INSO-ISO-IEC

27033-3

1st.Edition

2014

Identical with
ISO/IEC 27033-3:2010

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

استاندارد ایران-ایزو-آی ای سی

۲۷۰۳۳-۳

چاپ اول

۱۳۹۳

فناوری اطلاعات - فنون امنیتی- امنیت شبکه-

قسمت۳:

فرانامه‌های شبکه‌بندی مرجع - تهدیدها، فنون طراحی و مسائل کنترلی

Information technology — Security techniques — Network security

Part 3:

Reference networking scenarios — Threats, design techniques and control issues

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیردولتی حاصل می‌شود .پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع 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 به‌عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین‌شده تهیه می‌کنند در کمیته ملی طرح و بررسی و در صورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته‌شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به‌عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی‌شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

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

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی- امنیت شبکه-

قسمت۳:

فرانامه‌های شبکه‌بندی مرجع - تهدیدها، فنون طراحی و مسائل کنترلی»

رئیس:	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس مسئول سازمان فناوری اطلاعات ایران

دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار)	مدیرکل اداره خدمات ارزش‌افزوده سازمان فناوری اطلاعات ایران

اعضاء: (اسامی به ترتیب حروف الفبا)

جمیل پناه، ناصر (فوق‌لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق‌لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
طی نیا، رضا (فوق‌لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق‌لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
قسمتی، سیمین (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
مغانی، مهدی (فوق‌لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

ناظمی، اسلام
(دکتری کامپیوتر)
استادیار دانشگاه شهید بهشتی

نصیری آسایش، حمید رضا
(فوق لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

نیسی مینایی، آصف
(فوق‌لیسانس فناوری اطلاعات)
پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- فنون امنیتی- امنیت شبکه- قسمت۳: فرانامه‌های شبکه‌بندی مرجع - تهدیدها، فنون طراحی و مسائل کنترلی» که پیش نویس آن در کمیسیون های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و چهل و پنجمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۳/۰۳/۰۵ مورد تصویب قرار گرفته است ، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می شود .

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

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

ISO/IEC 27033-3:2010, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues.

فناوری اطلاعات- فنون امنیتی- امنیت شبکه- قسمت۳: فرانامه‌های شبکه‌بندی مرجع - تهدیدها، فنون طراحی و مسائل کنترلی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی، تعیین و توضیح تهدیدها، فنون طراحی و مسائل کنترلی مرتبط با فرانامه‌های[1] شبکه‌ی مرجع است. برای تمام فرانامه‌ها راهنمایی با جزئیات در مورد تهدیدهای امنیتی و فنون طراحی و کنترل‌های امنیتی لازم برای کاهش مخاطرات مرتبط است. درجای مناسب، به استانداردهای ISO/IEC 27033-4 تا ISO/IEC 27033-6 ارجاع داده شده است تا از تکرار مطالب آن مستندات پرهیز شود.

اطلاعات موجود در این قسمت از این سری استاندارد ملی برای استفاده در هنگام بازنگری گزینه‌های فنی معماری/طراحی امنیت و هنگام انتخاب و مستندسازی معماری/طراحی امنیت فنی ارجح، با توجه به استاندارد ISO/IEC 27033-2 است. اطلاعات ویژه‌ی برگزیده(به همراه اطلاعات برگزیده از استانداردهای ISO/IEC 27033-4 تا ISO/IEC 27033-6)، به مشخصات محیط شبکه تحت بازنگری وابسته خواهند بود، برای مثال فرانامه(ها)ی شبکه و موضوع(های) «فناوری» ویژه مورد نظر است.

به طور کلی این قسمت از این استاندارد ملی کمک قابل‌ملاحظه‌ای در تعریف جامع و پیاده‌سازی امنیت برای محیط شبکه‌ی هر سازمانی خواهد بود.

۲ مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary[2]

2-2 ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts[3]

1- Scenarios

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

۳- معادل این استاندارد به فارسی: استاندارد ملی ایران شماره ۱-۱۴۸۶۶: سال ۱۳۹۱،فناوری اطلاعات -فنون امنیتی -امنیت شبکه -قسمت ۱- مرور کلی و مفاهیم

۳ اصطلاحات و تعاریف

در این استاندارد ملی اصطلاحات و تعاریف ذکرشده در استاندارد ملی ایران به شماره‌ی ۱-۱۴۸۶۶ و استاندارد ملی ایران به شماره‌ی ۲۷۰۰۰ و مواردی که در زیر آمده است به‌کار می‌رود.

۳-۱

بدافزار[1]

نرم‌افزار مخرب[2]

به رسته‌ای[3] از نرم‌افزارها گفته می‌شود که با نیتی خرابکارانه طراحی شده‌اند و شامل ویژگی‌ها و قابلیت‌هایی هستند که می‌توانند به‌صورت بالقوه باعث آسیب مستقیم یا غیرمستقیم به کاربر و/یا سامانه‌ی رایانه‌ای کاربر شوند.

یادآوری- به استاندارد ISO/IEC 27032 مراجعه شود.

۳-۲

ناشفافی[4]

حفاظت از اطلاعاتی که ممکن است از مشاهده فعالیت‌های شبکه به‌دست آید. مانند استخراج نشانی‌های پایانگاهی[5] در تماس صدا روی پروتکل اینترنت (VoIP)[6]

یادآوری- ناشفّافی به این موضوع اشاره دارد که نیاز است علاوه بر حفاظت از اطلاعات از کنش‌ها[7] هم حفاظت شود.

۳-۳

برون‌سپاری[8]

کسب[9] خدمات توسط بهره‌بردار[10] به‌منظور اجرای فعالیت‌هایی که برای پشتیبانی از کارکردهای کسب‌وکار بهره-بردار مورد نیاز است.

۳-۴

مهندسی اجتماعی[11]

عمل اداره کردن افراد به‌منظور اجرای کنش‌ها یا افشای اطلاعات محرمانه است.

1- Malware
2- Malicious
3- Category
4- Opacity
5- End-point
6- Voice-over-Internet-Protocol
7- Actions
8- Outsourcing
9- Acquisition
10- Acquirer
11- Social Engineering

۴ کوته‌نوشت‌ها

در این استاندارد ملی کوته‌نوشت‌های زیر به‌کار می‌روند.

AAA	Authentication, Authorization and Accounting	احراز هویت، مجوزسنجی و پاسخگویی
DHCP	Dynamic Host Configuration Protocol	پروتکل پیکربندی میزبان پویا
DNS	Domain Name Service	خدمت نام دامنه
DNSSEC	DNS Security Extensions	گسترش‌های امنیت خدمت نام دامنه
DoS	Denial of Service	انکار خدمت
FTP	File Transfer Protocol	پروتکل انتقال پرونده
IDS	Intrusion Detection System	سامانه تشخیص نفوذ
IP	Internet Protocol	پروتکل اینترنت
IPSec	IP Security Protocol	پروتکل امنیت پروتکل اینترنت
OAM&P	Operations, Administration, Maintenance & Provisioning	عملیات، سرپرستی، نگهداری و تدارکات
OSI	Open Systems Interconnection	اتصال متقابل سامانه‌های باز
PDA	Personal Data Assistant	دستیار داده شخصی
PSTN	Public Switched Telephone Network	شبکه سودهی عمومی تلفن
QoS	Quality of Service	کیفیت خدمت
SIP	Session Initiation Protocol	پروتکل راه‌اندازی نشست
SMTP	Simple Mail Transfer Protocol	پروتکل انتقال نامه ساده
SNMP	Simple Network Management Protocol	پروتکل مدیریت شبکه ساده
SSL	Secure Socket Layer (Encryption and authentication protocol)	لایه دریچه امن(پروتکل احراز هویت و رمزگذاری)
VoIP	Voice over Internet Protocol	صدا مبتنی بر پروتکل اینترنت
VPN	Virtual Private Network	شبکه خصوصی مجازی

۵ ساختار سند

ساختار این استاندارد ملی از سری استانداردهای ۲۷۰۳۳ شامل موارد زیر است:

الف- مرور کلی رویکرد برای اشاره به امنیت در مورد هر فرانامه مرجع که در این قسمت از سری استانداردهای ملی ۲۷۰۳۳ فهرست شده است (بند ۶)؛

ب- بندی برای هر فرانامه مرجع (بندهای ۷ الی ۱۵) که موارد زیر را توصیف می‌کند:

– تهدیدها برای هر فرانامه مرجع،

–ارائه‌ی کنترل‌های امنیتی و فنون بر اساس رویکرد بند ۶.

فرانامه‌های موجود در این استاندارد ملی بر اساس چارچوب زیر مرتب شده‌اند. هدف ارزشیابی فرانامه‌های مفروض به‌عنوان کارکردی از موارد زیر است:

الف- نوع دسترسی کاربر، این‌که کاربر درون سازمان باشد یا یکی از کارکنانی باشد که از بیرون سازمان به منابع سازمان دسترسی پیدا می‌کند یا اینکه مصرف‌کننده، فروشنده یا شریک کسب‌وکار باشد و

ب- نوع منابع اطلاعاتی در دسترس که می‌توانند منابع باز، محدودشده[1] یا برون‌سپاری شده باشند.

بنابراین این چارچوب به ارائه‌ی ساختاری سازگار[2] کمک می‌کند و اضافه شدن فرانامه‌های جدید را قابل مدیریت می‌کند. همچنین این چارچوب نیاز به فرانامه‌های مختلفی را که در این استاندارد ملی از سری استانداردهای ۲۷۰۳۳ ارائه شده است، توجیه می‌کند.

جدول ۱- چارچوب مرتب‌سازی فرانامه‌های شبکه

		کاربران		
		درون	کارکنان از بیرون	بیرون
منابع اطلاعاتی دسترسی شده	باز	- خدمات دسترسی به اینترنت برای کارکنان - خدمات کسب‌وکار به کسب‌وکار		- خدمات کسب‌وکار به مشتری
	محدودشده	- خدمات همکاری ارتقاءیافته - خدمات کسب‌وکار به کسب‌وکار - قطعه‌بندی شبکه - پشتیبانی شبکه‌بندی برای منازل و دفاتر کسب‌وکار کوچک	- ارتباطات سیار - پشتیبانی شبکه‌ای برای کاربران در حال جابجایی	- خدمات همکاری ارتقاءیافته - خدمات کسب‌وکار به کسب‌وکار - خدمات کسب‌وکار به مشتری
	برون‌سپاری شده	- خدمات برون‌سپاری شده		- خدمات برون‌سپاری شده

بنابراین ترتیب فرانامه‌هایی که در این قسمت استاندارد ملی از سری ۲۷۰۳۳ آمده‌اند، به شرح زیر است:

- خدمات دسترسی به اینترنت برای کارکنان(بند ۷)؛
- خدمات کسب‌وکار به کسب‌وکار(بند ۸)؛
- خدمات کسب‌وکار به مشتری(بند۹)؛
- خدمات همکاری ارتقاءیافته(بند ۱۰)؛

1- Restricted
2- Consistent

- بخش‌بندی شبکه(بند ۱۱)؛
- پشتیبانی شبکه‌بندی برای منازل و دفاتر کسب‌وکار کوچک(بند ۱۲)؛
- ارتباطات سیار(بند ۱۳)؛
- پشتیبانی شبکه‌بندی برای کاربران در حال جابه‌جایی(بند ۱۴)؛
- خدمات برون‌سپاری شده(بند ۱۵).

۶ مرور کلی

راهنمایی که برای هر فرانامه شبکه‌ی مرجع شناسایی‌شده در این استاندارد ملی از سری ۲۷۰۳۳ ارائه شده است، بر پایه‌ی رویکرد زیر بنا شده است.

- مرور اطلاعات پس‌زمینه و دامنه کاربرد فرانامه.
- تشریح تهدیدهای مربوط به فرانامه.
- انجام تحلیل مخاطره برای آسیب‌پذیری‌های کشف‌شده.
- تحلیل تأثیر تجاری نشانی‌دهی آسیب‌پذیری‌ها.
- تعیین پیشنهادهای پیاده‌سازی برای امن‌سازی شبکه.

برای رسیدن به امنیت در هر شبکه، رویکردی مطلوب است که نظام‌مند[1] باشد و ارزشیابی سرتاسری[2] فراهم کند. پیچیدگی چنین تحلیلی، تابعی از ماهیت و اندازه‌ی شبکه‌ی موجود در دامنه کاربرد است. به‌هرحال با توجه به ماهیت رو به پیشرفت فناوری، روشگانی[3] سازگار برای مدیریت امنیت مهم است.

اولین موردی که باید در ارزیابی امنیت مورد نظر قرار گیرد، تعیین دارایی‌هایی است که نیاز به پشتیبانی دارند. این دارایی‌ها را می‌توان به‌طور عمده در رده‌های زیرساخت، خدمات و برنامه‌های کاربردی[4] قرار داد. بااین‌حال سازمان خود نیز می‌تواند رده‌های مخصوص به خود را تعریف کند اما تفکیک این رده‌ها بسیار مهم است چرا که در معرض قرارگرفتن[5] هر رده یا نوع دارایی در مقابل تهدیدها و حمله‌ها منحصربه‌فرد است. برای مثال اگر مسیریابی به‌عنوان دارایی زیرساخت و VoIP به‌عنوان خدمت به کاربر نهایی رده‌بندی شده باشند آن‌گاه حمله‌ی DoS به ملاحظات متفاوتی در هر مورد نیاز دارد. به طور مشخص مسیریاب به محافظت در مقابل سیلی از بسته‌های ساختگی[6] نیاز دارد که بر روی درگاه فیزیکی قرار می‌گیرد و می‌تواند مانع انتقال ترافیک قانونی شود یا آن را به تأخیر اندازد. به طور مشابه خدمت VoIP به محافظت از اطلاعات حساب/خدمت مشترک[7] در مقابل حذف یا خرابی به‌صورتی که مشترک قانونی از دسترسی به خدمت بازداشته نشود، نیاز دارد.

1- Systematic
2- End-to-End
3- Methodology
4- Application
5- Exposure
6- Bogus
7- Subscriber

امنیت شبکه همچنین مستلزم حفاظت از فعالیت‌هایی است که در شبکه از آن‌ها حمایت می‌شود. مانند فعالیت‌های مدیریتی، پیام‌های کنترل/علامت‌دهی[1] و داده‌ی کاربر نهایی(ثابت و در حال جابه‌جایی[2]). برای مثال مدیریت واسط کاربری گرافیکی(GUI)[3] در خطر افشا قرار بگیرد که نتیجه‌ی دسترسی غیرمجاز است (شناسه و گذرواژه‌ی سرپرست که به آسانی قابل حدس است). ترافیک مدیریت، خود نیز در خطر خرابی در اثر دستورات OA&M ساختگی است که به‌وسیله‌ی جعل[4] نشانی‌های IP سامانه انجام می‌شود. خطرهای دیگر افشاسازی در اثر دیدبانی[5] و یا خطر وقفه[6] در اثر حمله‌ی سیل‌گونه‌ی پیام است.

