استانداردایران-ایزو-آی‌ای‌سی
۲۷۰۳۵
چاپ اول
اردیبهشت ۱۳۹۲

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

INSO-ISO/IEC
27035
1st. Edition.
Identical with
ISO/IEC
27035:2011
Apr.2013

فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات

Information technology — Security techniques — Information security incident management

ICS 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

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

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

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

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

کمیسیون فنی تدوین استاندارد « فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات»

رئیس:	**سمت و/یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی برق مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا : (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذرا (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
عسگرزاده، مجید (فوق لیسانس مهندسی کامپیوتر)	مدیر پروژه موسسه تحقیقات ارتباطات و فناوری اطلاعات
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فیاضی، مهدی (لیسانس مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه

قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
معروف، سینا (لیسانس مهندسی کامپیوتر- سخت‌افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رییس اداره تدوین استانداردها و نظارت بر امنیت سرویس‌ها سازمان فناوری اطلاعات ایران
موجبی، محمود (فوق لیسانس مهندسی برق مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
ناصری، علی (دکتری برق مخابرات)	عضو هیأت علمی دانشگاه امام حسین (ع)

فهرست مندرجات

پیش گفتار

استاندارد «فناوری اطلاعات – فنون امنیتی – مدیریت رخداد امنیت اطلاعات» که پیش نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده و در دویست و پنجاه و ششمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۰/۳۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علـوم و خـدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل ایـن استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفـت. بنـابراین، بهتراست همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

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

ISO/IEC 27035:2011, Information technology — Security techniques — Information security incident management

مقدمه

به‌طور کلی، خط‌مشی‌ها یا کنترل‌های امنیت اطلاعات بـه تنهـایی حفاظـت کلـی از اطلاعـات، سـامانه‌هـای اطلاعاتی، خدمات یا شبکه‌ها را تضمین نخواهندکرد. بعد از این‌که کنترل‌ها پیاده سازی شدند، احتمـال دارد آسیب‌پذیری‌های دیگری باقی بمانند که مـی‌تواننـد امنیـت اطلاعـات را بـی‌اثـر و در نتیجـه رخـداد امنیـت اطلاعاتی را امکان‌پذیر کنند. این کار می‌تواند به‌طور بـالقوه اثـر نـامطلوب مسـتقیم و غیـر مسـتقیم بـر روی عملیات کسب‌وکار سازمان داشته باشد. به‌علاوه، وقوع نمونه‌های جدیـد ناشـی از تهدیـدات ناشـناخته قبلـی اجتناب‌ناپذیر است. عدم آمادگی کافی سازمان جهـت رسـیدگی بـه چنـین رخـدادهایی، از تـاثیر هـر گونـه پاسخگویی[1] می‌کاهد و درجه‌ی تاثیر کسب‌وکار نامطلوب را به طور بالقوه افـزایش خواهـد داد. بنـابراین، هـر سازمانی که در مورد امنیت اطلاعات جدی است بهتراست رویکردی سازمان یافته و برنامه‌ریزی‌شده به شـرح زیر داشته باشد:

- آشکارسازی، گزارش و ارزیابی رخدادهای امنیت اطلاعات
- پاسخ به رخدادهای امنیت اطلاعات که شامل فعال‌سازی کنترل‌هـای مناسـب پیشـگیری، کـاهش و بازیابی تاثیرات (برای مثال، در حمایت از زمینه‌های مدیریت بحران) می‌باشد
- گزارش آسیب‌پذیری‌های امنیت اطلاعات که هنوز به عنوان عامل آسیب‌ها بهـره‌بـرداری نشـده‌انـد و ارزیابی و برخورد صحیح به آن‌ها
- درس گرفتن از رخداد امنیت اطلاعات و آسیب‌پذیری‌ها، پی‌ریزی کنتـرل‌هـای پیشـگیرانه، و بهبـود رویکرد کلی مدیریت رخداد امنیت اطلاعات

این استاندارد ملی رهنمود مدیریت رخداد امنیت اطلاعات را در بندهای ۴ تا ۹ فراهم مـی‌کنـد. ایـن بنـدها دربرگیرنده بندهای فرعی محتوی یک شرح مفصل از هر مرحله هستند.
عبارت «مدیریت رخداد امنیت اطلاعات» در این استاندارد علاوه بر مدیریت رویداد امنیتی، مدیریت آسیب-پذیری‌ها را نیز شامل می‌شود.

1- Response

فناوری اطلاعات – فنون امنیتی – مدیریت رخداد[1] امنیت اطلاعات

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین رویکردی ساختاریافته و برنامه‌ریزی شده است برای:

الف- آشکارسازی، گزارش، ارزیابی رخدادهای امنیت اطلاعات؛

ب- مدیریت و پاسخگویی به رخدادهای امنیت اطلاعات؛

پ- آشکارسازی، ارزیابی و مدیریت آسیب‌پذیری‌های امنیت اطلاعات؛ و

ت- بهبود مستمر امنیت اطلاعات و مدیریت رخداد به عنوان نتیجه مدیریت آسیب‌پذیری‌ها و رخدادهای امنیت اطلاعات.

این استاندارد ملی راهنمای مدیریت رخداد امنیت اطلاعات را برای سازمان‌های بزرگ و متوسط فراهم می‌نماید. سازمان‌های کوچک در رابطه با موقعیت مخاطره امنیت اطلاعات می‌توانند به نسبت اندازه و نوع کسب‌وکار خود از مجموعه‌ای از اسناد، فرایندها، و روال‌های شرح داده شده در این استاندارد ملی استفاده‌کنند. این استاندارد ملی راهنمایی هم در اختیار سازمان‌های بیرونی که خدمات مدیریت رخداد امنیت اطلاعات را فراهم می‌کنند، قرارمی‌دهد.

۲ مراجع الزامی

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

در صورتی که به شواهدی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد شواهدی که بدون ذکر تاریخ انتشار به آن ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه های بعدی آن‌ها مورد نظر است.

استفاده از مرجع زیر برای این استاندارد الزامی است:

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

---

1 - Incident

[۲] – استاندارد ملی ایران شماره ۲۷۰۰۰ : سال ۱۳۹۱ معادل با مدرک بین‌المللی ISO/IEC 27000:2009 وجود دارد.

۳ اصطلاحات و تعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف داده شده در استاندارد ISO/IEC 27000، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

امور قانونی امنیت اطلاعات[1]

به‌کارگیری فنون بررسی و تحلیل جهت اخذ[2]، ثبت و تحلیل رخدادهای امنیت اطلاعات است.

۳-۲

گروه پاسخگویی به رخداد امنیت اطلاعات [3]

ISIRT

گروهی از اعضای دارای مهارت مناسب و مورد اطمینان سازمان که رخدادهای امنیت اطلاعات را در طول چرخه حیات آن‌ها ساماندهی می‌نماید.

یادآوری- همانگونه که در این استاندارد ملی توصیف‌شده‌است، ISIRT کارکردی سازمانی است که فرآیند رخداد های امنیت اطلاعات را پوشش می‌دهد و اساسا بر رخدادهای مرتبط با فناوری اطلاعات متمرکز است. کارکردهای عام دیگر (با کوته‌نوشته‌های مشابه) ممکن است در سامان‌دهی رخدادها تا حدودی دامنه کاربرد و هدف متفاوتی داشته‌باشند. کوته‌نوشته‌های زیربه طور عام معنی مشابه و نه دقیقی با تعریف ISIRT دارند:

- گروه پاسخگویی امداد رایانه‌ای (CERT)[4]: یک گروه پاسخگویی امداد رایانه‌ای به‌طور عمده بر رخدادهای فناوری اطلاعات و ارتباطات (ICT)[5] تمرکزمی‌کند. ممکن است تعاریف ملی مشخص دیگری برای CERT وجود داشته باشد.

- گروه پاسخگویی به رخداد امنیت رایانه‌ای (CSIRT)[6]: یک گروه پاسخگویی به رخداد امنیت رایانه‌ای سازمان خدماتی که مسئول دریافت، بازنگری و پاسخگویی با گزارشات و فعالیت رخداد امنیت رایانه‌ها است. این خدمات به‌طورمعمول برای حوزه قانونی[7] تعریف شده‌ای ارایه می‌شوند، که می‌تواند هستاری اصلی مانند یک شرکت، سازمان دولتی، یا سازمان آموزشی؛ یک منطقه یا کشور؛ شبکه‌ای پژوهشی؛ یا یک مشتری که بهای خدمت را می‌پردازد، داشته باشند.

1- Information Security Forensics
2- Capture
3 -Information Security Incident Response Team
4- Computer Emergency Response Team
5 -Information and Communication Technology
6- Computer Security Incident Response Team
7- Constituency

۳-۳

رویداد[1] امنیت اطلاعات

وقوع شناسایی‌شده موقعیتی برای یک سامانه، خدمت یا شبکه، نشان‌دهنده نقضی احتمالی در امنیت اطلاعات، خط‌مشی یا خرابی کنترل‌ها یا موقعیتی از پیش ناشناخته که ممکن است مرتبط با امنیت باشد.

{ISO/IEC 27000: 2009}

۴-۳

رخداد امنیت اطلاعات

یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا غیرمنتظره‌ای که احتمال قابل ملاحظه‌ای برای به‌خطرانداختن[2] عملیات کسب‌وکار و تهدید امنیت اطلاعات دارند.

{ISO/IEC 27000: 2009}

۴ مرور کلی

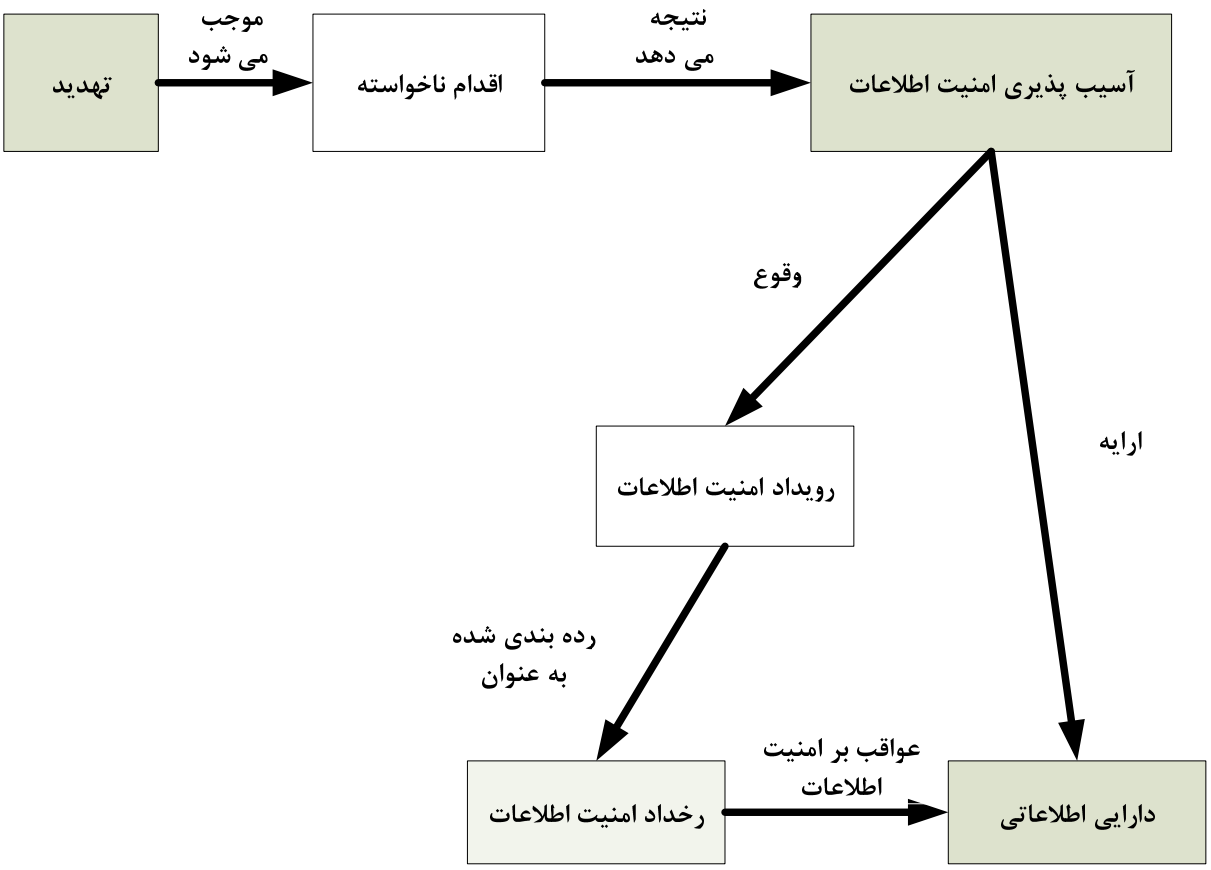
۴-۱ مفاهیم پایه

رویداد امنیت اطلاعات، وقوع شناسایی شده برای یک سامانه، خدمت یا وضعیت شبکه که نشان‌دهنده نقضی احتمالی در امنیت اطلاعات، خط‌مشی یا خرابی کنترل‌ها یا موقعیتی از پیش ناشناخته که ممکن است مرتبط با امنیت باشد. رخداد امنیت اطلاعات یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا غیر منتظره‌ای است که احتمال قابل ملاحظه‌ای برای به‌خطرانداختن عملیات کسب‌وکار و تهدید امنیت اطلاعات دارد.

وقوع رویداد امنیت اطلاعات ضرورتا تلاشی موفقیت آمیز تلقی نمی‌شود و یا به معنی وجود اشاراتی درباره محرمانگی، یکپارچگی و یا دسترسی‌پذیری نیست، یعنی همه رویداد های امنیت اطلاعات به عنوان رخدادهای امنیت اطلاعات رده‌بندی نمی‌گردد.

یک تهدید عبارت است از وقوع رویدادهای امنیت اطلاعات که به‌طور بالقوه باعث رخدادهای ناخواسته برای دارایی‌های اطلاعاتی می‌گردد. یک تهدید ازطریق آسیب‌پذیری‌ها خودرا نشان می‌دهد و برای بهره‌برداری از آسیب‌پذیری‌ها (ضعف‌ها)ی سامانه‌های اطلاعاتی، خدمات یا شبکه‌ها به روش‌های ناخواسته‌ای عمل می‌کند. شکل ۱ این رابطه‌ی موضوعات را در زنجیره‌ی رخداد امنیت اطلاعات نشان می‌دهد. موضوعات سایه‌خورده از قبل وجود داشته‌اند و تحت تاثیر موضوعاتی قرار می‌گیرند که رنگ روشن‌تری در زنجیره دارند و منجر به رخداد امنیت اطلاعاتی می‌شوند.

1- Event
2- Compromising



موضوعات سایه‌خورده از قبل وجود داشته‌اند، تحت تاثیر موضوعات سایه نخورده در زنجیره منجر به یک رخداد امنیت اطلاعات می‌شوند.

شکل ۱ - رابطه موضوعات در یک زنجیره‌ی رخداد امنیت اطلاعات

۲-۴ اهداف

سازمان بهتراست به عنوان قسمتی کلیدی از راهبرد کلی امنیت اطلاعات سازمانی، کنترل‌ها و روش‌های اجرایی درستی را که ایجاد رویکردی ساختاریافته و خوب برنامه‌ریزی شده برای مدیریت رخداد امنیت اطلاعات را تقویت کند، به‌کار ببرد. از منظر یک کسب‌وکار، هدف اوّلیه اجتناب کردن یا محدود کردن اثر[1] رخدادهای امنیت اطلاعات جهت کاهش هزینه‌های مستقیم یا غیر مستقیم ناشی از رخدادها است.

قدم‌های اولیه برای کمینه‌کردن اثر منفی مستقیم رخدادهای امنیت اطلاعات عبارتند از:

- متوقف و محدود کردن،
- ریشه‌کن کردن،

1-Impact

- تحلیل و گزارش کردن، و
- پیگیری نمودن.

اهداف یک رویکرد ساختاریافته و خوب برنامه‌ریزی‌شده مناسب‌تر هستند و توصیه می‌شود از موارد زیر اطمینان حاصل کنند:

الف- رویدادهای امنیت اطلاعات آشکارشده[1] و رسیدگی موثر در مورد آن‌ها صورت گرفته است، به ویژه در مورد شناسایی اینکه آن‌ها باید به عنوان رخداد امنیت اطلاعات رده‌بندی[2] و رسته‌بندی[3] شوند یا خیر.

ب- رخدادهای امنیت اطلاعات شناسایی شده، به مناسب‌ترین و کاراترین روش ارزیابی شده و به آن‌ها پاسخ داده می‌شود.

پ- تاثیرات نامطلوب رخدادهای امنیت اطلاعات بر سازمان و عملیات کسب‌وکار آن به وسیله کنترل‌های مناسب کمینه شده‌اند. این کنترل‌ها به عنوان قسمتی از پاسخگویی با رخداد، به طور بالقوه در پیوندی مناسب با عناصر مرتبط با برنامه یا برنامه‌های مدیریت بحران، هستند.

ت- گزارش آسیب‌پذیری‌های امنیت اطلاعات به‌طور مناسب ارزیابی و رسیدگی می‌شوند.

ث- درس‌ها به سرعت از رخدادهای امنیت اطلاعات، آسیب‌پذیری‌ها و مدیریت مرتبط فراگرفته می‌شوند. این کار برای افزایش فرصت‌های پیشگیری از رخدادهای امنیت اطلاعات آینده از رخ دادن، بهبود پیاده‌سازی و استفاده از کنترل‌های امنیت اطلاعات و بهبود طرح‌واره‌ی کلی مدیریت رخداد امنیت اطلاعات است.

برای کمک به دست‌یابی به این مسئله، بهتراست سازمان‌ها مطمئن شوند که رخدادهای امنیت اطلاعات با استفاده از استانداردهای مناسب رده‌بندی و رسته‌بندی رخداد، و اشتراک‌گذاری، به صورت یکنواختی مستند شده‌اند، به‌طوری‌که به ایجاد متریک‌ها[4] از داده‌های جمع‌آوری شده در یک دوره زمانی، منجر شود. این کار اطلاعات ارزشمندی را برای کمک به فرآیند تصمیم‌گیری راهبردی هنگام سرمایه‌گذاری در کنترل‌های امنیت اطلاعات فراهم می‌کند.

یادآوری می‌شود که هدف دیگر مرتبط با این استاندارد ملی، فراهم کردن راهنمایی برای سازمان‌ها است که آن‌ها را در زمینه رعایت الزامات مشخص‌شده در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ (و بنابراین پشتیبانی‌شده توسط راهنمای استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷) کمک کند. این کار شامل الزامات مرتبط با مدیریت رخداد امنیت اطلاعات می‌شود. جدول ارجاعات متقابل بندهای مرتبط با مدیریت

1- Detected
2- Classified
3- Categorized
4- Metrics

رخداد امنیت اطلاعات در استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ و استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ و بندهای این استاندارد ملی در پیوست الف نشان داده شده است.

۳-۴ مزایای رویکردی ساختار یافته

به سازمانی که از رویکردی ساختاریافته برای مدیریت رخداد امنیت اطلاعات استفاده می‌کند مزایای قابل توجهی تعلق می‌گیرد که تحت موارد ذیل قابل گروه‌بندی هستند:

الف- بهبود امنیت اطلاعات به طورکلی

فرآیندی ساختاریافته برای آشکارسازی، گزارش‌دهی و ارزیابی از و تصمیم‌گیری مرتبط با رویدادها و رخدادهای امنیت اطلاعات توان شناسایی و پاسخگویی سریع را فراهم خواهدساخت. این مسئله به طورکلی امنیت را از طریق کمک به شناسایی سریع و پیاده‌سازی راه حلی پایدار بهبود می‌بخشد و در نتیجه وسائلی برای پیشگیری از رخدادهای امنیت اطلاعات مشابه بیشتر در آینده، فراهم می‌کند. به علاوه، این مزایا تسهیلاتی از طریق متریک‌ها، به اشتراک گذاری و انبوهش[1] ایجاد خواهد کرد. اعتبار سازمان از طریق نمایش پیاده‌سازی بهترین تجارب خود در رابطه با مدیریت رخداد امنیت اطلاعات بهبود خواهد یافت.

ب- کم کردن اثرهای نامطلوب کسب وکار

رویکردی ساختاریافته در مدیریت رخداد امنیت اطلاعات می‌تواند به کاهش سطح اثرهای بالقوه نامطلوب کسب‌وکار مرتبط با رخداد امنیت اطلاعات کمک نماید. این اثرها می‌توانند شامل زیان‌های مالی سریع و زیان بلندمدّت ناشی از صدمه به شهرت و اعتبار باشند (برای راهنمایی درباره تحلیل اثرکسب‌وکار، استاندارد ملی ایران شماره ۲۷۰۰۵: ۱۳۸۸ ملاحظه شود).

پ- تقویت تمرکز بر پیشگیری از رخداد امنیت اطلاعات

به‌کارگیری رویکردی ساختاریافته در مدیریت رخداد امنیت اطلاعات به ایجاد تمرکز بهتری درباره پیشگیری از رخداد در داخل سازمان ازجمله روش‌های شناسایی تهدیدها و آسیب‌پذیری‌های جدید، کمک می‌نماید. تحلیل داده‌های مربوط به رخداد، شناسایی الگوها و رَوَندها[2] را ممکن می‌سازد، به این ترتیب تمرکز صحیح-تری در مورد پیشگیری از رخداد و بنابراین شناسایی عملیات مناسب برای پیشگیری از وقوع رخداد را تسهیل می‌کند.

1-Aggregation
2-Trends

ت- تقویت اولویت‌بندی

رویکردی ساختاریافته در مدیریت رخداد امنیت اطلاعات، پایه‌ی استواری را برای اولویت‌بندی در زمان رسیدگی‌های[1] به رویداد امنیت اطلاعات فراهم خواهدکرد که شامل به کارگیری مقیاس‌های رده‌بندی و رسته‌بندی موثر است. چنانچه روش‌های اجرایی روشنی وجود نداشته باشند، این مخاطره وجود دارد که فعالیت‌های رسیدگی به حالتی واکنشی، از طریق پاسخگویی با رخدادها در زمان وقوع آن‌ها و نادیده‌گرفتن فعالیت‌های موردنیاز، اجرا شوند. این کار می‌تواند از هدایت فعالیت‌های رسیدگی به حوزه‌هایی که ممکن است از اولویت بالاتری برخوردار باشند و درجایی‌که آن‌ها واقعا مورد نیاز بوده و در اولویت ایده‌آل قراردارند، پیشگیری کند.

ث- تقویت شواهد[2]

روش‌های اجرایی دقیق بررسی رخداد می‌تواند به حصول اطمینان از اینکه جمع‌آوری و ساماندهی داده به طرز مشهودی مناسب بوده و از نظر قانونی قابل‌پذیرش هستند، کمک نمایند. این شواهد، درصورتی‌که احتمال پی‌گرد قانونی یا اقدام انظباطی در ادامه وجود داشته‌باشد، از اهمیت قابل ملاحظه‌ای برخوردار هستند. با این‌حال بهتراست تصدیق کرد که این شانس وجود دارد که اقدامات لازم برای بازیابی رخداد امنیت اطلاعات ممکن است صحت شواهد جمع‌آوری‌شده‌ی این‌چنین را به خطر بیندازد.

ج- کمک به توجیه[3] بودجه و منابع

رویکردی درست تعریف‌شده و ساختار یافته در مدیریت رخداد امنیت اطلاعات، تخصیص بودجه‌ها و منابع در بین واحدهای سازمانی درگیر را توجیه و ساده می‌کند. به‌علاوه، به خود طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات این مزایا تعلق خواهد گرفت:

- استفاده از کارکنان دارای مهارت کمتر برای شناسایی و حذف هشدارهای ناهنجار یا غیرمتعارف،
- فراهم‌آوردن هدایت بهتر برای فعالیت‌های کارکنان ماهر
- اشتغال کارکنان ماهر تنها برای آن فرآیندهایی که مهارت آن‌ها مورد نیاز بوده و تنها در مرحله‌ای از فرآیند که مشارکت آن‌ها مورد نیاز است.

رویکرد سودمند دیگری برای کنترل و بهینه‌سازی بودجه و منابع، اضافه‌کردن ردیابی زمانی در مدیریت رخداد امنیت اطلاعات برای تسهیل ارزیابی‌های کمی ساماندهی رخداد امنیت اطلاعات سازمان است. برای مثال، بهتراست امکان فراهم‌آوردن اطلاعات درمورد اینکه چقدر طول می‌کشد تا رخدادهای امنیت اطلاعات

1- Investigations
2- Strengthening evidence
3- Justifications

را از اولویت‌های متفاوت و از سکوهای[1] متفاوت برطرف کردن کند، وجود داشته‌باشد. در صورت وجود تنگناهایی در فرآیند مدیریت رخداد امنیت اطلاعات، این تنگناها بهتراست قابل شناسایی باشند.

چ- بهبود روزآمدی[2] ارزیابی مخاطره امنیت اطلاعات و نتایج مدیریت
استفاده از رویکردی ساختاریافته در مدیریت رخداد امنیت اطلاعات تسهیل می‌کند:

- جمع‌آوری بهتر داده‌ها برای کمک به شناسایی و تعیین خصوصیات انواع مختلف تهدید و آسیب‌پذیری‌های مرتبط
- فراهم‌آوردن داده‌ها درباره بسامدهای[3] وقوع انواع تهدیدهای شناسایی‌شده.

داده‌های جمع آوری‌شده درباره اثرهای نامطلوب رخدادهای امنیت اطلاعات بر عملیات کسب‌وکار در تحلیل اثر کسب‌وکار، سودمند واقع خواهندشد. داده‌های جمع‌آوری شده برای شناسایی بسامد وقوع انواع تهدیدهای مختلف تا حد زیادی به کیفیت ارزیابی تهدید کمک خواهدکرد. به همین ترتیب، داده‌های جمع‌آوری‌شده درباره آسیب‌پذیری‌ها تا حد زیادی به کیفیت ارزیابی‌های آسیب‌پذیری در آینده کمک خواهدکرد (برای راهنمایی درباره ارزیابی و مدیریت مخاطره امنیت اطلاعات، استاندارد ISO/IEC27005:2008 ملاحظه شود).

ح- اطلاع‌رسانی قوی نسبت به امنیت اطلاعات و مطالب برنامه آموزشی
رویکردی ساختاری در مدیریت رخداد امنیت اطلاعات، اطلاعات متمرکزی را برای برنامه‌های اطلاع‌رسانی امنیت اطلاعات فراهم خواهدکرد. این اطلاعات متمرکز نمونه‌هایی واقعی از رخداد امنیت اطلاعات را که برای سازمان‌های واقعی رخ می‌دهند، ارایه می‌کند. همچنین نمایش مزایای مرتبط با دسترسی سریع به اطلاعات برطرف کردن رخداد را امکان‌پذیر خواهدساخت. علاوه بر این، چنین اطلاع‌رسانی به کاهش اشتباه یا ترس/دست‌پاچگی فردی در رویداد یک رخداد امنیت اطلاعات کمک می‌کند.

خ- ارایه ورودی به خط‌مشی امنیت اطلاعات و بازنگری‌های مستندات مربوط
داده‌های تهیه‌شده توسط طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، می‌تواند ورودی ارزشمندی را برای بازنگری‌های اثربخشی و بهبود بعدی خط‌مشی‌های امنیت اطلاعات (و دیگر اسناد مربوط به امنیت اطلاعات) ارایه نماید. این مسئله در مورد خط‌مشی‌ها و دیگر اسناد کاربست‌پذیر، هم در گستره سازمان‌ها و هم در سامانه‌ها، خدمات و شبکه‌های منفرد کاربرد دارد.

4- platforms
4-Update
1- Frequencies

۴-۴ سازگاری[1]

راهنمای ارایه شده در این استاندارد ملی گسترده‌است و چنانچه به طور کامل پذیرفته شود، می‌تواند به منابع قابل توجهی برای بهره‌برداری[2] و مدیریت نیاز داشته باشد. بنابراین مهم است سازمانی که این راهنمایی را به‌کار می‌بندد، بهتراست چشم انداز آن را به‌خاطر داشته باشد و اطمینان حاصل کند که منابع به‌کاربسته شده در مدیریت رخداد امنیت اطلاعات و پیچیدگی سازوکارهای پیاده‌سازی‌شده، به نسبت زیر حفظ خواهدشد:

الف- اندازه، ساختار و ماهیت کسب‌وکار یک سازمان،

ب- حوزه هر سامانه مدیریت امنیت اطلاعات که در آن رخدادها ساماندهی می‌شوند،

پ- تحمل بالقوه زیان ناشی از رخدادهای غیر قابل پیشگیری، و

ت- اهداف کسب وکار.

به این ترتیب سازمانی که از این استاندارد ملی استفاده می‌کند بهتراست راهنمای آن‌را به نسبت مقیاس و خصوصیات کسب و کار خود بپذیرد.

۴-۵ مراحل

برای دست‌یابی به اهداف طرح‌ریزی‌شده در بند۴-۲، مدیریت رخداد امنیت اطلاعات شامل پنج مرحله‌ی مشخص زیر است:

- برنامه‌ریزی و آماده‌سازی
- آشکارسازی و گزارش
- ارزیابی و تصمیم‌گیری،
- پاسخگویی، و
- درس‌های آموخته‌شده.

اوّلین مرحله عبارت است از تهیه تمامی چیزهای مناسبی که برای اجرای موفقیت آمیز مدیریت رخداد امنیت اطلاعات مورد نیاز است. چهار مرحله دیگر دربرگیرنده‌ی استفاده‌ی عملیاتی مدیریت رخداد امنیت اطلاعات است.

شکل ۲ این مراحل را با نگاهی از بالا نشان می‌دهد.

2- Adaptability
3- to operate

شکل ۲- مراحل مدیریت رخداد امنیت اطلاعات

۶-۴ مثال‌هایی از رخدادهای امنیت اطلاعات

رخدادهای امنیت اطلاعات ممکن است عمدی یا تصادفی باشند (برای مثال، از طریق خطا یا کارهای طبیعت)، و ممکن است از طریق وسایل فنی یا فیزیکی ایجاد شده‌باشند. پی‌آمد این رخدادها ممکن است شامل افشا، تغییر، تخریب، یا عدم دسترسی‌پذیری اطلاعات به صورت غیرمجاز ، یا صدمه یا سرقت دارایی-های سازمانی باشد. چنانچه رویدادهای گزارش نشده امنیت اطلاعات وقوع رخداد را تایید کند، بررسی رخداد و اعمال کنترل به منظور پیشگیری از وقوع مجدد آن، مشکل می‌شود.

پیوست ب توصیف‌های نمونه منتخب رخدادهای امنیت اطلاعات و علل آن‌ها را تنها برای اهداف اطلاعاتی فراهم می‌کند. توجه به این نکته مهم است که این مثال‌ها به هیچ وجه جامع[1] نیستند.

۵ مرحله برنامه‌ریزی و آماده سازی

۵-۱ مرور کلی فعالیت‌های کلیدی

مدیریت موثر رخداد امنیت اطلاعات نیاز به برنامه‌ریزی و آماده سازی مناسب دارد. برای اینکه طرح‌واره‌ی مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات کارآمد و موثر باشد تا عملیاتی شود، سازمان بهتراست تعدادی فعالیت‌های آماده‌سازی را بعد از برنامه‌ریزی لازم تکمیل نماید. سازمان بهتراست از فعالیت‌های مرحله برنامه‌ریزی و آماده‌سازی شامل موارد زیر اطمینان حاصل نماید:

الف- فعالیت برای تنظیم و ارائه خط‌مشی مدیریت رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات و جلب تعهد مدیریت ارشد برای آن خط‌مشی می‌باشد. پیش از این بهتراست آسیب‌پذیری‌های امنیت اطلاعات سازمان بازنگری، نیاز به طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات تایید و مزایای آن برای سازمان به صورت کلی و برای ادارات آن شناسایی شود (بند۵-۲ ملاحظه شود). حصول اطمینان از تعهد مستمر مدیریت برای پذیرش رویکردی ساختاریافته در مدیریت رخداد امنیت اطلاعات حیاتی است. کارکنان بهتراست یک رخداد را بشناسند، بدانند چه کاری انجام دهند و مزایای رویکرد را برای سازمان درک کنند. مدیریت برای حصول اطمینان از تعهد سازمان نسبت به تامین منابع و حفظ توانایی پاسخگویی با رخداد، باید پشتیبان طرح‌واره‌ی مدیریت باشد.

ب- فعالیت برای روزآمدکردن خط‌مشی‌های امنیت اطلاعات و مدیریت مخاطره در سطح شرکت و سطوح سامانه، خدمت و شبکه‌ی مشخص است. این فعالیت بهتراست مرجع مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات را شامل گردد. خط‌مشی‌ها باید به‌طور منظم در مقوله[2] خروجی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات بازنگری شوند (بند ۵- ۳ ملاحظه شود).

1- Exhaustive
2- Context

پ- فعالیت برای تعریف و مستند کردن یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات مفصل است. به‌طورکلی، مستندسازی طرح‌واره بهتراست شامل شکل‌ها، روش‌های اجرایی، عناصر سازمانی و ابزار پشتیبانی[1] برای آشکارسازی، گزارش، ارزیابی و تصمیم‌گیری مربوط به، پاسخگویی با و آموختن از رخدادهای امنیت اطلاعات باشند. موضوعات شامل موارد زیر هستند:

۱- مقیاس رده‌بندی رویداد/ رخداد امنیت اطلاعات که برای درجه‌بندی رویداد/ رخداد استفاده می‌شود. تصمیم بهتراست در هر رویدادی براساس تاثیرات نامطلوب واقعی یا برنامه‌ریزی‌شده بر عملیات کسب‌وکار سازمان باشند.

یادآوری- پیوست پ مثالی از یک رویکرد رده‌بندی و رسته‌بندی رویدادها و رخدادهای امنیت اطلاعات نشان می‌دهد.

۲- برگه‌های[2] رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات:

i- برگه‌ای که توسط شخص گزارش‌دهنده یک رویداد امنیت اطلاعات (یعنی شخصی که عضو گروه مدیریت رخداد امنیت اطلاعات نیست)، با استفاده از اطلاعات ضبط شده در دادگان[3] رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات تکمیل می‌شود.

ii- برگه‌ای که توسط کارکنان مدیریت رخداد امنیت اطلاعات برای تهیه گزارش آغازین اطلاعات رویداد امنیت اطلاعات و قادر ساختن ضبط مستمر ارزیابی رخداد و غیره در طول زمان تا وقتی که رخداد به‌طور کامل برطرف کردن شود، مورد استفاده قرارمی‌گیرد. در هر مرحله، روزآمدشدن در دادگان رویداد/رخداد/ آسیب‌پذیری امنیت اطلاعات ضبط می‌شود. سپس برگه کامل‌شده دادگان رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات پس از برطرف کردن[4] رخداد به‌کار برده می‌شوند، و

iii- برگه‌ای که توسط شخص گزارش‌دهنده آسیب‌پذیری امنیت اطلاعات (که هنوز به عنوان عامل رویداد و احتمالا رخداد امنیت اطلاعات مورد بهره‌برداری قرار نگرفته است)، با استفاده از اطلاعات ضبط‌شده در دادگان رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات تکمیل می‌شود.

توصیه می‌شود که این برگه‌ها الکترونیکی باشند (برای مثال در صفحه تارنمای[5] امن)، با پیوند مستقیم به دادگان رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات الکترونیکی. در دنیای امروز به‌کارگیری طرح‌واره‌ی مبتنی بر کاغذ زمان‌بر است. با این حال، ممکن است در مواردی که طرح‌واره‌ی الکترونیکی قابل استفاده نیست، مورد نیاز باشد.

یادآوری- برگه‌های نمونه در پیوست ت نشان داده شده است.

1-Support tools
2- Forms
3-Database
4- Resolution
5- Web page

۳- روش‌های اجرایی مستند شده و اقدامات مربوط به استفاده از برگه‌ها، یعنی مرتبط با آشکارسازی رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات، با پیوندهایی به روش‌های اجرایی عادی برای استفاده از پشتیبان‌های داده وسامانه، خدمت و/یا شبکه و برنامه‌های مدیریت بحران مرتبط است.

۴- روش‌های اجرایی عملیاتی برای ISIRT، با فرآیندهای مستند شده و مسئولیت‌های مرتبط و تخصیص نقش به کارکنان تعیین شده برای اجرای فعالیت‌های مختلف (بسته به اندازه، ساختار و طبیعت کسب و کار هر سازمان، ممکن است به هر فرد بیش از یک نقش تخصیص داده شود)، برای مثال شامل:

i - خاموش کردن سامانه، خدمات و/یا شبکه تحت تاثیر در شرایط خاص، با توافق و هماهنگی قبلی با مدیریت فناوری اطلاعات و یا کسب و کار مرتبط،

ii- ترک کردن سامانه، خدمت و یا شبکه تحت تاثیر به صورت متصل و در حال کار گذاشتن،

iii- پایش جریان داده‌ها از، به و میان یک سامانه، خدمت و یا شبکه‌ی تحت تاثیر ،

iv- فعال کردن روش‌های اجرایی و عملیات پشتیبانی عادی و مدیریت بحران هماهنگ با خط‌مشی امنیت سامانه، خدمت، و/یا شبکه،

v - پایش و استمرار حفاظت امن شواهد الکترونیکی در مواردی که برای پیگیری قانونی یا اقدام انضباطی داخلی مورد نیاز است، و

vi- ارتباط برقرار کردن با کارکنان یا سازمانهای داخلی و خارجی در مورد جزئیات رخداد امنیت اطلاعات.

