INSO-ISO-IEC
27032

1st. Edition

2014

Identical with
ISO/IEC
27032:2012

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

استاندارد ایران ایزو آی ای سی

۲۷۰۳۲

چاپ اول

۱۳۹۳

فناوری اطلاعات - فنون امنیتی- راهنماهایی برای امنیت فضای مجازی

Information technology — Security techniques — Guidelines for cybersecurity

ICS :35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

تدوین استاندارد در حوزه های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود 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 واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به‌عنوان استاندارد ملی ایران چاپ و منتشر می شود. بدین ترتیب ، استانداردهایی ملی تلقی می‌شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1] ،کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه شناسی 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 نیازمندی‌های خاص کشور، از آخرین پیشرفت های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌توانمی‌تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف‌کنندگان ، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می‌تواند به‌منظور حفظ بازارهای بین‌المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش، بازرسی، ممیزی و صدور گواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه 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 آن ها نظارت می‌کند. ترویج افزاره 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 - راهنمایی‌هایی برای امنیت فضای مجازی»

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
اعضاء : (اسامی به ترتیب حروف الفبا)	
جمیل پناه، ناصر (فوق‌لیسانس مدیریت)	کارشناس شرکت مخابرات ایران
سجادیه، علیرضا (فوق‌لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران داده آرای سپاهان
طی نیا، رضا (فوق‌لیسانس مدیریت فناوری اطلاعات)	مدیرعامل شرکت کاربرد سیستم
فولادیان، مجید (فوق‌لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
قسمتی، سیمین (فوق‌لیسانس مهندسی فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
مغانی، مهدی (فوق‌لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نیسی مینایی، آصف (فوق لیسانس فناوری اطلاعات)	پژوهش‌گر دانشگاه شهید بهشتی
یوسف‌زاده، سمیرا (فوق‌لیسانس مهندسی کامپیوتر نرم‌افزار)	پژوهش‌گر دانشگاه شهید بهشتی

فهرست مندرجات

پیش‌گفتار

استاندارد «فناوری اطلاعات - فنون امنیتی - راهنمایی‌هایی برای امنیت فضای مجازی» که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و درسیصد و چهل و پنجمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۹۳/۴/۲۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن‌ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ 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 27032:2012, Information technology — Security techniques Guidelines for cybersecurity

مقدمه

فضای مجازی[1] محیط پیچیده‌ای ناشی از تعامل مردم، نرم‌افزار و خدمات در اینترنت است، بوسیله‌ی افـزاره‌هـا و شبکه‌های متصل فناوری ارتباطات و اطلاعات[2] فیزیکی توزیع‌شده جهانی پشتیبانی شده است. بااین‌حال مسـائل امنیتی وجود دارد که به‌وسیله امنیت اطلاعات کنونی، امنیت اینترنت، امنیت شبکه و به‌روش‌های[3] امنیت ICT موجود، پوشش داده نمی‌شوند. همانگونه که شکاف‌هایی بین این حوزه‌ها وجود دارد، همچنین عدم ارتباط بـین سازمان‌ها و ارائه‌دهندگان خدمات در فضای مجازی نیز وجود دارد. دلیل این است کـه افـزاره‌هـا و شـبکه‌هـای متصل که فضای مجازی را پشتیبانی کرده‌اند مالکین مختلفی دارند که هر کدام کسب‌وکار خـود و نگرانـی‌هـای عملیاتی و نظارتی خاص خود را دارند. تمرکزهای مختلفی که توسط هر سازمان و ارائه‌دهنده در فضای مجـازی در حوزه‌های امنیتی مربوطه که در آن ورودی کمی از یک سازمان یا ارائه‌دهنـده گرفتـه شـده یـا هـیچ ورودی دریافت نکرده‌اند، قرار داده شده است و منجر به حالت پراکنده امنیت فضای مجازی شده است.

به‌این‌ترتیب، اولین حوزه تمرکز این استاندارد ملی ایران نشانی‌دهی به امنیت فضای مجازی یا مسائل مربوط به امنیت فضای مجازی[4] است که شکاف بین حوزه‌های مختلف امنیتی در فضای مجازی را به هم مرتبط می‌کنـد. به طور خاص این استاندارد ملی ایران راهنمایی فنی برای مقابله با مخاطرات امنیت فضای مجازی متداول ارائـه می‌دهد، شامل موارد زیر است:

- حمله‌های مهندسی اجتماعی؛
- رخنه کردن[5]
- گسترش نرم‌افزارهای مخرب یا خرابکارانه (بدافزار)[6]؛
- نرم‌افزارهای جاسوسی[7] و
- سایر نرم‌افزارهای ناخواسته بالقوه

راهنمایی فنی کنترل‌ها مخاطرات را ارائه می‌دهد، که از آن جمله به بازبینی‌های زیر می‌توان اشاره نمود:

- تجهیز در مقابل حمله، برای نمونه، بدافزار، افراد شرور، یا سازمان‌های جنایی[8] در اینترنت؛
- شناسایی و پایش بر حمله‌ها و
- پاسخ به حمله‌ها

ناحیه دوم تمرکز این استاندارد ملی ایران ، بر همکاری است اشتراک‌گذاری کارآمد و موثر اطلاعات، هماهنگی و رسیدگی به رخداد در میان ذی‌نفعان در فضـای مجـازی، مـورد نیـاز اسـت. ایـن تعامـل بایـد بـه روش امـن و قابل‌اعتماد انجام شود که از حریم خصوصی افراد نگران هم، حفاظت کند. بسیاری از این ذی‌نفعان می‌تواننـد در

1- Cyberspace
2- Information and Communications Technology (ICT)
3- Best Practices
4- Cybersecurity
5- Hacking
6- Malware
7- Spyware
8- Criminal organizations

مکان‌های مختلف جغرافیایی و محدوده‌های زمانی مستقر باشند و به‌احتمال زیاد با الزامات قانونی مختلف اداره شوند. ذی‌نفعان عبارت‌اند از:

- مصرف‌کنندگان که می‌توان انواع مختلف سازمان‌ها یا افراد را نام برد و
- ارائه‌دهندگان که شامل ارائه‌دهندگان خدمات است.

بنابراین، این استاندارد ملی ایران چارچوبی برای موارد زیر هم فراهم می‌کند:

- اشتراک‌گذاری اطلاعات،
- هماهنگی و
- رسیدگی به رخداد عملیاتی

چارچوب شامل موارد زیر است:

- عناصر کلیدی ملاحظات برای ایجاد اعتماد،
- فرایندهای لازم برای همکاری و تبادل و به اشتراک‌گذاری اطلاعات
- الزامات فنی برای یکپارچه‌سازی سامانه‌ها و قابلیت همکاری بین ذی‌نفعان مختلف.

با توجه به دامنه این استاندارد ملی ایران ، نظارت‌های ارائه‌شده لزوماً در سطح بالا است. برای راهنمایی بیشتر استانداردهای دقیق مشخصات فنی و راهنمایی‌های قابل‌اجرا برای هر ناحیه، داخل این استاندارد ملی ایران اشاره شده است.

فناوری اطلاعات - فنون امنیتی – راهنمایی‌هایی برای امنیت فضای مجازی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی ایران تعیین راهنما برای بهبود وضعیت امنیت فضای مجازی است و جنبه‌های منحصربه‌فرد فعالیت مورد نظر و وابستگی‌های آن در دیگر حوزه‌های امنیتی را گسترش می‌دهد، به‌ویژه:

- امنیت اطلاعات،
- امنیت شبکه،
- امنیت اینترنت و
- حفاظت زیرساخت اطلاعات حیاتی (CIIP)[1]

این استاندارد ملی ایران شیوه‌های امنیتی پایه برای ذی‌نفعان در فضای مجازی را با موارد زیر پوشش می‌دهد:

- مروری بر امنیت فضای مجازی،
- تبیین رابطه میان امنیت فضای مجازی و انواع دیگر امنیت،
- تعریف ذی‌نفعان و شرح نقش آن‌ها در زمینه امنیت فضای مجازی ،
- راهنمایی برای پرداختن به مسائل مربوط به امنیت فضای مجازی متداول و
- چارچوبی برای توانمندسازی ذی‌نفعان در همکاری برای حل و فصل مسائل مربوط به امنیت فضای مجازی.

۲ کاربردپذیری[2]

۲-۱ مخاطب[3]

این استاندارد ملی ایران برای ارائه‌دهندگان خدمات در فضای مجازی کاربردپذیر است. بااین‌حال، مخاطب، شامل مصرف‌کنندگانی است که از این خدمات استفاده می‌کنند. جایی که سازمان‌ها در فضای مجازی به مردم برای استفاده در خانه یا دیگر سازمان‌ها خدمات ارائه می‌دهند، ممکن است نیازمند ارائه راهنمایی بر اساس این استاندارد ملی ایران باشند که شامل توضیحات افزوده یا نمونه‌های کافی است تا به خواننده اجازه درک و عمل به آن را بدهد.

۲-۲ محدودیت‌ها[4]

این استاندارد ملی ایران برای موارد زیر کاربرد ندارد:

- ایمنی مجازی
- جرم مجازی
- CIIP

1- Critical information infrastructure protection
2- Applicability
3- Audience
4- Limitations

- ایمنی اینترنت و
- جرم مرتبط با اینترنت.

وجود رابطه‌ی موجود میان حوزه‌های ذکرشده و امنیت فضای مجازی به رسمیت شناخته شده است. بااین‌حال، حوزه این استاندارد ملی ایران برای رسیدگی به این روابط و به اشتراک‌گذاری بازبینی بین این حوزه فراتر است. توجه به این نکته مهم است که مفهوم جرم مجازی، اگر چه ذکر شد، مورد بررسی واقع نشده است. این استاندارد ملی ایران در مورد جنبه‌های مربوط به قانون فضای مجازی، یا تنظیم امنیت فضای مجازی رهنمودی ارائه نمی‌دهد. راهنمای این استاندارد ملی ایران به تحقق فضای مجازی در اینترنت، از جمله نقاط انتهایی[1] محدود شده است. بااین‌حال، گسترش فضای مجازی برای دیگر نمودهای فضایی از طریق رسانه‌های ارتباطی و سکو و نه جنبه‌های امنیت فیزیکی آنها نشان داده نشده است.

مثال ۱- حفاظت از عناصر زیرساخت مانند حامل‌های ارتباطات که زیربنای فضای مجازی هستند، نشان داده نشده است.

مثال ۲- امنیت فیزیکی تلفن‌های همراه که برای بارگیری محتوا و/یا دست‌کاری، به فضای مجازی متصل می‌شوند، نشان داده نشده است.

مثال ۳- پیام‌رسانی متنی و کارکردهای گپ صوتی[2] ارائه‌شده برای تلفن‌های همراه نشان داده نشده است.

۳ 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 تاریخ تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

3-1 ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

۴ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف مشخص‌شده در زیر و در استاندارد ملی ایران شمارهٔ ۲۷۰۰۰، به‌کار می‌روند:

۴-۱ آگهی‌افزار[3]

برنامه کاربردی[1] که تبلیغات را به کاربران ارائه و/یا رفتار برخط[2] کاربر را گردآوری می‌کند.

1- Endpoint
2- Voice chat
3- Adware

یادآوری- ممکن است این برنامه‌ها با آگاهی یا رضایت کاربر نصب شده باشند یا کاربر مجبور شود توافق کند که با صدور مجوز جهت نصب نرم‌افزار دیگری این برنامه را نصب کند.

۲-۴ برنامه کاربردی

راه حل مبتنی بر فناوری اطلاعات، از جمله نرم‌افزار کاربردی، داده‌ها و روش‌های برنامه کاربردی، که برای کمک به کاربران سازمان طراحی شده است تا کارهای خاص انجام دهد یا با خودکار کردن یک فرآیند کسب‌وکار یا کارکرد، به انواع خاصی از مشکلات فناوری اطلاعات رسیدگی کند. به استاندارد ملی ایران ۱-۲۷۰۳۴ مراجعه شود.

۳-۴ ارائه‌دهنده خدمات برنامه کاربردی

کاروری[3] که میزبانی یک راه‌حل نرم‌افزاری را فراهم می‌کند تا خدمات برنامه کاربردی را که شامل مدل‌های[4] انتقالی مبتنی بر وب یا کارساز-کارخواه هستند، ارائه دهد.

مثال- کارورهای بازی برخط، ارائه‌دهندگان برنامه کاربردی دفتری و ارائه‌دهندگان انباره‌ی برخط

۴-۴ خدمات برنامه کاربردی

نرم‌افزاری با قابلیت پاسخ، به‌محض تقاضای مشترکان از طریق یک مدل برخط شامل برنامه‌های کاربردی مبتنی بر وب یا کارساز-کارخواه است.

۵-۴ نرم‌افزار کاربردی[5]

نرم‌افزاری که مجزا از نرم‌افزاری که رایانه را کنترل می‌کند، برای کمک به کاربران برای انجام کارهای خاص یا رسیدگی به انواع خاصی از مشکلات طراحی شده است.

[ISO / IEC 18019]

۶-۴ دارایی

هر چیزی که برای فرد، سازمان یا دولت ارزش داشته باشد.

یادآوری- از استاندارد ملی ایران شماره ۲۷۰۰۰، پیش‌بینی برای افراد و جدایی دولت از سازمان برداشت شده است (۴-۳۷).

۷-۴ چهرک[6]

چهرک شخصی که در فضای مجازی شرکت می‌کند.

یادآوری ۱- همچنین چهرک می‌تواند به‌عنوان شخصیت همزاد[7] فرد نیز مورد ارجاع واقع شود.

یادآوری ۲- چهرک همچنین می‌تواند به‌عنوان «شیء» به نمایندگی از تصویر کاربر دیده شود.

1- Application
2- Online
3- Operator
4- Models
5- Application Software
6 -Avatar
7- Alter Ego

۴-۸ حمله[1]

تلاش برای از بین بردن، افشاء، تغییر، غیرفعال کردن، سرقت یا به‌دست آوردن دسترسی‌های غیرمجاز یا استفاده‌ی غیرمجاز از دارایی است.
استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱.

۴-۹ بالقوگی حمله[2]

برای احساس موفقیت بالقوه‌ی حمله، توصیه می‌شود حمله‌ای شروع و بر حسب تخصص، منابع و انگیزه مهاجم بیان شود.
[ISO / IEC 15408-1:2005]

۴-۱۰ بردار حمله[3]

مسیر یا وسیله‌ای که به‌وسیله آن مهاجم می‌تواند به یک رایانه یا کارساز شبکه به‌منظور انتقال خروجی‌های مخرب دست یابد.

۴-۱۱ حمله ترکیبی[4]

حمله‌ای که به دنبال بیشینه کردن شدت آسیب و سرعت انتقال با ترکیب روشگان‌های متعدد حمله است.

۴-۱۲ بات[5]

نرم‌افزار خودکار که برای انجام وظایف خاص استفاده می‌شود.

یادآوری ۱- این کلمه اغلب برای توصیف برنامه‌ها، به طور معمول آن دسته که روی کارساز اجرا می‌شود مورد استفاده قرار می‌گیرد که به طور خودکار وظایفی مانند ارسال یا مرتب‌سازی رایانامه را انجام می‌دهد.

یادآوری ۲- همچنین ربات به‌عنوان برنامه‌ای که به‌عنوان یک عامل برای یک کاربر یا یک برنامه دیگر یا شبیه‌سازی یک فعالیت انسانی است شرح داده شده است. در اینترنت، ربات‌هایی که در همه جا حاضرند برنامه‌های عنکبوت یا خزنده[6] نیز نامیده می‌شوند که با دسترسی به وب‌گاه‌ها مطالب آنها را برای شاخص‌گذاری موتورهای جستجو جمع‌آوری می‌کند.

۴-۱۳ بات‌نت[7]

نرم‌افزار کنترل از راه دور، به‌ویژه مجموعه‌ای از ربات‌های مخرب که به‌صورت خودگردان یا خودکار بر روی رایانه‌ی در معرض خطر اجرا می‌شوند.

1- Attack
2- Attack Potential
3- Attack Vector
4- Blended Attack
5- Bot
6- Spiders or Crawlers
7- Botnet

۴-۱۴ کوکی[1]

قابلیت <کنترل دستیابی> قابلیت در سامانه کنترل دسترسی است.

۴-۱۵ کوکی

<امنیت پروتکل اینترنت>[2] داده‌های مبادله شده توسط پروتکل کلیدی مدیریت و انجمن امنیتی اینترنت(ISAKMP)[3] که از برخی حملات منع خدمت[4] با ایجاد یک انجمن امنیت جلوگیری می‌کنند.

۴-۱۶ کوکی

<HTTP>[5]داده‌های مبادله شده بین کارساز HTTP و مرورگر برای ذخیره اطلاعات حالت در سمت کارخواه تا در آینده برای استفاده از آن در کارساز بازیابی شود.

یادآوری- مرورگر وب می‌تواند کارساز یا کارخواه باشد.

۴-۱۷ کنترل

اقدام متقابل[6]

ابزار مدیریت مخاطره، از جمله خط‌مشی‌ها، روش‌ها، دستورالعمل‌ها، شیوه‌ها یا ساختار سازمانی که به طور معمول می‌تواند اداری، فنی، مدیریتی، یا حقوقی محسوب شود.

[استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱]

یادآوری- راهنمای ISO شماره ۷۳ به سادگی، کنترل را به‌عنوان معیاری برای بهبود مخاطره تعریف می‌کند.

۴-۱۸ جُرم رایانه‌ای

فعالیت‌های مجرمانه که در آن خدمات یا برنامه‌های کاربردی در فضای مجازی برای اهداف مجرمانه استفاده می‌شوند یا هدف جرم و جنایت هستند، یا فضای مجازی منبع، ابزار، هدف یا محل جرم است.

۴-۱۹ ایمنی فضای مجازی

وضعیت محافظت در برابر نتایج فیزیکی، اجتماعی، معنوی، مالی، سیاسی، عاطفی، شغلی، روانشناسی، آموزشی یا دیگر انواع یا عواقب شکست، آسیب، خطا، حوادث، خسارت یا هر رویداد دیگر در فضای مجازی که ممکن است نامطلوب به نظر آید.

یادآوری ۱- این مورد می‌تواند شکل حفاظت از رویداد یا در معرض چیزی قرار گرفتن را بگیرد که باعث وارد شدن زیان سلامت یا اقتصادی شود. می‌تواند شامل حفاظت از مردم یا دارایی‌ها شود.

یادآوری ۲- به طور کلی ایمنی به‌عنوان حالتی از اطمینان تعریف می‌شود که عوارض جانبی بواسطه‌ی عامل‌ها تحت شرایط تعریف‌شده ایجاد نمی‌شود.

1- Cookie
2- Internet Protocol Security(IPSec)
3- Internet Security Association and Key Management Protocol
4- Denial-of-Service
5- Hyper text transfer Protocol
6- Countermeasure

۲۰-۴ امنیت فضای مجازی

امنیت فضای مجازی[1]

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات در فضای مجازی است.

یادآوری ۱- علاوه بر این، می‌تواند شامل دیگر ویژگی‌ها از قبیل اعتبار، مسئولیت‌پذیری، سلب انکار و قابلیت اطمینان نیز باشد.

یادآوری ۲- از تعریف امنیت اطلاعات در استاندارد ملی ایران شماره ۲۷۰۰۰، برداشت شده است.

۲۱-۴ فضای مجازی

محیط پیچیده ناشی از تعامل مردم، نرم‌افزار و خدمات اینترنت با استفاده از افزاره‌های فناوری و شبکه‌های متصل به آن که به شکل فیزیکی وجود ندارد.

۲۲-۴ خدمات برنامه کاربردی فضای مجازی

خدمات برنامه کاربردی (۴-۴) که روی فضای مجازی ارائه شده است.

۲۳-۴ فرصت‌طلب رایانه‌ای[2]

افراد یا سازمان‌هایی که URLهایی را که شبیه به مراجع یا نام دیگر سازمان‌ها در دنیای واقعی یا فضای مجازی است ثبت و نگهداری می‌کنند.

۲۴-۴ نرم‌افزار فریبنده

نرم‌افزاری که روی رایانه کاربر بدون اطلاع‌رسانی اولیه راجع به آنچه که نرم‌افزار بر روی رایانه انجام می‌دهد یا بدون پرسش در مورد رضایت کاربر برای این اقدامات به انجام فعالیت‌هایی می‌پردازد.

مثال ۱- برنامه‌ای که پیکربندی کاربر را می‌رباید.

مثال ۲- برنامه‌ای که موجب تبلیغات بالاپر[3] بی‌پایان می‌شود که به‌راحتی توسط کاربر متوقف نمی‌شود.

مثال ۳- آگهی‌افزار و جاسوس‌افزار[4]

۲۵-۴ ۲۵-۴ رخنه‌گری[5]

دسترسی عمدی به یک سامانه‌ی رایانه‌ای بدون اجازه گرفتن از کاربر یا مالک آن است.

۲۶-۴ اصول رخنه‌گری

رخنه به هدف سیاسی یا انگیزه‌های اجتماعی است.

۲۷-۴ دارایی اطلاعاتی

دانش یا داده‌هایی که برای فرد یا سازمان دارای ارزش است.

1- Cyberspace security
2- Cyber-squatter
3- Popup
4- Spyware
5- Hacking

یادآوری- از استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، برداشت شده است.

۲۸-۴ اینترنت

شبکه داخلی

مجموعه‌ای از شبکه‌های متصل است.

یادآوری ۱- اقتباس از استاندارد ملی ایران شماره ۱-۱۴۸۶۶ سال ۱۳۹۱.

یادآوری ۲- در این زمینه، مرجع به «یک اینترنت» خواهد بود. تفاوتی بین تعریف «یک اینترنت[1]» و «اینترنت[2]» وجود دارد.

۲۹-۴ اینترنت

سامانه جهانی از شبکه‌های متصل‌شده‌ی داخلی در دامنه‌ی عمومی است.

[استاندارد ملی ایران شماره ۱-۱۴۸۶۶ سال ۱۳۹۱]

یادآوری- بین تعریف «یک اینترنت» و «اینترنت» تفاوت وجود دارد.

۳۰-۴ جرم اینترنتی

خدمات یا برنامه‌های کاربردی در اینترنت که برای فعالیت‌های مجرمانه استفاده می‌شود یا هدف جرم است یا جایی که اینترنت منبع، ابزار، هدف یا محل جرم است.

۳۱-۴ ایمنی اینترنت

محافظت در برابر عواقب فیزیکی، اجتماعی، معنوی، مالی، سیاسی، عاطفی، شغلی، روانی، آموزشی و یا انواع دیگر یا نتیجه شکست، آسیب، خطا، حوادث، آزار یا هر رویداد دیگر در اینترنت که نامطلوب به نظر می‌آید.

۳۲-۴ امنیت اینترنت

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات در اینترنت است.

۳۳-۴ خدمات اینترنت

خدماتی که به کاربر برای فراهم کردن دسترسی به اینترنت از طریق یک نشانی IP اختصاص داده‌شده، ارائه می‌شود و به طور معمول شامل اصالت‌سنجی[3]، مجوزسنجی و دامنه‌ی خدمات نام دامنه است.

۳۴-۴ ارائه‌دهنده خدمات اینترنت

سازمانی که خدمات اینترنت را به کاربر ارائه می‌دهد و به مشتریان خود امکان دسترسی به اینترنت را می‌دهد.

یادآوری- همچنین گاهی اوقات به‌عنوان ارائه‌دهنده دسترسی به اینترنت خوانده می‌شود.

1- An Internet
2- The Internet
3- Authentication

۳۵-۴ بدافزار

نرم‌افزار مخرب

نرم‌افزاری که با قصد خرابکارانه طراحی شده است حاوی ویژگی‌ها یا قابلیت‌هایی است که به طور بالقوه باعث آسیب مستقیم یا غیرمستقیم به کاربر و/یا از سامانه رایانه‌ای کاربران می‌شود.

مثال- ویروس‌ها، کرم‌ها، اسب‌های تروا.

۳۶-۴ محتویات خرابکارانه

برنامه‌های کاربردی، اسناد، پرونده‌ها، داده‌ها یا منابع دیگر که دارای ویژگی‌های خرابکارانه یا قابلیت‌های تعبیه-شده، مبدل یا پنهان در آنها هستند.

۳۷-۴ سازمان

گروهی از مردم و امکانات با ترتیبی از مسئولیت‌ها، مقامات و روابط است.

[استاندارد ملی ایران شماره ۹۰۰۰: سال ۱۳۸۷]

یادآوری ۱- در متن این استاندارد ملی ایران، فرد مجزا از سازمان است.

یادآوری ۲- به طور کلی، دولت یک سازمان است. برای وضوح در متن این استاندارد ملی ایران، دولت‌ها را می‌توان جدای از سازمان‌های دیگر در نظر گرفت.

۳۸-۴ دزدی هویت[1]

فرآیند جعلی جهت به‌دست آوردن اطلاعات شخصی یا محرمانه با تغییر ظاهر به شکل یک هستار قابل‌اعتماد در ارتباطات الکترونیکی می‌باشد.

یادآوری- دزدی هویت را می‌توان با استفاده از مهندسی اجتماعی یا فریب فنی انجام داد.

۳۹-۴ دارایی فیزیکی

دارایی که وجود ملموس یا مادی دارد.

یادآوری- دارایی‌های فیزیکی معمولاً به پول نقد، تجهیزات، موجودی و اموال متعلق به فرد یا سازمان اشاره دارد. نرم‌افزار را می-توان به‌عنوان یک دارایی نامشهود، یا دارایی غیر فیزیکی فرض کرد.

۴۰-۴ نرم‌افزار ناخواسته بالقوه

نرم‌افزار فریبنده، شامل نرم‌افزارهای مخرب و غیر مخرب که ویژگی‌های نرم‌افزار فریبنده را به نمایش در می‌آورد.

۴۱-۴ کلاه‌برداری[2]

فریب یا کلاه‌برداری از راه جلب اعتماد[3].

1- Phishing
2- Scam
3- Confidence Trick

۴-۴۲ نامه الکترونیکی ناشناس[1]

سوءاستفاده از سامانه‌های پیام‌رسانی الکترونیکی تا پیام‌های ناخواسته را مداوم ارسال کنند.

یادآوری- درحالی‌که گسترده‌ترین شکل شناخته‌شده نامه الکترونیکی ناشناس، رایانامه نامه الکترونیکی ناشناس است، این عبارت به سوءاستفاده‌های مشابه در سایر رسانه‌ها اعمال می‌شود: پیام‌رسانی فوری نامه الکترونیکی ناشناس، نامه الکترونیکی ناشناس شبکه گروه خبری[2]، نامه الکترونیکی ناشناس وب‌گاه موتور جستجو، نامه الکترونیکی ناشناس در وب‌نوشت‌ها، نامه الکترونیکی ناشناس ویکی، نامه الکترونیکی ناشناس پیام‌های تلفن همراه ، نامه الکترونیکی ناشناس انجمن اینترنتی و انتقال دورنگارهای ناخواسته.

۴-۴۳ جاسوس‌افزار[3]

نرم‌افزار فریبنده است که اطلاعات خصوصی یا محرمانه را از رایانه کاربر جمع‌آوری می‌کند.

یادآوری- اطلاعات مورد توجه می‌تواند شامل موضوع‌هایی مانند وب‌گاه‌هایی که اخیراً بیشترین بازدید را داشته‌اند یا اطلاعات حساس‌تری مانند کلمات عبور باشد.

۴-۴۴ ذی‌نفع[4]

<مدیریت مخاطره> شخص یا سازمانی که می‌تواند روی تصمیم یا فعالیتی تأثیرگذارد یا از آن تأثیر پذیرد یا خود را تحت تأثیر آن‌ها بداند.

۴-۴۵ ذی‌نفع

<سامانه> فرد یا سازمان با داشتن حق به اشتراک‌گذاری، ادعا یا علاقه به یک سامانه یا در اختیار داشتن ویژگی‌های آن که نیازها و انتظارات آن را برآورده می‌کند.

[استاندارد ملی ایران شماره ۱۲۲۰۷: سال ۱۳۹۰]

۴-۴۶ تهدید[5]

علت بالقوه یک اتفاق ناخواسته که در نتیجه آن ممکن است به سامانه، افراد یا سازمان‌ها آسیب برسد.

یادآوری- از استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱، اقتباس شده است.

۴-۴۷ اسب تروا

بدافزاری که به نظر می‌رسد قصد انجام یک کار مطلوب دارد.

۴-۴۸ رایانامه ناخواسته[6]

رایانامه‌ای که از آن استقبال نمی‌شود یا درخواست یا فراخوانده نشده باشد.

1- Spam
2- Usenet Newsgroup
3- Spyware
4- Stakeholder
5- Threat
6- Unsolicited Email

۴-۴۹ دارایی مجازی

نمایانگر یک دارایی در فضای مجازی می‌باشد.

یادآوری- در این زمینه، پول رایج را می‌توان به‌صورت یک وسیله‌ی مبادله یا یک دارایی که در یک محیط خاص دارای ارزش است، مانند یک بازی ویدئویی یا یک تمرین شبیه‌سازی معاملات مالی تعریف نمود.

۴-۵۰ پول رایج مجازی

دارایی‌های مجازی پولی می‌باشد.

۴-۵۱ دنیای مجازی

محیط شبیه‌سازی که کاربران متعدد از طریق یک واسط[1] برخط به آن دسترسی دارند.

یادآوری ۱- اغلب محیط‌های شبیه‌سازی شده تعاملی هستند.

یادآوری ۱- دنیای فیزیکی و ویژگی‌های مرتبط که مردم در آن زندگی می‌کنند، برای متمایز ساختن از دنیای مجازی «دنیای واقعی» خوانده خواهد شد.

۴-۵۲ آسیب‌پذیری[2]

ضعف یک دارایی یا کنترل که ممکن است به‌واسطه‌ی یک تهدید مورد بهره‌کشی[3] قرار گیرد.

[استاندارد ملی ایران شماره ۲۷۰۰۰: سال ۱۳۹۱]

۴-۵۳ زامبی[4]

رایانه زامبی

رایانه بدون سرنشین و کنترل

رایانه‌ای که شامل نرم‌افزار پنهان است و قادر به کنترل دستگاه از راه دور است و معمولاً حمله‌ای را روی رایانه‌ی دیگری اجرا می‌کند.

یادآوری- به طور معمول رایانه تخریب شده تنها یکی از مواردی است که در باتنت است، و برای انجام فعالیت‌های خرابکارانه از راه دور استفاده می‌شود.