رویکرد شناسایی دارایی‌ها و فعالیت‌ها، ملاحظات پودمانی[7] و نظام‌مند تهدیدات را فعال می‌کند. تمام فرانامه‌های شبکه مرجع در برابر مجموعه‌ای از تهدیدهای شناخته‌شده امتحان شده‌اند تا معلوم شود چه تهدیدی کاربردپذیر است. پیوست ب فهرستی از تهدیدات صنعتی شناخته‌شده را ارائه می‌کند. البته بهتر است تصور نشود که این فهرست جامع است بلکه این فهرست می‌تواند نقطه شروعی برای تمام تحلیل‌ها باشد. هنگامی که نمایه‌ی[8] تهدید استخراج شد، آسیب‌پذیری‌ها مورد تحلیل قرار می‌گیرند تا تعیین شود که چگونه ممکن است تهدیدها در زمینه‌ی[9] دارایی مشخص مورد نظر تحقق یابند. چنین تحلیلی کمک می‌کند تا تعیین شود چه اقدامات کاهشی فراموش‌شده‌اند و چه اقدامات متقابلی نیاز است به‌کار گرفته شوند تا اهداف حفاظتی به‌دست آیند. یک اقدام متقابل احتمال موفقیت تهدید را کاهش می‌دهد و/یا از اثر آن می‌کاهد. تحلیل مخاطره به‌وسیله‌ی تحلیل مخاطراتی صورت می‌پذیرد که ناشی از آسیب‌پذیری‌های یافت شده‌اند. تحلیل اثر کسب‌وکار شامل تصمیمات کسب‌وکار پیش رو است که با توجه به چگونگی اشاره به هر آسیب‌پذیری صورت می‌پذیرد: اصلاح[10]، پذیرش مخاطره یا انتقال مخاطره.

طراحی اقدامات متقابل و پیاده‌سازی کنترل‌ها برای حفاظت از آسیب‌پذیری‌ها در مقابل تهدیدها بخشی از تمام روشگان‌های ارزیابی امنیتی است. مطابق با استانداردهای ملی ایران سری ۲۷۰۰۰، انتخاب و پیاده‌سازی کنترل‌های مربوط، برای حفاظت از دارایی‌ها/اطلاعات حیاتی است. استاندارد ملتزم به حفظ[11] محرمانگی، یکپارچگی و قابلیت دسترسی اطلاعات است و به طور مشخص عنوان می‌کند که مشخصات دیگری نیز مانند سندیت[12]، انکارناپذیری و اطمینان‌پذیری هم می‌تواند مطرح شود.

1- Signaling
2- Resident and In-Transit
3- Graphical user interface
4- Spoof
5- Sniffing
6- Interruption
7- Modular
8- Profile
9- Context
10- Remediate
11- Preservation
12- Authenticity

مجموعه مشخصات امنیتی که در زیر آمده است در این قسمت از این سری استاندارد ملی با شیوه‌ای هدفمند برای توسعه‌ی اقدامات کاهشی و اقدامات متقابل مورد استفاده قرار می‌گیرد. تعریف منطقی مورد نیاز برای هر مشخصه‌ی امنیتی (علاوه بر محرمانگی، یکپارچگی و قابلیت دسترسی) در زیر آمده است:

- محرمانگی در مورد حفاظت داده از افشاسازی غیرمجاز است.
- یکپارچگی در مورد نگهداری صحت و دقت داده و حفاظت از آن در مقابل تغییر[1]، حذف، ایجاد و همتاسازی[2] غیرمجاز است.
- قابلیت دسترسی در مورد اطمینان از نبود هیچ‌گونه مانعی برای دسترسی مجاز به عناصر شبکه، اطلاعات ذخیره‌شده، جریان‌های اطلاعات، خدمات و برنامه‌های کاربردی است.
- کنترل دسترسی با استفاده از احراز هویت و مجوزسنجی، کنترلی برای ایجاد دسترسی به افزاره‌ها و خدمات شبکه تأمین و تضمین می‌کند. فقط افراد و برنامه‌های کاربردی مجاز اجازه‌ی دسترسی به عناصر شبکه، اطلاعات ذخیره‌شده، جریان‌های اطلاعات، خدمات و برنامه‌های کاربردی را دارند. برای مثال در توسعه‌ی IPTV یکی از توصیه‌های امنیتی شناخته‌شده، از کار انداختن واسط اشکال‌زدایی[3] بر روی افزاره‌ی ست‌تاپ-باکس[4] مشترک است. این توصیه از ملاحظات مشخصه‌ی کنترل دسترسی به‌دست می‌آید. بازنگری مشخصات محرمانگی، یکپارچگی و قابلیت دسترسی نیز به توصیه‌ای غیر از این منجر نمی‌شود.
- احراز هویت در مورد تأیید و اثبات شناسه‌ی ادعایی کاربر یا طرف‌های ارتباطی برای زمانی است که توسط کنترل دسترسی برای مجوزسنجی مورد استفاده قرار می‌گیرد. هم‌چنین اطمینان می‌دهد که یک هستار[5] اقدام به دگرنمایی[6] و یا بازپخش[7] غیرمجاز ارتباط قبلی نکرده باشد. برای مثال فردی ممکن است به سامانه مدیریت شبکه دسترسی پیدا کند اما برای به‌روزرسانی سوابق خدماتی مشترک نیاز است احراز هویت شود. بنابراین توانایی اجرای فعالیت‌های مدیریتی شبکه تنها با استفاده از محرمانگی، یکپارچگی، قابلیت دسترسی و کنترل دسترسی قابل تضمین نیست.

یادآوری- در کنترل دسترسی مبتنی بر نقش، احراز هویت به کمک کاربری که نقش به وی واگذار شده است، جایگزین می‌شود.کنترل دسترسی، کاربری را که نقش مقدم برای واگذاری اجازه دسترسی دارد درستی‌سنجی می‌کند. به طور مشابه کنترل دسترسی، فهرستی از واگذاری اجازه‌ی دسترسی به هر آنچه مطابق با خطمشی است، می‌سازد. پس اگر شما الزامات خطمشی تطابق داشته باشید مجاز به دسترسی خواهید بود. در این مورد توابع احراز هویت و مجازشناسی تهی خواهند بود.

- امنیت ارتباط یا انتقال در مورد اطمینان از این است که اطلاعات فقط بین نقاط انتهایی مجاز در جریان باشد بدون اینکه تغییر مسیر[8] پیدا کند یا شنود[9] شود.

1- Modification
2- Replication
3- Debugging
4- Set top boxes
5- Entity
6- Masquerade
7- Replay
8- Divert
9- Intercept

- انکارناپذیری در مورد نگهداری از دنباله‌ی ممیزی[1] است که باعث می‌شود منشأ داده یا دلیل یک رویداد یا کنش غیرقابل‌انکار باشد. شناسایی یک شخص مجاز که یک کنش غیرمجاز بر روی یک داده محافظت‌شده انجام می‌دهد هیچ ربطی به محرمانگی، یکپارچگی و قابلیت دسترسی داده ندارد.
- ناشفافی در مورد حفاظت از اطلاعاتی است که ممکن است از مشاهده‌ی فعالیت‌های شبکه نتیجه شود. عدم وضوح نیاز به حفاظت از کنش‌ها را علاوه بر اطلاعات تشخیص می‌دهد. حفاظت از اطلاعات به‌وسیله‌ی محرمانگی تأمین می‌شود. حفاظت از مکالمه‌ی تلفنی بین شخص الف و ب از محرمانگی مکالمه‌ی آن‌ها حفاظت می‌کند. حفاظت از این موضوع که اصلاً شخص الف و ب تماس تلفنی با هم داشته‌اند ناشفافی را تضمین می‌کند.

در همه فرانامه‌هایی که در این قسمت از استاندارد ملی ایران سری ۲۷۰۳۳ توضیح داده شده‌اند به‌عنوان بخشی از مرحله فنون طراحی و کنترل امنیت تمام مشخصات امنیت مورد بازنگری قرار گرفته‌اند. جدول ۲ در زیر مثال‌هایی از سازوکارهای امنیت شبکه را که قابل پیاده‌سازی برای مشخصات امنیتی هستند و برای اقدامات کاهشی مخاطرات بالقوه انتخاب شده‌اند، نشان می‌دهد.

جدول ۲-نمونه فنون امنیت شبکه

ملاحظات امنیتی	سازوکارها/فنون امنیتی
کنترل دسترسی	سامانه‌ی نشانه‌ی[2] فیزیکی، فهرست‌های کنترل دسترسی(ACL)[3]، جداسازی وظایف
احراز هویت	ثبت ورود/گذرواژه ساده، گواهی‌های رقمی، امضای رقمی، CHAP، SSO،TLSv1.2
قابلیت دسترسی	افزونگی[4] و پشتیبان‌گیری[5]، دیواره‌های آتش، IDS/IPS(برای جلوگیری از DoS)، تداوم کسب‌وکار، شبکه و خدمات مدیریت شده با SLA ها
امنیت ارتباطات	IPSec / L2TP، خطوط خصوصی، شبکه‌های جدا از هم
محرمانگی	رمزنگاری(3DES, AES)، فهرست‌های کنترل دسترسی، اجازه[6]دسترسی به پرونده
یکپارچگی	IPSec HMACs(برای مثال SHA-256)، وارسی افزونگی چرخه‌ای، برنامه‌ی ضدویروس
انکارناپذیری	رویدادنگارها[7] ، کنترل دسترسی مبتنی بر نقش، امضاهای رقمی
ناشفافی	رمزنگاری سرآیندها (برای مثال VPN با حالت تونلIPSec)، NAT(برایIPv4)

در این قسمت از این استاندارد ملی، ملاحظات بالا در ذات طراحی و پیاده‌سازی بحث شده در متن هر فرانامه‌ی شبکه مرجع آمده‌اند. به طور معمول سازمان برای نیل به اهداف کسب‌وکار خود کنترل‌های مربوط را از استاندارد ملی ایران شماره ۲۷۰۰۲ انتخاب می‌کند و رهنمون‌های این قسمت از این استاندارد ملی در نظر گرفته شده‌اند تا ملاحظات لازم سطح شبکه را برای پیاده‌سازی کنترل‌های برگزیده تأمین نمایند.

1- Audit trail
2- Badge
3- Access Control Lists
4- Redundancy
5- Back-up
6- Permission
7- Log

۷ خدمات دسترسی به اینترنت برای کارکنان

۷-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که نیاز دارند برای کارکنانشان خدمات دسترسی به اینترنت تأمین کنند، این فرانامه را مورد نظر داشته باشند تا مطمئن شوند دسترسی فقط برای مقاصدی که به طور واضح شناسایی‌شده‌اند و مجاز هستند تأمین می‌شود نه دسترسی باز عمومی. نیاز است که در سازمان‌ها به مدیریت دسترسی برای جلوگیری از اتلاف پهنای باند و پاسخ‌دهی از نظر مسئولیت قانونی[1] در مواجهه با کاربری که دسترسی کنترل‌نشده‌ای به خدمات اینترنت دارد، اهمیت داده شود.

با توجه به گسترش قوانین در مورد اینترنت، کنترل دسترسی کارکنان به اینترنت نگرانی در حال رشدی است. ازاین‌رو سازمان‌ها وظیفه دارند خط‌مشی شفافی را برای استفاده از اینترنت ایجاد، پایش و اجرایی کنند. این کار از طریق ارزشیابی فرانامه‌های زیر و فراهم کردن دعاوی[2] مربوط به خط‌مشی قابل‌دسترسی است:

- اجازه دسترسی به اینترنت به دلایل مربوط به کسب‌وکار باشد؛
- اگر دسترسی به اینترنت در قالبی(محدود) برای مقاصد شخصی است، اجازه‌ی استفاده از چه خدماتی داده شده است.
- اگر خدمات همکاری ارتقاءیافته اجازه داده شده باشد.
- اگر کارکنان اجازه یافته باشند در کانال‌های گپ[3] و نظرآزمایی‌ها[4] و غیره شرکت کنند.

با وجود این که اغلب، خط‌مشی نوشته‌شده‌ای نقش بازدارندگی عمده‌ای را در برابر کاربری غیرقابل‌قبول اینترنت بازی می‌کند اما سازمان هنوز هم مورد هدف مخاطرات امنیت اطلاعات اساسی است. در بند زیر تهدیدهای امنیتی و توصیه‌هایی در مورد فنون طراحی و کنترل‌های امنیت برای کاهش مخاطرات ذکرشده توصیف شده است. این توصیف هم برای کاربر داخلی و هم کاربر داخلی به‌علاوه‌ی خارجی کاربرد دارد.

۷-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با خدمات دسترسی به اینترنت برای کارکنان عبارت‌اند از:

الف- حملات ویروسی و معرفی بدافزار:

- کارکنانی که از اینترنت استفاده می‌کنند هدفی ساده برای بدافزارها هستند که ممکن است منجر به خرابی یا از دست رفتن اطلاعات، از دست رفتن کنترل زیرساخت فناوری اطلاعات و مخاطره‌ی بسیار بزرگی برای امنیت شبکه سازمان شود.

- پرونده‌ها یا برنامه‌های بارگیری شده‌ی کاربر ممکن است حاوی کد مخرب باشد. با توجه به حضور همیشگی برنامه‌های کاربردی مانند پیام‌رسان فوری[5]، به اشتراک‌گذاری پرونده‌ی نظیر به نظیر و تلفن IP، کارکنانی که

1- Legal
2- Claim
3- Chat
4- Forum
5- Instant messaging

می‌توانند به‌صورت سهوی برنامه‌های کاربردی مخربی را بارگیری و نصب کنند و این برنامه‌ها می‌توانند موانع دفاعی شبکه را با استفاده از فنونی مانند چابکی درگاهی[1] (پرش میان درگاه‌های باز) و رمزنگاری دور بزنند. به‌علاوه برنامه‌های نظیر به نظیر این قابلیت را دارند که از آنها به‌عنوان کانال‌های پنهان برای شبکه‌های بات[2]، بهره‌جویی شود.

- آسیب‌پذیری‌های موجود در مرورگرهای وب یا دیگر برنامه‌های کاربردی تحت وب، ممکن است به‌وسیله بدافزارها مورد بهره‌جویی قرار گیرند و منجر به ویروسی شدن[3] یا نصب اسب‌های تروا شوند. هنگامی که آلودگی صورت گرفت ممکن است قابلیت دسترسی بر اثر فعالیت‌های انتشار ویروس که به هدف سرریز شبکه صورت می‌گیرد، آسیب ببیند. اسب‌های تراوا این قابلیت را دارند که دسترسی‌های بیرونی غیرمجازی را تأمین کنند که منجر به تخلف از محرمانگی می‌شود.

ب - نشت اطلاعات:

- برنامه‌های کاربردی که اجازه‌ی بارگذاری اطلاعات روی کارسازهای مبتنی بر وب را تأمین می‌کنند ممکن است منجر به انتقال کنترل‌نشده‌ی داده از درون سازمان به اینترنت شوند. اگر از نشست‌های رمزنگاری شده استفاده شود(مانند TLS) شاید رویدادنگاری چنین فعالیتی ممکن نباشد. مخاطرات امنیتی مشابهی نیز به هنگام اجرای کد انتقال‌پذیر احراز هویت نشده بر روی سامانه‌های درون سازمان پیش می‌آیند.

