، از طریق شماره‌گیری به سازمان، اتصالات اینترنت، شاهراه‌های[2] اختصاصی از سایر سازمان‌ها، یا دسترسی مشترک از طریق اینترنت، صورت می‌گیرد. این‌ها اتصالاتی هستند که بر حسب نیاز، توسط سامانه‌های داخلی یا شرکای قراردادی، با استفاده از شبکه‌های عمومی، دایر شده‌اند. لازم است در هرنوع ورود به سامانه راه دور، کنترل‌هایی اضافه و متناسب با ماهیت نوع اتصال، اعمال شود. نمونه‌هایی از این کنترل‌ها، به‌صورت زیر است:

- ممانعت از دسترسی مستقیم به سامانه و نرم‌افزار شبکه از طریق حساب‌های شخصی که برای دسترسی راه دور، مورد استفاده قرار می‌گیرند، غیر از مواردی که از فنون احراز اصالت اضافه استفاده شده است (به بند ۱۳-۶-۳ در زیر مراجعه شود)، و شاید رمزنگاری انتها به انتها صورت گرفته است.

[1] Firmware
[2] Trunk

- حفاظت از دسترسی غیر مجاز به اطلاعات مربوط به نرم‌افزار پست الکترونیکی و داده‌هایی که به‌طور مستقیم در PCها و رایانه‌های دستی، ذخیره شده و توسط کارکنان در خارج از یک سازمان مورد استفاده قرار می‌گیرد.

۱۳-۶-۳- ارتقاء احراز اصالت

استفاده از شناسه کاربر و کلمه عبور، یک شیوه ساده برای احراز اصالت کاربران است، ولی شناسه کاربر و کلمه عبور می‌توانند کشف و یا حدس‌زده شوند. راه‌های امن‌تر دیگری نیز به‌منظور احراز اصالت کاربران ، به‌ویژه کاربران راه دور موجود است. ارتقاء احراز اصالت، هنگامی مورد نیاز است که احتمال بالایی وجود دارد که یک شخص غیرمجاز به سامانه‌های حفاظت‌شده و مهم دسترسی پیدا کند. به‌عنوان مثال ممکن است این امر به‌دلیل دسترسی از طریق شبکه‌های عمومی صورت گرفته باشد و یا اینکه سامانه‌ای که از آن دسترسی صورت گرفته است خارج از کنترل مستقیم سازمان باشد (نظیر یک رایانه دستی).

در محل‌هایی که ارتقاء احراز اصالت روی اتصالات شبکه مورد نیاز است (به‌عنوان مثال به دلیل قرارداد) یا به‌دلیل وجود مخاطرات قابل توجیه باشد، لازم است سازمان، تقویت فرآیند احراز اصالت را از طریق اعمال کنترل‌های مناسب مدنظر قرار دهد.

نمونه‌های ساده‌ای که مورد استفاده قرار می‌گیرند:

- CLID، که با استفاده از آن شماره تلفن تماس‌گیرنده در دستگاه دریافت‌کننده، قابل رویت است. اگر چه CLID، به‌علت نمایش شناسه شخص تماس‌گیرنده حایز اهمیت است، ولی این شناسه قابل تقلید نیز است و لذا نباید به تنهایی و بدون استفاده از هیچ نوع دیگری از احراز اصالت، به‌عنوان یک شناسه معتبر مورد استفاده قرار گیرد. CLID اغلب به‌عنوان یک شناسه‌گر سریع در ایجاد پیوندهای پشتیبان (به‌ویژه از طریق ISDN) بین سایت‌ها مورد استفاده قرار می‌گیرد.
- اتصالات از طریق مودم که در صورت عدم استفاده قطع می‌شوند، و ارتباط تنها پس از تایید CLID برقرار می‌شود.

نمونه‌های پیچیده‌تر ولی حایز اهمیت، به‌ویژه در زمینه دسترسی راه دور به صورت زیر است:

- استفاده از سایر روش‌های شناسایی برای پشتیبانی از احراز اصالت کاربران نظیر نشانه‌های تصدیق شده راه دور و کارت‌های هوشمند (به‌عنوان مثال دستگاه‌های شناسایی‌کننده‌ای که به PCها متصل می‌شوند)، وسایل مولد دستی کلید یکباره[1]، و تسهیلات مبتنی بر زیست‌سنجی[2]،
- تضمین اینکه نشانه یا کارت فقط در صورت استفاده از حساب معتبر کاربران مجاز (و ترجیحاً در رایانه شخصی کاربر و محل/ نقطه دسترسی)، به درستی عمل می‌کند، به‌عنوان مثال هر شماره شناسه شخصی یا پروفایل زیست‌سنجی مربوطه.

به طورکلی این امر، احراز اصالت دوعاملی قوی نام دارد. اگر از نشانه‌ها استفاده می‌شود، یک کاربر باید PIN را بداند که نشانه با استفاده از این شماره، تولید یک مقدار احراز اصالتی[1] یکتا را امکان‌پذیر می‌سازد. در

[1] Hand Held One Time Pass Key Generator Devices
[2] Biometric

مورد کارت‌های هوشمند، این امر به معنی خودکار کردن استفاده از دسترسی نشانه است. به‌منظور "باز شدن"، لازم است کاربر پس از وارد نمودن کارت به دستگاه کارت خوان هوشمند، شماره شناسه شخصی را وارد نماید. ولی هنگامی‌که احراز اصالت توسط سامانه‌های مرکزی یا سامانه‌های راه دور مورد نیاز باشد، ممکن است کارت هوشمند به‌طور مستقیم فراخوانی شود تا با استفاده از کلیدی که در کارت هوشمند جایگذاری شده است به امضای داده (برای احراز اصالت) بپردازد.

۱۳-۶-۴- شناسایی سامانه راه دور

همان‌گونه که در بند ۱۳-۶-۳ عنوان شد، احراز اصالت بایستی از طریق تصدیق سامانه‌ای (و محل/ نقطه دسترسی آن) که دسترسی خارجی از طریق آن صورت می‌گیرد، ارتقاء یابد.
لازم به ذکر است که معماری‌های مختلف شبکه، توانایی‌های شناسایی هویت متفاوتی را ارایه می‌دهند. بنابراین یک سازمان با انتخاب یک معماری مناسب می‌تواند به ارتقاء احراز اصالت برای شبکه خود دست یابد که در این صورت لازم است تمام قابلیت‌های (جوانب) مربوط به کنترل‌های امنیتی معماری شبکه انتخاب‌شده، در نظر گرفته شود.