۵ کوته‌نوشت‌ها

AS	Autonomous System	سامانه خودگردان
AP	Access Point	نقطه دسترسی
CBT	Computer Based Training	آموزش مبتنی بر رایانه
CERT	Computer Emergency Response Team	گروه واکنش اضطراری رایانه‌ای

1- Interface
2- Vulnerability
3- Exploit
4- Zombie

CIRT	Computer Incident Response Team	گروه واکنش به رخداد رایانه
CSIRT	Computer Security Incident Response Team	گروه واکنش به رخداد امنیت رایانه
CIIP	Critical Information Infrastructure Protection	حفاظت زیرساخت اطلاعات حیاتی
DoS	Denial-of-Service	منع خدمت
DDoS	Distributed Denial-of-Service	منع خدمت توزیع‌شده
HIDS	Host-based Intrusion Detection System	سامانه تشخیص نفوذ مبتنی بر میزبان
IAP	Independent Application Provider	ارائه‌دهنده برنامه‌کاربردی مستقل
ICMP	Internet Control Message Protocol	پروتکل کنترل پیام اینترنت
ICT	Information and Communications Technology	فناوری اطلاعات و ارتباطات
IDS	Intrusion Detection System	سامانه تشخیص نفوذ
IP	Internet Protocol	پروتکل اینترنت
IPO	Information Providing Organization	سازمان ارائه‌دهنده اطلاعات
IPS	Intrusion Prevention System	سامانه جلوگیری از نفوذ
IRO	Information Receiving Organization	سازمان دریافت‌کننده اطلاعات
ISP	Internet Service Provider	ارائه‌دهنده خدمات اینترنت
ISV	Independent Software Vendor	فروشنده مستقل نرم‌افزار
IT	Information Technology	فناوری اطلاعات
MMORPG	Massively Multiplayer Online Role-Playing Game	بازی نقش افرینی بر خط چند نفره گسترده
NDA	Non-Disclosure Agreement	توافقنامه عدم افشا
SDLC	Software Development Life-cycle	چرخه عمر تولید نرم‌افزار
SSID	Service Set Identifier	شناسانه مجموعه خدمات
TCP	Transmission Control Protocol	پروتکل کنترل انتقال
UDP	User Datagram Protocol	پروتکل بسته داده کاربر
URI	Uniform Resource Identifier	شناساگر یکنواخت منبع
URL	Uniform Resource Locator	نشانی وب (موقعیت‌یاب همسان منبع)

۶ مرور کلی

۶-۱ مقدمه

امنیت در اینترنت و در فضای مجازی موضوع مورد توجه رو به رشدی بوده است. ذی‌نفعان حضور خود در فضای مجازی را از طریق وب‌گاه‌ها استقرار کرده‌اند و اکنون در تلاش برای نفوذ بیش‌تر در دنیای مجازی با کمک فضای مجازی هستند.

مثال: افزایش تعداد افرادی که مقادیر فزاینده‌ای از زمان را با چهرک‌های مجازی خود در MMORPGها سپری می‌کنند.

درحالی‌که برخی از افراد در مدیریت هویت برخط خود دقیق هستند، بسیاری از مردم جزئیات شخصی خود را برای به اشتراک گذاشتن با دیگران ارسال می‌کنند. بسیاری از اطلاعات اشخاص که در وب‌گاه‌ها، به‌ویژه وب‌گاه-های شبکه‌های اجتماعی و اتاق‌های گفتگو موجود است، ممکن است توسط اشخاص دیگر دریافت و ذخیره شود. ممکن است، پرونده اطلاعات شخصی ایجاد شود که می‌تواند مورد استفاده نابجا قرار گیرد و برای دیگران افشا شود، یا به جمع‌آوری داده‌های ثانویه منجر شود. درحالی‌که در دقت و یکپارچگی این داده‌ها تردید وجود دارد، به افراد و سازمان‌هایی که اغلب به طور کامل از بین نمی‌روند، پیوند ایجاد می‌کنند.

این پیشرفت‌ها در حوزه‌های ارتباطات، سرگرمی، حمل‌ونقل، خرید، مالی، بیمه و حوزه بهداشت و درمان مخاطرات جدیدی را برای ذی‌نفعان در فضای مجازی ایجاد می‌کند؛ بنابراین، مخاطرات با از دست دادن حریم خصوصی می‌توانند در ارتباط باشند.

همگرایی فناوری اطلاعات و ارتباطات، سهولت وارد شدن به فضای مجازی، و محدود شدن فضای شخصی بین افراد، توجه اشرار و سازمان‌های جنایی را جلب کرده است. این هستارها از ساز و کارهای موجود، مانند دزدی هویت، نامه الکترونیکی ناشناس و جاسوس‌افزارها و همچنین شیوه‌های جدیدتر حمله در حال توسعه، برای بهره‌کشی از نقاط ضعفی که در فضای مجازی کشف می‌کنند، استفاده می‌کنند. در سال‌های اخیر، حملات امنیتی در فضای مجازی از رخنه‌گری برای شهرت شخصی به جرم و جنایت سازمان‌یافته، یا جرم رایانه‌ای تبدیل شده است. در حال حاضر مجموعه‌ای از ابزارها و فرآیندهایی که اغلب برای رسیدن به اهداف بدخواهانه در حوادث امنیت فضای مجازی منفرد اخیراً مشاهده شده با حملات چند-ترکیبی[1] استفاده می‌شوند. این اهداف از حملات شخصی، سرقت هویت، کلاه‌برداری مالی یا دزدی تا اصول رخنه‌گری سیاسی گسترده شده‌اند. انجمن‌های تخصصی مسائل بالقوه امنیتی را برجسته می‌نمایند همچنین در جهت نمایش شیوه‌های حمله و فرصت‌های جنایی خدمت ارائه می‌دهند.

حالت‌های متعدد از تراکنش‌های کسب‌وکار که در فضای مجازی انجام شده‌اند به هدف اتحادیه‌های صنفی جرم رایانه‌ای تبدیل می‌شوند. مخاطرات مطرح شده برای خدمات کسب‌وکار به کسب‌وکار دیگر، کسب‌وکار به مصرف‌کننده و مصرف‌کننده به مصرف‌کننده، به‌ذات پیچیده هستند. مفاهیمی مانند آنچه که یک معامله یا قرارداد را تشکیل می‌دهند وابسته به تفسیر قانون هستند و هر یک از طرفین در رابطه با مدیریت مسئولیت خود هستند. اغلب، به مسئله استفاده از داده‌های جمع‌آوری شده در طول تراکنش یا رابطه به‌اندازه کافی پرداخته نشده است. این مسئله در نهایت می‌تواند به نگرانی‌های امنیتی مانند نشت اطلاعات منجر شود.

چالش‌های فنی و حقوقی که این مسائل امنیت فضای مجازی مطرح کرده‌اند ماهیت گسترده و جهانی دارند. چالش‌ها تنها با داشتن امنیت اطلاعات جامعه فنی، جامعه حقوقی، سازمان ملل و جامعه ملت‌ها از طریق یک راهبرد منسجم قابل رسیدگی هستند. این راهبرد باید نقش هر یک از ذی‌نفعان و ابتکارات موجود در چارچوب همکاری‌های بین‌المللی را مورد توجه قرار دهد.

1- Multi-blended

مثال: مثالی برای چالش از این واقعیت که فضای مجازی، موجب گمنامی مجازی و حمله پنهانی می‌شود، نشأت می‌گیرد و تشخیص را دشوار می‌کند. ایجاد اعتماد و هدایت برای افراد و سازمان‌ها، همچنین سازمان‌های مجری قانون برای اجرای خط‌مشی‌های مربوطه به طور فزاینده‌ای دشوار شود. حتی اگر منبع حمله قابل تعیین باشد، مسائل حقوقی و قانونی مرزی، اغلب از پیشرفت بیشتر هرگونه تحقیق یا خروجی قانونی جلوگیری می‌کند.

پیشرفت کنونی برای رسیدگی به این چالش‌ها به‌واسطه بسیاری از مسائل مختل شده است و مسائل مربوط به امنیت فضای مجازی در حال افزایش و تکامل است.

درحالی‌که عدم تهدیدات امنیت فضای مجازی که استاندارد هم نیست وجود ندارد، راه‌های زیادی برای مقابله با آن وجود دارد، تمرکز این استاندارد ملی ایران روی مسائل کلیدی زیر است:

- حملات با استفاده از نرم‌افزارهای مخرب و ناخواسته بالقوه؛
- حملات مهندسی اجتماعی و
- به اشتراک‌گذاری و هماهنگی اطلاعات.

به‌علاوه، برخی ابزارهای امنیت فضای مجازی به طور خلاصه در این استاندارد ملی ایران مورد بحث قرار خواهد گرفت. این ابزارها و مناطق پیشگیری از جرم، تشخیص، پاسخ و تحقیقات مربوطه ارتباط نزدیکی دارند. برای جزئیات بیشتر به ضمیمه الف مراجعه نمایید.

۶-۲ ماهیت فضای مجازی

فضای مجازی را می‌توان به‌عنوان محیطی مجازی که در شکل فیزیکی وجود ندارد، بلکه به عنوان محیط یا فضای ناشی از ظهور اینترنت، به‌علاوه مردم، سازمان‌ها و فعالیت‌ها در انواع افزاره‌های فناوری پیچیده و شبکه‌هایی که به آن متصل است توصیف نمود. امنیت فضای مجازی، یا امنیت فضای مجازی در مورد امنیت این دنیای مجازی است.

بسیاری از دنیاهای مجازی واحد پول رایج مجازی دارند، مانند استفاده از این واحدها برای خرید اقلام بازی[1]. میان واحد پول رایج دنیای واقعی و پول رایج مجازی حتی اقلام بازی، وابستگی وجود دارد. این اقلام مجازی پی‌درپی با پول رایج واقعی در وب‌گاه‌های حراجِ برخط دادوستد می‌شوند و برخی بازی‌ها حتی یک کانال رسمی با پول رایج مجازی یا واقعی اعلام شده برای نرخ مبادله به جهت کسب درآمد از اقلام مجازی دارند. اغلب این کانال‌های کسب درآمد باعث می‌شود دنیای مجازی با انتشار یا دیگر روش‌های دزدی اطلاعات حساب، هدف حمله قرار گیرد.

۶-۳ ماهیت امنیت فضای مجازی

ذی‌نفعان در فضای مجازی به‌منظور سودمندی فضای مجازی فراتر از حفاظت دارایی‌هایشان برای موفقیت باید نقش فعال ایفا کنند. برنامه‌های کاربردی در فضای مجازی فراتر از مدل کسب‌وکار به مصرف‌کنندگان و مصرف‌کنندگان به مصرف‌کنندگان، به‌صورت تراکنش‌ها و معاملات چند به چند[2] در حال گسترش هستند. الزامات

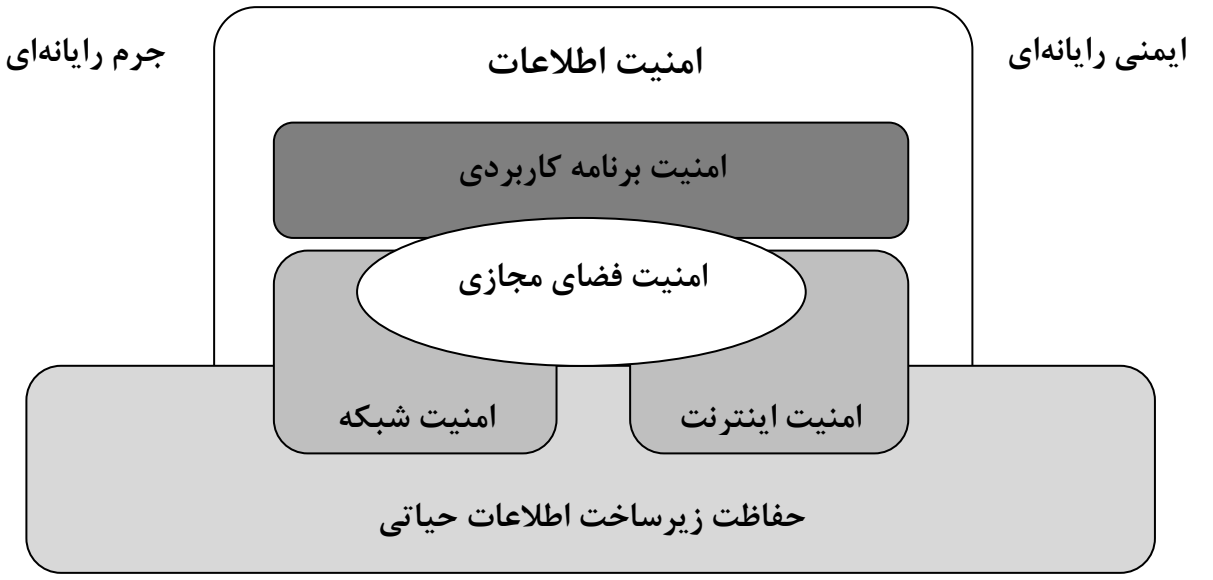
1- In-Game Items
2- Many-To-Many

برای افراد و سازمان‌ها برای آمادگی و رسیدگی به مخاطرات امنیتی در حال ظهور و چالش‌های موثر برای جلوگیری و پاسخ به استفاده‌نابجا و بهره‌کشی جنایی، در حال گسترش است.
توصیه می‌شود امنیت فضای مجازی به اقداماتی که ذی‌نفعان برای ایجاد و حفظ امنیت در فضای مجازی اتخاذ نمایند مربوط شود.
امنیت فضای مجازی اساساً بر امنیت اطلاعات، امنیت نرم‌افزار، امنیت شبکه و امنیت اینترنت متکی است. امنیت فضای مجازی یکی از فعالیت‌های لازم برای CIIP است و هم‌زمان، حفاظت کافی از خدمات زیرساخت حیاتی منجر به نیازهای امنیتی اساسی (به‌عنوان مثال، امنیت، قابلیت اطمینان و در دسترس بودن زیرساخت‌های حیاتی) برای دستیابی به اهداف امنیت فضای مجازی است.
هر چند امنیت مجازی، مترادف امنیت اینترنت، امنیت شبکه، امنیت نرم‌افزار، امنیت اطلاعات، یا CIIP نیست. درصورتی‌که کارایی و قابل‌اعتماد بودن فضای مجازی را بهبود نبخشد، امنیت مجازی دامنه منحصربه‌فردی دارد که نیازمند ایفای نقش فعال ذی‌نفعان به‌منظور نگهداری آن است. این استاندارد ملی ایران میان امنیت فضای مجازی و دیگر حوزه‌های امنیت به شرح زیر تفاوت قائل می‌شود:

- به طور کلی برای امنیت اطلاعات، حفاظت از محرمانگی، یکپارچگی و در دسترس بودن اطلاعات اهمیت دارد تا نیازهای اطلاعاتی کاربردی کاربر را تأمین کند.
- امنیت برنامه کاربردی فرآیندی برای اعمال کنترل و اندازه‌گیری برنامه‌های کاربردی سازمان به‌منظور مدیریت مخاطره است. کنترل‌ها و اندازه‌گیری ممکن است به برنامه کاربردی (فرآیندها، مؤلفه‌ها، نرم‌افزار و نتایج آن)، داده‌های آن (داده پیکربندی، داده‌های کاربر، داده‌های سازمان) و برای تمام فناوری، فرآیندها و عامل‌های درگیر در چرخه زندگی برنامه اعمال شود.
- امنیت شبکه به طراحی، پیاده‌سازی و بهره‌برداری از شبکه برای دستیابی به اهداف امنیت اطلاعات در شبکه درون سازمان، بین سازمان، و بین سازمان‌ها و کاربران رسیدگی می‌کند.
- امنیت اینترنت به حفاظت از خدمات مرتبط با اینترنت و سامانه‌های فناوری اطلاعات و ارتباطات و شبکه‌های مرتبط به‌عنوان الحاقی از امنیت شبکه در سازمان‌ها و در خانه، برای رسیدن به هدف امنیت رسیدگی می‌کند. همچنین امنیت اینترنت در دسترس بودن و قابلیت اطمینان خدمات اینترنت را تضمین می‌کند.
- CIIP به حفاظت سامانه‌هایی که توسط ارائه‌دهندگان زیرساخت حیاتی ارائه یا اداره شده، مانند انرژی، ارتباط از راه دور، اداره آب رسیدگی می‌کند. CIIP تضمین می‌کند که سامانه‌ها و شبکه‌ها در برابر مخاطرات امنیت اطلاعات، امنیت شبکه، امنیت اینترنت و همچنین مخاطرات امنیت فضای مجازی حافظت شده و انعطاف‌پذیر است.

شکل ۱ رابطه بین امنیت و دیگر حوزه‌های امنیتی رایانه‌ای را خلاصه می‌کند. رابطه‌ی بین این حوزه‌های امنیتی و امنیت فضای مجازی پیچیده است. برخی از خدمات در زیرساخت‌های حیاتی، به‌عنوان مثال آب و حمل‌ونقل، نیازمند برخورد مستقیم یا معنی‌دار دولت و امنیت فضای مجازی است. بااین‌حال، عدم وجود امنیت فضای

مجازی ممکن است بر در دسترس بودن سامانه‌های زیرساخت اطلاعاتی بحرانی مهم ارائه‌شده توسط ارائه-دهندگان زیرساخت حیاتی تأثیر منفی داشته باشد.



شکل ۱- ارتباط میان امنیت فضای مجازی و دیگر حوزه‌های امنیتی

از سوی دیگر، دسترس‌پذیری و قابلیت اطمینان فضای مجازی در بسیاری از موارد به دسترس‌پذیری و قابلیت اطمینان خدمات زیرساخت حیاتی مرتبط، از جمله زیرساخت‌های شبکه ارتباطات از راه دور متکی است. به طور کلی امنیت فضای مجازی نیز ارتباط نزدیکی با امنیت اینترنت، سازمان/شبکه خانگی و امنیت اطلاعات مرتبط است. لازم به ذکر است که حوزه‌های امنیتی که در این بخش شناسایی شده اهداف و دامنه تمرکز خود را دارند؛ بنابراین برای مقابله با مسائل مربوط به امنیت فضای مجازی، نیازمند ارتباطات قابل‌توجه و هماهنگی بین هستارهای مختلف خصوصی و دولتی از کشورها و سازمان‌های مختلف است. خدمات زیرساخت‌های بحرانی توسط برخی دولت‌ها به‌عنوان خدمات مرتبط با امنیت ملی در نظر گرفته شده است و در نتیجه ممکن است به طور آشکار مورد بحث قرار نگیرد یا افشا نشود. علاوه بر این، آگاهی از نقاط ضعف زیرساخت‌های بحرانی، در صورت استفاده نامناسب، می‌تواند مفهومی مستقیم برای امنیت ملی داشته باشد؛ بنابراین چارچوب اساسی برای به اشتراک‌گذاری اطلاعات و مسائل یا هماهنگی رویداد برای ایجاد پل بین شکاف‌ها و ارائه تضمین کافی برای ذی‌نفعان در فضای مجازی است.

۶-۴ مدل عمومی

۶-۴-۱ مقدمه

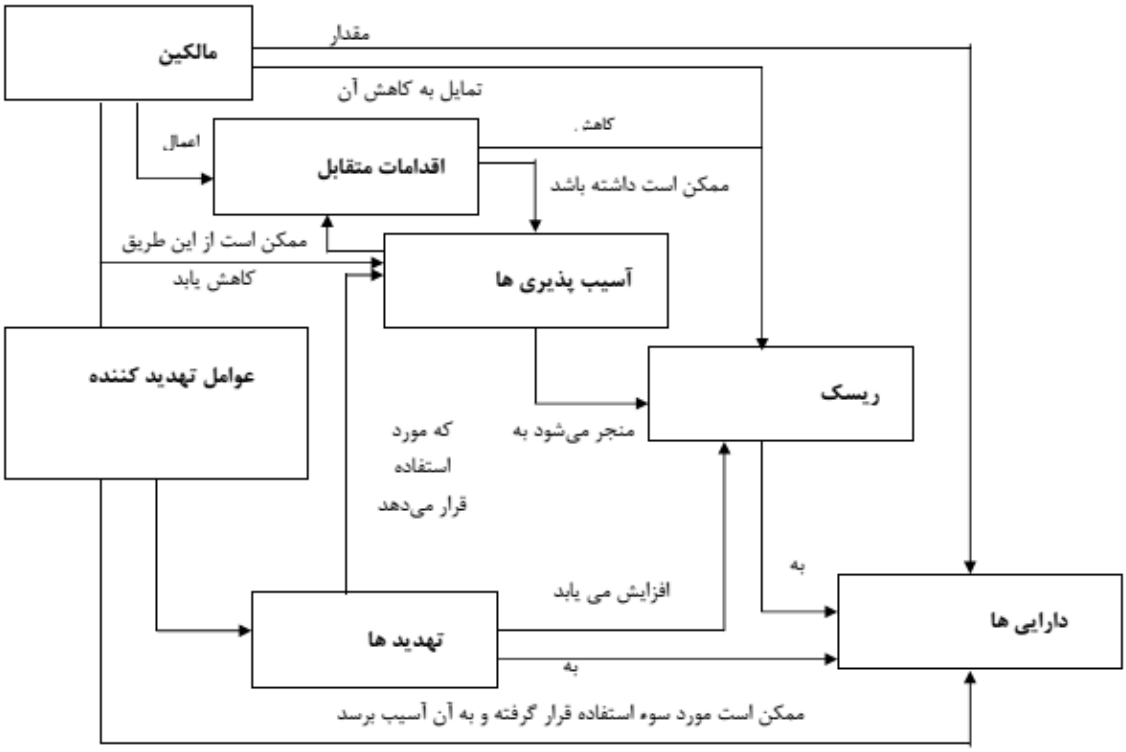
این بند مدل کلی مورد استفاده در سراسر این استاندارد ملی ایران را ارائه می‌دهد. در این بند فرض می‌شود مقداری دانش امنیت وجود دارد و راهنمای آموزشی در این زمینه پیشنهاد نمی‌دهد. این استاندارد ملی ایران با استفاده از مجموعه‌ای از مفاهیم و واژگان به بحث در مورد امنیت می‌پردازد. درک این مفاهیم و واژگان پیش‌نیاز

موثر برای استفاده از این استاندارد ملی ایران است. بااین‌حال، خود مفاهیم بسیار کلی هستند و قصد محدود کردن آن‌دسته مسائل امنیتی فناوری اطلاعات را که این استاندارد ملی ایران در مورد آن‌ها قابل‌اجرا است، ندارند.

۶-۴-۲ زمینه عمومی امنیت

امنیت به حفاظت دارایی‌ها در مقابل تهدیدات می‌پردازد که در آن تهدید به‌عنوان عامل بالقوه برای سوءاستفاده از دارایی‌های حفاظت‌شده دسته‌بندی شده است. توصیه می‌شود تمام دسته‌بندی‌های تهدیدات در نظر گرفته شود؛ اما در حوزه امنیت بیش‌تر توجه به تهدیداتی که مربوط به فعالیت‌های انسانی مخرب یا دیگر فعالیت‌ها معطوف است. شکل ۲ این مفاهیم سطح بالا و روابط را نشان می‌دهد.

یادآوری- شکل ۲ از استاندارد شماره ۱-۱۵۴۰۸ سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی- معیار ارزیابی امنیت فناوری اطلاعات- قسمت۱- معرفی و مدل عمومی برداشته شده است.



شکل ۲- مفاهیم امنیتی و روابط

ذی‌نفعان مسئول نگهداری از دارایی‌های مورد علاقه که به آن دارایی‌ها ارزش می‌نهند، هستند. عامل‌های واقعی یا فرضی تهدید ممکن است به دارایی‌ها ارزش نهند و به دنبال سوءاستفاده از دارایی‌ها باشند و این ارزش‌گذاری را به شیوه‌ای خلاف منافع ذی‌نفعان انجام دهند. ذی‌نفعان این تهدیدات را به‌عنوان خدشه‌ای بر دارایی‌هایی تلقی می‌کنند که ارزش دارایی ذی‌نفعان را کاهش خواهد داد. خدشه خاص بر امنیت معمولاً شامل افشای

مخرب دارایی به گیرندگان غیرمجاز (از دست دادن محرمانگی[1])، آسیب به دارایی‌ها از طریق تغییر غیرمجاز (از دست دادن یکپارچگی[2])، یا محرومیت غیرمجاز در دسترسی به دارایی (از دست دادن دسترس‌پذیری[3]) است.
ذی‌نفعان ارزیابی مخاطرات را با توجه به تهدیداتی که به دارایی‌هایشان اعمال می‌شود انجام می‌دهند. این تحلیل می‌تواند در انتخاب گروه کنترل‌ها برای مقابله با مخاطرات و کاهش آن به سطح قابل‌قبول کمک کند.
کنترل‌ها به‌منظور کاهش آسیب‌پذیری یا اثرات و برای پاسخگویی به نیازمندی‌های امنیتی ذی‌نفعان تحمیل می‌شوند (با ارائه مسیر به طرف‌های دیگر به طور مستقیم یا غیرمستقیم). آسیب‌پذیری‌های باقی‌مانده ممکن است پس از تحمیل کنترل باقی بمانند. چنین آسیب‌پذیری‌هایی ممکن است به‌وسیله عوامل تهدید که نمایانگر سطح باقی‌مانده از مخاطره دارایی‌ها هستند مورد سوءاستفاده قرار گیرند.
ذی‌نفعان به دنبال به حداقل رساندن مخاطره‌ای که دیگر محدودیت‌ها را معلوم می‌کند هستند. ذی‌نفعان نیازمند کسب اطمینان از جهت کافی بودن کنترل‌ها برای مقابله با تهدیدات به دارایی‌ها هستند، این نیاز باید پیش از اینکه اجازه افشای دارایی‌ها به تهدیدات مشخصی را بدهند، کسب شود. ذی‌نفعان ممکن است ظرفیت قضاوت همه جنبه‌های کنترل را نداشته باشند و بنابراین ممکن است به دنبال استفاده از سازمان‌های خارجی برای ارزیابی کنترل‌ها باشند.

۶-۵ رویکرد

با توجه به ذی‌نفعان مختلف، یک راه موثر برای مقابله با مخاطرات امنیت فضای مجازی، ترکیبی از راهبردهای چندگانه است. این راهبردها عبارت‌اند از:

- به‌روش صنعت، با همکاری همه ذی‌نفعان برای شناسایی و پرداختن به مسائل مربوط به امنیت رایانه‌ای و مخاطرات؛
- آموزش گسترده مصرف‌کننده و کارکنان، منبع مورد اعتمادی برای چگونگی شناسایی و رسیدگی به مخاطرات امنیت فضای مجازی خاص درون سازمان و همچنین فضای مجازی فراهم می‌کند و
- راه‌حل‌های فناوری‌های نوآورانه برای کمک به محافظت مصرف‌کنندگان از حمله‌های امنیت رایانه‌ای شناخته‌شده تا رایج باقی بمانند و در برابر بهره‌کشی‌های جدید آماده و مجهز باشند.

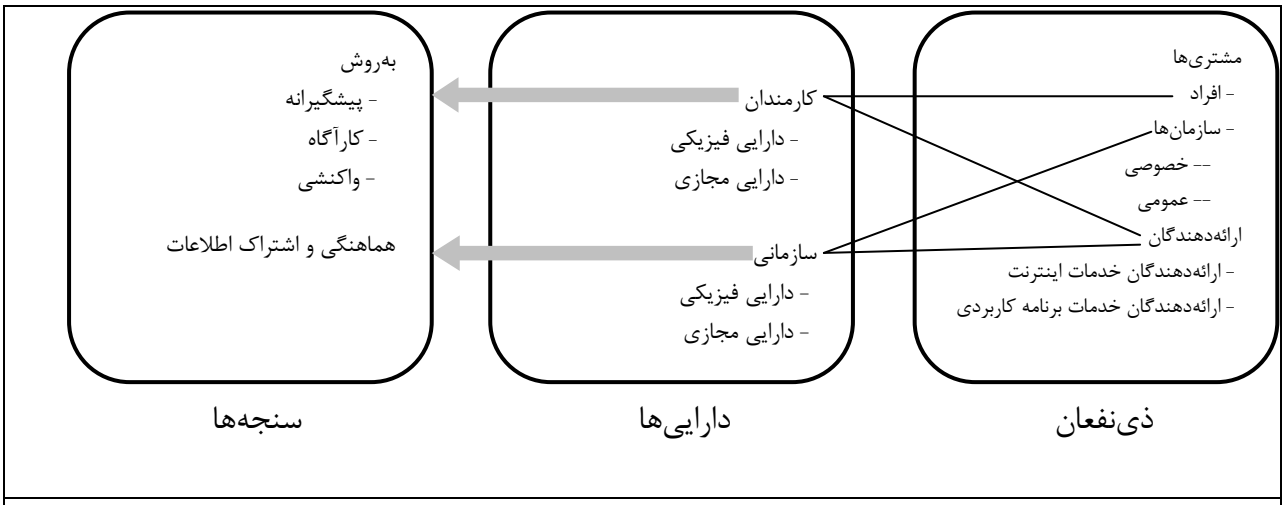
این استاندارد بر ارائه به‌روش صنعت و آموزش گسترده مصرف‌کنندگان و کارکنان برای کمک به ذی‌نفعان در فضای مجازی در ایفای نقش فعال برای رسیدگی به چالش‌های امنیت رایانه‌ای تمرکز دارد. شامل راهنمایی برای موارد زیر است:

- نقش‌ها؛
- خط‌مشی[4]؛
- روش؛

1- Confidentiality
2- Integrity
3- Availability
4- Policy

- فرآیندها و
- کنترل‌های فنی قابل‌اجرا.

شکل ۳ مرور کلی بر نکات برجسته رویکرد این استاندارد ملی ایران دارد. این استاندارد ملی ایران در پی استفاده مستقیم برای ارائه آموزش گسترده مصرف‌کننده نیست. در عوض، قصد استفاده توسط ارائه‌دهندگان خدمات در فضای مجازی را دارد، همچنین به‌عنوان سازمان‌های ارائه آموزش مرتبط با فضای مجازی بـه مصـرف‌کننـدگان، محتوای لازم برای آموزش گسترده‌ی مصرف‌کننده را تهیه می‌کند.