پ - استفاده و دسترسی غیرمجاز:

- از دست رفتن کنترل زیرساخت، سامانه‌ها و برنامه‌های کاربردی می‌تواند منجر به تقلب[4]، انکار خدمت و استفاده‌ی نادرست از امکانات شود.

ت - مسئولیت به سبب عدم انطباق مقررات[5]:

- مسئولیت حقوقی به سبب عدم انطباق با قانون‌گذاری[6] و الزامات[7] مقرراتی،

- عدم تطابق[8] با خط‌مشی مورد استفاده‌ی سازمان می‌تواند منجر به عدم انطباق با مقررات شود.

ث - کاهش قابلیت دسترسی به سبب پهنای ناکافی یا مشکلات پایداری:

- استفاده‌ی بیش از حد از خدمات پهنای باند بالا مانند رسانه جاری‌سازی[9] یا اشتراک‌گذاری پرونده‌ی نظیر به نظیر ممکن است باعث سرریز شبکه شود.

1- Port agility
2- Botnets
3- Virus Infection
4 - Fraud
5- Liability due to regulatory non-compliance
6- Legislation
7- Obligation
8- Non Conformance
9- Streaming

۳-۷ فنون و کنترل‌های طراحی امنیت

فنون طراحی امنیت و کنترل‌های مرتبط با خدمات دسترسی به اینترنت برای کارکنان در جدول ۳ بحث شده‌اند.

برای مخاطره‌ی امنیت مورد نظر، هر مشخصه‌ی امنیتی برای کاربردپذیری در کاهش مخاطره‌ی بازنگری و سپس در ستون دوم یک نمونه پیاده‌سازی فنی مربوط ارائه شده است. برای نمونه یکپارچگی، کنترل دسترسی و احراز هویت برای حفاظت در مقابل کدهای مخرب کاربردپذیر هستند.

جدول ۳- کنترل‌های امنیتی برای فرانامه دسترسی به اینترنت برای کارکنان

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
حملات ویروسی و معرفی بدافزار	
– یکپارچگی – کنترل دسترسی – احراز هویت	– فقط خدمات اینترنتی مرتبط به کارمند تأمین شود. از فهرست سیاه برای ارائه‌ی خدمات مجاز استفاده کنید تا به‌این‌ترتیب به کانال‌های گپ یا خدمات وب‌نامه یا پروتکل‌های شبکه‌بندی نظیر به نظیر اجازه داده‌نشود. – استفاده از برنامه‌ی ضدویروس روی دروازه‌ها برای اینترنت و پویش همه‌ی ترافیک از سمت اینترنت و به سمت آن. بهتر است پویش شامل تمام پروتکل‌های شبکه مجاز به استفاده باشد. اطمینان یابید که به طور خودکار به‌روزرسانی ضدویروس‌ها نصب می‌شود یا هنگام در دسترس بودن به‌روزرسانی‌ها به کاربر هشدار داده شود. – استفاده از برنامه‌ی ضدویروس بر روی تمام سامانه‌های کارخواه[1]، به‌خصوص آن‌هایی که توسط کارکنان برای اتصال به اینترنت به‌کار می‌رود. – پویش تمام پرونده‌ها و اطلاعات ذخیره‌شده برای یافتن ویروس، اسب تروا و سایر بدافزارها. – درستی‌سنجی یکپارچگی داده/پرونده با استفاده از الگوریتم‌هایی مانند چکیده‌ساز/جمع‌آزماها[2]، گواهی‌ها. – مسدود کردن[3] بالاپرها[4] و تبلیغات وب. – مسیردهی ترافیک مورد استفاده برای خدمات دسترسی به اینترنت به تعداد اندکی از دروازه‌های امنیتی کنترل‌شده. – احراز هویت محتوای فعال.
نشت اطلاعات	
– امنیت ارتباطات – یکپارچگی – کنترل دسترسی	– پیاده‌سازی پالایه‌ها برای کد سیار بر روی دروازه‌های متصل به اینترنت. – پذیرش کدهای سیار فقط از وب‌گاه‌های فهرست سفید غیرحساس. – فقط پذیرش کدهای سیار امضای رقمی‌شده توسط مراجع صدور گواهی مورد تأیید یا از

1- Client
2- Hash/Checksum
3- Blocking
4- Pop-up

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
	فروشندگان مورد تأیید، امکان گزینه‌های پیکربندی مربوطه در سمت کارخواه تأمین شود؛ برای نمونه مدیریت و پیاده‌سازی فعال فهرست سفیدی از کدهای اجازه‌داده شده که به‌وسیله مراجع صدور گواهی امضا شده‌اند.
استفاده و دسترسی غیرمجاز	
– کنترل دسترسی – انکارناپذیری	– تأمین خدمات اینترنتی فقط مربوط به کسب‌وکار با توجه به نیاز کارمند. استفاده از فهرست سیاه برای خدمات غیرمجاز، برای نمونه کانال‌های گپ یا خدمات وب‌نامه. پیاده‌سازی پالایه‌ها برای پروتکل‌های غیرمجاز مانند پروتکل‌های نظیر به نظیر شبکه‌بندی. – محدود ساختن استفاده از خدماتی که به سادگی قابلیت انتقال حجم بالایی از داده را فراهم می‌کنند. – اطمینان از اینکه رویدادنگاری و پایش مناسبی بر روی خدماتی اعمال شود که احتمال انتقال داده از آنها به اینترنت وجود دارد. – تعریف واضحی از کاربری مجاز و غیرمجاز دسترسی به اینترنت در خط‌مشی اختصاصی ارائه‌شود.(به الگوی نمونه در پیوست الف مراجعه شود). – اطمینان از آگاهی کاربر به‌وسیله تحصیل[1] و آموزش[2] کافی.
مسئولیت به سبب عدم انطباق مقررات	
– انکارناپذیری	رویدادنگارهای کارکرد، مُهرهای زمانی[3]. آگاهی و آموزش کاربر.
کاهش قابلیت دسترسی به سبب پهنای ناکافی یا مشکلات پایداری	
– یکپارچگی – قابلیت دسترسی	– مدیریت آسیب‌پذیری مناسب و وصله‌زنی آسیب‌پذیری‌ها درون قاب‌های زمانی[4] بر اساس بحرانی‌بودن آسیب‌پذیری. – توصیه می‌شود تمرکز مدیریت آسیب‌پذیری‌ها بر روی تمام سامانه‌های دریافت‌کننده‌ی ترافیک اینترنت باشد. هم بر روی لایه انتقال هم بر روی لایه برنامه‌کاربردی که شامل تمام سامانه‌های مورد استفاده در زمینه‌ی دروازه‌های اینترنت و همچنین تمام سامانه‌های کاربر نهایی است که برای خدمات دسترسی به اینترنت مورد استفاده قرار می‌گیرند به‌خصوص آنهایی که از سامانه‌ی عامل ویندوز استفاده می‌کنند. – تنظیم پهنای باند برای رسانه‌ی جریان‌سازی (تنها اگر در خطمشی کسب‌وکار اجازه داده‌شده باشد). – بهتر است شبکه و منابع سامانه مورد پایش قرار بگیرند(IDS، رویدادنگارها، ممیزی‌ها و غیره) تا رویدادهای سامانه، امنیت و عملیاتی آشکار شوند.

1- Education
2- Training
3- Time stamps
4- Timeframes

۸ خدمات «کسب‌وکار به کسب‌وکار»

۸-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که تراکنش‌هایی را با دیگر سازمان‌ها مانند تولیدکنندگان، عمده‌فروشان و خرده-فروشان، انجام می‌دهند این فرانامه را در نظر بگیرند.

به طور سنتی خدمات «کسب‌وکار به کسب‌وکار» به‌وسیله‌ی خطوط اجاره‌ای اختصاصی یا قطعه‌بندی شبکه پیاده‌سازی می‌شود. اینترنت و فناوری‌های مرتبط به طور یقین گزینه‌های بیشتری تأمین می‌کنند اما مخاطرات امنیتی جدیدی را نیز معرفی می‌کنند که در ارتباط با پیاده‌سازی‌های چنین خدماتی است. نمونه‌ی رشد یافته‌ی تجارت الکترونیک «کسب‌وکار به کسب‌وکار» به سازمان‌ها اجازه می‌دهد که کسب‌وکار را بر روی اینترنت انجام دهند و برنامه‌های کاربردی روی استفاده از اینترنت، برون‌نت یا هر دو تمرکز کنند تا برخلاف فرانامه »کسب‌وکار به مشتری» مشارکت کسب‌وکار را ارتقاء دهند به‌طوری که هستارها برای یکدیگر شناخته شده هستند و تمام کاربران ثبت‌شده‌اند.

به طور معمول خدمات «کسب‌وکار به کسب‌وکار» نیازمندی‌های مخصوص به خودشان را دارند. برای نمونه قابلیت دسترسی و اطمینان‌پذیری نیازمندی‌های بسیار مهمی هستند چنان‌که اغلب سازمان‌ها به طور مستقیم وابسته به «خدمات کسب‌وکار به کسب‌وکار» هستند.

هنگامی که از اینترنت به‌عنوان پایه‌ی اتصال شبکه برای پیاده‌سازی «خدمات کسب‌وکار به کسب‌وکار» استفاده می‌شود نیاز است الزاماتی مانند قابلیت دسترسی و اطمینان‌پذیری به گونه‌ای متفاوت از قبل سامان‌دهی شوند. سنجه‌های اثبات‌شده‌ای مانند فرضیاتی که در مورد کیفیت خدمات هستند برای خطوط اجاره‌ای دیگر قابل به‌کارگیری نیستند. مخاطرات امنیتی جدیدی هستند که نیاز است به‌وسیله فنون طراحی و کنترل‌های مناسب مرتفع گردند. تمرکز بر روی تقویت اعتماد بین سازمان‌ها با پیشگیری از دسترسی به داده غیرمجاز و جدا نگه‌داشتن سامانه‌های کسب‌وکار از یکدیگر است.

بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند، مرتفع کند.

۸-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با «خدمات کسب‌وکار به کسب‌وکار» به شرح زیر است:

الف- حمله ویروس و معرفی بدافزار:

- رفتار بدافزارها منجر به نفوذ به سامانه‌ها شده که این خود باعث ایجاد اختلال در اطلاعات حساس یا دسترسی غیرمجاز به آنها می‌شود.

- آسیب‌پذیری‌ها در مرورگرهای وب یا برنامه‌های کاربردی تحت وب ممکن است به‌وسیله بدافزار به کارگرفته شوند که نتیجه آن ویروسی شدن یا نصب اسب‌های تروا است.

ب- حمله‌های انکار خدمت و انکار خدمت توزیع‌شده به درگاه‌های کسب‌وکار به کسب‌وکار یا برون‌نت.

پ- حمله‌های خودی به‌وسیله شرکای کسب‌وکار مجاز.

ت- جعل[1] محتوای تراکنش (پیام‌ها به گیرنده مورد نظر نمی‌رسند یا داده در حین انتقال دست‌کاری می‌شوند).

۸-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با خدمات «کسب‌وکار به کسب‌وکار» با موارد زیر در ارتباط هستند:

جدول ۴- کنترل‌های امنیتی برای فرانامه «خدمات کسب‌وکار به کسب‌وکار»

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
حمله ویروس و معرفی بدافزار	
– یکپارچگی – کنترل دسترسی – احراز هویت	– استفاده از نرم‌افزار وارسی ویروس بر روی دروازه‌های متصل به اینترنت برای پویش تمام ترافیک از سمت اینترنت و به سمت آن. توصیه می‌شود پویش شامل تمام پروتکل‌های مجاز شبکه برای استفاده باشد و اطمینان حاصل شود که به طور خودکار به‌روزرسانی ضدویروس‌ها نصب می‌شود یا هنگام در دسترس بودن به‌روزرسانی‌ها به کاربر هشدار داده می‌شود. – پویش تمام پرونده‌ها و اطلاعات ذخیره‌شده برای یافتن ویروس، اسب تروا و سایر بدافزارها. – درستی‌سنجی یکپارچگی داده/پرونده با استفاده از الگوریتم‌هایی مانند چکیده‌ساز/جمع‌آزماها، گواهی‌ها. – مسدود کردن بالاپرها و تبلیغات وب. – مسیریابی ترافیک مورد استفاده برای خدمات دسترسی به اینترنت برای تعداد اندکی از دروازه‌های امنیتی کنترل‌شده. – احراز هویت محتوای فعال.
حمله‌های انکار خدمت	
– قابلیت دسترسی – ناشفافی	– غیرفعال کردن درگاه‌های پروتکل و خدمات برای جلوگیری از پاسخ آنها به پویش/کاوش[2] غیرمجاز که امکان بالقوه‌ی سیل ترافیک حمله انکار خدمت را دارد. – جلوگیری از انتشار اطلاعات تشریحی بر روی علائم هشدار به‌منظور جلوگیری از تأمین اطلاعات هدف‌گیری برای حمله‌کنندگان.
حمله‌های خودی	
– کنترل دسترسی – انکارناپذیری	– خط‌مشی امنیت خوش تعریف[3] برای مدیریت دسترسی(برای مدیریت رابطه کسب‌وکار). – نقش‌ها و مسئولیت‌های کاملاً شناسایی‌شده. – علائم هشدار سفارشی‌سازی شده. – محدودیت بر روی اختیارات ویژه[4]. – رویدادنگاری تراکنش‌های حیاتی/غیرحیاتی کاربران.

1- Forgery
2- Probe
3- Well defined
4- Privileges

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
جعل محتوای تراکنش	
– انکارناپذیری	– رویدادنگاری با جزئیات از تراکنش‌ها. – استفاده از امضاهای رقمی.

۹ خدمات کسب‌وکار به مشتری

۹-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که تراکنش‌هایی را با مشتریان انجام می‌دهند، این فرانامه را در نظر بگیرند.

خدمات «کسب‌وکار به مشتری» که به آنها خدمات کسب‌وکار الکترونیک نیز اطلاق می‌گردد شامل خدماتی مانند تجارت الکترونیکی[1]، بانکداری الکترونیکی و دولت الکترونیکی است. در خدمات «کسب‌وکار به مشتری» امنیت باید میان توانمندسازی[2] تراکنش و حفظ ارزش نمانام[3] و کسب‌وکار تعادل برقرار کند.

نیازمندی‌های امنیت اطلاعات مرتبط با مفاهیم زیر است:

الف- محرمانگی (به‌خصوص در مورد بانکداری الکترونیک)،

ب- احراز هویت،

پ- یکپارچگی،

ت- امنیت ارتباطات داده برای پشتیبانی مسیر تراکنش میان کاربر و تأمین‌کننده در جایی که کاربر نهایی انتظار دارد خدمت کسب‌وکار فراهم باشد. مقاومت در برابر حملات پیچیده (برای مثال حملات فردی در میان[4] یا فردی در مرورگر[5])،

ث- قابلیت دسترسی بعد بسیار مهمی برای تأمین‌کننده‌ی کسب‌وکار الکترونیک است.

مشخصه‌های امنیت اطلاعات شامل موارد زیراست:

– امنیت فقط بر روی سکوی[6] نهایی «ضمانت‌شده» است که به طور معمول تحت کنترل یک سازمان است. در جایی که محیط مناسبی برای پیاده‌سازی کنترل‌ها و نگهداری از سطح مناسبی از امنیت سکو فراهم می‌سازد.