دربعضی سازمان‌ها به این طرح‌واره ممکن است به عنوان یک برنامه پاسخگویی رخداد امنیت اطلاعات رجوع شود. (بند ۴-۵ ملاحظه شود).

ت- فعالیت برای استقرار **ISIRT**، با یک برنامه آموزشی مناسب، که مختص کارکنان سازمان طراحی، تدوین و ارایه شود. ممکن است یک سازمان بر اساس اندازه، ساختار و طبیعت کسب‌وکار، دارای یک **ISIRT** متشکل از یک گروه اختصاصی، یک گروه مجازی، یا ترکیبی از هر دو گزینه باشد. یک گروه اختصاصی ممکن است دارای اعضای مجازی شناسایی شده از واحدهایی/کارکردهایی باشد که بهتراست در طول برطرف کردن یک رخداد امنیت اطلاعات، همکاری نزدیکی با **ISIRT** داشته باشند (**ICT**، حقوقی، روابط عمومی، شرکت‌های برون‌سپاری و غیره). یک گروه مجازی که ممکن است دارای یک مدیرارشد باشد که این مدیر گروهی را رهبری می‌کند که توسط گروه‌های کارکنان متخصص در موضوعات خاص مانند ساماندهی حملات کد مخرب، پشتیبانی می‌شود. این گروه‌ها، بسته به نوع رخداد مورد نظر، فرا خوانده می‌شوند (بند ۵-۵ ملاحظه شود).

ث- فعالیت جهت ایجاد و حفظ روابط و پیوند مناسب با سازمان‌های داخلی و خارجی که به صورت مستقیم در مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات دخیل هستند.

ج- فعالیت جهت استقرار، پیاده سازی و عملیات فنی و دیگر سازوکارهای پشتیبانی (شامل سازمانی) برای پشتیبانی از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات (و بنابراین کار **ISIRT**)، و به‌منظور پیشگیری از وقوع رخداد امنیت اطلاعات یا کاهش احتمال وقوع رخداد امنیت اطلاعات (به بند ۵-۶ مراجعه شود). چنین سازوکارهایی می‌توانند در بر گیرنده موارد ذیل باشند:

۱- سازوکارهای ممیزی امنیت اطلاعات داخلی برای ارزیابی سطح امنیت و ردگیری سامانه‌های آسیب‌پذیر

۲- مدیریت آسیب‌پذیری (شامل روزآمدی امنیت و ترمیم کردن سامانه‌های آسیب‌پذیر).

۳- مراقبت از فناوری برای آشکارسازی انواع جدید تهدیدها و حمله‌ها.

۴- سامانه‌های آشکارسازی نفوذ[1] (برای جزئیات بیشتر استاندارد ملی ایران شماره ۱۸۰۴۳: سال ۱۳۸۸، ملاحظه شود).

۵- افزاره‌های امنیت شبکه، وسایل حفاظت و ابزارهای پایش (برای جزئیات بیشتر استاندارد

ISO/IEC 27033 ملاحظه شود).

۶- نرم‌افزار ضد کد مخرب

۷- ممیزی سوابق ثبت[2] و نرم‌افزار پایش سوابق[3].

۸- مسئولیت‌های مستندشده و روش‌های اجرایی عملیاتی برای گروه پشتیبانی عملیات.

چ- فعالیت برای طراحی و تدوین یک برنامه آموزش و اطلاع‌رسانی مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات است. بهتراست تمام کارکنان سازمانی از طریق جلسات توجیهی، و/یا دیگر سازوکارها از وجود طرح‌واره‌ی مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات، مزایای آن و چگونگی گزارش کردن رویدادها و/یا رخدادهای امنیت اطلاعات (و آسیب‌پذیری‌ها) آگاه شوند. به موازات، بهتراست آموزش مناسب برای کارکنانی که مسئولیت اداره طرح‌واره‌ی مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات را به‌عهده دارند، تصمیم گیرندگان دخیل در تعیین اینکه آیا رویدادهای امنیت اطلاعات رخداد هستند و کارکنان دخیل در رسیدگی به رخدادها، ارایه شود. بهتراست جلسات توجیهی اطلاع‌رسانی وجلسات آموزشی برای تطبیق تغییرات به کارکنان بعدا تکرار شوند (بند ۵- ۷ ملاحظه شود).

1- Intrusion Detection System
2- Log record
3-Log

ح- فعالیت برای آزمایش استفاده از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، فرآیندها و روش‌های اجرایی آن است. بهتراست آزمونها به‌صورت دوره‌ای نه تنها برای آزمون طرح‌واره در یک موقعیت واقعی، بلکه برای سنجش درستی چگونگی رفتار **ISIRT** تحت فشار یک رخداد پیچیده جدی، سازماندهی شوند. بهتراست توجه مخصوص به ایجاد آزمونهایی که بر روی وقوع سناریوهای آسیب‌پذیری، تهدید و مخاطره تمرکز می‌یابند معطوف شود (بند ۵- ۸ ملاحظه شود). بهتراست طرح‌واره شامل استانداردهایی باشد که اشتراک‌گذاری اطلاعات هم در داخل و هم خارج از سازمان(در صورت نیاز سازمان) را پشتیبانی نماید. یکی از مزایای اشتراک‌گذاری، انباشته شدن داده‌ها در متریک‌هایی سودمند جهت کمک به تصمیم‌های راهبردی کسب وکار است. عضویت در یک جامعه اشتراک‌گذاری اطلاعات مورد اعتماد، دریافت زود هنگام اخطارهای حملات را میسر می‌نماید و بهتراست در هر طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات و خط‌مشی مرتبط، تشویق گردد.

با تکمیل شدن این مرحله، بهتراست سازمان‌ها به‌طور کامل آماده اداره صحیح رخدادهای امنیت اطلاعات باشند. بندهای زیر، هریک از فعالیت‌های فهرست شده فوق ، شامل محتوای هر یک از مستندات مورد نیاز را توصیف می‌کند.

۵-۲ خط‌مشی مدیریت رخداد امنیت اطلاعات

۵-۲-۱ مقدمه

یک سازمان بهتراست خط‌مشی خود را برای اداره کردن رویدادها، رخدادها و آسیب‌پذیری‌های امنیت اطلاعات، به‌صورت یک مستند آزاد[1]، به عنوان بخشی از خط‌مشی کلی سامانه مدیریت امنیت اطلاعات (بند۴- ۲- ۱ب از استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ملاحظه شود)، یا به عنوان قسمتی از خط‌مشی امنیت اطلاعات خود (بند ۵-۱-۱ از استاندارد ملی ایران شماره ۲۷۰۰۲: سال ۱۳۸۷ملاحظه شود) مستند نماید. اندازه، ساختار و طبیعت کسب و کار یک سازمان و گستره برنامه مدیریت رخداد امنیت اطلاعات، عوامل تصمیم‌گیری در تعیین پذیرش هرکدام از این گزینه‌ها هستند. هر سازمان بهتراست خط‌مشی مدیریت رخداد امنیت اطلاعات خود را به سوی هر شخصی که دارای دسترسی قانونی به سامانه‌های اطلاعاتی و مکان‌های مربوط به آن است، هدایت کند.

قبل از اینکه خط‌مشی تنظیم شود، سازمان بهتراست یک بازنگری امنیت اطلاعات را که آسیب‌پذیری‌ها، تائید نیاز برای مدیریت رخداد امنیت اطلاعات و شناسایی مزایای آن برای کل سازمان و برای هر یک از واحدهایش برجسته می‌سازد، اجرا نماید.

1- Free-standing document

۵-۲-۲ طرف‌های دخیل

بهتر است سازمان اطمینان حاصل نماید که خط‌مشی مدیریت رخداد امنیت اطلاعات آن توسط یک مقام ارشد اجرایی سازمان، با تعهد مستندشده مورد تایید ازسوی کل مدیریت ارشد، تصویب می‌شود. این مستند بهتراست در دسترس همه کارمندان و پیمانکاران قرار داده شود، همچنین بهتراست در جلسات آموزشی و توجیهی اطلاع‌رسانی امنیت نسبت به آن تاکید شود (بند ۵– ۷ ملاحظه شود).

۵-۲-۳ محتوا

بهتر است سازمان اطمینان حاصل نماید که محتوای خط‌مشی مدیریت رخداد امنیت اطلاعات آن بر موضوعات زیر تاکید می‌کند:

الف- اهمیت مدیریت رخداد امنیت اطلاعات برای سازمان، و تعهد مدیریت ارشد به آن و طرح‌واره‌ی مربوط.

ب- مرور کلی بر آشکارسازی، گزارش و جمع آوری اطلاعات مرتبط با رویداد امنیت اطلاعات و اینکه چگونه این اطلاعات بهتراست جهت تعیین رخدادهای امنیت اطلاعات مورد استفاده قرارگیرند.

این مرور کلی، بهتراست شامل خلاصه‌ای از انواع احتمالی رویداد امنیت اطلاعات، چگونگی گزارش آن‌ها، محتوای گزارش، ارایه آن به کجا و چه کسی، و چگونگی ساماندهی انواع کاملا جدید رویدادهای امنیت اطلاعات باشد. همچنین بهتراست حاوی خلاصه‌ای از گزارش مدیریت آسیب‌پذیری امنیت اطلاعات و ساماندهی آن باشد.

پ- مروری کلی بر ارزیابی رخداد امنیت اطلاعات شامل خلاصه‌ای از معرفی فرد مسئول، چه کاری باید انجام شود، اعلام و ارجاع به مرجع بالاتر[1] آن.

ت- تهیه خلاصه‌ای از فعالیت‌های مربوط به پس از تایید اینکه یک رویداد امنیت اطلاعات یک رخداد امنیت اطلاعات است.

ث- مرجعی برای تامین نیاز مربوط به حصول اطمینان از اینکه تمام فعالیت‌های مدیریت رخداد امنیت اطلاعات، برای تحلیل بعدی به درستی ثبت شده و اینکه پایش مستمر برای حصول اطمینان از حفظ ایمنی شواهد الکترونیکی، در صورت نیاز احتمالی به پیگیری قانونی یا اقدام انتظامی داخلی، اعمال شده است.

ج- فعالیت‌های پس از برطرف کردن رخداد امنیت اطلاعات، شامل یادگیری از و بهبود فرایند رخدادهای امنیت اطلاعات بعدی است.

چ- یک مرور کلی بر گزارش دهی و سامان‌دهی آسیب‌پذیری امنیت اطلاعات است.

1- Escalation

ح- جزئیات مکانی که مستند سازی طرح‌واره، ازجمله روش‌های اجرایی، نگهداری می‌شوند.

خ- مروری کلی بر **ISIRT**، در بر گیرنده عناوین زیر:

۱- ساختار سازمانی **ISIRT** و هویت مدیر **ISIRT** و دیگر کارکنان کلیدی، ازجمله کارکنانی که مسئول امور زیر هستند:

i- توجیه کردن مدیریت ارشد نسبت به رخدادها

ii- رسیدگی کردن به پرسش‌ها، تحریک کردن[1] به پیگیری، غیره و

iii- پیوند با سازمان‌های خارجی (در زمان ضرورت)

۲- منشور[2] مدیریت امنیت اطلاعات مشخص می‌کند **ISIRT** قرار است چه کارهایی و تحت نظر چه مقام قانونی[3] انجام می‌دهد. منشور در کمینه بهتراست حاوی یک بیانیه ماموریت، تعریفی از حوزه **ISIRT**، و جزئیات حامی سطح هیأت مدیره و مقام قانونی **ISIRT** باشد.

۳- بیانیه ماموریت**ISIRT** که بر روی فعالیت‌های اصلی گروه تمرکز می‌کند. به منظور اینکه گروه به عنوان یک **ISIRT** مورد توجه قرار گیرد، گروه بهتراست از ارزیابی، پاسخگویی با و اداره کردن رخدادهای امنیت اطلاعات تا رسیدن به یک نتیجه موفقیت آمیز پشتیبانی نماید. اهداف و مقاصد گروه مخصوصا مهم بوده وبه تعریف شفاف و بدون ابهام نیاز دارد.

۴- تعریفی از محدوده فعالیت‌های**ISIRT**. به‌طور عادی محدوده **ISIRT** یک سازمان تمامی سامانه‌های اطلاعات، خدمات و شبکه‌های سازمان را پوشش می‌دهد. در دیگر موارد، یک سازمان ممکن است به هر دلیلی، به محدوده‌ای در سطح پایین تر از آن نیاز داشته باشد که در این مورد بهتراست به‌صورت روشن آنچه را که در آن محدوده و آنچه که در خارج از آن محدوده قرار می‌گیرد، مستند نماید.

۵- هویت یک مقام ارشد اجرایی، عضو هیأت مدیره یا مدیر ارشد که قدرت تصمیم‌گیری درباره**ISIRT** و همچنین استقرار سطوح مقامات قانونی برای**ISIRT** را دارد. دانستن این به تمامی کارکنان در سازمان کمک می‌کند تا پیشینه و پایه‌گذاری **ISIRT** را درک کنند و این اطلاعات برای ایجاد اعتماد در **ISIRT** حیاتی است. بهتراست توجه داشت که این جزئیات پیش از انتشار، بهتراست از یک دیدگاه قانونی مورد وارسی قرار گیرند. در بعضی شرایط افشای مقام قانونی گروه ممکن است آن را در معرض ادعاهای احتمالی قرار دهد.

1-Instigating
2- Charter
3-Authority

۶- پیوند با سازمان‌هایی که پشتیبان خارجی مشخصی را فراهم می‌نمایند، مانند گروه‌های امور قانونی(بند۵-۵-۴ ملاحظه شود).

د- مرور کلی پشتیبانی فنی و دیگر سازوکارهای پشتیبانی.

ذ- مرور کلی برنامه‌های اطلاع‌رسانی و آموزشی مدیریت رخداد امنیت اطلاعات.

ر- خلاصه‌ای از جنبه‌های قانونی و تنظیم مقررات که بهتراست مورد تاکید قرارگیرند. (برای جزئیات بیشتر، پیوست ث ملاحظه شود).

۵-۳ یکپارچه سازی مدیریت رخداد امنیت اطلاعات با دیگر خط‌مشی‌ها

۵-۳-۱ مقدمه

یک سازمان بهتراست محتوای مدیریت رخداد امنیت اطلاعات را در خط‌مشی‌های مدیریت امنیت و مخاطره خود در سطح شرکت و همین‌طور در سطوح سامانه، خدمت و شبکه‌ی خاص بگنجاند و این محتوا را با خط‌مشی مدیریت رخداد مرتبط سازد. بهتراست یکپارچه سازی به موارد زیر کمک کند:

الف- توصیف کند چرا مدیریت رخداد امنیت اطلاعات و به ویژه طرح‌واره‌ی گزارش‌دهی و سامان‌دهی رخداد امنیت اطلاعات، مهم است.

ب- نشان دهد تعهد مدیریت ارشد به آماده‌سازی و پاسخگویی درست با رخدادهای امنیت اطلاعات نیاز دارد، یعنی تعهد به طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات.

پ- از وجود سازگاری در سراسر خط‌مشی‌های مختلف اطمینان حاصل کند.

ت- از پاسخگویی سامان‌یافته و آرام با رخدادهای امنیت اطلاعات و در نتیجه کمینه شدن تاثیرات نامطلوب رخدادها اطمینان حاصل کند.

برای راهنمایی درباره ارزیابی مخاطره و مدیریت امنیت اطلاعات استاندارد ISO/IEC 27005:2008 ملاحظه شود.

۵-۳-۲ محتوا

بهتراست هرسازمان خط‌مشی‌های مدیریت امنیت اطلاعات و مخاطره خود در سطح شرکت و خط‌مشی‌های امنیت اطلاعات سامانه، خدمت یا شبکه مشخص را نگهداری و روزآمدی کند. این خط‌مشی‌ها بهتراست به صورت صریح به یک خط‌مشی مدیریت رخداد امنیت اطلاعات شرکت و طرح‌واره‌ی مرتبط ارجاع نمایند.

الف- بهتراست بخش‌های مرتبط به تعهد مدیریت ارشد اشاره نمایند.

ب- بهتراست بخش‌های مرتبط پیرامون خط‌مشی باشند.

پ- بهتراست بخش‌های مرتبط پیرامون فرآیندهای طرح‌واره و زیر ساخت‌های مرتبط باشند.

ت- بهتراست بخش‌های مرتبط پیرامون الزامات آشکارسازی، گزارش‌دهی، ارزیابی و مدیریت رویدادها، رخدادها و آسیب‌پذیری‌های امنیت اطلاعات باشند.

ث- بهتراست بخش‌های مرتبط به دقت کارکنان مسئول صدور مجوز و/یا عهده‌دار عملیات بحرانی را معرفی‌کنند. (برای مثال کارکنان مسئول برون خط کردن[1] یک سامانه اطلاعاتی و یا حتی خاموش کردن[2] آن).

بهتراست در خط‌مشی‌ها الزام به استقرار سازوکارهای بازنگری مناسب گنجانده شود. این سازوکارها بهتراست اطمینان دهد که از اطلاعات حاصله از آشکارسازی، پایش و برطرف کردن رخدادهای امنیت اطلاعات و از رسیدگی به گزارش آسیب‌پذیری‌های امنیت اطلاعات، به عنوان ورودی جهت حصول اطمینان از اثر بخشی مستمر خط‌مشی‌های مدیریت امنیت اطلاعات و مخاطره شرکت و خط‌مشی‌های امنیت اطلاعات سامانه،خدمت یا شبکه‌ی خاص، استفاده می‌شود.

۵-۴ طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات

۵-۴-۱ مقدمه

هدف از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات تهیه مستند مفصل برای توصیف فعالیت‌ها و روش‌های اجرایی رسیدگی به رویدادها، رخدادها و آسیب‌پذیری‌های امنیت اطلاعات و مبادله چنین رویدادها، رخدادها و آسیب‌پذیری‌هایی می‌باشد. طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات زمانی موثر واقع می‌شود که یک رویداد امنیت اطلاعات آشکار و/یا یک آسیب‌پذیری امنیت اطلاعات گزارش شده باشد.

بهتراست هر سازمانی طرح‌واره را یه عنوان یک راهنما برای موارد زیر استفاده نماید:

الف- پاسخگویی با رویدادهای امنیت اطلاعات،

ب- تعیین این که آیا رویدادهای امنیت اطلاعات تبدیل به رخدادهای امنیت اطلاعات می‌شوند،

پ- مدیریت رخدادهای امنیت اطلاعات به سمت یک نتیجه‌گیری،

ت- پاسخگویی با آسیب‌پذیری‌های امنیت اطلاعات،

1- Off-line
2- Shutting down

ث- شناسایی کلی درس‌های آموخته شده و بهبودهایی که در طرح‌واره و/یا در امنیت مورد نیاز هستند، و

ج- اعمال بهبودهای شناسایی شده.

۵-۴-۲ طرف‌های دخیل

بهتراست سازمان اطمینان حاصل نماید که طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات روی تمامی کارکنان و پیمانکاران مرتبط، ارایه کنندگان خدمات **ICT** ، ارایه کنندگان خدمات مخابراتی و شرکت‌های برون‌سپاری تأکید دارد، بنابراین مسئولیت‌های زیر را پوشش می‌دهد:

الف- آشکارسازی و گزارش رویدادهای امنیت اطلاعات (این مسولیت هر کارمند دائمی یا پیمانکار یک سازمان و شرکت‌های آن است)،

ب- ارزیابی و پاسخگویی با رویدادها و رخدادهای امنیت اطلاعات، دخالت در فعالیت‌های آموختن و بهبود امنیت اطلاعات و خود طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، بعد از برطرف کردن رخداد (این مسئولیت اعضای نقطه تماس **(PoC)**[1]، **ISIRT**، مدیریت، کارکنان روابط عمومی و نمایندگان قانونی می‌باشد)، و

پ- گزارش دهی آسیب‌پذیری‌های امنیت اطلاعات (این مسولیت هر کارمند دائمی یا پیمانکار یک سازمان یا شرکت‌های آن است) و رسیدگی کردن به آن‌ها.

همچنین طرح‌واره بهتراست همه کاربران طرف سوم، و رخدادهای امنیت اطلاعات و آسیب‌پذیری‌های مرتبط گزارش‌شده از سازمان‌های طرف سوم و دولت و سازمان‌های تجاری فراهم‌کننده رخداد امنیت اطلاعات و اطلاعات آسیب‌پذیری را در نظر بگیرد.

۵-۴-۳ محتوا

بهتراست هر سازمانی اطمینان حاصل نماید که محتوای مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات حاوی موارد زیر است:

الف- مروری کلی بر خط‌مشی مدیریت رخداد امنیت اطلاعات.

ب- مروری کلی بر کل طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات.

پ- جزئیات فعالیت‌ها، روش‌های اجرایی و اطلاعات، با موارد زیر مرتبط است :

۱- برنامه‌ریزی و آماده‌سازی.

1-Point of Contact (PoC)

i - رویکردی استانداردشده به رده‌بندی و رسته‌بندی رویداد/ رخداد امنیت اطلاعات، جهت افزایش توان به دست آوردن نتایج سازگار است. در هر صورت، بهتراست این تصمیم بر اساس تاثیرات نامطلوب رخداده یا پیش‌بینی شده بر روی عملیات کسب وکار سازمان و راهنمای مرتبط اتخاذ شود.

یادآوری- پیوست پ رویکردی نمونه برای رده‌بندی و رسته‌بندی رخدادها و رویدادهای امنیت اطلاعات را نشان می‌دهد.

ii- یک ساختار استاندارد دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات، که احتمالا قابلیت مقایسه نتایج، بهبود اطلاعات هشدار و فراهم‌کردن یک دید دقیق‌تر از تهدیدات به، و آسیب‌پذیری‌ها از سامانه‌های اطلاعاتی را فراهم نماید.

iii- راهنمایی برای تصمیم‌گیری در مورد اینکه آیا ارجاع به مرجع بالاتر در طی هر فرایند مرتبط الزامی است و توسط چه کسی و با کدام روش‌های اجرایی مرتبط است. براساس راهنمای ارایه شده در مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، هر کس که یک رویداد، رخداد و یا آسیب‌پذیری امنیت اطلاعات را ارزیابی می‌کند، بهتراست بداند که تشدید در چه شرایطی ضروری است و برای چه کسی این تشدید بهتراست انجام شود. به علاوه، شرایط پیش بینی نشده‌ای وجود دارند که تحت آن‌ها این اقدام ممکن است، ضروری باشد. برای مثال اگر یک رخداد امنیت اطلاعات جزئی به درستی سامان‌دهی نشود، می‌تواند به یک موقعیت فوق‌العاده و بحرانی منجر شود یا اگر یک رخداد امنیت اطلاعات جزئی در یک‌هفته پیگیری نشود، می‌تواند به یک رخداد امنیت اطلاعات عمده تبدیل شود. بهتراست راهنما، انواع رویداد و رخداد امنیت اطلاعات، انواع ارجاع به مرجع بالاتر و اینکه چه‌کسی این ارجاع به مرجع بالاتر را اعمال کند، تعریف نماید.

iv- روش‌های اجرایی دنبال شوند برای حصول اطمینان از اینکه تمام فعالیت‌های مدیریت رخداد امنیت اطلاعات در یک برگه مناسب ثبت گردد و تحلیل این برگه‌ها توسط کارکنان تعیین شده انجام می‌شوند.

v- روش‌های اجرایی و سازوکارهایی برای حصول اطمینان از اینکه رژیم کنترل تغییر برای پوشش دادن به ردگیری رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات، و روزآمدکردن گزارش رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات و روزآمدکردن خود طرح‌واره، برقرار شود،

vi- روش‌های اجرایی برای تحلیل امور قانونی امنیت اطلاعات.

vii- روش‌های اجرایی و راهنما درباره‌ی استفاده از سامانه‌های آشکارسازی نفوذ (**IDS**)، برای حصول اطمینان از این که جنبه‌های قانونی و مقرراتی مرتبط مورد تاکید قرارگرفته‌اند. بهتراست راهنما حاوی مبحث مزایا و معایب مراقبت[1] بر فعالیت‌های حمله کننده باشد. اطلاعات بیشتر در مورد **IDS** در استاندارد ملی ایران شماره ۱۸۰۴۳: سال ۱۳۸۸ منظور شده است.

1-Surveillance

viii- راهنما و روش‌های اجرایی مرتبط با سازوکارهای فنی و سازمانی که به‌منظور پیشگیری از وقوع رخداد امنیت اطلاعات و کاهش احتمال وقوع رخدادهای امنیت اطلاعات و برای رسیدگی به رخداد امنیت اطلاعات به وقوع پیوسته مستقر، پیاده‌سازی و بهره‌برداری می‌شوند.

ix- مطلب برای برنامه اطلاع‌رسانی و آموزش مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات.

x- روش‌های اجرایی و مشخصات برای آزمون طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات.

xi- طرح‌واره‌ی ساختار سازمانی برای مدیریت رخداد امنیت اطلاعات.

xii- شرایط مرجع و مسولیت‌های **ISIRT** به صورت کلی، و برای کارکنان عضو.

xiii- اطلاعات تماس مهم.

۲- آشکارسازی و گزارش

i- آشکارسازی و گزارش رویدادهای امنیت اطلاعات (توسط انسان یا وسیله خودکار).

ii- جمع آوری اطلاعات در باره‌ی رویدادهای امنیت اطلاعات.
iii- آشکارسازی و گزارش آسیب‌پذیری‌های امنیت اطلاعات.

iv- ثبت کامل تمام اطلاعات جمع آوری شده در دادگان مدیریت رخداد امنیت اطلاعات.

۳- ارزیابی و تصمیم‌گیری

i- نقطه تماس **(PoC)** ارزیابی‌های رویداد امنیت اطلاعات (ازجمله ارجاع به مرجع بالاتر بر حسب نیاز) را، با استفاده از مقیاس مورد توافق رده‌بندی رویداد/رخداد /آسیب‌پذیری امنیت اطلاعات (شامل تعیین اثرهای رویدادها براساس دارایی‌ها/خدمات آسیب‌دیده) و تصمیم‌گیری درمورد ضرورت رده‌بندی رویدادها به عنوان رخداد امنیت اطلاعات، اجرا می‌کند.

ii- بهتراست **ISIRT** رویدادهای امنیت اطلاعات را ارزیابی و تایید کند که آیا یک رویداد، یک رخداد امنیت اطلاعات است یا خیر، و سپس بهتراست ارزیابی دیگری با استفاده از مقیاس توافق شده رده‌بندی رویداد/رخداد امنیت اطلاعات، برای تایید جزئیات نوع رویداد (رخداد بالقوه) و منبع آسیب‌دیده (رسته‌بندی) اجرا شود. بهتراست این کار از طریق اتخاذ تصمیماتی درباره‌ی اینکه رخداد امنیت اطلاعات تایید شده چگونه، توسط چه کسی و با چه اولویتی رسیدگی شود، همین‌طور سطوح ارجاع به مرجع بالاتر، دنبال شود.

iii- ارزیابی آسیب‌پذیری‌های امنیت اطلاعات (که هنوز به‌عنوان عامل بالقوه رویدادهای امنیت اطلاعات و یا رخداد امنیت اطلاعات بهره‌برداری نشده‌اند)، با اخذ تصمیماتی درباره‌ی اینکه بهتراست به چه چیزی، توسط چه کسی، چگونه و با چه اولویتی رسیدگی شود.

iv- ثبت کامل تمامی نتایج ارزیابی و تصمیمات مرتبط در دادگان مدیریت رخداد امنیت اطلاعات.

۴- پاسخگویی‌ها

i- بازنگری توسط **ISIRT** جهت تعیین اینکه آیا رخداد امنیت اطلاعات تحت کنترل است، و

- در صورتی که رخداد تحت کنترل باشد، پاسخگویی مورد نیاز را یا به سرعت (در زمان واقعی یا نزدیک به زمان واقعی) یا بصورت تاخیری به جریان بیاندازید ،

- در صورتی که رخداد تحت کنترل نبوده و یا تاثیر شدیدی بر روی خدمات اصلی سازمان می‌گذارد، فعالیت‌های بحران را از طریق ارجاع به مرجع بالاتر، برای ساماندهی بحران تحریک نمائید.

ii- تعریف نقشه ای از تمام کارکردهای داخلی و خارجی و سازمان‌هایی که بهتراست در طی مدیریت یک رخداد دخیل باشند.

iii- اجرای تحلیل امور قانونی امنیت اطلاعات، بر حسب نیاز.

iv- ارجاع به مرجع بالاتر، بر اساس یک نیاز.

v- حصول اطمینان از اینکه تمام فعالیت‌های دخیل، برای تحلیل در آینده به درستی ثبت شده‌اند.

vi- حصول اطمینان از اینکه شواهد الکترونیکی، گردآوری و با امنیت قابل اثباتی ذخیره می‌شوند.

vii- حصول اطمینان از اینکه رژیم کنترل تغییر حفظ می‌شود، و در نتیجه دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات به صورت روزآمد نگهداری می‌شود.

viii- در مورد وجود رخداد امنیت اطلاعات یا دیگر جزئیات مرتبط با آن، به دیگر اشخاص یا سازمان‌های داخلی و خارجی اطلاع‌رسانی می‌شود.

ix- رسیدگی به آسیب‌پذیری‌های امنیت اطلاعات

x- همین‌که به رخداد با موفقیت رسیدگی شد، آنرا به طور رسمی بسته و در دادگان مدیریت رخداد امنیت ثبت می‌نمائیم.

بهتراست هر سازمان اطمینان حاصل نماید که مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، به پاسخگویی‌های رخداد امنیت اطلاعات بصورت بلند مدت و سریع اجازه می‌دهد. بهتراست تمامی رخدادهای امنیت اطلاعات، برای اندازه‌گیری اثرهای نامطلوب بالقوه بر عملیات کسب و کار، بصورت کوتاه مدت و بلند مدت، تحت ارزیابی قرار بگیرند (به عنوان مثال یک فاجعه عمده می‌تواند مدتی پس از یک رخداد اولیه امنیت اطلاعات به وقوع بپیوندد). به‌علاوه در جایی که کنترل‌های موردی ضروری است، این کار بهتراست به بعضی پاسخگویی‌های لازم برای رخدادهای امنیت اطلاعات کاملا پیش بینی نشده، اجازه دهد. حتی برای این موقعیت، سازمان‌ها بهتراست راهنمایی‌های کلی را در باره‌ی گام‌هایی که ممکن است ضروری باشند، در مستند طرح‌واره در نظر بگیرند.

۵- درس‌های آموخته‌شده

i- اجرای تحلیل امور قانونی امنیت اطلاعات، بر حسب نیاز.

ii- شناسایی درس‌های آموخته شده از رخدادها و آسیب‌پذیری‌های امنیت اطلاعات.

iii- بازنگری، شناسایی و بهبودبخشیدن به پیاده‌سازی کنترل امنیت اطلاعات (کنترل‌های جدید و یا روزآمدشده)، همین‌طور خط‌مشی مدیریت رخداد امنیت، به عنوان نتیجه‌ی درس‌های آموخته‌شده.

iv- بازنگری و شناسایی و در صورت امکان بهبودبخشیدن به نتایج بازنگری و ارزیابی و مدیریت مخاطره امنیت اطلاعات موجود سازمان، به عنوان درس‌های آموخته‌شده.

v- بازنگری چگونگی فرایندها، روش‌های اجرایی ، قالب‌های گزارش‌دهی و/یا ساختار سازمانی در پاسخگویی با ارزیابی و بازیابی هر رخداد امنیت اطلاعات و رسیدگی به آسیب‌پذیری‌های امنیت اطلاعات و شناسایی و بهبودبخشیدن به طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات و مستندسازی آن بر اساس درس‌های آموخته‌شده.

vi- روزآمد کردن دادگان رویداد/ رخداد/ آسیب‌پذیری امنیت اطلاعات.

vii- مبادله و به اشتراک‌گذاری نتایج بازنگری با جامعه‌ای مورد اعتماد (چنانچه سازمان چنین بخواهد).

۵-۴-۴ روش‌های اجرایی

پیش از آمادگی برای آغاز عملیات طرح‌واره‌ی مدیریت رخداد امنیت، مسئله مهم این است که سازمان در دسترس بودن روش‌های اجرایی را مستند و وارسی کرده باشد. بهتراست هر روش اجرایی ، گروه‌ها یا کارکنانی را که مسئول استفاده و مدیریت آن هستند، متناسب با **PoC** و/یا **ISIRT** مشخص کند. بهتراست چنین روش‌های اجرایی اطمینان دهند که شواهد الکترونیکی به صورت امن گردآوری و ذخیره شده‌اند و حفاظت امن، برای پیگیری قانونی و یا اقدام انضباطی داخلی مورد نیاز، به طور مستمر پایش می‌شود. به

علاوه بهتراست روش‌های اجرایی مستند شده که نه تنها فعالیت‌های **PoC** و **ISIRT**، بلکه کارکنانی را که درتحلیل امور قانونی امنیت اطلاعات و فعالیت‌های بحران دخیل هستند - در صورتی که در جای دیگری پوشش داده نشده باشند - پوشش دهد، برای مثال در یک برنامه استمرار کسب و کار یا یک برنامه مدیریت بحران. بهتراست روش‌های اجرایی مستند شده، به طور کامل با مستند خط‌مشی مدیریت رخداد امنیت اطلاعات و دیگر مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات هماهنگ باشند.

درک این مسئله که تمامی روش‌های اجرایی نباید در دسترس عموم قرارگیرند، مهم است. برای مثال، لازم نیست همه‌ی کارکنان سازمانی، تمامی عملیات داخلی یک **ISIRT** را برای تعامل با آن درک کنند. بهتراست **ISIRT** اطمینان حاصل کند که راهنمای قابل‌دسترس عموم، ازجمله اطلاعات حاصل از تحلیل رخداد امنیت اطلاعات، در برگه‌ای که به آسانی قابل دسترسی است، برای مثال، در شبکه‌ی داخلی[1] سازمان، وجود دارد. نگهداری محرمانه‌ی برخی جزئیات طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، برای پیش‌گیری از دستکاری فرایند رسیدگی توسط کارمندان داخلی، نیز ممکن است مهم باشد. برای مثال، چنانچه کارمند بانکی که اقدام به اختلاس پول میکند از برخی جزئیات شما آگاه باشد، ممکن است بهتر بتواند این فعالیت‌ها را از بررسی کنندگان مخفی کرده و یا به نحوی دیگر در آشکارسازی، رسیدگی و بازیابی یک رخداد امنیت اطلاعات مانع ایجاد کند.

محتوای روش‌های اجرایی عملیاتی بستگی دارد به تعداد معیار، به ویژه معیارهای بالقوه شناخته‌شده مرتبط با ماهیت رویدادها، رخدادها و آسیب‌پذیری‌های امنیت اطلاعات و انواع دارایی‌های سامانه اطلاعاتی که ممکن است دخیل باشند و محیط آن‌ها. بنابراین یک روش اجرایی عملیاتی می‌تواند با نوع ویژه‌ای از رخداد یا محصول (برای مثال دیواره‌های آتش، دادگان‌ها، سامانه‌های عامل، برنامه‌های کاربردی) یا با محصول مشخصی، مرتبط باشد. بهتراست هر روش اجرایی عملیاتی گام‌هایی را که باید برداشته شوند و فرد مسئول آن‌را به دقت شناسایی نماید. بهتراست این روش اجرایی تجربه حاصل از منابع خارجی (مانند دولت، **ISIRT**های تجاری یا مشابه آن‌ها و تامین‌کنندگان) و همین‌طورمنابع داخلی را منعکس نماید.

برای رسیدگی به انواع رویدادها و رخدادها و همین‌طور آسیب‌پذیری‌های امنیت اطلاعات که از قبل شناخته شده‌اند، بهتراست روش‌های اجرایی عملیاتی وجودداشته باشند. بهتراست روش‌های اجرایی عملیاتی هم برای انواع ناشناخته رویداد، رخداد یا آسیب‌پذیری امنیت اطلاعات، وجود داشته باشد. بهتراست در این مورد بر مسائل زیر تأکید شود:

الف- فرایند گزارش‌دهی برای سامان‌دهی این گونه استثنائات مشخص شود،

ب- به منظور اجتناب از هر گونه تاخیر در پاسخگویی، راهنما در مورد زمان‌بندی دریافت مصوبه از مدیریت تهیه شود، و

1- Intranet

پ- هیأتی از قبل تشکیل شود که مجاز باشد بدون رعایت فرایند عادی تصویب، تصمیم‌گیری نماید.