شکل ۳- **مرور کلی بر رویکرد**

۷ ذی‌نفعان در فضای مجازی

۷-۱ مرور کلی

فضای مجازی متعلق به هیچ کس نیست، هر کسی می‌تواند در آن مشارکت کند و سـهمی از آن داشـته باشـد. به‌عنوان هدفی برای این استاندارد ملی ایران ، ذی‌نفعان در فضای مجازی در گروه‌های زیر دسته‌بندی شده‌اند:

الف - مصرف‌کنندگان از جمله:

- افراد و
- سازمان‌های خصوصی و دولتی؛

ب- ارائه‌دهندگان شامل و نه محدود به:

- ارائه‌دهندگان خدمات اینترنت؛ و
- ارائه‌دهندگان خدمات برنامه کاربردی

۲-۷ مصرف‌کنندگان

همان طور که در شکل ۳ شرح داده شد، مصرف‌کنندگان به افراد و همچنین سازمان‌های خصوصی و دولتی اشاره دارند. سازمان‌های خصوصی شامل سازمان‌های کوچک و متوسط (SMEها)[1] و همچنین سازمان‌های بزرگ می‌باشند. دولت و دیگر سازمان‌های دولتی در مجموع به‌عنوان سازمان‌های دولتی شناخته می‌شوند. یک فرد یا یک سازمان زمانی که به فضای مجازی یا هر گونه خدمات در فضای مجازی دسترسی می‌یابند مصرف-کننده محسوب می‌شوند. درصورتی‌که مصرف‌کننده خدمتی در فضای مجازی ارائه دهد یا یکی دیگر از مصرف-کنندگان را قادر به دسترسی به فضای مجازی سازد می‌تواند ارائه‌دهنده محسوب شود. مصرف‌کننده‌ی خدمت دنیای مجازی با دسترس‌پذیر ساختن محصولات مجازی و خدمات موجود برای دیگر مصرف‌کنندگان ممکن است به ارائه‌دهنده تبدیل شود.

۳-۷ ارائه‌دهندگان

ارائه‌دهندگان به ارائه‌دهندگان خدمات در فضای مجازی اشاره دارند، این خدمات می‌تواند شامل ارائه‌دهندگان خدمات اینترنت که مصرف‌کنندگان را قادر به دسترسی به فضای مجازی می‌کنند و خدمات مختلف در دسترس فضای مجازی، باشد. ممکن است ارائه‌دهندگان در مقابل توزیع‌کنندگان و خرده‌فروشان خدمات دسترسی، به‌عنوان حامل‌ها یا عمده‌فروشان شناخته شوند. این تمایز از امنیت و به‌ویژه، چشم‌انداز اجرای قانون مهم‌تر است، زیرا چنانچه یک توزیع‌کننده یا خرده‌فروش قادر به تأمین امنیت کافی یا دسترسی قانونی نباشد، خدمات پشتیبانی اغلب به طور پیش‌فرض به حامل یا عمده‌فروش بازگردانده می‌شوند.

درک ماهیت ارائه‌دهنده خدمات مفروض عامل مفیدی در مدیریت مخاطره فضای مجازی است. ارائه‌دهندگان خدمات برنامه کاربردی، خدمات را از طریق نرم‌افزار در دسترس مصرف‌کنندگان خود قرار می‌دهد. این خدمات اشکال مختلف به خود گرفته و شامل ترکیبی از فهرست غیر جامع زیر است:

- ویرایش، ذخیره و توزیع سند؛
- محیط‌های مجازی برخط برای سرگرمی، ارتباطات و تعامل با دیگر کاربران؛
- مخازن رسانه‌های رقمی برخط با تراکم، شاخص‌گذاری، جستجو، نمای فروشگاه، فهرست قطعات، سبد خرید و خدمات پرداخت و
- کارکرد مدیریت منابع سازمان از جمله منابع انسانی، امور مالی و حقوق و دستمزد، مدیریت زنجیره تأمین، ارتباط با مشتری، صورتحساب.

1- Small and Medium Enterprises

۸ دارایی‌ها در فضای مجازی

۸-۱ مرور کلی

چیزی که برای یک فرد یا یک سازمان ارزشمند باشد دارایی خوانده می‌شود. دارایی‌ها انواع بسیاری دارند که شامل موارد زیر است اما محدود به آنها نیست:

الف- اطلاعات؛

ب- نرم‌افزار مانند یک برنامه رایانه‌ای؛

پ- فیزیکی، مانند یک رایانه؛

ت- خدمات؛

ث- مردم ، صلاحیت، مهارت‌ها و تجربه آنها و

ج- ناملموس، مانند شهرت و پندار

یادآوری ۱- اغلب، دارایی‌ها به سادگی تنها به‌عنوان اطلاعات یا منابع دیده می‌شوند.

یادآوری ۲- استاندارد ملی ایران ۱-۱۵۴۰۸ سال ۱۳۸۷، دارایی را به‌عنوان اطلاعات یا منابعی که باید به‌واسطه کنترل‌های هدف ارزیابی[1] مورد حفاظت قرار گیرد، تعریف می‌کند

یادآوری ۳- علت ایجاد استاندارد ISO/IEC 19770-1 این است که سازمان، به طور کلی، برای برآوردن نیازهای اداره امور شرکت و حصول اطمینان از حمایت موثر از مدیریت خدمات فناوری اطلاعات، قادر به اجرای مدیریت دارایی نرم‌افزار[2] است. استاندارد ISO/IEC 19770 قصد ایجاد هم ترازی نزدیک و پشتیبانی استاندارد ملی ایران شماره ۲۰۰۰۰ سال ۱۳۸۰ را دارد.

یادآوری ۴- استاندارد ملی ایران شماره ۲۰۰۰۰ سال ۱۳۸۰، ترویج پذیرش یک رویکرد فرآیند یکپارچه در هنگام ایجاد، پیاده-سازی، عملیاتی شدن، پایش، اندازه‌گیری، بررسی و بهبود یک سامانه مدیریت خدمات (SMS)[3] برای طراحی و ارائه خدمات را انجام می‌دهد که با نیازهای کسب‌وکار و نیاز مشتری مصادف می‌شود.

هدف این استاندارد ملی ایران، تقسیم دارایی‌ها در فضای مجازی به طبقات زیر است.

- شخصی و
- سازمانی

برای هر دو دسته، در ادامه یک دارایی نیز می‌تواند به‌عنوان موارد زیر طبقه‌بندی شود:

- یک دارایی فیزیکی که قالب آن در دنیای واقعی وجود دارد یا
- دارایی مجازی که تنها در فضای مجازی وجود دارد و در دنیای واقعی قابل مشاهده یا لمس نمی‌باشد.

۸-۲ دارایی‌های شخصی

یکی از دارایی‌های کلیدی مجازی، هویت برخط یک فرد مصرف‌کننده و اطلاعات اعتباری برخط او است. هویت برخط، ازآنجاکه برای هر فرد مصرف‌کننده در فضای مجازی شناسه کلیدی است، دارایی در نظر گرفته می‌شود.

1- Target Of Evaluation(TOE)
2- Software Asset Management(SAM)
3- Service Management System

سایر دارایی‌های مجازی فرد مصرف‌کننده شامل منابع دنیای مجازی هستند. اعضاء در دنیای مجازی، برای نشان دادن یا شناسایی خود یا برای وارد عمل شدن از طرف آنها، اغلب از چهرک‌های مجازی استفاده می‌کنند.
اغلب پول رایج مجازی برای انجام تراکنش‌های مجازی مورد استفاده قرار می‌گیرد. این چهرک‌ها و پول‌های رایج را می‌توان به‌عنوان دارایی‌های متعلق به یک فرد مصرف‌کننده در نظر گرفت.

مثال- برخی بانک‌ها در دنیای مجازی کار می‌کنند و پول دنیای مجازی را به‌عنوان پول رایج به رسمیت می‌شناسند.

فناوری اطلاعات، سخت‌افزار و نرم‌افزار و همچنین افزاره‌های رقمی شخصی یا نقطه انتهایی که اجازه‌ی اتصال و ارتباط به مصرف‌کننده در فضای مجازی می‌دهند، به‌عنوان دارایی در زمینه‌ی این استاندارد ملی ایران در نظر گرفته شده است.

۸-۳ دارایی‌های سازمانی

یکی از جنبه‌های کلیدی فضای مجازی زیرساخت است که تحقق آن را امکان‌پذیر می‌سازد. این زیرساخت اتصال داخلی درهم شبکه‌ها، کارسازها و برنامه‌های کاربردی است که متعلق به بسیاری از ارائه‌دهندگان خدمات است. بااین‌حال، قابلیت اطمینان و دسترس‌پذیری این زیرساخت در تضمین در دسترس بودن خدمات فضای مجازی و برنامه‌های کاربردی برای هر شخص در فضای مجازی بسیار قاطع است.
درحالی‌که هر زیرساختی اجازه می‌دهد که هر مصرف‌کننده به فضای مجازی متصل شود، یا به هر مصرف‌کننده اجازه می‌دهد به خدمات موجود در فضای مجازی دسترسی یابد، به‌عنوان یک دارایی فیزیکی که باید در این استاندارد ملی ایران در نظر گرفته شود مطرح می‌شود، ممکن است در سنجه‌های امنیتی[1] که پیشنهاد شده‌اند همپوشانی وجود داشته باشد، CIIP، امنیت اینترنت و امنیت شبکه مثال‌هایی از آن هستند.
بااین‌حال، تمرکز این استاندارد ملی ایران باید بر تضمین مسائل امنیتی باشد که ممکن است این دارایی‌های سازمانی را تحت تأثیر قرار دهد و باید بدون تاکید بیش‌ازحد بر مسائل دیگر که در حوزه این استاندارد ملی ایران نیستند به‌صورت مناسب مورد توجه قرار گیرد.
علاوه بر دارایی‌های فیزیکی، دارایی‌های مجازی سازمان به طور فزاینده‌ای ارزشمندتر می‌شوند. نام تجاری برخط و دیگر موارد نمایانگر سازمان‌ها در فضای مجازی به‌صورت منحصربه‌فرد سازمان را در فضای مجازی شناسایی کرده و به‌اندازه آجر و سیمان آن سازمان مهم هستند.

مثال ۱- اطلاعات وب‌گاه و URL، دارایی‌های سازمان هستند.

مثال ۲- کشورها حتی سفارتخانه‌های خود را در دنیای بزرگ مجازی برای محافظت از وجهه‌ی کشور راه‌اندازی کرده‌اند.

سایر دارایی‌های سازمانی که از طریق آسیب‌پذیری در فضای مجازی افشاء می‌شوند شامل، مالکیت معنوی[2](فرمول‌ها، فرآیندهای اختصاصی، اختراع ثبت‌شده، نتایج تحقیقات) و برنامه‌های کسب‌وکار و راهبردها (راه‌اندازی محصول و تدابیر بازاریابی، اطلاعات رقابتی، اطلاعات مالی و گزارش داده‌ها) است.

1- Security Measures
2- Intellectual Property

۹ تهدیداتی در برابر امنیت فضای مجازی

۹-۱ تهدیدات

۹-۱-۱ مرور کلی

تهدیداتی که در فضای مجازی وجود دارد نسبت به دارایی‌های موجود در فضای مجازی مورد بحث قرار گرفته است.

تهدید موجود در فضای مجازی را می‌توان به دو حوزه اصلی تقسیم نمود:

- تهدید وارد بر دارایی‌های شخصی؛
- تهدید وارد بر دارایی‌های سازمانی.

۹-۱-۲ تهدید وارد بر دارایی‌های شخصی

تهدیدات وارد بر دارایی‌های شخصی اساساً حول مسائل مربوط به هویت، ناشی از نشت یا سرقت اطلاعات شخصی است.

مثال ۱- اطلاعات اعتباری را می‌توان در بازار سیاه به فروش رساند که سرقت هویت برخط را تسهیل می‌بخشد.

اگر هویت برخط یک شخص سرقت شود یا ظاهر خود را تغییر دهد، آن شخص ممکن است از دسترسی به خدمات و برنامه‌های کاربردی کلیدی محروم شود. در فرانامه[1]های جدی‌تر، نتایج می‌تواند در گستره‌ای از مسائل مالی تا حوادث در سطح ملی باشد.

همچنین دسترسی‌های غیرمجاز به اطلاعات مالی شخص امکان سرقت پول و تقلب[2] را فراهم می‌کند. تهدید دیگر این است که نقطه انتهایی امکان ساخته شدن از یک زامبی یا بات ساخته شده باشند. ممکن است افزاره-های محاسبات شخصی مورد تخریب قرار گیرند و به بخشی از یک بات‌نت بزرگ‌تر تبدیل شوند. علاوه بر موارد فوق، سایر دارایی‌های مجازی که مورد هدف هستند، شامل دارایی‌های شخصی در دنیای مجازی و بازی‌های بر-خط می‌باشند. دارایی‌ها در دنیای مجازی یا دنیای بازی‌های برخط در معرض حمله و بهره‌کشی نیز می‌باشند.

مثال ۲: جزئیات چهرک‌ها و پول رایج مجازی که می‌تواند در برخی موارد، قابل ردیابی و بازگشت به دنیای واقعی باشد قابل تبدیل شدن به مهم‌ترین هدف خواهد بود.

سرقت و ضربه[3] مجازی واژه‌هایی هستند که برای این نوع از حمله به‌تازگی ابداع شده‌اند. امنیت، در این مورد، بستگی به این دارد که چه مقدار از اطلاعات جهان واقعی در دسترس است، بعلاوه به چارچوب امنیت دنیای مجازی که توسط مدیر تعریف و اجرا شده است بستگی دارد.

همان طور که قوانین و مقررات برای حفاظت از دارایی‌های فیزیکی واقعی، در ارتباط با فضای مجازی، هنوز در حال نوشته شدن هستند، آن دسته که مربوط به دارایی‌های مجازی است تقریباً موجود[4] نیست. باید توجه

1- Scenario
2- Fraud
3- Mug
4- Non-existent

افزوده و احتیاط با اکتشاف[1] شرکت‌کنندگان تضمین حفاظت مناسب از دارایی‌های مجازی صورت پذیرد تعهد گردد. مراقبت و احتیاط اضافی به‌وسیله حفاظت از مشارکت‌کنندگان برای حصول اطمینان از حفاظت درست از دارایی‌های مجازی آن‌ها باید اعمال شود.

۹-۱-۳ تهدید وارد بر دارایی سازمانی

حضور برخط سازمان‌ها و کسب‌وکار برخط اغلب مورد هدف اشراری[2] که قصدشان بیش از شرارت ساده است قرار داد.

مثال ۱: اتحادیه‌های جرائم سازمان‌یافته اغلب سازمان‌ها را این‌گونه تهدید می‌کنند که به وب‌گاه آنها آسیب وارد خواهند نمود یا از طریق اقداماتی همچون بدشکل کردن[3] یا خرابی وب‌گاه موجب شرمساری آنها می‌شود.

مثال ۲: اگر URL سازمان توسط متصرفان مجازی ثبت شود یا مورد سرقت واقع شود و به سازمان‌هایی که به سازمان در دنیای واقعی مربوط نیست فروخته شود، ممکن است اعتماد برخط توافق شده به سازمان قربانی را از بین ببرد.

درصورتی‌که مشخص شود حمله موفق ناشی از مدیریت یا محافظت ناکافی بوده و در خسارت مشارکت شده است، اطلاعات شخصی کارکنان، مشتریان، شرکا یا تأمین‌کنندگان ممکن است افشا و منجر به تضمین اجرایی، بر ضد سازمان شود.

اگر دستاوردهای سازمان به گونه‌ای غیرمجاز فاش شود، مقررات بایگانی مالی ممکن است مورد نقض واقع شود.

حکومت‌ها اطلاعات مربوط به امنیت ملی، راهبردی، نظامی، مسائل مربوط به اطلاعات نظامی در میان بسیاری عناصر دیگر مربوط به حکومت و دولت را نگهداری می‌کنند، همچنین آرایه‌ای وسیع از اطلاعات افراد، سازمان‌ها و جامعه را به طور کلی نگهداری می‌کنند.

حکومت‌ها باید از دسترسی بیش‌ازحد و بهره‌کشی از زیرساخت و اطلاعات محافظت کند. با روند رو به رشد و گسترش ارائه خدمات دولت الکترونیک[4] از طریق فضای مجازی، کانال جدیدی، در میان دیگر خدمات است که برای راه‌اندازی حملات و دسترسی به اطلاعات فوق، در صورت موفقیت ممکن است مخاطرات جدی، به ملت، حکومت و جامعه وارد آورد.

در مقیاس بزرگ‌تر، ممکن است زیرساختی که از اینترنت پشتیبانی می‌کند و در نتیجه فضای مجازی، هدف واقع شود. درحالی‌که به عملکرد فضای مجازی به طور دائم تأثیرگذار نیست، بر قابلیت اطمینان و دسترس-پذیری زیرساخت تأثیر خواهد داشت که منجر به امنیت فضای مجازی می‌شود.

در سطح ملی و بین‌المللی، فضای مجازی حوزه‌ی مبهمی[5] است که وحشت‌افکنی[6] رشد می‌کند. یکی از دلایل سهولت ارتباطات ارائه‌شده توسط فضای مجازی است. به سبب ماهیت فضای مجازی، مخصوصاً چالش در تعریف مرزها و حریم‌ها، تنظیم و کنترل راهی که می‌تواند مورد استفاده قرار گیرد دشوار است.

1- Prospecting
2- Miscreants
3- Defacement
4- e-government
5- Grey Area
6- Terrorism

گروه‌های وحشت‌افکن هم می‌توانند به‌صورت قانونی برنامه‌های کاربردی، خدمات و منابعی خریداری کنند که موجب تسهیل رسیدن به هدف خود شوند، یا به روش‌های غیرقانونی برای تأمین امنیت این منابع برای متوسل شوند تا از شناسایی و ردیابی جلوگیری بعمل آورند. این مسئله می‌تواند شامل دستیابی به منابع محاسباتی گسترده از طریق بات‌نت‌ها باشد.

۹-۲ عامل‌های تهدید[1]

عامل تهدید فرد یا گروهی از افراد است که نقشی در اجرا یا حمایت از یک حمله دارد. درک کامل، انگیزه‌ها (مذهبی، سیاسی، اقتصادی و غیره)، توانمندی‌ها (دانش، بودجه، اندازه و غیره) و نیت(سرگرم‌کننده، تبهکارانه، جاسوسی و غیره) آن‌ها و همچنین در توسعه و به‌کارگیری کنترل‌ها در ارزیابی آسیب‌پذیری و مخاطرات حیاتی، بسیار مهم است.

۹-۳ آسیب‌پذیری[2]

آسیب‌پذیری عبارت است از ضعف دارایی یا کنترلی که می‌تواند مورد بهره‌برداری یک تهدید قرار گیرد. در چارچوب سامانه اطلاعات و استاندارد ISO/IEC TR 19791:2006 آسیب‌پذیری به‌عنوان یک نقص، ضعف یا ویژگی‌ای از طراحی یا پیاده‌سازی یک سامانه اطلاعاتی (شامل کنترل‌های امنیتی آن) یا محیط آن تعریف شده است که می‌تواند دانسته یا نادانسته بر دارایی یا عملیات سازمان تأثیرگذار بوده و مورد سوءاستفاده قرار گیرد.

ارزیابی آسیب‌پذیری باید کار مداومی باشد. همان‌طور که سامانه وصله[3] دریافت می‌کند، به‌روز رسانی می‌شود یا عناصر جدید به آن افزوده می‌شود، ممکن است آسیب‌پذیری‌های جدید مطرح شود. ذی‌نفعان به‌منظور انجام یک ارزیابی جامع، نیازمند شناخت و درک دارایی یا کنترل مورد بحث هستند. به‌علاوه تهدیدات، عوامل تهدید و مخاطرات مورد بحث از مواردی هستند که باید شناخته و درک شوند.

یادآوری: استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، راهنمایی‌هایی را برای شناسایی آسیب‌پذیری فراهم می‌کند.

توصیه می‌شود موجودی آسیب‌پذیری‌های شناخته‌شده با دقیق‌ترین پروتکل دسترسی نگهداری شود و ترجیحاً از نظر فیزیکی و منطقی از، دارایی یا کنترلی که برای آنها قابل‌اجرا است جدا نگهداری شود. باید نقض دسترسی رخ دهد و موجودی آسیب‌پذیری مورد تخریب قرار گیرد، موجودی آسیب‌پذیری یکی از موثرترین ابزارها در انبارِ[4] یک عامل تهدید خواهد بود و این موجودی در اقدام به حمله و انجام عمل غیرقانونی استفاده می‌شود.

زمانی که راه‌حل امکان‌پذیر و شدنی نیست، باید به دنبال راه‌حلی برای آسیب‌پذیری، اجرا، بود و کنترل‌ها باید در جای خود قرار داده شوند. توصیه می‌شود این رویکرد بر اساس اولویت استفاده شود تا آسیب‌پذیری‌هایی که مخاطره بالاتری را نشان می‌دهند همان ابتدا مورد توجه قرار گیرند. فرآیند افشاءسازی آسیب‌پذیری را می‌توان تحت چارچوب به اشتراک‌گذاری اطلاعات و هماهنگی در بند ۱۳ از همین استاندارد ملی ایران تعریف کرد.

1- Threat Agents
2- Vulnerability

۳- بسته نرم‌افزاری که تولیدکنندگان برای حل مشکل آسیب‌پذیری محصولات خود ارائه می‌دهند.

4- Arsenal

یادآوری: استاندارد ملی آینده، ISO/IEC 29147، در راستای افشای آسیب‌پذیری راهنمایی ارائه خواهد داد.

۹-۴ سازوکارهای حمله

۹-۴-۱ مقدمه

بسیاری از حملات در فضای مجازی با استفاده از نرم‌افزارهای مخرب، مانند نرم‌افزارهای جاسوسی، کرم‌ها[1] و ویروس‌ها انجام می‌شود. اطلاعات اغلب از طریق روش‌های دزدی هویت گردآوری می‌شود. حمله می‌تواند به‌عنوان یک بردار حمله منحصربه‌فرد رخ دهد یا به‌عنوان یک سازوکار حمله مخلوط انجام شود. این حمله‌ها می‌توانند به‌عنوان مثال، از طریق وب‌گاه‌های مشکوک، بارگیری‌های تأیید نشده، رایانامه‌های نامه الکترونیکی ناشناس ، بهره‌کشی از راه‌دور و رسانه‌های جداشدنی آلوده منتشر شوند.

حمله‌ها ممکن است از دو دسته عمده آمده باشند:

- حمله‌های درون شبکه خصوصی و
- حمله‌های خارج از شبکه خصوصی.

هر چند مواردی وجود دارد که حمله‌ها ترکیبی از داخل و خارج شبکه خصوصی هستند. سازوکارهای دیگر در استفاده و کامل شدن[2]، برای انجام حملات رو به رشد، آنهایی هستند که شامل وب‌گاه‌های شبکه‌های اجتماعی و بکار بردن پرونده‌های تخریب شده در وب‌گاه‌های مشروع می‌باشند. افراد تمایل دارند به طور ضمنی به پیام‌ها و محتوای دریافتی از مخاطبینی که قبلاً در نمایه[3] خود بر روی وب‌گاه‌های شبکه‌های اجتماعی پذیرفته‌اند اعتماد کنند. هنگامی که یک مهاجم، از طریق سرقت هویت، می‌تواند خود را به‌عنوان مخاطب مشروع پنهان کند، مهاجم می‌تواند دیگران را بکار گمارد و یک راه جدید برای راه‌اندازی انواع مختلف حمله‌هایی که قبلاً مورد بحث بود باز کند.

همچنین ممکن است وب‌گاه‌های مشروع نیز مورد رخنه واقع شوند و برخی از پرونده‌های آن‌ها خراب شوند و به‌عنوان وسیله‌ای برای انجام حمله‌ها مورد استفاده قرار گیرند. افراد تمایل دارند که به طور ضمنی به وب‌گاه‌هایی که معمولاً از آنها بازدید به عمل آورده‌اند اعتماد کنند و اغلب برای مدت طولانی در مرورگرهای اینترنت خود آنها را نشانک‌گذاری کرده‌اند و حتی آنهایی که از سازوکارهای امنیتی مانند SSL (لایه حفره ایمن) [4] استفاده می‌کنند، درحالی‌که اصالت‌سنجی طرف و یکپارچگی اطلاعات منتقل یا دریافت شده هنوز بجا است، SSL بین محتوای اصلی و محتوای جدید خراب‌شده که توسط مهاجم مستقر شده تمایز قائل نیست، در نتیجه کاربران آن وب‌گاه را در پاسخ به حمله‌ها فاش می‌کند.

1- Worms
2- Sophistication
3- Profile
4- Secure Sockets Layer (SSL)

با وجود منبع مشروع دیده‌شده، مانند نمونه‌های بالا، افراد هنوز باید اقدامات احتیاطی مشخص‌شده در بند ۱۱ را برای محافظت بهتر از خود انجام دهند.

۹-۴-۲ حمله‌های درون شبکه خصوصی

این حمله‌ها معمولاً در داخل شبکه خصوصی یک سازمان، به طور معمول در شبکه‌های محلی راه‌اندازی می‌شود و توسط کارکنان یا کسی که دسترسی به یک رایانه یا شبکه در سازمان یا محل فرد دارد، می‌تواند آغاز شود.

مثال ۱: یک مورد ممکن این است که سرپرستان سامانه‌ها از امتیازات دسترسی به سامانه‌هایی که آنها را نگهداری می‌کنند استفاده کنند، مانند دسترسی به اطلاعات رمز عبور کاربران و استفاده از آن برای آغاز حمله. از سوی دیگر سرپرستان سامانه، پیش از انجام هدف یا اهداف قصد اصلی خود، به وسیله‌ای برای حمله مهاجم جهت به‌دست آوردن اطلاعات اضافی (نام کاربری، کلمه عبور و غیره)، تبدیل می‌شوند.

مهاجم می‌تواند از سازوکارهایی مانند بسته نرم‌افزاری جاسوس[1] برای به‌دست آوردن کلمه عبور یا دیگر اطلاعات هویتی استفاده کند. به طور متناوب، مهاجم می‌تواند به‌عنوان یک هستار مجاز تغییر ظاهر و به‌عنوان فرد در میان[2] برای سرقت اطلاعات هویتی وارد عمل شود.

مثال ۲: یکی از نمونه‌ها استفاده از نقاط دسترسی[3] برای سرقت هویت است. در این مورد، مهاجم ممکن است در یک فرودگاه، قهوه‌خانه یا دیگر اماکن عمومی که دسترسی رایگان Wi-Fi به اینترنت را ارائه می‌دهند بنشیند. در برخی موارد، در این فرض با استفاده از خدمات تنظیم شناسه (SSID) [4] فرض اولیه، مهاجم حتی ممکن است به‌عنوان مالک مشروع نقطه دسترسی بی‌سیم خود را جا بزند. اگر کاربر به این نقاط دسترسی سرکش دسترسی داشته باشد، مهاجم می‌تواند به‌عنوان فرد در میان عمل کند و رمز عبور باارزش را کسب کند و/یا اطلاعات شناسه را از کاربر به‌دست آورد، به‌عنوان نمونه، اطلاعات حساب بانکی و رمز عبور، رمز عبور حساب رایانامه و غیره.

مثال ۳: اغلب، برای سرقت اطلاعات در شبکه تنها کافی است نزدیک به شبکه Wi-Fi حفاظت نشده باشیم، مانند نشستن در ماشینی خارج از خانه.

علاوه بر حمله‌های مهاجمان انسانی، رایانه‌های آلوده به بدافزار نیز حملات مختلف به رایانه‌های اطراف موجود در داخل شبکه خصوصی را راه‌اندازی می‌کنند.

مثال ۴: بسیاری بدافزارها اغلب بسته‌های کاوشی را به شبکه‌های خصوصی ارسال می‌کنند تا رایانه‌های اطراف را پیدا کنند و سپس تلاش کنند تا از رایانه‌های یافته شده بهره‌کشی کنند.

مثال ۵: برخی بدافزارها از حالت بی‌قاعده یک واسط شبکه‌ای از رایانه آلوده‌شده به‌منظور استراق سمع[5] جریان ترافیک از طریق شبکه خصوصی استفاده می‌کنند.

مثال ۶: ثبت‌کننده‌های[1] کلید، برنامه‌های کاربردی سخت‌افزاری یا نرم‌افزاری که تمام کلیدهای فشار داده‌شده بر روی سامانه هدف را ضبط می‌کنند. این کار را می‌توان به‌صورت مخفی برای نظارت بر اقدامات یک کاربر انجام داد. کلیدخوانها اغلب برای ضبط اطلاعات مربوط به اصالت‌سنجی از صفحات ورود به سامانه نرم‌افزار مورد استفاده قرار می‌گیرند.

1- Packet Sniffer
2- Man-In-The-Middle
3- Access Point
4- Service Set Identifier (SSID)
5- Eavesdrop

۹-۴-۳ حملات خارج از شبکه خصوصی (برای مثال اینترنت)

حملات مختلفی وجود دارد که می‌تواند خارج از شبکه خصوصی، از جمله اینترنت، راه‌اندازی شود. درحالی‌که حمله اولیه همواره نمای عمومی سامانه (مثل مسیریاب، کارساز، دیواره‌ی آتش، وب‌گاه و غیره) را مورد هدف قرار می‌دهد، مهاجمان نیز ممکن است به دنبال بهره‌کشی از دارایی‌های مقیم داخل شبکه خصوصی باشند.

روش‌های قدیمی حمله بهبود یافته‌اند و انواع جدید بر اساس پیشرفت مداوم توسعه یافته‌اند. مهاجم‌ها به گونه‌ی فزاینده‌ای خبره هستند و به طور معمول روش‌های مختلف حمله و سازوکارها را برای به حداکثر رساندن موفقیت خود ترکیب می‌کنند که باعث می‌شود تشخیص و پیشگیری حمله سخت‌تر شود.

پویشگر مجرا[۲] یکی از قدیمی‌ترین روش‌ها است و هنوز هم یکی از موثرترین ابزارهای مورد استفاده توسط مهاجمان است. آنها همه مجراهای در دسترس روی کارساز را برای تأیید این‌که کدام مجرا «باز» است پویش می‌کنند. به طور معمول این روش یکی از اولین مراحل اجراشده توسط مهاجم آینده‌نگر بر روی سامانه هدف است.

این حملات می‌تواند حملات مختلف منع خدمت به برنامه کاربردی کارساز یا سایر تجهیزات شبکه را آشکار سازد و این کار را از طریق بهره‌کشی از آسیب‌پذیری‌های پروتکل یا طراحی نرم‌افزار انجام می‌دهد.

مثال: با کمک باتنت، حملات منع خدمت با مقیاس بزرگ را می‌توان راه‌اندازی کرد که دسترسی یک کشور به فضای مجازی را آشکارا صدمه بزند.