– امنیت بر روی سکوی مشتری که اغلب رایانه شخصی است به طور معمول ضعیف است. بنابراین کنترل‌های پیاده‌سازی‌شده در چنین محیطی سخت‌تر است و چنین سکوهایی مخاطرات بسیاری را برای این

1- E-Commerce
2- Enabling
3- Brand
4- Man in the middle
5- Man in the browser
6- Platform

فرانامه دارند (بدون قید شرایطی برای مجموعه الزامات اتصال امن در قرارداد که تحمیل آن در چنین محیطی دشوار است).

در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی برای برطرف کردن مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی تشریح شده‌اند.

۹-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با خدمات «کسب‌وکار به مشتری» به شرح زیر است:

الف- حمله‌ی ویروسی و معرفی بدافزار:

- رفتار بدافزارها منجر به نفوذ به سامانه‌ها شده که این خود سبب بروز اختلال در اطلاعات حساس یا دسترسی غیرمجاز به آنها می‌شود.
- آسیب‌پذیری‌ها در مرورگرهای وب یا برنامه‌های کاربردی تحت وب ممکن است به‌وسیله بدافزار استفاده شوند که نتیجه‌ی آن ویروسی شدن یا نصب اسب‌های تروا است.

ب- دسترسی غیرمجاز:

- دسترسی غیرمجاز به دادگان انتهایی (برای مثال حمله‌های تزریق SQL، حمله‌های نبشته[1] سایت قلابی[2])؛
- برداشت از حساب که در واقع توانایی استخراج اطلاعات از حساب معتبر است بسته به اینکه برنامه کاربردی تحت وب به اقدامات یک کاربر احراز هویت شده چگونه پاسخ می‌دهد. اغلب از نبشته‌های خودکار برای برداشت شناسه‌های کاربری و نام‌های حساب معتبر استفاده می‌شود.
- دزدی شناسه برخط با استفاده از حملات مهندسی اجتماعی موفق(از طریق استفاده از فنون فریب‌کاری)، مانند حمله‌های صیادی[3] و حملات مبتنی بر DNS که کاربر را به یک کارساز وب کلاه‌بردار که به نظر قانونی می‌رسد اما در واقع چنین نیست، متصل می‌سازد؛
- دسترسی غیرمجاز به سامانه‌ها و شبکه‌ها با نیت مخرب به‌منظور رونوشت[4]، دست‌کاری[5] یا تخریب داده؛
- رمزگشایی غیرقانونی محتوا که منجر به تخلفات حق نشر و دزدی محتوا می‌شود.

پ- حملات انکار خدمت.

ت- جعل محتوای تراکنش(پیام‌ها به گیرنده مورد نظر نمی‌رسد یا داده در حین انتقال دست‌کاری می‌شود).

۹-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت مرتبط با خدمات کسب‌وکار به مشتری در جدول ۵ بحث شده‌اند.

1- Script
2- Cross-Site Scripting
3- Phishing attacks
4- Copy
5- Modify

جدول ۵- کنترل‌های امنیتی برای فرانامه خدمات کسب‌وکار به مشتری

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
حمله‌ی ویروسی و معرفی بدافزار	
– یکپارچگی – کنترل دسترسی – احراز هویت	– استفاده از نرم‌افزار وارسی ویروس روی دروازه‌های متصل به اینترنت برای پویش تمام ترافیک از سمت اینترنت و به سمت آن. توصیه می‌شود پویش شامل تمامی پروتکل‌های شبکه مجاز برای استفاده باشد. – پویش تمام پرونده‌ها و اطلاعات ذخیره‌شده برای یافتن ویروس، اسب تروا و سایر بدافزارها. – درستی‌سنجی یکپارچگی داده/پرونده با استفاده از الگوریتم‌هایی مانند چکیده‌ساز/جمع‌آزماها، گواهی‌ها. – مسدود کردن بالاپرها و تبلیغات وب. – مسیریابی ترافیک مورد استفاده برای خدمات دسترسی به اینترنت به تعداد اندکی از دروازه‌های امنیتی کنترل‌شده. – احراز هویت محتوای فعال.
دسترسی غیرمجاز	
– کنترل دسترسی – احراز هویت – محرمانگی – امنیت ارتباطات – یکپارچگی – ناشفافی	– محدود کردن اجازه برنامه‌های کاربردی تحت وب به هنگام دسترسی به دادگان‌های انتهایی. – قطعه‌بندی شبکه و ردیف‌های امنیتی موجود در مناطق غیرنظامی[1](DMZ) برای جلوگیری از یکی شدن مسیرهای اتصال جهت با دارایی‌های داده‌ای. – ثبت کاربر امن به‌منظور اطمینان از اینکه اعتبارنامه‌های[2] دسترسی فقط در اختیار افراد موثق[3] قرار بگیرد. مانند استفاده از مرجع ثبت مستقل در فرآیند. – احراز هویت با استفاده از گواهی‌های رقمی، گذرواژه‌ها، زیست‌سنجی یا کارت‌های هوشمند. – دیواره‌های آتش و فهرست‌های کنترل دسترسی برای جلوگیری از دسترسی کاربران غیرمجاز. – کنترل دسترسی مبتنی بر نقش برای محدود ساختن کارکردهای کاربر به آنهایی که مجاز به اجرای آن هستند. – سطوح مناسبی از رمزنگاری اطلاعات ذخیره‌شده. – اطمینان از امنیت میان مرورگرهای وب و کارسازهای وب با استفاده از فناوری‌هایی مانند SSLv3/TLS. – امن‌سازی ارتباطات خدمات وب اولیه به طور مثال با استفاده از پیام‌های SOAP[4]. – درستی‌سنجی یکپارچگی داده/پرونده با استفاده از الگوریتم‌هایی مانند چکیده‌ساز/جمع‌آزماها، گواهی‌ها.

1- Demilitarized Zone
2- Credential
3- Authentic
4- Simple Object Access Protocol

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
	– برای یکپارچگی سطح داده برنامه‌های کاربردی تحت وب URL ها،کوکی‌ها[1] یا عناصری به شکل پنهان: – رمزنگاری تمام داده‌ها(حتی اگر از SSLv3 استفاده می‌شود)؛ – استفاده از برچسب زمانی همراه متغیرها. – امضای رقمی یا استفاده از چکیده‌ساز کلیددار برای داده‌های حساس. – استفاده از پیشکار معکوس بین کارساز وب و شبکه بیرونی.
حملات انکار خدمت	
– قابلیت دسترسی – ناشفافی	– غیرفعال کردن درگاه‌های پروتکل و خدمات برای جلوگیری از پاسخ آنها به پویش/کاوش غیرمجاز که امکان بالقوه‌ی سیل ترافیکی حمله‌ی انکار خدمت رادارد. – جلوگیری از انتشار اطلاعات تشریحی بر روی علائم هشدار به‌منظور جلوگیری از تأمین اطلاعات هدف‌گذاری برای حمله‌کنندگان.
جعل محتوای تراکنش	
– انکارناپذیری	– رویدادنگاری‌های با جزییات از تراکنش‌ها. – استفاده از امضاهای رقمی.

۱۰ خدمات همکاری ارتقاءیافته

۱۰-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که خدماتی را به‌کار می‌گیرند که شامل چندین کارمند می‌شود، فرانامه زیر را در نظر بگیرند. مثال‌هایی از چنین خدماتی عبارت‌اند از:

- گروه‌افزار
- کارسازهای پرونده
- فهرست نامه‌نگاری
- خدمات مبتنی بر وب

خدمات همکاری ارتقاءیافته که ارتباطات و اشتراک‌گذاری اسناد مختلفی را یکپارچه می‌کند، جنبه‌ی بسیار مهمی برای محیط‌های کسب‌وکار است.

چنین خدمات همکاری به طور معمول تلفن تصویری، ارتباطات صوتی به‌وسیله‌ی کانال‌های گپ، سامانه‌های رایانامه، هم‌چنین به اشتراک‌گذاری مستندات و محیط‌های هم‌کاری[2] برخط را یکپارچه می‌کند.

1- Cookies
2- Co-Working

برای سازمان دو راه اساسی استفاده از چنین خدماتی وجود دارد:
الف- از آنها فقط به‌عنوان خدمات داخلی استفاده شود اما با این اشکال که شرکای خارجی دیگر نمی‌توانند از این خدمات استفاده کنند و غیره.
ب- استفاده از آنها به‌عنوان خدمات داخلی و خدمات خارج از سازمان. این نحوه‌ی استفاده از طرفی موجب منافع بیشتر برای سازمان می‌شود اما از طرف دیگر در مقایسه با استفاده‌ی داخلی، مخاطرات بیش‌تری دارد.
پیاده‌سازی خدمات ممکن است:

- درون‌سازمانی باشد یا
- به‌وسیله طرف سوم انجام شود.

اگر قرار است خدمات به‌صورت داخلی و خارجی مورد استفاده قرار گیرند، خرید چنین خدماتی از طرف سوم مناسب‌تر به نظر می‌رسد.
در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون طراحی و کنترل‌های امنیتی برای کاهش مخاطرات مرتبط در موارد کاربری داخلی و استفاده‌ی داخلی و خارجی توضیح داده شده است. کنترل‌های امنیتی در مورد مدیریت، علامت‌دهی و ترافیک کاربر اعمال می‌شوند.

۱۰-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مربوط به خدمات همکاری ارتقا یافته به شرح زیر هستند:
الف- دسترسی غیرمجاز که منجر به افشای اطلاعات حساس می‌شود:
- سوءاستفاده از ابزارهای همکاری برای به اشتراک‌گذاری غیرقانونی مواد حق‌نشردار[1]، حصول داده‌های محرمانه و کاربران را در معرض محتوا یا تبلیغات دروغین[2] ناخواسته قراردادن.
- تخلف از اصل ناشفافی به‌وسیله‌ی پایش الگوهای کاربری، هرزنویسی[3] و حملات شناسه‌ای.
ب- حمله‌ی ویروسی و معرفی بدافزار:
- توزیع و اجرای بدافزار با بهره‌گیری از منابع مشترک.
پ- کاهش قابلیت دسترسی به شبکه:
- ازدیاد بار شبکه به‌وسیله‌ی ایجاد ترافیک قانونی؛
- بهره‌گیری از آسیب‌پذیری‌های پروتکل‌های استفاده‌شده در خدمات همکاری.

۱۰-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با خدمات همکاری ارتقاءیافته، با موارد زیر در ارتباط هستند:

1- Copyrighted material
2- Propaganda
3- Spamming

جدول ۶- کنترل‌های امنیتی برای خدمات همکاری ارتقاءیافته

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
دسترسی غیرمجاز که منجر به افشای اطلاعات حساس می‌شود	
– کنترل دسترسی – احراز هویت – محرمانگی – امنیت ارتباطات – انکارناپذیری	– دسترسی مبتنی بر نقش به برنامه‌های کاربردی، شبکه‌ها و ذخیره‌سازی[1] – تخصیص کاربران با نقش‌های متفاوت به VLANهای متفاوت با مجوزهای متفاوت – خط‌مشی‌های مبتنی بر نقش برای حقوق استفاده و دسترسی به منابع، مانند برنامه‌های کاربردی که کاربر می‌تواند اجرا کند – فهرست‌های کنترل دسترسی – احراز هویت و مجوزسنجی قوی – VLAN برای مجازی‌سازی شبکه – IDS مبتنی بر میزبان – رمزنگاری داده
حملات ویروسی و معرفی بدافزار	
– یکپارچگی	– استفاده از نرم‌افزار انتقال صفحه‌نمایش[2] مانند کارسازهای پایانه‌ای[3] برای کمینه‌سازی ورود داده و بد افزار احتمالی به محیط همکاری
کاهش قابلیت دسترسی شبکه	
– قابلیت دسترسی	– استفاده از شبکه‌های ذخیره‌سازی مجازی به‌منظور بهبود قابلیت دسترسی و امنیت داده‌ها در حالت بدون استفاده، – جلوگیری از حذف اطلاعات با استفاده از ابزارهای نرم‌افزاری برای جلوگیری ازرونوشت/پچسبان[4] اطلاعات، بازداری از تلاش‌ها برای نوشتن روی رسانه‌ی متحرک یا چاپ، – نرم‌افزار پایش به‌منظور آشکارسازی تخلفات از خط‌مشی مانند تخلفات دسترسی برنامه‌های کاربردی و منابع دیگر شبکه

۱۱ قطعه‌بندی شبکه

۱۱-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که قصد دارند برای هم‌راستایی ساختار سازمانی با شبکه داخلی خود، آن را به چندین دامنه تقسیم کنند این فرانامه را در نظر بگیرند.

1- Storage
2- Screen
3- Terminal servers
4- Copy/Paste

قطعه‌بندی شبکه‌ها، فنّی است که می‌تواند برای افزایش کنترل‌های دسترسی سامانه و برنامه‌ی کاربردی مورد استفاده قرار گیرد. قطعه‌بندی شبکه می‌تواند برای گروه‌بندی انواع معینی از فعالیت، برنامه کاربردی یا سامانه‌ها استفاده شود به طریقی که دسترسی فقط برای افرادی که به آن بخش از شبکه دسترسی دارند، ممکن باشد. ازاین‌رو کنترل‌های دسترسی شبکه، سایر کنترل‌های دسترسی نقطه نهایی را افزایش می‌دهند و سطحی افزون از دفاع در عمق را فراهم می‌کنند. برای مثال قطعه‌بندی شبکه می‌تواند به‌عنوان موارد زیر استفاده شود:

- تفکیک توانمندی‌های اداری و نگهداری از روال دسترسی کاربر به برنامه‌های کاربردی کسب‌وکار؛
- تفکیک برنامه‌های کاربردی حیاتی از دیگر برنامه‌های کاربردی؛
- تفکیک دادگان‌ها از اغلب کاربران.

برای سازمان‌های چندملیتی، قانون‌گذاری خاص هر کشور تأثیر چشمگیری بر نیازمندی‌های امنیت اطلاعات دارد. برای پوشش نیازمندی‌های متفاوت امنیت اطلاعات در کشورهایی که سازمان در آنها کسب‌وکار انجام می‌دهد قطعه‌بندی شبکه می‌تواند رویکرد مؤثری باشد به‌طوری که مرزهای شبکه درون مرزهای کشور قرار گیرند. برای مثال در قانون‌گذاری یک کشور خاص ممکن است برای داده‌ی مشتری/کارخواه حفاظت خاصی لازم باشد و اجازه انتقال چنین داده‌ای را به کشور دیگری ندهد. این موضوع به طور معمول، به کنترل‌های امنیت اطلاعات نیاز دارد تا انطباق با چنین قانون‌گذاری را ضمانت کند.

در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند، مرتفع کند.

۱۱-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با قطعه‌بندی شبکه در سازمان‌های بین‌المللی برای برآوردن نیازمندی‌های انطباق در کشوری مشخص عبارت‌اند از:

الف- مسئولیت به سبب عدم انطباق مقررات؛

ب- نشت داده:

- رخنه در محرمانگی، برای مثال هنگامی که داده مشتری/کارخواه از کشورهایی دسترسی‌پذیر است که توصیه می‌شود از آنها دسترسی وجود نداشته‌باشد،
- رخنه در نیازمندی‌های حریم خصوصی در یک کشور خاص،
- انکار مخاطرات مرتبط که دلالت بر عدم برآورده‌سازی انتظارات مشتری/کارخواه را با توجه به محرمانگی یا ناشفافی، دارد.