۱۳-۶-۵- ورود یک مرحله‌ای امن

زمانی‌که اتصالات شبکه برقرار می‌شود، کاربران با چندین نوع شناسایی و بررسی احراز اصالت مواجه می‌شوند. در چنین شرایطی، کاربران ممکن است به انجام اعمالی غیرامن نظیر یادداشت کردن کلمه‌های عبور یا استفاده مجدد از داده احراز اصالت، بپردازند. واردشدن امن یک‌مرحله‌ای به سامانه می‌تواند مخاطرات ناشی از چنین رفتارهایی را، از طریق کاهش تعداد کلمه‌های عبوری که کاربران بایستی به‌خاطر داشته باشند، کاهش دهد. علاوه بر کاهش مخاطرات، بهره‌وری کاربر نیز ممکن است بهبود یابد و بار کاری میز کمک مرتبط با راه‌اندازی مجدد رمزعبور، ممکن است کاهش یابد.

قابل ذکر است که نتایج حاصل از شکست واردشدن امن یک‌مرحله‌ای به سامانه، می‌تواند بسیار شدید باشد زیرا ممکن است نه تنها یک، بلکه چندین سامانه و برنامه کاربردی در معرض خطر قرار گیرند (که گاهی اوقات مخاطره "شاه‌کلید"[2] نامیده می‌شود).

از این‌رو ممکن است استفاده از سازوکارهایی قوی‌تر از سازوکارهای معمول احراز اصالت و شناسایی، مورد نیاز باشد و بهتر است که عمل شناسایی و احراز اصالت، از طریق توابع با امتیاز بالا (سطح سامانه) از یک رژیم ورود امن یک‌مرحله‌ای به سامانه، صورت گیرد.

۱۳-۷- پایش و واقعه‌نگاری ممیزی شبکه

اطمینان از میزان اثر بخشی امنیت شبکه حایز اهمیت است. این امر از طریق واقعه‌نگاری ممیزی و پایش پیوسته همراه با تشخیص سریع، رسیدگی و ارایه گزارش از رویدادها و حوادث امنیتی و در نهایت

---

[1] Authentication Value
[2] Keys To Kingdom

واکنش مناسب به آنها صورت می‌گیرد. بدون چنین فعالیتی، حصول اطمینان از موثر باقی ماندن کنترل‌های امنیتی شبکه و عدم وقوع حوادث امنیتی با تاثیرات منفی شدید در عملیات کسب‌وکار امکان‌پذیر نیست.

اطلاعات کافی ثبت ممیزی از شرایط خطا و رویدادهای معتبر بایستی ذخیره شوند تا در مواقع بازنگری، در هنگام بروز حوادث مشکوک و واقعی مورد استفاده قرار گیرند. با این حال حجم زیاد اطلاعات ممیزی ثبت‌شده، می‌تواند تحلیل را برای مدیریت بسیار سخت کند و کارایی را تحت‌تاثیر قرار دهد. آن‌چه که در طول زمان واقعاً ثبت می‌شود، بایستی مورد ملاحظه دقیق قرار گیرد. برای اتصالات شبکه بایستی ثبت‌های ممیزی که شامل رویدادهای زیر هستند، پشتیبانی شوند:

- تلاش‌های ناموفق ورود به سامانه راه دور به‌همراه ثبت زمان و تاریخ،
- رخدادهای احراز اصالت مجدد ناموفق(یا نشانه استفاده شده)،
- نقض‌های ترافیکی دروازه‌های امنیتی،
- تلاش‌های راه دور برای دسترسی به ثبت‌های ممیزی،
- اعلان‌ها/اخطارهای مدیریتی سامانه با تاثیرات امنیتی (به‌عنوان مثال دوگانه‌کردن آدرس IP، قطع مدار حامل)

در زمینه شبکه‌بندی، ثبت‌های ممیزی توسط تعدادی از منابع مانند مسیریاب‌ها، دیواره‌های آتش، IDS صورت می‌گیرد و به سرویس‌دهنده ممیزی مرکزی، برای یکپارچه‌سازی و تحلیل کامل، ارسال می‌شوند. همه‌ی ثبت‌های ممیزی بایستی هم در زمان واقعی و هم به صورت برون‌خطی آزمایش شوند. در زمان واقعی، ثبت‌ها ممکن است بر روی صفحه غلتان[1] نمایش داده شوند و برای اعلان حمله‌های بالقوه مورد استفاده قرار گیرند. تحلیل برون‌خطی، از آن جهت ضروری است که اجازه می‌دهد تصویر جامع‌تری از طریق تحلیل روندها، مشخص شود. وجود ضعف‌های اساسی در وقایع ثبت‌شده در دیواره آتش می‌تواند نخستین نشانه‌های یک حمله باشد که نشان‌دهنده فعالیت‌های کاوش‌گرانه دربرابر یک مقصد بالقوه است. یک IDS می‌تواند به‌صورت بلادرنگ، از یک امضا، حمله را تشخیص دهد. ازاین‌رو تاکید می‌شود که در انتخاب درست ابزارهای تحلیل ثبت ممیزی، به‌منظور به‌دست‌آوردن خروجی‌های سریع، متمرکز و قابل فهم، بایستی دقت زیادی صورت گیرد.

دنباله‌های ممیزی بایستی، بر حسب نیاز سازمان برای مدتی به صورت برخط نگهداری شوند، در این مدت بایستی تمام دنباله‌های ممیزی پشتیبان‌گیری شوند و به‌گونه‌ای ذخیره شوند که از یکپارچگی و دسترس‌پذیری آنها اطمینان حاصل شود. به عنوان مثال با استفاده از رسانه‌های WORM، مانند دیسک‌های فشرده. به‌علاوه ثبت‌های ممیزی اطلاعات حساس یا اطلاعاتی برای استفاده افرادی که قصد حمله به سامانه ازطریق اتصالات شبکه را دارند، را شامل می‌شود، از این‌رو مالکیت ثبت‌های ممیزی می‌تواند به عنوان مدرکی برای اثبات انتقالات از طریق شبکه، در مواقع اختلاف مورد استفاده قرار گیرد – و بنابراین به‌طورخاص برای حصول اطمینان در زمینه یکپارچگی و انکارناپذیری مورد نیاز هستند. بنابراین تمام ثبت‌های ممیزی بایستی به شیوه مناسبی حفاظت شوند که شامل از بین بردن دیسک‌های فشرده بایگانی در

[1] Rolling Screen

تاریخ معین است. دنباله‌های ممیزی بایستی برای مدت زمانی مطابق با الزامات سازمان و قوانین ملی به صورت امن، نگهداری شوند. همزمانی برای همه دنباله‌های ممیزی و سرویس‌دهندگان مرتبط، نیز حایز اهمیت است، به‌عنوان مثال استفاده از NTP، به ویژه برای دادگاه‌ها و استفاده از آن در پیگردهای قانونی.
پایش پیوسته، بایستی موارد زیر را پوشش دهد:

- ثبت‌های ممیزی اعم از دیواره‌های آتش، مسیریاب‌ها، سرویس‌دهنده‌ها،
- اعلان‌ها/اخطارها از ثبت‌های ممیزی مربوط به دیواره‌های آتش، مسیریاب‌ها، سرویس‌دهندگان به منظور آگاه ساختن از برخی رخدادهای معین، قبل از بروز آنها،
- خروجی‌های IDS،
- نتایج حاصل از فعالیت‌های پویشی امنیت شبکه،
- اطلاعات در مورد رخدادها و حوادثی که توسط کاربران و کارکنان پشتیبان گزارش می‌شود،

(و نیز نتایج حاصل از بازنگری‌های مطابقت امنیتی)

رویدادها ممکن است حوادث امنیتی پیش‌گیری‌شده نظیر ورود نادرست به سامانه باشند و یا واقعاً منجر به یک حادثه امنیتی شده باشند که درحال حاضر کشف شده‌اند، به‌عنوان مثال تشخیص کاربری که یک تغییر غیرمجاز در پایگاه داده ایجاد نموده است.