با گسترش برنامه‌های کاربردی همتا به همتا[۳] که معمولاً برای به اشتراک گذاشتن پرونده‌ها مانند موسیقی رقمی، ویدیوها، عکس‌ها و غیره، استفاده می‌شوند، مهاجمان به طور فزاینده‌ای در این‌که چگونه خود و کدهای مخربشان را با استفاده از پرونده‌های مبادله شده به‌عنوان یک اسب تروا برای حملات پنهان کنند خبره می‌شوند.

سرریزهای میانگیر[۴] یکی دیگر از روش‌های محبوب تخریب کارساز بر روی اینترنت است. با بهره‌کشی از آسیب-پذیری‌های برنامه‌نویسی و ارسال رشته‌ای از کاراکترهای بسیار طولانی تر از مورد انتظار، مهاجمان باعث می-شوند کارساز خارج از محیط طبیعی خود (حالت کنترل‌شده) عمل کند، در نتیجه درج/اجرای کدهای مخرب را تسهیل می‌بخشد.

یک روش دیگر جعل IP است، این روش شامل تلاش مهاجم در دست‌کاری نشانی IP مرتبط با پیام‌های او است تا بتواند خود را به‌عنوان یک منبع شناخته‌شده، مورد اعتماد مخفی کند و در نتیجه دسترسی غیرمجاز به سامانه به‌دست آورد.

1- Key Loggers
2- Port
3- Peer to Peer
4- Buffer Overflows

۱۰ نقش ذی‌نفعان در امنیت فضای مجازی

۱۰-۱ مرور کلی

برای بهبود وضعیت امنیت فضای مجازی، ذی‌نفعان در فضای مجازی نیازمند ایفای نقش فعال مربوطه در استفاده و توسعه اینترنت می‌باشند. این نقش‌ها گاهی ممکن است با نقش‌های فردی و سازمانی خود در شبکه-های شخصی یا سازمانی هم‌پوشانی داشته باشند.

واژه شبکه سازمان به ترکیبی از شبکه‌های خصوصی یک سازمان (معمولاً درون‌نت)، برون‌نت و شبکه‌های قابل‌مشاهده عموم اشاره دارد. با توجه به هدف این استاندارد ملی ایران، شبکه‌های قابل‌مشاهده عموم شبکه‌هایی هستند که در معرض شبکه اینترنت می‌باشند، برای مثال میزبان یک وب‌گاه.

به دلیل این همپوشانی، این نقش‌ها می‌توانند به نظر ناچیز برسند یا هیچ سود مستقیمی برای فرد و سازمان مربوطه نداشته باشند. بااین‌حال، زمانی که همه درگیر فعالیت هستند، بر افزایش امنیت فضای مجازی قابل توجه هستند.

۱۰-۲ نقش مصرف‌کنندگان

۱۰-۲-۱ مقدمه

مصرف‌کنندگان می‌توانند اطلاعات را مشاهده یا جمع‌آوری کنند و همچنین اطلاعات خاص در فضای برنامه کاربردی فضای مجازی را ارائه دهند، یا برای اعضای محدود یا گروه‌های موجود در فضای برنامه کاربردی، یا عموم مردم باز باشند. عملیاتی که توسط مصرف‌کنندگان در این نقش برعهده‌گرفته می‌شود می‌تواند فعال یا غیرفعال باشد و به طور مستقیم و غیرمستقیم به وضعیت امنیت فضای مجازی کمک کند.

۱۰-۲-۲ نقش افراد

مصرف‌کنندگان منحصربه‌فرد فضای مجازی ممکن است نقش‌های مختلف در زمینه‌های مختلف و برنامه‌های کاربردی را به‌عهده بگیرند. نقش مصرف‌کننده می‌تواند شامل موارد زیر باشد، اما محدود به آنها نیست:

- فضای مجازی عمومی برنامه کاربردی کاربر، یا کاربر عمومی، همچون بازیکن بازی برخط، کاربر پیام‌رسان فوری، یا وب‌گرد[1]؛
- خریدار/فروشنده، درگیر در قرار دادن کالا و خدمات در حراج‌های برخط و وب‌گاه‌های بازار برای خریداران علاقه‌مند و بالعکس؛
- بلاگرها و دیگر شرکت‌کنندگان محتوایی (به‌عنوان مثال، نویسنده‌ی مقاله‌ای در ویکی) که اطلاعات متن و چندرسانه‌ای (برای مثال، برش‌های ویدئویی) برای مصرف عموم مردم یا مخاطبان محدود منتشر شده است؛
- IAP در زمینه برنامه کاربردی (مانند بازی برخط)، یا به طور کلی فضای مجازی؛
- عضو سازمان (مانند کارمند یک شرکت، یا شکل دیگر ارتباط با یک شرکت)؛
- سایر نقش‌ها. این امکان وجود دارد که به کاربر نقشی ناخواسته یا بدون رضایت وی اختصاص داده شود.

1- Web Surfer

مثال: هنگامی که یک کاربر از یک وب‌گاه که نیاز به مجوز دارد، بازدید کند و ناخواسته اجازه دسترسی یابد، ممکن است کاربر به‌عنوان یک مزاحم[1] نشان‌گذاری شود.

در هر یک از این نقش‌ها، افراد می‌توانند اطلاعات را مشاهده یا جمع‌آوری کنند و همچنین اطلاعات خاص در فضای برنامه کاربردی فضای مجازی ارائه دهند، یا فضای برنامه کاربردی برای اعضای محدود یا گروه یا عموم مردم باز شود. عملیاتی که توسط افراد در این نقش‌ها انجام می‌شود می‌تواند فعال یا غیرفعال باشد و به طور مستقیم و غیرمستقیم به وضعیت امنیت فضای مجازی کمک کند.

مثال ۱: اگر IAP برنامه‌ای کاربردی را که شامل آسیب‌پذیری‌های امنیتی است ارائه کند، این آسیب‌پذیری‌ها می‌توانند توسط اشرار رایانه‌ای به‌عنوان یک کانال برای رسیدن به کاربران برنامه کاربردی استفاده شود.

مثال ۲: وب‌نوشت نویسان یا دیگر اشکال تولیدکنندگان محتوا می‌توانند درخواستی در قالب پرسش‌های ساده در مورد مطالبی که نوشته‌اند دریافت کنند. در پاسخ دادن به آنها، ممکن است ناخواسته اطلاعات شخصی خود یا شرکت را بیشتر از حد مطلوب به عموم مردم فاش کنند.

مثال ۳: یک فرد به‌عنوان خریدار یا فروشنده ایفای نقش می‌کند، می‌تواند ندانسته در تراکنش‌های تبهکارانه فروش کالای به سرقت رفته یا فعالیت‌های پول‌شویی شرکت کند.

در نتیجه، همانند دنیای واقعی، مصرف‌کنندگان فردی نیازمند تمرین احتیاط، در هر نقشی که در فضای مجازی بازی می‌کنند، هستند.

۱۰-۲-۳ نقش سازمان

سازمان‌ها اغلب از فضای مجازی برای انتشار اطلاعات شرکت و اطلاعات مرتبط و همچنین محصولات و خدمات مرتبط بازار استفاده می‌کنند. شرکت‌ها و سازمان‌ها نیز از فضای مجازی به‌عنوان بخشی از شبکه خود برای تحویل و دریافت پیام‌های الکترونیکی (برای مثال رایانامه) و دیگر اسناد (برای مثال، انتقال پرونده) استفاده می‌کنند.

در راستای همان اصول شهروندی خوب، این سازمان‌ها باید وظایف و تعهدات سازمانی خود را به فضای مجازی گسترش دهند و فعالانه و پیشگیرانه اطمینان حاصل کنند که اعمال و اقدامات خود در فضای مجازی مخاطرات امنیتی بیشتری را به فضای مجازی معرفی نمی‌کند. برخی از اقدامات پیشگیرانه عبارت‌اند از:

- مدیریت امنیت اطلاعات مناسب با پیاده‌سازی و عملیاتی کردن موثر سامانه مدیریت امنیت اطلاعات (ISMS)[2]؛

یادآوری ۱: استاندارد ملی ایران شماره ۲۷۰۰۱، نیازمندی‌های سامانه مدیریت امنیت اطلاعات را فراهم می‌کند.

- نظارت مناسب بر امنیت و پاسخ؛
- ترکیب امنیت به‌عنوان بخشی از چرخه زندگی توسعه نرم‌افزار (SDLC)[3] که سطح امنیت ایجادشده درون سامانه بر اساس حیاتی بودن داده‌های حیاتی سازمان تعیین می‌شود؛

1- Intruder
2- Information Security Management System (ISMS)
3- Software Development Life-cycle (SDLC)

- آموزش منظم امنیت به کاربران درون سازمان برای به‌روزرسانی به‌روز مداوم فناوری و پیگیری آخرین تحولات فناوری؛ و
- درک و استفاده از کانال‌های مناسب در برقراری ارتباط با فروشندگان و ارائه‌دهندگان خدمات در مسائل امنیتی کشف‌شده در طول استفاده.

یادآوری ۲: استاندارد ملی آینده، ISO/IEC 29147، راهنمایی‌هایی در ارتباط با افشای آسیب‌پذیری ارائه خواهد داد.

یادآوری ۳: استاندارد ملی ایران شماره ۲۷۰۳۱، راهنمایی‌هایی برای آمادگی فنّاوری ارتباطات و اطلاعات برای تداوم کسب‌وکار ارائه می‌دهد.

یادآوری ۴: استاندارد ملی ایران شماره ۲۷۰۳۵، راهنمایی‌هایی برای مدیریت رخداد امنیت اطلاعات ارائه می‌دهد.

یادآوری ۵: استاندارد ملی ایران شماره ۱-۲۷۰۳۴، راهنمایی‌هایی برای امنیت برنامه کاربردی ارائه می‌دهد.

حکومت، سازمان‌های مجری و تنظیم‌کننده مقررات در درجه اول، ممکن است نقش‌های مهم زیر را بازی کنند:

- مشاوره سازمان‌ها از نقش‌ها و مسئولیت‌هایشان در فضای مجازی؛
- به اشتراک‌گذاری اطلاعات با دیگر ذی‌نفعان در مورد آخرین روندها و توسعه در فناوری؛
- به اشتراک‌گذاری اطلاعات با دیگر ذی‌نفعان در مورد مخاطرات امنیتی که در حال حاضر شایع است؛
- یک مجرا برای دریافت هر گونه اطلاعات، اعم از بسته یا باز، با توجه به مخاطرات امنیتی به فضای مجازی؛ و
- در صورت بروز بحران ناشی از حمله مجازی عظیم، هماهنگ‌کننده اصلی برای انتشار اطلاعات و سازمان‌دهی منابع مورد نیاز، در هر دو سطح ملی یا شرکت‌های بزرگ باشد.

۳-۱۰ نقش ارائه‌دهندگان

سازمان‌های ارائه خدمات می‌توانند شامل دو دسته باشند:

- ارائه‌دهندگان دسترسی به کارمندان و شرکای فضای مجازی و
- ارائه‌دهندگان خدمات از طریق ارائه برنامه‌های کاربردی فضای مجازی به مصرف‌کنندگان فضای مجازی، یا به یک جامعه بسته، یا عموم مردم (به‌عنوان مثال، کاربران ثبت‌نام‌شده)

به‌عنوان مثال: نمونه‌های خدمات بازار تجارت برخط، پایگاه خدمات انجمن بحث و گفتگو، پایگاه خدمات وب‌نویسی و خدمات شبکه‌های اجتماعی.

ارائه‌دهندگان خدمات، سازمان‌های مصرف‌کننده نیز هستند. به‌این‌ترتیب از آنها انتظار می‌رود که نقش‌ها و مسئولیت‌های یکسان را به‌عنوان سازمان‌های مصرف‌کننده مورد ملاحظه قرار دهند؛ به عنوان مثال ارائه‌دهندگان خدمات، در حفظ یا حتی بالا بردن امنیت فضای مجازی مسئولیت‌های اضافی بر عهده دارند:

- ارائه محصولات و خدمات امن و مطمئن؛
- ارائه راهنمایی‌های ایمنی و امنیتی برای کاربران نهایی؛ و
- ارائه ورودی‌های امنیتی به دیگر ارائه‌دهندگان و مصرف‌کنندگان در مورد روندها و مشاهدات ترافیک در شبکه‌ها و خدمات.

۱۱ راهنمایی برای ذی‌نفعان

۱۱-۱ مرور کلی

راهنمایی در این بند در سه زمینه اصلی متمرکز است:

- راهنمایی امنیتی برای مصرف‌کنندگان؛
- اطلاعات مربوط به مدیریت مخاطرات امنیت داخلی سازمان؛
- نیازمندی‌های امنیتی که ارائه‌دهندگان باید برای مصرف‌کنندگان به پیاده‌سازی مشخص کنند.

توصیه‌ها به شرح زیر سازمان یافته‌اند:

الف- مقدمه‌ای بر ارزیابی و برطرف‌سازی مخاطره؛

ب- راهنمایی برای مصرف‌کنندگان؛ و

پ- راهنمایی برای سازمان‌ها، از جمله ارائه‌دهندگان خدمات:

- مدیریت مخاطره امنیت اطلاعات در کسب‌وکار؛ و
- نیازمندی‌های امنیتی برای خدمات میزبانی وب و دیگر خدمات برنامه کاربردی.

۱۱-۲ ارزشیابی و برطرف‌سازی مخاطره

استاندارد ملی ایران ۳۱۰۰۰، مدیریت مخاطره -اصول و راهنمایی‌ها که اصول و راهنمایی‌های عمومی در مدیریت بحران را فراهم می‌کند، درحالی‌که استاندارد ملی ایران شماره ۲۷۰۰۵، فناوری اطلاعات -فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات، راهنمایی‌ها و فرآیندهای مدیریت مخاطرات امنیت اطلاعات در یک سازمان را فراهم می‌کند که در تأیید الزامات ویژه ISMS بر اساس استاندارد ملی ایران شماره ۲۷۰۰۱ است.

این راهنمایی‌ها و فرآیندها برای پرداختن به مدیریت مخاطره در زمینه فضای مجازی به‌اندازه کافی در نظر گرفته شده است. استاندارد ملی ایران شماره ۲۷۰۰۵، هیچ روش خاصی برای مدیریت مخاطره امنیت اطلاعات ارائه نمی‌دهد. تعریف رویکرد مدیریت مخاطره به عهده‌ی مصرف‌کنندگان و ارائه‌دهندگان خدمات است. برای پیاده‌سازی الزامات ISMS، تعدادی از روش‌های موجود را می‌توان در چارچوب تشریح شده در استاندارد ملی ایران شماره ۲۷۰۰۵ استفاده نمود.

جنبه‌های زیر را باید در هنگام تعریف یک رویکرد مدیریت مخاطره مورد توجه قرار داد:

- شناسایی دارایی‌های حیاتی: اتصال یا استفاده از فضای مجازی که دامنه تعریف دارایی را گسترش می‌دهد. ازآنجاکه برای محافظت از تمام دارایی‌ها مقرون‌به‌صرفه نیست، ضروری است که دارایی‌های حیاتی شناخته شوند تا توجه ویژه‌ی ممکن برای حفاظت از آنها اتخاذ گردد. توصیه می‌شود تأثیر از دست دادن یا افت دارایی در زمینه‌ی کسب‌وکار به طور کلی از طریق عنوانی که از زمینه کسب‌وکار گرفته می‌شود، مورد توجه قرار گیرد.

- شناسایی مخاطرات[1]: ذی‌نفعان باید مخاطرات اضافی، تهدیدات و حملاتی که مربوط به زمانی است که در فضای مجازی شرکت دارند، به‌درستی بررسی کرده و مورد توجه قرار دهند.
- مسئولیت[2]: با شرکت در فضای مجازی، ذی‌نفع باید مسئولیت بیشتری نسبت به سایر ذی‌نفعان قبول کند. این موارد عبارت‌اند از:
  - تصدیق[3]: تشخیص مخاطرات ممکن که با مشارکت ذی‌نفع در فضای مجازی به طور کلی در سامانه‌های اطلاعاتی سایر ذی‌نفعان به‌طور خاص ممکن است معرفی و مطرح گردد.
  - گزارش‌گیری[4]: ممکن است لازم باشد زمان توزیع گزارش‌های مربوط به مخاطرات، حوادث و تهدیدات ذی‌نفعان خارج از سازمان را نیز شامل شود.
  - اشتراک‌گذاری اطلاعات[5]: همراه با گزارش‌گیری، ممکن است لازم باشد اطلاعات مرتبط با سایر ذی‌نفعان به اشتراک گذاشته شود.
  - ارزیابی مخاطره[6]: تعیین حوزه فعالیت ذی‌نفع و حضور آنها در فضای مجازی، در به وجود آوردن یا منجر به مخاطره‌ای برای ذی‌نفع دیگر شدن، امری ضروری است.
  - تنظیم مقررات/قانون‌گذاری[7]: با اتصال به فضای مجازی، تشخیص مرزهای قانونی و نظارتی به‌سختی قابل تمیز است و به نوعی، گاهی اوقات الزامات متناقض قابل‌اجرا است.
- بازنشستگی سامانه یا خدمات: هنگامی که یک سامانه یا خدماتی دیگر مورد نیاز نباشد، باید بازنشسته شود و البته باید تضمین کند خدمات مرتبط یا واسطها تحت فشار نیستند. توصیه می‌شود همه اطلاعات مربوط به امنیت باطل شود تا عدم تخریب سامانه‌هایی که واسط آنها است یا در ارتباط هستند را تضمین کند.
- سازگاری[8]: رویکرد مدیریت مخاطره در سراسر فضای مجازی اعمال می‌شود. مطابق این رویکرد یا روشگان، مصرف‌کنندگان و ارائه‌دهندگان فضای مجازی مسئولیت‌هایی برای فعالیت‌های خاص، مانند طرح‌ریزی احتمالی، بازیابی حوادث بد و توسعه و پیاده‌سازی برنامه‌های محافظ برای سامانه‌های تحت کنترل خود و/یا مالکیت خود اختصاص داده‌اند.

به طور کلی، روشگان مدیریت مخاطره در استاندارد ملی ایران ۲۷۰۰۵ چرخه کامل زندگی یک سامانه عمومی را تحت پوشش قرار می‌دهد، بنابراین برای سامانه‌های جدید امنیتی و همچنین برای سامانه‌های موروثی آن را کاربردی می‌کند. ازآنجاکه به برطرف‌سازی سامانه می‌پردازد، برای تمام مدل‌های کسب‌وکار قابل پیاده‌سازی است. فرآیندهای موجود در چارچوب ممکن است شبکه و خدمات ارائه‌دهندگان خدمات را به‌عنوان یک سامانه یکپارچه بهسازی کنند که متشکل است از زیرسامانه‌هایی که خدمات عمومی ارائه می‌دهند و زیرسامانه‌های

1- Identification of Risks
2- Responsibility
3- Acknowledgement
4- Reporting
5- Information sharing
6- Risk Assessment
7- Regulatory/Legislative
8- Consistency

خصوصی که از خدمات داخلی پشتیبانی می‌کنند، یا ممکن است خدمات افراد (به‌عنوان مثال، میزبانی وب) را به طور جداگانه مورد بحث قرار دهد و شرایط را بر حسب سامانه‌های تعاملی جداگانه توصیف کند. برای سادگی ممکن است سودمند باشد که همه‌چیز را که برای حمایت از خدمات ارائه‌دهنده به‌عنوان یک سامانه بزرگ نیاز است در نظر گرفت که آن هم به‌نوبه خود می‌تواند به سامانه‌های کوچک‌تر تجزیه شود که هر یک از آنها خدمات قابل‌عرضه در بازار یا بخشی از زیرساخت را فراهم می‌کنند.

جنبه‌های مهم که با توجه به اهداف و مقاصد امنیت فضای مجازی باید به یاد آورد عبارت‌اند از:

الف- محافظت کلی از امنیت فضای مجازی؛

ب- طرح‌ریزی برای شرایط اضطراری و حیاتی از طریق مشارکت در تمرین و به‌روزرسانی طرح‌های پاسخ و طرح‌هایی برای تداوم عملیات؛

پ- آموزش ذی‌نفعان در شیوه‌های امنیت فضای مجازی و مدیریت مخاطره؛

ت- اطمینان به‌موقع، از به اشتراک‌گذاری اطلاعات مناسب و دقیق تهدید، میان مجریان قانون و جوامع اطلاعاتی[1] و تصمیم‌گیرندگان کلیدی مربوط به فضای مجازی؛ و

ث- ایجاد موثر سازوکارهای هماهنگی بین بخش سراسری[2] و ذی‌نفع سراسری[3] برای نظارت وابستگی‌های داخلی حیاتی، از جمله آگاهی موقعیتی از رخداد و مدیریت رخداد بخش متقاطع و ذی‌نفع متقاطع.

اهداف کلان[4] و اهداف خرد[5] الف تا پ، به طور مستقیم به ارائه‌دهندگان خدمات جاری هستند که مسئول تجهیزات و خدمات تحت کنترل خود هستند. برای اهداف کلان و اهداف خرد، ت و ث، ارائه‌دهندگان خدمات به‌عنوان شرکت‌کنندگان فعال در اشتراک‌گذاری اطلاعات و فعالیت‌های هماهنگی نقش دارند. اهداف خاص ارائه‌دهنده خدمات، مانند اینکه چه خدماتی را عرضه کنند، از مقوله کسب‌وکار جریان می‌یابد.

۳-۱۱ راهنمایی برای مصرف‌کنندگان

این استاندارد ملی ایران به طور خاص به افراد در فضای مجازی اشاره ندارد، اما بر سازمان‌هایی که ارائه‌دهنده خدمات به مصرف‌کنندگان هستند، و کارکنان یا کاربران نهایی سازمان‌هایی که نیازمند اعمال استفاده امن از فضای مجازی برای مدیریت موثر مخاطره امنیت فضای مجازی هستند، تمرکز دارد. راهنمایی در مورد نقش و امنیت کاربران در فضای مجازی و این‌که چگونه می‌توانند به شکل مثبت بر وضعیت امنیت فضای مجازی تأثیر بگذارند، در زمینه تدارک خدمت و آگاهی‌رسانی و آموزش برنامه‌ها برای تحویل به کاربران نهایی، ارائه خدمت به‌عنوان یک راهنما برای طراحی و توسعه محتوا توسط این سازمان‌ها را هدف قرار می‌دهد. همان طور که در بند ۲-۱۰ توضیح داده شد، مصرف‌کنندگان می‌توانند اطلاعات را مشاهده یا جمع‌آوری کنند و همچنین اطلاعات خاص در فضای برنامه کاربردی فضای مجازی را ارائه دهند، یا برای اعضای محدودی یا گروه‌ها در

1- Intelligence Communities
2- Cross-Sector
3- Cross-Stakeholder
4- Goals
5- Objectives

فضای برنامه کاربردی، یا عموم مردم باز باشند. عملیاتی که در این نقش‌ها توسط مصرف‌کنندگان به‌عهده گرفته شده است، فعال یا غیرفعال باشد و به طور مستقیم و غیرمستقیم در وضعیت امنیت فضای مجازی مشارکت کند.

به‌عنوان مثال، به‌عنوان یک IAP، درصورتی‌که برنامه کاربردی ارائه‌شده شامل آسیب‌پذیری‌های امنیتی باشد، می‌توانند منجر به بهره‌کشی اشرار مجازی و اعمال نفوذ آنها به‌عنوان کانالی برای رسیدن به کاربران معمولی برنامه کاربردی شوند. همچنان که وب‌نویسان یا اشکال دیگر شرکت‌کنندگان محتوا، ممکن است درخواستی به شکل سؤالات بی‌ضرر مربوط به محتویات دریافت کنند و ناخواسته اطلاعات شخصی یا اطلاعات مربوط به شرکت را بیش‌ازحد مطلوب به عموم مردم ابلاغ کنند. مصرف‌کننده به‌عنوان یک خریدار یا فروشنده، ممکن است ندانسته در تراکنش تبهکارانه فروش کالای به سرقت رفته یا فعالیت‌های پول‌شویی شرکت کند. در نتیجه، همانند دنیای فیزیکی، مصرف‌کنندگان باید در مورد هر نقشی که در فضای مجازی بازی می‌کنند احتیاط بیشتری به‌خرج دهند.

به طور کلی، مصرف‌کنندگان باید به راهنمایی‌های زیر توجه داشته باشند:

الف- یادگیری و درک امنیت و خط مشی‌های حفظ حریم خصوصی وب‌گاه و برنامه کاربردی مربوطه، همان‌طور که ارائه دهنده وب‌گاه منتشر کرده است.

ب- یادگیری و درک امنیت و حفظ حریم خصوصی مخاطرات درگیر و تعیین کنترل‌های مناسب قابل‌اجرا. شرکت در بحث و تبادل‌نظر برخط مرتبط، یا مداخله و هم‌کاری اطلاعات، یا پیش از این‌که اطلاعات شخصی یا سازمان ارائه شود از کسی که در مورد وب‌گاه یا برنامه کاربردی آگاهی دارد پرسیده شود.

پ- ایجاد و اعمال خط‌مشی حفظ حریم خصوصی شخصی برای حفاظت از هویت و تعیین دسته‌بندی اطلاعات شخصی در دسترس و اشتراک‌گذاری اصول مربوط به آن اطلاعات.

ت- مدیریت هویت برخط. از شناسه‌های مختلف برای برنامه‌های کاربردی تحت وب مختلف استفاده می‌کند و اشتراک‌گذاری اطلاعات شخصی به هر وب‌گاه یا برنامه کاربردی را که چنین اطلاعاتی را درخواست می‌کند به حداقل می‌رساند. ثبت هویت برخط در وب‌گاه‌های شبکه اجتماعی محبوب حتی اگر حساب غیرفعال رها شده باشد.

مثال- ورود[1] تکی، شکلی از مدیریت هویت برخط است.

ث- گزارش رویدادهای مشکوک یا برخورد به مراجع مربوطه (در پیوست ب، مثالی از فهرست مخاطبین قابل‌دسترس عموم مردم وجود دارد).

ج- به عنوان یک خریدار یا فروشنده، خواندن و درک امنیت وب‌گاه بازار برخط و خط‌مشی حفظ حریم خصوصی و اقداماتی که به‌منظور بررسی صحت طرف‌های ذی‌نفع درگیر به عمل می‌آید. داده‌های شخصی، از جمله اطلاعات بانکی را به اشتراک نگذارید، مگر اینکه علاقه واقعی به فروش یا خرید محرز شده باشد. از یک سازوکار پرداخت قابل‌اعتماد استفاده کنید.

1- Sign On

چ- به‌عنوان یک IAP، عمل توسعه امن نرم‌افزار و ارائه یک مقدار درهم[1] از کد برخط به‌طوری که طرف‌های دریافت‌کننده در صورت لزوم، برای اطمینان از یکپارچگی کد بتوانند ارزش را تأیید کنند. مستندات کد امنیتی و خط‌مشی حفظ حریم خصوصی و شیوه‌ها و احترام به حریم خصوصی کاربران کد را ارائه می‌دهد.

ح- به‌عنوان یک وب‌نوشت نویس یا دیگر شرکت‌کننده محتوا (از جمله نگهداری-کنندگان وب‌گاه)، تضمین می‌کند که حفظ حریم خصوصی قابل‌اجرای ذی‌نفع و اطلاعات حساس از طریق وب‌نوشت‌ها یا نشریات برخط فاش نمی‌شوند، اطمینان حاصل شود. بررسی نظرها و پیام‌های دریافت شده[2] در وب‌گاه و حصول اطمینان از این مسئله که حاوی مطالب مخرب مانند پیوند به وب‌گاه‌ها دزدی هویت یا دریافت‌های مخرب نیست.

خ- به‌عنوان عضو سازمان، فرد مصرف‌کننده باید خط‌مشی امنیت اطلاعات صنفی[3] سازمان را بیاموزد و درک کند و اطمینان حاصل کند که اطلاعات طبقه‌بندی‌شده و/یا اطلاعات حساس به طور عمدی یا تصادفی در هر وب‌گاهی در فضای مجازی منتشر نشود، مگر اینکه مجوز چنین افشایی از پیش و به طور رسمی اعطا شده باشد.

د- نقش‌های دیگر. هنگامی که مصرف‌کننده‌ای سایتی را که نیاز به مجوز دارد بازدید می‌کند و غیرعمدی اجازه دسترسی یابد، ممکن است کاربر به‌عنوان یک مزاحم نشان‌گذاری شود. ازآنجاکه ممکن بود دسترسی نشانه‌ای از تخریب باشد بلافاصله از سایت خارج شود و مراتب به مراجع مربوطه گزارش شود.

۱۱-۴ راهنماهایی برای سازمان‌ها و ارائه‌دهندگان خدمات

۱۱-۴-۱ مرور کلی

کنترل برای مدیریت مخاطره امنیت فضای مجازی به طور قابل‌توجهی به بلوغ فرآیندهای مدیریت امنیت درون سازمان‌ها بستگی دارد (از جمله ارائه‌دهندگان خدمات). درحالی‌که راهنمایی‌های پیشنهاد شده برای سازمان‌ها به طور عمده از روی احتیاط ارائه می‌شوند، توصیه می‌شود که ارائه‌دهندگان خدمت با راهنمایی‌ها به‌عنوان سنجه‌های اجباری خط مبنای رفتار کنند.

در این بند راهنمایی‌هایی را می‌توان به شکل زیر خلاصه کرد:

- مدیریت مخاطره امنیت اطلاعات در کسب‌وکار.
- نشانی الزامات امنیتی برای میزبانی وب و سایر خدمات برنامه کاربردی مجازی.
- ارائه راهنمایی‌های امنیتی به مصرف‌کنندگان.

1- Hash
2- Postings
3- Corporate

۱۱-۴-۲ مدیریت مخاطره امنیت اطلاعات در کسب‌وکار

۱۱-۴-۲-۱ سامانه مدیریت امنیت اطلاعات

در سطح سازمانی، سازمان‌های متصل به فضای مجازی باید یک سامانه مدیریت امنیت اطلاعات (ISMS) را برای شناسایی و مدیریت مخاطره امنیت اطلاعات مربوط به کسب‌وکار پیاده‌سازی کنند. مجموعه‌ی استانداردهای ملی ۲۷۰۰۰ برای سامانه‌های اطلاعاتی مدیریت امنیت اطلاعات، راهنمایی‌های لازم را ارائه می‌دهد همچنین به‌روش پیاده‌سازی چنین سامانه‌هایی را ارائه می‌دهد.