۵-۴-۵ اعتماد

گروه **ISIRT** نقش حیاتی در امنیت کلی یک سازمان ایفا می‌کند. گروه **ISIRT** برای آشکارکردن، برطرف کردن‌کردن و رسیدگی به رخدادهای امنیت اطلاعات به همکاری همه‌ی کارکنان سازمان نیاز دارد. این‌که **ISIRT** در داخل و خارج از سازمان مورد اعتماد همه باشد، امری بنیادی است. پذیرش بی‌نامی[1]، در زمینه گزارش آسیب‌پذیری‌ها، رویدادها و رخدادهای امنیت اطلاعات ممکن است برای اعتمادسازی مفید باشد.

بهتراست سازمان اطمینان حاصل کند که طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات آن بر موقعیت‌هایی تاکید می‌کند که در آن موقعیت‌ها حصول اطمینان از بی‌نامی شخص یا طرفی[2] که رخدادها یا آسیب‌پذیری‌های امنیت اطلاعات را تحت شرایط مشخصی گزارش می‌کند، مهم است. بهتراست هر سازمانی مقرراتی[3] داشته باشد که به روشنی انتظار خود از بی‌نامی، یا عدم آن را، برای کارکنان یا طرف‌هایی که یک رخداد یا آسیب‌پذیری امنیت اطلاعات را گزارش می‌کنند، توضیح دهد. ممکن است **ISIRT** نیاز به کسب اطلاعات بیشتری داشته باشد که در ابتدا توسط شخص یا طرف گزارش‌دهنده رخداد اعلان نشده باشد. علاوه بر این، اطلاعات مهم در باره‌ی خود رخداد یا آسیب‌پذیری امنیت اطلاعات ممکن است از فردی که ابتدا آن را آشکار می‌کند، به‌دست آید.
یک رویکرد دیگر که ممکن است توسط **ISIRT** پذیرفته شود، جلب اعتماد کاربران از طریق فرآیندهای شفاف و کامل است. بهتراست **ISIRT** برای آموزش کاربران، تشریح چگونگی کار خود، چگونگی محرمانه نگه داشتن اطلاعات جمع‌آوری شده و چگونگی مدیریت گزارشاتی رویداد، رخداد و آسیب‌پذیری کاربران، تلاش کند.

بهتراست **ISIRT** قابلیت تامین نیازهای کارکردی، مالی، قانونی، و سیاسی سازمان را به صورت کارآمد داشته باشد و هنگام مدیریت آسیب‌پذیری‌ها و رخدادهای امنیت اطلاعات، بتواند صلاحدید سازمان را درنظربگیرد. برای تائید اینکه تمام الزامات کسب‌وکار به طور موثر تأمین شده‌اند، بهتراست کارکرد **ISIRT** به صورت مستقل نیز مورد ممیزی قرار گیرد.

یک روش خوب برای دست‌یابی به جنبه دیگری از استقلال، جدا سازی زنجیره‌ی گزارش رخداد و آسیب‌پذیری، از مدیریت خط عملیات و گماردن یک مدیر ارشد برای اداره مستقیم پاسخگویی با رخداد و آسیب‌پذیری است. بهتراست به منظور اجتناب از نفوذ نا خواسته، امور مالی تفکیک شود.

1- Anonymity
2- Party
3-Provisions

۵-۴-۶ محرمانگی

یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات ممکن است حاوی اطلاعات حساس باشد، و ضروری است اشخاص دخیل در پرداختن به رخدادها و آسیب‌پذیری‌ها، اطلاعات حساس را سامان‌دهی کنند. بهتراست یک سازمان اطمینان حاصل کند که فرآیندهای لازم برای بی‌نام‌کردن اطلاعات حساس مستقر و امضای موافقت‌نامه‌ی محرمانگی توسط کارکنانی که به اطلاعات حساس دسترسی دارند الزامی می‌شود. اگر اطلاعات امنیت رویدادها/رخدادها/آسیب‌پذیری‌ها توسط یک سامانه‌ی تعمیم‌یافته مدیریت حل مشکل[1] ثبت شود، می‌توان برخی جزئیات حساس را حذف نمود. علاوه بر این، یک سازمان بهتراست اطمینان حاصل کند که طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، برای کنترل مبادله رخدادها و آسیب‌پذیری‌ها با طرف‌های خارجی ، از جمله رسانه‌ها، شرکای کسب‌وکار، مشتریان، سازمان‌های مجری قانون و عموم جامعه، مقرراتی ایجاد خواهد کرد.

۵-۵ استقرار ISIRT

۵-۵-۱ مقدمه

هدف از ایجاد ISIRT، ایجاد قابلیت ارزیابی، پاسخگویی با و آموختن از رخدادهای امنیت اطلاعات، و فراهم سازی هماهنگی، مدیریت، بازخورد و ارتباط لازم در سازمان است. یک ISIRT، در کاهش خسارت فیزیکی و مالی و همینطور کاهش صدمه به وجهه‌ی سازمان که گاهی مرتبط با رخداد امنیت اطلاعات است، مشارکت می‌کند.

۵-۵-۲ اعضا و ساختار

بهتراست اندازه، ساختار و ترکیب ISIRT مناسب با اندازه، ساختار و ماهیت کسب‌وکار سازمان باشد. اگر چه ISIRT ممکن است از یک گروه یا اداره مجزا تشکیل گردد، اعضا مجازند در سایر وظایف سهیم باشند و این امر مشارکت اعضای گستره‌ای از حوزه‌های درون سازمان را جلب خواهد کرد. بهتراست سازمان ارزشیابی کند که آیا به یک گروه اختصاصی، یک گروه مجازی و یا ترکیبی از هردوی این‌ها نیاز دارد. تعداد رخدادها و فعالیت‌های انجام شده توسط ISIRT، سازمان را در این انتخاب راهنمایی می‌کند.

گروه ISIRT، مراحل مختلف بلوغ را طی می‌کند و اغلب اصلاحات مدل سازمانی بر اساس سناریوی مشخصی پیش روی سازمان پذیرفته می‌شود. هرگاه اصلاح شد، وجود یک گروه دائمی به رهبری یک مدیر ارشد، توصیه می‌شود. گروه‌های مجازی ISIRT، ممکن است توسط یک مدیر ارشد رهبری شوند. مدیر ارشد بهتراست توسط کارکنانی پشتیبانی شود که در موضوعات ویژه تخصص دارند، برای مثال در سامان‌دهی حملات کدهای مخرب، که بر اساس نوع رخداد امنیت اطلاعات مورد نظر، فرا خوانده می‌شوند. بسته به

1- a generalized problem management system

اندازه، ساختار و ماهیت کسب و کار سازمان، ممکن است یک عضو، بیش از یک نقش را در ISIRT ایفا کند. ممکن است ISIRT از کارکنانی از قسمت‌های مختلف سازمان (برای مثال فعالیت‌های کسب و کار، ICT، ممیزی، منابع انسانی و بازاریابی) تشکیل شود. این موضوع همچنین در ISIRTهای دائمی کاربرد دارد؛ حتی در صورت وجود کارکنان ویژه، ISIRT همواره نیاز به پشتیبانی سایر ادارات دارد.

بهتراست اعضای گروه برای تماس در دسترس باشند، بنابراین بهتراست اسامی و جزئیات تماس هر عضو و اعضای جایگزین آن‌ها در سازمان در دسترس باشد. جزئیات لازم بهتراست به روشنی در مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، و نه در بیانیه‌های خط‌مشی، نشان داده شوند و شامل مستندات روش‌های اجرایی و برگه‌های گزارش دهی باشند.

مدیر ISIRT معمولا بهتراست یک خط جداگانه گزارش دهی به مدیریت ارشد داشته باشد، جدا از عملیات عادی کسب‌وکار. او برای اتخاذ تصمیمات فوری در خصوص رسیدگی به یک رخداد، بهتراست قدرت تفویض اختیار داشته باشد، و بهتراست اطمینان داشته باشد که همه‌ی اعضای ISIRT دارای سطوح دانش و مهارت لازم بوده و این کار قراراست استمرار یابد. بهتراست مدیرISIRT رسیدگی به هر رخداد را بر عهده‌ی مناسب ترین عضو گروه خود بگذارد و برای هر رخداد یک مدیر مشخص تعیین شود.

۵-۵-۳ رابطه با سایر قسمت‌های سازمان

بهتراست ISIRT مسئولیت ایجاد اطمینان برای برطرف کردن رخدادها را داشته باشد، ودر این مقوله مدیر ISIRT و اعضای گروه او بهتراست تا حدودی دارای اختیار لازم برای عملیات مورد نیاز پاسخگویی با رخدادهای امنیت اطلاعات که مناسب به نظر می‌رسند، باشد. در هر صورت، عملیاتی که ممکن است بر کل سازمان تاثیرهای نامطلوب داشته باشند، یا مالی یا از نظر شهرت، بهتراست با موافقت مدیر ارشد انجام شوند. به همین علت، لازم است که طرح‌واره و خط‌مشی مدیریت رخداد امنیت اطلاعات به تفصیل اختیارات مناسبی را که مدیر ISIRT رخدادهای امنیت اطلاعات جدی اعلام می‌کند، بیان نماید.

همچنین بهتراست روش‌های اجرایی و مسئولیت‌های رسیدگی به رسانه‌ها با موافقت مدیریت ارشد باشد و مستند شود. بهتراست این روش‌های اجرایی مشخص کند که چه کسی در سازمان به درخواست‌های رسانه‌ها رسیدگی و آن قسمت از سازمان چگونه با ISIRT تعامل می‌کند.

۵-۵-۴ رابطه با طرف‌های ذی‌نفع خارجی

سازمان‌ها بهتر است روابط بین ISIRT با طرف‌های ذی‌نفع مناسب خارجی ، برقرار سازند.

طرف‌های ذی‌نفع خارجی ممکن است شامل موارد زیر باشند:

الف- کارکنان پشتیبانی بیرونی قراردادی [کارکنان شرکتی]

ب- ISIRTهای برون سازمانی

پ- ارایه‌کنندگان خدمات مدیریت شده، شامل ارایه‌کنندگان خدمات مخابراتی، ارائه‌کنندگان خدمات اینترنتی (ISP)[1] و دیگر تامین‌کنندگان،

ت- سازمان‌های مجری قانون،

ث- مقامات امداد[2]

ج- سازمان‌های دولتی مربوط،

چ- کارکنان حقوقی،

ح- مسئولین روابط عمومی و/یا اعضای رسانه،

خ- شرکای کسب‌وکار،

د) مشتریان، و

ذ) عموم جامعه.

۵-۶ پشتیبانی فنی ودیگر پشتیبانی‌ها (از جمله پشتیبانی عملیاتی)

جهت حصول اطمینان از این که پاسخگویی‌های سریع و کارآمد با امنیت اطلاعات محقق می‌گردد، یک سازمان بهتراست همه‌ی وسایل پشتیبانی فنی و دیگر پشتیبانی‌های لازم را آماده و آن‌ها را آزمایش کند. این کار شامل موارد زیر می‌شود:

الف- دستیابی به جزئیات دارایی‌های سازمان با یک ثبت روزآمد دارایی‌ها و اطلاعات درمورد پیوندهای مربوط به کارکردهای کسب‌وکار،

ب- دستیابی به روش‌های اجرایی مستند مرتبط با مدیریت بحران،

پ- فرآیندهای ارتباطات گسترده و مستند شده ،

ت- استفاده از یک دادگان امنیت اطلاعات درمورد رویداد/رخداد/آسیب‌پذیری و وسایل فنی جهت گردآوری و روزآمدکردن سریع دادگان، تحلیل اطلاعات آن و تسهیل پاسخگویی‌ها (در بعضی موارد، ممکن است ثبت‌های دستی مورد نیاز یک سازمان باشد)، با دادگانی که به صورت قابل اثبات، امن نگه داشته می‌شود،

1- Internet Service Providers
2- Emergency authorities

ث- تسهیلات برای جمع‌آوری و تحلیل شواهد امور قانونی امنیت اطلاعات، و

ج- مقدمات کافی در زمینه مدیریت بحران برای دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات (برای راهنمایی در مورد مدیریت استمرار کسب‌وکار استاندارد ISO/IEC 27031 ملاحظه شود).

یک سازمان بهتراست اطمینان حاصل کند که وسایل فنی که جهت گردآوری و روزآمدکردن سریع دادگان، تحلیل اطلاعات خود و تسهیل پاسخگویی با رخدادهای امنیت اطلاعات استفاده می‌شوند، موارد زیر را پشتیبانی می‌کنند:

چ- دریافت سریع گزارش‌های رویداد/رخداد/ آسیب‌پذیری امنیت اطلاعات،

ح- معرفی کارکنان خارجی ازپیش انتخاب شده با وسایل مناسب (برای مثال با رایانامه، دورنگار یا تلفن)، بنابراین نیاز به نگهداری یک دادگان تماس قابل اطمینان، سریعا قابل دستیابی (شامل کاغذ و دیگر پشتیبان‌ها) و تسهیل در انتقال اطلاعات به افراد به صورت امن در جای مناسب،

خ- اقدامات احتیاطی متناسب همراه با مخاطرات ارزیابی شده به منظور اطمینان از اینکه ارتباط الکترونیکی، اینترنتی یا غیر اینترنتی، نمی‌توانند استراق سمع شوند و مادامی‌که سامانه، خدمت و یا شبکه تحت حمله است، قابل دستیابی است (این ممکن است نیاز به کاربرد مناسب سازوکارهای ارتباطی جایگزین از قبل برنامه‌ریزی شده باشد)،

د- اطمینان از جمع‌آوری همه‌ی داده‌ها درباره‌ی سامانه اطلاعاتی، خدمت و/یا شبکه، و همه اطلاعات پردازش شده.

ذ- استفاده از کنترل یکپارچه‌ی رمزنگاری[1] برای کمک به تعیین اینکه آیا سامانه، خدمت و/یا شبکه تغییر یافته و متناسب با مخاطرات ارزیابی شده، کدام قسمت‌ها و چه داده‌هایی تغییر یافته است،

ر- تسهیل بایگانی و ایمنی اطلاعات جمع‌آوری شده (برای مثال، ازطریق کاربرد امضاهای دیجیتال برای سوابق[2] و سایر شواهد، قبل از اینکه به‌صورت برون‌خط در رسانه فقط خواندنی مانند حافظه فقط خواندنی لوح فشرده[3] و لوح فشرده تصویری دیجیتالی[4] ذخیره شوند)

ز- فراهم‌کردن وسیله آماده سازی خروجی‌های چاپی (مانند سوابق)، ازجمله خروجی‌هایی که پیشرفت یک رخداد و فرایند برطرف کردن و زنجیره‌ی حفاظت[5] را نشان می‌دهد.

1- Cryptographic
2- Logs
3- Compact Disc (CD)
4- Digital Video Disk (DVD)
5- Chain of custody

س- بازیابی سامانه اطلاعات، خدمت و/یا شبکه برای فعالیت عادی با روش‌های اجرایی زیر که هماهنگ با مدیریت بحران مرتبط می‌باشند:

۱- آزمونهای پشتیبان،

۲- کنترل کدهای خرابکار،

۳- رسانه‌ی اصلی با نرم‌افزار سامانه و برنامه‌کاربردی،

۴- رسانه‌ی قابل راه‌اندازی[1]، و

۵- وصله‌های پاک، قابل اطمینان و روزآمد سامانه‌ها و برنامه‌های کاربردی.

ایجاد یک تصویر استاندارد پایه از رسانه نصب و استفاده از آن تصویر به عنوان یک مبنای پاک برای سامانه‌های ایجادکننده روز به روز در سازمان‌ها عمومی می‌شود. استفاده از چنین تصویری بجای رسانه‌ی اصلی اغلب ترجیح داده‌می‌شود زیرا این تصویر از پیش اصلاح، مستحکم و آزمایش و غیره، گردیده است.

ممکن است یک سامانه، خدمت یا شبکه اطلاعات که مورد حمله واقع شده، کارکرد درستی نداشته باشد. بنابراین برای پاسخگویی با یک رخداد امنیت اطلاعات تا حد امکان، هیچگونه وسایل فنی (نرم‌افزار یا سخت‌افزار) لازم نیست و بهتراست به عملیات آن‌ها در «مسیر اصلی»[2] سامانه‌ها، خدمات و/یا شبکه‌های سازمان متناسب با مخاطرات ارزیابی شده، تکیه شود. بهتراست همه‌ی این وسایل به‌طور دقیق انتخاب، به درستی پیاده‌سازی و به‌طور منظم آزمایش گردند (ازجمله آزمون پشتیبان‌های ایجادشده). در صورت امکان، بهتراست این وسایل فنی کاملا مستقل باشند.

یادآوری- وسایل فنی توصیف شده در این بند شامل وسایل فنی که به طور مستقیم برای آشکارسازی رخدادهای امنیت اطلاعات و ورودهای غیرمجاز و برای اعلام خودکار اشخاص مناسب استفاده می‌شوند، نیستند. چنین وسایل فنی در استاندارد ملی ایران شماره ۱۸۰۴۳: سال ۱۳۸۸توصیف گردیده است.

در حالی که PoC سازمان نقش بسیار روان‌تری برای تامین پشتیبانی تمام جنبه‌های IT و سامان‌دهی اطلاعات مرتبط در سازمان ایفا می‌کند، نقش کلیدی در مدیریت رخداد امنیت اطلاعات دارد. هنگامی که رویدادهای امنیت اطلاعات برای اولین بار گزارش می‌شود، PoC در مرحله آشکارسازی و گزارش رویداد به آن‌ها رسیدگی می‌کند. بهتراست PoC اطلاعات گردآوری شده را بازیابی کرده و ارزیابی اولیه را در مورد اینکه آیا رویدادها تحت عنوان رخدادها رده‌بندی شوند یا خیر، انجام دهد. درصورتی که یک رویداد به عنوان یک رخداد رده‌بندی نشود، بهتراست PoC آن را برحسب مورد رسیدگی کند. اگر رویداد به عنوان یک رخداد

1- Bootable
2- Mainstream

رده‌بندی شود، ممکن است PoC به آن رسیدگی کند، البته در بیشتر موارد انتظار می‌رود که مسئولیت رسیدگی به یک رخداد، به ISIRT سپرده شود. انتظار نمی رود کارکنان PoC، کارشناسان امنیت باشند.

۵-۷ اطلاع‌رسانی و آموزش

مدیریت رخداد امنیت اطلاعات فرآیندی است که نه تنها وسائل فنی، بلکه اشخاص را نیز دربر می‌گیرد. بنابراین بهتراست توسط افرادی که در سازمان به طورمناسبی از امنیت اطلاعات مطلع و آموزش دیده هستند، پشتیبانی گردد.

آگاهی و مشارکت تمامی کارکنان سازمان برای موفقیت یک رویکرد مدیریت ساختاریافته‌ی رخداد امنیت اطلاعات حیاتی است. در حالی که توصیه میشود کاربران ملزم به شرکت شوند، در صورتی که نسبت به چگونگی مزایای مشارکت در یک رویکرد مدیریت ساختاریافته‌ی رخداد امنیت اطلاعات برای خود و ادارات خود ناآگاه باشند، احتمال کمتری دارد که به‌طور موثری در این عملیات شرکت نمایند. به علاوه، کارآیی عملیاتی و کیفیت یک رویکرد ساختاریافته‌ی مدیریت رخداد امنیت اطلاعات به چند عامل بستگی دارد ازجمله تعهد در اعلام رخدادها، کیفیت اعلام، سهولت استفاده، سرعت و آموزش. بعضی از این عوامل به داشتن اطمینان از اینکه کاربران از ارزش مدیریت رخداد امنیت اطلاعات آگاه بوده و انگیزه گزارش‌کردن درمورد این رخدادها را دارند، مربوط می‌شوند.

بهتراست سازمان اطمینان حاصل کند که نقش مدیریت رخداد امنیت اطلاعات به عنوان بخشی از برنامه‌ی اطلاع‌رسانی و آموزشی شرکت درباره‌ی امنیت اطلاعات به‌صورت فعال ارتقاء یافته است.برنامه‌ی اطلاع‌رسانی و مطالب مرتبط بهتراست در دسترس همه‌ی کارکنان قرار گیرند، از جمله کارکنان جدید، کاربران طرف سوم و پیمانکاران درصورت مرتبط بودن. بهتراست یک برنامه‌ی آموزشی مشخصی برای اعضای ISIRT و PoC، کارکنان امنیت اطلاعات و مدیران اداری[1] مشخصی برحسب نیاز وجودداشته‌باشد. هر گروه از اشخاص که به‌طور مستقیم در مدیریت رخدادها دخیل هستند، ممکن است بر حسب نوع، بسامد و حیاتی بودن تعامل آن‌ها با طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، نیازمند سطوح متفاوتی از آموزش باشند.

برنامه‌ی توجیهی اطلاع‌رسانی[2] سازمان، بهتراست موارد زیر را دربر داشته باشد :

الف- مزایایی که از یک رویکرد ساختار یافته به مدیریت رخداد امنیت اطلاعات، هم برای سازمان و هم کارکنان آن حاصل می‌شود،

ب- طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات چگونه کار می‌کند، ازجمله حوزه آن وگردش کار مدیریت رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات،

1- Administrators
2- awareness briefings

پ- چگونه رویدادها، رخدادها و آسیب‌پذیری‌های امنیت اطلاعات راگزارش داد،

ت- نگهداری اطلاعات و خروجی‌های دادگان رویداد/رخداد/ آسیب‌پذیری امنیت اطلاعات،

ث- کنترل‌های مرتبط با محرمانگی منابع اطلاعات،

ج- موافقت‌های سطح خدمات طرح‌واره ،

چ- اعلام خروجی‌ها - منابع اطلاعاتی تحت چه شرایطی توصیه شده‌اند،

ح- هر گونه محدودیت‌های تحمیلی توسط موافقت‌نامه‌های غیر قابل افشا،

خ- مقام قانونی مدیریت رخداد امنیت اطلاعات سازمان و خط گزارش‌دهی آن، و

د- چه کسی گزارشات طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات را دریافت می‌کند و چگونه این گزارشات توزیع می‌شوند.

در بعضی موارد، ممکن است گنجاندن جزئیات برنامه اطلاع‌رسانی، به خصوص درباره‌ی مدیریت رخداد امنیت اطلاعات در دیگر برنامه‌های آموزشی برای سازمان مطلوب باشد (برای مثال، برنامه‌های توجیهی کارکنان یا برنامه‌های اطلاع‌رسانی امنیت کل شرکت). این رویکرد اطلاع‌رسانی می‌تواند محتوای ارزشمندی مرتبط با گروههای ویژه اشخاص ارایه داده و اثربخشی و بازدهی برنامه آموزش را بهبود بخشد.

قبل از عملیاتی شدن طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، بهتراست سازمان اطمینان حاصل کند که تمامی کارکنان دخیل با روش‌های اجرایی مرتبط با آشکارسازی و گزارش رویدادهای امنیت اطلاعات آشنا بوده و کارکنان منتخب دارای معلومات زیادی درباره فعالیت‌های بعدی هستند. این کار بهتراست با دوره‌های توجیهی اطلاع‌رسانی و آموزشی منظم پیگیری شود. آموزش‌ها بهتراست ازطریق تمرین‌ها و آزمون‌های مشخص برای اعضایPoC و ISIRT، و کارکنان امنیت اطلاعات و مدیران اداری مشخص پشتیبانی گردد.

به‌علاوه، به منظور کمینه‌کردن تاخیر در گزارش‌دهی و سامان‌دهی رویدادها، رخدادها وآسیب‌پذیری‌های امنیت اطلاعات، بهتراست برنامه‌های اطلاع‌رسانی و آموزشی ازطریق استقرار و عملیاتی کردن پشتیبانی از کارکنان مدیریت رخداد امنیت اطلاعات، تکمیل شوند.

۸-۵ آزمودن طرح‌واره

بهتراست سازمان جهت برجسته‌کردن مشکلات و معایب بالقوه‌ای که ممکن است در حین مدیریت رویدادها و رخدادها و آسیب‌پذیری‌های امنیت اطلاعات بروز کنند، وارسی و آزمون منظمی از فرآیندها و روش‌های اجرایی مدیریت رخدادهای امنیت اطلاعات را زمانبندی کند. بهتراست آزمونهای ادواری برای وارسی

فرآیندها/ روش‌های اجرایی را سازمان‌دهی و چگونگی پاسخگویی ISIRT با رخدادهای پیچیده شدید از طریق شبیه‌سازی حملات، شکست‌ها یا نواقص واقعی درستی‌سنجی کند. بهتراست توجه ویژه به ایجاد سناریوهای شبیه‌سازی که توصیه می‌شود مبتنی بر تهدیدات واقعی امنیت اطلاعات باشند، به عمل‌آید. بهتراست این آزمونها نه تنها ISIRT، بلکه همه‌ی سازمان‌های داخلی و خارجی دخیل در مدیریت رخدادهای امنیت اطلاعات را دربر داشته باشد. بهتراست سازمان‌ها اطمینان حاصل کنند که هر تغییری که در نتیجه‌ی بازیابی‌های پس از آزمون ایجاد شود باید قبل از این که طرح‌واره‌ی تغیر یافته اجرا شود، مورد وارسی کامل، ازجمله آزمون بیشتر، قرار گیرد.

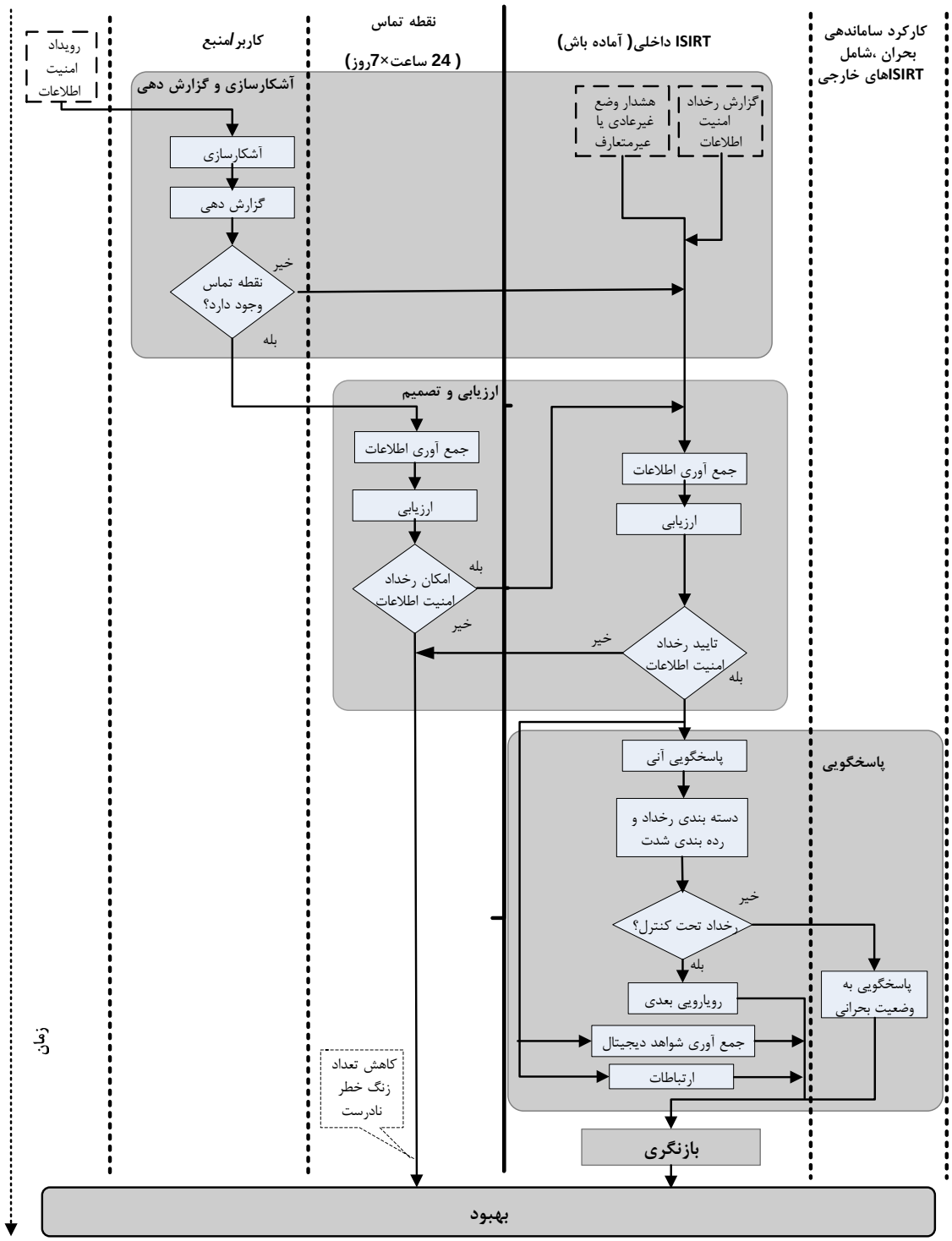
۶ مرحله‌ی آشکارسازی و گزارش‌دهی

۶-۱ مرور کلی فعالیت‌های کلیدی

اولین مرحله‌ی استفاده عملیاتی از یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، شامل آشکارسازی ، جمع آوری اطلاعات مرتبط با، و گزارش وقوع رویدادهای امنیتی و وجود آسیب‌پذیری‌های امنیت اطلاعات توسط کارکنان یا وسایل خودکار است. مدیریت رخدادهای امنیت اطلاعات در عمل از سه مرحله‌ی اصلی تشکیل می‌شود: مراحل آشکارسازی و گزارش دهی، ارزیابی و تصمیم گیری (بند ۷ ملاحظه شود) و پاسخگویی‌ها (بند ۸ ملاحظه شود). این مراحل با مرحله‌ی درس‌های آموخته‌شده دنبال می‌شود (بند ۹ ملاحظه شود) مرحله‌ای که بهبودها شناسایی و اعمال می‌شوند. این مراحل و فعالیت‌های مرتبط به آن‌ها در بند ۴- ۵ معرفی شده‌اند.

بندهای بعدی ترجیحا بر سامان‌دهی رویدادها ورخدادهای امنیت اطلاعات تاکید می‌کند. بهتراست سازمان اطمینان حاصل کند که کارکنان مناسبی به گزارشات آسیب‌پذیری‌های امنیت اطلاعات رسیدگی می‌کنند، به همان ترتیبی که نواقص غیر مرتبط با امنیت اطلاعات رسیدگی می‌شوند، احتمالا با ارزیابی و راه حل‌هایی که از کارکنان فنی استفاده می‌کنند (که ممکن است اعضای ISIRT باشند یا نباشند). بهتراست اطلاعات درباره آسیب‌پذیری‌ها و برطرف کردن آن‌ها در دادگان رویداد/رخداد/ آسیب‌پذیری امنیت اطلاعات که توسط ISIRT مدیریت می‌شود، وارد شوند. پیوست ت یک الگوی نمونه در مورد برگه گزارش‌دهی آسیب‌پذیری امنیت اطلاعات را نشان می‌دهد

شکل ۳ تمامی مراحل عملیاتی و فعالیت‌های مرتبط را نشان می‌دهد.



شکل ۳- نمودار جریان رویداد و رخداد امنیت اطلاعات

یادآوری- هشدار نادرست، نشان‌هایی از رویداد ناخواسته است که واقعیت نداشته و یا بدون هرگونه نتیجه‌ای می‌باشد.

اولین مرحله‌ی استفاده‌ی عملیاتی از یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، شامل آشکارسازی از، جمع آوری اطلاعات مرتبط با، و گزارش‌دهی درمورد، وقوع رویداد امنیت اطلاعات توسط انسان یا وسایل خودکار است. بهتراست سازمان اطمینان حاصل کند که این مرحله شامل آشکارسازی آسیب‌پذیری‌های امنیت اطلاعاتی است که هنوز به عنوان رویداد، و احتمالا رخداد امنیت اطلاعات، بهره‌برداری نشده‌اند و درمورد آن‌ها گزارش نشده‌است.

برای مرحله‌ی آشکارسازی و گزارش دهی، یک سازمان بهتراست اطمینان حاصل کند فعالیت‌های کلیدی عبارتند از:

الف- فعالیت در آشکارسازی و گزارش وقوع یک رویداد امنیت اطلاعات یا وجود یک آسیب‌پذیری امنیت اطلاعات، توسط یکی از کارکنان/مشتریان سازمان یا به‌صورت خودکار، به کمک موارد زیر:

۱- هشدارها از سامانه‌های پایش امنیتی مانند سامانه آشکارسازی نفوذ[1]/ آشکارسازی و پیشگیری نفوذ[2]، نرم‌افزارهای ضدویروس، کوزه‌های عسل[3] (اصطلاح عمومی درمورد یک سامانه طعمه که برای فریب دادن، منصرف‌کردن، منحرف‌کردن و تشویق حمله کننده به صرف وقت بر روی اطلاعاتی که به ظاهر بسیار ارزشمند به‌نظر می‌رسد، اما در واقع ساختگی‌اند و مورد علاقه هیچ کاربر قانونی نیست [استاندارد ملی ایران شماره ۱۸۰۴۳: سال ۱۳۸۸])/ تارپیت‌ها[4] (سامانه‌هایی که برای به تاخیرانداختن حمله‌ها به‌طور عمدی ایجاد و طراحی شده‌اند)، سامانه‌های ثبت پایش[5]، سامانه‌های مدیریت امنیت اطلاعات، موتورهای ارتباط[6] و دیگر موارد،

۲- هشدارها از سامانه‌های پایش شبکه مانند دیواره‌های آتش، تحلیل‌های جریان شبکه، فیلترکردن تارنما و دیگر موارد ،

۳- تحلیل‌های ثبت اطلاعات از افزاره‌ها، خدمات، میزبان‌ها و سامانه‌های گوناگون،

۴- ارجاع به مرجع بالاتر درمورد رویدادهای غیرعادی آشکار شده توسط ICT،

۵- ارجاع به مرجع بالاتر درمورد رویدادهای غیرعادی آشکار شده توسط پیشخوان‌ها،

۶- گزارشات کاربران، و

1-Intrusion Detection System(IDS)
2- Intrusion Detection and Prevention (IDP)
3-Honeypots
4-Tarpits
5- log monitoring systems
6- Correlations Engines

۷- اعلان‌های خارجی، دریافتی از طرف‌های سوم مانند سایر ISIRTها، خدمات امنیت اطلاعات، ISPها، ارایه‌کنندگان خدمات مخابراتی، شرکت‌های برون سپاری یا ISIRTهای ملی.

ب- فعالیت جمع‌آوری اطلاعات در باره یک رویداد یا آسیب‌پذیری امنیت اطلاعات.

پ- فعالیت برای حصول اطمینان از اینکه تمام عوامل دخیل در PoC، همه‌ی فعالیت‌ها، نتایج و تصمیمات مرتبط را برای تحلیل‌های بعدی ثبت می‌کنند.

ت- فعالیت برای حصول اطمینان از اینکه شواهد الکترونیکی به‌طور امن گردآوری و ذخیره شده، و حفاظت ایمن از آن به صورت مستمر پایش می‌گردد، برای زمانی که اعمال دادرسی قانونی و یا اقدامات انضباطی داخلی مورد نیاز است.

یادآوری- استاندارد ملی آتی (ISO/IEC 27037) اطلاعات مفصل‌تری درمورد شناسایی، جمع آوری، دریافت و حفظ شواهد دیجیتالی ارایه خواهد کرد.

ث- فعالیت برای حصول اطمینان از اینکه رژیم کنترل کننده‌ی تغییر برای پوشش دادن به ردگیری رویداد و آسیب‌پذیری امنیت اطلاعات و روزآمدکردن گزارشات رویداد و آسیب‌پذیری، و در نتیجه روزآمدکردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات، برقرار است.

ج- فعالیت برای تشدید بازیابی و/یا تصمیمات بیشتر، بر حسب ضرورت در سراسرمرحله.

چ- فعالیت برای ثبت در یک سامانه ردگیری رخداد[1].

بهتراست تمامی اطلاعات جمع‌آوری‌شده که مربوط به رویداد یا آسیب‌پذیری امنیت اطلاعات است، در دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات که توسط ISIRT مدیریت می‌شود، ذخیره گردد. برای حصول اطمینان ازاینکه مبنای خوبی برای ارزیابی‌ها و تصمیماتی که بایداتخاذ شود، و البته عملیاتی که باید انجام شود، دردسترس است، توصیه می‌شود اطلاعاتی که در طول هر فعالیت گزارش می‌شود درزمان ارائه‌ی گزارش تا حد امکان تکمیل باشد.