تاکید می‌شود که پایش شبکه بایستی کاملاً منطبق بر قوانین و مقررات ملی و بین المللی انجام گیرد. این امر شامل قوانینی برای حفاظت از داده‌ها و مقررات مربوط به ارگان‌هایی که وظیفه تحقیق و بازپرسی را بر عهده دارند، می باشد (بر طبق قانون همه کاربران بایستی از هرگونه پایش آنها، قبل از اعمال آن آگاه شوند). به عبارت کلی پایش بایستی مسوولانه صورت گیرد و نه برای استفاده موردی برای بازنگری رفتار کارمندان در کشورهایی با قوانین حریم خصوصی سطح پایین. بدیهی است که اقدامات انجام‌شده، بایستی منطبق با امنیت و خط مشی‌های حریم خصوصی سازمان باشد و رویه‌های مناسب متناظر با مسوولیت‌های مرتبط انجام پذیرند. اگر مدارک ثبت ممیزی در امور مربوط به جرایم یا پیگردها مورد استفاده قرار می‌گیرد، بایستی پایش و ثبت کردن ممیزی شبکه در حالت امن قانونی انجام شود.

اغلب کنترل‌های پایشی واقعه‌نگاری ممیزی مرتبط با اتصالات شبکه و سامانه‌های اطلاعاتی مربوطه مورد نیاز، در استانداردهای ISO/IEC 17799 و ISO/IEC 13335-2 ارایه شده‌اند و پس از انتشار در دسترس خواهد بود.

۱۳-۸- تشخیص نفوذ

با افزایش اتصالات شبکه، انجام اعمال زیر برای نفوذگران ساده‌تر خواهد شد:

- یافتن چندین راه برای نفوذ به یک سازمان یا سامانه‌ها و شبکه‌های اطلاعاتی جامعه،
- مخفی کردن نقطه شروع دسترسی خود و
- دسترسی از طریق شبکه‌ها و هدف قرار دادن سامانه‌های اطلاعاتی داخلی.

علاوه بر این، نفوذگران روز به روز خبره‌تر می‌شوند و فنون و ابزارهای پیشرفته‌تری برای حمله در اینترنت یا ادبیات باز[1] فراهم می‌شود. درحقیقت بسیاری از این ابزارها خودکار هستند و می‌توانند بسیار تاثیرگذار باشند و به سهولت حتی توسط افراد با تجربه محدود نیز به کار گرفته شوند.

برای بسیاری از سازمان‌ها پیش‌گیری از تمام نفوذهای بالقوه، از نظر اقتصادی مقرون به صرفه نیست، در نتیجه رخداد برخی از نفوذها امکان‌پذیر است. مخاطرات مرتبط با اغلب این نفوذها بایستی از طریق اجرای شناسایی و احراز اصالت مناسب، کنترل دسترسی منطقی و حسابرسی وکنترل‌های ممیزی و در صورت امکان همراه با قابلیت آشکارسازی نفوذها تعیین شوند. چنین قابلیتی، روشی برای پیش‌بینی نفوذها و شناسایی آنها در زمان واقعی و ایجاد هشدارهای مناسب را فراهم می‌نماید. به‌علاوه، جمع‌آوری اطلاعات محلی در مورد نفوذها و در نهایت یکپارچه‌سازی و تحلیل آنها و همچنین تحلیل الگوهای رفتاری/کاربردی طبیعی سامانه اطلاعاتی یک سازمان را، امکان‌پذیر می‌سازد.

ممکن است در بسیاری مواقع، وقوع رویدادی غیرمجاز یا ناخواسته، بدیهی باشد. به عنوان مثال به دلایلی ظاهراً نامعلوم، سرویس‌های شبکه تنزل کنند یا تعدادی دسترسی غیرمنتظره در زمان‌های نامعمول به شبکه صورت گیرد و یا سرویس‌های خاصی از شبکه مسدود شوند. در اغلب وضعیت‌ها، مهم است که تا حد امکان سریع، علت، شدت و قلمرو نفوذ شناخته شود.

قابل ذکر است که این قابلیت، پیچیده‌تر از ابزارها و روش‌های تحلیل ثبت ممیزی است که در بند ۷-۱۳ و بندهای مربوطه دراستانداردهای ISO/IEC 17799 و ISO/IEC 13335-2 پس از انتشار، به آن پرداخته شده است. اغلب قابلیت‌های کشف نفوذ موثر، از پس‌پردازش‌گرهای خاصی استفاده می‌کنند. این پردازش‌گرها با استفاده از قوانینی به تحلیل خودکار فعالیت‌های گذشته ثبت‌شده در دنباله‌های ممیزی می‌پردازند و از ثبت‌های دیگر برای پیش‌بینی نفوذها و همچنین تحلیل دنباله‌های ممیزی برای الگوهای شناخته‌شده رفتارهای مخرب یا رفتارهایی که از نوع یک کاربرد طبیعی نیستند، استفاده می‌کنند.

به این ترتیب یک IDS، سامانه‌ای برای کشف نفوذ در یک شبکه است. دو نوع IDS وجود دارد، شامل:

- IDS شبکه،
- HIDS،

IDS شبکه، بسته‌های شبکه را پایش می‌کند و با تطبیق الگوی حمله به یک پایگاه داده از الگوهای شناخته‌شده حمله، سعی در آشکارسازی یک نفوذگر می‌کند. یک مثال نمونه، جستجوی تعداد زیادی از درخواست‌های اتصالTCP(SYN) به درگاه‌های متفاوت روی ماشین هدف است. نتیجه این عمل، کشف این است که آیا فردی سعی در پویش درگاه TCP دارد یا خیر. یک IDS شبکه، با مشاهده گاه‌به‌گاه و نامنظم ترافیک شبکه، آن را بررسی می‌نماید.