ملاحظه کلیدی در پیاده‌سازی ISMS برای تضمین این است که سازمان دارای سامانه‌ای است که پیوسته در حال شناسایی، ارزیابی، درمان و مدیریت مخاطره امنیت اطلاعات مربوط به کسب‌وکار خود است، از جمله ارائه خدمات در اینترنت، به طور مستقیم به کاربران نهایی[1] یا مشترک، باید ارائه‌دهنده خدمات باشد.

یادآوری ۱: استاندارد ملی ایران شماره ۲۷۰۰۵، فناوری اطلاعات - فنون امنیتی- مدیریت مخاطره امنیت اطلاعات، راهنمایی‌هایی برای مدیریت مخاطره امنیت اطلاعات در یک سازمان را ارائه می‌دهد، مخصوصاً پشتیبانی الزامات ISMS بر اساس استاندارد ملی ایران شماره ۲۷۰۰۱.

یادآوری ۲: استاندارد ملی ایران ۳۱۰۰۰، مدیریت مخاطره-اصول و رهنمودها، اصول و راهنمایی‌های عمومی در مدیریت مخاطره را ارائه می‌دهد.

همچنین شرکت‌ها و سازمان‌ها ممکن است یک گواهینامه رسمی از انطباق آن با الزامات ISMS، از جمله استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ را در نظر بگیرند.

به‌عنوان بخشی از پیاده‌سازی ISMS، سازمان باید نظارت رخداد امنیتی و قابلیت پاسخ را ایجاد کند و فعالیت‌های پاسخ به رخداد خود را با CIRT، CERT، یا سازمان‌های CSIRT در کشور هماهنگ کند. شرط لازم و اضطراری رخداد باید شامل نظارت و ارزیابی وضعیت امنیتی استفاده از خدمات سازمان به کاربران نهایی و مشتریان باشد و برای کمک به طرف‌های درگیر در واکنش به حوادث امنیتی به طور موثر راهنمایی ارائه می‌دهد.

یادآوری- استاندارد ملی ایران شماره ۲۷۰۳۵، فناوری اطلاعات - فنون امنیتی – مدیریت رخداد امنیت اطلاعات، ارائه راهنمایی در مورد مدیریت رخداد امنیت اطلاعات.

۱۱-۴-۲-۲ ارائه محصولات امن

برخی از سازمان‌ها نوار ابزارهای مرورگر وب خود را توسعه داده[2]، برنامه‌های شماره‌گیر[3]، یا کد ارائه‌دهنده خدمات ارزش‌افزوده به کاربران نهایی، یا تسهیل سهولت دسترسی به خدمات سازمان یا برنامه‌های کاربردی را منتشر می‌کنند.

1- End-users

۲- توسط ارائه‌دهندگان درون سازمان یا توسط طرف سوم

3- Diallers

در چنین مواردی، توصیه می‌شود توافق مناسب کاربر نهایی وجود داشته باشد، ترکیب دستورات بیانیه در مورد خطمشی برنامه‌نویسی، خطمشی حفظ حریم خصوصی و وسایل[1] این سازمان که به‌موجب آن کاربران می‌توانند پذیرش خود را بعداً تغییر دهند یا هر گونه مسائل را با توجه به خطمشی‌ها و شیوه‌ها تشدید کنند. هنگامی که چنین توافقنامه‌ای استفاده می‌شود، توصیه می‌شود تحت کنترل نسخه[2] قرار داده شود و این سازمان باید مطمئن شود که کاربران نهایی پیوسته آن را امضاء می‌کنند.

همان طور که در استاندارد ملی ایران شماره ۱۵۴۰۸، شرح داده شد، جایی که درجه بالایی از اتکا به امنیت محصولات نرم‌افزاری وجود دارد، توصیه می‌شود به طور مستقل تحت ضوابط متداول طرح تأیید اعتبار شوند. سازمان‌ها باید رفتار کد را مستندسازی کنند و درباره اینکه آیا رفتار می‌تواند به مناطق بالقوه که ممکن است به‌عنوان نرم‌افزارهای جاسوسی یا نرم‌افزارهای فریبنده در نظر گرفته شوند تطبیق یابد، ارزیابی انجام دهند.

در مورد دوم، باید یک ارزیاب واجد شرایط مناسب برای ارزیابی اینکه آیا کد بین فروشندگان معیارهای عینی افتاده است استخدام کند که آنها نیز به‌نوبه خود پایبند به‌روش هستند و در نتیجه ابزارهای نرم‌افزار که برای کاربران نهایی توسط سازمان ارائه‌شده است، به‌عنوان نرم‌افزارهای جاسوسی یا آگهی‌افزار توسط فروشندگان ضد جاسوس‌افزارها[3] برچسب ضد جاسوس‌افزار یا ابزارهای تبلیغاتی مزاحم نخورد. بسیاری از فروشندگان ضد جاسوس‌افزار معیارهایی که ارزیابی نرم‌افزار را انجام می‌دهد، منتشر می‌کنند.

سازمان‌ها باید کد امضای رقمی را برای پرونده‌های دودویی پیاده‌سازی کنند در نتیجه فروشندگان ضد بدافزار و ضد جاسوس‌افزار بتوانند به‌راحتی صاحب پرونده و ISV[4] ها را تعیین کنند، این فروشندگان به طور مداوم نرم‌افزاری تولید می‌کنند که از به‌روش تبعیت می‌کند و حتی پیش از تحلیل[5] احتمالاً در دسته‌های امن دسته-بندی شوند.

سازمان باید فنون مفید نرم‌افزار را کشف کند که مشکل نرم‌افزارهای جاسوسی یا بدافزارها را کاهش دهد، سازمان باید همکاری و کار با فروشنده را برای این‌که به طور گسترده در دسترس باشند در نظر داشته باشد. به‌منظور تحقق این الزامات، آموزش امنیت به توسعه‌دهندگان بسیار مهم است. توصیه می‌شود چرخه زندگی توسعه امن نرم‌افزار جایی که امکان به حداقل رساندن آسیب‌پذیری‌های نرم‌افزار وجود دارد مورد استفاده قرار گیرد ازاین‌رو محصول امن‌تر نرم‌افزار آماده و فراهم می‌شود.

یادآوری: استاندارد ISO/IEC 27034، فناوری اطلاعات - فنون امنیتی - امنیت برنامه کاربردی، راهنمایی‌هایی را برای تعریف، توسعه، پیاده‌سازی، مدیریت، پشتیبانی و بازنشستگی برنامه فراهم کند.

۱۱-۴-۲-۳ نظارت و پاسخ شبکه

نظارت بر شبکه معمولاً توسط سازمان‌ها مورد استفاده قرار می‌گیرد تا از قابلیت اعتماد و کیفیت خدمات شبکه خود را تضمین کند. همزمان، این قابلیت می‌تواند وسیله‌ی نفوذی جستجوی برای شرایط استثنایی ترافیک

1- Means
2- Version
3- Anti-spyware
4- Independent software vendor
5- Analysis

شبکه و شناسایی فعالیت‌های مخرب در حال ظهور در شبکه باشد. به طور کلی، سازمان باید موارد زیر را انجام دهد:

- درک ترافیک بر روی شبکه – این‌که چه چیزی طبیعی است و چه چیزی غیرطبیعی است.
- از ابزار مدیریت شبکه برای شناسایی افزایش ناگهانی[1] ترافیک استفاده کنید، ترافیک/مجرا «غیرمعمول» و تضمین اینکه ابزارهایی که با دقت به علت اصلی اشاره می‌کنند و به آن پاسخ می‌دهند در دسترس است.
- آزمایش توانمندی پاسخ پیش از اینکه برای یک رویداد واقعی مورد نیاز باشد. فنون پالایش و پاسخ، فرآیندها و ابزارها بر اساس نتیجه تمرین قاعده‌مند است.
- درک ترکیبات به‌صورت فردی - اگر کسی که به طور معمول یک کاربر غیرفعال است و به طور ناگهانی در ۱۰۰ درصد پهنای باند موجود در دسترس قرار گیرد، ممکن است لازم باشد تا زمانی که دلیل پیدا شود کاربری که مورد تخطی واقع شده است منزوی شود. انزوای شبکه می‌تواند از گسترش نرم‌افزارهای بدخواه جلوگیری کند با این حال برخی پیاده‌سازی‌ها نیازمند رضایت کاربر یا به‌روزرسانی شرایط و ضوابط خدمت است.
- نظارت بر فعالیت از نظرگاه اطلاعات در شبکه مانند DNS[2] و پالاینده‌ی پیام است، که می‌تواند در خدمت علامت‌گذاری[3] افزاره‌هایی که با بدافزارها مورد تخریب قرار گرفته‌اند باشد، اما به دلایل مختلف، توسط ضد ویروس یا خدمات IDS تشخیص داده نشده‌اند.

مثال: با توجه به حجم اطلاعات در شبکه، ابزارهایی مانند IDSها و IPSها می‌توانند برای پایش بر گزارش استثنا، مورد استفاده قرار گیرد.

۱۱-۴-۲-۴ پشتیبانی و تشدید

کسب‌وکار، شامل ارائه‌دهندگان خدمات و سازمان‌های حکومتی است که به طور معمول دارای خدمات پشتیبانی برای پاسخگویی به درخواست‌های مشتریان است و کمک‌های فنی و پشتیبانی برای رسیدگی به مشکلات کاربران نهایی را ارائه می‌دهد. با افزایش تکثیر نرم‌افزارهای بدخواه در اینترنت، امکان دارد سازمان ارائه‌دهنده خدمات، گزارش‌های مربوط به آلوده شدن جاسوس‌افزارها و بدافزارها و دیگر مسائل مربوط به امنیت فضای مجازی را دریافت کند. چنین اطلاعاتی برای فروشندگان برای ارزیابی مخاطره و وضعیت بدافزارها مهم و مفید است و ارائه به‌روزرسانی برای ابزارهای لازم، حذف یا غیرفعال شدن هر گونه جاسوس‌افزار و بدافزار کشف‌شده، را به‌صورت موثر تضمین می‌کند.

در این راستا، سازمان باید با فروشندگان امنیتی ارتباط ایجاد کند و گزارش مربوطه و نمونه‌ی نرم‌افزارهای بدخواه را برای پیگیری - به‌خصوص اگر به نظر می‌رسد در نفوذ افزایش شدید وجود به فروشندگان ارائه دهد.

1- Spikes
2- Domain Name Service
3- Flag

بیشتر فروشندگان فهرستی از رایانامه برای دریافت چنین گزارش‌ها یا نمونه‌هایی برای تحلیل و پیگیری نگهداری می‌کنند. برای مثال، به جدول ب-۱ در پیوست ب مراجعه شود.

۱۱-۴-۲-۵ به‌روز باقی ماندن با آخرین توسعه‌ها

به‌عنوان بخشی از پیاده‌سازی ISMS برای مدیریت مخاطره امنیت اطلاعات سازمانی و همچنین تضمین پیگیری سازمان از به‌روش‌های صنعت و بهره‌برداری از آخرین آسیب‌پذیری‌ها و حفظ وضعیت بهره‌کشی/حمله است، سازمان‌ها باید در جامعه مربوطه یا صنف صنعت برای اشتراک‌گذاری به‌روش‌های خود و یادگیری از دیگر ارائه-دهندگان همکار شرکت کنند.

۱۱-۴-۳ نیازمندی‌های امنیتی برای میزبانی وب و سایر خدمات برنامه کاربردی مجازی

بسیاری از ارائه‌دهندگان خدمات، خدمات میزبانی وب بر روی شبکه و مرکز داده را به‌عنوان بخشی از خدمات کسب‌وکار خود ارائه می‌دهند. این خدمات که شامل وب‌گاه‌ها و دیگر برنامه‌های کاربردی برخط است، اغلب دوباره بسته‌بندی می‌شوند و توسط مشترکین خدمات میزبانی به دیگر مصرف‌کنندگان مانند کسب‌وکارهای کوچک و کاربران نهایی فروخته می‌شود. مشترکین میزبانی وب باید کارساز ناامنی راه‌اندازی کنند، یا میزبان محتوای خرابکارانه در وب‌گاه‌ها یا برنامه‌های کاربردی خود باشند، درهرصورت امنیت مصرف‌کنندگان تحت تأثیر قرار خواهد گرفت. به همین دلیل، مهم است که خدمات، حداقل، مطابق با استانداردهای به‌روش موافق با خط-مشی یا شرایط قرارداد باشد.

هر جا که ارائه‌دهندگان متعدد استفاده می‌شوند، توصیه می‌شود تعامل بین ارائه‌دهندگان باید تحلیل شود و موافقت‌نامه خدمات مربوطه هر تعامل حیاتی را نشان دهد. به‌عنوان مثال، توصیه می‌شود به‌روزرسانی یا بسته-های وصله سامانه‌ی ارائه‌دهنده با ارائه‌دهندگان دیگر هماهنگ باشد، باید نتیجه در تعامل منفی به‌روزرسانی شود.

شرایط قرارداد باید حداقل موارد زیر را پوشش دهد:

الف- اطلاع‌رسانی واضح، توصیف وب‌گاه برخط یا برنامه‌های کاربردی امنیتی و شیوه‌های حفظ حریم خصوصی، شیوه‌های جمع‌آوری داده‌ها و رفتار هر کد (برای مثال، شی مرورگر کمک) که وب‌گاه برخط یا برنامه‌کاربردی می‌تواند در میزکار[1] کاربر نهایی یا محیط‌های مرورگر وب اجرا و توزیع شود.

ب- رضایت کاربر، تسهیل توافق کاربر یا مخالفت با شرایط خدمات شرح داده‌شده در یادداشت‌ها. این امر به کاربر اجازه می‌دهد تا ملاحظات را ابراز کند و در نتیجه تعیین کند که آیا می‌تواند شرایط خدمات را بپذیرد.

پ- کنترل‌های کاربر، پس از توافق اولیه، به کاربران برای تغییر تنظیمات خود کمک کند یا در غیر این صورت هر موقعی در آینده، به پذیرش آنها خاتمه دهد.

1- Desktops

شرایط و تضمین این‌که کاربران نهایی رفتار و اعمال وب‌گاه برخط یا برنامه کاربردی را فهمیده‌اند، برای حفظ حریم خصوصی و امنیت کاربران نهایی مهم است. توصیه می‌شود شرایط با کمک یک حرفه‌ای مجاز ایجاد شود، که در نتیجه وارد شدن زیان‌های خاص یا آسیب وارده با توجه به محتوای خرابکارانه یا خط مشی‌ها و شیوه‌های نامشخص در وب‌گاه، تضمین که غرامت ارائه‌دهنده خدمات را از اقدامات قانونی بالقوه و از کاربران نهایی پرداخت می‌کند.

علاوه بر حفاظت از داده‌ها و مقررات حفظ حریم خصوصی شخصی در وب‌گاه برخط یا برنامه کاربردی، ارائه-دهندگان خدمات باید نیازمند وب‌گاه‌های برخط یا برنامه‌های کاربردی باشند که میزبان آنها در شبکه خود هستند، تا قبل از اجرای زنده آنها مجموعه‌ای از کنترل‌های امنیتی به‌روش در سطح برنامه کاربردی تنظیم شود. این موارد می‌تواند شامل نمونه‌های موجود در بند ۱۲-۲ باشد البته محدود به آنها نیست. به‌عنوان بخشی از زیرساخت‌های ارائه‌دهنده خدمات میزبانی وب، توصیه می‌شود کارسازها در مقابل دسترسی‌های غیرمجاز و توانایی میزبانی محتوای خرابکارانه محافظت شوند. برای مشاهده نمونه‌های کنترل به بند ۱۲-۳ مراجعه شود.

برای دادن مجوز به اجرای این کنترل‌های امنیتی، به‌ویژه، کنترل‌هایی که با وب‌گاه و امنیت برنامه کاربردی برخط مرتبط هستند، توصیه می‌شود ارائه‌دهندگان خدمات این مقررات را در شرایط توافق‌نامه‌های خدمات شرکت لحاظ کنند.

۱۱-۴-۴ راهنمایی امنیتی برای مصرف‌کنندگان

ارائه‌دهندگان خدمات باید به مصرف‌کنندگان در مورد چگونگی برخط باقی ماندن امن راهنمایی ارائه دهند. ارائه‌دهندگان خدمات ممکن است به طور مستقیم راهنمایی را ایجاد کنند، یا کاربران را به وب‌گاه‌های راهنمای قابل‌دسترس که می‌توانند مطالب را تهیه کنند ارجاع دهند.

همان‌گونه که در بند ۷ شرح داده شده است، آموزش کاربران نهایی در مورد این‌که چگونه می‌توانند در ایجاد اینترنت امن شرکت کنند و در رابطه با نقش‌های متعدد که می‌توانند در فضای مجازی بازی کنند، بسیار حائز اهمیت و حیاتی است. همان‌گونه که در بند ۱۱-۳ شرح داده شده است، علاوه بر این توصیه می‌شود، به کاربران نهایی اتخاذ کنترل‌های فنی امنیتی لازم را توصیه کرد تا ارائه‌دهندگان خدمات نیز بتوانند نقش فعالی بازی کنند. نمونه‌هایی از فعالیت‌های راهنمایی ممکن است شامل موارد زیر باشد:

الف- دوره‌ای (به‌عنوان مثال، ماهانه) خبرنامه‌های امنیتی برای توصیه در مورد فنون امنیتی خاص (به‌عنوان مثال، چگونه یک رمز عبور خوب انتخاب کنیم)، به‌روزرسانی در روند امنیتی؛ و ارائه اطلاعیه‌های رسانه-ای امنیتی، دیگر فیلم‌های مبتنی بر تقاضا، پخش صوتی و اطلاعات امنیت که از طریق درگاه وب سازمان یا دیگر ارائه‌دهندگان محتوای امنیت در دسترس است.

ب- پخش مستقیم بر حسب تقاضای فیلم آموزش امنیت یا رسانه‌ای که موضوعات مختلف امنیتی را برای بهبود شیوه‌های امنیتی کاربران نهایی و بهبود آگاهی تحت پوشش قرار می‌دهد.

پ- ترکیب یک ستون امنیتی در خبرنامه نسخه چاپی[1] ارائه‌دهنده خدمات که به محل سکونت یا دفتر کار کاربران نهایی برای برجسته کردن محتوا یا رویدادهای امنیتی کلیدی ارسال می‌شود.

ت- برگزاری سالانه یا دوره‌ای هم‌اندیشی‌ها یا جلسات سیار [2] در زمینه امنیت کاربر نهایی، در صورت امکان با مشارکت دیگر نقش‌آفرینان صنعت، فروشندگان و دولت‌ها.

ارائه‌دهندگان خدمات با استفاده از رایانامه به‌عنوان راه اصلی برقراری ارتباط با کاربران نهایی کار بسیار مهمی در کمک به مقابله در برابر حملات مهندسی اجتماعی به کاربران نهایی انجام دهند. به طور خاص، توصیه می‌شود به طور مداوم به کاربران نهایی یادآوری شود تا رایانامه‌های ناخواسته را از رایانامه ارائه‌دهنده خدمات تمیز دهند و ارائه‌دهنده هرگز درخواست:

- اطلاعات شخصی؛
- نام کاربر؛
- رمز عبور؛ و
- هرگز شامل پیوندهای مرتبط با امنیت نخواهد بود تا خواننده نامه روی آن کلیک کند.

هنگامی که یک ارائه‌دهنده خدمات از کاربر بخواهد به وب‌گاه مراجعه کند و اطلاعاتی را بدهد، باید به کاربر بگوید که چگونه با خیال راحت به URL مورد نیاز متصل شود. برای مثال، ممکن است از کاربر بخواهد URL منتقل‌شده را به مرورگر خود وارد کند و مطمئن شود که URL منتقل‌شده حاوی پیوند کلیک نیست.

توصیه می‌شود به‌عنوان بخشی از آموزش امنیتی و راهنمایی کاربر در برابر نرم‌افزار فریبنده و جاسوس‌افزار، سازمان‌ها و ارائه‌دهندگان خدمات به کاربران نهایی خود در استفاده از کنترل‌های امنیت فنی مناسب برای حفاظت از سامانه خود در برابر بهره‌کشی و حملات شناخته‌شده مشاوره و توصیه ارائه کنند.

به‌عنوان یک راهنمای کلی، مصرف‌کنندگان باید به پیاده‌سازی کنترل‌های موجود در بند ۱۲-۴ تشویق شوند پیوست ب مثالی از فهرست مراجع و منابع برخط که در پشتیبانی از پیاده‌سازی و اجرای توصیه‌های بالا می‌تواند مورد استفاده قرار گیرد را فراهم می‌کند.

۱۲ کنترل‌های امنیت فضای مجازی

۱۲-۱ مرور کلی

هنگامی که مخاطرات وارد بر امنیت فضای مجازی شناسایی شدند و راهنمایی‌های مناسب طرح شد، کنترل‌های امنیت فضای مجازی که نیازمندی‌های امنیتی را پشتیبانی می‌کند می‌تواند انتخاب و اجرا شود. این بند مرور کلی از کنترل‌های کلیدی امنیت فضای مجازی ارائه می‌دهد که برای پشتیبانی از راهنمایی‌ها می‌تواند اجرا شود و در این استاندارد ملی ایران طرح‌ریزی و قرار داده شده است.

1- Hard-Copy
2- Road Show

۱۲-۲ کنترل‌های سطح برنامه کاربردی

کنترل‌های سطح برنامه کاربردی عبارت‌اند از:

الف- نمایش اعلامیه‌های کوتاه، که خلاصه‌ای روشن، مختصر یک صفحه‌ای (با استفاده از زبان ساده) از خط - مشی‌های برخط ضروری شرکت را ارائه می‌دهد. با استفاده از این، کاربران قادر به انتخاب آگاهانه‌تر در مورد به اشتراک‌گذاری اطلاعات برخط خود خواهند بود. اطلاع‌رسانی‌های کوتاه باید با همه الزامات قانونی مطابقت داشته و به اظهارات قانونی و سایر اطلاعات مربوطه پیوندهای کامل ارائه دهند، بنابراین مشتریانی که جزئیات بیشتری می‌خواهند به‌راحتی با کلیک می‌توانند نسخه طولانی‌تر را بخوانند. با یک اطلاع‌رسانی، مشتریان می‌توانند تجربه سازگارتری با استانداردهای یکنواخت حفظ حریم خصوصی در سراسر ویژگی‌های شرکت و انتظاراتی که به بسیاری از وب‌گاه‌ها عمومیت داده شده است، داشته باشند.

ب- ساماندهی[1] امن نشست برای برنامه‌های کاربردی تحت وب؛ که می‌تواند شامل ساز و کارهای برخط مانند کوکی‌ها باشد.

پ- اعتبارسنجی ورودی امن، رسیدگی و مدیریت جلوگیری از حملات متداول مانند تزریق زبان پرس‌وجوی ساخت‌یافته[2]. بر اساس این واقعیت که وب‌گاه‌ها، به طور کلی قابل‌اعتماد در نظر گرفته می‌شوند، به طور فزاینده‌ای برای توزیع کدهای خرابکارانه استفاده می‌شوند، اعتبارسنجی ورودی و خروجی باید به‌وسیله محتوای فعال و همچنین محتوای پویا انجام شود.

ت- برنامه‌نویسی امن صفحه وب برای جلوگیری از حملات متداول مانند تزریق کد[3].

ث- بررسی و آزمایش امنیت کد به شیوه‌ای مناسب توسط هستارهای ماهر.

ج- خدماتی که سازمان ارائه می‌دهد، چه توسط سازمان چه توسط طرفی که نماینده سازمان است، توصیه می‌شود به روشی که مصرف‌کننده بتواند خدمت را تأیید هویت کند ارائه شود. ممکن است شامل استفاده ارائه‌دهنده از زیر دامنه‌ی علامت‌دار از نام سازمان باشد و احتمالاً استفاده از اعتبار پروتکل امن انتقال ابرمتن[4]ای که در سازمان ثبت شده است. این خدمت باید از استفاده روش‌های فریبنده که در آن ممکن است مصرف‌کننده در تعیین این‌که با چه کسی در خرید و فروش است مشکل داشته باشد، اجتناب کند.

۱۲-۳ حفاظت از کارساز

کنترل های زیر را می‌توان برای محافظت از کارسازها در مقابل دسترسی‌های غیرمجاز و میزبانی محتوای خرابکارانه روی کارساز مورد استفاده قرار داد:

الف- پیکربندی کارسازها، شامل سامانه‌های عامل اساسی مطابق با پایه پیکربندی راهنمای امنیت است. این راهنما باید شامل تعریف مناسب کاربران کارساز در مقابل مدیران باشد، اجرای کنترل دسترسی بر روی

1- Handling
2- SQL (Structured Query Language)
3- Cross-Site Scripting
4- HTTPS (Hypertext Transfer Protocol Secure)

برنامه و پوشه‌ها و پرونده‌ها و مسیرهای ممیزی، به‌ویژه، برای امنیت و سایر رویدادهای شکست بر روی سامانه را فراهم می‌کند. علاوه بر آن به‌منظور کاهش بردار حمله توصیه می‌شود حداقل سامانه بر روی کارساز نصب شود.

ب- پیاده‌سازی یک سامانه برای آزمایش و گسترش به‌روزرسانی‌های امنیتی، و تضمین کند هنگامی که به‌روزرسانی‌های جدید امنیتی در دسترس هستند، سامانه عامل و برنامه‌های کاربردی فورا بروز نگهداری شوند.

پ- پایش عملکرد امنیت کارساز از طریق بررسی‌های منظم مسیرهای ممیزی.

ت- بررسی پیکربندی امنیتی.

ث- اجرای کنترل‌های نرم‌افزاری ضد مخرب (مانند ضد ویروس و ضد جاسوس‌افزار) بر روی کارساز.

ج- پیمایش منظم میزبانی و بارگذاری تمام محتوا با استفاده از کنترل‌های بروز نرم‌افزاری ضد مخرب. تشخیص این‌که یک پرونده می‌تواند به‌عنوان مثال، هنوز جاسوس‌افزار یا بدافزار باشد، حتی اگر به دلیل محدودیت اطلاعات ناقص توسط کنترل‌های کنونی تشخیص داده نشود.

ح- انجام ارزیابی آسیب‌پذیری و آزمایش امنیتی منظم برای وب‌گاه‌های امنیتی برخط و برنامه‌های کاربردی و اطمینان حاصل شود که امنیت آنها به‌اندازه کافی حفظ شده است.

خ- پیمایش منظم برای کشف تخریب‌ها.

۱۲-۴ کنترل‌های کاربر نهایی

در زیر فهرستی ناقص از کنترل‌هایی که کاربران نهایی می‌توانند استفاده کنند تهیه شده است تا از سامانه خود در برابر بهره‌کشی و حملات شناخته‌شده حفاظت کنند:

الف- استفاده از سامانه‌های عامل پشتیبانی‌شده، با بسته‌های نرم‌افزاری وصله امنیتی به‌روزرسانی و نصب‌شده. مصرف‌کنندگان سازمانی تعهد دارند که از خط‌مشی سازمانی در مورد سامانه‌های عامل پشتیبانی شده آگاه بوده و پیروی کنند. توصیه می‌شود افراد حقیقی مصرف‌کننده آگاه بوده و در نظر داشته باشند که سامانه عاملی را که توسط ارائه‌دهنده پیشنهاد داده شده است استفاده کنند. توصیه می‌شود در تمام موارد، سامانه عامل با توجه به بسته‌های نرم‌افزاری امنیتی وصله، به‌روز نگه‌داشته شود.

ب- استفاده از آخرین پشتیبانی برنامه‌های کاربردی، با وصله‌هایی که بیشترین به‌هنگام‌سازی را داشته‌اند. مصرف‌کنندگان سازمانی مسئولیت آگاهی و پیروی از خط‌مشی سازمانی در مورد نرم‌افزار برنامه کاربردی پشتیبانی شده را دارند. افراد حقیقی مصرف‌کننده باید آگاه بوده و در نظر داشته باشند که برنامه‌های کاربردی را که توسط ارائه‌دهنده پیشنهاد داده شده است استفاده کنند. در تمام موارد، برنامه‌های کاربردی با توجه به بسته‌های نرم‌افزاری امنیتی وصله، باید به‌روز نگه‌داشته شوند.

پ- استفاده از ضد ویروس و ابزار ضد جاسوس‌افزار. در صورت امکان، ارائه‌دهنده خدمات مانند ISP باید همکاری با فروشندگان امنیتی مورد اعتماد را در نظر داشته باشد تا این ابزارها را به‌عنوان بخشی از

بسته‌ی اشتراک خدمات به کاربران نهایی پیشنهاد دهد به‌طوری که کنترل‌های امنیتی پس از امضای اشتراک یا پس از تجدید در دسترس قرار گیرد. مصرف‌کنندگان سازمانی تعهد دارند که از خطمشی سازمانی در مورد استفاده از ابزارهای نرم‌افزاری امنیتی آگاه بوده و پیروی کنند. افراد حقیقی مصرف-کننده باید از ابزارهای نرم‌افزاری امنیتی استفاده کنند آنها باید پیگیر ارائه‌دهنده باشند تا از هر توصیه، ارائه، یا توقف نرم‌افزار امنیتی باخبر شوند. توصیه می‌شود در تمام موارد، نرم‌افزار امنیتی با توجه به وصله امنیتی و دادگان‌های امضاء، به‌روز نگه‌داشته شود.

ت- پیاده‌سازی مناسب ضد ویروس و ضد جاسوس‌افزار پادمان[1]. مرورگرهای متداول وب و نوار ابزارهای مرورگر در حال حاضر قابلیت‌هایی مانند مسدودکننده بالاپرها را دارند که از نمایش پنجره وب‌گاه‌های مخرب که حاوی نرم‌افزارهای جاسوس‌افزار یا نرم‌افزارهای فریبنده هستند جلوگیری می‌کند، زیرا آنها می‌توانند از نقاط ضعف سامانه یا مرورگر بهره‌کشی کنند، یا از حقه‌های مهندسی اجتماعی برای فریب کاربران برای دانلود و نصب آنها بر روی سامانه استفاده کنند. سازمان‌ها باید برای استفاده از چنین ابزارهایی خط مشی تأسیس نمایند. سازمان‌های ارائه‌کننده خدمات باید فهرستی از ابزارهای توصیه‌شده را جمع‌آوری کنند و توصیه می‌شود کاربران نهایی به استفاده از آنها تشویق شوند، با این راهنمایی در مورد امکان توانمندسازی و اعطای مجوز برای وب‌گاه‌ها، فقط در صورت علاقه‌مندی کاربر به دادن مجوز به آن وب‌گاه‌ها صورت خواهد گرفت.