۶-۲ آشکارسازی رویداد

رویدادهای امنیت اطلاعات، می‌توانند مستقیما ازطریق توجه شخص یا اشخاص به چیزی که عامل نگرانی است، اعم از فنی، فیزیکی و یا روش‌های اجرایی مربوط، آشکار شوند. برای مثال، آشکارسازی می‌تواند از طریق آشکارسازهای آتش/دود و یا هشدارهای ورود غیر مجاز (سرقت)، همراه با علامت‌های هشدار دهنده در مناطقی که از پیش برای مقابله با اقدام انسانی تعیین شده، انجام شود. رویدادهای فنی امنیت اطلاعات

1- Incident Tracking System

می‌توانند ازطریق وسایل خودکار، برای مثال، هشدارهایی که از تسهیلات تحلیل رد ممیزی[1]، دیواره‌های آتش، سامانه‌های آشکارسازی نفوذ، و ابزارهای ضد کد مخرب (ازجمله ویروس‌ها) آشکار شوند. این روش‌ها در هر مورد ازطریق پارامترهای از پیش تنظیم‌شده شبیه‌سازی می‌شوند.

منابع ممکن برای آشکارسازی رویداد امنیت اطلاعات عبارتند از:

الف- کاربران

ب- مدیران عملیاتی و مدیران امنیتی.

پ- مشتریان.

ت- اداره IT، شامل مرکز عملیات شبکه و مرکز عملیات امنیتی (ازطریق پشتیبانی سطح دوم)،

ث- پیشخوان[2] IT (ازطریق پشتیبانی سطح یکم)،

ج- ارایه‌کنندگان خدمات مدیریت شده، (ازجمله ISPها، ارایه‌کنندگان خدمات مخابراتی و تأمین‌کنندگان)،

چ- ISIRTها،

ح- و دیگر واحدها و کارکنان که ممکن است مزاحمت‌ها را حین کار روزانه آشکارکنند،

خ- رسانه‌ی عمومی (روزنامه، تلویزیون، غیره)، و

د- پایگاه‌های اینترنتی[3] (پایگاه‌های اینترنتی امنیت اطلاعات عمومی، پایگاه‌های اینترنتی توسط پژوهشگران امنیت، پایگاه‌های اینترنتی بایگانی حملات تغییردهنده ظاهر صفحات[4] و پایگاه‌های اینترنتی، غیره).

۶-۳ گزارش‌دهی رویداد

منبع آشکارسازی یک رویداد امنیت اطلاعات هر چه باشد، شخصی که از طریق وسایل خودکار متوجه می‌شود یا مستقیما متوجه چیزی غیر عادی می‌گردد، مسئول شروع فرآیند آشکارسازی و گزارش دهی می‌باشد. این شخص میتواند یک عضو از کارکنان سازمان، اعم از رسمی یا قراردادی باشد.

این شخص برای این که توجه PoC و مدیریت را به رویداد امنیت اطلاعات جلب کند، بهتراست از روش‌های اجرایی رویداد امنیت اطلاعات پیروی کند و از برگه گزارش‌دهی که توسط طرح‌واره‌ی مدیریت رخداد امنیت

1- Audit trail
2-Help desk
3- Websites
4- Defacement archive

اطلاعات مشخص شده، استفاده نماید. بر این اساس، لازم است که همه‌ی کارکنان، کاملا از راهنماهای مبنی بر گزارش‌دهی انواع مختلف رویدادهای ممکن امنیت اطلاعاتی آگاه بوده و به آن دسترسی داشته باشند. این راهنمایی شامل قالب برگه گزارش دهی رویدادهای امنیت اطلاعات وجزئیات کارکنانی است که بهتراست از هر واقعه مطلع شوند (بهتراست همه‌ی کارکنان حداقل از قالب برگه گزارش دهی رخدادهای امنیت اطلاعاتی، جهت کمک به درک آن‌ها از طرحواره‌ی مورد نظر، آگاهی داشته باشند). بهتراست توجه داشت که استفاده از تلفن ثابت، تلفن بی سیم و تلفن همراه بدون محافظ، ناامن تلقی می‌شوند. هنگام رسیدگی به اطلاعات محرمانه یا سرّی، بهتراست محافظ‌های بیشتری تدارک شوند.

به عنوان مبنای برگه سامانه ردگیری رخداد، می‌توان از اطلاعات زیر استفاده نمود:

- زمان/تاریخ آشکارسازی ،
- مشاهدات، و
- اطلاعات تماس (اختیاری)

برگه تکمیل‌شده (ارسال ازطریق کتبی یا رایانامه یا تارنما) بهتراست هنگام ثبت رخدادهای امنیت اطلاعات در سامانه‌ی ردگیری آشکارسازی فقط توسط کارکنان ISIRT استفاده شود. تهیه گزارشاتی عمدی از یک رویداد امنیت اطلاعات مشکوک/تجربه شده/ آشکار شده، از گزارشاتی که تمام اطلاعات آن تکمیل شده‌باشد، سخت‌تر است.

ردگیری رویداد امنیت اطلاعات (رخداد احتمالی) بهتراست در هر زمان ممکن، به‌وسیله یک برنامه کاربردی خودکار پشتیبانی گردد. استفاده از یک سامانه اطلاعاتی برای مجبورکردن کارکنان به پیروی از روش‌های اجرایی و بازبینه‌ها[1]، تعیین شده اساسی است. همچنین ادامه ردگیری مسائلی چون «چه کسی در چه زمانی چه کاری را انجام داده» بسیار مفید است، چراکه این جزئیات ممکن است در طول یک رویداد (رخداد احتمالی) امنیت اطلاعات، اشتباهی نادیده گرفته شوند.

چگونگی رسیدگی به یک رویداد امنیت اطلاعات، بستگی به ماهیت آن، عواقب و واکنش‌هایی دارد که ممکن است از آن سرچشمه بگیرد. برای اشخاص بسیاری ، این تصمیمی فراتر از شایستگی آن‌ها خواهد بود. بنابراین شخصی که یک رخداد امنیت اطلاعات را گزارش می‌کند، بهتراست برگه گزارش را تا حد امکان با جزئیات و سایر اطلاعات موجود در آن‌هنگام تکمیل نموده و در صورت نیاز با مدیر بخش خود در جریان بگذارد. بهتراست برگه مذکور به صورت امن با PoC تعیین شده مبادله و یک رونوشت از آن نیز به ISIRT مسئول تحویل شود. توصیه می‌شود خدمات PoC ترجیحا به صورت شبانه روزی و در ۷ روز هفته ارائه شود. پیوست ت الگوی نمونه‌ای از برگه گزارش دهی رخداد امنیت اطلاعات را نشان می‌دهد.

[1] - checklists

بهتراست ISIRT یک عضو گروه و یا یک شیفت‌کاری را به عنوان مسئول دریافت برگه گزارشات از طریق رایانامه، تلفن، فکس، و مکالمات مستقیم تعیین نماید. این مسئولیت می‌تواند به طور هفتگی در بین اعضای گروه در چرخش باشد. این عضو تعیین شده، ارزیابی و عملیات مناسب را در اطلاع رسانی به کارکنان مسئول و طرف‌های دخیل و همین‌طور برطرف کردن رویداد امنیت اطلاعات مربوطه انجام میدهد.

تاکید می‌شود که نه تنها صحت بلکه زمان‌بندی نیز در محتوای برگه پرشده گزارش رویداد امنیت اطلاعات حائز اهمیت است. تاخیر در ارسال یک برگه گزارش به منظور بهبود صحّت محتوای آن عمل به جایی محسوب نمی گردد. اگر شخص گزارش‌دهنده در مورد هر یک از فیلدهای برگه گزارش محرم نباشد، بهتراست آن اطلاعات با یادآوری مناسب ارسال و اصلاحات بعدا اعلام شوند. همچنین بهتراست خاطر نشان ساخت که برخی سازوکارهای گزارش‌دهی (مانند رایانامه) خود اهداف قابل رویتی برای حمله می‌باشند.

هنگامی که برای سازوکارهای گزارش‌دهی الکترونیکی (مانند رایانامه) مشکلاتی به‌وجود می‌آید یا پیش‌بینی می‌شود به وجود آید، بهتراست وسایل ارتباطی جایگزین مورد استفاده قرارگیرند. ازجمله زمانی که تصور می‌شود سامانه درمعرض حمله است و اشخاص غیر مجاز می‌توانند برگه‌های الکترونیکی گزارش‌شده را بخوانند. وسایل جایگزین می‌تواند شامل مراجعه شخصی، به‌وسیله تلفن یا پیام متنی باشند. بهتراست این وسایل جایگزین، به ویژه هنگامی مورد استفاده قرارگیرند که در یک بررسی اولیه محرز شود یک رویداد امنیت اطلاعات احتمالا باید به عنوان یک رخداد امنیت اطلاعات، به ویژه نوع قابل‌توجه آن، رده بندی شود.

در حالی که در بسیاری از موارد، یک رویداد امنیت اطلاعات بهتراست جهت اقدامات لازم به PoC گزارش شود، برخی موقعیت‌ها ممکن است ایجاد شوند که در آن‌ها به یک رویداد امنیت اطلاعات به صورت محلی و احیانا توسط مدیریت محلی[1] ساماندهی شود. توصیه می‌شود که مدیریت محلی برای صورت دادن ارزیابی یکسان با ISIRT و به‌دست آوردن معیارهای مشترک یکسان/مشابه با آن‌ها و نیز استفاده از یک سامانه ردگیری به منظور استفاده موفقیت‌آمیز از منابع داخلی، آموزش‌های لازم را ببینند. این کار از دوباره کاری‌های ISIRT پیش‌گیری خواهد کرد.

یک رویداد امنیت اطلاعات می‌تواند به سرعت به عنوان یک هشدار نادرست تشخیص داده شود یا ممکن است با یک نتیجه‌گیری رضایت‌بخش برطرف کردن شود. در چنین مواردی بهتراست یک برگه گزارش‌دهی تکمیل گردیده و به منظور ثبت جهت مدیریت محلی، جهت PoC، و جهتISIRT فرستاده شود، یعنی به دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات. در چنین موردی، شخصی که بسته‌شدن یک رویداد امنیت اطلاعات را گزارش می‌کند، ممکن است بتواند بعضی از اطلاعات مورد درخواست در برگه گزارش‌دهی رویدادهای امنیت اطلاعات را تکمیل نماید. در چنین موردی بهتراست متعاقبا برگه گزارش‌دهی رخداد امنیت اطلاعات نیز تکمیل شده و ارسال گردد. استفاده از ابزارهای خودکار می‌تواند به تکمیل برخی از

1- Local Management

فیلدها کمک کند، برای مثال مهرهای زمانی[1]، این کار همچنین می‌تواند در اشتراک گذاری/انتقال اطلاعات لازم، کمک نماید.

۷ مرحله ارزیابی و تصمیم

۷-۱ مرور کلی اقدامات کلیدی

دومین مرحله استفاده عملیاتی از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، شامل ارزیابی اطلاعات مرتبط با وقوع رویدادهای امنیت اطلاعات و تصمیم درمورد رویداد امینت اطلاعات بودن آن است.

در مرحله ارزیابی و تصمیم، یک سازمان بهتراست اطمینان حاصل کند که فعالیت‌های کلیدی عبارتند از:

الف- اقدام درمورد PoC برای اجرای ارزیابی که مشخص‌کند یک رویداد، یک رخداد امنیت اطلاعات محتمل یا قطعی یا یک هشدار نادرست است و اگر یک هشدار نادرست نیست، آیا ارجاع به مرجع بالاتر لازم است. بهتراست ارزیابی‌ها شامل استفاده از مقیاس رده‌بندی رویداد/رخداد امنیت اطلاعات توافق‌شده باشد (شامل تعیین اثرهای رویدادها بر اساس دارایی‌ها/خدمات آسیب‌دیده) و توصیه می‌شود درمورد اینکه آیا رویدادها بهتراست به‌عنوان رخدادهای امنیت اطلاعات رده‌بندی گردند، تصمیم‌گیری شود (برای نمونه راهنمای پیوست پ ملاحظه شود.) در حالی که اثرهای رویدادهای امنیت اطلاعات (و بنابراین رخدادهای ممکن) بر حسب میزان رخنه در محرمانگی، صحت و دسترسی‌پذیری تعیین می‌گردد، سازمان‌ها بهتراست از شناسایی موارد زیر مطمئن شوند:

۱- دامنه اثر(فیزیکی یا منطقی)

۲- دارایی‌ها، زیرساخت‌ها، اطلاعات، فرآیندها، خدمات و کاربردهایی که تاثیر می‌گیرند یا تحت تاثیر قرار خواهند گرفت، و

۳- اثرهای احتمالی بر خدمات اصلی سازمان

ب- فعالیت برای ISIRT جهت اجرای ارزیابی درمورد تائید نتایج ارزیابی توسط PoC مبنی بر اینکه آیا رویداد، درصورت کاربردپذیری، یک رخداد امنیت اطلاعات است یا خیر. در صورت نیاز، بهتراست ارزیابی دیگری با استفاده از مقیاس رده‌بندی توافق‌شده رویداد/رخداد امنیت اطلاعات همراه با جزئیات نوع رویداد (رخداد احتمالی) و منبع تحت تاثیر(رسته‌بندی)، صورت پذیرد (نمونه راهنمایی‌ها در پیوست پ ملاحظه شود). توصیه می‌شود در مرحله بعد، در مورد چگونگی رسیدگی به تایید رخداد امنیت اطلاعات، شامل اینکه رخداد به تایید چه کسی با چه اولویتی برسد، تصمیماتی اتخاذ شود. برای اینکه بتوان تمرکز دقیقی اعمال کرد، بهتراست این رسیدگی شامل فرآیند ازپیش‌تعیین شده اولویت‌بندی باشد. فرآیندی که هر رخداد امنیت

2- Time stamps

اطلاعات را به اشخاص ذی صلاح تخصیص داده و فوریت ساماندهی و پاسخگویی با رخداد امنیت اطلاعات را تعیین کند. این فرآیند شامل تعیین ضرورت یک پاسخگویی سریع، تحلیل امور قانونی امنیت اطلاعات و فعالیت‌های ارتباطاتی هم باشد (پاسخگویی‌ها - بند۸ نیز ملاحظه شود).

پ- فعالیت برای افزایش براساس نیاز درسرتاسر مرحله، جهت ارزیابی‌ها و/یا تصمیم گیری‌های بیشتر.

ت- فعالیت برای حصول اطمینان از اینکه همه عوامل دخیل، به‌ویژه ISIRT، تمام فعالیت‌های خود را جهت تحلیل بعدی، با صحت ثبت می‌نمایند.

ث - فعالیت برای حصول اطمینان از اینکه شواهد الکترونیکی به‌طور امن گردآوری و ذخیره شده، و حفاظت ایمن از آن به صورت مستمر پایش می‌گردد، برای زمانی که اعمال دادرسی قانونی و یا اقدامات انظباطی داخلی مورد نیاز است.

ج- فعالیت برای حصول اطمینان از اینکه رژیم کنترل کننده‌ی تغییر برای پوشش دادن به ردگیری رخداد امنیت اطلاعات و روزآمدکردن گزارشات رخداد، و درنتیجه روزآمدکردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات، برقرار است.

بهتراست تمامی اطلاعات جمع‌آوری‌شده که مربوط به رویداد، رخداد یا آسیب‌پذیری امنیت اطلاعات است، در دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات که توسط ISIRT مدیریت می‌شود، ذخیره گردد. برای حصول اطمینان ازاینکه مبنای خوبی برای ارزیابی‌ها و تصمیماتی که بایداتخاذ شود، و البته عملیاتی که باید انجام شود، دردسترس است، توصیه می‌شود اطلاعاتی که در طول هر فعالیت گزارش می‌شود درزمان ارایه گزارش تا حد امکان تکمیل باشد.

همین‌که یک رویداد امنیت اطلاعات آشکار و گزارش شود. فعالیت‌های بعدی عبارتند از:

چ- فعالیت برای تقسیم مسئولیت فعالیت‌های مدیریت رخداد امنیت اطلاعات ازطریق سلسله مراتبی از کارکنان مناسب، همراه با ارزیابی، تصمیم گیری و اقداماتی که هم کارکنان امنیتی و هم غیر امنیتی درآن دخالت دارند.

ح- فعالیت برای تهیه روش‌های اجرایی رسمی محتوی بازیابی و اصلاح گزارشاتی تهیه‌شده، ارزیابی خسارت و اطلاع‌رسانی به کارکنان مرتبط، برای اینکه هر شخص مطلع از آن‌ها پیروی کند (با اقدامات انفرادی بر حسب نوع و شدت رخداد).

خ- فعالیت برای استفاده از راهنماها در جهت مستندسازی کامل یک رویداد امنیت اطلاعات.

د- فعالیت برای استفاده از راهنماها در جهت مستندسازی کامل عملیات بعدی برای یک رخداد امنیت اطلاعات در صورتیکه رویداد امنیت اطلاعات به عنوان یک رخداد امنیت اطلاعات رده‌بندی شده باشد.

ذ- فعالیت برای روزآمدکردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات.

سازمان بهتراست اطمینان حاصل کند که این مرحله در بر دارنده ارزیابی اطلاعات گردآوری‌شده از گزارش-های آسیب‌پذیری‌های امنیت اطلاعات است (که تاکنون به عنوان عامل رویدادهای امنیت اطلاعات و یا احتمالا رخدادهای امنیت اطلاعات بهره‌برداری نشده‌اند)، همراه با تصمیم‌گیری درمورد اینکه کدامیک توسط چه کسی و با چه اولویتی باید رسیدگی شوند.

۲-۷ ارزیابی و تصمیم اولیه توسط PoC

شخص دریافت‌کننده در PoC ، بهتراست دریافت برگه تکمیل‌شده گزارش رویداد امنیت اطلاعات را تایید، آن را در دادگان رویداد/رخداد/آسیب‌پذیر امنیت اطلاعات وارد و آن را بازنمایی کند. بهتراست درصدد هرگونه روشن‌گری از شخص گزارشگر رویداد امنیت اطلاعات برآمده و هرگونه اطلاعات دیگر را یا از شخص گزارشگر یا از جای دیگر جمع آوری کند. سپس، توصیه می‌شود PoC یک ارزیابی انجام‌دهد برای تعیین اینکه آیا رویداد امنیت اطلاعات بهتراست به عنوان یک رخداد امنیت اطلاعات رده‌بندی شود و یا تنها یک هشدار نادرست است (ازجمله از طریق استفاده از مقیاس توافق‌شده رده‌بندی رویداد). اگر معلوم شود که رویداد امنیت اطلاعات یک هشدار نادرست است، بهتراست برگه گزارش رویداد امنیت اطلاعات تکمیل و برای اضافه‌کردن به دادگان رویداد/رخداد/آسیب‌پذیر امنیت اطلاعات و بازنگری جهت ISIRT مبادله شود، و رو نوشت آن برای شخص گزارشگر و مدیر محلی ارسال گردد.

اطلاعات و سایر شواهد جمع آوری شده در این مرحله ممکن است زمانی در آینده جهت اقدامات انضباطی یا روش‌های اجرایی دادرسی مورد استفاده قرار گیرند. بهتراست شخص یا اشخاص عهده‌دار وظایف جمع‌آوری اطلاعات و ارزیابی آن‌ها در زمینه الزامات جمع‌آوری و ذخیره شواهد، آموزش ببینند.

علاوه بر ثبت تاریخ (ها) و زمان (ها)ی عملیات، لازم است که موارد زیر را به‌طور کامل مستند کرد:

الف- آن چه که دیده شده و انجام شده است (شامل ابزارهای مورد استفاده) و چرا،

ب- محل شواهد بالقوه،

پ- چگونه شواهد بایگانی شده‌است (در صورت کاربرد پذیری)،

ت- چگونه درست‌سنجی شواهد انجام شده بود (در صورت کاربرد پذیری)، و

ث- جزئیات حفاظت از ذخیره/ایمنی مواد و دسترسی‌های بعدی به آن.

در صورتیکه محرز شود رویداد امنیت اطلاعات، احتمالا یک رخداد امنیت اطلاعات است، و اگر شخص شاغل در PoC از سطح شایستگی مناسبی برخوردار است، ممکن است ارزیابی‌های بیشتری انجام شود. این کار

ممکن است نیازمند عملیات اصلاحی، برای مثال شناسایی کنترل‌های اضطراری دیگر باشد، تا به عنوان مرجع، مورد استفاده شخص ذی‌صلاح قرارگیرد. ممکن است محرز شود یک رویداد امنیت اطلاعات، یک رخداد امنیت اطلاعات قابل‌توجه است (با استفاده از مقیاس از پیش تعیین‌شده شدت[1] رخدادتوسط سازمان)، درهر مورد بهتراست مدیر ISIRT مستقیما مطلع شود. ممکن است اعلام یک موقعیت بحرانی محرزشود، و برای مثال، مسئول مدیریت بحران جهت فعال‌سازی برنامه مدیریت بحران و مدیر ISIRT و مدیریت ارشد مطلع شوند. به هر حال، محتمل ترین موقعیت این است که رخداد امنیت اطلاعات باید به صورت مستقیم جهت ارزیابی و اقدام بعدی به ISIRT ارجاع داده شود.

گام بعدی هر چه که باید باشد، PoC بهتراست برگه گزارش رخداد امنیت اطلاعات را تا حد امکان تکمیل نماید. برگه گزارش رخداد امنیت اطلاعات بهتراست حاوی جزئیات بوده و تا حد امکان موارد زیر را تایید و توصیف نماید:

الف- ماهیت رخداد امنیت اطلاعات چیست،

ب- چگونه، بوسیله چه چیزی یا چه کسی ایجاد شده است،

پ- این رویداد بر چه چیزی تاثیر گذار است یا می‌تواند تاثیر گذار باشد،

ت- اثر واقعی یا بالقوه‌ی رویداد امنیت اطلاعات بر کسب‌وکار سازمان،

ث- تغییرات شاخص درمورد این که آیا رخداد امنیت اطلاعات قابل ملاحظه تلقی می‌شود یا خیر (با استفاده از مقیاس از پیش تعیین شده رده‌بندی سازمان)، و

ج- تاکنون چگونه به آن رسیدگی شده است

هنگام توجه به اثرهای نامطلوب یا واقعی یک رخداد امنیت اطلاعات بر روی کسب و کار یک سازمان، برخی مثال‌های زیر ارایه می‌شوند:

الف- افشای غیرمجاز اطلاعات،

ب- تغییر غیر مجاز اطلاعات،

پ- انکار اطلاعات،

ت- دسترسی‌ناپذیری اطلاعات و/یا خدمت،

ث- تخریب اطلاعات و/یا خدمت، و

1- Pre-determined severity scale

ج- کاهش عملکرد خدمت.

اولین گام توجه به این است که کدامیک از نتایج مرتبط است. برای آن رسته که مرتبط تلقی می‌شوند، بهتراست راهنمای رسته‌بندی مرتبط جهت استقرار تاثیرات بالقوه یا واقعی ورودی‌های گزارش امنیت اطلاعات مورد استفاده قرارگیرند. مثال راهنماها در پیوست پ ارایه‌شده است. مثال رسته‌بندی‌های در زیر آمده است:

الف- عملیات زیان/اختلال[1] مالی عملیات کسب‌وکار،

ب- منافع تجاری و اقتصادی،

پ- اطلاعات شخصی،

ت-تعهدات قانونی و مقرراتی،

ث- عملیات مدیریت و کسب و کار،

ج- ازدست‌رفتن حسن شهرت[2]،

چ- جراحت یا فوت، و

ح- اغتشاشات اجتماعی[3].

اگر یک رخداد امنیت اطلاعات برطرف شده‌باشد، بهتراست گزارش مربوط حاوی جزئیات کنترل‌هایی که اعمال‌شده و درس‌های آموخته‌شده، باشد (برای مثال کنترل‌هایی جهت پیش‌گیری از وقوع دوباره یا مشابه). همین‌که که گزارش تا حد امکان کامل شد، پس از آن بهتراست برگه گزارش جهت ثبت و بازیابی در دادگان رویداد/ رخداد/آسیب‌پذیری امنیت اطلاعات به ISIRT ارسال گردد.

در صورتیکه یک رسیدگی احتمالا طولانی تر از دوره زمانی تعریف شده در خط‌مشی مدیریت رخداد امنیت اطلاعات باشد، بهتراست یک گزارش موقت در دوره زمانی مشخص شده در خط‌مشی، تولید شود.

تاکید می‌گردد که بهتراست PoC ارزیابی‌کننده یک رخداد امنیت اطلاعات، از اساس راهنمای ارائه‌شده در مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات آگاه باشد. مثال‌های این آگاهی عبارتند از:

الف- چه وقتی و با چه کسی لازم است که موضوعات تشدید شود، و

1- Loss/disruption
2- Loss of goodwill
3- Societal disruption

ب- بهتراست روش‌های اجرایی تغییر کنترل در تمام فعالیت‌های انجام‌شده توسط PoC دنبال شوند.

همانگونه که در بندهای ۶-۲ و ۶-۳ بالا در مورد آشکارسازی و گزارش‌دهی رویداد ذکر گردید، هنگامی که مشکلاتی وجود دارند و یا به نظر میرسد وجود داشته باشند، بهتراست وسایل ارتباطی جایگزینی برای روزآمدکردن برگه‌های گزارش دهی، همراه با سازوکارهای گزارش‌دهی الکترونیک استفاده شود (مانند رایانامه).

۳-۷ ارزیابی و تایید رخداد توسط ISIRT

مسئولیت ارزیابی و تایید تصمیم در باره اینکه یک رویداد امنیت اطلاعات باید به عنوان یک رخداد امنیت اطلاعات رده‌بندی شود، بر عهده ISIRT است. بهتر است شخص دریافت کننده در ISIRT اقدامات زیر را به عمل آورد:

الف- تایید دریافت برگه گزارش‌دهی رخداد امنیت اطلاعات، تا حد امکان تکمیل شده توسط PoC.

ب- در صورت عدم انجام این کار توسطPoC، ثبت برگه در دادگان رویداد/رخداد/ آسیب‌پذیری امنیت اطلاعات و درصورت لزوم روزآمد کردن دادگان.

پ- پیگیری روشنگری از PoC، در صورت لزوم.

ت- بازنگری محتوای برگه گزارش دهی.

ث- جمع آوری هرگونه اطلاعات بیشتر مورد نیاز و اطلاع از دسترس‌پذیر بودن آن‌ها، از طریق PoC، شخص تکمیل کننده برگه گزارش رویداد امنیت اطلاعات یا از هر جای دیگر.

در صورتی که هنوز درجه‌ای از تردید درمورد اصالت‌سنجی[1] رخداد امنیت اطلاعات یا کامل بودن اطلاعات گزارش شده وجود داشته باشد، عضو ISIRT بهتراست یک ارزیابی جهت تعیین این که آیا رخداد واقعی است یا درحقیقت یک هشدار نادرست، انجام دهد (از طریق استفاده از مقیاس توافق‌شده رده‌بندی رخداد سازمان). اگر معلوم شود که رخداد امنیت اطلاعات یک هشدار نادرست بوده است، گزارش امنیت اطلاعات مذکور بهتراست تکمیل شده، به دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات ثبت شده و با مدیر ISIRT مبادله گردد. بهتراست رونوشت‌هایی از این گزارش برای PoC، و شخص گزارشگر و مدیر محلی او ارسال شود.

بهتراست یک رخداد امنیت اطلاعات، در ارتباط با هر رویداد/رخداد دیگر که به ISIRT گزارش می‌شود قرارگیرد. هدف این فعالیت مهم، درستی‌سنجی این است که رخداد متصل به رویداد/رخداد دیگری است یا

1- Authenticity

تنها اثر رخداد دیگری است، یعنی حملات انکار خدمت (DOS)[1] یا حملات توزیع‌شده انکار خدمت (DDOS)[2]. ارتباط رویدادها نیز در اولویت‌بندی تلاش‌های ISIRT حائز اهمیت است.

در صورتی که مشخص شود رخداد امنیت اطلاعات واقعی است، بهتراست عضو ISIRT و همکاران او ارزیابی‌های بیشتری را، بر حسب ضرورت، صورت دهند. هدف از این ارزیابی، تایید هرچه زودتر موارد زیر است:

الف- ماهیت رخداد امنیت اطلاعات چیست، چگونه، توسط چه چیزی یا چه کسی ایجاد گردید، بر چه چیزهایی تاثیر گذار است یا می‌تواند تاثیر گذار باشد، اثر یا اثر بالقوه‌ی رخداد امنیت اطلاعات بر کسب و کارسازمان، نشان‌های از این که آیا رخداد امنیت اطلاعات به عنوان یک رخداد قابل ملاحظه تلقی می‌شود یا خیر (با استفاده از مقیاس از پیش تعیین‌شده شدت رخداد توسط سازمان). اگر رویداد اثر شدید منفی بر کسب و کار سازمان داشته باشد، بهتراست فعالیت‌های مدیریت بحران آغاز شود (بند ۸- ۲- ۴ ملاحظه شود).

ب- جنبه‌های زیر از حمله عمدی فنی انسانی به یک سامانه، خدمت و/یا شبکه‌ی اطلاعات، برای مثال:

۱- عمق نفوذ به این سامانه، خدمت و/یا شبکه‌ی اطلاعات تاچه حدی شده است و حمله‌کننده دارای چه سطحی از کنترل است.

۲- حمله‌کننده به چه داده‌هایی دسترسی پیداکرده، احتمالا از آن‌ها رونوشت برداشته، تغییرداده یا نابودکرده است.

۳- حمله‌کننده از کدام نرم‌افزار رونوشت برداشته، آن‌را تغییرداده یا نابودکرده است.

پ- آثار مستقیم و غیرمستقیم (برای مثال، آیا دسترسی فیزیکی به‌دلیل یک آتش‌سوزی، آزاد است، آیا یک سامانه اطلاعاتی به‌دلیل خرابی نرم‌افزار یا خط مخابرات، یا به‌دلیل خطای انسانی آسیب‌پذیر است)، و

ت- تا حالا چگونه به رخداد امنیت اطلاعات رسیدگی شده است و توسط چه کسی.

هنگام بازنگری آثار نامطلوب یک رخداد امنیت اطلاعات بر روی کسب و کار یک سازمان، از برخی اطلاعات و/یا خدمات نشان داده شده در بند ۷- ۲، لازم است تعداد نتایج مرتبط تایید شود. رسته بندی‌های نمونه در بند ۷- ۲ و پیوست پ نشان داده شده‌اند.

به منظور تسهیل پاسخگویی کافی با رخداد امنیت اطلاعات، بهتراست یک فرآیند اولویت‌بندی برای اختصاص دادن یک رخداد امنیت اطلاعات به ذی‌صلاح‌ترین شخص یا گروهی از اشخاص در ISIRT استفاده

1- Denial of Service (DoS)
2- Distributed Denial of Service (DDOS)

شود. به‌ویژه، هنگامی که چندین رخداد امنیت اطلاعات به صورت هم‌زمان مورد رسیدگی قرارمی‌گیرد، اولویت‌ها باید به ترتیب پاسخگویی‌هایی که با رخدادهای امنیت اطلاعات اعمال میشود، تنظیم گردد.

بهتراست اولویت‌ها بر طبق اثرهای نامطلوب معین بر روی کسب و کار مرتبط با رویداد امنیت اطلاعات سازمان، و میزان تلاش تخمینی مورد نیاز برای پاسخگویی با رخداد امنیت اطلاعات، تنظیم شود. در مورد رخدادهایی که اولویت یکسانی دارند، تلاش مورد نیاز ، متریکی است برای تعیین ترتیب پاسخگویی. برای مثال، رخدادی که به راحتی برطرف شده است، می‌تواند قبل از رخدادی که نیاز به تلاش بیشتری دارد، مورد رسیدگی قرار گیرد.

برای تایید اثرها بالقوه یا واقعی رخدادهایی که مرتبط درنظر گرفته می‌شوند، بهتراست جهت درج در گزارش رخداد امنیت اطلاعات، از رسته‌بندی راهنمای مربوط استفاده شود. راهنماهای نمونه در پیوست‌های پ و ت نشان داده شده است.

۸ مرحله‌ی پاسخگویی

۸-۱ مرور کلی بر اقدامات کلیدی

مرحله‌ی سوم استفاده عملیاتی از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، شامل پاسخگویی با رخداد امنیت اطلاعات بر طبق اقدامات توافق شده در مرحله‌ی ارزیابی و تصمیم است. این پاسخگویی‌ها بسته به تصمیمات می‌تواند آنی، بلادرنگ، یا نزدیک زمان بلادرنگ اتخاذ شوند و برخی به خوبی میتواند شامل تحلیل‌های امور قانونی امنیت اطلاعات باشند.

در مرحله‌ی پاسخگویی‌ها، بهتراست یک سازمان از فعالیت‌های کلیدی زیر مطمئن شود:

الف- فعالیت برای بازنگری درمورد تعیین اینکه رخداد امنیت اطلاعات توسط ISIRT تحت کنترل است، به شرح زیر:

۱) فعالیت برای تحریک پاسخگویی مورد نیاز، اگر تحت کنترل باشد. این کار می‌تواند یک پاسخگویی آنی، شامل فعال‌سازی روش‌های اجرایی بازیابی و/یا ایجاد ارتباط با کارکنان مرتبط دخیل، یا یک پاسخگویی بعدی با سرعت کم‌تر باشد (برای مثال، در تسهیل بازیابی کامل یک فاجعه)، درحالیکه اطمینان حاصل شود که همه‌ی اطلاعات برای رسیدگی به بازنگری های پس از رخداد آماده است.

۲) فعالیت برای تحریک فعالیت‌های مدیریت بحران از طریق ارجاع به مرجع بالاترِ کارکردِ رسیدگی به بحران، در صورت تحت کنترل نبودن و یا در صورت دارا بودن اثر شدید بر خدمات اصلی سازمان (بند ۸- ۲- ۴ ملاحظه شود). در این صورت مسئول رخداد، کارکرد رسیدگی به بحران با پشتیبانی کامل ISIRT (شامل فعال سازی یک برنامه مدیریت بحران)، و دخالت کارکنان مربوط

است، برای مثال مدیر و گروه مدیریت بحران سازمان (برای راهنما در مورد مدیریت استمرار کسب و کار ISO/IEC 22399:2007 و ISO /IEC 27031 ملاحظه شود).

ب- فعالیت برای تخصیص منابع داخلی و شناسایی منابع خارجی به منظور پاسخگویی با یک رخداد.

پ- فعالیت برای اجرای تحلیل‌های امور قانونی امنیت اطلاعات، براساس نیاز و ارتباط با رتبه مقیاس رده‌بندی رخداد امنیت اطلاعات، و تغییر آن رتبه مقیاس در صورت ضرورت.

ت- فعالیت برای تشدید، براساس لزوم در طول مرحله، برای ارزیابی‌ها و تصمیمات بیشتر.

ث- فعالیت برای حصول اطمینان از این که همه‌ی عوامل دخیل، به ویژه ISIRT، به طور مناسبی همه‌ی فعالیت‌ها را جهت تحلیل‌های بعدی، ثبت می‌کنند.

ج- فعالیت برای حصول اطمینان از اینکه شواهد الکترونیکی با ایمنی قابل اثبات، گردآوری و ذخیره گردیده است و این که امنیت حفاظت به طور دائمی پایش می‌شود، تا در صورت لزوم جهت پی‌گردهای قانونی و یا اقدام انضباطی داخلی به کار گرفته شوند.

چ- فعالیت برای حصول اطمینان از اینکه رژیم کنترل کننده‌ی تغییر برای پوشش دادن به ردگیری رخداد امنیت اطلاعات و روزآمدکردن گزارشات رخداد، و در نتیجه روزآمد نگه‌داشتن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات، برقرار است.

ح- فعالیت برای مبادله وجود یک رخداد امنیت اطلاعات و یا هر جزئیات مربوط به آن با دیگر اشخاص داخلی یا خارجی سازمان‌ها، به‌ویژه مالکین دارایی/اطلاعات/خدمت (تعیین‌شده درطول تحلیل اثر) و سازمان‌های داخلی/خارجی که بهتراست در مدیریت و برطرف کردن رخداد دخیل باشند.

بهتراست همه‌ی اطلاعات گردآوری شده‌ی مربوط به یک رویداد، رخداد و یا آسیب‌پذیری رخداد امنیت اطلاعات، در یک دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات که تحت مدیریت ISIRT باشد، جهت تحلیل‌های بیشتر ذخیره شوند. بهتراست اطلاعات گزارش شده در طول هر فعالیت تا حد امکان به موقع کامل شوند، تا اطمینان حاصل شود که مبنای خوبی برای ارزیابی‌ها و تصمیماتی که باید اخذ و البته اقداماتی که انجام شود، در دسترس می‌باشد.

همین‌که یک رخداد امنیت اطلاعات مشخص گردید، و پاسخگویی‌های مربوط مورد توافق قرار گرفت، اقدامات بعدی عبارتند از:

الف- فعالیت برای توزیع مسئولیت فعالیت‌های مدیریت رخداد از طریق سلسله مراتبی مناسب از کارکنان، برای تصمیم‌گیری و اقدامات درمورد هر دو کارکنان امنیتی و غیر امنیتی، بر حسب ضرورت.

ب- فعالیت برای ارایه روش‌های اجرایی مرسوم جهت پیروی هر یک از کارکنان دخیل، شامل بازنگری و اصلاح گزارشات، ارزیابی مجدد خسارت، و اعلام به کارکنان مربوط (با اقدامات انفرادی بر حسب نوع و شدت رخداد).