HIDS، فعالیت‌های روی میزبان‌ها (سرویس‌دهندگان) را پایش می‌کند. به این صورت که ثبت‌های رویدادهای امنیتی را پایش می‌کند یا بررسی می‌کند که تغییراتی نظیر تغییر روی فایل‌های مهم سامانه، یا محل ثبت اطلاعات سامانه‌ها در سامانه رخ داده است یا خیر. دو نوع HIDS، وجود دارد:

[1] Open Literature

- بررسی‌کننده‌های یکپارچگی سامانه که فایل‌های و محل‌های ثبت اطلاعات سامانه را، پایش می‌کنند تا تغییرات رخداده توسط نفوذگران را کشف کنند.
- پایشگران فایل‌های ثبت (که فایل‌های ثبت سامانه را پایش می‌کنند). سیستم‌های عامل، به تولید رخدادهایی امنیتی در مورد مقوله‌های بحرانی امنیت، می‌پردازند، نظیر اینکه یک کاربر امتیازاتی را در سطح پایه به‌دست آورد.

در بعضی حالات واکنش‌ها در برابر نفوذهای کشف‌شده، در سامانه پیش‌گیری از نفوذ، به طور خودکار انجام می‌گیرد.

جزییات بیشتر در مورد تشخیص نفوذ، در استاندارد ISO/IEC 18043 ارایه شده است.

۱۳-۹- حفاظت در برابر کدهای مخرب

کاربران بایستی مطلع باشند که ممکن است کدهای مخرب که شامل ویروس‌ها هستند از طریق اتصالات شبکه به داخل محیط آن‌ها وارد شوند. کدهای مخرب می‌توانند موجب اجرای کارکردهای غیرمجاز در یک رایانه شوند (به عنوان مثال بمباران کردن یک هدف داده‌شده توسط پیام‌ها، در تاریخ و زمان معین)، به‌علاوه، این کدها در مواردی که برای یافتن دیگر میزبان‌های آسیب‌پذیر، تکرار می‌شوند، می‌توانند منابع ضروری را تخریب نمایند (به عنوان مثال فایل‌ها را حذف کنند). ممکن است کدهای مخرب، قبل از خراب کردن، کشف نشوند، مگر در صورت اعمال کنترل های مناسب. همچنین ممکن است این کدها موجب به خطر افتادن کنترل‌های امنیتی (نظیر به‌دست آوردن و فاش کردن کلمه‌های عبور)، افشا و تغییرات ناخواسته و از بین رفتن اطلاعات و/یا استفاده غیرمجاز از منابع سامانه شوند.

برخی از انواع کدهای مخرب بایستی به وسیله نرم‌افزار پویش‌گر ویژه‌ای، کشف و حذف شوند. پویش‌گرها برای برخی از انواع کدهای مخرب، در دیواره‌های آتش، سرویس‌دهندگان فایل، سرویس‌دهندگان نامه و ایستگاه‌های کاری موجود هستند. به‌علاوه، برای کشف کد مخرب جدید، اطمینان از اینکه نرم‌افزار پویش‌گر همواره به روز می‌شود، حایز اهمیت است. به هر حال بایستی کاربران و مدیران اجرایی آگاه شوند که اعتماد بر پویش‌گرها به‌تنهایی برای کشف تمام انواع کدهای مخرب (یا حتی تمام کدهای مخرب از یک نوع)، کافی نیست. زیرا شکل‌های جدید این کدها پیوسته در حال به وجود آمدن است. نوعاً فنون دیگری از کنترل به منظور تکمیل حفاظتی که توسط پویش‌گرها (جایی که وجود داشته باشند) صورت می‌گیرد، لازم است.

به‌طور کلی وظیفه نرم‌افزار ضد کد مخرب، پویش کردن داده‌ها و برنامه‌ها برای شناسایی الگوهای مشکوک مرتبط با ویروس‌ها، کرم‌ها و اسب‌های تراواست (به مجموعه این انواع بعضاً "بدافزار" گفته می‌شود). کتابخانه الگوهایی که باید پویش شوند، با نام امضاها شناخته می‌شود و بایستی در فواصل زمانی منظم یا هرگاه که امضاهای جدیدی برای هشدارهای نرم‌افزار مخرب خطرناک، به دست می‌آید، به روز شود. در زمینه دسترسی راه دور، بایستی نرم‌افزار ضدویروس روی سامانه‌های راه دور و نیز سرویس‌دهندگان روی سامانه مرکزی – مخصوصاً ویندوز و سرویس‌دهندگان پست الکترونیکی، اجرا شود.

به اطلاع کاربران و مدیران اجرایی سامانه‌های متصل به شبکه بایستی رسانده شود که مخاطرات نرم‌افزارهای مخرب هنگام برقراری ارتباط بخش‌های بیرونی از طریق پیوندهای خارجی، بیشتر از حد معمول است. برای کاربران و مدیران اجرایی بایستی دفترچه‌های راهنمایی تدوین شود تا رویه‌ها و فعالیت‌های کمینه کردن احتمال ایجاد کد مخرب را آموزش دهند.

بایستی کاربران و مدیران اجرایی برای ایجاد پیکربندی سامانه‌ها و کاربردهای مرتبط با اتصالات شبکه و نیز برای غیرفعال کردن کارکردهایی که ضروری نیستند، بسته به شرایط، دقت خاصی مبذول دارند (به‌عنوان مثال برنامه‌های کاربردی PCها به‌گونه‌ای قابل پیکربندی هستند که ماکروها به‌طور پیش‌فرض غیرفعال شوند و یا نیاز به تایید کاربر قبل از اجرا داشته باشند).

به‌علاوه، جزییات حفاظت در برابر کد مخرب در استاندارد ISO/IEC 17799 شرح داده شده است و همچنین در استاندارد ISO/IEC 13335-2 پس از انتشارموجود خواهد بود.

۱۳-۱۰- زیرساخت معمول سرویس‌های مبتنی بر رمزنگاری

۱۳-۱۰-۱- مقدمه

با جایگزین شدن فرم‌های الکترونیکی به جای همتاهای کاغذی، نیاز به امنیت و حریم خصوصی ارتقاءیافته، رو به افزایش است. ضرورت استفاده از اینترنت و وسعت یافتن شبکه‌های سازمانی که دسترسی مشتریان و تولیدکنندگان از خارج یک سازمان به آن را به‌دنبال خواهد داشت، تقاضا برای راه حل‌های مبتنی بر فنون رمزنگاری را شتاب بخشیده است. این فنون برای پشتیبانی از احراز اصالت و VPNها برای حصول اطمینان از محرمانگی به‌کار می روند.

۱۳-۱۰-۲- محرمانگی داده در شبکه‌ها

در محیط‌هایی که وجود محرمانگی اطلاعات در آنها حایز اهمیت است، لازم است فنون کنترلی رمزنگاری، برای به رمز در آوردن اطلاعات عبوری از اتصالات شبکه‌ها به کار رود. در استفاده از این فنون کنترلی رمزنگاری، بایستی توجه به قوانین و مقررات مربوطه حکومتی، الزامات مدیریت کلید و تناسب مکانیسم‌های رمزنگاری که برای انواع اتصالات درگیر شبکه استفاده می‌شوند و نیز درجه حفاظت مورد نیاز، لحاظ شود.