ث- فعال کردن مسدودکننده نویسه. فعال کردن مسدودکننده نویسه یا تنظیم امنیتی بالاتر برای وب، برای تضمین این‌که تنها نویسه‌هایی که از منابع قابل‌اعتماد دریافت شده‌اند بر روی رایانه‌ی محلی اجرا شوند.

ج- استفاده از پالاینده‌های دزدی هویت. مرورگرهای وب متداول و نوار ابزار مرورگر اغلب دارای این قابلیت هستند که می‌تواند تعیین کند که آیا یک وب‌گاه که یک کاربر در حال دیدن آن است درون دادگان وب‌گاه‌های دزدی هویت شناخته‌شده وجود دارد، یا حاوی الگوهای[2] اسکریپتی است که شبیه به وب‌گاه-های دزدی هویت معمولی هستند. مرورگر برای اخطار به کاربران از مخاطره بالقوه باید هشدار ارائه دهد که به طور معمول به شکل کد-رنگی برجسته است. سازمان‌ها باید خطمشی‌ای ایجاد کنند که استفاده از چنین ابزاری را ممکن سازد.

ح- استفاده از دیگر ویژگی‌های امنیتی در دسترس مرورگر وب. گاه، همان‌گونه که مخاطره امنیت فضای مجازی جدید پدیدار می‌شود، مرورگرهای وب و ارائه‌دهندگان نوار ابزار مرورگر، قابلیت‌های امنیتی جدید برای محافظت از کاربران در برابر مخاطرات اضافه می‌کنند. کاربران نهایی باید از این تحولات مطلع باشند و این مطلع شدن با آموزش این به‌روزرسانی‌ها که معمولاً توسط ارائه‌دهندگان ابزار ارائه می‌شود میسر است. سازمان‌ها و ارائه‌دهندگان خدمات باید به طور مشابه این قابلیت‌های جدید را

1 -Safe guards
2- Patterns

بازبینی کنند و خطمشی‌ها و خدمات مرتبط را برای خدمات بهتر به نیازهای سازمان و مشتریان به‌روزرسانی کنند و مخاطره مربوط به امنیت فضای مجازی را تعیین کنند.

خ- فعال کردن دیواره‌آتش شخصی و HIDS. دیواره‌آتش شخصی و HIDS ابزارهای مهمی برای کنترل خدمات شبکه در دسترسی به سامانه‌های کاربر هستند. تعدادی از سامانه‌های عامل جدیدتر دارای دیواره‌آتش شخصی و HIDS به‌هم پیوسته هستند. درحالی‌که به طور پیش‌فرض فعال هستند، در نتیجه قرار گرفتن در معرض امنیت شبکه نامطلوب، کاربران یا برنامه‌های کاربردی ممکن است آنها را غیرفعال کنند. سازمان‌ها باید خطمشی‌ای در استفاده از دیواره‌آتش شخصی و HIDS اتخاذ کنند و ابزار مناسب یا محصولات مورد نیاز برای اجرا را ارزیابی کنند به‌نحوی که استفاده از آنها را به طور پیش‌فرض برای همه کارکنان خود فعال کنند. ارائه‌دهندگان خدمات باید به استفاده از دیواره‌آتش شخصی و توابع HIDS تشویق کنند و/یا به طرف سوم دیگر پیشنهاد دهند که دیواره‌آتش شخصی و محصولات HIDS مورد ارزیابی قرار گرفت و قابل‌اعتماد در نظر گرفته شده است و آموزش و کمک به کاربران در فعال کردن امنیت شبکه‌ی پایه‌ای در سطح کاربر پایانی سامانه کاربر.

د- فعال کردن به‌روزرسانی‌های خودکار. درحالی‌که کنترل‌های فنی امنیت فوق قادر به برخورد با اکثر نرم‌افزارهای مخرب در سطح عملیاتی مربوطه می‌باشند، در برابر بهره‌کشی از آسیب‌پذیری‌های که در سامانه عامل و محصولات برنامه کاربردی وجود دارد بسیار موثر نیست. برای جلوگیری از چنین بهره-کشی‌هایی، کارکرد به‌روزرسانی شده موجود در سامانه عامل و همچنین آنهایی که توسط برنامه‌های کاربردی مورد اعتماد کاربر ارائه‌شده است (به‌عنوان مثال، ارزیابی محصولات ضد جاسوس‌افزار مورد اعتماد طرف سوم و محصولات ضد ویروس)، توصیه می‌شود برای اینکه به‌روزرسانی خودکار انجام شود فعال شوند. سپس هر زمان در دسترس باشند، در نتیجه تضمین می‌شود که سامانه‌ها با آخرین وصله‌های امنیتی بروزرسانی شده‌اند، و هر زمان که در دسترس باشند فاصله زمانی برای به واقوع پیوستن بهره‌کشی را مسدود می‌کنند.

۱۲-۵ کنترل‌های در برابر حملات مهندسی اجتماعی

۱۲-۵-۱ مرور کلی

به‌منظور موفق شدن، مجرم‌های مجازی[1] به طور فزاینده‌ای به فنون[2] روانی یا مهندسی اجتماعی دسته‌بندی می‌شوند.

مثال ۱: استفاده از رایانامه‌های حامل URI که کاربران قابل‌اعتماد را به وب‌گاه‌های دزدی هویت راهنمایی می‌کند.

1- Cybercriminals
2- Tactics

مثال ۲: رایانامه‌های فریبنده که از کاربران، ارائه اطلاعات شناسایی شخصی یا اطلاعات مربوط به مالکیت معنوی شرکت را درخواست می‌کنند.

گسترش شبکه‌های اجتماعی و وب‌گاه‌های اجتماعی حامل‌های جدیدی که بیشتر باورهای فریبنده و متقلب را افزایش می‌دهد، فراهم می‌کند. به طور فزاینده، چنین حملاتی نیز فراتر از فناوری، فراتر از سامانه‌های رایانه‌ای شخصی و اتصال[1] به شبکه‌های سنتی، اعمال‌نفوذ تلفن همراه، شبکه‌های بی‌سیم[2] (بلوتوث[3]) و صدا بر روی پروتکل اینترنتی[4] است.

این بند چارچوبی از کنترل‌های قابل‌استفاده برای مدیریت و به حداقل رساندن مخاطره‌ی امنیت فضای مجازی در رابطه با حملات مهندسی اجتماعی فراهم می‌کند. راهنمایی ارائه‌شده در این بند بر اساس این تصور بنا شده است که تنها راه موثر برای کاهش تهدید مهندسی اجتماعی از طریق ترکیب زیر به‌دست می‌آید:

- فناوری‌های امنیتی؛
- خطمشی‌های امنیتی که مجموعه قوانین اساسی برای رفتار شخصی تنظیم می‌کند، هم به‌عنوان فرد و هم به‌عنوان کارمند و
- آموزش و پرورش مناسب.

بنابراین چارچوب موارد زیر را پوشش می‌دهد:

- خط مشی‌ها؛
- روش‌ها و فرآیندها؛
- افراد و سازمان‌ها و
- کنترل فنی اجرایی.

۱۲-۵-۲ خط مشی‌ها

توصیه می‌شود هم‌راستا با اعمال متداول برای مدیریت مخاطره امنیت اطلاعات، خط مشی‌های اساسی حاکم بر ایجاد، جمع‌آوری، ذخیره‌سازی، انتقال، به اشتراک‌گذاری، پردازش و استفاده عمومی از اطلاعات شخصی و سازمانی و مالکیت معنوی در اینترنت و فضای مجازی مشخص و مستند شود. به طور خاص، به برنامه‌های کاربردی مانند پیام بی‌درنگ، وب‌نویسی، به اشتراک‌گذاری پرونده‌ی P2P و شبکه‌های اجتماعی که معمولاً فراتر از محدوده شبکه‌های سازمانی و امنیت اطلاعات است، مربوط است.

به‌عنوان بخشی از خطمشی‌های شرکت، بیانیه‌ها و مجازات نیز مربوط به استفاده‌نابجا از فضای مجازی هستند، برنامه‌های کاربردی نیز باید ترکیب شوند تا از شیوه‌های استفاده‌نابجا کارکنان و طرف‌های سوم در شبکه‌ی شرکت‌ها یا سامانه‌هایی که به فضای مجازی دسترسی دارند جلوگیری شود.

1- Connectivity
2- Wireless
3- Bluetooth
4- VOIP

خط‌مشی‌های اداری ارتقاء آگاهی و درک مخاطرات امنیت فضای مجازی و تشویق، اگر الزامی نیست، یادگیری و توسعه مهارت‌ها در برابر حملات امنیت فضای مجازی، به‌ویژه، حملات مهندسی اجتماعی، توصیه می‌شود توسعه یابد و اعلام شود و این باید شامل الزامات مورد نیاز برای حضور منظم در چنین جلسات و آموزش‌هایی باشد.
با ترویج خط مشی‌های مناسب و آگاهی در مورد مخاطرات مهندسی اجتماعی، کارکنان دیگر نمی‌توانند ادعای نادیده گرفتن چنین مخاطرات و الزاماتی را داشته باشند و هم‌زمان توسعه و درک به‌روش و خط مشی‌هایی که از شبکه‌های اجتماعی خارجی انتظار می‌رود و دیگر برنامه‌های کاربردی فضای مجازی، برای مثال، توافق خط مشی امنیتی ارائه‌دهنده خدمات را گسترش دهند.

۱۲-۵-۳ روش‌ها و فرآیندها

۱۲-۵-۳-۱ دسته‌بندی و طبقه‌بندی اطلاعات

توصیه می‌شود از خط‌مشی‌ها که شامل دارایی‌های معنوی، فرآیندهای دسته‌بندی و طبقه‌بندی اطلاعاتی هستند برای ترویج آگاهی و حمایت از اطلاعات حساس شخصی و طبقه‌بندی‌شده شرکت‌های بزرگ پشتیبانی شود، اجرایی شود.
توصیه می‌شود برای هر دسته و طبقه‌بندی اطلاعات مربوط، کنترل‌های امنیتی ویژه‌ای برای محافظت در برابر افشای اتفاقی و دسترسی‌های غیرمجاز عمدی توسعه یابد و مستند شود. سپس کاربران سازمان‌ها می‌توانند بین دسته‌ها و طبقه‌بندی مختلف اطلاعاتی که آن‌ها تولید کرده‌اند، یا جمع‌آوری و مدیریت نموده‌اند تمایز قائل شوند.
پس از آن کاربران در هنگام استفاده از فضای مجازی، می‌توانند احتیاط لازم و کنترل‌های محافظتی را اعمال کنند. روش رسیدگی و مدیریت بر دارایی‌های معنوی شرکت، یا داده‌های شخصی و دیگر اطلاعات محرمانه نیز باید ایجاد و ابلاغ شود.

۱۲-۵-۳-۲ آگاهی و آموزش

آگاهی و آموزش امنیت، از جمله به‌روزرسانی منظم دانش و یادگیری مرتبط عناصر مهمی برای مقابله با حملات مهندسی اجتماعی هستند. توصیه می‌شود کارکنان و پیمانکاران طرف سوم، به‌عنوان بخشی از برنامه امنیت فضای مجازی سازمان، حداقل ساعت محتمل برای آموزش و آگاهی را بگذرانند تا تضمین شود که از نقش‌ها و مسئولیت‌های خود در فضای مجازی و اجرای کنترل‌های فنی که باید به‌عنوان افرادی که از فضای مجازی استفاده می‌کنند آگاهی دارند.
علاوه بر این، به‌عنوان بخشی از برنامه که باید با حملات مهندسی اجتماعی مقابله کند، چنین آگاهی‌رسانی باید شامل محتویات زیر باشد:

الف- آخرین تهدیدات و اشکال حملات مهندسی اجتماعی، به‌عنوان مثال، چگونه دزدی هویت از وب‌گاه‌های جعلی به تنهایی به ترکیبی از نامه‌های الکترونیکی ناشناس، تزریق کد و حملات تزریق SQL تبدیل شده است.

ب- چگونه اطلاعات فردی و سازمانی از طریق حملات مهندسی اجتماعی، به سرقت می‌رود و دست‌کاری می‌شود، در صورت درک اینکه مهاجم چگونه از طبیعت انسانی[1] سوءاستفاده می‌کند، مانند تمایل به موافقت با درخواست‌هایی که با مجوز به وجود می‌آیند (حتی اگر غیرواقعی باشد)، رفتار دوستانه، قربانی به نظر آمدن و عمل مبادله مانند دادن چیزی با ارزش یا کمک کردن در همان اول کار.

پ- مطابق با خطمشی‌های امنیت اطلاعات چه اطلاعاتی باید محافظت و چگونه این کار انجام شود.

ت- برای نزدیک شدن به متولیان یا دایره پاسخ و اطلاعات در دسترس این تماس‌ها، چه موقع گزارش یا تشدید برای رویداد مشکوک یا برنامه‌های کاربردی مخرب داده شود. به‌عنوان مثال، به پیوست ب مراجعه شود.

سازمان‌هایی که برنامه‌های کاربردی فضای مجازی و خدمات برخط ارائه می‌دهند باید اصول آگاهی به مشترکین و مصرف‌کنندگان که محتوای آنچه بالاتر گفته شد را پوشش می‌دهد و در زمینه‌ی برنامه‌های کاربردی و خدمات آن‌ها است، ارائه کنند.

۱۲-۵-۳-۳ آزمودن[2]

کارکنان باید تأییدیه‌ای که محتوای خطمشی امنیتی سازمان را قبول و درک کرده‌اند را امضا کنند. به‌عنوان بخشی از فرآیند برای بهبود آگاهی و اطمینان از توجه به چنین مخاطره‌ای، سازمان باید برگزاری آزمون‌های دوره‌ای برای تعیین سطح آگاهی و انطباق با خطمشی‌ها و شیوه‌های مرتبط را در نظر بگیرد.

کارکنان می‌توانند آزمون کتبی یا CBT بدهند تا معین شود آیا آن‌ها محتوای خطمشی امنیتی سازمان را درک کرده‌اند. این آزمون‌ها ممکن است شامل، ایجاد وب‌گاه‌های هدف اما تحت کنترل دزدی هویت، نامه‌های الکترونیکی ناشناس و رایانامه‌های فریبنده با استفاده از محتوای مهندسی اجتماعی باورکردنی باشد البته محدود به این‌ها نیست. هنگام انجام این آزمون‌ها، مهم است اطمینان حاصل شود که:

الف- کارسازها و محتویات آزمون همگی تحت کنترل و فرمان گروه آزمون است؛

ب- حرفه‌ای‌هایی که تجربه قبلی از اجرای چنین آزمونی داشته‌اند جایی که امکان‌پذیر است به‌کار گماشته شوند؛

پ- کاربران از طریق برنامه‌های آگاهی‌رسانی و آموزشی برای این آزمون‌ها آماده می‌شوند؛ و

ت- تمام نتایج آزمون در قالب مجموعه ارائه می‌شود، زیرا هدف آن محافظت از حریم خصوصی افراد است چون ممکن است نتیجه آزمون موجب شرمساری افراد شود و اگر به طور مناسب مدیریت نشود باعث نگرانی‌های حریم خصوصی شود.

یادآوری- اصول اخلاقی و قانون هر کشور نیز باید در نظر گرفته شود.

۱۲-۵-۴ مردم و سازمان

1- Human Nature
2- Testing

درحالی‌که افراد اهداف اصلی حملات مهندسی اجتماعی هستند، سازمان نیز می‌تواند به‌عنوان کاندیدایی برای قربانی در نظر گرفته شود. بااین‌حال، مردم، نقطه ورودی اصلی برای حملات مهندسی اجتماعی باقی می‌مانند. به‌این‌ترتیب، مردم نیازمند آگاهی از مخاطرات مرتبط در فضای مجازی هستند و سازمان‌ها باید خط مشی‌های مربوطه را ایجاد کنند و برای حمایت از برنامه‌های مرتبط اقدامات پیشگیرانه انجام دهند تا آگاهی و مهارت مردم تضمین شود.

به‌عنوان یک راهنمایی کلی، همه شرکت‌ها و سازمان‌ها (از جمله سرمایه‌گذاری، ارائه‌دهندگان خدمات و دولت) باید مصرف‌کنندگان فضای مجازی را ترغیب کنند که خطرات مهندسی اجتماعی در فضای مجازی را یاد بگیرند و درک کنند و آن‌ها را تشویق کنند تا مراحلی را که باید در محافظت از خود در برابر حملات بالقوه اتخاذ کنند، طی نمایند.

۱۲-۵-۵ فنی

علاوه بر ایجاد خط مشی‌ها و اقدامات در مقابل حملات مهندسی اجتماعی، جایی که امکان‌پذیر است کنترل فنی توصیه می‌شود در نظر گرفته شود، کنترل فنی برای کمینه کردن افشاءسازی و بهره‌کشی بالقوه اشرار فضای مجازی اتخاذ شده است.

در سطح شخصی، کاربران فضای مجازی باید راهنمایی‌های مورد بحث در بند ۱۱-۳ را اتخاذ کنند. سازمان‌ها و ارائه‌دهندگان خدمات باید مراحل مربوطه شرح داده‌شده در بند ۱۱-۴-۴ را برای تسهیل پذیرش و استفاده‌ی کنترل‌های امنیتی فنی کاربران را بر عهده بگیرند.

سازمان‌ها و ارائه‌دهندگان خدمات همچنین باید راهنمایی‌های ارائه‌شده در بند ۱۱-۴ را اتخاذ کنند که به‌عنوان کنترل‌های پایه در برابر حملات مهندسی اجتماعی در فضای مجازی مهم هستند. علاوه بر این توصیه می‌شود، کنترل‌های فنی زیر که در برابر حملات مهندسی اجتماعی خاص مفید هستند در نظر گرفته شوند:

الف- جایی که اطلاعات شخصی یا حساس شرکت‌های بزرگ در برنامه‌های کاربردی برخط درگیر هستند، شرایط ارائه راه‌حل‌های اصالت‌سنجی قوی را یا به‌عنوان بخشی از احراز هویت ورود به سامانه و/یا زمانی که معاملات بحرانی در حال اجرا هستند در نظر بگیرید. اصالت‌سنجی قوی، به استفاده از دو یا چند عامل اضافی برای تصدیق هویت بیشتر یا بالاتر از استفاده شناسه کاربری و رمز عبور اشاره دارد. عامل-های دوم و اضافی ممکن است با استفاده از کارت هوشمند[1]، زیست سنجی[2]، یا دیگر نشانه‌های امنیتی دستی ارائه شود.

ب- برای خدمات مبتنی بر وب، سازمان‌ها باید استفاده از یک «گواهی تضمین بالا» برای ارائه تضمین افزوده به کاربران برخط را در نظر بگیرند. بسیاری از مراجع تجاری صدور گواهینامه (CA)[3] و مرورگرهای اینترنتی قادر به حمایت از استفاده از این گواهینامه‌ها هستند که باعث کاهش خطر حملات دزدی

1- Smartcard
2- Biometrics
3 Certification Authorities

هویت می‌شود.

پ- توصیه می‌شود برای اطمینان از امنیت رایانه‌های کاربران متصل به سازمان یا وب‌گاه ارائه‌دهنده خدمات یا برنامه کاربردی در فضای مجازی، کنترل‌های اضافی برای اطمینان از حداقل سطح امنیت، از جمله نصب و راه‌اندازی آخرین به‌روزرسانی‌های امنیتی، در نظر گرفته شود. توصیه می‌شود استفاده از این کنترل‌ها در توافقنامه خدمات کاربر نهایی و/یا وب‌گاه حفظ حریم خصوصی و خط مشی امنیتی که هر کدام قابل‌اجرا است منتشر شود

۱۲-۶ آمادگی امنیت فضای مجازی

پیوست الف کنترل‌های اضافی فنی که برای بهبود آمادگی امنیت فضای مجازی سازمان در منطقه تشخیص رویداد، از طریق پایش دارک‌نت[1]، تحقیق، از طریق ردیابی پیشینه[2] و پاسخ، از طریق عملیات گودال قابل استفاده است شرح می‌دهد.

۱۲-۷ دیگر کنترل‌ها

دیگر کنترل‌ها ممکن است شامل کنترل‌های مربوط به هشدار و قرنطینه افزاره‌هایی که در فعالیت‌های مشکوک شرکت دارند که از طریق مشاهده ارتباط رویدادها از ارائه‌دهنده خدمات و/یا عناصر سازمانی از قبیل کارسازهای DNS، مسیریاب جریان شبکه، پالایش پیام خروجی و ارتباطات همکار به همکار به‌دست می‌آید.

۱۳ چارچوب اشتراک‌گذاری اطلاعات و هماهنگی

۱۳-۱ عمومی

رخدادهای امنیت فضای مجازی اغلب از مرزهای جغرافیایی ملی و سازمانی عبور می‌کند و سرعت جریان اطلاعات و تغییرات رخداد فاش شده اغلب فرصت محدودی برای واکنش افراد و کنش سازمان‌ها ایجاد می‌کند. سامانه لزوماً برای اشتراک‌گذاری اطلاعات و ایجاد هماهنگی برای کمک به آمادگی و واکنش به رویدادها و رخدادهای امنیت فضای مجازی مستقر می‌شود. این عمل گام مهمی در به‌انجام رساندن کنترل‌های امنیت فضای مجازی سازمان‌ها است که باید برداشته شود. توصیه می‌شود چنین سامانه‌ای برای به اشتراک‌گذاری اطلاعات و هماهنگی امن، مؤثر، قابل‌اعتماد و کارآمد باشد.

توصیه می‌شود سامانه امن باشد و تضمین شود که اطلاعات مشترک، از جمله جزئیات هماهنگی فعالیت‌ها، در مقابل دسترسی‌های غیرمجاز محافظت شود، مخصوصاً توسط مجرم رخداد، در نظر گرفته شود. امنیت اطلاعات مربوط به رویداد امنیت فضای مجازی نیز لازم است تا از سوءتعبیر و موجبات وحشت بی‌مورد یا هشدار به عموم مردم جلوگیری به عمل آورد.

درعین‌حال، یکپارچگی و اصالت‌سنجی اطلاعات برای اطمینان از صحت و صرف‌نظر از قابلیت اعتماد، مهم است تا مشخص شود آیا چنین اطلاعاتی در گروه بسته به اشتراک گذارده شده است، یا به‌صورت عمومی افشا شده

1 -Darknet

2- Traceback

است. توصیه می‌شود سامانه موثر و کارآمد باشد در این صورت با حداقل منابع و در زمان و فضای مورد نیاز به هدف خدمت خود می‌رسد.

این بند یک چارچوب پایه‌ای برای پیاده‌سازی سامانه و برای به اشتراک‌گذاری اطلاعات و هماهنگی فراهم می‌کند. چارچوب شامل چهار حوزه برای بررسی است، که عبارت‌اند از خط مشی‌ها، روش‌ها و فرآیندها، مردم و عناصر فنی.

یادآوری- گروه مطالعاتی ITU-T 17 در حال انجام کار گسترده در امنیت فضای مجازی تبادل اطلاعات است. برای کسب اطلاعات بیشتر، به جدول پ-۱۷ مراجعه شود- تبادل اطلاعات امنیت فضای مجازی.

۱۳-۲ خطمشی‌ها

۱۳-۲-۱ سازمان‌های ارائه‌دهنده اطلاعات و سازمان‌های دریافت‌کننده اطلاعات

به‌عنوان هدف این چارچوب، دو نوع از اشتراک‌گذاری اطلاعات سازمان به شرح زیر معرفی می‌شوند:

- IPO و
- IRO.

همان طور که IPO، خط مشی‌های پایه‌ای را با توجه به دسته‌بندی و طبقه‌بندی اطلاعات، توصیه می‌شود شدت رویدادها و رخدادها و شکل ممکن به اشتراک‌گذاری را قبل از وقوع هرگونه رخداد امنیت فضای مجازی، یا در صورت اشتراک (در صورت تبدیل IPO به IRO برای به اشتراک گذاشتن اطلاعات دریافت شده با دیگر هستارهای مجاز در زنجیره اطلاعات) تعیین کرد.

در پایان دریافت، IRO باید موافقت خود را برای اجرای حفاظت از امنیت و روش‌های مربوطه پس از دریافت اطلاعات از IPO اعلام کند، مطابق با توافقی که اخیراً به آن دست یافته است دسته‌بندی و طبقه‌بندی اطلاعات مربوط اساس این کار است.

۱۳-۲-۲ طبقه‌بندی و دسته‌بندی اطلاعات

IPO باید دسته‌های مختلف اطلاعاتی را که جمع‌آوری، تلفیق، نگهداری امن و توزیع می‌کنند تعیین کنند.

نمونه‌هایی از دسته‌بندی اطلاعات می‌تواند شامل رویدادهای امنیتی، تهدیدات امنیتی، آسیب‌پذیری‌های امنیتی، مشخصات نمایه متخلفین مشکوک/تأییدشده، گروه‌های سازمان‌یافته، اطلاعات قربانیان و دسته‌بندی مشخصات نمایه‌ی فناوری اطلاعات و ارتباطات سامانه باشد.

توصیه می‌شود هر دسته، بر اساس محتوای اطلاعات مربوطه به دو یا چندطبقه شکسته شود.

کمینه طبقه‌بندی ممکن است حساس و نامحدود باشد. اگر اطلاعات شامل اطلاعات شخصی باشد، طبقه‌بندی حریم خصوصی نیز ممکن است.

۱۳-۲-۳ کمینه کردن اطلاعات

برای هر دسته و طبقه‌بندی، IPO باید برای کمینه کردن اطلاعات توزیع‌شده احتیاط کند. برای جلوگیری از اضافه‌بار اطلاعات در پایان دریافت کمینه کردن بایسته است تا از استفاده موثر از سامانه‌های اشتراک‌گذاری، بدون تخریب کارایی اطمینان حاصل شود. یکی دیگر از اهداف کمینه کردن حذف اطلاعات حساس برای حفظ حریم خصوصی مردم در سازمان ارائه‌دهنده اطلاعات و IPO است. در این رابطه، IPO و IRO باید سطح مورد نظر از جزئیات را، هر جا که ممکن است برای هر دسته و طبقه‌بندی از اطلاعات که می‌تواند قبل از اشتراک-گذاری واقعی شناسایی شود، تعیین کنند.

۱۳-۲-۴ مخاطبان محدود

هم‌راستا با اصل کمینه کردن، خطمشی محدود کردن مخاطبان که ممکن است تماس با فرد خاص، گروه، یا سازمان باشد، هنگام اشتراک‌گذاری اطلاعات شامل اطلاعات خصوصی یا محرمانه توزیع لازم است. توصیه می-شود برای اطلاعات با حساسیت کمتر، چنین خطمشی‌ای برای جلوگیری از اضافه‌بار اطلاعات در نظر گرفته شود، مگر اینکه مزایای حداکثر توزیع (مانند اشتراک‌گذاری هشدارهای امنیتی حیاتی) بیشتر از تأثیر اضافه‌بار اطلاعات بر روی IRO باشد.

۱۳-۲-۵ پروتکل هماهنگی

توصیه می‌شود خطمشی سطح بالا برای هماهنگی درخواست و توزیع (آیا IPO یا IRO آن را آغاز کرده است) تأسیس شود. چنین خط‌مشی‌ای پروتکل‌های درگیر را رسمی می‌کند که وسیله‌ای برای سازمان ارائه‌دهنده اطلاعات و سازمان دریافت‌کننده اطلاعات برای پاسخ موثر و کارآمد فراهم می‌کند.

رویه‌های اصالت‌سنجی و تأییدهویت متقابل پس از آن می‌تواند بر فراز چنین پروتکلی ساخته شود مخصوصاً، برای اطلاعات حساس، شخصی و/یا محرمانه تا از اصالت‌سنجی مبدأ و اثبات تحویلی که مورد نظر است اطمینان حاصل کند.

۱۳-۳ روش‌ها و فرآیندها

۱۳-۳-۱ مرور کلی

توصیه می‌شود برای اجرای خطمشی‌های اشتراک‌گذاری اطلاعات و حصول اطمینان از سازگاری شیوه، اثربخشی، کارایی و قابلیت اطمینان اجرا، روش‌های مرتبط و فرآیندهای مرتبط توسعه یابند و اجرا شوند. توصیه می‌شود چنین روش‌ها و فرآیندهایی بر مبنای استانداردهای موجود بنیان گذاشته شوند. در غیر این صورت، پس از اعتبارسنجی عملیاتی، ممکن است برای استانداردسازی رسمی شوند. بندهای زیر در مورد روش‌ها و فرآیندها راهنمایی ارائه می‌دهد که معمولاً توسط سازمان‌ها برای دستیابی به اهداف و خطمشی‌های مربوطه و اشتراک-گذاری اطلاعات و هماهنگی در زمینه امنیت فضای مجازی در صنعت استفاده می‌شوند.

۱۳-۳-۲ طبقه‌بندی و دسته‌بندی اطلاعات

اطلاعاتی که باید به اشتراک گذاشته شود از دو منبع باز و بسته می‌آید. اطلاعات منبع باز اغلب بر روی اینترنت یا سایر منابع عمومی، از جمله روزنامه‌ها موجود است. اطلاعات منبع باز به طور کلی در پایین‌ترین دسته‌بندی است، زیرا بنیان‌گذار اطلاعات می‌تواند متعدد یا ناشناخته باشد و سن اطلاعات ممکن است نامشخص باشد و موضوع صحت مورد پرسش باشد.

اطلاعات با منبع بسته در دسترس عموم نیست، اغلب مربوط به یک منبع و سن شناخته شده است. نمونه‌هایی از اطلاعات با منبع بسته تحقیقات و تحلیل اختصاصی یا هوش تجربی جمع‌آوری شده است.

یادآوری- راهنمایی برای این بند ممکن است در نتیجه‌ی دوره مطالعه (SP)[1] در مورد این موضوع بنیاد نهاده شده باشد، اگر SP به رشد و توسعه اقدام کند به استاندارد ارجاع داده می‌شود، یا اگر بدون توسعه بیشتر خاتمه یابد خلاصه‌ای از متن SP اتخاذ می‌شود.

۱۳-۳-۳ توافق عدم افشا[2]

توافقنامه عدم افشا (NDA) ممکن است برای حداقل دو هدف در زمینه اشتراک‌گذاری اطلاعات و هماهنگی برای بهبود امنیت فضای مجازی استفاده شود. استفاده معمولی از یک NDA، برای اطمینان از رسیدگی مناسب و حفاظت از اطلاعات حساس، شخصی و/یا محرمانه است که میان IPO و IRO، به اشتراک گذاشته است و پیش‌استقرار[3] از شرایط اشتراک‌گذاری و توزیع بیشتر و استفاده از چنین اطلاعاتی را عرضه می‌کند. در زمینه‌ی پاسخگویی به رویدادهای امنیت فضای مجازی، پیش‌استقرار NDA، اشتراک‌گذاری سریع و توزیع‌شده میان هستارهای مجاز برای رخداد موثر قادر می‌سازد و البته این کار حتی اگر دسته‌بندی اطلاعات به وضوح تعریف نشده باشد انجام می‌شود.