پ- فعالیت برای استفاده از راهنماهایی جهت مستندسازی دقیق از یک رخداد امنیت اطلاعات، از اقدامات بعدی، روزآمدکردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات.

ت- فعالیت برای استفاده از راهنماهایی جهت مستندسازی کامل اقدامات بعدی.

ث- فعالیت برای روزآمدکردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات.

همین‌که هر رخداد امنیت اطلاعات با موفقیت مورد رسیدگی قرار گرفت، بهتراست به صورت رسمی بسته شده و سابقه آن در دادگان مدیریت رخداد امنیت اطلاعات ثبت گردد. بهتراست سازمان اطمینان حاصل کند که در این مرحله، پاسخگویی‌هایی با آسیب‌پذیری‌های امنیت اطلاعات گزارش شده، برطبق اقدامات مورد توافق در مرحله‌ی ارزیابی و تصمیم نیز انجام می‌گیرد. همین‌که هرگونه آسیب‌پذیری مورد رسیدگی قرار گرفت، بهتراست جزئیات آن در دادگان مدیریت رخداد امنیت اطلاعات ثبت گردد.

راهنمای پاسخگویی با رخدادهای امنیت اطلاعات در بخش ۸-۲ ارئه گردیده است.

۸-۲ پاسخگویی‌ها

۸-۲-۱ پاسخگویی‌های آنی

۸-۲-۱-۱مرور کلی

در بیشتر موارد، فعالیت‌های بعدی برای عضو ISIRT، شناسایی اقدامات پاسخگویی آنی برای رسیدگی به رخداد امنیت اطلاعات، ثبت جزییات در برگه رخداد امنیت اطلاعات و در دادگان رویداد/ رخداد/آسیب‌پذیری امنیت اطلاعات، و اعلام اقدامات لازم به اشخاص یا گروه‌ها می‌باشد. این کار ممکن است به کنترل‌های فوری منتج شود (برای مثال، قطع‌کردن/خاموش‌کردن یک سامانه، خدمت و/یا شبکه‌ی اطلاعاتی آسیب دیده با توافق قبلی مدیریت IT و/یا کسب و کار مرتبط)، و/یا کنترل‌های دائمی دیگر شناسایی شده، و اعلام شده به شخص یا گروه واجد شرایط جهت اقدام. درصورتی که این اقدام از پیش صورت نگرفته باشد، بهتراست اهمیت رخداد امنیت، با استفاده از مقیاس رده‌بندی از پیش تعیین شده سازمان، تعیین گردد و در صورتی که به حد کفایت مهم باشد، بهتراست مدیریت ارشد مربوطه مستقیما آگاه شود. در صورتی که نیاز به اعلام موقعیت بحرانی محرز شود، برای مثال، بهتراست مسئول مدیریت بحران جهت فعال سازی احتمالی یک برنامه مدیریت بحران، همراه با مطلع ساختن مدیرISIRT و نیز مدیریت ارشد، مطلع شود.

اهداف کمی کلی در پاسخگویی به رخدادهای امنیت اطلاعات عبارتند از:

الف- محدود سازی اثرهای نامطلوب (مربوط به رخدادهای امنیت اطلاعات)، و

ب- بهبود امنیت اطلاعات.

بهتراست هدف اولیه‌ی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات و فعالیت‌های مرتبط، کمینه‌کردن اثرهای کسب و کار نامطلوب باشد، درحالی که شناسایی حمله‌کننده بهتراست به عنوان هدف ثانویه در نظر گرفته شود.

۸-۲-۱-۲ نمونه اقدامات

نمونه‌ای مرتبط از اقدامات پاسخگویی آنی درمورد حمله‌ی عمدی به یک شبکه یا سامانه، خدمت و/یا شبکه اطلاعاتی، حمله‌ای است که می‌تواند متصل به اینترنت یا شبکه‌ای دیگر باقی‌بماند. این کار به برنامه‌های کاربردی حیاتی کسب و کار اجازه می‌دهد که به درستی کارکنند، و تا حد امکان اطلاعات بیشتری درباره حمله‌کننده، به‌نحوی که حمله‌کننده اطلاع ندارد تحت مراقبت است، جمع‌آوری‌کند.

پیروی از فرایندهای برنامه‌ریزی شده و نگهداری سوابق اقدامات اهمیت حیاتی دارد. مراقب تروجان‌ها[1]، روت کیت‌ها[2] و ماژول‌های هسته[3] باشید که می‌توانند صدمات جدی بر سامانه وارد آوردند. شواهد را می‌توان با رمزنگاری، قفل‌ها و سوابق دسترسی محافظت کرد.

الف- هنگام اتخاذ چنین تصمیماتی، لازم است که درنظر گرفته شود حمله‌کننده ممکن است پی‌ببرد که تحت مراقبت است و ممکن است اقداماتی را که باعث وارد آمدن صدمات بیشتری به سامانه، خدمات و یا شبکه‌ی اطلاعاتی آسیب‌دیده و داده‌های مربوط شود، انجام‌دهد و حمله‌کننده می‌تواند اطلاعاتی را که ممکن است جهت ردگیری خود مفید باشد، نابود کند.

ب- بدیهی است، همین‌که تصمیم به قطع و/یا خاموش‌کردن سامانه، خدمت و/یا شبکه‌ی اطلاعات مورد حمله گرفته شود، از نظر فنی امکان اجرای سریع و قابل اطمینان آن وجود دارد. این کار به مهارکردن رخداد کمک می‌کند.

به‌طور معمول توجه به پیشگیری از وقوع دوباره از اولویت بالایی برخوردار است، و ممکن است به‌خوبی نتیجه گرفت که باید کاری کرد که برای حمله‌کننده، تلاش‌های ردگیری و تصحیح آسیب‌پذیری که ایجاد کرده است، دست آوردهای آن را توجیه نکند. این مسئله به‌خصوص هنگامی مناسبت دارد که حمله‌کننده مخرب نبوده و باعث ایجاد صدمه‌ای اندک و یا هیچ صدمه‌ای نشده است.

درمورد رخدادهای امنیت اطلاعات که در اثر عواملی غیر از حمله عمدی رخ داده باشد، بهتراست منبع آن‌ها شناسایی شود. ممکن است، در حالی‌که کنترل‌ها پیاده‌سازی شده‌اند، لازم باشد سامانه، خدمت و/یا شبکه

1-Trojans
1- Rootkits
2- Kernel Modules

اطلاعاتی و یا قسمت مرتبط جداشده آن‌را خاموش کرد (با موافقت قبلی با مدیریت IT و/یا کسب و کاری مرتبط)، در صورتی که آسیب‌پذیری برای سامانه، خدمت و/یا شبکه اطلاعاتی اساسی، یا یک آسیب‌پذیری حیاتی باشد، زمان خاموشی ممکن است مدت بیشتری به طول بیانجامد.

فعالیت پاسخگویی دیگر می‌تواند فعال‌سازی فنون مراقبت باشد (برای مثال، کوزه‌های عسل - استاندارد ملی ایران شماره۱۸۰۴۳: سال ۱۳۸۸ملاحظه شود). بهتراست این کار بر اساس روش‌های اجرایی مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات انجام شود.

اطلاعاتی که احتمال دارد ازطریق رخدادهای امنیت اطلاعات خراب شده‌باشد، بهتراست توسط عضو ISIRT ازنظر تغییرات، حذف‌ها، یا درج‌های اطلاعات، در مقایسه با سوابق پشتیبان وارسی شود. ممکن است لازم باشد صحت سوابق وارسی شود، زیرا یک حمله‌کننده عمدی ممکن است این سوابق را، برای پوشاندن ردگیری‌هایش دستکاری کرده باشد.[1]

۸-۲-۱-۳ روزآمدکردن اطلاعات رخداد

گام بعدی هر چه قرار است باشد، عضو ISIRT بهتراست گزارش رخداد امنیت اطلاعات را تا حد امکان روزآمد، آن را به دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات اضافه و مدیر ISIRT و در صورت لزوم، سایرین را مطلع نماید. روزآمدکردن می‌تواند اطلاعات را درموارد زیر بیشتر پوشش دهد:

الف- ماهیت رویداد امنیت اطلاعات چیست،

ب- چگونه و توسط چه چیزی و چه کسی ایجاد شده بود ،

پ- این رویداد بر چه چیزی تاثیر گذار است یا می‌تواند تاثیر گذار باشد،

ت- اثر واقعی یا بالقوه‌ی رویداد امنیت اطلاعات بر کسب‌وکار سازمان،

ث- تغییرات شاخص درمورد این که آیا رخداد امنیت اطلاعات قابل ملاحظه تلقی می‌شود یا خیر (با استفاده از مقیاس از پیش تعیین شده رده‌بندی سازمان)، و

ج- تاکنون چگونه به آن رسیدگی شده است.

اگر یک رویداد امنیت اطلاعات حل شده باشد، بهتراست گزارش شامل جزئیات کنترل‌های صورت‌گرفته و درس‌های آموخته باشد (مانند کنترل‌های بیشتری که باید جهت پیشگیری از وقوع دوباره یا وقوع موارد مشابه صورت‌گیرد). بهتراست گزارش در دادگان رویداد/رخداد/آسیب پذیری امنیت اطلاعات ثبت و به مدیر ISIRT و سایرین، برحسب نیاز، اعلام شود.

1- Manipulated

تاکید می شود که ISIRT مسئول اطمینان از نگهداری امن تمام اطلاعات مربوط به یک رخداد امنیت اطلاعات برای تحلیل‌های بیشتر، و استفاده‌ی به عنوان مدارک قانونی بالقوه می باشد. برای مثال، برای‌یک رخداد امنیت اطلاعات IT محور ، اقدامات زیر باید صورت پذیرد:

پس از کشف اولیه‌ی رخداد، بهتراست پیش از خاموش‌کردن سامانه، خدمت و یا شبکه‌ی آسیب‌دیده، همه‌ی داده‌های فرّار موجود برای بررسی کامل امور قانونی امنیت اطلاعات، جمع آوری گردند. اطلاعاتی که باید جمع آوری شود، شامل محتوای حافظه[1]، حافظه موقت[2] و ثبات‌ها[3]، و جزئیات هرگونه فعالیت در حال اجرا، و موارد زیر می‌باشد:

الف- بر حسب ماهیت رخداد امنیت اطلاعات، یک نسخه کامل از امور قانونی امنیت اطلاعات و یا یک پشتیبان سطح پایین از سوابق و پرونده‌های مهم در سامانه‌ی آسیب‌دیده قرار گرفته بهتراست تکثیر گردد.

ب- بهتراست سوابق سامانه‌ها، خدمات و شبکه‌های همسایه شامل مسیریاب‌ها و دیواره‌های آتش جمع‌آوری و بازنگری شود.

پ- بهتراست همه‌ی اطلاعات جمع‌آوری شده در رسانه فقط قابل خواندنی به‌طور امن ذخیره‌گردد.

ت- بهتراست هنگام اجرای امور قانونی امنیت اطلاعات، دو نفر و یا بیشتر، به منظور اثبات و گواهی این که همه‌ی فعالیت‌ها بر طبق قوانین و مقررات مرتبط بوده‌اند، در محل حاضر باشند.

ث- بهتراست مشخصات و توصیفات ابزارها و دستورات مورد استفاده در اجرای امنیت اطلاعات قانونی مستند و همراه رسانه‌ی اصلی ذخیره گردند.

یک عضو ISIRT همچنین مسئول ایجاد تسهیلات برای بازگرداندن امکانات آسیب‌دیده (اعم از IT یا غیر از آن) به موقعیت عملیاتی امن است. موقعیتی که امکانات، حتی الامکان در این مرحله، مستعد تخریب به وسیله حمله مشابه نیستند.

۸-۲-۱-۴ فعالیت‌های بیشتر

اگر یک عضو ISIRT حکم به واقعی بودن رخداد امینت اطلاعات بدهد، بهتر است سایر فعالیت‌های مهم موارد زیر باشند:

الف- فعالیت برای نهادینه‌کردن تحلیل امور قانونی امنیت اطلاعات، و

1- Memory
2- Cache
3- Registers

ب- فعالیت برای مطلع‌کردن مسئولین مبادلات حقایق و پیشنهادات داخلی و خارجی در زمینه اینکه چه چیزی بهتراست مبادله گردد، روی چه برگه‌ای و برای چه کسی.

همین‌که یک گزارش رخداد امنیت اطلاعات تکمیل شده‌است تا آنجا که ممکن است، بهتراست در دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات ثبت و با مدیر ISIRT مبادله شود.

در صورت احتمال طولانی تر شدن رسیدگی بیش از مدت زمان توافق شده توسط سازمان، بهتراست گزارشی موقت تهیه گردد.

بهتراست عضو ISIRT که ارزیابی یک رخداد امنیت اطلاعات را به عهده دارد، براساس راهنمای ارائه شده در مستندات طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات از موارد زیر آگاه باشد:

الف- چه وقت لازم است که مسائل تشدید شوند و برای چه کسی، و

ب- بهتراست ISIRT از روش‌های اجرایی کنترل تغییر در اجرای همه‌ی فعالیت‌ها پیروی کند.

هنگامی که مشکلاتی در تسهیلات ارتباطات الکترونیکی وجود دارد یا بنظر می‌رسد وجود داشته باشد (برای مثال در رایانامه یا تارنما) ازجمله زمانی که اندیشه امکان تحت حمله بودن سامانه وجوددارد، بهتراست گزارش آن به وسیله تلفن و یا پیام متنی برای اشخاص مرتبط ارسال گردد.

اگر نتیجه‌گیری شود که رخداد امنیت اطلاعات قابل‌ملاحظه بوده یا حکم به موقعیت بحرانی داده شود، بهتراست مدیر ISIRT به همراه مدیر امنیت اطلاعات سازمان و عضو مرتبط هیأت مدیره/ مدیر ارشد، با تمام طرف‌های مربوط هم داخلی و هم خارجی سازمان ارتباط برقرار نمایند.

برای حصول اطمینان از اینکه ارتباطات سریعا سازمان‌دهی شده و کارآمد می‌باشند، لازم است که از قبل یک روش امن ارتباطی برقرار گردد که تماما متکی به سامانه، خدمت و/یا شبکه که ممکن است تحت تاثیر رخداد امنیت اطلاعات واقع گردد، نباشد. این ترتیبات می‌تواند شامل تعیین مشاورین پشتیبان و یا در صورت نبودن آن‌ها، نماینده‌هایشان باشد.

۸-۲-۲ ارزیابی کنترل بر رخدادهای امنیت اطلاعات

پس از این که عضو ISIRT پاسخگویی‌های آنی و تحلیل امور قانونی فعالیت‌های امنیت اطلاعات مرتبط و ارتباطات را تحریک کرد، باید به سرعت معلوم شود که آیا رخداد امنیت اطلاعات تحت کنترل است. در صورت لزوم، عضو ISIRT می‌تواند با همکاران، مدیرISIRT و/یا اشخاص یا گروه‌های دیگر مشورت نماید.

اگر کنترل رخداد امنیت اطلاعات مورد تایید قرارگیرد، بهتراست عضو ISIRT هرگونه پاسخگویی و تحلیل امور قانونی امنیت اطلاعات و ارتباطات ضروری بعدی را جهت خاتمه دادن به رخداد امنیت اطلاعات و بازگرداندن[1] سامانه‌ی اطلاعاتی آسیب‌دیده به عملیات عادی، برقرارکند[2].

اگر تایید شود که رخداد تحت کنترل در نیامده است، در این صورت عضو ISIRT بهتراست فعالیت‌های بحرانی را نهادینه کند.

اگر رخداد امنیت اطلاعات مربوط به فقدان دسترسی‌پذیری است، متریک ارزیابی اینکه یک رخداد امنیت اطلاعات تحت کنترل است می‌تواند زمان سپری‌شده قبل از دوره بازیابی به یک وضعیت عادی باشد، بیشتر از اینکه مربوط به وقوع یک رخداد امنیت اطلاعات باشد. سازمان بهتراست بر مبنای نتایج ارزیابی مخاطره‌ی امنیت اطلاعات، برای هر دارایی بازه زمانی وقفه قابل قبول خودرا تعیین کند، این زمان بازیابی مورد نظر قبل از ادامه خدمت یا دسترسی به اطلاعات را پشتیبانی می‌کند. همین که زمان پاسخگویی از زمان وقفه قابل قبول تعیین شده دارایی هدف تجاوزکند، ممکن است دیگر رخداد امنیت اطلاعات تحت کنترل نباشد و تصمیم برای تشدید رخداد امنیت اطلاعات بهتراست اتخاذ گردد.

رخدادهای امنیت اطلاعاتی مربوط به فقدان محرمانگی، صحّت وغیره، به انواع دیگری از قضاوت‌ها برای تعیین اینکه آیا موقعیت تحت کنترل است و متریک‌های ممکن مرتبط با برنامه‌ی مدیریت بحران سازمان، نیاز دارد.

۸-۲-۳ پاسخگویی‌های بعدی

با تعیین اینکه یک رخداد امنیت اطلاعات تحت کنترل است و تابع فعالیت‌های بحران نیست، بهتر است عضو ISIRT ضرورت و ماهیت پاسخگویی‌های مورد نیاز بعدی را جهت رسیدگی رخداد امنیت اطلاعات شناسایی کند. این کار می‌تواند شامل بازسازی سامانه(ها)، خدمت(ها) و/یا شبکه(ها)ی آسیب‌دیده برای بازگشت به عملیات عادی باشد. این فرد بهتراست جزئیات را بر روی برگه گزارشات امنیت اطلاعات و دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات ثبت نموده و مسئولین تکمیل اقدامات مربوط را مطلع نماید. همین‌که این اقدامات با موفقیت تکمیل شد، جزییات عملیات بهتراست بر روی برگه گزارش رخداد امنیت اطلاعات و در دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات ثبت شده، و سپس بهتراست رخداد امنیت اطلاعات مذکور بسته شده و کارکنان ذی‌صلاح از آن مطلع گردند.

برخی از پاسخگویی‌ها در جهت پیش‌گیری از وقوع دوباره یا وقوع موارد مشابه رخداد امنیت اطلاعات می‌باشد. برای مثال اگر معلوم شود که علت یک رخداد امنیت اطلاعات یک خطای سخت‌افزار یا نرم‌افزار IT بدون یک وصله قابل دستیابی است، بهتراست سریعا با تامین‌کننده آن تماس گرفته شود. اگر یک

1- Restoring
2- Instituite

آسیب‌پذیری شناخته شده مشخص IT در یک رخداد امنیت اطلاعات دخیل باشد، بهتراست به امنیت اطلاعات روزآمد مرتبط وصل شود. هر نوع مشکلات مربوطه به پیکربندی IT که توسط رخداد امنیت اطلاعات برجسته شده باشند, بهتراست پس از آن مورد رسیدگی قرار گیرد. معیارهای دیگری برای کاهش امکان تکرار یا وقوع موارد مشابه یک رخداد امنیت اطلاعات IT می‌تواند شامل تغییر رمزهای عبور سامانه و غیبرطرف کردنال‌کردن خدمات بدون استفاده باشد.

حوزه‌ی دیگر فعالیت پاسخگویی می‌تواند دربردارنده‌ی پایش سامانه، خدمت و/یا شبکه IT باشد. به دنبال ارزیابی یک رخداد امنیت اطلاعات، ممکن است به‌کاربردن کنترل‌های پایش بیشتری جهت آشکارسازی رویدادهای غیرعادی و مشکوک که علامت[1] رخدادهای امنیت اطلاعات بیشتری خواهدبود، امری مناسب باشد. چنین پایشی همچنین می‌تواند عمق بیشتری از رخداد امنیت اطلاعات و تشخیص دیگر سامانه‌های IT که به مخاطره افتاده بودند را آشکار سازد.

ممکن است فعال‌سازی پاسخگویی‌های مشخص مستند شده در برنامه‌ی مدیریت بحران مرتبط کاملا ضروری باشد. این کار می‌تواند درمورد رخدادهای امنیت اطلاعات مربوط به IT و غیرIT کاربرد داشته باشد. چنین پاسخگویی‌هایی بهتراست شامل همه‌ی جنبه‌های کسب‌وکار، نه تنها آن چه مستقیما مربوط به IT ، بلکه همچنین کارکرد کلیدی نگهداری و بازسازی بعدی کسب‌وکار– شامل، برحسب ارتباط، مخابرات صوتی، و سطوح کارکنان و تسهیلات فیزیکی گردد.

آخرین حوزه‌ی فعالیت، بازسازی سامانه(ها)، خدمت(ها) و/یا شبکه(ها)ی آسیب‌دیده به عملیات عادی است. بازسازی یک سامانه(ها)، خدمت(ها) و/یا شبکه(ها)ی آسیب‌دیده به شرایط عملیاتی امن، می‌تواند از طریق کاربرد وصله‌ها در مورد آسیب‌پذیری‌های شناخته‌شده، و یا غیر فعال‌سازی عنصری که مورد مخاطره قرار گرفته بود، محقق گردد. اگر سراسر گستره‌ی رخداد امنیت اطلاعات به خاطر تخریب سوابق در طول رخداد، ناشناخته مانده است، در این صورت یک بازسازی[2] کامل سامانه، خدمت و/یا شبکه ممکن است ضروری باشد. فعال سازی قسمت‌های مرتبط با برنامه مدیریت بحران ممکن است کاملا ضروری باشد.

اگر یک رخداد امنیت اطلاعات غیر مرتبط با IT باشد، برای مثال در اثر یک آتش سوزی، سیل یا انفجار بمب، در این صورت فعالیتهای بازیابی که باید از آن‌ها پیروی کرد عبارتند از فعالیتهایی که در برنامه مدیریت بحران مرتبط مستند شده‌اند.

۸-۲-۴ پاسخگویی‌ها با موقعیت‌های بحرانی

همانطور که در بند ۸-۲-۲ بحث شد، ممکن است ISIRT معین کند یک رخداد امنیت اطلاعات تحت کنترل نیست و نیاز به تشدید آن به موقعیت بحرانی، با استفاده یک برنامه از قبل طراحی شده دارد.

1- Symptomatic
2- Rebuild

بهترین گزینه‌ها برای رسیدگی به تمام انواع ممکن رخدادهای امنیت اطلاعات که ممکن است بر دسترسی‌پذیری و تا حدی بر صحت سامانه‌ی اطلاعات تاثیر گذار باشند، بهتراست در برنامه‌ی مدیریت بحران سازمان شناسایی شده‌باشند. بهتراست این گزینه‌ها مستقیما با اولویت‌های مربوط به کسب‌وکار سازمان و معیارهای زمانی مربوط به بازیابی، و بنابراین بیشینه‌کردن بازه زمانی قابل‌قبول قطع خدمات IT، صوت، اشخاص و اماکن، باشد. این راهبرد بهتراست موارد زیر را شناسایی کند:

الف- معیارهای پیش‌گیرانه، تنش پذیری[1] و مدیریت بحران مورد نیاز،

ب- ساختار و مسئولیت‌های سازمانی مورد نیاز برای پاسخگویی با بحران ، و

پ- ساختار و محتوی کلی مورد نیاز برای برنامه یا برنامه‌های مدیریت بحران.

برنامه(ها)ی مدیریت بحران و کنترل‌هایی که به منظور پشتیبانی از فعال‌سازی این برنامه(ها) به کار برده شده‌اند، همین‌که به‌طور رضایت‌بخشی آزموده می‌شوند، مبنایی برای رسیدگی به شدیدترین رخدادهایی که زمانی برای آن طراحی شده‌اند، تشکیل می‌دهند.
بسته به نوع رخداد و در صورتی که تحت کنترل نیست، این ارجاع به مرجع بالاتر ممکن‌است به فعالیت‌های جدی برای رسیدگی به رخداد و فعال‌ساختن برنامه مدیریت بحران، در صورت به‌کاربردن چنین برنامه‌ای، منجر گردد. چنین فعالیت‌هایی می‌تواند شامل فعال‌سازی موارد زیر باشد، اما محدود به آن‌ها نمی‌شود:

الف- امکانات اطفاء حریق و روش‌های اجرایی تخلیه‌ی محل،

ب- تسهیلات پیشگیری از سیل و روش‌های اجرایی تخلیه‌ی محل،

پ- ساماندهی بمب و روش‌های اجرایی تخلیه‌ی مربوط،

ت- بررسی‌کنندگان متخصصین تقلب[2] در سامانه‌ی اطلاعات، و

ث- بررسی‌کنندگان متخصصین حمله فنی.

۸-۲-۵ تحلیل امور قانونی امنیت اطلاعات

جایی که بنا بر ارزیابی غیررسمی قبلی از شواهد در مقوله یک رخداد امنیت اطلاعات، یک رخداد قابل ملاحظه شناخته می‌شود، بهتراست تحلیل امور قانونی امنیت اطلاعات، توسط ISIRT انجام شود. بهتراست این تحلیل با جزییات بیشتری که تاکنون نسبت به فرآیند مدیریت رخداد امنیت اطلاعات انجام می‌شده است، با استفاده از ابزار و فنون بررسی مبتنی بر IT و باپشتیبانی روش‌های اجرایی مستند شده برای

1- Resilience
2-Fraud Investigators

بازنگری رخداد(ها)ی امنیت اطلاعات تعیین شده، انجام شود. این تحلیل بهتراست به روشی ساختار یافته انجام شود و، برحسب مورد، چیزهایی را که ممکن است برای روش‌های اجرایی انضباطی داخلی یا برای اقدامات قانونی به عنوان شواهد مورد استفاده قرار گیرند، شناسایی کند.

تسهیلات لازم برای تحلیل امور قانونی، احتمالا به تسهیلات فنی (برای مثال ابزار ممیزی، تسهیلات بازیابی شواهد)، روش اجرایی ، کارکنان و ایمنی دفتری رسته‌بندی شوند. هر فعالت تحلیل امور قانونی امنیت اطلاعات، بهتراست به صورت کامل مستند شود، ازجمله عکس‌های مرتبط، گزارش‌های تحلیل سابقه‌ی ممیزی، و سوابق بازیابی داده. کارآیی شخص یا اشخاصی که تحلیل امور قانونی امنیت اطلاعات را انجام می‌دهند، بهتراست همراه با سوابق آزمون‌های کارآیی مستند شوند. هر نوع اطلاعات دیگری که عینیت و ماهیت منطقی تحلیل را نشان می‌دهد، نیز بهتراست مستند شود. بهتراست خود همه‌ی سوابق رخدادهای امنیت اطلاعات، فعالیت‌های تحلیل امور قانونی امنیت اطلاعات، غیره و رسانه مرتبط، در محیط فیزیکی امن ذخیره شوند و با استفاده از روش‌های اجرایی کنترل شده، از دسترسی، تغییر یا نمایش دسترسی ناپذیری آن‌ها توسط اشخاص غیرمجاز، پیشگیری به‌عمل آید.تحلیل امور قانونی امنیت اطلاعات مبتنی بر ابزارهایIT بهتر است مطابق با استانداردهایی باشد که صحت آن‌ها بطور قانونی امکان چالش نداشته باشند و باید با تغییرات فناوری روزآمد گردند. بهتراست محیط فیزیکی ISIRT شرایط قابل اثباتی [1]را برای حصول اطمینان از اینکه شواهد طوری سامان‌دهی می‌شود که امکان چالش با آن‌ها وجود نداشته‌باشد، فراهم‌سازد. در صورت لزوم، بهتراست تعداد کافی از کارکنان، به صورت آماده به خدمت برای پاسخگویی در هر زمان، در دسترس باشند.

به مرور زمان ممکن است الزامات جدیدی برای بازنگری در شواهد رخدادهای امنیت اطلاعات گوناگون پدید آید، از جمله کلاه‌برداری، دزدی و خرابکاری. بنابراین، باید تعدادی وسایل مبتنی بر IT و روش‌های اجرایی پشتیبانی دردسترس باشد، تا ISIRT را برای آشکارساختن اطلاعات مخفی در یک سامانه، خدمت و یا شبکه اطلاعات کمک کند. این اطلاعات مخفی شامل اطلاعاتی است که به نظر می رسد در بازرسی اولیه حذف یا کد گذاری شده‌اند، و یا آسیب دیده‌اند. بهتراست این وسایل بر همه‌ی جنبه‌های شناخته شده‌ی مرتبط با انواع شناخته شده‌ی رخدادهای امنیت اطلاعات تاکید نموده و براساس روش‌های اجرایی ISIRT مستند شوند.

در جامعه‌ی امروز، غالبا تحلیل امور قانونی امنیت اطلاعات برای دربرگرفتن[2] محیط‌های شبکه‌ای پیچیده مورد نیاز هستند، در جایی که بررسی باید سراسر یک محیط عملیاتی، شامل تعدادی خدمتگزار (برای مثال پرونده، چاپ، ارتباطات و رایانامه)، همین‌طور تسهیلات دسترسی از راه دور، را دربربگیرد. ابزارهای زیادی وجوددارند، ازجمله ابزارهای جستجوی متن، درایو نرم‌افزار تصویربرداری[3] و اقامه دعاوی[4] در امور قانونی

1- Demonstrable
2- to encompass
3- Drive imaging software
4- Suites

امنیت اطلاعات. تمرکز اصلی روش‌های اجرایی تحلیل امور قانونی امنیت اطلاعات، حصول اطمینان از این است که شواهد دست نخورده حفظ شوند و وارسی کند تا اطمینان یابد این شواهد در برابر هر چالش قانونی قوی هستند.

تاکید می‌شود برای پیشگیری از تحلیلی که به صحت رسانه‌ی اصلی لطمه بزند، بهتراست کار تحلیل امور قانونی امنیت اطلاعات روی رونوشتی دقیق از داده اصلی انجام شود. فرایند تحلیل امور قانونی امنیت اطلاعات بهتراست فعالیت‌های زیر را، تا آنجا که مرتبط است، دربرگیرد:

الف- فعالیت برای حصول اطمینان از این که سامانه، خدمت و/یا شبکه هدف درطول تحلیل امور قانونی امنیت اطلاعات، از غیر قابل دسترس شدن، تغییر یافتن یا به مخاطره افتادن، از جمله با ورود کدمخرب (از قبیل ویروس‌ها) در امان است و این کار هیچ گونه آثاری روی عملیات عادی نخواهد داشت و یا اثر آن بسیار اندک خواهد بود.

ب- فعالیت برای اولویت‌بندی کسب و جمع‌آوری شواهد یعنی پیشرفت از فرّارترین تا غیرفرّارترین‌ها (این کار به میزان زیادی به ماهیت رخداد امنیت اطلاعات بستگی دارد).

پ- فعالیت برای شناسایی همه‌ی پرونده‌های مرتبط با سامانه، خدمت و/یا شبکه مورد نظر، از جمله پرونده‌های عادی، پرونده‌های دارای رمزعبور یا به طریق دیگری محافظت شده، و پرونده‌های رمزبندی شده[1].

ت- فعالیت برای بازیابی پرونده‌های حذف‌شده که کشف گردیده‌اند و سایر داده‌ها، تا حد امکان.

ث- فعالیت برای آشکارکردن اطلاعات آدرس‌های IP، اسامی میزبان‌ها، مسیرهای شبکه و پایگاه‌های اینترنتی.

ج- فعالیت برای استخراج محتوای پرونده‌های پنهان، موقت و جانشین[2] مورد استفاده به‌وسیله برنامه‌های کاربردی و نرم‌افزار سامانه عامل.

چ- فعالیت برای دسترسی به محتوای پرونده‌های محافظت شده یا رمزبندی شده (مگر این که منع قانونی وجود داشته باشد).

ح- فعالیت برای تحلیل همه داده‌های مرتبط ممکن موجود در فضاهای ذخیره لوح فشرده (و نوعاً غیرقابل دسترسی).

خ- فعالیت برای تحلیل زمان دسترسی، تغییر و ایجاد پرونده‌ها.

1- Encrypted
2- Swap

د- فعالیت برای تحلیل سوابق سامانه/خدمت/شبکه و برنامه کاربردی.

ذ- فعالیت برای تعیین فعالیت کاربران و/یا برنامه‌های کاربردی برروی یک سامانه/خدمت/شبکه.

ر- فعالیت برای تحلیل رایانامه‌ها برای منبع اطلاعات و محتوا.

ز- فعالیت برای انجام وارسی صحت پرونده برای آشکارسازی پرونده‌های[1] اسب تروجان و پرونده‌هایی که دراصل روی سامانه نیستند.

ژ- فعالیت برای تحلیل شواهد فیزیکی، درصورت امکان، برای مثال اثر انگشت، آسیب به دارایی، مراقبت تصویری، سوابق سامانه‌ی هشدار، سوابق دسترسی به کارت عبور و مصاحبه با شاهدان.

س- فعالیت برای حصول اطمینان از این که شواهد بالقوه‌ی استخراج شده طوری سامان‌دهی و ذخیره شوند که نتوانند صدمه ببینند یا غیر قابل استفاده شوند، و این که مطالب حساس توسط کارکنان غیرمجاز دیده نشوند. تاکید می شود که گردآوری شواهد همیشه بهتراست برطبق قوانین دادگاه و یا دادرسی انجام شود که در آن ممکن است نیاز به ارائه شواهد باشد.

ش- فعالیت برای رسیدن نتایج به دلایل وقوع رخداد امنیت اطلاعات، اقدامات لازم و برنامه زمان‌بندی، همراه با شواهدی شامل فهرست پرونده‌های مرتبط که در ضمیمه‌ی گزارش اصلی گنجانده شده‌اند.

ص- فعالیت برای فراهم‌کردن پشتیبانی تخصصی از هر نوع اقدام قانونی و انضباطی برحسب نیاز.

روش(ها)یی که باید تبعیت شوند بهتراست با روش‌های اجرایی ISIRT مستند گردند.

بهتراست ISIRT برای پوشش‌دادن به دانش فنی وسیعی (از جمله ابزارها و فنونی که احتمالا توسط حمله‌کنندگان عمدی مورد استفاده قرار می گیرند)، ارتقای تجربه تحلیل/بررسی (از جمله با توجه به حفظ از شواهد قابل استفاده)، دانش مفاهیم قانون‌گذاری و تنظیم مقررات مرتبط، و دانش پیشرفت رَوَندهای رخداد، ترکیب کاملی ازمهارت‌ها را مهیا کند.

بهتراست موارد زیر تشخیص داده شوند[2]:

الف- برخی سازمان‌ها ممکن است تمامی این منابع را در دسترس نداشته باشند و ممکن است لازم شود کار تحلیل امور قانونی امنیت اطلاعات به کارشناسان برون‌سپاری شود،

ب- در جائیکه احتمال وقوع لطمه جدی و/یا اقدامات جنایی وجوددارد، جمع‌آوری مطالب مربوط به امور قانونی امنیت اطلاعات ممکن است فقط یک پناهگاه باشد (یعنی تلاش و هزینه توجیه می‌شود)، و

1- Files
2- Recognized

پ- عدم استفاده از منابع کارشناسی برای اخذ مطالب مربوط به امور قانونی امنیت اطلاعات، در صورت نیاز به اقدام قانونی، ممکن است منجر به ناروا شدن یافته‌ها گردد.

۸-۲-۶ ارتباطات

در بسیاری از موارد، هنگامی که واقعی بودن یک رخداد امنیت اطلاعات توسط ISIRT تائید شده است، لازم است این موضوع به کارکنان خاصی در داخل (خارج از خطوط عادی ارتباطی مدیریت ISIRT) و در خارج، از جمله مطبوعات اطلاع داده شود. ممکن است لازم باشد این کار در چند مرحله به وقوع بپیوندد، برای مثال هنگامی که واقعی بودن یک رخداد امنیت اطلاعات تائید می‌شود، هنگامی که تحت کنترل بودن آن تائید می‌شود، هنگامی که فعالیت‌های بحرانی تعیین می‌شود، هنگامی که مسدود می‌شود، هنگامی که بازیابی پس از رخداد کامل شده‌است و نتایج حاصل می‌شود.

هنگامی که ارتباطات مورد نیاز است، بهتراست دقت زیادی برای حصول اطمینان از اینکه چه کسی نیاز به دانستن چه چیزی در چه هنگامی دارد، به عمل آید. ذی‌نفعانی که آسیب دیده‌اند، بهتراست معلوم شوند و ترجیحاً به گروه‌های زیر تقسیم شوند:

الف- ذی‌نفعان مستقیم داخلی (مدیریت بحران، کارمندان مدیریت و غیره)،

ب- ذی‌نفعان مستقیم خارجی (مالکین، مشتریان، شرکای، تامین‌کنندگان و غیره) ، و

پ- سایر تماس‌های خارجی مانند مطبوعات و/یا سایر رسانه‌ها.

هر گروه ممکن است به اطلاعات خاصی نیاز داشته‌باشد که بهتراست از مجاری مناسب سازمان تامین شود. یکی از مهم‌ترین وظایف ارتباطی پس از وقوع رخداد امنیت اطلاعات، این است که اطمینان حاصل شود که ذی‌نفعان مستقیم داخلی و خارجی، پیش از این که این اطلاعات از طریق سایر تماس‌های خارجی مانند مطبوعات به آن‌ها برسد، دارای اطلاعات هستند.