سازوکارهای رمزنگاری در ISO/IEC 18033، استاندارد شده‌اند. یک شیوه رایج رمزنگاری که با عنوان رمز قالبی شناخته می‌شود و روش‌های استفاده از رمزهای قالبی برای حفاظت توسط رمزنگاری،که تحت عنوان حالت‌های کاری شناخته می‌شود، در ISO/IEC 10116، استانداردسازی شده‌اند.

۱۳-۱۰-۳- یکپارچگی داده در شبکه‌ها

بایستی در محیط‌هایی که یکپارچگی داده مدّ نظر است، از فنون کنترلی امضای دیجیتالی و/یا یکپارچگی پیام برای حفاظت از داده‌هایی که در طول شبکه عبور می کنند، استفاده شود. فنون امضای

دیجیتالی در حفاظت، مشابه با فنون احراز اصالت پیام، عمل می‌کنند. ولی غیر از آن دارای خصوصیاتی هستند که می توانند رویه‌های انکارناپذیری را فعال نمایند (به بند ۱۳-۱۰-۴ مراجعه شود). استفاده از فنون کنترلی امضای دیجیتالی یا یکپارچگی پیام، بایستی با توجه به قوانین و مقررات مرتبط، زیرساخت‌های کلید عمومی، الزامات مدیریت کلید، مناسب بودن مکانیسم‌های مورد استفاده برای انواع اتصالات درگیر شبکه و درجه حفاظت مورد نیاز و نیز قابلیت اطمینان و اعتماد ثبت‌نام کاربران موجودیت‌های مرتبط با کلیدهای (تاییدشده در موارد مربوط) استفاده‌شده در پروتکل‌های امضای دیجیتالی، انجام گیرد.

فنون کنترلی یکپارچگی پیام که کدهای احراز اصالت پیام[1] نام دارند، در ISO/IEC 9797 و فنون امضای دیجیتالی در ISO/IEC 9796 و ISO/IEC 14888، استاندارد شده‌اند.

۱۳-۱۰-۴- انکارناپذیری

جایی که نیاز باشد اثباتی مستدل مبنی بر حمل و عبور اطلاعات از یک شبکه ارایه شود، بایستی کنترل‌هایی نظیر موارد زیر، مورد ملاحظه قرار گیرد:

- پروتکل‌های ارتباطی که تایید ثبت نام را ارایه می‌کنند؛
- پروتکل‌های کاربردی که به آدرس یا شناسه مبدا نیاز دارند و آنها را برای تعیین وجود این اطلاعات، مورد بررسی قرار دهند؛
- دروازه‌هایی که قالب‌های آدرس فرستنده و گیرنده را برای تصدیق نحوی و سازگاری با اطلاعات در فهرست‌یارهای مربوطه بررسی می‌کنند؛
- پروتکل‌هایی که تحویل از شبکه‌ها را تایید می‌کنند و از این جهت اجازه می دهند تا ترتیب اطلاعات مشخص شود.

جایی که مهم است که انتقال یا دریافت اطلاعات اثبات شود، بایستی این موضوع مورد بررسی قرار گیرد. تضمین بیشتر بایستی با استفاده از یک روش استاندارد امضای دیجیتال، به‌دست آید. زمانی که اثبات مبدا اطلاعات حایز اهمیت باشد، لازم است فرستندگان اطلاعات با استفاده از یک امضای دیجیتال استاندارد، اطلاعات را به شکل یک استاندارد رایج مهر کنند و زمانی که اثبات تحویل اطلاعات مورد نیاز باشد، بایستی فرستندگان یک پاسخ مهر شده با امضای دیجیتالی را درخواست نمایند.

اطلاعات بیشتر راجع به انکارناپذیری، در استانداردهای ISO/IEC 14516 و ISO/IEC 13888 ارایه شده است.

[1] Message Authentication Codes, Macs

۱۳-۱۰-۵- مدیریت کلید

۱۳-۱۰-۵-۱ دید کلی

مدیریت کلید به عنوان یک سرویس پایه برای تمام سرویس‌های رمزنگاری دیگر، اطمینان می‌دهد که تمام کلیدهای رمزنگاری ضروری، در مدت دوره حیات خود مدیریت شده و با یک شیوه امن، مورد استفاده قرار گیرند.

در حالی که در محیط‌های بسیارکوچک، مدیریت کلید تنها با تعداد کمی از اتصالات و با رویه‌های دستی سازمانی قابل حصول است (به‌عنوان نمونه تبادل دستی کلیدهای رمزنگاری متقارن)، در محیط‌های بزرگ‌تر نیاز به رویه‌هائی از قبل تعیین‌شده و خودکار است و استفاده از فناوری‌های رمزنگاری کلید عمومی/خصوصی در بسیاری از حالات مزایای زیادی را به‌دنبال خواهد داشت.

فناوری‌های رمزنگاری کلید عمومی/خصوصی یک مساله مهم در مورد فناوری‌های رمزنگاری متقارن را حل کرده‌اند. در فناوری‌های متقارن لازم است یک کلید یکسان در دو طرف ارتباط (که به آنها فناوری راز به اشتراک گذاشته نیز اتلاق می‌شود) به‌کار رود و بنابراین نیاز به یک انتقال کلید رمز متقارن وجود خواهد داشت. از آنجا که بایستی خود کلید رمز متقارن محرمانه بماند، لازم است یک کانال داده امن برای مبادله کلید ایجاد شود. فناوری‌های رمزنگاری کلید عمومی/خصوصی بر این مساله چنین فائق آمده‌اند که دو کلید تهیه کرده و تنها یکی را به طرف دیگر ارتباط منتقل می‌کنند. بنابراین به دلیل اینکه کلید منتقل‌شده دیگر محرمانه نیست (این کلید، کلید عمومی نام دارد)، می‌تواند در طول کانال‌های مخابراتی عمومی منتقل شود. کلید دیگر که منتقل نشده است، هنوز می تواند به صورت محرمانه پنداشته شود (به این کلید، کلید خصوصی می گویند).

در هر حال مشکلاتی همچنان باقی می‌مانند که اساساً شامل موارد زیر هستند:

- انتقال موثق کلید عمومی، یا اینکه چگونه کلید عمومی موجودیت‌های دیگر به صورت قابل اعتماد به‌دست آید؛
- حفاظت مناسب کلید خصوصی.

برای انتقال کلید عمومی، لازم است از دریافت کلیدی که موجودیت فرستنده، فرستاده است، توسط موجودیت گیرنده اطمینان حاصل شود. به عبارت دیگر لازم است انتقال موثق باشد، در غیر این صورت ممکن است یک مهاجم، کلید عمومی در حال انتقال را مشاهده کند و بتواند یک کلید شناخته شده را با آن مبادله کند (این حمله با نام " واسطه‌گرانه" نیز مشهور است).