۱۱-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با قطعه‌بندی شبکه در سازمان‌های بین‌المللی برای برآوردن نیازمندی‌های انطباق در کشوری خاص با موارد زیر در ارتباط هستند:

جدول ۷- کنترل‌های امنیتی برای قطعه‌بندی شبکه

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
مسئولیت به سبب عدم انطباق مقررات	
– ناشفافی محرمانگی	– خط مشی و آگاهی کاربر: – قوانین حریم خصوصی – فنون رمزنگاری مجاز[1] – قوانین ذخیره‌سازی و انتقال داده – قوانین شنود قانونی
نشت داده	
– کنترل دسترسی – احراز هویت – یکپارچگی	– دروازه‌های امنیتی – پیشکارهای سطح برنامه کاربردی – رمزنگاری داده

۱۲ پشتیبانی شبکه‌بندی برای دفاتر خانگی و کسب‌وکار کوچک

۱۲-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که نیاز دارند دسترسی به منابع داخلی را برای کارکنانشان در دفاتر خانگی و کوچک فراهم کنند فرانامه زیر را در نظر بگیرند.

برای دفاتر خانگی و کسب‌وکار کوچک اغلب لازم است که شبکه داخلی سازمان تا مکان استقرار این دفاتر گسترش یابد. هزینه‌ی این گسترش تا مکان استقرار این دفاتر مسئله‌ای حیاتی است. چرا که برگشت‌های سود/هزینه معمولاً هزینه‌های پیاده‌سازی زیادی ندارند. این بدین معنی است که محدودیت‌های هزینه‌ای روی کنترل‌های امنیتی برای امن‌سازی گسترش چنین شبکه‌ای مورد استفاده قرار می‌گیرند و به طور معمول از استفاده‌ی کنترل‌های امنیتی درون‌شبکه‌ای ایجاد شده‌ی مورد استفاده برای اتصال بخش‌های بزرگ‌تر درون‌نِت، جلوگیری می‌کنند.

در بسیاری از فرانامه‌های خانگی و کسب‌وکار کوچک، زیرساخت موجود می‌تواند هم استفاده‌ی شخصی و هم استفاده‌ی تجاری داشته‌باشد که این خود ممکن است به مخاطرات امنیت اطلاعات دیگری منجر شود.

در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی آمده است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند مرتفع کند.

1- Allowable

۱۲-۲ تهدیدهای امنیتی

الف- دسترسی غیرمجاز :

- پیکربندی ضعیف تنظیمات در تجهیزات دسترسی به شبکه، برای مثال در مسیریاب‌های دفتر خانگی و دفتر کوچک (SOHO)[1]،
- استفاده از تونل‌زنی مجزا[2]،
- نبود یا کمبود کنترل‌های امنیت فیزیکی،
- فرصت بیشتر با توجه به ماهیت «همیشه برخط» اتصال شبکه،
- استفاده از حساب‌های میهمان و تنظیمات پیش‌فرض.

ب- حملات ویروسی و معرفی بدافزار:

- تجهیزات شامل رایانه‌های شخصی استفاده‌شده در شبکه‌های دفاتر خانگی و کوچک که با کنترل‌های امنیتی نامناسب در حال کار هستند، برای مثال نبود یا ضعف حفاظت در مقابل بدافزار و غیره،
- مشکلات ناشی از تداخل محیط‌های حریم خصوصی و کسب‌وکار، برای مثال استفاده‌ی خصوصی از پروتکل-های با مخاطرات زیاد مانند پروتکل‌های به اشتراک‌گذاری نظیر به نظیر،
- شکست در وصله‌زنی[3]،
- دسترس‌پذیری می‌تواند تنها با یک بار ویروسی شدن به سبب فعالیت‌های انتشار ویروس که منجر به ازدیاد بار شبکه می‌شود به‌شدت تحت تأثیر قرار بگیرد.

پ- افشای غیرمجاز اطلاعات حساس:

- نبود رمزنگاری داده ذخیره‌شده روی سامانه‌ها و در حین انتقال در شبکه خانگی و کسب‌وکار کوچک،
- سوءاستفاده از امکانات دسترسی مانند دسترسی به WAN در شبکه خانگی و کسب‌وکار کوچک،
- عدم آگاهی و نبود آموزش در زمینه روش‌های امنیتی برای کاربران نهایی،
- نامعتبر بودن فرضیات راجع به حفاظت از درون‌نِت‌ها، با توجه به این که دروازه‌های شبکه در محیط‌های خانگی یا دفاتر کوچک همان سطح حفاظت دروازه‌های مورد استفاده در اتصال درون شبکه‌ای شعبه‌های دفاتر را ارائه نمی‌کند.

۱۲-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با پشتیبانی شبکه‌بندی برای دفاتر خانگی و کسب‌وکار کوچک به موارد زیر مربوط هستند:

1- Small Office and Home Office
2- Split-tunneling
3- Patching

جدول ۸- کنترل‌های امنیتی برای فرانامه پشتیبانی شبکه‌بندی برای منازل و دفاتر کسب‌وکار کوچک

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
دسترسی غیرمجاز	
– کنترل دسترسی – احراز هویت – امنیت ارتباطات	– از کار انداختن واسط‌های شبکه و خدماتی که مورد استفاده قرار نمی‌گیرند – نصب دیواره‌ی آتش میزبان، دور انداختن یا رد کردن تمام اتصال‌های ورودی از بیرون – حفاظت‌های فناوری و طراحی برای تونل‌زنی مجزا – توصیه می‌شود سامانه‌ها از گذرواژه‌های خالی، تهی یا پیش‌فرض استفاده نکنند. – توصیه به اجبار از استفاده از گذرواژه‌های قوی برای همه‌ی کاربران می‌شود. توصیه می‌شود دسترسی بی‌نام/میهمان جایز نباشد. – وارسی‌های انطباق فنی به‌منظور اطمینان از پیکربندی و برپایی مناسب تمام تجهیزات حساس امنیتی، برای مثال مسیریاب یا نقاط دسترسی WLAN – فناوری‌های شبکه خصوصی مجازی امن در مؤلفه‌های دسترسی به شبکه مانند مسیریاب‌های دسترسی به شبکه
حملات ویروسی و معرفی بدافزار	
– یکپارچگی – قابلیت دسترسی	– نگهداری از نسخه‌های فعلی نرم‌افزار و سطوح وصله‌ها – حصول اطمینان از نصب خودکار به‌روزرسانی ضدویروس‌ها یا هشدار به کاربر هنگام در دسترس بودن به‌روزرسانی‌ها – استفاده از سامانه تشخیص نفوذ مبتنی بر میزبان (HIDS)[1] که به‌صورت کمینه، یکپارچگی نرم-افزار/دادگان را آشکار می‌کند (اگر کاربردپذیر باشد) – پویش تمام پرونده‌ها و اطلاعات ذخیره‌شده برای یافتن ویروس، اسب تروا و سایر بدافزارها – پشتیبان‌گیری از داده‌های پیکربندی و پرونده‌ها به‌منظور پاسخ به رخداد و بازیابی
افشای غیرمجاز اطلاعات حساس	
– محرمانگی – ناشفافی	– آگاهی و آموزش کاربران با بهترین روش‌های امنیتی – رمزنگاری داده‌های ذخیره‌شده و منتقل‌شده

۱۳ ارتباطات سیار

۱۳-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که مجاز به استفاده از افزاره‌های سیار برای کارکنان هستند، این فرانامه را در نظر بگیرند.

1- Host based Intrusion Detection System

این فرانامه بر روی ملاحظات امنیتی سازمان‌هایی تمرکز می‌کند که افزاره‌ها و برنامه‌های کاربردی سیار را به‌کار می‌گیرند. محرک اصلی توسعه سریع افزاره‌های سیار مانند تلفن‌های هوشمند یا دستیارهای داده شخصی (PDAs)[1] ناشی از بازار مصرف‌کننده است. همچنین این افزاره‌ها در محیط‌های کسب‌وکار استفاده می‌شوند. اغلب چنین افزاره‌هایی مالکیت شخصی دارند و هم برای اهداف کسب‌وکار و هم برای اهداف خصوصی مورد استفاده قرار می‌گیرند. در برخی موارد ممکن است افزاره‌ها توسط مؤسسه تأمین و برای اهداف شخصی استفاده شوند. بنابراین نیاز است افزاره‌هایی که روانه بازار کسب‌وکار می‌شوند ویژگی‌هایی را به بازار مصرف‌کننده نیز معرفی کنند چرا که فروشندگان قصد دارند تا در حد امکان در بازار رقابتی، سهم کسب‌وکار بیشتری به‌دست‌آورند.

افزاره‌های ارتباطات سیار اجازه می‌دهند که کاربران راه دور با دادگان‌های شخصی هم‌زمان شوند و دسترسی به خدمات شبکه را مانند رایانامه‌ی بی‌سیم، مرور وب و دسترسی به اینترنت فراهم کنند. هنگامی که شخصی از یک افزاره هم برای اهداف خصوصی و هم برای اهداف کسب‌وکار استفاده کند همواره این تمایل وجود دارد که خط‌مشی‌ها را دور بزند یا آنها را نادیده بگیرد و این‌گونه سازمان را با مخاطرات امنیت اطلاعات فراوانی روبرو - کند.

در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی آمده است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند مرتفع کند.

۲-۱۳ تهدیدهای امنیتی

الف- دسترسی غیرمجاز به اطلاعات ذخیره شده روی افزاره‌های سیار به دلیل:

- کنترل دسترسی یا حفاظت نامناسب از اطلاعات حساس ،
- عدم آگاهی و استفاده از گذرواژه‌های نامناسب،
- پیکربندی ضعیف،
- حملات دزدی به‌وسیله افزاره‌های تقلبی،
- نبود آگاهی کاربر نهایی از الزامات حفاظت امنیت اطلاعات مانند درهم آمیختن اطلاعات خصوصی و کسب-وکار.

ب- افشای غیرمجاز داده‌های حساس و اطلاعات مکانی:

- خدمات مبتنی بر مکان می‌تواند اطلاعات موقعیت کاربر را برای طرف‌های سوم غیرمجاز افشا کند که منجر به نگرانی‌هایی در مورد حریم خصوصی می‌شود،
- شنود غیرمجاز[2]،
- دخالت طرف‌های سوم با حفاظت نامناسب در جریان‌های ارتباطی،
- استفاده از متن رمز نشده یا پروتکل‌های انتقال با حفاظت نامناسب،

1- Personal Data Assistant
2- Eavesdrop

- روش امحای[1] نامناسب.

پ- دست‌کاری/حذف غیرمجاز اطلاعات ذخیره شده (شامل نرم‌افزار) به دلیل:

- معرفی بدافزار به‌وسیله‌ی نصب نرم‌افزار از منابع غیرمجاز،
- بهره‌جویی از آسیب‌پذیری‌ها در سامانه عامل زیرین[2].

ت- هرزنامه که منجر به موارد زیر می‌شود:

- افزایش هزینه‌های خدمات،
- توانمندسازی حملات صیادی،
- حملات انکار خدمت.

ث- دزدی یا از دست رفتن اتفاقی که هر دو منجر به موارد زیر می‌شوند:

- از دست رفتن اطلاعات داده‌های حساس هنگامی که داده‌های ذخیره شده بر روی افـزاره در جـای دیگـری آینه یا پشتیبان‌گیری نشده است،
- مسائل محرمانگی هنگامی که اطلاعات حساس ذخیره شده، حفاظت مناسبی ندارند،
- پشتیبان داده‌ی امن.

۱۳-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با افزاره‌های ارتباط سیار با موارد زیر در ارتباط هستند:

جدول ۹- کنترل‌های امنیتی برای فرانامه ارتباطات سیار

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
دسترسی غیرمجاز به اطلاعات ذخیره شده بر روی افزاره‌های سیار	
- کنترل دسترسی - احراز هویت - انکارناپذیری	- آگاهی کاربر از کنترل فیزیکی - دوری از پیکربندی‌های پیش‌فرض - احراز هویت قوی - فعال‌سازی گزینه‌های رویدادنگاری - قفل زمان فعالیت نکردن - دیواره‌ی آتش - خط‌مشی امنیتی سازمان برای گذرواژه‌ها و استفاده‌ی تجاری (محدود کردن استفاده شخصی از افزاره‌های متعلق به سازمان)
افشای غیرمجاز داده‌های حساس و اطلاعات مکانی	
- محرمانگی	- رمزنگاری داده‌های ذخیره شده و در حین انتقال (بی‌سیم)

1- Disposal
2- Underlying

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
– احراز هویت – امنیت ارتباطات – ناشفافی	– حفاظت از گذرواژه – دوری از خدمات طرف سوم که دسترسی به متن رمز نشده را برای انتقال داده نیاز دارند یا اگر امکان‌پذیر نبود درخواست تضمین محرمانگی داده‌های پردازش‌شده ضروری است – اطمینان از رویه‌های هم‌زمان‌سازی امن، – VPN امن برای اتصال‌های دسترسی راه دور، – رویه‌های انجام کار به‌جا برای پاک کردن داده‌های حساس – رضایت کاربر برای استفاده از اطلاعات مکانی
دست‌کاری/حذف غیرمجاز اطلاعات ذخیره شده	
– محرمانگی – قابلیت دسترسی – یکپارچگی	– غیرفعال‌سازی واسط‌ها، خدمات و برنامه‌های کاربردی بی‌سیم، – وصله‌زنی به‌روز سامانه عامل، – رویه‌های انجام کار بجا برای پاک کردن داده حساس، – حصول اطمینان از نصب خودکار به‌روزرسانی ضدویروس‌ها یا هشدار به کاربر هنگام در دسترس بودن به‌روزرسانی‌ها – بارگیری نرم‌افزارها فقط از سامانه‌ی توزیع نرم‌افزار سازمان (دوری جستن از نصب نرم‌افزارهای بدون پروانه) – امضاهای رقمی برای درستی‌سنجی منابع بارگیری
هرزنامه	
– کنترل دسترسی	پالایش محتوا افزایش آگاهی کاربر
دزدی یا از دست رفتن اتفاقی	
– محرمانگی – قابلیت دسترسی	مدیریت راه دور دارایی (غیرفعال‌سازی/ قفل افزاره) پشتیبان‌گیری امن دوره‌ای مدیریت متمرکز برای ردگیری دارایی و انطباق خط‌مشی

۱۴ پشتیبانی شبکه‌بندی برای کاربران در حال جابه‌جایی

۱۴-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که به کارکنان در حال جابه‌جایی اجازه می‌دهند به منابع سازمان دسترسی داشته باشند این فرانامه را در نظر بگیرند.