برای کمک به این فعالیت در هنگام نیاز، کار معقولی است که اطلاعات خاصی از پیش طوری تطبیق شوند که به سرعت با شرایط یک رخداد امنیت اطلاعات ویژه قابل تنظیم باشند و جهت گروه‌های مرتبط ، به‌ویژه به مطبوعات و/یا رسانه‌های دیگر ارسال شوند. اگر قرار باشد هر گونه اطلاعات مربوط به رخدادهای امنیت اطلاعات در مطبوعات منتشر شود، این کار بهتراست مطابق خط‌مشی انتشار اطلاعات[1] سازمان انجام شود. اطلاعاتی که قرار است منتشر شود، بهتراست توسط طرف‌های مرتبط که ممکن است شامل مدیریت ارشد، مسئولین هماهنگی روابط عمومی و کارکنان امنیت اطلاعات باشند، بازنگری گردد.

1-Information Dissemination Policy

یادآوری- ارتباطات رخداد امنیت اطلاعات ممکن است با توجه به رخداد و اثر آن در ترکیب با روابط سازمان و نوع کسب و کار، متفاوت باشد. نوع کسب و کار ممکن است قواعد[1] مشخصی را برای چگونگی انجام ارتباطات تنظیم کند، برای مثال اگر نام سازمان در فهرست بازار سهام عمومی[2] باشد.

۸-۲-۷ ارجاع به مرجع بالاتر

در شرایط حاد، اوضاع ممکن است برای اصلاح رخدادهایی که خارج از کنترل و خطری بالقوه برای اثر ناپسند بر کسب و کار هستند، تشدید شود. این رخدادها باید برای فعال‌سازی برنامه استمرار کسب‌وکار اگر مناسب باشد از طریق گزارش‌دهی به مدیریت ارشد، گروه دیگر در سازمان یا اشخاص یا گروه‌هایی در بیرون از سازمان، تشدید شوند. این تصمیم ممکن است براساس اقدامات توصیه شده برای رسیدگی به یک رخداد امنیت اطلاعات یا برای ارزیابی بیشتر به منظور تعیین اقدامات مورد نیاز، اتخاذ شود. این کار می‌تواند به دنبال فعالیت‌های ارزیابی که در بندهای ۷-۲ و ۷-۳ بالا توصیف شد، یا در طول فعالیت‌هایی که بعضی مسائل اصلی زود مشهود می‌شوند، انجام گردند. در مستندسازی طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات بهتر است راهنمایی برای کسانی که تا حدودی نیاز به تشدید کردن اوضاع دارند ارائه شود، یعنی اعضای PoC و ISIRT .

۸-۲-۸ ثبت‌کردن فعالیت و کنترل تغییر

تاکید شده است که همه‌ی آن‌هایی که در گزارش‌دهی و مدیریت یک رخداد امنیت اطلاعات دخیل هستند، بهتراست به درستی همه‌ی فعالیت‌ها را برای تحلیل‌های بعدی ثبت کنند. این امر بهتراست در برگه گزارش دهی رخداد امنیت اطلاعات و در دادگان رویداد/رخداد/آسیب پذیری امنیت اطلاعات گنجانده شود، مدام در سرتاسر چرخه‌ی یک رخداد امنیت اطلاعات از نخستین گزارش‌دهی تا تکمیل بازنگری پس از رخداد روزآمد شود.

این اطلاعات بهتراست به طور قابل اثباتی امن و با یک رژیم پشتیبان مناسب نگهداری شود. علاوه بر این، همه‌ی تغیرات ایجاد شده در مقوله ردگیری یک رخداد امنیت اطلاعات و روزآمدکردن برگه گزارش رخداد امنیت اطلاعات و دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات بهتراست تحت یک طرح‌واره‌ی کنترل تغییر رسمی، مقبول باشند.

1- Rules
2- Public stock market

۹ مرحله‌ی درس‌های آموخته شده

۹-۱ مرور کلی بر فعالیت‌های کلیدی

چهارمین مرحله‌ی استفاده عملیاتی از یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات به دنبال برطرف کردن/بسته شدن رخدادهای امنیت اطلاعات فرا می‌رسد، و شامل آموختن درس‌هایی است از این که چگونه رخدادها (آسیب‌پذیری‌ها) رسیدگی و ساماندهی شده‌اند. در مرحله‌ی درس‌های آموخته شده، سازمان بهتراست اطمینان حاصل کند که فعالیت‌های کلیدی عبارتند از:

الف- فعالیت برای انجام تحلیل امور قانونی بیشتر امنیت اطلاعات، برحسب نیاز .

ب- فعالیت برای شناسایی درس‌های آموخته شده از رخدادها و آسیب‌پذیری‌های امنیت اطلاعات.

پ- فعالیت برای بازنگری، شناسایی و بهبود پیاده سازی کنترل امنیت اطلاعات (کنترل‌های جدید و/یا روزآمد)، همین‌طور خط‌مشی مدیریت رخداد امنیت اطلاعات، در نتیجه‌ی درس‌های آموخته شده، چه از یک رخداد امنیت اطلاعات و یا از چند رخداد (و یا در واقع از آسیب‌پذیری‌های امنیتی گزارش شده). این کار با متریک‌هایی که به راهبرد سازمان کمک می‌کند که کجا روی کنترل‌های امنیت اطلاعات سرمایه گزاری شود، مورد حمایت قرار می‌گیرد.

ت- فعالیت برای بازنگری، شناسایی و بهبود ارزیابی مخاطره امنیت اطلاعات موجود سازمان و نتایج بازنگری مدیریت، به عنوان نتیجه‌ی درس‌های آموخته شده.

ث- فعالیت برای بازنگری میزان موثر بودن فرآیندها، روش‌های اجرایی ، قالب‌های گزارش‌دهی و/یا ساختار سازمانی در پاسخگویی، ارزیابی و بازیابی از هر رخداد امنیت اطلاعات و ساماندهی به آسیب‌پذیری‌های امنیت اطلاعات، و بر اساس درس‌های آموخته شده، شناسایی و بهبود در طرح‌واره‌ی مدیریت امنیت اطلاعات و مستندسازی آن.

ج- فعالیت برای روزآمد کردن دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات.

چ- فعالیت برای مبادله و به اشتراک‌گذاری نتایج بازنگری در یک جامعه قابل اعتماد [1] (اگر سازمان این را بخواهد).

تاکید می‌شود که فعالیت‌های مدیریت رخداد امنیت اطلاعات تکرار شوند، و بنابراین بهتراست یک سازمان به مرور زمان اصلاحات منظمی برای تعدادی از عناصر امنیت اطلاعات اعمال کند. این بهبودها بهتراست بر اساس بازنگری‌های داده مربوط به رخدادهای امنیت اطلاعات و پاسخگویی‌های با آن‌ها، و بر اساس آسیب‌پذیری امنیت اطلاعات گزارش شده، و همین‌طور رَوَندها به مرور زمان، پیشنهاد شوند.

1- A trusted community

۹-۲ تحلیل امور قانونی امنیت اطلاعات بیشتر

ممکن است همین‌که یک رخداد برطرف کردن می‌شود، هنوز به تحلیل امور قانونی امنیت اطلاعات برای شناسایی شواهد نیاز باشد. این کار بهتراست با استفاده از همان ابزار و روش‌های اجرایی که در بند ۸- ۲- ۵ پیشنهاد شده است، توسط ISIRT انجام شود.

۹-۳ شناسایی درس‌های آموخته شده

همین‌که پرونده رخداد امنیت اطلاعات بسته شد، بهتراست سازمان به سرعت درس‌هایی از سامان‌دهی رخداد امنیت اطلاعات را شناسایی کرده و بیاموزد و مهم این است اطمینان حاصل کند که براساس نتایج عمل میشود. علاوه بر این، ممکن است درس‌هایی از ارزیابی و برطرف کردن آسیب‌پذیری‌های امنیت اطلاعات گزارش شده، گرفته شود. درس‌ها می‌توانند به صورت زیر باشند:

الف- نیازهای جدید یا تغییر یافته برای کنترل‌های امنیت اطلاعات. این کنترل‌ها می تواند فنی یا غیرفنی (ازجمله فیزیکی) باشد. بسته به درس‌های آموخته شده، این نیازها می‌تواند شامل نیاز به روزآمدکردن سریع مطالب و ارائه آن‌ها در جلسات توجیهی اطلاع‌رسانی امنیت (برای کاربران و همین‌طور دیگر کارکنان)، و اصلاح و انتشار سریع راهنماها و/یا استانداردهای امنیتی باشد.

ب- اطلاعات تهدید و آسیب‌پذیری جدید و یا تغییر یافته و بنابراین تغییرات در نتایج بازنگری ارزیابی و مدیریت مخاطره امنیت اطلاعات کنونی سازمان.
پ- تغییرات در طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات و فرایندها، روش‌های اجرایی قالب گزارشات و/یا ساختار سازمانی، و دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات.

بهتراست یک سازمان به ماورای یک رخداد یا آسیب‌پذیری امنیت اطلاعات منفرد نگاه کند و رَوَندها/نمونه‌هایی[1] را وارسی کند که خود ممکن است به شناسایی نیاز به کنترل‌ها و یا تغییرات رویکرد کمک نمایند. پیگیری یک رخداد امنیت اطلاعات IT محور، برای اجرای آزمون امنیت اطلاعات، به‌ویژه ارزیابی آسیب‌پذیری نیز کار عاقلانه‌ای است. بنابراین سازمان بهتراست داده‌های موجود در دادگان رویداد/رخداد/آسیب‌پذیری امنیت اطلاعات را بر یک مبنای منظم برای کارهای زیر تحلیل کند:

الف- شناسایی روندها/نمونه‌ها،

ب- شناسایی حوزه‌های نگرانی، و

پ- تحلیل وضعیتی که در آن عمل پیشگیرانه می‌تواند برای کاهش احتمال رخدادهای آتی انجام شود.

1- Trends/Patterns

بهتراست اطلاعات مرتبط حاصل از کل دوره یک رخداد امنیت اطلاعات از کانال رَوَند/نمونه تحلیل شود (مشابه روشی که آسیب‌پذیری‌های رخداد امنیت اطلاعات گزارش شده سامان‌دهی می‌شوند). این امر در شناسایی زودهنگام رخدادهای امنیت اطلاعات نقش بسزایی داشته و بر اساس تجربه قبلی و دانش مستندشده درمورد اینکه در آینده چه رخدادهای امنیت اطلاعات، ممکن است رخ‌دهد، هشدار می‌دهد.

بهتراست از اطلاعات رخداد امنیت اطلاعات و آسیب‌پذیری مرتبط که از دولت، ISIRT های تجاری و تأمین‌کنندگان دریافت می‌گردد، استفاده شود.

آزمون ارزیابی/امنیت آسیب‌پذیری یک سامانه، خدمت و/یا شبکه اطلاعات بعد از یک رخداد امنیت اطلاعات، بهتراست فقط به سامانه، خدمت و/یا شبکه اطلاعاتی آسیب دیده از رخداد امنیت اطلاعات محدود نشود. این آزمون بهتراست ازطریق گنجاندن هر سامانه، خدمت و/یا شبکه اطلاعات گسترش یابد. یک ارزیابی کامل آسیب‌پذیری برای برجسته‌کردن وجود آسیب‌پذیری‌های استخراج‌شده در طول رخداد امنیت اطلاعات در سایر سامانه‌ها، خدمات و/یا شبکه‌های و برای حصول اطمینان از اینکه آسیب‌پذیری‌های جدید ایجاد نشده‌اند، استفاده می‌شود.

تأکید بر اینکه ارزیابی‌های آسیب‌پذیری بهتراست بر مبنای منظمی انجام شوند، و اینکه ارزیابی مجدد آسیب‌پذیری‌ها پس از اینکه یک رخداد امنیت اطلاعات به وقوع پوسته است بهتراست قسمتی از این فرایند ارزیابی مستمر، نه به عنوان یک جایگزین باشند، حائز اهمیت است.

بهتراست خلاصه تحلیل‌های رخدادها و آسیب‌پذیری‌های امنیت اطلاعات برای ارائه در همه جلسات گردهمایی[1] مدیریت امنیت اطلاعات سازمان و/یا سایر گردهمایی‌ها که در خط‌مشی امنیت اطلاعات کلی سازمان تعریف شده‌اند، تهیه شود.

۹-۴ شناسایی و ایجاد بهبود در کاربرد نظارت امنیت اطلاعات

درطول بازنگری پس از اینکه یک یا چند رخداد یا آسیب‌پذیری امنیت اطلاعات برطرف کردن شده‌اند، ممکن است طبق نیاز، کنترل‌های جدید یا تغییریافته شناسایی شوند. توصیه‌ها و الزامات مربوط به کنترل ممکن است طوری باشند که پیاده‌سازی فوری آن‌ها از نظر مالی و عملیاتی امکان پذیر نباشد و در هر مورد، آن‌ها بهتراست در اهداف بلندمدت سازمان تعریف[2] شوند. برای مثال، مهاجرت به یک دیواره آتش مستحکم و امن تر ممکن است در کوتاه‌مدت، به لحاظ مالی امکان‌پذیر نباشد اما لازم است این کار در اهداف امنیت اطلاعات بلندمدت سازمان قرار داده شود.

بر طبق توصیه‌های مورد توافق، سازمان بهتراست کنترل‌های روزآمد و/یا جدید را پیاده‌سازی کند. این کنترل‌ها می‌توانند کنترل‌های فنی (شامل فیزیکی) باشند و ممکن است شامل لزوم روزآمدکردن سریع

1- Forum
2- Feature

مطالب برای جلسات توجیهی اطلاع‌رسانی امنیتی (برای کاربران و همین‌طور سایر کارکنان) و ارایه در آن جلسات، و بازنگری سریع و صدور راهنماها و/یا استانداردهای امنیتی باشد. علاوه براین، بهتراست سامانه‌ها، خدمات و/یا شبکه‌های اطلاعات سازمان تابع ارزیابی‌های منظم آسیب‌پذیری، برای کمک به شناسایی آسیب‌پذیری‌ها و ارائه فرآیند تقویت مداوم سامانه، خدمت و شبکه باشند.

علاوه بر این، درحالیکه ممکن است بازنگری روش‌های اجرایی و مستندسازی شده مربوط به امنیت اطلاعات بلافاصله هنگام رشد فوری، بعد از رخدادهای امنیت اطلاعات یا یک آسیب‌پذیری برطرف کردن شده، انجام شود، به احتمال زیاد این بازنگری هنگام یک پاسخگویی بعدی مورد نیاز باشد. سازمان بهتراست پس از یک رخداد امنیت اطلاعات یا برطرف کردن یک آسیب‌پذیری، روش‌های اجرایی و خط‌مشی‌های امنیت اطلاعات خود را، درصورت مناسب بودن، روزآمد کند تا اطلاعات جمع‌آوری شده، و همه مشکلات شناسایی شده در طول دوره فرآیند مدیریت رخداد را مورد نظر قراردهد. این کار بهتراست یک هدف بلندمدت برای ISIRT، در پیوند با مدیریت امنیت اطلاعات سازمان باشد تا اطمینان حاصل شود که این خط‌مشی امنیت اطلاعات و روزآمدکردن روش اجرایی در سرتاسر سازمان تبلیغ[1] می‌شوند.

۹-۵ شناسایی و ایجاد بهبود در مدیریت مخاطره امنیت اطلاعات ونتایج بازنگری مدیریت

بسته به شدت و اثر یک رخداد امنیت اطلاعات (یا شدت و اثر بالقوه مربوط به یک آسیب‌پذیری امنیت اطلاعات گزارش‌شده)، ممکن است یک ارزیابی نتایج بازنگری ارزیابی و مدیریت مخاطره امنیت اطلاعات برای در نظر گرفتن تهدیدها و آسیب‌پذیری‌های جدید لازم باشد. به عنوان یک پیگیری تکمیل روزآمدکردن بازنگری ارزیابی و مدیریت مخاطره امنیت اطلاعات، ممکن است لازم باشد کنترل‌های جدید یا تغییر یافته مطرح شوند (بند ۹- ۴ ملاحظه شود).

۹-۶ شناسایی و بهبود طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات

بهتراست قطعنامه پس از رخداد، مدیر ISIRT یا یک کاندیدای احراز این پست، همه‌ی چیزهایی که در ارزیابی رخ داده اند را بازنگری کند و کمیّت[2] اثربخشی کل پاسخگویی با یک رخداد امنیت اطلاعات را تعیین کند. هدف چنین تحلیلی این است که تعیین کند کدام قسمت از طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات با موفقیت انجام می‌شوند و نیاز به هر بهبودی راشناسایی کند.

یک جنبه مهم تحلیل پاسخگویی پس از رخداد، دادن بازخورد اطلاعات و دانش به طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات است. اگر سازمان به اندازه کافی سخت‌گیر باشد، بهتراست اطمینان حاصل کند که برگزاری جلسه‌ای متشکل از همه گروه‌های مرتبط بلافاصله پس از برطرف کردن مشکل، درحالیکه اطلاعات

1- Propagated
2- Quantify

هنوز در ذهن کارکنان مرتبط تازه است، زمان‌بندی شود. عواملی که در چنین جلساتی مورد توجه قرار می-گیرند عبارتند از:

الف- آیا روش‌های اجرایی مشخص شده در طرح‌واره‌ی مدیریت رخدادهای امنیت اطلاعات طبق خواسته عمل نمود؟

ب- آیا روش‌های اجرایی یا شیوه‌هایی که به آشکارسازی رخداد کمک کرده باشند وجود دارد؟

پ- آیا روش‌های اجرایی یا ابزارهایی که در فرآیند پاسخگویی کمک کرده‌باشند شناسایی شدند؟

ت- آیا روش‌های اجرایی که در بازیابی سامانه‌های اطلاعاتی پس از شناسایی رخداد، کمک کرده‌باشند موجود بود ؟

ث- آیا ارتباط رخداد با همه طرف‌های مرتبط در سرتاسر فرآیند آشکارسازی ، گزارش‌دهی و پاسخگویی مؤثر بود؟

بهتراست نتایج جلسه مستند شوند. بهتراست سازمان اطمینان حاصل کند که حوزه‌های شناسایی شده برای بهبود طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات بازنگری و تغییرات موجه در یک مستندسازی طرح‌واره‌ی روزآمد گنجانده می‌شوند. تغییرات در فرآیندها، روش‌های اجرایی و برگه‌های گزارش مدیریت رخداد امنیت اطلاعات باید قبل از اجرا، وارسی کامل و آزموده شوند.

۹-۷ سایر بهبودها

سایر بهبودها ممکن است در مرحله درس‌های آموخته شده شناسایی شده باشند، برای مثال تغییرات در خط‌مشی‌ها، استانداردها و روش‌های اجرایی امنیت اطلاعات و تغییرات در پیکربندی‌های سخت‌افزار و نرم-افزار IT. بهتر است سازمان از عملیاتی شدن این فعالیت‌ها اطمینان حاصل نماید.

پیوست الف

(اطلاعاتی)

جدول مرجع متقاطع استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷ در مقایسه با این استاندارد ملی

بند استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷	بند ISO/IEC 27035
۴-۲-۲ پیاده‌سازی و عملیاتی‌کردن سامانه مدیریت امنیت اطلاعات (ISMS)[1] سازمان بهتراست کارهای زیر را انجام دهد. ح- پیاده‌سازی روش‌های اجرایی و سایر کنترل‌هایی که ظرفیت توانایی آشکارسازی فوری رویدادهای امنیتی و پاسخگویی با رخدادهای امنیتی را امکان پذیر می‌سازند.	۴ (مرور کلی) برای مرور کلی پیاده‌سازی مدیریت رخداد امنیت اطلاعات ۵ (برنامه‌ریزی و آماده‌سازی) - محتوا می‌تواند به پیاده‌سازی مدیریت رخداد امنیت اطلاعات کمک کند. ۶ (آشکارسازی و گزارش‌دهی)، ۷ (ارزیابی و تصمیم)، ۸ (پاسخگویی‌ها) و ۹ (درسهای آموخته‌شده) – محتوا می‌تواند به عملیاتی‌کردن مدیریت رخدادهای امنیت اطلاعات کمک کند.
۴-۲-۳ پایش و بازنگری ISMS سازمان بهتراست کارهای زیر را انجام دهد. الف- اجرای روش‌های اجرایی و کنترل‌های پایش و بازنگری و سایر کنترل‌ها برای: ۲- اقدام به شناسایی فوری رخنه‌ها و رخدادهای موفق امنیت؛ ۴- کمک به آشکارسازی رویدادهای امنیتی و در نتیجه پیشگیری از رخدادهای امنیتی با استفاده از شاخص‌ها. ب- تعهد نسبت به بازنگری‌های منظم از اثربخشی ISMS (از جمله پرداختن خط‌مشی و اهداف ISMS، و بازنگری کنترل‌های امنیت) در نظر گرفتن نتایج ممیزی امنیتی، **رخدادها**، اندازه‌گیری اثربخشی، پیشنهادات و بازخورد از همه طرف‌های علاقمند.	۹ (درس‌های آموخته‌شده) - محتوا می‌تواند به پایش و بازنگری مدیریت رخداد امنیت اطلاعات کمک کند.
۴-۳-۳ کنترل سوابق سوابق بهتراست محل نگهداری عملکرد فرایند همانگونه که در بند ۴- ۲ خلاصه شده‌است و همه وقایع فوق‌العاده **رخدادهای** امنیت اطلاعات مرتبط با ISMS باشند.	۵- ۱ (مرور کلی فعالیت‌های کلیدی)، ۶ (آشکارسازی و گزارش‌دهی) و پیوست ت (مثال رویداد امنیت اطلاعات، گزارشات و برگه‌های رخداد و آسیب‌پذیری)، محتوا می‌تواند به تعریف حوزه سوابق کمک کند.
۱۳ مدیریت رخداد امنیت اطلاعات	۴ (مرور کلی) برای بازنگری پیاده‌سازی مدیریت رخداد

1- Information Security Management System

بند استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷	بند ISO/IEC 27035
	امنیت اطلاعات. ۵ (برنامه‌ریزی و آماده‌سازی) - محتوا می‌تواند به پیاده‌سازی مدیریت رخداد امنیت اطلاعات کمک کند.
الف-۱۳-۱گزارش رویدادها و آسیب‌پذیری‌ها امنیت اطلاعات هدف: برای حصول اطمینان از اینکه رویدادها و آسیب‌پذیری‌های امنیت اطلاعات مرتبط با سامانه‌های اطلاعاتی به نحوی مبادله می‌شوند که موجب می‌شوند اقدام اصلاحی به موقع انجام شود. بهتراست روش‌های اجرایی رسمی گزارش‌دهی و ارجاع به مرجع بالاترِ رویداد درست به کار روند. همه کارمندان، پیمانکاران، و کاربران طرف سوم بهتراست از روش‌های اجرایی گزارش دهی انواع مختلف رویداد و آسیب‌پذیری‌هایی که ممکن است بر امنیت دارایی‌های سازمانی تأثیر بگذارند آگاه باشند. آن‌ها بهتراست هر نوع رویداد یا آسیب‌پذیری را با سرعت ممکن به PoC معین گزارش کنند. **الف-۱۳-۱-۱ گزارش دهی رویدادهای امنیت اطلاعات** کنترل:رویدادهای امنیت اطلاعات بهتراست ازطریق کانال‌های مناسب مدیریت با سرعت ممکن گزارش شوند. **الف-۱۳-۱-۲ گزارش‌دهی آسیب‌پذیری‌های امنیتی** کنترل: بهتر است از همه کارمندان، پیمان کاران و کاربران طرف سوم سامانه‌های اطلاعاتی و خدمات، خواسته شود هرگونه آسیب‌پذیری امنیتی مشهود و یا مشکوک سامانه‌ها یا خدمات را گزارش نمایند.	۵ (برنامه‌ریزی و آماده‌سازی) (به ویژه، بند۵- ۴ ملاحظه شود طرح‌واره‌ی مدیریت رخدادهای امنیت اطلاعات، ۵- ۵ ایجاد ISIRT، ۵- ۶ پشتیبانی فنی و دیگر پشتیبانی‌ها ، ۵- ۷ اطلاع‌رسانی و آموزش و ۵- ۸ آزمون طرح‌واره)، ۶ (آشکارسازی و گزارش‌دهی)، پیوست پ (مثال رویکردهای رده‌بندی و رسته‌بندی رویدادها و رخدادهای امنیت اطلاعات) و پیوست ت (مثال برگه‌ها و گزارشات رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات) – محتوا می‌تواند به گزارش رویدادها و آسیب‌پذیری‌های امنیت اطلاعات کمک کند. پیوست ت-۲-۱ (مثال اقلام سابقه رویداد امنیت اطلاعات) و پیوست ت-۴-۱ (مثال از گزارش رویداد امنیت اطلاعات) مثال برای برگه گزارش. پیوست ت-۲-۳ (مثال اقلام سابقه آسیب‌پذیری امنیت اطلاعات) و پیوست ت-۴-۳ (مثال برگه گزارش پرونده آسیب‌پذیری امنیت اطلاعات) مثال برای برگه گزارش.
الف-۱۳-۲ مدیریت رخدادها و بهبودهای امنیت اطلاعات هدف: حصول اطمینان از اینکه یک رویکرد ثابت و مؤثر برای مدیریت رخدادهای امنیت اطلاعات به کار می‌رود. بهتراست مسئولیت‌ها و روش‌های اجرایی مناسب باشند تا هنگام گزارش رویدادها و آسیب‌پذیری‌های امنیت اطلاعات، به‌طور موثری سامان‌دهی شوند. بهتراست فرآیند بهبود مستمر برای پاسخگویی، پایش، ارزشیابی و مدیریت کلی رخدادهای امنیت اطلاعات به کار رود.	۷ (ارزیابی و تصمیم)، ۸ (پاسخگویی‌ها)، و ۹ (درس‌های آموخته شده) و پیوست ب (مثال رخدادهای امنیت اطلاعات و علل آن‌ها)، پیوست پ (مثال رویکردهای رده‌بندی و رسته‌بندی رویدادها و رخدادهای امنیت اطلاعات) و پیوست ث (ابعاد قانونی و حقوقی).

بند استاندارد ملی ایران شماره ۲۷۰۰۱: سال ۱۳۸۷	بند ISO/IEC 27035
اگر شواهدی لازم باشد بهتراست آن را جمع‌آوری کرد تا اطمینان شود که کار مطابق الزامات قانون انجام می‌شود. **الف-۱۳-۲-۱ مسئولیت‌ها و روش‌های اجرایی** کنترل: روش‌های اجرایی و مسئولیت‌های مدیریت بهتراست برای حصول اطمینان از یک پاسخگویی سریع، مؤثر و منظم به رخدادهای امنیت اطلاعات، مستقر شود.	۷ (ارزیابی و تصمیم)، ۸ (پاسخگویی‌ها)، پیوست ت-۲- ۲ (مثال اقلام سابقه برای رخدادهای امنیت اطلاعات) و پیوست ت ۴- ۲ (مثال برگه گزارش رخداد امنیت اطلاعات) – محتوا می‌تواند به تعریف روش‌های اجرایی و مسئولیت‌ها کمک کند...
الف-۱۳-۲-۲ آموختن از رخدادهای امنیت اطلاعات کنترل: بهتراست سازوکارهایی وجود داشته باشد که به درستی قادر به کمّی‌کردن و پایش کردن انواع، مقادیر و هزینه‌های رخدادهای امنیت اطلاعات باشد. **الف-۱۳-۲-۳ جمع‌آوری شواهد** کنترل: پس از اقدام قانونی برای یک رخداد امنیت اطلاعات (مدنی یا جنایی)، چنانچه اقدامی برای پیگیری برعلیه یک شخص یا سازمانی انجام شود، بهتراست شواهد جمع‌آوری، نگهداری و ارائه شوند تا با قواعد شواهد تنظیم شده در دادگاه(های) مربوط مطابقت داشته باشد.	۹ (درس‌های آموخته‌شده) و پیوست ب (مثال رخدادهای امنیت اطلاعات و علل آن‌ها) و پیوست پ (مثال رویکردهای رده‌بندی و رسته‌بندی رویدادها و رخدادهای امنیت اطلاعات) – محتوا می‌تواند به آموختن از رخدادهای امنیت اطلاعات کمک کند. ۷ (ارزیابی و تصمیم گیری)، ۸ (پاسخگویی‌ها) (به ویژه تحلیل امور قانونی امنیت اطلاعات،بند ۸- ۲- ۵ ملاحظه شود) و پیوست ث (جنبه‌های قانونی و مقرراتی) – محتوا می‌تواند به تعریف روش‌های اجرایی جمع‌آوری شواهد کمک کند.

پیوست ب

(اطلاعاتی)

مثال‌هایی از رخدادهای امنیت اطلاعات و علل آن‌ها

ب-۱ حملات

ب-۱-۱ انکار خدمت

انکار خدمت (DoS) و انکار خدمت توزیع شده (DDoS) رسته وسیعی از رخدادهایی هستند که در یک راستا قرار دارند. این رخدادها موجب می‌شوند یک سامانه، خدمت یا شبکه، قادر به ادامه فعالیت نبوده و طبق ظرفیت مورد نظر کار نکنند، اغلب در آن، دسترسی به کاربران مشروع به طور کامل انکار می‌شود. دو نوع رخداد اصلی DoS/DDoS توسط وسایل فنی وجود دارند: حذف منابع و قحطی منابع.

بعضی از مثال‌های رایج رخدادهای DoS/DDoS فنی عمدی عبارتند از:

- رسیدگی[۱] به آدرس‌های شبکه پخش به منظور پرکردن پهنای باند شبکه با ترافیک پاسخ[۲]،
- ارسال داده در یک قالب غیر منتظره به یک سامانه، خدمت یا شبکه در تلاشی برای ساقط کردن و یا ایجاد اختلال در عملیات عادی آن،
- گشایش نشست‌های[۳] چندگانه مجاز با یک سامانه، خدمت یا شبکه ویژه در تلاشی برای تمام کردن منابع آن (یعنی کندکردن، قفل‌کردن، یا خراب‌کردن آن).

این حملات اغلب از طریق باتنت‌ها[۴]، مجموعه‌ای از ربات‌های نرم‌افزار (کد مخرب) که به طور خودگردان و خودکار اجرا می‌شوند، انجام می‌شوند. باتنت‌ها می‌توانند با چند صد الی چند میلیون رایانه آسیب دیده ارتباط داشته باشند.

بعضی از رخدادهای فنیDoS ممکن است به طور تصادفی ایجاد شوند، برای مثال ممکن است به خاطر پیکربندی غلط توسط بهره‌بردار[۵] یا ازطریق ناسازگاری نرم‌افزار کاربردی، اما بیشتر اوقات این رخدادهای تعمدی هستند. بعضی از رخدادهای فنی DoS عمداً برای خراب کردن یک سامانه یا خدمت، یا از کار انداختن یک شبکه، آغاز می‌شوند اما سایر رخدادها صرفاً محصول فرعی سایر فعالیت‌های مخرب هستند.

1- Pinging
2- Response Traffic
3 -Sessions
4-Botnets
5- Operator

برای نمونه، بعضی از فنون رایج‌تر پویش‌کردن[1] و شناسایی پنهانی می‌توانند هنگام پویش، موجب خرابی بعضی از خدمات یا سامانه‌های قدیمی‌تر یا آن‌هایی که پیکربندی درستی ندارند، شوند. بهتراست یادآوری کرد که بسیاری از رخدادهای تعمدی فنی DoS اغلب به صورت ناشناس اجرا می‌شوند (یعنی منبع حمله «ساختگی» است)، زیرا آن‌ها نوعاً تکیه بر بازگشت اطلاعات از شبکه یا سامانه مورد حمله به حمله کننده ندارند.

رخدادهای DoS که به وسیله ابزار غیر فنی ایجاد می‌شوند و موجب از دست رفتن اطلاعات، خدمات و/یا تسهیلات می‌شوند برای مثال می‌توانند به دلایل زیر ایجاد شوند:

- رخنه‌ها در تنظیمات امنیت فیزیکی که منجر به سرقت یا صدمه‌ی جدی و خرابی تجهیزات می‌شود،
- صدمه اتفاقی به سخت‌افزار (و/یا مکان آن) توسط آتش‌سوزی یا سیل،
- شرایط محیطی سخت، برای مثال دمای بالا هنگام عملیات (مانند براثر نقص دستگاه تهویه هوا)،
- نقص عملکرد یا بار زیاد سامانه،
- تغییرات کنترل نشده سامانه،
- نقص عملکرد سخت‌افزار یا نرم‌افزار.

ب-۱-۲ دسترسی غیرمجاز

به طور کلی این رسته از رخدادها شامل اقدامات واقعی برای دسترسی غیر مجاز به یک سامانه، خدمات، شبکه و یا سوء استفاده از آن‌ها هستند. چند مثال از رخدادهای دسترسی غیرمجاز شبیه‌سازی شده فنی شامل موارد زیر می‌باشند:

- تلاش برای بازیابی[2] پرونده‌های دارای رمز عبور،
- حملات سیل‌آسای بافر به عنوان تلاشی برای حصول دسترسی مجاز به هدف (برای مثال مدیر سامانه)،
- بهره‌برداری از آسیب‌پذیری‌های پروتکل برای ربودن یا راهنمایی غلط اتصالات قانونی شبکه،
- تلاش برای ارتقاء امتیازات برای منابع یا اطلاعات فراتر از آنچه که کاربر یا مدیر به طور قانونی دراختیار دارد.

1- Scanning
2- Retrieve

رخدادهای دسترسی غیرمجاز که توسط وسایل غیرفنی به وجود آمده اند و مستقیم یا غیر مستقیم منجر به افشا یا تغییر اطلاعات، رخنه‌ها در جوابگویی[1] یا سوء استفاده از سامانه‌های اطلاعاتی می‌شوند ممکن است برای مثال از طرق زیر ایجاد شوند:

- رخنه‌ها در تنظیمات امنیت فیزیکی منجر به دسترسی غیرمجاز به اطلاعات،
- پیکربندی ضعیف و/یا غلط سامانه‌های عامل براثر تغییرات کنترل نشده سامانه، یا نقص عملکرد نرم‌افزار یا سخت‌افزار.

ب-۱-۳ کد مخرب

کد مخرب، یک برنامه یا قسمتی از یک برنامه را شناسایی می‌کند که با نیت تغییر رفتار اصلی آن در یک برنامه دیگر داخل شده است تا فعالیت‌های سوئی همانند دزدی اطلاعات و هویت، تخریب اطلاعات و منابع، انکار خدمت، هرزنامه[2] و غیره را انجام دهد. حملات کد مخرب می‌تواند به پنج رسته تقسیم شوند: ویروس‌ها، کرم‌ها، اسب‌های تروجان، کد متحرک و مخلوط[3]. علی رغم اینکه چند سال پیش ویروس‌ها خلق شدند تا هر نوع سامانه آلوده آسیب‌پذیری مورد هدف قرار گیرد، اما امروزه کدهای مخرب برای هدف قرار دادن حملات به کار می‌روند. این کار، گاه یک کد مخرب موجود را تغییر می‌دهد و یک متغیر ایجاد می‌کند که اغلب توسط فناوری‌های آشکارسازی کد مخرب بازشناسی نمی شود.

ب-۱-۴ استفاده نامناسب

این نوع رخداد زمانی اتفاق می‌افتد که یک کاربر از خط‌مشی‌های امنیتی سامانه اطلاعات تخطی کند. چنین رخدادهایی، طبق مفهوم دقیق واژه، حمله تلقی نمی‌شوند، بلکه اغلب به عنوان رخدادها گزارش می‌شوند و بهتراست توسط ISIRT اداره شوند. استفاده نامناسب می‌تواند یکی از موارد زیر باشد:

- دریافت و نصب ابزارهای رخنه‌گری[4]،
- استفاده از رایانامه شرکت برای هرزنامه یا ترویج کسب‌وکار شخصی،
- استفاده از منابع شرکت برای راه‌اندازی یک وب سایت غیرمجاز،
- استفاده از فعالیت‌های نظیر به نظیر[5]، برای به‌دست آوردن یا توزیع پرونده‌های سرقت‌شده (موسیقی، ویدئو و نرم‌افزار).

1- Breaches of Accountability
2-Spam
3- Blended
4- Hacking
5- Peer-to Peer

ب-۲ گردآوری اطلاعات

به‌طور کلی، رسته‌بندی گردآوری اطلاعات رخدادها شامل فعالیت‌هایی می‌شود که به شناسایی اهداف بالقوه و درک خدماتی که براساس آن اهداف اجرا می‌شوند، مرتبط است. این نوع رخداد شامل عملیات اکتشافی[۱] می‌باشند و هدف این است که موارد زیر شناسایی شوند:

- وجود یک هدف و درک مکان‌نگاری[۲] شبکه اطراف آن و کسی که هدف به‌روال عادی با آن ارتباط دارد، و
- آسیب‌پذیری‌های بالقوه در هدف یا محیط شبکه بلافصل[۳] آن که می‌تواند مورد بهره‌برداری قرار گیرد.