چندین فن برای بررسی اعتبارکلید عمومی انتقالی، وجود دارند. واضح‌ترین راه، بررسی معادل بودن کلید عمومی فرستاده شده و دریافت شده است. این بررسی اغلب با مقایسه مقدار درهم ساخته[1] (در این زمینه اغلب به مقدار درهم ساز شده «اثر انگشت» گفته می‌شود) کلید فرستاده شده و کلید دریافتی و با یک روش متقابل انجام می‌شود. ممکن است موجودیتهای فرستنده و گیرنده کلید از کانال‌های جداگانه استفاده کنند

[1] Hash

(به عنوان مثال خط تلفن)، که در این صورت مهم است که کانال‌ها اجازه احراز اصالت مناسب را به موجودیت‌های فرستنده و گیرنده بدهند (به‌عنوان مثال موجودیت گیرنده بتواند موجودیت فرستنده را با تشخیص صوت، احراز اصالت نماید).

از آنجا که این روش دوطرفه مبادله کلید عمومی، تنها درصورتی کارآمد است که تعداد کمی از موجودیت‌هایی که ارتباط برقرار می‌کنند، درگیر باشند، این روش قابل توسعه به مقیاس‌های بالاتر نیست. این موضوع با معرفی زیرساخت‌هایی که برای هر موجودیت، کلید عمومی تهیه کرده و اعتبار کلیدهای عمومی تهیه‌شده را تایید می‌نمایند، قابل حل خواهد بود. چنین زیرساخت‌هایی که به‌طور نوعی PKI نام دارند، از اجزای گوناگونی تشکیل می‌شوند. موجودیت‌های جدیدی که به این زیرساخت می‌پیوندند، به‌وسیله یک مرجع متولی ثبت‌نام، ثبت نام می‌شوند. این مرجع ثبت‌نام وظیفه اصلی تصدیق شناسه مناسب موجودیت را برعهده دارد. پس از آن بر اساس چنین ثبت نامی، متولی صدور گواهی قادر خواهد بود کلید عمومی موجودیت را گواهی نماید و در این صورت سرویس‌های فهرست‌یار برای دردسترس قراردادن کلیدهای عمومی تاییدشده برای تمام موجودیت‌هایی که از سامانه استفاده می‌کنند، وجود خواهد داشت (اغلب به چنین کلیدهایی «گواهی« گفته می‌شود). از لحاظ فنی، یک گواهی شامل مجموعه‌ای کاملاً معلوم از مشخصات موجودیت (به‌عنوان مثال نام و آدرس‌های الکترونیکی کاربران موجودیت) وکلید عمومی موجودیت‌ها است. اعتبار این اطلاعات با امضاء دیجیتالی آنها توسط مرجع صدور گواهی تضمین می‌شود.

از آنجا که امنیت تمامی سرویس‌های رمزنگاری با استفاده از کلیدهای عمومی تامین و به‌وسیله PKI مبتنی بر اعتبار آنها، مدیریت می‌شود، زیر ساخت‌های کلید عمومی دارای الزامات امنیتی بسیار بالایی خواهند بود. به عنوان نمونه، اگر یک مهاجم به زیرساخت مرجع صدور گواهی دسترسی یابد، می‌تواند گواهی‌هایی به منظور استفاده شخصی موجودیت‌ها صادر نماید.

به علت دلایل عملکردی، لازم است بیشتر زیر ساخت‌های کلید عمومی به شبکه ضمیمه شوند و بنابراین به‌منظور برآوردن الزامات درجه بالای امنیتی PKI، بایستی کنترل‌های امنیتی شبکه‌ای مناسبی اتّخاذ شود. این کنترل‌های امنیتی در بسیاری حالات، مشتمل بر تأسیس یک شبکه اختصاصی برای مولفه‌های هسته PKI و حفاظت از این شبکه توسط دروازه‌های امنیتی مناسب یا دیواره‌های آتش هستند.

با توجه به اهمیت حفاظت مناسب از کلیدهای خصوصی، این حفاظت تاثیر حیاتی بر امنیت شبکه خواهد داشت، به این دلیل که اگر یک مهاجم به کلید خصوصی یک موجودیت دسترسی پیدا کند، قادر به استفاده شخصی از آن موجودیت خواهد بود. معمولاً بسته به الزامات امنیتی سازمان‌ها، محیط‌ها یا کاربردهای خاص، راه حل‌هایی امنیتی گوناگونی وجود دارد.

ساده‌ترین راه حل، حفاظت از کلید خصوصی به وسیله ذخیره آن در یک فرم رمزشده متقارن روی سامانه‌های موجودیت و یا در حالت کمی بهتر، روی یک رسانه پاک‌شدنی است. این راه حل دارای این مزیت مهم است که کاملاً مبتنی بر نرم‌افزار بوده و بنابراین می تواند به آسانی قابل پیاده‌سازی در اغلب محیط‌ها باشد. با این حال از نقطه نظر امنیتی چند اشکال عمده وجود دارد؛ به این ترتیب که حفاظت:

- وابسته به کیفیت کلمه عبور انتخاب شده است؛

- متکی به یکپارچگی سامانه استفاده شده توسط موجودیت است. اگر یک مهاجم بر این سامانه کنترل پیدا کند، قادر خواهد بود کلید خصوصی را که در طول پردازش توابع رمزنگاری به‌صورت رمز نشده در حافظه ذخیره شده است را کپی کند و یا ممکن است با به‌دست آوردن کلمه عبور و کلید عمومی به همان نتیجه در یک شکل رمزشده، دست یابد.

برای غلبه بر این مشکلات، راه حل‌های مبتنی بر کارت‌های هوشمند وجود دارند. این راه حل‌ها یک احراز اصالت دو عامله در دست‌یابی به کلید خصوصی ارایه می‌دهند (نوعاً داشتن کارت هوشمند و اطلاع داشتن از کلمه عبور یا شماره شناسه شخصی برای رمزگشایی آن). معماری این کارت‌ها به‌گونه‌ای است که اطمینان می‌دهد کلید خصوصی، هیچ‌گاه کارت هوشمند را ترک نمی‌کند (از روی کارت هوشمند پاک نمی‌شود)، به‌این معنا که تمام محاسبات هسته رمزنگاری که به کلید خصوصی نیاز دارند، روی خود کارت هوشمند پردازش می‌شوند. یک مزیت مهم این است که این راه حل از کلید خصوصی، حتی در وضعیت‌هایی که یکپارچگی سامانه استفاده شده توسط موجودیت، در معرض خطر است، حفاظت می نماید. اشکال اصلی راه‌حل‌های مبتنی بر کارت هوشمند، نیاز به توزیع و مجتمع‌سازی سخت‌افزار خاص مربوط به کارت هوشمند، برای موجودیت‌ها و سامانه‌های آنها است. اگرچه استانداردهایی فنی در این زمینه وجود دارد ولی این موضوع اغلب پیچیده و دارای فرایندی بسیار پرهزینه است.