راه‌حل‌ها و پیشنهادهای این حوزه اغلب روی جنبه‌ی کارکردی تمرکز دارند و به طور عمده بازار مصرف‌کننده را مورد هدف قرار می‌دهند. از دیدگاه امنیت اطلاعات سطوح کارکردی پیشنهادشده مخاطرات جدیدی را مانند اثرگذاری یا نامعتبر کردن فرضیات در مورد امنیت اطلاعات معرفی می‌کنند. برای نمونه اگر دسترسی کاربر در

حال جابه‌جایی به درون‌نِت با کنترل‌های مناسب پیاده‌سازی نشده باشد، ممکن است این فرض که نگهداری درون‌نِت به‌خوبی کنترل و (نسبت به محیط بیرونی) حفاظت‌شده است، مورد تردید قرار گیرد.
در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیت است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند، مرتفع کند.

۱۴-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با پشتیبانی شبکه‌بندی کاربران در حال جابه‌جایی عبارت‌اند از:
الف- دسترسی غیرمجاز:

- سوءاستفاده از پشتیبانی شبکه‌بندی کاربر در حال جابه‌جایی برای به‌دست آوردن دسترسی غیرمجاز به درون‌نِت سازمان،
- لو رفتن[1] دروازه‌های امنیتی استفاده‌شده در مرز شبکه درون‌نِت،
- دسترسی غیرمجاز به داده‌های ذخیره‌شده روی افزاره‌های کاربر در حال جابه‌جایی.

ب- کاهش قابلیت دسترسی شبکه:

- مشکلات قابلیت دسترسی به شبکه زمانی به وجود می‌آیند که انتظارات کاربر راجع به پشتیبانی شبکه قابل برآورده‌سازی نیست، برای مثال این مسئله وابسته به قابلیت دسترسی فراهم‌آورندگان خدمت اینترنت است.

۱۴-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با پشتیبانی شبکه‌بندی برای کاربران در حال جابه‌جایی به موارد زیر مربوط هستند:

جدول ۱۰- کنترل‌های امنیتی برای پشتیبانی شبکه‌بندی برای کاربران در حال جابه‌جایی

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
دسترسی غیرمجاز	
– کنترل دسترسی – احراز هویت – امنیت ارتباطات – محرمانگی	– ارتقای فنون احراز هویت (احراز هویت مبتنی بر گواهی، احراز هویت دوعاملی یا پاسخ به چالش) – خدمات اختصاصی برای کاربران در حال جابه‌جایی مبتنی بر واسط‌های وب حفاظت‌شده به‌وسیله TLS/SSLv3 – استفاده از فناوری‌های شبکه خصوصی مجازی امن که با دروازه‌های امنیتی مناسب روی سامانه-های کارخواه ادغام شده‌اند (دیواره‌های آتش شخصی): – پیاده‌سازی‌های لایه‌ی ۲یا ۳ برای مثال IPSec، – VPNهای سطح برنامه کاربردی برای مثال مبتنی بر TLS. – رمزنگاری داده‌های ذخیره‌شده‌ی کاربر

1- Compromise

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	طراحی و فناوری‌های پیاده‌سازی
کاهش قابلیت دسترسی شبکه	
– قابلیت دسترسی	– تأمین‌کنندگان خدمات قابل توجه، با استفاده از موافقت‌نامه‌ی سطح خدمات(SLA) جهانی برای اطمینان‌پذیری و کارآیی

۱۵ خدمات برون‌سپاری شده

۱۵-۱ پس‌زمینه

توصیه می‌شود سازمان‌هایی که از خدمات برون‌سپاری‌شده استفاده می‌کنند این فرانامه را در نظر بگیرند.

به این دلیل که سازمان‌ها از خدمات برون‌سپاری‌شده استفاده می‌کنند راهبرد کسب‌وکار قابل دوامی است اما این استفاده به‌خصوص برای اطمینان از کیفیت و امنیت خدمات برون‌سپاری شده، پیچیدگی‌های سازمانی و عملیاتی نیز ایجاد می‌کند.

سازمان‌های گسترش‌یافته، مخاطرات افزوده‌ای به دلیل وابستگی به تأمین‌کنندگان خدمت به ارث می‌برند. برای نمونه تأمین‌کنندگان خدمات یا فروشندگان، دسترسی مستقیم به دارایی‌های درون سازمان برای پشتیبانی و/یا مسائل مدیریت رخداد لازم دارند از این‌رو دارایی‌های مهم را در معرض مخاطرات امنیتی قرار می‌دهند. درحالی‌که بسیاری از خدمات پشتیبانی برای پشتیبانی از زیرساخت، اجازه‌ی دسترسی دائمی لازم دارند دیگران ممکن است به دسترسی موقت نیاز داشته باشند. اغلب خدمات پشتیبانی به‌منظور انجام وظایف خود به حقوق دسترسی با اختیارات ویژه نیاز دارند.

با توجه به نوع فرانامه‌های برون‌سپاری، ملاحظات امنیتی و اشتباهات سهوی در تمام تنظیم قرارداد[1] وجود دارد. دیدگاهی عمومی از تهدیدها و ملاحظات در این سند ارائه شده است. برای اطلاعات عمیق‌تر در مورد امن‌سازی خدمات برون‌سپاری شده به استاندارد ISO/IEC 27036 مراجعه شود.

در بندهای زیرین تهدیدهای امنیتی و توصیه‌هایی در مورد فنون و کنترل‌های طراحی امنیتی است تا مخاطرات مرتبط با کاربری داخلی و کاربری داخلی و خارجی را که تشریح شده‌اند، مرتفع کند.

۱۵-۲ تهدیدهای امنیتی

تهدیدهای امنیتی مرتبط با خدمات برون‌سپاری شده عبارت‌اند از:

الف- دسترسی غیرمجاز به دیگر سامانه‌های داخلی (هنگامی که تأمین‌کننده[2] به سامانه‌های داخلی برای پشتیبانی و نگهداری راه دور دسترسی پیدا می‌کند):

- سوءاستفاده از درگاهی‌های نگهداری راه دور،
- سوءاستفاده از حقوق سرپرستی.

1- Contractual Arrangements

2- Supplier

ب- افشای غیرمجاز داده‌های حساس به‌وسیله‌ی تأمین‌کننده‌ی خدمات:
- احترام نگذاشتن به حقوق مالکیت معنوی،
- جدا نکردن محیط‌های چند مشتری،
- نبود بهترین روش‌های امنیت اطلاعات (برای نمونه اشتراک‌گذاری گذرواژه ممکن است جنبه‌ی عمومی داشته باشد)،
- اداره‌ی نادرست رسانه‌ی ذخیره‌سازی،
- استفاده از روش‌های ارتباطات ناامن.
پ- معرفی بدافزار (در محیط‌های توسعه نرم‌افزار):
- امنیت نامناسب در توسعه‌ی نرم‌افزار و رویه‌های انتشار آن،
- انتقال پرونده‌ها و داده به‌صورت ناامن،
- به‌کارگیری همکاری‌های برخط ناامن.
ت- مسئولیت به سبب عدم انطباق مقررات:
- عدم درک مقررات کشور خاص و قوانین مسئولیتی اگر تأمین‌کننده‌ی خدمت در کشور دیگری قرار گرفته باشد،
- حریم داده قانونی و الزامات حفاظتی کاربردپذیر ناکافی در کشوری که تأمین‌کننده در آن واقع شده است؛ این موضوع می‌تواند تأثیر منفی اساسی بر حریم داده قانونی و الزامات حفاظتی کاربردپذیر بهره‌بردار داشته باشد.

۱۵-۳ فنون و کنترل‌های طراحی امنیت

فنون و کنترل‌های طراحی امنیت اطلاعات مرتبط با خدمات خارجی یا برون‌سپاری شده به موارد زیر مربوط هستند:

جدول ۱۱- کنترل‌های امنیتی برای خدمات برون‌سپاری شده

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	**طراحی و فناوری‌های پیاده‌سازی** (پیاده‌سازی می‌تواند به‌وسیله‌ی سازمان برون‌سپاری کننده یا برون‌سپاری‌شده، بسته به مفاد کار فرض شود)
دسترسی غیرمجاز به دیگر سامانه‌های داخلی	
– کنترل دسترسی – احراز هویت – انکارناپذیری	– اختصاص اکید شناسه‌های منفرد کاربر – احراز هویت قوی (برای نمونه احراز هویت دو عاملی) برای ثبت ورود ریشه/سرپرست[1] – درگاه پیشانه[2] یا درگاه دستی در پایگاه که به‌وسیله‌ی شناسه‌ی کاربر و گذرواژه حفاظت می‌شود (در مواردی که تأمین‌کننده خدمت دسترسی فیزیکی در پایگاه لازم دارد) – رویدادنگاری تشریحی از فعالیت‌های دسترسی و بازنگری‌های رویدادنگار
افشای غیرمجاز داده‌های حساس به‌وسیله تأمین‌کننده خدمات	

1- Admin
2- Console

مشخصات امنیتی کاربردپذیر برای تهدیدهای شناسایی‌شده	**طراحی و فناوری‌های پیاده‌سازی** (پیاده‌سازی می‌تواند به‌وسیله‌ی سازمان برون‌سپاری کننده یا برون‌سپاری‌شده، بسته به مفاد کار فرض شود)
– محرمانگی	– بهترین روش‌های حفاظت داده‌های کارخواه از طریق رمزنگاری – آگاهی و آموزش امنیتی – پایش و ممیزی تسهیلات و رویه‌ها – خط‌مشی امنیت قراردادی و هدایت‌گرهای[1] رویه‌ها
معرفی بدافزار	
– یکپارچگی	– آیین کار[2] امن – فرآیندهای مدیریت تغییر – حصول اطمینان از نصب خودکار به‌روزرسانی ضدویروس‌ها یا هشدار به کاربر هنگام در دسترس بودن به‌روزرسانی‌ها
مسئولیت به سبب عدم انطباق مقررات	
– محرمانگی – ناشفافی	– آگاهی از مقررات محلی – استفاده از نرم‌افزارهای رمزنگاری سازگار – سازوکارهای ناشفافی (IPSec VPNs)

1- Directive
2- Coding Practices

پیوست الف
(اطلاعاتی)
مثالی از خط‌مشی استفاده از اینترنت

الف-۱ مرور کلی

اهداف InfoSec از انتشار خط‌مشی استفاده‌ی قابل‌قبول، اعمال محدودیت‌های مغایر با فرهنگ بازبودن[1]، اعتماد[2] و یکپارچگی ایجادشده در <نام مؤسسه> نیست. دیدگاه InfoSec متعهد به حفاظت از کارکنان <نام مؤسسه>، شرکاء و شرکت در مقابل کنش‌های غیرقانونی یا زیان‌آور عمدی یا سهوی توسط افراد است.

سامانه‌های مرتبط با اینترنت/درون‌نِت/برون‌نِت که شامل تجهیزات رایانه‌ای، نرم‌افزارها، سامانه‌های عامل، رسانه-های ذخیره‌سازی، حساب‌های شبکه‌ی ارائه‌دهنده‌ی رایانامه، مرورگرWWW و FTP می‌شوند، اما تنها محدود به این موارد نیستند، دارایی <نام مؤسسه> هستند. این سامانه‌ها، برای مقاصد تجاری جهت ارائه‌ی موارد مطلوب شرکت و مشتریان در حین عملیات عادی استفاده می‌شوند. برای مشاهده جزییات بیشتر، خط‌مشی‌های منابع انسانی را مشاهده کنید.

امنیت اثربخش کاری تیمی است که شامل مشارکت و پشتیبانی هر یک از کارکنان و وابستگان <نام مؤسسه> بوده که در ارتباط با اطلاعات یا سامانه‌های اطلاعاتی هستند. وظیفه‌ی هر کاربر رایانه است که این راهنماها را بشناسد و فعالیت‌هایش را مطابق آن مدیریت کند.

الف-۲ هدف

هدف از این خط‌مشی ارائه‌ی نمایی کلی از استفاده‌ی درست از تجهیزات رایانه‌ای در <نام مؤسسه> است. این قوانین برای محافظت از کارکنان و <نام مؤسسه> هستند. استفاده‌ی نامناسب، <نام مؤسسه> را در معرض مخاطراتی قرار می‌دهد که شامل حملات ویروسی، لو رفتن سامانه‌های شبکه‌ای و خدمت‌ها و مسائل حقوقی می‌شود.

الف-۳ دامنه کاربرد

این خط‌مشی در مورد کارکنان، پیمانکاران، مشاوران، کارگران موقت و سایر کارگران <نام مؤسسه>، شامل همه‌ی افراد مرتبط با طرف سوم اعمال می‌شود. این خط‌مشی برای تمام تجهیزات مایملک یا اجاره‌ای <نام مؤسسه> اعمال می‌شود.

1- Culture of openness
2- Trust

الف-٤ خط‌مشی

الف-۴-۱ استفاده‌ی عمومی و مالکیت

۱- درحالی‌که سرپرست شبکه‌ی <نام مؤسسه> تمایل دارد که سطح متعارفی از ناشفافی را ارائه کند، توصیه می‌شود کاربران آگاه باشند که داده‌ای که آن‌ها روی سامانه‌های اشتراکی تولید می‌کنند، دارایی <نام مؤسسه> خواهد بود. به دلیل نیاز به محافظت از شبکه‌ی <نام مؤسسه>، مدیریت نمی‌تواند محرمانگی اطلاعات ذخیره‌شده را روی هر افزاره‌ی شبکه، متعلق به شرکت تضمین کند.

۲- کارکنان مسئول هستند در مورد معقول بودن استفاده‌ی شخصی، قضاوت خوبی داشته باشند. هر اداره مسئول ایجاد راهنماهایی در خصوص استفاده‌ی شخصی از سامانه‌های اینترنت/درون‌نِت/برون‌نِت است. توصیه می‌شود کارکنان در غیاب چنین خط‌مشی‌هایی، به‌وسیله‌ی خط‌مشی‌های اداری در مورد استفاده‌های شخصی راهنمایی شوند و توصیه می‌شود اگر ابهامی وجود داشته باشد، کارکنان با ناظر[1] یا مدیر خود مشورت کنند.

۳- راهنمای InfoSec پیشنهاد می‌کند هرگونه اطلاعاتی که کاربران احساس می‌کنند حساس یا آسیب‌پذیر است، رمزنگاری شود. برای مشاهده‌ی راهنماها درباره‌ی طبقه‌بندی اطلاعات[2]، خط‌مشی حساسیت اطلاعات InfoSec را ببینید. برای مشاهده‌ی راهنماها در مورد رمزنگاری رایانامه و مستندات، به آگاهی‌رسانی‌های اولیه‌ی InfoSec مراجعه کنید.

۴- افراد مجاز در <نام مؤسسه> اجازه دارند تجهیزات، سامانه‌ها و ترافیک شبکه را طبق خط‌مشی ممیزی InfoSec، جهت امنیت و نگهداری شبکه پایش نمایند.

۵-<نام مؤسسه> دارای این حق است که شبکه‌ها و سامانه‌ها را به‌صورت دوره‌ای جهت اطمینان از تطبیق با این خط‌مشی ممیزی کند.