مثال‌های رایج از حملات گردآوری اطلاعات با وسایل فنی عبارتند از:

- نسخه برداری[۴] از سوابق سامانه نام دامنه (DNS)[۵] برای دامنه اینترنت هدف (انتقال ناحیه DNS)،
- رسیدگی به آدرس‌های شبکه، برای یافتن سامانه‌هایی که« فعال» هستند،
- جستجو در سامانه برای شناسایی (برای مثال، اثر انگشت) سامانه عامل میزبان،
- پویش‌کردن ورودی‌های شبکه موجود روی یک سامانه برای شناسایی خدمات مربوط (برای مثال، رایانامه، پروتکل انتقال پرونده (FTP)[۶]، تارنما، و غیره) و همچنین نسخه نرم‌افزار آن خدمات،
- پویش‌کردن یک یا چند خدمات شناخته شده آسیب پذیر در سرتاسر گستره آدرس شبکه[۷] (پیداکردن افقی).

در بعضی از موارد، گردآوری اطلاعات به دسترسی غیر مجاز کشانیده می‌شود، اگر برای مثال، حمله کننده به عنوان قسمتی از جستجو برای آسیب‌پذیری‌ها، برای دست‌یابی به دسترسی غیرمجاز نیز تلاش کند. این کار عموما با ابزارهای رخنه‌گری خودکار انجام می‌شود که نه تنها آسیب‌پذیری‌ها را جستجو می‌کنند بلکه به طور خودکار، تلاش می‌کنند تا از سامانه‌ها، خدمات یا شبکه‌های آسیب‌پذیری که یافت می‌شوند بهره‌برداری کنند.

1- Reconnaissance
2- Topology Surrounding
3- Immediate Network Environment
4- Dumping
5- Domain Name System (DNS)
6-File Transfer Protocol (FTP)
7- Across a Network Address Range

رخدادهای گردآوری اطلاعات که توسط وسایل غیر فنی ایجاد می‌شوند، منجر به موارد زیر می‌شوند:

- افشا یا تغییر اطلاعات به طور مستقیم یا غیرمستقیم،
- سرقت مالکیت معنوی[1] ذخیره شده به صورت الکترونیکی،
- رخنه‌های پاسخگویی برای مثال ثبت سوابق حساب،
- سوء استفاده از سامانه‌های اطلاعاتی (برای مثال خلاف قانون یا خط‌مشی سازمان).

این موارد، برای مثال، می‌توانند به دلایل زیر ایجاد شوند:

- رخنه‌های تنظیمات امنیت فیزیکی که منجر به دسترسی غیرمجاز به اطلاعات، و سرقت تجهیزات ذخیره اطلاعات که حاوی داده‌های مهم، برای مثال، کلیدهای رمزنگاری هستند،
- سامانه‌های عامل که به علت تغییرات کنترل نشده، یا سوء کارکرد نرم‌افزار یا سخت‌افزار دارای پیکربندی ضعیف یا پیکربندی غلط و منجر به دسترسی کارکنان داخلی یا خارجی به اطلاعاتی می‌شود که اجازه آن را ندارند.

1- Intellectual property

پیوست پ

(اطلاعاتی)

مثال رویکردهایی برای رده‌بندی و رسته‌بندی رویدادها و رخدادهای- امنیت اطلاعات

پ-۱ مقدمه

این پیوست مثال رویکردهای رده‌بندی و رسته‌بندی رخداد امنیت اطلاعات را ارائه می‌کند. این رویکردها کارکنان یا سازمان را قادر می‌سازد رخدادهای امنیت اطلاعات را به شیوه‌ای پایدار مستند کنند که مزایای زیر حاصل شوند:

- ارتقاء تبادل و به اشتراک‌گذاری اطلاعات مربوط به رخدادهای امنیت اطلاعات،
- آسان‌ترکردن خودکارسازی گزارش‌دهی پاسخگویی و رخدادهای امنیت اطلاعات،
- بهبود کارآیی و اثربخشی سامان‌دهی و مدیریت رخدادهای امنیت اطلاعات،
- تسهیل جمع‌آوری و تحلیل داده مربوط به رخدادهای امنیت اطلاعات، و
- شناسایی سطوح شدت رخدادهای امنیت اطلاعات با استفاده از یک معیار پایدار

این رویکردهای نمونه رده‌بندی و رسته‌بندی می‌توانند برای رویدادهای امنیت اطلاعات نیز به کار روند، اما آسیب‌پذیری‌های امنیت اطلاعات را پوشش نمی‌دهند.

پ-۲ رسته‌بندی رخدادهای امنیت اطلاعات

رخدادهای امنیت اطلاعات ممکن است به دلیل اقدامات عمدی یا تصادفی انسانی، و ممکن است ازطریق وسایل فنی یا فیزیکی به وجود آمده باشند. رویکرد زیر رخدادهای امنیت اطلاعات را با درنظرگرفتن تهدیدات به عنوان عوامل رسته‌بندی، رسته‌بندی می‌کند. (درباره تهدیدات، در استاندارد ملی ایران شماره ۲۷۰۰۵: سال ۱۳۸۸، پیوست پ، به مثال تهدیدات رایج اشاره می‌شود). فهرستی از رسته‌بندی‌های رخدادهای امنیت اطلاعات در جدول پ- ۱ نشان داده شده است.

جدول پ- ۱ رسته‌های رخدادهای امنیت اطلاعات با توجه به تهدیدها

رسته	شرح	مثال‌ها
رخداد بلایای طبیعی	از دست‌رفتن امنیت اطلاعات براثر بلایای طبیعی فراتر از کنترل انسان	زلزله، آتشفشان، سیل، تندباد، رعد و برق، سونامی، سقوط، غیره.
رخداد ناآرامی‌های اجتماعی	از دست‌رفتن اطلاعات به علت اغتشاشات اجتماعی.	وضعیت فوق‌العاده[1]، حمله تروریستی، جنگ و غیره
رخداد صدمه فیزیکی	از دست‌رفتن امنیت اطلاعات به علت اقدامات فیزیکی عمدی یا تصادفی.	آتش، آب، الکترواستاتیک، محیط‌های کثیف (مانند آلودگی، غبار، فرسودگی، انجماد)، خرابی تجهیزات، خرابی رسانه، سرقت تجهیزات، سرقت رسانه، از دست‌رفتن تجهیزات، از دست‌رفتن رسانه، دستکاری تجهیزات، دستکاری رسانه و غیره.
رخداد خرابی زیرساخت	از دست‌رفتن امنیت اطلاعات به علت خرابی سامانه‌ها و خدمات پایه که اجرای سامانه‌های اطلاعاتی را پشتیبانی می‌کنند.	خرابی منبع تغذیه، خرابی شبکه، خرابی دستگاه تهویه هوا، خرابی منبع آب و غیره
رخداد تشعشع رادیویی	از دست‌رفتن امنیت اطلاعات براثر اختلال ناشی از تشعشعات است.	تشعشع الکترومغناطیس[2]، پالس الکترومغناطیس[3]، تراکم الکترونیکی[4]، نوسان ولتاژ[5]، تشعشع حرارتی[6] و غیره.
رخداد خرابی فنی	از دست‌رفتن اطلاعات براثر خرابی در سامانه‌های اطلاعاتی و یا تسهیلات غیر فنی مربوط، همین‌طور مشکلات غیرعمدی انسانی است که منجر به دسترس‌ناپذیری و خرابی سامانه‌های اطلاعاتی می‌شوند.	خرابی سخت‌افزار، خرابی نرم‌افزار، سربار (اشباع ظرفیت سامانه‌های اطلاعاتی)، رخنه در نگهداری و غیره

1-Bedin
2- Electromagnetic radiation
3- Electromagnetic pulse
4- Electronic jamming
5- Voltage fluctuation
6- Thermal radiation

رسته	شرح	مثال‌ها
رخداد بدافزار	از دست‌رفتن امنیت اطلاعات بر اثر برنامه‌های مخربی است که به‌طورعمدی ایجاد و منتشر می‌شوند. یک برنامه مخرب در سامانه‌های اطلاعاتی وارد می‌شود و به محرمانگی، صحت یا دسترسی‌پذیری به داده، برنامه‌های کاربردی یا سامانه‌های عامل صدمه می‌زند، و/یا بر عملیات عادی سامانه‌های اطلاعاتی تأثیر می‌گذارد.	ویروس رایانه‌ای، کرم شبکه، اسب تروجان، بات-نت[1]، حملات مخلوط، کد مخرب تعبیه‌شده در صفحه تارنما[2]، پایگاه میزبانی کد مخرب[3]، غیره. ویروس رایانه، مجموعه‌ای از دستورالعمل‌های رایانه ای یا کدی است که وارد برنامه‌های رایانه می‌شود. برخلاف برنامه‌های عادی، این ویروس توانایی تکثیر خود را دارد و به‌طورعادی بار سنگینی را حمل می‌کند که ممکن است به عملکرد رایانه صدمه بزند و یا داده‌ها را خراب کند. کرم شبکه، برخلاف ویروس رایانه، نوعی برنامه مخرب است که خود را ازطریق شبکه‌ها به طور خودکار گسترش می‌دهد و تکثیر می‌کند، و این کار را با بهره برداری از آسیب‌پذیری سامانه‌های اطلاعاتی در شبکه انجام می‌دهد. اسب تروجان نوعی برنامه مخرب است که در سامانه‌های اطلاعاتی، ظاهر کارکردهای بی مخاطره را به خود می‌گیرد و می‌تواند سازنده را قادر کند کنترل سامانه‌های اطلاعاتی، از جمله سرقت یا جدا کردن اطلاعات از سامانه‌ها، را در اختیار بگیرد. بات‌نت، گروهی از رایانه‌های به مخاطره افتاده (زامبی[4]) در شبکه‌هایی است که به طور مرکزی توسط سازنده بات‌نت – که به عنوان کنترل کننده بات‌نت یا محافظ آن شناخته می‌شود – کنترل می‌گردد. باتنت‌ها به طور عمدی از طریق آلوده کردن انبوهی از رایانه‌های شبکه‌هایی که برنامه‌های بات[5] دارند ساخته می‌شوند. بات‌نت‌ها را می‌توان برای حملات فرصت طلبانه شبکه‌ای، سرقت اطلاعات، و پخش اطلاعات اسب‌های تروجان، کرم‌های شبکه و سایر برنامه‌های مخرب مورد

1- Botnet
2- Malicious code embedded web
3- Malicious code hosting site
4- Zombie
5- Bot programs

رسته	شرح	مثال‌ها
		استفاده قرارداد. حملات مخلوط ممکن است خصوصیات ویروس‌های رایانه، کرم‌های شبکه، اسب‌های تروجان یا باتنت‌ها را ترکیب کرده باشند. حملات مخلوط ممکن است ناشی از عملیات مرکب مجموعه‌ای از برنامه‌های مخرب مختلف باشند. برای مثال، یک ویروس رایانه یا کرم شبکه وارد سامانه رایانه می‌شود، و سپس یک اسب تروجان را در سامانه نصب می‌کند. یک کد مخرب تعبیه‌شده در صفحه تارنما، پایگاه اینترنتی را ازطریق گنجاندن کد مخرب که بدافزاری را برروی سامانه رایانه‌ای نصب می‌کند، محو می‌نماید. سایت کد مخرب میزبان، یک وب سایت را برای کد مخربی که توسط کاربران هدف دریافت می‌شود به عنوان طعمه قرار می‌دهد.
رخداد حمله فنی	از دست‌رفتن امنیت اطلاعات براثر حمله سامانه‌های اطلاعاتی در شبکه‌ها یا سایر وسایل فنی ایجاد می‌شود و این کار یا با بهره‌برداری از آسیب‌پذیری‌های سامانه‌های اطلاعات در پیکربندی‌ها، پروتکل‌ها یا برنامه‌ها انجام می‌شود یا به زور، و این منجر به وضعیت غیرعادی سامانه‌های اطلاعاتی، و یا صدمه بالقوه به عملکردهای سامانه کنونی می‌شود.	پویش‌کردن شبکه، بهره‌برداری از آسیب‌پذیری، بهره برداری از درب پشتی[1] (مسیر غیرمجاز برای دسترسی به اطلاعات)، تلاش‌های ثبت ورود، تداخل[2]، انکار خدمت (DoS)، و غیره. پویش‌کردن شبکه از نرم‌افزار پویش‌کردن شبکه استفاده می‌کند تا اطلاعاتی درباره پیکربندی شبکه‌ها، ورودی‌ها، خدمات و آسیب‌پذیری‌های موجود بدست آورد. بهره برداری از آسیب‌پذیری، از نقایص سامانه اطلاعات مانند پیکربندی، پروتکل یا برنامه‌ها استفاده می‌کند و نفع می‌برد. بهره برداری از درب پشتی، از درب‌های پشتی یا برنامه‌های مضری استفاده می‌کند که در فرایندهای

1-Backdoor
2-Interference

رسته	شرح	مثال‌ها
		طراحی سامانه نرم‌افزار و سخت‌افزار به جا می‌مانند. تلاش‌های ورود به سیستم[1]، می‌کوشند رمزهای عبور را حدس بزنند، قفل شکنی[2] نموده یا حمله سیل‌آسا[3] به عمل آورند. تداخل موجب مسدود شدن شبکه‌های رایانه‌ای، شبکه‌های انتقال بی سیم یا با سیم رادیویی و تلویزیونی، یا سیگنال‌های رادیویی و تلویزیونی ماهواره‌ای، از طریق وسایل فنی می‌شوند. DoS با استفاده حریصانه از منابع سامانه اطلاعات و شبکه مانند واحد پردازش مرکزی، حافظه، فضای دیسک یا پهنای باند شبکه ایجاد می‌شود و بر عملیات عادی سامانه‌های اطلاعاتی، برای مثال، SYS-a، PING-flooding، بمباران رایانامه تأثیر می‌گذارد.
رخداد رخنه قواعد	از دست‌رفتن امنیت اطلاعات به علت رخنه عمدی و یا تصادفی قواعد.	کاربرد غیر مجاز منابع، رخنه قانون حق تکثیر[4]، غیره. استفاده غیرمجاز از منابع، دسترسی به منابع برای اهداف غیرمجاز، از جمله معاملات سودآور برای مثال، استفاده از رایانامه برای مشارکت در نامه‌های زنجیره‌ای غیر قانونی برای سود یا طرح‌واره‌های هرمی. رخنه قانون حق تکثیر به علت فروش یا نصب رونوشت‌هایی از نرم‌افزارهای تجاری بدون مجوز یا سایر مطالبی که با قانون حق تکثیر محافظت می‌شوند برای مثال، اسرقت نرم‌افزار[5]
رخداد به مخاطره انداختن کارکردها	از دست‌رفتن امنیت اطلاعات به علت به مخاطره انداختن عمدی یا تصادفی کارکردهای سامانه‌های اطلاعات از لحاظ امنیتی.	سوءاستفاده از حقوق، جعل حقوق، انکار اقدامات، سوء عملیات ، رخنه دسترسی‌پذیری کارکنان، غیره.

l- Login
2- Crack
3- Brute force
4- Copyright
5- Warez

رسته	شرح	مثال‌ها
		سوءاستفاده از حقوق، از حقوقی فراتر از شرایط مرجع استفاده می‌کند. جعل حقوق از حقوق نادرست برای کلاهبرداری استفاده می‌کند. انکار اقدامات زمانی است که کسی اقدام خود را انکار می‌کند. سوء عملیات یعنی انجام‌دادن عملیات به صورت غلط و یا ناخواسته. رخنه دسترسی‌پذیری کارکنان به علت عدم وجود یا غیبت منابع انسانی ایجاد می‌شود.
رخداد به مخاطره انداختن اطلاعات	از دست‌رفتن امنیت اطلاعات به علت به مخاطره انداختن عمدی یا تصادفی امنیت اطلاعات مانند محرمانگی، صحت، دسترسی‌پذیری و غیره.	ایجاد اختلال[1]، جاسوسی[2]، استراق سمع[3]، فاش کردن[4]، دگرنمایی[5]، مهندسی اجتماعی[6]، کلاهبرداری اینترنتی[7]، سرقت داده، از دست‌رفتن داده‌ها، دستکاری داده، خطای داده، تحلیل گردش داده، آشکارسازی موقعیت، غیره. ایجاد اختلال اخذ داده پیش از رسیدن به گیرندگان موردنظر. جاسوسی یعنی جمع‌آوری و گزارش‌دهی اطلاعات درباره فعالیت‌های یک سازمان دیگر. استراق‌سمع یعنی گوش‌دادن به مکالمه طرف خارجی بدون اطلاع آن‌ها. فاش‌کردن یعنی اطلاعات حساس را به اطلاع عموم رساندن. دگرنمایی زمانی است که یک هستار، خود را به

1-Interception
2-Spying
3-Eavesdropping
4-Disclousure
5-Masquerade
6-Social engineering
7-Network phishing

رسته	شرح	مثال‌ها
		جای دیگری جا می‌زند. مهندسی اجتماعی، یعنی گردآوری اطلاعات از انسان‌ها به روشی غیر فنی، برای مثال، دروغ‌ها، حقه‌ها، رشوه‌ها یا تهدیدها. کلاهبرداری اینترنتی، یعنی استفاده از فناوری اینترنتی برای تطمیع کاربران به فاش‌کردن اطلاعات مهم مانند: گرفتن جزئیات حساب بانکی کاربران و رمزهای عبور با رایانامه‌های تقلبی. سرقت داده، یعنی دزدیدن داده. دستکاری داده یعنی دسترسی به داده یا ایجاد تغییر در داده بدون داشتن مجوز. خطای داده یعنی ارتکاب اشتباه هنگام واردکردن یا پردازش داده. آشکارسازی موقعیت، یعنی آشکارسازی موقعیت اطلاعات یا سامانه‌های حساس.
رخداد محتویات مضر	از دست‌رفتن امنیت اطلاعات به علت پخش‌کردن محتویات ناخواسته در شبکه‌های اطلاعاتی انجام می‌شود که امنیت ملی، ثبات اجتماعی و/یا ایمنی عمومی و مزایای آن‌ها را به مخاطره می‌اندازد.	محتویات غیرقانونی، محتویات ترسناک، محتویات مخرب، محتویات توهین‌آمیز، غیره. محتویات غیر قانونی محتویات منتشره‌ای هستند که قوانین اساسی ملی و بین المللی، قوانین و مقررات را زیر پا می‌گذارند، برای مثال، سوء استفاده‌های تصویری از کودکان، ترویج خشونت، کلاهبرداری و تقلب. محتویات ترسناک بحث یا تفسیری احساسی بدخواهانه است که در خصوص موضوعات حساس روی اینترنت مطرح و موجب رویدادهایی از قبیل تشویش عمومی و ترس می‌شوند. محتویات مخرب یعنی انتشار محتوایی که از روی بداندیشی به جامعه، یا اشخاص حمله می‌کنند، برای مثال، دست انداختن دیگران و آزار رساندن.

رسته	شرح	مثال‌ها
		محتویات ناراحت کننده، پخش محتوایی است که دریافت‌کنندگان خواهان دریافت آن‌ها نبوده‌اند، مانند هرزنامه.
سایر رخدادها	در هیچ رسته‌ای از رخدادهای فوق رسته-بندی نمی‌شوند.	

پ-۳ رده‌بندی رخدادهای امنیت اطلاعات

در زیر دو مثال از رویکردهای رده‌بندی رخدادهای امنیت اطلاعات معرفی می‌شوند.

تأکید می‌شود که این‌ها به عنوان مثال مطرح می‌شوند. مثال‌های دیگری مانند انجمن پاسخگویی به رخداد و گروههای امنیت (FIRST)[1] / سامانه امتیازدهی آسیب‌پذیری مشترک (CVSS)[2] / شرکت میتره[3] و قالب هشدار اطلاعات ساختاربندی شده دولت انگلستان (SWIF)[4] وجود دارد.

پ-۳-۱ مثال رویکرد ۱

پ-۳-۱-۱ عوامل رده‌بندی

پ-۳-۱-۱-۱ مقدمه

این رویکرد رخدادهای امنیت اطلاعات را با درنظر گرفتن سه عامل زیر رده‌بندی می‌کند:

- اهمیت سامانه اطلاعات،
- ازدست رفتن کسب‌وکار،
- اثر اجتماعی.

پ-۳-۱-۱-۲ اهمیت سامانه اطلاعات

اهمیت سامانه‌های اطلاعاتی تحت تأثیر رخدادهای امنیت اطلاعات، با در نظر گرفتن اهمیت عملیات کسب-وکار سازمان که ازطریق سامانه‌های اطلاعاتی پشتیبانی می‌گردد، تعیین می‌شود. اهمیت را می‌توان در رابطه با امنیت ملی، نظم اجتماعی، توسعه اقتصادی و منافع عمومی و وابستگی کسب‌وکار به سامانه‌های اطلاعاتی

1- Forum of Incident Response and Security Teams (FIRST)
2- Common Volunerability Scoring System (CVSS)
3- Mitre Corporation (www.mitre.org)
4- Structured Warning Informatin Format (SWIF)

بیان کرد. این رویکرد، اهمیت سامانه اطلاعات را در سه سطح گسترده رده‌بندی می‌کند: سامانه اطلاعات مخصوصا مهم، سامانه اطلاعات مهم و سامانه اطلاعات معمولی.

پ-۳-۱-۱-۳ ازدست رفتن کسب‌وکار

ازدست رفتن کسب‌وکار سازمان به دلیل رخدادهای امنیت اطلاعات با در نظر گرفتن شدت اثر وقفه کسب‌وکاری به خاطر صدمه سخت‌افزار /نرم‌افزار، کارکردها و داده سامانه‌های اطلاعاتی، تعیین می‌شود. شدت اثر می‌تواند به هزینه بازیابی کسب‌وکار به حالت عادی و سایر آثار منفی رخدادهای امنیت اطلاعات از جمله ازدست رفتن سود و/یا فرصت‌ها بستگی داشته باشد. این رویکرد، ازدست رفتن کسب‌وکار را به چهار سطح گسترده رده‌بندی می‌کند: ازدست رفتن کسب‌وکار مخصوصا جدی، ازدست رفتن کسب‌وکار جدی، ازدست رفتن کسب‌وکار قابل ملاحظه، ازدست رفتن کسب‌وکاری جزئی، که به صورت زیر توصیف می‌شوند.

الف- ازدست رفتن کسب‌وکار مخصوصا جدی، یعنی فلج شدن شدید کسب‌وکار تا حد از دست رفتن توانایی داد و ستد و/یا صدمه شدید به محرمانگی، صحت و دسترسی‌پذیری داده‌های کلیدی کسب‌وکار. این کار یعنی هزینه گزاف برای بازیابی عملیات عادی و حذف آثار منفی. سازمان نمی تواند این سطح ازدست رفتن کسب‌وکار را تحمل کند.

ب- ازدست رفتن کسب‌وکار جدی یعنی وقفه در عملیات کسب‌وکار برای بلند مدت یا فلج شدن کسب‌وکار محلی تا حدی که به شدت بر توانایی کسب‌وکاری اثر بگذارد و/یا صدمه شدید به محرمانگی، صحت و دسترسی‌پذیری داده‌های کلیدی کسب‌وکار برسد. این یعنی هزینه گزاف برای بازیابی کسب‌وکار به وضعیت عادی و حذف آثار منفی. سازمان می‌تواند این سطح ازدست رفتن را تحمل کند.

پ- ازدست رفتن کسب‌وکاری قابل ملاحظه، یعنی وقفه در عملیات کسب‌وکار تا حدی که تأثیر قابل ملاحظه‌ای بر توانایی کسب‌وکار بگذارد و/یا صدمه قابل ملاحظه‌ای بر محرمانگی، صحت و دسترسی‌پذیری به داده‌های کلیدی کسب‌وکار برسد. این یعنی هزینه قابل ملاحظه برای بازیابی کسب‌وکار به حالت عادی و حذف آثار منفی. سازمان می‌تواند این سطح ازدست رفتن کسب‌وکار را کاملا تحمل کند.

ت- ازدست رفتن کسب‌وکاری جزئی یعنی وقفه در عملیات کسب‌وکار برای مدت کوتاه تا حدی که کمی تأثیر بر توانایی کسب‌وکاری بگذارد و/یا بر محرمانگی، صحت و دسترسی‌پذیری اطلاعات کلیدی کسب‌وکار اثر جزئی بگذارد. این یعنی هزینه جزئی برای بازگرداندن کسب‌وکار به وضعیت عادی و حذف آثار منفی.

پ-۳-۱-۱-۴ اثر اجتماعی

اثر بر جامعه به دلیل رخدادهای امنیت اطلاعات با درنظر گرفتن مقیاس و درجه اثر بر امنیت ملی، نظم اجتماعی، پیشرفت اقتصادی و منافع عمومی تعیین می‌شود. این رویکرد، اثر اجتماعی را به چهار سطح

تقسیم می‌کند: اثر اجتماعی مخصوصا مهم، اثر اجتماعی مهم، اثر اجتماعی قابل ملاحظه، اثر اجتماعی جزئی، که به صورت زیر توصیف می‌شوند.

۱- اثر اجتماعی مخصوصا مهم، یعنی آثار نامطلوب در بیشتر حوزه‌های یک یا چند استان درحال گسترش بوده، امنیت ملی را به شدت تهدید می‌کنند، موجب اغتشاش در جامعه می‌شوند، پیامدهای به شدت نامطلوبی بر توسعه اقتصاد می‌گذارند، و/یا به منافع عمومی آسیب جدی وارد می‌کنند.

۲- اثر اجتماعی مهم یعنی آثار نامطلوب در بیشتر حوزه‌های یک یا چند شهر درحال گسترش بوده، امنیت ملی را تهدید می‌کنند، موجب ترس در جامعه می‌شوند، پیامدهای فوق‌العاده نامطلوبی بر توسعه اقتصادی می‌گذارند و/یا به منافع عمومی صدمه می‌زنند.

۳- اثر اجتماعی قابل ملاحظه یعنی آثار نامطلوب که در پاره‌ای از حوزه‌های یک یا چند شهر درحال گسترش بوده و تهدید محدودی بر امنیت اجتماعی می‌گذارد، با کمی اختلال در نظم اجتماعی، موجب برخی پیامدهای نامطلوب بر توسعه اقتصادی می‌شوند و/یا بر منافع عمومی تأثیر می‌گذارند.

۴- اثر اجتماعی جزئی یعنی آثار نامطلوب بر یک حوزه کوچک از یک شهر، و احتمال اندک تهدید امنیت ملی، نظم اجتماعی، توسعه اقتصادی، منافع عمومی، اما با صدمه به منافع کارکنان، شرکت‌ها و سایر سازمان‌ها.

پ-۳-۱-۲ رده‌ها

پ-۳-۱-۲-۱ مقدمه

براساس عوامل رده‌بندی، بهتراست رخدادهای امنیت اطلاعات با توجه به شدت با استفاده از یک مقیاس رده‌بندی شوند. چنین مقیاسی می‌تواند «کلی» یا «جزئی» باشد، جزئیات بشتر:

- فوری: اثر شدید؛
- بحرانی: اثر متوسط؛
- هشدار: اثر کم؛
- اطلاعات: بدون اثر، اما برای بهبود خط‌مشی‌ها، روش‌های اجرایی و کنترل‌های امنیت اطلاعات می‌توان از تحلیل استفاده کرد.

این رویکرد، طبق عوامل رده‌بندی فوق، رخدادهای امنیت اطلاعات را به چهار رده تقسیم می‌کند:

- بسیار جدی (رده ۴)

- جدی (رده ۳)
- کمی جدی (رده ۲)
- کوچک (رده ۱)

تأکید می‌شود که رده‌های شدت، فقط به عنوان مثال مطرح شده‌اند. در بعضی از رویکردها، جدی‌ترین رده به عنوان بالاترین سطح مقیاس ارایه می‌شود. در سایر رویکردها، جدی‌ترین رده به عنوان پایین‌ترین سطح مقیاس ارایه می‌شود.

پ-۳-۱-۲-۲ بسیار جدی (رده ۴)

رخدادهای بسیار جدی آن‌هایی هستند که:

الف) در سامانه‌های اطلاعاتی مخصوصا مهم عمل می‌کنند، و
ب) منجر به ازدست رفتن کسب‌وکار مخصوصا جدی می‌شود، یا
پ) منجر به اثر اجتماعی مخصوصا مهم می‌شود.

پ-۳-۱-۲-۳ جدی (رده ۳)

رخدادهای جدی آن‌هایی هستند که:

الف) در سامانه‌های اطلاعاتی مخصوصا مهم یا سامانه‌های اطلاعاتی مهم عمل می‌کنند، و
ب) منجر به ازدست رفتن جدی کسب‌وکار می‌شوند، یا
پ) منجر به اثر اجتماعی مهم می‌شوند.

پ-۳-۱-۲-۴ کمی جدی (رده ۲)

رخدادهای کمی جدی، آن‌هایی هستند که:

الف) در سامانه‌های اطلاعاتی مهم یا سامانه‌های اطلاعاتی معمولی عمل می‌کند،
ب) منجر به ازدست رفتن کسب‌وکار قابل ملاحظه می‌شود، یا
پ) منجر به اثر اجتماعی قابل ملاحظه می‌شود.

پ-۳-۱-۲-۵ کوچک (رده ۱)

رخدادهای کوچک آن‌هایی هستند که:

الف) در سامانه‌های مهم معمولی عمل می‌کنند، و

ب) منجر به ازدست رفتن جزئی کسب‌وکار می‌شوند و یا ضرری بر جای نمی گذارند، و
پ) منجر به اثر اجتماعی جزئی می‌شوند و یا اثری بر جای نمی گذارند،
ت) نیاز به هیچ اقدامی نخواهد داشت و هیچ پیامدی بر جای نمی ماند.

پ-۳-۱-۳رسته رخداد و رده شدت

رسته رخداد امنیت اطلاعات و رده شدت اغلب به هم ربط دارند. ممکن است یک رسته رخداد امنیت اطلاعات بسته به نه تنها کسب‌وکار، بلکه با توجه به ماهیت رخداد امنیت اطلاعات ، در رده شدت متفاوتی قرار بگیرد، از قبیل:

- عمدی،
- هدف‌مند،
- زمان بندی،
- مقدار.

بعضی از مثال‌های رسته‌بندی‌های رخداد امنیت اطلاعات که ممکن است بسته به ماهیت آن‌ها دارای رده شدت متفاوتی باشند در جدول پ-۲ ارایه شده اند.

جدول پ- ۲ – مثال‌هایی از رسته رخداد و رده شدت

رده شدت / رسته رخداد	کوچک	کمی جدی	جدی	بسیار جدی
حملات فنی	تلاش‌های ناموفق	معمولی منفرد (به مخاطره افتادن کاربر)	چندگانه (به مخاطره افتادن کاربر) مهم منفرد (برنامه کاربردی، به مخاطره افتادن ریشه ای)	انبوه (برنامه کاربردی، به مخاطره افتادن ریشه ای)
حملات فنی		آزار (خراش دادن سطح)	اختلال (اثر سراسری)	عدم دسترسی‌پذیری (توقف در خدمات)
بدافزار	شناخته شده منفرد (آشکار و مسدود شده با محافظ ضد ویروس)	ناشناخته منفرد	آلودگی‌های چندگانه آلودگی‌های شدید	آلودگی‌های انبوه

پ-۳-۲ مثال رویکرد ۲

پ-۳-۲-۱ مقدمه

این رویکرد برای ارزیابی پیامدهای نامطلوب رخدادهای امنیت اطلاعات، خلاصه راهنماهای مثال را ارائه می‌دهد. هر راهنما از مقیاس ۱ (کم) تا مقیاس ۱۰ (زیاد) برای رده‌بندی رخدادهای امنیت اطلاعات استفاده می‌کند. (در عمل، می‌توان از مقیاس‌های دیگر مانند ۱ تا ۵ استفاده کرد و بهتراست هر سازمان بهترین مقیاس مناسب محیط خود را انتخاب کند).

پیش از خواندن راهنماهای زیر، بهتراست به توضیحات بعدی توجه شود:

- در بعضی از راهنماهای مثال زیر، بعضی از موارد ثبتی[1] به صورت «عدم ثبت» وارد شده‌اند. علت آن این است که راهنماها طوری تنظیم شده‌اند که پیامدهای نامطلوب در هر سطح صعودی، که با مقیاس ۱ تا ۱۰ بیان می‌شود، بسیار شبیه تمامی شش نوعی هستند که در پ- ۳- ۲- ۲ تا پ- ۳- ۲- ۷ نشان داده شده‌اند. به هرحال، در بعضی از سطوح (در مقیاس ۱ تا ۱۰) برای بعضی از انواع، چنین درنظرگرفته می‌شود که تفاوت مهمی در ثبت‌های سریع پیامد کم‌تر برای یک ثبت وجود ندارد - و این امر با «ثبت‌نشده» نوشته می‌شود. به همین صورت، در بالاترین سطح برخی انواع درنظرگرفته می‌شود پیامدی بزرگتر از بالاترین سطح نشان‌داده‌شده وجود ندارد - و بنابراین ثبت‌های بالاتر به صورت «ثبت‌نشده» اعلام می‌شوند (بنابراین، به لحاظ منطقی درست نیست که خطوط «ثبت‌نشده» حذف و مقیاس فشرده شود).

بنابراین، هنگام در نظر گرفتن پیامدهای نامطلوب یک رخداد امنیت اطلاعات بر کسب‌وکار یک سازمان، از موارد زیر به عنوان مثالی از مجموعه راهنماها استفاده شود.

- افشای غیر مجاز اطلاعات،
- تغییر غیر مجاز اطلاعات،
- انکار اطلاعات،
- عدم وجود اطلاعات و/یا خدمات،
- خرابی اطلاعات و/یا خدمات.

1- Entries

نخستین گام توجه به این است که کدام یک از انواع زیر مرتبط هستند. برای انواعی که مرتبط به نظر می‌رسند، بهتراست نوع راهنمایی استفاده شود که اثر نامطلوب واقعی بر عملیات کسب‌وکار (یا ارزش) به منظور ثبت در برگه گزارش رخدادهای امنیت اطلاعات را تعیین کند.

پ-۳-۲-۲ زیان/ورشکستگی[1] مالی بر عملیات کسب‌وکار

رخدادهای افشا و بهبود غیر مجاز، انکار و همچنین موجود نبودن و خرابی این اطلاعات، می‌توانند موجب ضرر مالی شوند مانند کاهش قیمت سهام، کلاهبرداری یا نقض قرارداد به خاطر عدم اقدام یا اقدام دیرهنگام. به همین صورت، خصوصا پیامدهای موجودنبودن یا خرابی اطلاعات می‌توانند موجب خراب شدن عملکردهای کسب‌وکاری شوند. تصحیح و/یا بهبود یافتن از رخدادها نیازمند صرف زمان و تلاش است. در بعضی از موارد این مهم است و بهتراست در نظر گرفته شود. به منظور استفاده از یک مخرج مشترک، زمان بهبودی بهتراست برای یک واحد از زمان کارکنان محاسبه شود و به صورت یک هزینه مالی درآید. این هزینه بهتراست با مراجعه به هزینه عادی برای یک ماه فرد در سطح مناسب در سازمان محاسبه شود. راهنمای بعدی بهتراست مورد استفاده قرار گیرد.

۱- نتیجه درمورد زیان‌ها/هزینه‌های مالی از x_1 یا کمتر

۲- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_1 + 1$ و x_2

۳- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_2 + 1$ و x_3

۴- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_3 + 1$ و x_4

۵- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_4 + 1$ و x_5

۶- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_5 + 1$ و x_6

۷- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_6 + 1$ و x_7

۸- نتیجه درمورد زیان‌ها/هزینه‌های مالی بین $x_7 + 1$ و x_8

۹- نتیجه درمورد زیان‌ها/هزینه‌های مالی بیش از x_8

۱۰- سازمان از عرصه کسب‌وکار خارج می‌شود

جایی که x_i (i= 1, 2, …, 8) زیان‌ها/هزینه‌های مالی در هشت درجه‌ها/سطح‌ها را ارایه می‌دهدکه توسط سازمان، در مقوله خود تعیین می‌شوند.

2- loss/disruption

پ-۳-۲-۳ منافع تجاری و اقتصادی

اطلاعات تجاری و اقتصادی باید محافظت شوند، و ازطریق توجه به ارزش آن‌ها برای رقبا یا اثری که به‌مخاطره افتادن آن‌ها می‌تواند روی منافع تجاری داشته باشد، ارزش‌گذاری می‌شود. راهنمای زیر بهتراست مورد استفاده قرار گیرد:

۱- مورد علاقه یک رقیب است اما برای او ارزش تجاری ندارد

۲- تا ارزشی معادل y_1 یا کمتر مورد علاقه یک رقیب است (بازگشت سرمایه)[1]

۳- برای یک رقیب ارزش دارد تا ارزشی که بین $y_1 + 1$ و y_2 (برگشت سرمایه) است، یا موجب زیان مالی، یا ازدست‌رفتن درآمد بالقوه می‌شود، یا اینکه کسب درآمد یا مزیت نامناسبی را برای کارکنان یا سازمان‌ها تسهیل می‌سازد، یا عهدشکنی ظاهرپسندی برای ایجاد اعتماد نسبت به اطلاعات ارائه شده توسط طرف‌های سوم برقرار می‌کند.