تاکید می‌شود که این بند تنها یک چشم انداز اصلی از موضوع مدیریت کلید را ارایه کرده است. برای اطلاعات بیشتر در این زمینه و موضوعات مرتبط با آن نظیر PKI یا موضوعات با ارتباط بیشتر به مدیریت شناسه، به مراجع و متن‌های دیگر رجوع شود. مراجعی نظیر:

- ISO/IEC 11770- مدیریت کلید؛
- استاندارد ملی ایران شماره ۸-۱۱۰۸۷ - دایرکتوری: چارچوب‌های کلید عمومی و گواهی‌نامه نشان؛
- ISO 11166-2- بانکداری- مدیریت کلید با ابزار الگوریتم‌های نامتقارن؛
- ISO IS 11568- بانکداری- مدیریت کلید خرد؛
- ISO IS 11649 - بانکداری- مدیریت کلید چند مرکزی؛
- ISO IS 13492 - عناصر داده مدیریت کلید خرد[1]؛
- ISO IS 21118 - PKI بانکداری.

۱۳-۱۰-۵-۲ ملاحظات امنیتی

در زمینه مدیریت به‌ویژه در هنگام استفاده یا پیاده‌سازی سرویس‌های PKI، برخی ملاحظات امنیتی موجود است که لازم است مد نظر قرار گیرد.

این ملاحظات شامل عناوینی همچون:

- دامنه کاربرد- استفاده منظور شده از PKI تاثیر قابل توجهی در امنیت واقعی مورد نیاز دارد. به‌عنوان مثال، استفاده از گواهی‌نامه‌های صادرشده تاثیر عمده‌ای در الزامات امنیتی PKI دارد،

[1] Retail Key Management Data Elements

- خط مشی‌ها- سرویس‌های فراهم‌شده PKI و اهداف آنها، سطحی از حفاظت که در یک PKI پیاده‌سازی شده است و همچنین فرآیندهای تعاملی، به‌طور مناسب در یک خطی‌مشی صدور گواهی[1] و یک بیانیه اجرایی صدور گواهی [2]مستند شود،
- موضوعات مربوط به پیاده‌سازی- یک سازمان ممکن است، به پیاده‌سازی یک PKI در درون خود بپردازد، یا اینکه بخواهد سرویس‌های PKI را از بیرون خریداری کند و یا ممکن است بخواهد به پیاده‌سازی ترکیبی از این دو بپردازد (به‌عنوان مثال تنها سرویس‌های اصلی صدور گواهی را خریداری نماید، ولی سرویس‌های دیگری همچون فهرست‌یار جابه‌جایی[3] را به‌طور محلی پیاده‌سازی کند)،
- الزامات کارکردی خاص، به‌عنوان مثال برای کاربران جابه‌جا شونده[4]- بسیاری از الزامات کارکردی مستلزم کنترل‌های امنیتی خاص هستند. یک مثال در این زمینه، چگونگی حفاظت از کلیدهای خصوصی و دسترسی به گواهی‌نامه‌ها برای کاربران سیار است. از این‌رو یک راه‌حل در این زمینه، استفاده از کارت‌های هوشمند است (به مطلب شرح داده شده در زیر توجه کنید)،
- استفاده از کارت‌های هوشمند-کارت‌های هوشمند برای برآوردن الزامات امنیتی در سطح بالا (به‌عنوان مثال همان‌گونه که در بند ۱۳-۱۰-۵-۱ در بالا اشاره شد) یا برای حل موضوعات مرتبط با کاربران سیار مورد استفاده قرار می‌گیرند. البته قابل ذکر است که استفاده از کارت‌های هوشمند، خود نیازمند برخی ملاحظات اضافه، همچون فرآیند چرخه عمر کارت‌های هوشمند، توزیع فیزیکی و مدیریت کارت‌های هوشمند، فرآیندهای پشتیبانی (به‌عنوان مثال هنگامی که یک کاربر به جعل کارت هوشمند می‌پردازد) و موضوعات امنیتی مرتبط با دستگاهی که اطلاعات را از سخت‌افزار می‌خواند و همچنین یکپارچه سازی نرم‌افزار در سامانه مشتری، است که در زیر ذکر شده است،
- موضوعات عملیاتی، همچون عملکرد برخط/برون‌خط مرجع صدور گواهی ریشه[5]- تمهیدات عملیاتی خاص می‌تواند به‌منظور برآوردن الزامات خاص امنیتی مورد استفاده قرار گیرد. به‌عنوان مثال، خارج از خط کردن مرجع صدور گواهی اصلی هنگامی که سرویس‌های آن در حال استفاده نیستند، می‌تواند به همراه حفاظت فیزیکی کافی برای ارایه سطح بالاتری از حفاظت در زمینه بخش‌های حساس سامانه، مورد استفاده قرار گیرد.

---

[1] Certificate Policy, CP
[2] Certificate Practice Statement, CPS
[3] Roaming Directory
[4] Roaming Users
[5] Root Certification Authority

۱۳-۱۱- مدیریت تداوم کسب‌وکار

این مساله حایز اهمیت است که کنترل‌ها به گونه‌ای اعمال شوند تا از کارکرد پیوسته کسب‌وکار در مواقع بروز بلایا، از طریق ایجاد قابلیت بازیابی هر بخشی از کسب‌وکار که در اثر یک فاجعه و در یک مقطع زمانی از بین رفته است، اطمینان حاصل شود. از این‌رو یک سازمان باید دارای برنامه‌ای در زمینه مدیریت تداوم کسب‌وکار در محل، به همراه فرآیندهایی که تمام مراحل پیوستگی کسب‌وکار را تحت پوشش قرار می‌دهند - بر پایه اولویت‌های کسب‌وکار ، مقیاس‌های زمانی و نیازمندی‌ها (که توسط بازنگری تحلیل پیامد کسب‌وکار، پشتیبانی می‌شود)، تدوین راهبرد[1] تداوم کسب‌وکار، تهیه طرح تداوم کسب‌وکار، آزمودن طرح تداوم کسب‌وکار، حصول اطمینان ازاینکه تمام کارمندان از تداوم کسب‌وکار مطلع هستند، نگهداری مداوم از طرح تداوم کسب‌وکار و کاهش مخاطرات - باشد. فقط در صورت دنبال نمودن تمام این مراحل، می‌توان از حصول موارد زیر اطمینان حاصل نمود:

- اولویت‌های کسب‌وکار مورد نیاز و مقیاس‌های زمانی با نیازهای کسب‌وکار هم‌راستا هستند،
- گزینه‌های راهبردی تداوم کسب‌وکار ارجح با اولویت‌ها و مقیاس‌های زمانی متناسبند و بنابراین،
- طرح و تسهیلات صحیح و ضروری به‌کار گرفته و مورد آزمایش قرار می‌گیرند که این امر منجر به دربر گرفتن اطلاعات، فرآیندهای کسب‌وکار ، سامانه‌های اطلاعاتی و سرویس‌ها، ارتباطات صوت و داده، افراد و تسهیلات فیزیکی می‌شود.