الف-۴-۲ امنیت و اطلاعات اختصاصی[3]

توصیه می‌شود واسط کاربر برای سامانه‌های مرتبط با اینترنت/درون‌نِت/ برون‌نِت به‌صورت محرمانه یا غیرمحرمانه همان طور که در خطوط راهنمای محرمانگی اشتراکی تعریف شده است، طبقه‌بندی شود که جزئیات آن را در خط‌مشی‌های منابع انسانی می‌توان پیدا کرد. مثال‌هایی از اطلاعات محرمانه شامل موارد زیر اما نه محدود به آن‌ها است: حریم خصوصی شرکت[4]، راهبردهای شرکت، رقبای حساس، رازهای تجاری، ویژگی‌ها، فهرست مشتریان و داده‌های تحقیقاتی. توصیه می‌شود کارکنان تمامی گام‌های لازم به‌منظور جلوگیری از دسترسی غیرمجاز به این اطلاعات را اجراکنند.

گذرواژه‌ها را امن نگه‌دارید و حساب‌ها را به اشتراک نگذارید. کاربران مجاز مسئول امنیت گذرواژه‌ها و حساب-های خود هستند. توصیه می‌شود گذرواژه‌های سطح سامانه هر سه ماه یک‌بار و گذرواژه‌های سطح کاربر هر شش ماه یک‌بار تغییر داده شوند.

1- Supervisor
2- Information Classification
3- Proprietary
4- Company Private

توصیه می‌شود همه‌ی رایانه‌های شخصی، رایانه‌های کیفی و ایستگاه‌های کاری با استفاده از محافظ صفحه نمایش دارای گذرواژه با ویژگی فعال‌سازی خودکار که برای ۱۰ دقیقه یا کمتر تنظیم شده است یا با خروج از سامانه[1] (گرفتن هم‌زمان کلیدهای Ctrl-Alt-Delete برای کاربران Win2k) زمانی که سامانه‌ی میزبان بدون متصدی است، امن شوند.

۱- رمزنگاری اطلاعات را مطابق با خط‌مشی رمزنگاری قابل‌قبول InfoSec استفاده کنید.

از آنجا که اطلاعات موجود در رایانه‌های قابل‌حمل به طور ویژه‌ای آسیب‌پذیر است، توصیه می‌شود در این مورد دقت زیادی انجام شود. رایانه‌های کیفی را مطابق با نکات امنیتی آن‌ها محافظت کنید.

توصیه می‌شود نامه‌های ارسالی کاربران از نشانی رایانامه <نام مؤسسه> به گروه‌های خبری حاوی سلب-مسئولیتی[2] باشد که اظهار کند نظرات بیان‌شده شخصی است و به‌طور الزامی نظرات <نام مؤسسه> نیست، مگر آنکه ارسال در ارتباط با وظایف حرفه‌ای باشد.

همه میزبان‌هایی که به‌وسیله‌ی کارکنان متصل به اینترنت/ درون‌نِت/برون‌نِت <نام مؤسسه> استفاده شده‌اند، چه مایملک کارکنان باشند چه <نام مؤسسه>، باید به طور پیوسته نرم‌افزار ویروس‌یابی تأییدشده‌ای با دادگان ویروس به‌روز اجرا کنند، مگر آنکه تحت خط‌مشی‌های گروهی یا اداری قرار گرفته باشند[3].

توصیه می‌شود کارکنان در بازکردن پیوست‌های رایانامه‌های دریافت شده از فرستنده‌های ناشناس که ممکن است حاوی ویروس، بمب‌های رایانامه‌ای یا کد اسب تروا باشند، دقت زیادی داشته باشند.

الف-۴-۳ استفاده‌ي غیرقابل‌قبول

فعالیت‌های زیر به طور کلی، ممنوع شده‌اند. کاربران ممکن است از این محدودیت‌ها در زمان مسئولیت‌های شغلی قانونی مستثنی شوند (به‌طور مثال ممکن است نیاز باشد کارکنان سرپرست سامانه‌ها، درصورتی‌که میزبانی خدمات تولید را مختل کند، دسترسی به شبکه‌ی آن میزبان را غیرفعال کنند).

کارمند <نام مؤسسه> درحالی‌که از منابع <نام مؤسسه> بهره می‌برد، تحت هیچ شرایطی مجاز به انجام فعالیتی غیرقانونی طبق قوانین محلی، ایالتی، فدرال یا بین‌المللی نیست.

فهرست زیر به‌هیچ‌وجه جامع نیست، اما سعی دارد چارچوبی برای فعالیت‌هایی ارائه نماید که در دسته‌ی استفاده‌ی غیرقابل‌قبول جای می‌گیرند.

الف-٤-۳-۱ فعالیت‌های شبکه و سامانه

فعالیت‌های زیر با تأکید بسیار و بدون هیچ استثنایی منع شده‌اند:

۱- نقض حقوق هر شخص یا شرکت که به‌وسیله‌ی حق نشر، رمز تجاری، حق مالکیت انحصاری اختراع[4] یا دیگر مالکیت‌های معنوی، یا حقوق مشابه یا نظام‌نامه‌ها محافظت شده است و شامل نصب یا توزیع نرم‌افزارهای

1- Logging Off
2- Disclaimer
3- Overridden By Departmental Or Group Policy
4- Patent

رونوشت شده بدون اجازه‌ی ناشر[1] یا سایر محصولات نرم‌افزاری که فاقد مجوز مناسب استفاده برای <نام مؤسسه> هستند، می‌شود اما تنها محدود به این موارد نیست.

۲- رونوشت غیرمجاز کالاهای دارای حق نشر که شامل این موارد و نه محدود به آن‌ها است: رقمی‌سازی[2] و توزیع عکس‌های مجلات، کتاب‌ها یا سایر منابع با حق نشر، موسیقی دارای حق نشر، نصب نرم‌افزارهای دارای حق نشر که <نام مؤسسه> یا کاربر نهایی مجوز فعال آن را ندارد، اکیداً ممنوع شده است.

۳- صادرات نرم‌افزار، اطلاعات فنی، نرم‌افزار یا فناوری رمزنگاری مغایر با قوانین صادراتی محلی یا بین‌المللی، غیرقانونی است. توصیه می‌شود قبل از صادرات هرگونه کالای بحث‌برانگیز با مدیریت مرتبط مشورت کرد.

۴- تزریق برنامه‌های مخرب به شبکه یا کارساز (به‌عنوان مثال ویروس‌ها، کرم‌ها، اسب‌های تروا، بمب‌های رایانامه‌ای و ...)

۵- آشکار ساختن گذرواژه حساب خود برای دیگران یا اجازه دادن به دیگران جهت استفاده از حساب شما. این شامل خانواده و سایر اعضای خانه، هنگامی که کار در خانه انجام می‌گیرد، می‌شود.

۶- استفاده از دارایی محاسباتی <نام مؤسسه> به‌منظور مداخله فعالانه در تأمین یا انتقال کالاهایی که ناقض قوانین حوزه قضایی محلی در مورد آزار جنسی یا محل‌کار زیان‌آور[3] (مشاغل سخت و زیان‌آور) کاربر هستند.

۷- پیشنهاد فریب‌دهنده‌ی محصولات، موارد یا خدماتی که منشأ آن‌ها حساب‌های <نام مؤسسه> باشد.

۸- ارائه اظهاراتی در مورد ضمانت، به طور صریح یا ضمنی، مگر آنکه بخشی از وظایف شغلی معمول باشد.

۹- نقض امنیتی مؤثر یا اختلال در ارتباطات شبکه‌ای. نقض‌های امنیتی شامل موارد زیر هستند اما تنها محدود به این موارد نمی‌شوند: دسترسی به داده‌هایی که کارمند گیرنده‌ی موردنظر آن‌ها نیست، یا ثبت ورود به کارساز یا حسابی که کارمند برای دسترسی به آن مجاز نیست، مگر اینکه این وظایف در حیطه‌ی وظایف مقرر باشد. برای اهداف این بخش، «اختلال» شامل موارد زیر است اما تنها محدود به این موارد نیست: دیده‌بانی شبکه، سیلاب پینگ‌شده[4]، جعل بسته، انکار خدمت و اطلاعات مسیریابی ساختگی برای اهداف مخرب.

۱۰- پویش درگاه یا پویش امنیتی که به طور صریح منع شده است، مگر آنکه از قبل به InfoSec اعلام شده باشد.

۱۱- انجام هر گونه پایش شبکه که موجب شنود داده‌ای شود که مرتبط با سامانه‌ی میزبان کارمند[5] نیست، مگر آنکه این کار بخشی از شغل/وظیفه‌ی عادی کارمند باشد.

۱۲- دور زدن[6] احراز هویت کاربر یا امنیت هر سامانه‌ی میزبان، شبکه یا حساب.

۱۳- ایجاد مزاحمت یا مانع در ارائه‌ی خدمت به هر کاربر غیر از کاربر سامانه‌ی میزبان کارمند(به‌عنوان مثال حمله‌ی انکار خدمت).

1- Pirated
2- Digitization
3- Hostile Workplace
4- Pinged Flood
5- Employee Host
6- Circumventing

۱۴- استفاده از یک برنامه/وب‌نوشت/دستور یا ارسال پیام‌هایی از هر نوع، با هدف ایجاد مزاحمت یا غیرفعال-سازی نشست پایانه‌ی کاربر به هر وسیله، به طور محلی یا از طریق اینترنت/درون‌نِت/برون‌نِت.
۱۵- ارائه‌ی اطلاعات یا فهرست‌هایی درباره کارکنانِ <نام مؤسسه> به طرف‌هایی خارج از <نام مؤسسه>

الف-۴-۳-۲ فعالیت‌های ارتباطاتی و رایانامه

۱- ارسال پیام‌های رایانامه‌ی ناخواسته، شامل ارسال «نامه‌ی درخواست نشده[1]» یا سایر موارد تبلیغاتی به افرادی که این موارد را به طور مشخص درخواست نکرده‌اند.
۲- هر گونه آزار از طریق رایانامه، تلفن یا فراخوانی[2] از طریق زبان، بسامد یا اندازه پیام.
۳- استفاده‌ی غیرمجاز یا جعل اطلاعات سرآیند رایانامه.
۴- درخواست رایانامه برای هر نشانی رایانامه، غیر از حساب ارسال‌کننده، با هدف آزار یا جمع‌آوری پاسخ‌ها.
۵- ساخت یا باز ارسال «نامه‌های زنجیره‌ای[3]»، [طرح]«پونزی[4]» یا سایر طرح‌های «هرمی[5]» از هر نوع.
۶- استفاده از رایانامه‌ی ناخواسته‌ی نشأت‌گرفته از درون شبکه‌های <نام مؤسسه> از دیگر تأمین‌کنندگان خدمت اینترنت/درون‌نِت/برون‌نِت که از طرف آن‌ها یا برای تبلیغ هر خدمتی که در شبکه‌ی <نام مؤسسه> میزبانی می‌شود یا به شبکه <نام مؤسسه> متصل است.
۷- ارسال پیام‌های یکسان یا مشابه، غیر مرتبط تجاری تعداد زیادی از گروه‌های خبری (هرزنامه گروه‌های خبری).

الف-۴-۴ وب‌نویسی

۱- وب‌نویسیِ کارکنان به‌وسیله سامانه‌ها و دارایی‌های <نام مؤسسه>، چه به‌وسیله‌ی سامانه‌های رایانه‌ای شخصی، مشمول محدودیت‌ها و شرایطی است که در این خط‌مشی بیان شده‌اند. استفاده‌ی محدود و پراکنده از سامانه‌های <نام مؤسسه> برای وب‌نویسی قابل‌قبول است، به‌شرطی که به‌صورت حرفه‌ای و مسئولیت‌پذیرانه صورت گیرد، خط‌مشی‌های <نام مؤسسه> را نقض نکند، برای مصالح <نام مؤسسه> زیان‌آور نباشد و در وظایف کاری کاربر اختلال ایجاد نکند. وب‌نویسی با استفاده از سامانه‌های <نام مؤسسه> مشمول پایش است.
۲- خط‌مشی اطلاعات محرمانه <نام مؤسسه> نیز در مورد وب‌نویسی اعمال می‌شود. بنابراین کارکنان از افشای اطلاعات اختصاصی یا محرمانه‌ی «مؤسسه»، رمزهای تجاری یا هر موردی که به‌وسیله خط‌مشی اطلاعات محرمانه شرکت پوشش داده می‌شود، در هنگام وب‌نویسی منع شده‌اند.
۳- کارکنان نباید به هیچ‌گونه وب‌نویسی که تصویر[6]، اعتبار و یا حسن نیت <نام مؤسسه> را لکه‌دار کند یا به آن آسیب زند، انجام دهند. هم‌چنین کارکنان در حین وب‌نویسی نباید نظرات تبعیض‌آمیز، اهانت‌آمیز، افتراآمیز یا

1- Junk Mail
2- Paging
3- Chain Letters
4- Ponzi(نوعی طرح کسب‌وکار شیادانه)
5- Pyramid
6- Image

آزاردهنده داشته باشند یا مبادرت به فعالیت‌های ممنوع شده در خط‌مشی ضدآزار وعدم تبعیض <نام مؤسسه> کنند.

۴- کارکنان همچنین مجاز نیستند که گفته‌ها، نظرات یا عقاید شخصی را در وب‌نویسی به <نام مؤسسه> نسبت دهند. اگر کارمندی عقاید و یا نظراتش را در وب‌نوشت اظهار کند، مجاز نیست که به طور صریح یا ضمنی خود را کارمند یا نماینده <نام مؤسسه> نشان دهد. کارکنان تمام مخاطرات مرتبط با وب نویسی را باید در نظر بگیرند و تقبل کنند.

۵- جدا از پیروی تمامی قوانین مرتبط با سامان‌دهی و افشای کالاهایی با حق نشر یا صادرات کنترل‌شده، هم‌چنین مجاز نیست علامت‌های تجاریِ <نام مؤسسه>، نشان‌واره و سایر دارایی‌های معنوی در هر گونه فعالیت مرتبط با وب‌نویسی استفاده شوند.

الف-۵ اجرا

هر کارمند که ناقض این خط‌مشی شناخته شود، ممکن است که مشمول اقدامات تنبیهی، حداکثر تا اخراج ویا شامل اخراج از کار گردد.

الف-٦ تعاریف

اصطلاح	تعریف
وب‌نویسی	نوشتن یک وب‌نوشت. وب‌نوشت، نوشته شخصی برخطی است که به طور متناوب به‌روزرسانی می‌شود و جهت استفاده‌ی عموم است.
هرزنامه	انبوه رایانامه‌های ناخواسته یا غیرمجاز.

الف-۷ تاریخچه بازبینی

پیوست ب
(اطلاعاتی)
کالانمای[1] تهدیدها

ب-۱ بدجلوه دادن مرجع قانونی و حقوق[2]

- ارائه‌ی یک مجوز اشتباه با هدف گمراه ساختن به‌صورتی که گویی درست بوده است.
- ارائه‌ی گذرواژه، کلید یا گواهی فرد دیگری (به طور مثال سرپرست سامانه).
- به‌دست آوردن و استفاده‌ی غیرمجاز از اطلاعات احراز هویت مرتبط با خدمت مشترکان(به طور مثال شناسه‌ی کاربر/گذرواژه، کلیدهای نشست) محدود به مشترکان شخصی.
- به‌دست آوردن غیرمجاز و استفاده از اطلاعات احراز هویت سرپرست(به طور مثال شناسه‌ی کاربر/گذرواژه)
- حملات تکراری که شامل علامت‌دهی[3] است.