۱۳-۳-۴ کد عملی

معمولاً روش مورد استفاده برای تضمین اشتراک‌گذاری مناسب و رسیدگی به اطلاعات حساس، استقرار کد عملی است که روش‌های دقیق، مسئولیت‌ها و تعهدات ذی‌نفعان سازمان را (به‌عنوان مثال، IPO و IRO) برای واکنش و اقداماتی که توسط هستارهای مربوطه و برای هر دسته و طبقه‌بندی از اطلاعات اتخاذ می‌شود پوشش می‌دهد.

مثال: استاندارد ISO/IEC 29147 را مشاهده کنید، فناوری اطلاعات - فنون امنیتی - افشای آسیب‌پذیری.

۱۳-۳-۵ آزمون و تعلیم

توصیه می‌شود برای اطمینان از اثربخشی و قابلیت اطمینان و برای رسیدن به سطح مورد نظر بهره‌وری، روش‌ها و فرآیندها برای انجام آزمون و هدایت منظم و بکار انداختن فرانامه‌های تعلیم توسعه یابند. توصیه می‌شود

1- Study Period
2- Non-disclosure Agreement
3- Pre-establishing

به‌منظور جا کردن و مطابقت با اهداف و نیازهای سازمان، روشگان استانداردی به‌عنوان مرجع برای آزمون امنیت استفاده شود.

آزمون‌های امنیتی را می‌توان روی دارایی‌های با مخاطره بالا انجام داد. این روش با کمک و کاربرد دسته‌بندی داده‌های سازمان نام‌گذاری می‌شود. توصیه می‌شود ارزیابی امنیت به طور منظم و بر پایه موارد زیر انجام داد:

- برنامه کاربردی
- سامانه عامل
- سامانه مدیریت دادگان

۱۳-۳-۶ زمان‌بندی و برنامه‌ریزی اشتراک اطلاعات

نیاز اشتراک گذاری اطلاعات به‌صورت فعالانه یا در پاسخ به رخداد از هستاری به هستار دیگر متفاوت خواهد بود. برخی از سازمان‌ها به اطلاعات بلادرنگ نیاز دارند: لحظه‌ای که هشدار یا علامت خطر رخ می‌دهد اطلاعات بیشتری را برای تحلیل درخواست می‌کنند. هستارهای دیگر برای مدیریت اشتراک‌گذاری اطلاعات بلادرنگ، منابع در اختیار ندارند.

در واقع، بسیاری از سازمان‌ها ممکن است توانایی مدیریت اشتراک‌گذاری اطلاعات زمان‌بندی را در هر بازه زمانی نداشته باشند. توصیه می‌شود زمان‌بندی و برنامه‌ریزی اشتراک‌گذاری اطلاعات، با اهداف سطح خدمات خاص برای روابط داوطلبانه و موافقت‌نامه سطح خدمات برای روابط تجاری، به وضوح تعریف شود.

۱۳-۴ افراد و سازمان‌ها

۱۳-۴-۱ مرور کلی

مردم و سازمان‌ها عوامل کلیدی تعیین‌کننده برای موفقیت امنیت فضای مجازی هستند. مردم به افراد درگیر در اجرای روش‌ها و فرآیندها برای اشتراک‌گذاری اطلاعات و هماهنگی برای ایجاد یک اختلاف مثبت به نتایج رویدادهای امنیت فضای مجازی ارجاع می‌دهند. سازمان‌ها به گروهی از مردم درون شرکت ترجیح می‌دهند تا اینکه کل شرکت در چنین فعالیتی درگیر باشند. برای اثربخشی و کارایی، نیازهای مردم و سازمان‌ها باید در نظر گرفته شود.

۱۳-۴-۲ اطلاعات تماس

توصیه می‌شود فهرستی از مخاطبین توسط IPO و IRO جمع‌آوری شده و متقابلاً تبادل شود به‌طوری که در انجمن اشتراک‌گذاری هر یک از هستارها بتوانند شخصی که اطلاعات را درخواست یا ارسال کرده شناسایی کنند. فهرست تماس‌ها با دانه‌بندی[1] ریزتر نیز مطابق با مخاطبان محدود (بند ۱۳-۲-۴) و خطمشی‌های طبقه-بندی و دسته‌بندی اطلاعات (بند ۱۳-۲-۲)، ممکن است توسعه داده و به اشتراک گذاشته شوند.

فهرست تماس باید شامل اطلاعات حساس شخصی، مطابق با خطمشی کمینه کردن اطلاعات (بند ۱۳-۲-۳) باشد. برای مقاصد حفظ حریم خصوصی، نام مستعار نیز ممکن است به‌جای نام و نام خانوادگی در نظر گرفته

1- Granular

شود. حداقل اطلاعات برای فهرست تماس باید شامل نام (یا نام مستعار)، شماره تماس (تلفن همراه در صورت امکان) و نشانی ایمیل باشد. شماره تماس جایگزین نیز ممکن است برای هر فرد کلیدی در فهرست تماس محرز شود. بعلاوه، برای یک فهرست تماس برای اشتراک‌گذاری اطلاعات و ایجاد هماهنگی، برای تسهیل افزایش سریع فهرست تماس جداگانه برای تشدید رخداد نیز ممکن است گردآوری شود.

چنین فهرستی معمولاً شامل مخاطبین خارجی که در شبکه‌ی اشتراکی وجود ندارند است. برای مثال، به پیوست ب مراجعه کنید.

توصیه می‌شود حداقل فهرست تماس در برابر تغییرات غیرمجاز محافظت تا از خرابی جلوگیری شود و یکپارچگی حفظ گردد. توصیه می‌شود کنترل فنی‌های (بند ۱۳-۵) به شکل مناسبی بکار گرفته شود.

۱۳-۴-۳ پیوستگی [1]

به‌منظور تسهیل اشتراک‌گذاری اطلاعات و استقرار شیوه‌های متداول و سازگار توسط یک کد مورد پذیرش شیوه و/یا NDA، سازمان‌ها و گروه افراد ممکن است بر اساس مناطق مورد علاقه خود پیوستگی ایجاد کنند که ممکن است صنعت، فناوری، یا دیگر عرصه‌های مورد علاقه باشد. به پیوست ب برای یک فهرست نمونه از اتحادهای موجود و سازمان‌های غیرانتفاعی که در خدمت چنین هدفی است توجه نمایید.

۱۳-۴-۴ آگاهی و آموزش

توصیه می‌شود در سازمان‌ها افراد را از پدیداری مخاطرات امنیت فضای مجازی جدید آگاه ساخت تا بتوانند مهارت‌ها و تخصص‌های مورد نیاز برای واکنش موثر و کارآمد را برای زمانی که با مخاطره خاص روبرو می‌شوند، یا اطلاعات دریافتی نیازمند اقدامات آنها برای کاهش یا بهبود یک موقعیت خاص است توسعه دهند.

برای رسیدن به این اهداف،

- توصیه می‌شود جلسات منظم در مورد وضعیت مخاطره امنیت فضای مجازی برقرار شود و یافته‌های مربوط به سازمان و صنعت ارائه شود.
- توصیه می‌شود نشست متمرکز آموزش فرانامه‌های شبیه‌سازی شده حمله مجازی که در رأس کار هستند و کارگاه‌های آموزشی به تازه‌واردهای به گروه/سازمان با به‌روزرسانی‌های منظم، در حوزه‌های خاص مورد نیاز طراحی، سازمان‌دهی و تحویل داده می‌شد.
- آزمون منظم، همراه با گردش فرانامه‌های مرتبط، برای حصول اطمینان از درک جامع و توانایی برای اجرای روش‌ها و ابزار خاص.

این آگاهی، آموزش و آزمون ممکن است توسط کارشناسان داخلی، مشاوران خارجی[2]، یا دیگر کارشناسان اعضای اتحاد مرتبط که در اشتراک‌گذاری اطلاعات و تلاش‌های هماهنگی درگیر هستند انجام شود.

استفاده از فرانامه‌ها به‌عنوان بخشی از مراحل آموزش و آزمون به شدت توصیه می‌شود در نتیجه چنین رویکردی افراد را قادر می‌سازد تا تجربه نزدیکی به زندگی واقعی از شرایط مربوطه به‌دست آورند و واکنش‌های

1- Alliance
2- External Vonsultant

مورد نیاز را یاد بگیرند و تمرین کنند. علاوه بر این، رخدادهای گذشته ممکن است به‌عنوان فرانامه‌ها برای به حداکثر رساندن اشتراک‌گذاری مفاهیم آموخته‌شده و درک به‌دست آمده از این موقعیت‌ها استفاده شود.

۱۳-۵ فنی[1]

۱۳-۵-۱ مرور کلی

کنترل‌های فنی و استانداردشده ممکن است برای بهبود بهره‌وری، کاهش خطای انسانی و افزایش امنیت درگیر در اشتراک‌گذاری اطلاعات و فرآیندهای هماهنگی مورد استفاده قرار گیرند. تعدادی از سامانه‌های فنی و راه-حل‌ها ممکن است طراحی، توسعه و اجرا شوند. این استاندارد ملی ایران برخی از رویکردها و روش‌هایی که به طور معمول استفاده می‌شود را که توسط برخی از سازمان‌ها پذیرفته شده است، فراهم می‌کند و بیشتر ممکن است برای بهبود اشتراک‌گذاری اطلاعات و نیازهای هماهنگی و فرآیندهای مقابله با خطر امنیت فضای مجازی در حال تغییر محیط تطبیق داده شود.

۱۳-۵-۲ استانداردسازی داده‌ها برای سامانه‌های خودکار

به‌عنوان بخشی از شبکه اشتراک‌گذاری، سامانه‌های خودکار ممکن است میان سازمان‌های هماهنگ برای جمع-آوری داده‌ها بر رویدادهای امنیت فضای مجازی نتیجه شده، برای تحلیل بلادرنگ و برون‌خطی[2] و ارزیابی توسعه یابند و مستقر شوند تا آخرین وضعیت امنیتی در فضای مجازی درون مرز سازمان‌های درگیر را بررسی کنند. این داده‌ها ممکن است شامل اطلاعات ترافیک شبکه، به‌روزرسانی امنیتی برای سامانه‌های نرم‌افزاری و افزاره-های سخت‌افزاری، آسیب‌پذیری‌های امنیتی داده‌ها و بدافزارها، نامه الکترونیکی ناشناس، داده‌های نرم‌افزارهای جاسوس‌افزار، باشند که شامل حداکثر بار اطلاعات جدا[3] شده است. سامانه‌های خودمختار همان طور که در بند ۱۳-۴-۲ توضیح داده شد، از اولین واکنش‌دهندگان و تشدید رخداد حمایت می‌کنند، همچنین شامل اطلاعات مربوط به سازمان‌ها و مردم است. از دیدگاه حساسیت و حجم محتویات داده‌های درگیر در این سامانه‌ها، سازمان‌ها (به طور خاص، اتحاد سازمان‌ها) باید طرح‌واره داده‌ها و محتویات را برای تعیین کنترل‌های فنی مناسب برای بهبود بهره‌وری، اثربخشی و امنیت ارزیابی کند. می‌تواند شامل، اما نه محدود به موارد زیر باشد:

الف- استانداردسازی طرح‌واره داده برای هر دسته‌بندی و طبقه‌بندی داده‌های جمع‌آوری شده، اجرای کمینه-سازی اطلاعات و خط‌مشی‌های حفظ حریم خصوصی و ارائه تضمین‌های فنی به تمام هستارهای شرکت‌کننده و صاحبان داده‌های چنین شیوه‌ای؛

ب- استانداردسازی قالب داده‌ها برای سهولت و اشتراک‌گذاری و بهبود ذخیره‌سازی، انتقال، رسیدگی و قابلیت همکاری بین سامانه‌ها. برای مثال، به ITU-T X.1205 نگاه کنید؛ و

پ- استانداردسازی قابلیت پردازش داده‌های پایه و الگوریتم‌های مورد استفاده، برای مثال، تابع درهم‌سازی برای گمنام‌سازی نشانی IP و سایر موارد مورد نیاز پیش از پردازش.

1- Technical
2- Offline
3- Intercept

۱۳-۵-۳ مصورسازی داده‌ها[1]

استفاده از روش‌های مصورسازی داده‌ها را برای ارائه اطلاعات رویدادها در نظر گرفته شود که برای بهبود قابلیت رویت تغییرات و وقوع رخداد امنیت پدیدار شده کمک می‌کند. این عمل نیازمند به خواندن جزئیات هر رویداد که پدیدار می‌شود توسط کارورها نیست.

برای مثال، پیوست الف، یک نمایش تصویری از فعالیت‌های دارک‌نت را ارائه می‌دهد که واکنش کارآمد به تغییرات را تسهیل می‌بخشد.

۱۳-۵-۴ تبادل کلید رمزنگاری و پشتیبان‌گیری از نرم‌افزار/سخت‌افزار

به‌منظور تسهیل اشتراک‌گذاری اطلاعات محرمانه، سامانه رمزنگاری، شامل سامانه‌ای برای تبادل کلید که می‌تواند به‌سرعت مستقر شود، توصیه می‌شود برای پیاده‌سازی مورد توجه قرار گیرد. سامانه باید شامل پشتیبان‌گیری کافی برای نرم‌افزار و سخت‌افزار باشد و همچنین شامل کلیدهای مورد استفاده در آماده‌سازی برای اشتراک‌گذاری اهداف و نیازهای بازیابی اضطراری باشد.

۱۳-۵-۵ اشتراک‌گذاری امن پرونده، پیام‌های فوری، درگاه وب و انجمن گفتگو

برای تسهیل تعامل برخط و اشتراک‌گذاری سریع و امن اطلاعات که ممکن است شامل اشتراک‌گذاری محتویات رقمی مانند متن و پرونده‌های چندرسانه‌ای و هر دو بحث‌های برخط و برون‌خط باشد، سازمان‌های اشتراک‌گذاری (IPO و IRO) باید اتخاذ ابزار مناسب اشتراک‌گذاری پرونده، پیام‌رسان فوری[2] و ابزار انجمن بحث برخط را در نظر داشته باشد که می‌تواند امنیت، اثربخشی، بهره‌وری و نیازهای قابلیت اطمینان را تأمین کند.

توصیه می‌شود تدارک تغذیه[3] درگاه وب روی رویدادها و وضعیت امنیت فضای مجازی به‌عنوان شکلی از ارتباط برای جامعه اعم از دولتی و خصوصی علاقه‌مند و درگیر به ترتیب پیاده‌سازی شود. جایی که چنین درگاه وبی استفاده می‌شود، توصیه می‌شود مالکیت اداری و مسئولیت روشن وجود داشته باشد تا از امنیت و در دسترس بودن آن و نواحی خصوصی برای اطلاعات مخاطبین محدود در صورت نیاز اطمینان حاصل شود.

۱۳-۵-۶ سامانه‌های آزمون

توصیه می‌شود درحالی‌که هر سامانه فنی و روش‌ها و فرآیندهای مرتبط به‌دقت مورد آزمایش قرار گیرند تا قابلیت اعتماد و یکپارچگی خود را تضمین کنند، توصیه می‌شود یک یا چند سامانه فنی برای حصول اطمینان از بهبود کارایی و اثربخشی آزمون مخصوصاً، آزمون فرانامه، تخصیص یابد.

چنین سامانه‌ای ممکن است در قالب سامانه‌ی شبیه‌سازی برای محیط‌های عامل که توسط هر سازمان درون فضای مجازی تشخیص داده می‌شود و در حال تکامل وضعیت امنیت فضای مجازی است شبیه‌سازی شود، مشروط بر اینکه قابلیت معرفی زنجیره‌ای از رویدادهای امنیتی برای تسهیل آزمون‌های مورد نیاز انجام شود.

1- Data Visualization
2- Instant Messenger
3- Feed

۱۳-۶ راهنمای پیاده‌سازی

پیاده‌سازی چنین چارچوبی نیازمند همکاری سازمان‌ها و افراد (مجازی یا فیزیکی) همراه با هم است تا خط مشی خاص، کنترل‌ها و مراحلی که به‌منظور دستیابی به اهداف امن، مؤثر، قابل‌اعتماد و کارآمد اشتراک‌گذاری اطلاعات و هماهنگی در واکنش به رخدادهای امنیت فضای مجازی پدیدار شده را تعیین کنند. مراحل سطح بالای زیر به‌عنوان یک راهنمای برای اجرا توصیه می‌شود:

الف- شناسایی و جمع‌آوری سازمان‌ها و افراد مربوطه تا اشتراک‌گذاری اطلاعات مورد نیاز و هماهنگی انجمن شبکه، به‌صورت غیررسمی یا رسمی شکل بگیرد؛

ب- تعیین نقش (های) هر سازمان/فرد به‌عنوان IPO، IRO، یا هر دو (بند ۱۳-۲-۱).

پ- ایجاد نوع اطلاعات و هماهنگی موردنیاز خواهد بود که به نفع انجمن است؛

ت- گروه‌بندی اطلاعات و طبقه‌بندی تا معین شود آیا اطلاعات حساس و/یا حریم خصوصی درگیر هستند (بند ۱۳-۲-۲)؛

ث- ایجاد خط مشی‌ها و اصول حاکم بر انجمن و اطلاعات درگیر (بند ۱۳-۲)؛

ج- تعیین روش‌ها و فرآیندهای مورد نیاز برای هر دسته و طبقه‌بندی اطلاعات مربوط (بند ۱۳-۳)؛

چ- تعیین الزامات و معیارهای عملکرد و ایجاد آیین‌کار[1] و ثبت NDA در صورت لزوم (بند ۱۳-۳-۳ و ۱۳-۳-۴)؛

ح- شناسایی استانداردهای مورد نیاز و مناسب و سامانه‌های فنی برای حمایت از پیاده‌سازی و عملیات انجمن (بند ۱۳-۵)؛

خ- آماد انجام عملیات؛ فهرست تماس تلفیقی؛ و اداره کارگاه‌های هدایت آگاهی و آموزشی برای آماده‌سازی ذی‌نفعان؛

د- انجام آزمون منظم، از جمله فرانامه‌های کاربردی بودن و شبیه‌سازی، در صورت لزوم (بند ۱۳-۳-۵ و ۱۳-۵-۶)؛

ذ- هدایت دوره‌ای، برگزاری بازنگری-های پس آزمون[2]، حادثه پس رخداد[3] برای بهبود اشتراک‌گذاری و هماهنگی سامانه‌ها، شامل مردم، فرآیندها و فناوری درگیر، حجم انجمن را در صورت لزوم گسترش یا کاهش می‌دهد.

یادآوری: استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات - الزامات و استاندارد ملی ایران شماره ۲۷۰۰۳: سال ۱۳۸۹، فناوری اطلاعات - فنون امنیتی - راهنمای اجرای سامانه مدیریت امنیت اطلاعات، به ترتیب راهنمای نیازمندی‌ها و اجرا را ارائه می‌دهد.

1- Code of Practice
2- Post-Test
3- Post-Incident

پیوست الف
(اطلاعاتی)
آمادگی امنیت فضای مجازی

الف-۱ مرور کلی

کنترل‌های امنیت فضای مجازی که در بند ۱۲ توضیح داده شدند، اثر بسیاری از حملات شناخته‌شده به امنیت فضای مجازی، مخاطره و افشاسازی، سازمان‌ها و کاربران نهایی را به حداقل می‌رساند. پس از پیدایش رخدادهای امنیت فضای مجازی، چارچوب اشتراک‌گذاری اطلاعات و هماهنگی‌ای که در بند ۱۱ شرح داده شد یک سامانه اشتراک‌گذاری و هماهنگی اطلاعات برای آمادگی در پاسخگویی به رخدادها و رویداد امنیت فضای مجازی را ایجاد می‌کند. چنین اطلاعاتی به‌قدر کافی بین IPO و IRO ها محافظت می‌شود.

درحالی‌که این کنترل‌ها مخاطره را کاهش می‌دهد و مدیریت رخداد و رسیدگی را بهبود می‌بخشد، مجرمان اینترنتی یا سایر اشرار به توسعه حملات جدید یا تکامل حملات کنونی می‌پردازند تا بر حراست‌های کنونی غلبه کنند. در نتیجه پیاده‌سازی سامانه‌ها و زیرساخت‌ها برای سازمان‌ها مهم است تا یک رویکرد پویاتر و جدی‌تر را برای تشخیص حمله امنیتی، تحقیق و واکنش توانمند سازد.

استاندارد شماره ۲۷۰۳۱، راهنمایی‌هایی در مورد مدیریت سامانه‌ها و فرآیندهای مرتبط برای آماده‌سازی سامانه‌های فناوری اطلاعات و ارتباطات یک سازمان را ارائه می‌دهد تا رویدادهای امنیتی پدیدارشده را شناسایی کند و واکنش نشان دهد، این مسئله شامل رویدادهای امنیت فضای مجازی نیز می‌شود.

این راهنما رویکردهای فنی افزوده که در حوزه تشخیص رویداد برای بهبود آمادگی امنیت فضای مجازی سازمان است را مشخص‌تر می‌کند، برای این کار از پایش دارک‌نت، تحقیق، از طریق ردیابی پیشینه و واکنش، از طریق عملیات فروچاله[1] استفاده می‌شود. سازمان‌ها، در CIIPهای خاص باید نفوذ این رویکردها برای بهبود آمادگی امنیت فضای مجازی و در نتیجه وضعیت را در نظر داشته باشند.

الف-۲ پایش دارک‌نت

الف-۲-۱ مقدمه

اشتراک‌گذاری پرونده‌های دارک‌نت مجموعه‌ای از نشانی‌های IP است که در سازمان مورد استفاده قرار نگرفته است. نشانی IP در دارک‌نت به هر کارساز عملیاتی/سامانه‌های PC واگذار نشده است. با استفاده از بسته‌های پایش در حوزه‌ی دامنه‌های IP مربوط به دارک‌نت، سازمان‌ها می‌توانند حملات شبکه‌ای پدیدار شده را مشاهده کند، این حمله‌ها شامل پویش شبکه که با بدافزار آغاز می‌شود، رفتاری که از آلوده شدن به بدافزار ایجاد می‌شود و پراکندگی به‌عقب DDoS است. ازآنجاکه نشانی IP مربوط به دارک‌نت عمومی است اما به میزبان‌های مشروع اختصاص داده نشده است، تمام ترافیک‌های ورودی متعلق به حوزه‌های IP، دارک‌نت را می‌توان به‌عنوان نتیجه‌ای از هر دو فعالیت‌های مخرب، یا تنظیمات نادرست استنباط کرد.

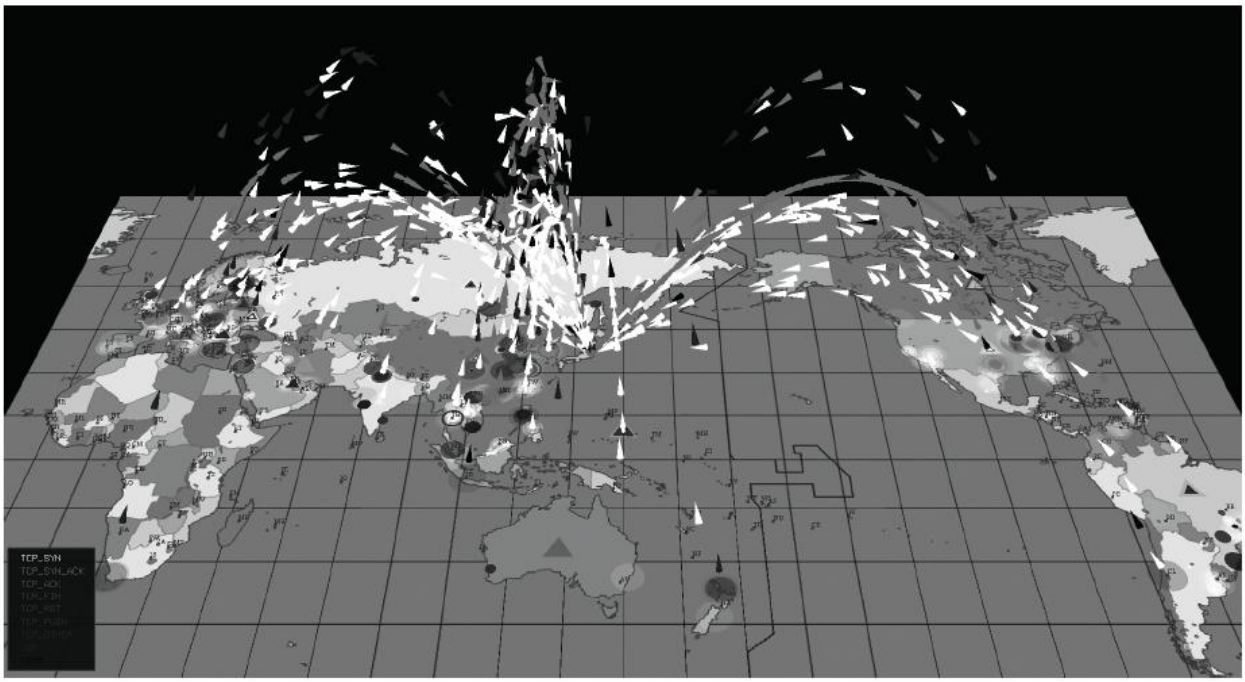
1- Sinkhole

به طور کلی، سه روش در دارک‌نت برای مشاهده فعالیت‌های مخرب مرتبط به ترافیک روی اینترنت وجود دارد، که عبارت‌اند از پایش سیاه‌چاله[1]، پایش تعامل بالا و پایین.

الف-۲-۲ پایش سیاه‌چاله

پایش سیاه‌چاله به سامانه‌های پایش که به هر چیزی در برابر بسته‌های دریافتی در داخل دامنه IP، دارک‌نت پاسخ نمی‌دهند اشاره دارد. این نوع سامانه پایش اغلب برای مشاهده بی‌سروصدای درگاه‌های شبکه با نرم-افزارهای بدخواه و رفتار آلوده‌شده به نرم‌افزار بدخواه (UDP با حداکثر بار شامل کد پوسته[2]) و پراکندگی به‌عقب DDoS، استفاده می‌شوند. پویش درگاه شبکه که اغلب گام اولیه‌ای است که توسط مهاجمان برای جستجوی میزبان آسیب‌پذیر برداشته می‌شود که قابلیت بهره‌کشی دارد. به طور معمول رفتارهای حاکی از آلوده شدن به بدافزار مراحل پس از شناسایی سامانه‌های میزبان آسیب‌پذیر توسط مهاجمان است. چنین اقدامات سرایتی اغلب برای استفاده از UDP با حداکثر بار در پایش سیاه‌چاله مشاهده شده‌اند.

به‌علاوه، پراکندگی به‌عقب DDoS نیز با استفاده از مشاهده پایش سیاه‌چاله انجام می‌شود، در صورت تقلید[3] کردن نشانی IP منبع، (مهاجمان) و هدف DDoS توسط ترافیک پراکندگی به‌عقب قابل‌شناسایی است. شکل الف-۱ صفحه نمایشی را نشان می‌دهد که فعالیت نرم‌افزارهای بدافزار شناسایی‌شده توسط سامانه‌های پایش سیاه‌چاله را مصورسازی می‌کند. در زیر می‌توان پیوند به یک نمونه تصویری را مشاهده کرد:



شکل الف-۱ – نمونه‌ای از مصورسازی از فعالیت‌های بدافزار با استفاده پایش سیاه‌چاله

1- Black Hole Monitoring
2- Shell Code
3- Spoof

«پیکان‌های» بالای نقشه جهان (شکل الف-۱) پیمایش بسته‌های IP از منابع به نقاط هدف را به تصویر می‌کشد. سایه‌های مختلف (رنگ در این ویدئو) نوع بسته را به تصویر می‌کشد (به‌عنوان مثال، TCP SYN، TCP SYN ACK، انواع دیگری از TCP، UDP و ICMP[1]). ارتفاع هر یک از فلش‌ها نسبت به شماره پورت آن است.

الف-۲-۳ پایش با تعامل کم[2]

یک سامانه پایش با تعامل کم، همان سامانه پایش دارک‌نت است که به بسته‌هایIP ، شناسایی‌شده در دارک‌نت پاسخ می‌دهد و این کار را با تلاش به اتصال به سامانه‌های میزبان مشکوک انجام می‌دهد. هدف از ارتباط تلاش انجام‌شده، به‌دست آوردن اطلاعات بیشتر در مورد سامانه‌های میزبان حمله است، در صورت امکان، تلاش می‌شود مسیرهایی که در حمله به شبکه استفاده می‌شود و دیگر اطلاعات مربوط به حمله را به‌دست آورد. سامانه پایش اغلب خود را به‌عنوان یک سامانه با آسیب‌پذیری‌های برطرف نشده پنهان می‌کند تا توجه مهاجمان را به خود جلب کند. همچنین سامانه پایش با تعامل کم برای مشاهده واکنش بیشتر رفتار و فعالیت‌های مخرب مانند اجرای نویسه‌های پوسته پس از پویش اولیه درگاه شبکه استفاده می‌شود.

الف-۲-۴ پایش با تعامل زیاد[3]

سامانه پایش بر تعامل زیاد (همچنین هانی‌پات[4] با تعامل زیاد نامیده می‌شود) نیز یک سامانه پایش دارک‌نت است که به بسته‌هایIP ، شناسایی‌شده در دارک‌نت پاسخ می‌دهد و این کار را با تلاش به اتصال به سامانه‌های میزبان مشکوک انجام می‌دهد و تا جایی که امکان دارد با سامانه‌ها تعامل دارد. هدف از تعامل، به‌دست آوردن اطلاعات بسیار عمیق‌تر از جمله راهبرد بهره‌کشی از آسیب‌پذیری‌ها، نرم‌افزارهای بدخواه قابل‌اجرا که بعد از بهره‌کشی به سامانه تزریق شده است و رفتار نرم‌افزارهای بدخواه آلوده کننده است. سامانه پایش با تعامل زیاد می‌تواند در سامانه‌های واقعی یا مجازی با آسیب‌پذیری‌های برطرف نشده پیاده‌سازی شود در نتیجه توجه مهاجمان را جلب می‌کنند، بهره‌کشی را دریافت می‌کنند و در نهایت نمونه بدافزار تزریق‌شده را تحت تصرف خود در می‌آورد.