راهنمائی‌هایی در زمینه مدیریت پیوستگی کسب‌وکار، شامل تدوین یک راهبرد پیوستگی کسب‌وکار مناسب و طرح‌های مربوطه، و در نهایت آزمایش نمودن و بررسی طرح‌ها، در استاندارد ISO/IEC 177799 موجود است و در استاندارد ISO/IEC 13335-2 پس از انتشار ارایه خواهد شد.

از نقطه‌نظر شبکه‌بندی، نگهداری اتصالات شبکه، پیاده‌سازی اتصالات جایگزین با ظرفیت کافی و همچنین بازیابی اتصالات پس از یک رویداد ناخواسته بایستی مورد توجه قرار گیرد. این جنبه‌ها و نیازمندی‌ها بایستی بر پایه اهمیت اتصالات روی عملکرد کسب‌وکار در طول زمان و پیامدهای تصویرشده منفی کسب‌وکار در صورت وقوع یک قطعی، باشد. با اینکه برقراری اتصال مزایای زیادی را برای یک سازمان به‌دنبال خواهد داشت، در هنگام وقوع یک قطعی، از نقطه نظر انعطاف‌پذیری و قدرت استفاده از رویکردهای سازنده، این اتصالات موجب ایجاد نقاط آسیب‌پذیری و "نقاط خرابی" خواهند شد که ممکن است پیامدهای مخرب بزرگی بر سازمان داشته باشد.

۱۴- پیاده‌سازی و اجرای کنترل‌های امنیتی

به محض اینکه معماری و کنترل‌های امنیتی فنی، مشخص و مستندسازی شده و مورد توافق قرار گرفتند، بایستی کنترل‌های امنیتی پیاده‌سازی شوند. علاوه بر این بایستی پیش از اینکه اجازه شروع به عملکردهای شبکه‌بندی داده شود، پیاده‌سازی‌ها بازنگری و آزمودن شوند و هرگونه نقص امنیتی معلوم و

[1] Strategy

مورد رسیدگی قرار گیرد (به بند ۱۵ مراجعه شود). سپس وقتی که امنیت شبکه تایید شد، عملیات جاری بایستی شروع شود. در طول زمان و اگر تغییر مهمی رخ دهد، آن‌گاه بازنگری‌هایی در مورد پیاده‌سازی مجدد، بایستی اجرا شود (به بند ۱۵ مراجعه شود).

۱۵- پایش و بازنگری پیاده‌سازی

همان‌طور که در بند ۱۴ بیان شد، اولین پیاده‌سازی بایستی مورد بازنگری قرار گیرد. این بازنگری برای بررسی تطبیق با معماری امنیتی فنی مستندشده و کنترل‌های امنیتی مشخص‌شده در سندهای زیر انجام می‌شود:

- معماری امنیتی فنی،
- خط‌مشی امنیتی شبکه‌بندی،
- رویه‌های عملیاتی امنیتی مربوطه،
- خط‌مشی (امنیتی) دسترسی به سرویس دروازه امنیتی،
- طرح‌های مربوط به تداوم کسب‌وکار،
- شرایط امنیتی برای اتصال در موارد مربوط.

بازنگری مطابقت بایستی قبل از عملیات جاری تکمیل شود. بازنگری هنگامی تکمیل می‌شود که تمام نقص‌ها توسط مدیر ارشد شناسایی، برطرف و خاتمه یابند. عملیات جاری بعدی، بایستی پایش مداوم و فعالیت‌های بازنگری، به‌ویژه قبل از یک ویرایش عمده جدید، به علت تغییرات مهم در الزامات کسب‌وکار، فناوری، راه‌حل‌های امنیتی و غیره انجام گیرد و در غیر این صورت به‌صورت سالیانه، صورت گیرد.

تاکید می‌شود که این بازنگری بایستی شامل پیش‌برد آزمون‌های امنیتی به‌سمت استانداردهای معین همراه با یک راهبرد آزمایشات امنیتی و طرح‌های متناظر از پیش ایجادشده و بیان‌کننده اینکه دقیقا چه آزمایش‌هایی، با چه ابزارهایی، کجا و چه زمانی انجام شوند، باشد. به‌طور معمول انجام این کار مشتمل بر ترکیبی از پویش آسیب‌پذیری و آزمایشات نفوذ خواهد بود. قبل از انجام هرگونه آزمایشی، بایستی به‌منظورحصول اطمینان از اینکه آزمایشات به روشی کاملاً سازگار با قوانین و مقررات انجام می‌شوند، برنامه آزمایش مورد بررسی قرار گیرد. هنگام انجام این بررسی، لازم است توجه شود که ممکن است شبکه محدود به یک کشور خاص نباشد به این معنا که ممکن است در کشورهای مختلف با قوانین متفاوت، توزیع شده باشد. پس از انجام آزمایشات، لازم است گزارشی مبنی بر تعیین مشخصات آسیب‌پذیری‌های سازمان و تعمیرات مورد نیاز و تقدم آنها، همراه با ضمیمه‌ای مؤید بر اینکه تمامی روش‌های رفع مورد توافق به‌کار رفته‌اند، ارایه شود. چنین گزارشاتی بایستی توسط مدیر ارشد امضا شوند.

مراجع

[1] ISO/IEC TR 14516:2002, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
[2] ISO/IEC 13888 (all parts), IT security techniques — Non-repudiation
[3] ISO/IEC 7498-1:1994, Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model
[4] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture
[5] ISO/IEC 7498-3:1997, Information technology — Open Systems Interconnection — Basic Reference Model: Naming and addressing
[6] ISO/IEC 7498-4:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework
[7] ISO/IEC 27005, Information technology — Information security risk management[1]
[8] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements
[9] ITU-T X.810|ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection —Security frameworks for open systems: Overview
[10] IETF Site Security Handbook (RFC 2196), September 1997
[11] IETF IP Security Document Roadmap (RFC 2411), November 1998.
[12] IETF Security Architecture for the Internet Protocol (RFC 2401), November 1998.
[13] IETF Address Allocation for Private Internets (RFC 1918), February 1996.
[14] IETF SNMP Security Protocols (RFC 1352), July 1992.
[15] IETF Internet Security Glossary (RFC 2828), May 2000.
http://www.ietf.org/rfc/rfc2828.txt
[16] NIST Special Publications 800 series on Computer Security, including:
_ NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Firewalls.

[1] در دست چاپ، (بازنگری ISO/IEC TR 13335-3:1998 و ISO/IEC TR 13335-4:2000)

ICS: 35.040

صفحه : ۸۸