ب-۲ دزدی خدمت

- گرفتن غیرقانونی منافع تأمین‌کننده‌ی خدمت[4] مورد نظر به‌منظور محروم کردن آن از درآمد قانونی
- فریب دادن تأمین‌کننده‌ی خدمت
- پاک کردن یا تغییر غیرمجاز اطلاعات صورت‌حساب
- همسانه‌سازی[5] افزاره‌ها.
- فریب دادن سامانه‌های دسترسی مشروط(CAS)[6].
- تکرار/ انتشار انبوه داده‌هایی که دزدی خدمت را میسر می‌سازند.

ب-۳ تعرض[7] به حریم خصوصی مشترک و شنود غیرقانونی

- ردیابی الگوهای تماس به‌منظور کشف هویت، وابستگی[8]، حضور و استفاده.
- گیراندازی[9] ترافیک: ضبط غیرمجاز ترافیک، شامل ضبط بسته‌ها، ضبط رویدادنگاری و پویش بسته‌ها. شامل علامت‌دهی و مدیریت ترافیک.
- دسترسی غیرمجاز به جریان رسانه مشترکان

1- Catalogue
2- Misrepresenting Authority & Rights
3- Signaling
4- Service Provider
5- Cloning
6- conditional access systems
7- Invasion
8- Affiliation
9- Capture

- دسترسی غیرمجاز به عملیات، سرپرستی، مدیریت و تدارکات(OAM&P) ترافیک
- دسترسی غیرمجاز به ترافیک علامت‌دهی
- برداشت اطلاعات- روش غیرمجاز گیراندازی هویت که به دنبال آن ارتباطات غیرمجاز و دزدی اطلاعات را میسر می‌سازد. شامل جمع‌آوری شناسه‌ها، که ممکن است اعداد، رشته‌ها، URLها و ... باشند.
- بازسازی[1] رسانه: پایش غیرمجاز، ضبط، ذخیره، بازسازی، بازشناسی[2]، تفسیر، ترجمه و یا استخراج ویژگی هر بخش از ارتباطات تصویری شامل هویت، حضور یا وضعیت.
- افشای غیرمجاز قابلیت‌های خدمات مشترکین.
- افشای غیرمجاز فعالیت‌ها و کاربری قبلی یا فعلی مشتریان (به طور مثال مشاهده‌ی تاریخچه‌ی محتوای پخش یا ویدئو براساس تقاضا (VoD)[3]، یا فعالیت‌های بازی برخط مشترکین).
- حملات بازپخشی[4] که رسانه را دربر می گیرد (بازپخش رسانه‌ی ضبط‌شده[5] برای منافع بدخواهانه، یا تعرض به حریم خصوصی با بازپخش یک رسانه برای استفاده‌ی شخصی)

ب-۴ شنود و دست‌کاری[6]

- جعل هویت و ربودن مکالمه – تزریق[7]، حذف، اضافه، پاک‌سازی[8]، تعویض یا جایگزینی[9] یا سایر دست‌کاری‌های هر بخشی از ارتباطات با اطلاعاتی که هر بخش از آن و/یا هویت، حضور یا وضعیت هر کدام از طرفین را تغییر می‌دهد. شامل علامت‌دهی و مدیریت ترافیک.
- دسترسی غیرمجاز، تغییر و یا حذف اطلاعات رقمی.
- ربودن جریان داده. درج[10]، تغییر و حذف جریان داده به روشی غیرمجاز.
- هر شکلی از هرزنامه.
- انتقال غیرمجاز مواد (به دلایل سیاسی یا سایر دلایل).

ب-۵ سیلاب‌سازی ترافیک/بسته

- حمله انکار خدمت به پایانگاهی کاربر با ارسال تعداد زیادی از بسته‌های معتبر که موجب وقفه در خدمات می‌شود، بعضی از آن‌ها ممکن است عناصر شبکه را نیز تحت تأثیر قرار دهند. برنامه‌ی کاربردی به دلیل سرریز[11] متوقف خواهد شد.

1- Reconstruction
2- Recognition
3- Video on Demand
4- Replay
5- Captured Media
6- Interception & Modification
7- Injection
8- Removal
9- Replacement
10- Insertion
11- Overload

- فرانامه‌های سیلاب‌سازی بسته پایانگاهی باعث می‌شوند عنصر شبکه یا کارساز ازکارافتاده[1]، راه‌اندازی مجدد شده[2]، یا تمامی منابع را مصرف کند.
- حمله‌ی انکار خدمت- مصرف پهنای باند یا مصرف منبع. حجم زیادی از ترافیک (به طور مثال به گروهی چندپخشی).
- احتمال تأثیر روی هزاران مشترک (به طور مثال DSLAMها[3]، کارسازانی که از هزاران مشترک پشتیبانی می‌کنند).

ب-۶ بسته‌ها و پیام‌های ناهنجار[4]

- پایانگاه‌ها را با پیام‌های نامعتبر غیرفعال می‌سازد- حمله‌ی انکار خدمت به پایانگاه (به طور مثال کارساز) با ارسال تعدادی بسته که موجب شود پایانگاه ازکار بیافتد، راه‌اندازی مجدد شود یا تمامی منابع را مصرف کند.
- پیام‌های پروتکل ناهنجار – ارسال پیام‌های پروتکل ناهنجار (به طور مثال پیام‌هایی با سرریز یا پاریز[5]) به افزاره‌ای که کارایی آن را تا حدی که قادر به پردازش پیام‌های عادی نباشد، پایین می‌آورد.
- پیام‌های ناهنجار که باعث سرریز میانگیر[6] می‌شوند.
- احتمال تأثیر روی هزاران مشترک (به طور مثال کارسازانی که از هزاران مشترک پشتیبانی می‌کنند).

ب-۷ پیام‌های ساختگی

- حمله‌ی انکار خدمت که با اتمام ناگهانی نشست باعث اختلال خدمات می‌شود.
- جعل پیام‌های کنترل. ترافیک کنترل مخرب – تزریق‌شده به ارتباطات که باعث کارکرد نامناسب کارسازها یا برنامه‌های کاربردی می‌شود یا ترافیکی که اشتباهی به مقصد فرستاده شده است. پیام‌های کنترل ساختگی که برای تغییر ساختار درخت توزیع چندپخشی و تأثیر بر توزیع داده‌ها در آن‌ها، استفاده می‌شوند. حمله‌ی انکار خدمت - پیام‌های پخش ساختگی که ادعا می‌کنند نرخ اتلاف یا ازدحام زیادی روی کانال وجود دارد. منبع نرخ انتقال تأثیرگذار روی سایر مشترکین را کاهش خواهد داد.
- پیام‌های استفاده‌ی نهایی ساختگی و پاسخ‌های برنامه‌ی کاربردی یا کارساز
- تغییر نشانی IP یا MAC برای جعل نشانی‌های MAC یا IP سایر کاربران به‌منظور گیراندازی جریان‌های داده.

1- Crash
2- Reboot
3- Digital Subscriber Line Access Multiplexers
4- Malformed
5- Underflow
6- Buffer

ب-۸ حمله‌ی انکار خدمت سکوی زیرین

- آسیب‌پذیری‌های سامانه‌عامل یا سفت‌افزار[1] زیرین که برنامه‌کاربردی یا خدمت روی آن اجرا می‌شود.
- محصولات قابل سوءاستفاده‌ی «نشانه‌گیری و شلیک» که به طور رایگان برای بارگیری، در اینترنت در دسترس هستند.
- حملات انکار خدمت که کارایی افزاره را کاهش می‌دهند.

سوءاستفاده از این آسیب‌پذیری‌ها احتمال بالقوه‌ی انتشار به هزاران افزاره را دارد(به طور مثال افزاره‌های مشتریان). احتمال منجر به استقرارمجدد[2] یا نگهداری هزاران افزاره خواهد شد.

ب-۹ لو رفتن نرم‌افزار نصب‌شده، داده‌ی مرتبط با خدمت یا پیکربندی سامانه

- جاسازی بدافزار، جاسوس‌افزار یا ردگم‌کن[3]
- تکثیر، نصب، تغییر یا حذف غیرمجاز محصول نرم‌افزاری یا پرونده‌های پیکربندی.
- تکثیر، افشا، ایجاد، تغییر یا حذف غیرمجاز داده‌های مرتبط با خدمت (برای مثال رویدادنگارهای سامانه، اطلاعات صورت‌حساب، کلیدهای رمزگشایی، مخازن ذخیره‌سازی کلیدهای رمزگشایی و ...).
- حمله‌ی انکار خدمت توزیع‌شده با استفاده از افزاره‌های در معرض خطر[4] برای از کار انداختن خدمت.
- ایجاد یا تغییر غیرمجاز اطلاعات مرتبط با خدمت مشترکین (به طور مثال اطلاعات احراز هویت، کلیدهای نشست).
- فعال‌سازی/غیرفعال‌سازی غیرمجاز یا غیرضروری درگاه‌های منطقی(پروتکل).

ب-۱۰ اتلاف منابع

- نقص‌هایی[5] در نرم‌افزار یا سخت‌افزار که باعث اتلاف منبع حافظه (به طور مثال میانگیرها) در یک سامانه می‌شوند.
- نقص‌هایی در نرم‌افزار یا سخت‌افزار که بیشتر منبع پردازشگر را در سامانه مصرف می‌کنند.
- خطاهای سخت‌افزاری یا نرم‌افزاری که پهنای باند در دسترس یک پیوند ارتباطی را محدود می‌کنند.
- نقص‌هایی در نرم‌افزار یا سخت‌افزار که پیام‌های غیرضروری تولید می‌کنند که منابع پهنای باند را کاهش می‌دهند.
- به طور مثال حلقه‌های نامتناهی نرم‌افزاری، حلقه‌های مسیریابی.

1- Firmware
2- Redeployment
3- Rootkit
4- Compromised Devices
5- Deficiencies

ب-۱۱ پویش‌ها و کاوش‌های[1] غیر مجاز شبکه

- پویش/پینگ درگاه. حمله‌کننده می‌تواند نرم‌افزار پویش قابل دسترس برای عموم را روی میزبانی که به شبکه متصل است اجرا کند. پاسخ را خدمات میزبانی موجود در افزاره‌هایی که درگاه‌ها را پایش می‌کنند، خواهند داد و از این طریق به طور بالقوه اطلاعاتی برای حمله‌کننده فراهم می‌کنند.
- پویش آسیب‌پذیری (به طور مثال nessus)، نگاشت شبکه (به طور مثال NMAP). حمله‌کننده می‌تواند نرم‌افزارهای قابل دسترس برای عموم را روی میزبانی که به شبکه متصل است اجرا کند که پیکربندی افزاره و توپولوژی شبکه را پرس و جو می‌کند.
- دسترسی راه‌دور به نرم‌افزار یا کارکردهایی که روی افزاره هستند (به طور مثال استفاده از یک ردگم‌کن به‌منظور ایجاد یک درِ پشتی[2]).

ب-۱۲ لو رفتن داده‌ی برنامه کاربردی مشترک

- افشای غیرمجاز، ایجاد، تغییر، تکثیر یا حذف داده‌هایی که به‌وسیله‌ی برنامه‌های کاربردی در دسترس مشترکین ایجاد یا استفاده شده است.
- شامل اطلاعاتی است که در شبکه تأمین‌کننده خدمات، از طرف مشترکین ذخیره شده است (به طور مثال محتوای ویدیوی ذخیره‌شده به‌وسیله nDVR[3]).

ب-۱۳ دزدی محتوا

- گیراندازی[4] گواهی‌نامه‌های رقمی به‌منظور به‌دست آوردن محتوا و یا حتی / بازتوزیع جریان به دیگر مشترکین.
- گیراندازی بسته روی شبکه خانگی و زیرشبکه IP.
- خروجی از درگاه خروجی قیاسی[5] به افزاره‌ی ضبط‌کننده خارجی.
- خروجی از درگاه رقمی به افزاره‌ی ضبط‌کننده خارجی.
- پخش بیشتر از تعداد دفعات مجاز پخش.
- دسترسی به محتوای غیرقانونی (به طور مثال محتوای دزدیده‌شده).
- دور زدن سامانه‌های دسترسی مشروط.
- رونوشت محتوا از دیسک ذخیره‌ساز[6] روی کارساز یا افزاره‌ی کاربر نهایی.

ب-۱۴ دسترسی به محتوای نامناسب

1- Scans And Probes
2- Backdoor
3- network Digital Video Recorder
4- Capturing
5- Analog
6- Disk Storage

- دسترسی سهوی[1]
- دسترسی عمدی[2]

ب-۱۵ لو رفتن اطلاعات مشترک

- مهندسی اجتماعی به‌منظور کسب اطلاعات مشترکین
- افشا، ایجاد، تغییر، تکرار یا حذف غیرمجاز اطلاعات مشترکین (به طور مثال نشانی، شماره تلفن، شماره‌حساب، اطلاعات کارت اعتباری، مدخل‌های DNS/ENUM[3] و ...).
- محدود به مشترکین منفرد.

ب-۱۶ نشست‌ربایی و دگرنمایی خدمت

- جعل هویت کارگزار خدمات قانونی. گیراندازی گواهی‌نامه‌های رقمی از کارگزار به‌منظور تغییر جریان و جای‌گذاری هر اطلاعاتی که بخواهند.
- جعل هویت افزاره شبکه قانونی، کارساز ویدیو، کارساز بازی، کارساز DRM[4]
- حمله‌ی فردی در میان.
- هدایت جریان ویدیو به افزاره‌ی غیرمجاز

ب-۱۷ مدیریت غیرمجاز

- استفاده‌ی غیرمجاز از برنامه‌های کاربردی مدیریت پردازش[5] یا اجرای دستورات مدیریت. به طور مثال دست‌کاری پیکربندی مودم به‌منظور انسداد خدمتی مشخص.
- پیام‌های پروتکل مدیریت جعل/تغییر داده‌شده. به طور مثال دست‌کاری پیکربندی مودم به‌منظور مسدود کردن یا مجاز ساختن یک پروتکل خاص (به طور مثال SNMP).
- تغییر پیام‌های مدیریتِ از راه دور (به طور مثال MITM[6]).
- کنش‌های خودتأمینی غیرقانونی مشترکین. به طور مثال بازپیکربندی STB به‌منظور حذف محدودیت‌های پهنای باند به‌منظور ایجاد اتصالات کُند برای دیگر مشترکان یا افزایش پهنای باند خود.
- عامل[7] مدیریت مجاز که فعالیت‌های غیرمجاز انجام می‌دهد.
- مدیریت محتوای غیرمجاز، به طور مثال بارگذاری یا حذف محتوا یا تغییر تاریخ چکانه[8] (تاریخی که محتوا برای مشاهده‌ی عموم در دسترس قرار می‌گیرد).

1- Accidental Access
2- Deliberated Access
۳- نوعی پروتکل نگاشت شماره‌های تلفن به شناسه‌های منحصر به فرد است که بر اساس پروتکل DNS کار می‌کند
4- Digital Rights Management
5- On-board
6- Man In The Middle
7- Agent
8- Trigger Date

- مدیریت مشترک غیرمجاز. به طور مثال فعالیت‌های تدارکاتی غیرمجاز مشترکین شامل ارتقاء/تنزل اختیارات ویژه‌ی مشاهده‌ی[1] مشترکین.

1- Viewing Privileges