الف-۳ عملیات فروچاله

عملیات فروچاله به‌عنوان روشی برای تغییر مسیر ترافیک IP خاص به یک افزاره فروچاله (به‌عنوان مثال، مسیریاب فروچاله)، به هدف تحلیل ترافیک، انحراف حملات و تشخیص رفتارهای غیرعادی در یک شبکه تعریف شده است. برای مثال، اگر عملیات کسب‌وکار سامانه هدف با استفاده از حمله انکار خدمت توزیع‌شده مختل شده باشد، یکی از راه‌حل‌های موثر شروع یک عملیات فروچاله با تزریق یک مسیر جایگزین برای هدف و هدایت ترافیک DDoS در طول مسیر تا به‌جای جریان در مسیر هدف اصلی به این مسیر جایگزین روی آورد.

1- Internet Control Message Protocol
2- Low interaction monitoring
3- High interaction monitoring
4- Honeypot

افزاره فروچاله قادر به جذب، تحلیل و/یا دور ریختن ترافیک DDoS شده است. تغییر مسیر هدف که رو به‌سوی مسیریاب فروچاله دارد معمولاً به‌وسیله یک مسیریاب مرزی BGP[1] منتشر می‌شود. وقتی عملیات فروچاله‌ها مورد حمله قرار می‌گیرد برای ارتباط با سایر کاربران شبکه تا مسیر برداشته نشود، نمی‌تواند مورد استفاده قرار گیرد.

با استفاده از پیکربندی BGP که در RFC 3882 شرح داده شده است. نقطه‌ضعف این روش این است که نشانی IPای که مورد حمله قرار می‌گیرد تا زمانی که مسیر برداشته شود برای برقراری ارتباط با سایر کاربران شبکه نمی‌تواند مورد استفاده قرار گیرد. عملیات فروچاله اغلب برای محافظت در برابر حملات DDoS همان طور که بالا توضیح داده شد استفاده می‌شود.

همچنین برای محافظت در برابر حملات باتنت با هدایت فرمان باتنت و کنترل (C & C) به افزاره فروچاله، مستقر شده‌اند. ازآنجاکه هر بات به‌منظور دریافت دستورالعمل حمله از کنترل‌گر باتنت نیازمند ایجاد ارتباط با کارساز C & C است، ربات‌ها درخواست‌های DNS را برای حل و فصل URL نمایش داده‌شده از کارساز C & C ارسال می‌کنند. سپس کارساز DNS یک نشانی IP افزاره فروچاله را به‌جای ارسال نشانی واقعی IP کارساز C & C به بات‌ها ارسال می‌کند. در نتیجه، کنترل‌کننده باتنت از ارتباط با ربات‌ها محروم می‌شود و بنابراین نمی‌تواند دستورالعمل‌های حمله را به آنها ارسال کند.

الف-۴ ردیابی پیشینه[2]

به‌منظور خودکار کردن یا تسریع نمودن ردیابی دستی، در برابر حملات خرابکارانه مانند حملات انکار خدمت که در آن میزبان منشأ تحریف شده است، بسیاری از روش‌های ردیابی پیشینه خودکار مورد مطالعه قرار گرفته‌اند. روش‌های ردیابی پیشینه به‌عنوان روش‌هایی که مسیر حمله را بازسازی می‌کنند به رسمیت شناخته شده‌اند و گره‌های مهاجم را با تصحیح ترافیک حمله، مسیریابی اطلاعات، بسته‌های نشان‌دار، یا ممیزی ترافیک ورود حمله به سامانه، جایابی می‌کنند.

هیچ روش ردیابی پیشینه که بتواند مسیر حمله در سراسر چندین حوزه شبکه را بازسازی کند، در محیط عملیاتی شبکه واقعی به‌کار گماشته نمی‌شوند و مورد آزمون و تمرین قرار نمی‌گیرند. مشکلات استقرار بین دامنه (در سراسر چندین حوزه شبکه) روش‌های ردیابی پیشینه از مسائل عملیاتی زیر مشتق شده‌اند:

الف- هدف ردیابی پیشینه بین دامنه، تبادل اطلاعات حساس مانند جزئیات هم‌بندی[3] ستون فقرات[4] می‌تواند منجر به مشکلات جدی برای کارورهای شبکه شود.

ب- ازآنجاکه عملیات ردیابی پیشینه می‌تواند از نزدیک به ستون فقرات امنیت شبکه ISP گره خورده باشد، آزمایش‌های دلخواه از تلاش ردیابی پیشینه توسط افراد غیرمجاز برای بیش‌تر ISP ها قابل‌قبول نخواهد بود؛ بنابراین، ترس از استفاده‌نابجا از روش ردیابی پیشینه در هر حوزه شبکه توسط دیگران وجود دارد.

1- Border Gateway Protocol
2- Traceback
3- Topology
4- Backbone

پ- اگر یک روش ردیابی پیشینه تک و خاص میان-دامنه‌ای در سراسر چندین حوزه شبکه اعمال شود، توصیه می‌شود همزمان روش تک و منحصربه‌فرد با شرکت سامانه‌های خودمختار[1] (AS) مستقر می‌شود. علاوه بر این، مهاجمان دیر یا زود حملات فرار را توسعه خواهند داد. در عمل، بسیاری از شرکت‌های ISP ابزارهای چندگانه‌ی تشخیص و ردیابی پیشینه را در شبکه خود به‌کار می‌گمارند. مسائل عملیاتی فوق زمانی به وجود می‌آیند که آزمایشی از تلاش ردیابی پیشینه برای گسترش فراتر از مرزهای شبکه صورت گرفته باشد.

روش‌های ردیابی پیشینه باید مرزهای عملیات شبکه و تفاوت خطمشی‌های عملیاتی میان حوزه‌های مختلف شبکه را در نظر بگیرند. بسیاری به‌صورتی پایدار و محکم بر این باور بودند که ردیابی پیشینه میان‌دامنه‌ای و سازوکارهای کاهش حمله باید در سراسر اینترنت مستقر شود. توصیه می‌شود در توسعه فن‌های ردیابی پیشینه بین دامنه و سامانه در عمل، معماری ردیابی پیشینه به‌صورت زیر در نظر گرفته شود:

الف- برای حفظ مرزهای عملیات شبکه، معماری ردیابی پیشینه باید هر سامانه خودمختار را رها کند تا تصمیم بگیرد که آیا درخواست ردیابی خط مشی عملیاتی سامانه خودمختار را ارث ببرد یا خیر.

ب- معماری ردیابی پیشینه همچنین باید هر AS را رها کند تا تصمیم بگیرد که آیا داخل دامنه شبکه خود را عمیق‌تر بررسی کند یا خیر؛

پ- همچنین معماری باید اجازه دهد تا هر یک از زیر دامنه‌های سامانه خودمختار تصمیم بگیرد که آیا شبکه هر زیر دامنه با خطمشی عملیات آن مورد بررسی قرار گیرد یا خیر. عملیات ردیابی پیشینه بسیاری از منابع مرتبط با AS را مصرف خواهند نمود، بنابراین، معماری ردیابی پیشینه در صورت امکان نباید درخواست‌های بی‌معنی یا سیل‌آسا، تولید کند و بنابراین، معماری ردیابی پیشینه نباید پیام‌های درخواست به AS را که هیچ رابطه‌ای با حمله نصب‌شده ندارند ارسال کند؛

ت- به‌منظور کاهش خسارات ناشی از استفاده‌نابجا، پیام نباید چنین اطلاعات حساسی که ممکن است باعث نشت اسرار یا اعتماد به AS شود منتقل کند، بنابراین، معماری ردیابی پیشینه نباید اطلاعات حساس را از AS به دیگران نشان دهد؛

ث- حتی زمانی که یک استفاده‌نابجا یا اقدام به مخاطره اتفاق بیفتد، قابلیت ردیابی پیام مجرم را شناسایی خواهد کرد، ازاین‌رو، یک پیام رد و بدل شده در معماری باید قابلیت ردیابی خود را به اثبات یا تأیید صادرکنندگان برساند؛

ج- اگر معماری به یک روش ردیابی پیشینه خاص بستگی داشته باشد، مهاجمان حملات گریززنی[2] و پنهان کردن محل گره‌های مهاجم را توسعه خواهند داد. برای غلبه بر حملات گریززنی، معماری ردیابی پیشینه توصیه می‌شود مستقل از روش ردیابی پیشینه خاص باشد؛

چ- بسیاری از سامانه‌های عملیاتی برای حمایت از پشته دوگانه IPv4/IPv6 آمده‌اند و چندین حمله از

1- Autonomous Systems
2- Evasion Attacks

طریق IPv6 در تونل‌زنی[1] to4۶ آمده است. اگر معماری ردیابی پیشینه نتواند حملات در شبکه‌های IPv6 یا حملات از طریق برخی از مترجمان را پیگیری کند، اکثر حملات به حمله‌ای پیچیده تغییر ماهیت می‌دهند؛ بنابراین، معماری ردیابی پیشینه باید یک حمله در یک محیط پشته دوگانه را پیگیری کند، حتی زمانی که این حمله برخی از روش‌های ترجمه نشانی را به‌کار گماشته باشد؛

ح- برای خودکار کردن فرآیند کاهش مخاطرات حمله، توصیه می‌شود معماری قادر به صدور نتایج ناشی از یک آزمون ردیابی پیشینه به‌عنوان راه‌انداز کاهش حمله باشد؛ بنابراین، معماری ردیابی پیشینه باید به هر سامانه خودمختار اجازه دهد تا اقدام دیگری همراه با نتیجه ردیابی مانند یک فیلتر یا ردیابی دیگری را اتخاذ کنند؛

خ- معماری باید توانایی همکاری با سامانه‌های تشخیص یا سامانه‌های حفاظت را داشته باشد.

د- یک مهاجم می‌تواند الگوی ترافیک حمله را برای جلوگیری از اثر چنین اقدامات کاهشی تغییر دهد. مبارزه با تغییرات یک حمله پیچیده، زمان صرف‌شده برای ردیابی یک مسیر حمله باید تا حد ممکن کوتاه باشد؛ بنابراین، توصیه می‌شود معماری انسان‌ها را تا حد امکان حذف کند.

1- Tunnelling

پیوست ب
(اطلاعاتی)
منابع اضافی

ب-۱ امنیت برخط و مراجع ضد جاسوس‌افزار

تعدادی وب‌گاه وجود دارد که برای اطلاعات بیشتر مربوط به ایمنی و امنیت فضای مجازی اینترنت می‌توانند به‌عنوان مرجع معرفی شوند و تأثیرگذار باشند. در ادامه فهرستی غیرجامع از نمونه‌های آن آورده شده است:

- ائتلاف نرم‌افزارهای ضد جاسوس‌افزار[1] (http://www.antispywarecoalition.org/) - گروهی که به بنای یک اجماع در مورد تعاریف و به‌روش در بحث پیرامون نرم‌افزارهای جاسوسی و سایر فناوری‌های بالقوه ناخواسته اختصاص داده شده است. ASC از شرکت‌های نرم‌افزارهای ضد جاسوس‌افزار، دانشگاهیان و گروه-های مصرف‌کننده، جستجوی صعودی برای هم‌آوردن[2] آرایه‌های گوناگون از دیدگاه‌ها برای کنترل مشکل نرم‌افزارهای جاسوس‌افزار و دیگر فناوری‌های بالقوه ناخواسته تشکیل شده است.
- وب‌گاه APWG (http://www.antiphishing.org) - وب‌گاه آموزشی و آگاهی‌رسانی در مورد دزدی هویت است که هر سه ماه یک‌بار گزارش‌های معتبر[3] به‌روز در مورد روند حملات، توزیع، تأثیر و اخبار تهیه می-کند.
- وب‌آگاه بودن[4] (http://www.bewebaware.ca) - برنامه ملی دو زبانه آموزش عمومی در مورد طراحی ایمن اینترنت برای اطمینان از بهره‌مندی جوان کانادایی از اینترنت، درحالی‌که این استفاده امن بوده و آنها مسئول فعالیت‌های برخط خود هستند.
- مرکز امن و مسئول استفاده از اینترنت[5] (http://csriu.org) – سازمانی که خدمات توسعه‌ی پرداختن به مسائل استفاده ایمن و مسئول از اینترنت را ارائه می‌دهد.
- شبکه بین‌المللی کودک[6] (http://www.childnet-int.org) - سازمان غیرانتفاعی است که در مشارکت با دیگران در سراسر جهان برای کمک به ایجاد اینترنت به‌عنوان مکانی امن برای کودکان است.
- وب‌گاه ECPAT (http://www.ecpat.net) – شبکه‌ای از سازمان‌ها و افراد که با یکدیگر برای از بین بردن بهره‌کشی جنسی تجاری از کودکان همکاری می‌کنند.
- وب‌گاه GetNetWise (http://www.getnetwise.org) - خدمات عمومی که توسط ائتلاف شرکت‌های بزرگ صنعت اینترنت و سازمان‌های منافع عمومی ارائه می‌شود که می‌خواهند کاربران فقط به‌اندازه «یک

1- Anti-Spyware Coalition
2- Bring Together
3- White-Paper
4- Be Web Aware
5- Centre for Safe and Responsible Internet Use
6- Childnet International

کلیک» از منابع مورد نیاز برای تصمیم‌گیری آگاهانه در مورد استفاده خود و خانواده‌شان از اینترنت فاصله داشته باشند.

- زیرساخت اتحاد جهانی برای ایمنی اینترنت (GIAIS) (http://www.microsoft.com/security/msra/default.mspx)- اتحاد برخی از ارائه‌دهندگان خدمات که برای بهبود امنیت و ایمنی در وب، مدیریت مداوم تهدید در سراسر طیف گسترده و شناسایی و کاهش آسیب‌پذیری های موجود سازمان‌دهی شده‌اند.
- وب‌گاه INHOPE (http://inhope.org) - انجمن بین‌المللی است که از خطوط تماس ویژه‌ی اینترنت در پاسخ به هدف آنها برای ارائه گزارش مربوط به محتوای غیرقانونی پشتیبانی می‌کند تا اینترنت را امن‌تر سازد.
- گروه ایمنی اینترنت[1] (www.netsafe.org.nz) – وب‌گاه NetSafe، محل برخط گروه ایمنی اینترنت نیوزیلند (ISG) است و بر محافظت تسلط دارد.
- پلیس بین‌الملل[2] (http://www.interpol.int) - سازمان پلیس بین‌الملل است که همکاری پلیس مرزی را تسهیل می‌بخشد و همه سازمان‌ها، مراجع و خدماتی را که مأموریت آن‌ها جلوگیری یا مبارزه با جرم و جنایت بین‌المللی است، پشتیبانی و کمک می‌کند.
- وب‌گاه iSafe (http://www.isafe.org) - رهبر جهانی در آموزش ایمنی اینترنت؛ که برنامه آموزشی و کلاس درس را با توسعه جامعه پویا ترکیب نموده و دانش‌آموزان، معلمان، والدین، مجری قانون و بزرگسالان مضطرب را توانمند می‌کند تا اینترنت را به مکان امنی تبدیل کند.
- وب‌گاه ISECOM (http://www.isecom.org) -روشگان‌های رایگان، منبع باز[3] در مورد امنیت حرفه‌ای آزمون (ارزیابی آسیب‌پذیری، آزمون نفوذ، رخنه اخلاقی)، ارزیابی مخاطرات فنی (RAVها و غیره). ISECOM، OSSTMM (کتابچه راهنمای منبع باز آزمون روشگان) را اجرا می‌کند که استاندارد جهانی عملی برای اجرای امنیت فناوری اطلاعات/فناوری اطلاعات و ارتباطات است (http://www.osstmm.org).
- وب‌گاه COP (http://www.itu.int/cop) – حفاظت برخط کودکان (COP)[4] پروژه خاص که توسط ITU (اتحادیه بین‌المللی مخابرات) و دیگر مؤسسات تخصصی/شرکت‌ها انجام شده است و راهنمایی‌های امنیتی برای والدین، سرپرستان و مربیان، صنعت و سیاست‌گذاران ارائه می‌دهد.
- امنیت مایکروسافت در خانه (http://www.microsoft.com/protectها) - اطلاعات و منابع برای کمک به حفاظت مردم از رایانه‌ها، خود، خانواده‌های آن‌ها.
- موسسه ملی فناوری‌های ارتباطات[5]، (http://www.inteco.es، http://certinteco.es، http://www.osi.es، http://observatorio.inteco.es) - خدمات عمومی رایگان که توسط ادارات دولتی اسپانیا برای ترویج

1- Internet Safety Group
2- Interpol
3- FDL
4- Children Online Protection
5- INTECO

اعتماد و امنیت در اینترنت برای شهروندان، SMEها، کاردان‌ها، کودکان و غیره، از طریق گروه پاسخ‌دهنده پدیداری رایانه[1]، مرکز امنیت برای شهروندان[2] و رصدخانه امنیت اطلاعات ارائه‌شده است.

- اخطار شبکه محدودشده[3] (http://www.netalert.net.au) - سازمان اجتماعی غیرانتفاعی که توسط دولت استرالیا برای ارائه مشاوره و آموزش و پرورش مستقل در مدیریت دسترسی به محتوای برخط ایجاد شده است.
- وب‌گاهNetSmartzKids (http://www.netsmartzkids.org) ، NetSmartz، منبع ایمنی آموزشی تعاملی از مرکز ملی کودکان گمشده و مورد بهره‌کشی[4] شده و پسران و دختران باشگاه آمریکا[5] برای کودکان ۵ تا ۱۷ ساله، سرپرستان، مربیان و مجری قانون است که با استفاده از فعالیت‌های متناسب با سن و آموزش با فعالیت‌های ۳ بعدی به کودکان، به آنها می‌آموزد چگونه در اینترنت امن‌تر باقی بمانند.
- وب‌گاه Saferinternet.be(www.saferinternet.be) - این وب‌گاه اطلاعات مفیدی در مورد مخاطرات عمده و محتوای مضر برای افراد زیر سن قانونی برخط یا در زمینه فناوری اطلاعات و ارتباطات (و همچنین از طریق شبکه‌های تلفن همراه و غیره) که ممکن است با آنها مواجه شوند را پیشنهاد می‌دهد، این موارد شامل، روابط نامشروع کودکان، نژادپرستی و تبعیض، فرقه‌ها[6]، کلاه‌برداری‌ها[7] و شیوه‌ی بازرگانی نامشروع و در نهایت مخاطرات فنی. همچنین وب‌گاهی که راهبردهایی برای مقابله درست با این مخاطرات را ارائه می‌دهد، متشکل از چندین بخش است که مرکز هدف گروه‌های مختلف است. در میان چیزهای دیگر پرونده‌های آموزشی و فنی را برای مربیان (والدین و معلمان)، بازی‌های کودکان (۶ تا ۱۲ ساله) و یک وب‌گاه کاملاً جداگانه (web4me.be) برای نوجوانان فراهم می‌کند.
- وب‌گاه SafeKids.com(http://www.safekids.com) - منابعی برای کمک به خانواده‌ها تا اینترنت و فناوری را سرگرم‌کننده، امن و پربار کنند.
- صندوق حمایت از کودکان ملل متحد[8] (http://www.unicef.org) - مدافع جهانی، که به حفاظت از حقوق کودکان اختصاص داده شده است و در درازمدت به ارائه کمک‌های بشردوستانه و توسعه‌گرا به کودکان و والدین در کشورهای در حال توسعه می‌پردازد.
- وب‌گاه WebSafe Crackerz در (http://www.websafecrackerz.com) – بازی‌های تعاملی و چیستان، که برای کمک به نوجوانان طراحی شده است و برای برخورد با موقعیت‌های مختلف برخط از جمله نامه الکترونیکی ناشناس، دزدی هویت و کلاه‌برداری راهبردهایی را ارائه می‌دهد.

ب-۲ نمونه فهرستی از تماس‌های تشدید رخداد

1- INTECO-CERT
2- OSI
3- NetAlert Limited
4- NCMEC (National Centre for Missing and Exploited Children)
5- BGCA (Boys and Girls Clubsof America)
6- Sects
7- Swindle
8- UNICEF (The United Nations Children's Fund)

فهرستی غیر جامع از نمونه‌هایی از امنیت اینترنت و تماس‌های تشدید رخداد در جدول ب-۱ زیر ارائه شده است:

جدول ب-۱ نمونه فهرستی از اطلاعات تماس‌های تشدید رخداد

سازمان‌ها	تماس
سامانه‌های شرکت سیسکو	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
شرکت مایکروسافت	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
انجمن گروه واکنش به رخداد وتیم‌های امنیتی (FIRST)	http://www.first.org/about/organization/teams/
گروه‌های ملی مربوطه CERT (به‌عنوان مثال)	
موسسه ملی فناوری‌های ارتباطات، INTECO، اسپانیا	http://cert.inteco.es (انگلیسی:http://cert.inteco.es/cert/INTECOCERT_1/?postAction=getCertHome)
Telecom ISAC ژاپن	https://www.telecom-isac.jp/contact/index.html
(مرکز امنیت اینترنت کره جنوبی)[1]	http://www.krcert.or.kr/index.jsp

1- KrCERT/CC

پیوست پ
(اطلاعاتی)
نمونه‌هایی از اسناد مرتبط

پ-۱ مقدمه

این پیوست فهرستی غیر جامع از نمونه‌هایی از اسنادی را که با توجه به امنیت فضای مجازی ممکن است مفید باشد فراهم می‌کند. هدف آن فهرست کاملی از استانداردهای ملی و گزارش‌های فنی برای امنیت فضای مجازی نیست.

پ-۲ ISO و IEC

مرجع	عنوان
ISO/IEC 27000	فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات - مرور کلی و واژگان
ISO/IEC 27001	فناوری اطلاعات - فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات - الزامات
ISO/IEC 27002	فناوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات
ISO/IEC 27003	فناوری اطلاعات - فنون امنیتی - راهنمای اجرای سامانه مدیریت امنیت اطلاعات
ISO/IEC 27010	فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات برای ارتباطات درون‌بخشی[1]

جدول پ-۲ مدیریت مخاطره

عنوان	مرجع
ISO/IEC 27005	فناوری اطلاعات - فنون امنیتی - مدیریت مخاطرات امنیت اطلاعات
ISO/IEC 16085	سامانه‌ها و مهندسی نرم‌افزار – چرخه حیات فرآیند – مدیریت مخاطره

جدول پ-۳ ارزیابی امنیت فناوری اطلاعات

عنوان	مرجع
ISO/IEC 15408	فناوری اطلاعات-فنون امنیتی-معیار ارزیابی امنیت فناوری اطلاعات-
ISO/IEC 18045	فناوری اطلاعات -فنون امنیتی - روشگان برای ارزشیابی امنیت فناوری اطلاعات(IT)

1- Intersector communic

ISO/IEC TR 19791	فناوری اطلاعات -فنون امنیتی – ارزیابی امنیت سامانه‌های عامل

جدول پ-۴ ضمانت (بیمه) امنیت

عنوان	مرجع
ISO/IEC TR 15443	فناوری اطلاعات-فنون امنیتی-چارچوبی برای ضمانت امنیت فناوری اطلاعات-
ISO/IEC 15026	فناوری اطلاعات -فنون امنیتی – بیمه سامانه‌ها و نرم‌افزار

جدول پ-۵ طراحی و پیاده‌سازی

عنوان	مرجع
ISO/IEC 12207	مهندسی سامانه‌ها و نرم‌افزار-فرآیندهای چرخه حیات نرم‌افزار
ISO/IEC 14764	مهندسی نرم‌افزار- فرآیند چرخه زندگی نرم‌افزار - نگهداری
ISO/IEC 15288	مهندسی سامانه‌ها و نرم‌افزار-فرآیندهای چرخه زندگی سامانه
ISO/IEC 23026	مهندسی نرم‌افزار-شیوه‌ی پیشنهادی برای اینترنت –مهندسی وب‌گاه، مدیریت وب‌گاه و چرخه زندگی وب‌گاه
ISO/IEC 42010	مهندسی نرم‌افزار و سامانه - توصیف معماری

جدول پ-۶ خدمات برون‌سپاری و طرف سوم

عنوان	مرجع
ISO/IEC TR 14516	فناوری اطلاعات -فنون امنیتی-راهنمایی‌هایی برای استفاده و مدیریت خدمات طرف سوم قابل‌اعتماد
ISO/IEC 15945	فناوری اطلاعات -فنون امنیتی-مشخصه خدمات TTP برای پشتیبانی برنامه کاربردی امضای رقمی

جدول پ-۷ امنیت شبکه و برنامه کاربردی

عنوان	مرجع
ISO/IEC 18028	فن‌آوری اطلاعات - فنون امنیتی – امنیت شبکه فناوری اطلاعات
ISO/IEC 18043	فن‌آوری اطلاعات - فنون امنیتی - انتخاب - استقرار و عملیات سامانه‌های تشخیص نفوذ
ISO/IEC 27033	فن‌آوری اطلاعات - فنون امنیتی - امنیت شبکه
ISO/IEC 27034	فن‌آوری اطلاعات - فنون امنیتی –راهنمایی‌هایی برای امنیت برنامه کاربردی

جدول پ-۸ تداوم و رخداد مدیریت

عنوان	مرجع
ISO/IEC TR 18044	فناوری اطلاعات - فنون امنیتی- مدیریت رویداد امنیت اطلاعات
ISO/IEC 24762	فن‌آوری اطلاعات - فنون امنیتی - رهنمودهایی برای خدمات بازیابی از حادثه

	در فن آوری ارتباطات و اطلاعات
ISO/IEC 27031	فناوری اطلاعات -فنون امنیتی -راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به‌منظور تداوم کسب‌وکار
ISO/IEC 27035	فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

جدول پ-۹ مدیریت شناسایی

عنوان	مرجع
ISO/IEC 24760	فناوری اطلاعات - فنون امنیتی- چارچوبی برای مدیریت هویت

جدول پ-۱۰ حریم خصوصی

عنوان	مرجع
ISO/IEC 29100	فناوری اطلاعات - فنون امنیتی- چارچوب حریم خصوصی

جدول پ-۱۱ مدیریت دارایی

عنوان	مرجع
ISO/IEC 19770	فناوری اطلاعات – مدیریت دارایی نرم‌افزار

جدول پ-۱۲ مدیریت خدمات

عنوان	مرجع
ISO/IEC 20000	فناوری اطلاعات – مدیریت خدمات

پ-۳ ITU-T

جدول پ-۱۳ امنیت فضای مجازی

عنوان	مرجع
ITU-T X.1200 – X.1299 Series	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات - امنیت فضای مجازی
ITU-T X.1205	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات- مرور کلی امنیت فضای مجازی

جدول پ-۱۴ مدیریت تداوم و رخداد

عنوان	مرجع
ITU-T X.1206	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات – فروشنده – چارچوب خنثی برای ابلاغ خودکار اطلاعات مرتبط با امنیت و انتشار به‌روزرسانی

جدول پ-۱۵ نرم‌افزار ناخواسته[1]

عنوان	مرجع
ITU-T X.1207	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات – راهنمایی‌هایی خدمات ارتباطات برای اداره مخاطره جاسوس‌افزار و نرم‌افزار ناخواسته بالقوه

جدول پ-۱۶ نامه الکترونیکی ناشناس

عنوان	مرجع
ITU-T X.1231	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات – راهبردهای فنی برای مقابله با نامه‌های الکترونیکی ناشناس
ITU-T X.1240	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات-فناوری‌های شامل مقابله با نامه‌های الکترونیکی ناشناس
ITU-T X.1240	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات-چارچوب فنی برای مقابله با نامه‌های الکترونیکی ناشناس
ITU-T X.1244	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز، امنیت ارتباطات-جنبه‌های کلی مقابله با نامه‌های الکترونیکی ناشناس در برنامه‌های کاربردی چندرسانه‌ای مبتنی بر IP

جدول پ-۱۷ تبادل اطلاعات امنیت فضای مجازی

عنوان	مرجع
ITU-T X.1500 –X.1598 Series (CYBEX)	دنباله ۱۰: داده‌های شبکه، امنیت و ارتباطات سامانه باز - تبادل اطلاعات امنیت فضای مجازی

1- Unwanted

یادآوری- از سپتامبر ۲۰۱۱، به‌عنوان کار CYBEX در ITU-T در حال پیشرفت است، تنها X.1500، X.1520، X.1521 و X.1570 به‌عنوان توصیه یا پیش‌نویس در دسترس است. در آینده دیگران نیز پیروی خواهند کرد، پس توصیه می‌شود کاربران وب‌گاه ITU-T را برای آخرین اطلاعات در دسترس بررسی کنند.

کتاب‌نامه

[1] An Autonomous Architecture for Inter-Domain Trace back across the Borders of Network Operation (iscc06)

[2] IETF RFC 3882, Configuring BGP to Block Denial-of-Service Attacks

[3] ISO Guide 73:2009, Risk management — Vocabulary

[۴] استاندارد ملی ایران شماره ۱۲۲۰۷: سال ۱۳۹۰، مهندسی سامانه‌ها و نرم افزار-فرآیندهای چرخه حیات نرم‌افزار

[۵] استاندارد ملی ایران شماره ۱-۱۵۴۰۸: سال ۱۳۸۷، فناوری اطلاعات-فنون امنیتی-معیار ارزیابی امنیت فناوری اطلاعات-قسمت ۱-معرفی و مدل عمومی

[6] ISO/IEC 19770-1, Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance

[7] ISO/IEC TR 19791, Information technology — Security techniques — Security assessment of operational systems

[8] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements

[۹] استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - سامانه‌های مدیریت امنیت اطلاعات - الزامات

[۱۰] استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - آیین کار مدیریت امنیت اطلاعات

[۱۱] استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۹۲، فناوری اطلاعات - فنون امنیتی - مدیریت مخاطرات امنیت اطلاعات

[12] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[۱۳] استاندارد ملی ایران شماره ۲۷۰۳۱: سال ۱۳۹۲، فناوری اطلاعات -فنون امنیتی -راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به‌منظور تداوم کسب‌وکار

[14] ISO/IEC 27033 (all parts), Information technology — Security techniques — Network security

[15] ISO/IEC 27034 (all parts), Information technology — Security techniques — Application security

[۱۶] استاندارد ملی ایران شماره ۲۷۰۳۵: سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

[17] ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure

[18] ISO 31000, Risk management — Principles and guidelines

[19] ITU-T X.1200 – X.1299, Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Cyberspace security

[20] ITU-T X.1500 – X.1598, Series X: Data Networks, Open System Communications and Security – Cybersecurity Information Exchange