۴- تا ارزشی که بین$y_2 + 1$ و y_3 است برای یک رقیب ارزش دارد (بازگشت سرمایه)

۵- تا ارزشی که بین $y_3 + 1$ و y_4 است برای یک رقیب ارزش دارد (بازگشت سرمایه)

۶- تا ارزشی که بین $y_4 + 1$ است برای یک رقیب ارزش دارد (بازگشت سرمایه)

۷- *ثبت‌نشده*[2]

۸- *ثبت‌نشده*

۹- به طرز قابل توجهی می‌توانند منافع تجاری یا ثبات مالی سازمان را به تحلیل ببرند

۱۰- *ثبت‌نشده*

جایی که yi ($i= 1, 2, \ldots, 4$)، معرف مقادیر مربوط به گردش کار در چهار درجه‌ها /سطح‌ها برای‌یک رقیب می باشد که توسط سازمان تامین شوند.

پ-۳-۲-۴ اطلاعات شخصی

هنگامی که اطلاعات درباره اشخاص نگهداری و پردازش می‌شود، از لحاظ روحی و اخلاقی صحیح است، و گاهی از لحاظ قانونی نیاز است، که اطلاعات در مقابل افشای غیرمجاز محافظت شود که می‌تواند در بهترین

1- Turnover

[2] - اصطلاح «ثبت نشده» بدین معنی است که ثبت متناظری مربوط به این سطح اثر وجود ندارد.

حالت به دشوارشدن و دربدترین حالت به اقدام قانونی نامطلوب منجر شود، برای مثال تحت قانون حفاظت اطلاعات. به طور یکسان، لازم است که اطلاعات درباره اشخاص صحیح باشد زیرا دست بردن در اطلاعات شخصی کارکنان، می‌تواند منجر به همین عواقب قانونی شود. همچنین مهم است که اطلاعات درباره اشخاص، غیرقابل دسترس و یا مخدوش نشود زیرا این امر می‌تواند منجر به تصمیمات نادرست یا عدم اقدام در زمان لازم شود. توصیه می‌شود راهنمای زیر مورد استفاده قرار گیرد:

۱- پریشانی جزئی (نگرانی) برای یک فرد (خشم، پوچی، ناامیدی) اما بدون نقض قانون یا مقررات

۲- پریشانی (نگرانی) برای یک فرد (خشم، پوچی، ناامیدی) اما بدون نقض قانون یا مقررات

۳- نقض یک قانون، مقررات یا الزام اخلاقی یا نیت علنی‌شده محافظت از اطلاعات، که منجر به ناراحتی جزئی یک فرد شود

۴- نقض یک قانون، مقررات یا الزام اخلاقی یا نیت علنی‌شده محافظت از اطلاعات، که منجر به ناراحتی فوق‌العاده یک فرد یا ناراحتی جزئی گروهی از کارکنان شود

۵- نقض یک قانون، مقررات یا الزام اخلاقی یا نیت علنی‌شده محافظت از اطلاعات، که منجر به ناراحتی جدی برای یک فرد شود

۶- نقض یک قانون، مقررات یا الزام اخلاقی یا نیت علنی‌شده محافظت از اطلاعات، که منجر به ناراحتی جدی گروهی از کارکنان شود

۷- ثبت‌نشده

۸- ثبت‌نشده

۹- ثبت‌نشده

۱۰- ثبت‌نشده

پ-۳-۲-۵ تعهدات قانونی و مقرراتی

داده نگهداری‌شده و پردازش‌شده توسط یک سازمان ممکن است برای تبعیت از، یا به منظور رعایت تعهدات قانونی و مقرراتی باشد. قصور در رعایت چنین تعهداتی، اعم از عمدی یا غیرعمدی، ممکن است منجر به اقدامات قانونی یا اداری علیه کارکنان در سازمان مورد نظر شود. این اقدامات ممکن است منجر به جرایم نقدی و/یا احکام زندان شود. بهتراست راهنمای زیراستفاده شود:

۱- ثبت‌نشده

۲- ثبت‌نشده

۳- اخطار اجرایی[1]، اقامه دعوا[2]، جرم جنایی[3] که منجر به خسارات/جرائم مالی z_1 یا کمتر می‌شود

۴- اخطار اجرایی، اقامه دعوا، جرم جنایی که منجر به خسارات/جرائم مالی بین z_1+1 و z_2 می‌شود

۵- اخطار اجرایی، اقامه دعوا، جرم جنایی که منجر به خسارات/جرائم مالی بین z_2+1 و z_3 یا یک جریمه زندانی بالغ بر ۲سال می‌شود

۶- اخطار اجرایی، اقامه دعوا، جرم جنایی که منجر به خسارات/جرائم مالی بین z_3+1 و z_4، یا یک مجازات زندان بین ۲ تا۱۰ سال می‌شود

۷- اخطار اجرایی، اقامه دعوا، جرم جنایی که منجر به خسارات/جرائم مالی نامحدود، یا یک حکم زندان بیش از۱۰ سال می‌شود

۸- *ثبت‌نشده*

۹- *ثبت‌نشده*

۱۰- *ثبت‌نشده*

پ-۳-۲-۶عملیات مدیریت و کسب وکار

اطلاعات ممکن است طوری باشد که به مخاطره انداختن آن منجر به لطمه به عملکرد مؤثر یک سازمان شود. برای مثال، اطلاعات مربوط به تغییر در یک خط‌مشی، چنانچه افشا شود می‌تواند منجر به واکنش‌های عمومی شود، تا آنجا که پیاده‌سازی خط‌مشی امکان پذیر نخواهد بود. تغییر، انکار یا عدم دسترسی به اطلاعات مربوط به جنبه‌های مالی یا نرم‌افزارهای رایانه‌ای، می‌تواند آثار جدی زیانباری برای عملیات یک سازمان داشته باشد. به علاوه، انکار تعهدات می‌تواند نتایج کسب‌وکار نامطلوبی به بار آورد. توصیه می‌شود راهنمای زیر استفاده شود:

۱- فعالیت غیرکارآمد قسمتی از یک سازمان

۲- ثبت‌نشده

۳- تحلیل‌رفتن مدیریت صحیح سازمان و عملیات آن

1- Enforcement notice
2- Civil suit
3- Criminal offence

۴- ثبت‌نشده

۵- مانع توسعه موثر یا اعمال خط‌مشی‌های سازمان شدن

۶- عدم مزیت سازمان در مورد مذاکرات تجاری یا خط‌مشی با دیگران

۷- ممانعت جدی از توسعه یا اعمال خط‌مشی‌های اصلی سازمانی، یا متوقف‌کردن عملیات یا در غیراینصورت وارد نمودن صدمه اساسی به عملیات اصلی

۸- ثبت‌نشده

۹- ثبت‌نشده

۱۰- ثبت‌نشده

پ-۳-۲-۷ ازدست‌رفتن حسن شهرت

افشا یا تغییر، انکار یا عدم دسترسی مطلق به اطلاعات، می‌تواند منجر به ازدست رفتن حسن شهرت سازمان، در نتیجه صدمه به شهرت آن، ازدست رفتن اعتبار و سایر نتایج نامطلوب گردد. توصیه می‌شود راهنمای زیر استفاده شود:

۱- ثبت‌نشده

۲- باعث ناراحتی در سطح سازمان شود

۳- اثر نامطلوب بر روابط با سهام‌داران، مشتریان، تامین‌کنندگان، کارمندان، کاربران طرف سوم، نهادهای تنظیم مقررات، دولت، دیگر سازمان‌ها یا عموم، که در سطح محلی/منطقه‌ای منجر به تبلیغات نامطلوب می‌شود

۴- ثبت‌نشده

۵- اثر نامطلوب بر روابط با سهام‌داران، مشتریان، تامین‌کنندگان، کارمندان، کاربران طرف سوم، نهادهای تنظیم مقررات، دولت، دیگر سازمان‌ها یا عموم، که در سطح ملی منجر به تبلیغات نامطلوب می‌شود

۶- ثبت‌نشده

۷- اثر مادی بر روابط با سهام‌داران، مشتریان، تامین‌کنندگان، کارمندان، کاربران طرف سوم، نهادهای تنظیم مقررات، دولت، دیگر سازمان‌ها یا عموم، که در سطح گسترده منجر به تبلیغات نامطلوب می‌شود

۸- *ثبت‌نشده*

۹- *ثبت‌نشده*

۱۰- *ثبت‌نشده*

پیوست ت

(اطلاعاتی)

مثال گزارش‌ها و برگه‌های رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات

ت-۱ مقدمه

این پیوست محتوی مثال‌هایی است که باید برای رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات بایگانی شود، و مثال برگه‌هایی برای گزارش‌دهی رویداد، رخداد و آسیب‌پذیری امنیت اطلاعات، همراه با یادآوری‌های مربوط می‌باشد. تأکید می‌شود که این‌ها مثال هستند. استانداردهای دیگری، مانند استاندارد طرح‌واره‌ی توصیف موضوع و قالب تبادل رخداد (IODEF)[1] وجود دارد.

ت-۲ مثال بخش‌های مربوط به سوابق

ت-۲-۱ مثال بخش‌های مربوط به سابقه رویداد امنیت اطلاعات

این سابقه شامل اطلاعات پایه از رویداد امنیت اطلاعات، مانند چه موقع، چه‌چیز، چگونه و چرا رویداد به وقوع پیوسته است، همین‌طور اطلاعات تماس با فرد گزارش‌دهنده.

اطلاعات پایه
- زمان رویداد
- تعداد رویداد
- تعداد رویداد و/یا رخداد مربوط (اگر کاربردپذیر باشد)

جزئیات فرد گزارش‌دهنده
- نام
- اطلاعات تماس مانند آدرس، سازمان، اداره، تلفن و رایانامه

توصیف رویداد
- چه رویدادی به وقوع پیوسته است
- چگونه به وقوع پیوسته است
- چرا به وقوع پیوسته است

دیدگاه‌های اولیه درمورد مولفه‌ها/دارایی‌هایی که تحت تأثیر قرارگرفته‌اند

اثرهای نامطلوب کسب‌وکار

هر آسیب‌پذیری شناسایی‌شده

1- Incident Object Description and Exchange Format (IODEF)

جزئیات رویداد
تاریخ و زمان وقوع رویداد
تاریخ و زمان کشف رویداد
تاریخ و زمان گزارش رویداد

ت-۲-۲ مثال بخش‌های مربوط به سابقه رخداد امنیت اطلاعات

این سابقه شامل اطلاعات پایه از رخداد امنیت اطلاعات است، مانند چه وقت، چه‌چیز، چگونه و چرا رخداد اتفاق افتاده است، همین‌طور رسته‌بندی، اثر و نتیجه پاسخگویی با رخداد را در بردارد.

اطلاعات پایه
تاریخ رخداد
شماره رخداد
تعداد رویداد و/یا رخداد (اگر کاربردپذیر باشد)
شخص گزارش‌هنده
نام
اطلاعات تماس مانند آدرس، سازمان، اداره، تلفن و رایانامه
نقطه تماس عضو (PoC)
نام
اطلاعات تماس مانند آدرس، سازمان، اداره، تلفن و رایانامه
جزئیات عضو ISIRIT
نام
اطلاعات تماس مانند آدرس، سازمان، اداره، تلفن و رایانامه
توصیف رخداد
چه رخدادی به وقوع پیوسته است
چگونه به وقوع پیوسته است
چرا به وقوع پیوسته است
دیدگاه‌های اولیه درمورد مولفه‌ها/دارایی‌هایی که تحت تأثیر قرارگرفته‌اند
اثرهای نامطلوب کسب‌وکار
هر آسیب‌پذیری شناسایی‌شده
جزئیات رخداد
تاریخ و زمان وقوع رخداد
تاریخ و زمان کشف رخداد
تاریخ و زمان گزارش رخداد

رسته‌بندی رخداد
مولفه‌ها/دارایی‌هایی که تحت تأثیر قرارگرفته‌اند
اثر شدید/اثر نامطلوب رخداد برکسب و کار
کل هزینه‌های بازیابی ناشی از رخداد
برطرف کردن رخداد
شخص (اشخاص)/مقصر (مقصرین) دخیل در این مسئله (اگر عامل رخداد اشخاص هستند)
توصیف مقصر
انگیزه واقعی یا مورد نظر
اقدامات صورت گرفته برای برطرف کردن رخداد
اقدامات برنامه‌ریزی شده برای برطرف کردن رخداد
اقدامات ممتاز
نتیجه‌گیری
کارکنان/هستارهای داخلی مطلع
کارکنان/هستارهای خارجی مطلع

ت-۲-۳ مثال بخش‌های مربوط به سابقه آسیب‌پذیری امنیت اطلاعات

این سابقه اطلاعات پایه آسیب‌پذیری امنیت اطلاعات مانند، چه وقت، چه‌چیز و چگونه آسیب‌پذیری شناسایی شد، همین‌طور اثر بالقوه و برطرف کردن آن را شامل میشود.

اطلاعات پایه
- زمان شناسایی آسیب‌پذیری
- تعداد آسیب‌پذیری

جزئیات شخص گزارش‌دهنده
- نام
- اطلاعات تماس مانند آدرس، سازمان، اداره، تلفن و رایانامه

توصیف آسیب‌پذیری

برطرف کردن آسیب‌پذیری

ت-۳ چگونگی استفاده از برگه‌ها

ت-۳-۱ قالب تاریخ و زمان

بهتراست، تاریخ‌ها در قالب CCYY-MM-DD (و اگر مورد نیاز است HH-MM-SS) باشد. اگر مرتبط باشد، بهتر است وقتی که وقوع اکثر رویدادها در تمام مناطق زمانی امکان‌پذیر است، از زمان هماهنگ جهانی (UTC)[1] برای مقایسه آسان استفاده شود (و در وضعیت حداقل مبداء UTC برای زمان کاربرد دارد).

ت-۳-۲ یادآوری‌هایی برای تکمیل برگه‌ها

هدف از برگه‌های گزارش رویداد و رخداد امنیت اطلاعات ارایه اطلاعات درباره یک رویداد امنیت اطلاعات، و سپس، اگر تعیین شود که یک رخداد امنیت اطلاعات است، درباره رخداد، به افراد مناسب مربوط می‌شود.

اگر مظنون هستید که یک رویداد امنیت اطلاعات در حال پیشرفت است یا ممکن است به وقوع پیوسته باشد – به ویژه رویدادی که باعث زیان یا صدمه به دارایی یا شهرت سازمان شود، بهتراست بی درنگ برگه گزارش رویداد امنیت اطلاعات، برطبق روش‌های اجرایی توصیف‌شده در طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات سازمان تکمیل و ارسال گردد (اولین قسمت این پیوست ملاحظه شود).

اطلاعاتی که فراهم می‌شود، برای ارزیابی اولیه مورد استفاده قرار می‌گیرد و معلوم می‌کند که آیا رویداد باید به عنوان یک رخداد امنیت اطلاعاتی رده‌بندی شود یا خیر، و آیا اقدامات درمانی لازم برای پیشگیری یا محدودکردن هر زیان یا صدمه وجودارد. با توجه به طبیعت بالقوه زمان- بحران[2] این فرایند، *نیازی به تکمیل تمام فیلدهای برگه گزارش‌دهی در این زمان وجود ندارد.*

اگر شما عضوی از PoC هستید که هم اکنون برگه‌های تکمیل‌شده یا نیمه تکمیل را بازنگری می‌کنید، اتخاذ این تصمیم که آیا رویداد باید به عنوان یک رخداد امنیت اطلاعات رده‌بندی شود به عهده شما است. درصورتی که رویدادی چنین رده‌بندی شود، بهتراست اطلاعات برگه گزارش رخداد را تا جایی‌که قادر هستید تکمیل کنید، و برگه هردو، هم رویداد و هم رخداد امنیت اطلاعات را برای ISIRT ارسال نمایید. خواه رویداد امنیت اطلاعات به عنوان رخداد رده‌بندی شود یا خیر، بهتر است دادگان رویداد/ رخداد/آسیب‌پذیری روزآمد شود.

اگر شما عضوی از ISIRT هستید که برگه‌های رویداد و رخداد امنیت اطلاعات ارسال شده توسط یک عضو PoC را بازنگری می کنید، سپس بهتر است به موازات پیشرفت بررسی‌ها و روزآمدی برگه رخداد، دادگان رویداد/ رخداد/آسیب‌پذیری، روزآمد شود.

1- Coordinated Universal Time (UTC)
2- Potentially time-critical nature

هدف از برگه گزارش آسیب‌پذیری امنیت اطلاعات، فراهم‌کردن اطلاعات درباره یک آسیب‌پذیری مورد نظر، و ایفای نقش یک مخزن اطلاعات درمورد برطرف کردن آسیب‌پذیری گزارش شده است.

لطفا هنگام تکمیل برگه‌ها، راهنماهای زیر را مورد توجه قراردهید:

- توصیه می‌شود برگه به صورت الکترونیکی تکمیل و ارسال گردد[1] (هنگامی که مشکلاتی وجود دارند یا به نظر می‌رسد، به وجود آیند، با سازوکارهای گزارش‌دهی الکترونیکی (برای مثال رایانامه) از جمله هنگامی که امکان در معرض حمله بودن سامانه به ذهن می‌رسد و برگه‌های گزارش می‌تواند توسط اشخاص غیرمجاز خوانده شود، سپس بهتراست وسایل جایگزین گزارش‌دهی مورد استفاده قرارگیرد. وسایل جایگزین می‌توانند خود شخص، به وسیله تلفن، یا پیام متنی باشند).

- تنها اطلاعاتی را فراهم کنید که از واقعی بودن آن‌ها اطلاع دارید- برگه را به طور غیر واقعی تکمیل نکنید. اگر لازم است اطلاعاتی را که نمی‌توانید تایید کنید فراهم نمایید، لطفا مورد تایید نبودن اطلاعات را، و آنچه که شما را به این باور می‌رساند که ممکن است حقیقت باشد، به روشنی اعلام نمایید.

- شما بهتراست، جزئیات کامل اطلاعات تماس خود را فراهم کنید. ممکن است، نیاز باشد برای کسب اطلاعات بیشتر در مورد گزارش شما - بلافاصله یا در یک تاریخ بعدی - با شما تماس گرفته شود.

اگر بعدها کشف کردید که هر یک از اطلاعاتی که ارایه نموده‌اید نادرست، ناقص یا گمراه‌کننده است، بهتراست گزارش خود را اصلاح و دوباره ارسال کنید.

[1] - برای مثال روی برگه صفحه تارنما با ایجاد پیوند به دادگان رویداد/ رخداد/آسیب‌پذیری امنیت اطلاعات. در دنیای امروز، بهره‌برداری از یک طرح-واره‌ی مبتنی برکاغذ بسیار زمان‌بر است. به‌هرحال، هرگاه نتوان از طرح‌واره‌ی الکترونیکی استفاده کرد کماکان نیاز به تهیه طرح‌واره‌ی مبتنی برکاغذ وجوددارد.

ت-۴ مثال از برگه‌ها

ت-۴-۱ مثال از برگه‌های گزارش رویداد اطلاعات امنیت

گزارش رویداد امنیت اطلاعات

۱- تاریخ رویداد **صفحه ۱ از ۱**

۲- شماره رویداد[1] **۳- (اگر کاربردپذیر باشد)**

شماره‌های شناسایی رویداد و یا پیشامد مربوط

۴- جزئیات فرد گزارش‌دهنده

۴-۱ نام ..... ۴-۲ آدرس .....

۴-۲ سازمان ..... ۴-۴ اداره .....

۴-۵ تلفن ..... ۴-۶ رایانامه .....

۵- توصیف رویداد امنیت اطلاعات

۵-۱ توصیف رویداد

- چه رویدادی به وقوع پیوسته است
- چگونه به وقوع پیوسته است
- چرا به وقوع پیوسته است
- دیدگاه‌های اولیه درمورد مولفه‌ها/دارایی‌هایی که آسیب دیده‌اند
- اثرهای نامطلوب کسب‌وکار

۶- جزئیات رویداد امنیت اطلاعات

۶-۱ تاریخ و زمان وقوع رویداد

۶-۲ تاریخ و زمان کشف رویداد

۶-۳ تاریخ و زمان گزارش رویداد

۶-۴ پاسخگویی با این رویداد تمام شده‌است بله ☐ خیر ☐

(مورد صحیح را تیک بزنید)

۶-۵ درصورت پاسخ مثبت، طول عمر رویداد را به روز/ساعت/دقیقه مشخص کنید

---

۱ - بهتراست شماره‌های رویداد توسط مدیر ISIRT سازمان تخصیص داده شود.

ت-۴-۲ مثال از برگه‌های گزارش رخداد امنیت اطلاعات

گزارش رخداد امنیت اطلاعات

۱- تاریخ رویداد صفحه ۱ از ۶

۲- شماره رخداد[1] ۳- (اگر کاربردپذیر باشد)

شماره‌های شناسایی رویداد و یا پیشامد مربوط

۴- جزئیات عضو نقطه تماس

۴-۱ نام ..... ۴-۲ آدرس .....

۴-۲ سازمان ..... ۴-۴ اداره .....

۴-۵ تلفن ..... ۴-۶ رایانامه .....

۵ - جزئیات عضو ISIRT

۵-۱ نام ..... ۵-۲ آدرس .....

۵-۲ سازمان ..... ۵-۴ اداره .....

۵-۵ تلفن ..... ۵-۶ رایانامه .....

۶- توصیف رخداد امنیت اطلاعات

۶-۱ توصیف بیشتری از رخداد

- چه رخدادی به وقوع پیوسته است
- چگونه به وقوع پیوسته است
- چرا به وقوع پیوسته است
- دیدگاه‌های اولیه درمورد مولفه‌ها/دارایی‌هایی که تحت تأثیر قرارگرفته‌اند
- اثرهای نامطلوب کسب‌وکار
- آسیب‌پذیری‌های شناسایی شده

۷- جزئیات رخداد امنیت اطلاعات

۷-۱ تاریخ و زمان وقوع رخداد

۷-۲ تاریخ و زمان کشف رخداد

۷-۳ تاریخ و زمان گزارش رخداد

۷-۴ جزئیات شناسایی/ تماس شخص گزارش‌دهنده

۷-۵ پاسخگویی با این رخداد تمام شده‌است (مورد صحیح را تیک بزنید) بله☐ خیر☐

۷-۶ درصورت پاسخ مثبت، طول عمر رویداد را به روز/ساعت/دقیقه مشخص کنید.

---

۱ - بهتراست شماره رخدادها توسط مدیر ISIRT سازمان تخصیص، و با شماره رویدادهای مرتبط پیوند داده شود.

۸- رسته‌بندی رخداد امنیت اطلاعات

(یکی‌را تیک بزنید، سپس بخش مربوط را تکمیل کنید)

۸-۱ قطعی ☐ (رخداد به وقوع پیوسته است)

۸-۲ مشکوک ☐ (به‌نظر می‌رسد به وقوع پیوسته ولی تایید نشده است)

(یکی از) **۸-۳ بلایای طبیعی ☐** *(انواع تهدید وارد شده را نشان دهید)*

زلزله ☐ آتش‌فشان ☐ سیل ☐ تندباد ☐

رعدوبرق ☐ سونامی ☐ سقوط ☐ سایر ☐

مشخص کنید:

(یکی از) **۸-۴ ناآرامی اجتماعی ☐** *(انواع تهدید وارد شده را نشان دهید)*

وضعیت فوق العاده ☐ حمله تروریستی ☐ جنگ ☐ سایر ☐

مشخص کنید:

(یکی از) **۸-۵ صدمه فیزیکی ☐** (انواع تهدید وارد شده را نشان دهید)

آتش ☐ آب ☐ الکترواستاتیک ☐

محیط آلوده (مانند آلودگی، غبار، خوردگی، یخ‌زدگی) ☐

خرابی تجهیزات ☐ خرابی رسانه ☐ سرقت تجهیزات ☐ سرقت رسانه ☐ ازدست‌رفتن تجهیزات ☐

ازدست رفتن رسانه ☐ دستکاری با تجهیزات ☐ دستکاری با رسانه ☐ سایر ☐

مشخص کنید:

(یکی از) **۸-۶ نقص زیر ساخت ☐** *(انواع تهدید وارد شده را نشان دهید)*

نقص منبع تغذیه ☐ نقص شبکه ☐ نقص دستگاه تهویه هوا ☐

نقص منبع آب ☐ سایر ☐

مشخص کنید:

(یکی از) **۸-۷ تشعشع رادیویی ☐** *(انواع تهدید وارد شده را نشان دهید)*

تشعشع الکترومغناطیس ☐ پالس الکترومغناطیس ☐ تراکم الکترونیکی ☐

نوسان ولتاژ ☐ تشعشع حرارتی ☐ سایر ☐

مشخص کنید:

(یکی از) **۸-۸ نقص فنی ☐** (انواع تهدید وارد شده را نشان دهید)

نقص سخت‌افزار ☐ کارکرد خرابی نرم‌افزار ☐

سربار (اشباع ظرفیت سامانه‌های اطلاعاتی) ☐ رخنه در نگهداری ☐ سایر ☐

مشخص کنید:

گزارش رخداد امنیت اطلاعات

۸- رسته‌بندی رخداد امنیت اطلاعات

(یکی از) **۸-۹ بدافزار** ☐ *(انواع تهدید وارد شده را نشان دهید)*

کرم شبکه ☐ **اسب تروجان** ☐ **بات نت** ☐ **حملات مخلوط** ☐

کد مخربی تعبیه‌شده در صفحه تارنما ☐ **پایگاه میزبانی کد مخرب** ☐ **سایر** ☐

مشخص کنید:

(یکی از) **۸-۱۰ حمله فنی** ☐ *(انواع تهدید وارد شده را نشان دهید)*

پویش کردن شبکه ☐ **بهره‌برداری از آسیب‌پذیری** ☐ **بهره برداری از درب پشتی** ☐

تلاش‌های ثبت ورود، تداخل ☐ **انکار خدمت (DoS)** ☐ **سایر** ☐

مشخص کنید:

(یکی از) **۸-۱۱ نقض قاعده** ☐ *(انواع تهدید وارد شده را نشان دهید)*

کاربرد غیرمجاز منابع ☐ **نقض قانون حق تکثیر** ☐ **سایر** ☐

مشخص کنید:

(یکی از) **۸-۱۲ مخاطره انداختن کارکردها** ☐ *(انواع تهدید وارد شده را نشان دهید)*

سوء استفاده از حقوق ☐ **جعل حقوق، انکار اقدامات** ☐ **سوء عملیات** ☐

نقض دسترسی پذیری کارکنان ☐ **سایر** ☐

مشخص کنید:

(یکی از) **۸-۱۳ به مخاطره انداختن اطلاعات** ☐ *(انواع تهدید وارد شده را نشان دهید)*

ایجاد اختلال ☐ **جاسوسی، استراق سمع** ☐ **فاش کردن** ☐

دگرنمایی، مهندسی اجتماعی ☐ **کلاهبرداری اینترنتی** ☐ **سرقت داده** ☐

از دست رفتن داده ☐ **دست‌کاری داده** ☐ **خطای داده** ☐ **تحلیل گردش داده** ☐

آشکارسازی موقعیت ☐ **سایر** ☐

مشخص کنید:

(یکی از) **۸-۱۴ محتویات مضر** ☐ *(انواع تهدید وارد شده را نشان دهید)*

محتویات غیرقانونی ☐ **محتویات ترسناک** ☐ **محتویات مخرب** ☐

محتویات توهین‌آمیز ☐ **سایر** ☐

مشخص کنید:

۸-۱۵ سایر ☐ *(اگر هنوز معلوم نشده رخداد متعلق به کدامیک از رسته‌های فوق است، اینجا را تیک بزنید)*

مشخص کنید:

۹- مولفه‌ها/دارایی‌های آسیب‌دیده[۱]

مولفه‌ها/دارایی‌های آسیب‌دیده (درصورتی که موجود باشد)

(برای مولفه‌ها/دارایی‌های آسیب‌دیده به‌وسیله یا مربوط به رخداد، در جایی‌که مرتبط باشد توصیفاتی محتوی شماره‌های سری، حق امتیاز و نسخه ارایه گردد.)

۹-۱ اطلاعات/داده .....

۹-۲ سخت‌افزار .....

۹-۳ نرم‌افزار .....

۹-۴ ارتباطات .....

۹-۵ مستندسازی .....

۹-۶ فرایندها .....

۹-۷ سایر .....

۱۰- تاثیر/اثر نامطلوب حاصل از رخداد

در مقابل هریک از موارد مرتبط با رخدادهای زیر تیک بزنید، سپس سطح یا سطوح اثر نامطلوب را با پوشش دادن همه طرف‌هایی که تحت تاثیر رخداد قرارگرفته‌اند، در مقیاس ۱ تا ۱۰ با استفاده از راهنماهای رسته‌بندی در زیر «مقدار» ثبت کنید. رسته‌بندی‌های مندرج در راهنما عبارتند از: زیان/خسارت مالی به عملیات کسب وکار، منافع تجاری و اقتصادی، اطلاعات شخصی، تعهدات قانونی و مقرراتی، عملیات مدیریت کسب وکار، و ازدست رفتن حسن شهرت. (مثال‌ها در پیوست پ-۳-۲ ملاحظه شود). حروف کد راهنماهای کاربست‌پذیر را در مقابل «راهنما»، و اگر هزینه‌های واقعی معلوم هستند در مقابل «هزینه» ثبت کنید.

	ارزش	راهنما(ها)	هزینه
۱۰-۱ نقض محرمانگی (یعنی افشای غیرمجاز)	☐		
۱۰-۲ نقض یکپارچگی (یعنی تغییر غیرمجاز)	☐		
۱۰-۳ نقض دسترس‌پذیری (یعنی دسترس‌ناپذیری)	☐		
۱۰-۴ نقض عدم انکار	☐		
۱۰-۵ خرابی	☐		

۱۱- کل هزینه‌های بازیابی رخداد

(درصورت امکان، بهتر است جمع هزینه‌های واقعی بازیابی رخداد درکل نشان‌داده شود، در زیر «مقدار» با استفاده از مقیاس ۱ تا ۱۰ و درزیر «هزینه« مبالغ واقعی.)	ارزش	راهنما(ها)	هزینه

۱ - این قسمت برای جزئیات بیشتر درباره مولفه‌ها/دارایی‌هایی آسیب‌دیده است، که درجریان بررسی و تحلیل در دسترس قرار می‌گیرند (معمولا در مراحل اولیه تحلیل رویداد و رخداد امنیت اطلاعات فقط اطلاعات «سطح بالا» جمع‌آوری خواهد شد).

گزارش رخداد امنیت اطلاعات

۱۲- برطرف کردن رخداد

۱۲-۱ تاریخ اغاز بررسی رخداد .....

۱۲-۲ نام (ها)ی بررسی‌کنندگان رخداد .....

۱۲-۳ تاریخ پایان رخداد .....

۱۲- ۴ تاریخ پایان اثر .....

۱۲-۵ تاریخ تکمیل بررسی رخداد .....

۱۲-۶ مرجع و محل گزارش بررسی .....

۱۳- (اگر عامل رخداد، انسان باشد) شخص(اشخاص) /عامل(عاملین) درگیر

(یکی از) **شخص** ☐ **سازمان/نهاد تاسیس‌شده قانونی** ☐

گروه سازمان‌یافته ☐ **تصادف** ☐

بدون عامل مثال عناصر طبیعی، نقص تجهیزات، خطای انسانی ☐

۱۴- توصیف آماده‌کننده

۱۵- انگیزه واقعی یا موردنظر

(یکی از) **دستاورد جنایی/مالی** ☐ **سرگرمی/رخنه‌گری** ☐

سیاسی/تروریسم ☐ **انتقام** ☐

سایر ☐

مشخص کنید:

۱۶- اقدامات به‌عمل آمده برای برطرف کردن رخداد

(مثال «بدون اقدام»، «اقدام داخل سازمان»، «بررسی داخل سازمان»، «بررسی خارج از سازمان توسط...»)

۱۷- اقدامات برنامه ریزی‌شده برای برطرف کردن رخداد

(مثال‌های بالا ملاحظه شوند)

۱۸- اقدامات برجسته

(مثال هنوز بررسی توسط سایر کارکنان مورد نیاز است)

گزارش رخداد امنیت اطلاعات

۱۹- نتیجه گیری

(برای نشان‌دادن اینکه رخداد عمده یا جزئی درنظرگرفته شده است، و گنجاندن شرح کوتاهی برای توجیه نتیجه‌گیری) **عمده** ☐ **جزئی** ☐ *(به هر نتیجه‌گیری دیگری اشاره شود)*

۲۰- افراد /هستارهای داخلی مطلع

(این جزئیات که اقدامات ضروری را بیان می‌کند، توسط شخص مرتبط با مسئولیت‌های امنیت اطلاعات تکمیل می‌شود. برحسب مورد، ممکن است توسط مدیر امنیت اطلاعات سازمان یا مقام رسمی دیگری تایید شود)

مدیر /مقام مسئول

امنیت اطلاعات ☐

مدیر پایگاه ☐

(پایگاه را مشخص کنید)

مبدأ گزارشگر ☐

مدیر ISIRT ☐

مدیر سامانه‌های اطلاعاتی ☐

مدیر مبدأ گزارشگر /مدیریت کاربر خط آسیب‌دیده ☐

سایر ☐

(برای مثال پیشخوان، مدیریت منابع انسانی،ممیزی داخلی)

مشخص کنید:

۲۱- افراد /هستارهای خارجی مطلع

(این جزئیات که اقدامات ضروری را بیان می‌کند، توسط شخص مرتبط با مسئولیت‌های امنیت اطلاعات تکمیل می‌شود. برحسب مورد، ممکن است توسط مدیر امنیت اطلاعات سازمان یا مقام رسمی دیگری تایید شود)

پلیس ☐

سایر ☐

(برای مثال نهاد تنظیم مقررات، ISIRT خارجی)

مشخص کنید:

۲۲- محل امضاء

گزارشگر مبدأ	بازبین	بازبین
امضای دیجیتالی	**امضای دیجیتالی**	**امضای دیجیتالی**
_____	_____	_____
نام	**نام**	**نام**
_____	_____	_____
نقش	**نقش**	**نقش**
_____	_____	_____
تاریخ	**تاریخ**	**تاریخ**
_____	_____	_____

ت-۴-۳ مثال از برگه‌های گزارش آسیب‌پذیری امنیت اطلاعات

گزارش آسیب پذیری امنیت اطلاعات

۱- تاریخ شناسایی آسیب‌پذیری

۲- شماره آسیب‌پذیری[1]

۳- جزئیات شخص گزارش‌دهنده

۳-۱ نام ..... ۳-۲ آدرس .....

۳-۲ سازمان ..... ۳-۴ اداره .....

۳-۵ تلفن ..... ۳-۶ رایانامه .....

۴- توصیف آسیب پذیری امنیت اطلاعات

۴-۱ تاریخ و زمان آسیب‌پذیری گزارش‌شده

۴-۲ توصیف آسیب‌پذیری امنیت اطلاعات مورد نظر به تفصیل:

- چگونگی اعلام آسیب‌پذیری
- خصوصیات آسیب‌پذیری – فیزیکی، فنی، غیره.
- اگر آسیب‌پذیری فنی است، چه فناوری اطلاعات/مولفه‌های شبکه/دارایی‌هایی مورد توجه هستند
- مولفه‌ها/دارایی‌هایی که ممکن بود آسیب ببینند اگر باید آسیب‌پذیری بهره‌برداری می‌شد
- تاثیرات بالقوه نامطلوب کسب‌وکار اگر باید آسیب‌پذیری بهره‌برداری می‌شد

۵- برطرف کردن آسیب‌پذیری امنیت اطلاعات

۵-۱ آیا آسیب‌پذیری تایید شده‌است؟ (مورد صحیح را تیک بزنید) **بله** ☐ **خیر** ☐

۵-۲ تاریخ و زمان تایید آسیب‌پذیری

۵-۳ نام شخص صادرکننده مجوز **۵-۴ آدرس**

۵-۶ تلفن **۵-۷ رایانامه**

۵-۸ آیا آسیب‌پذیری برطرف کردن شده‌است؟ (مورد صحیح را تیک بزنید) **بله** ☐ **خیر** ☐

۵-۹ توصیف اینکه آسیب‌پذیری امنیت اطلاعات چگونه برطرف کردن شده‌است به تفصیل، با ذکر تاریخ و نام شخصی که مجوز برطرف کردن را صادر کرده‌است.

۱ - بهتراست شماره‌های آسیب‌پذیری توسط مدیر ISIRT سازمان تخصیص داده شود.

پیوست ث

(اطلاعاتی)

جنبه‌های قانونی و مقرراتی

بهتراست در خط‌مشی مدیریت رخداد امنیت اطلاعات و طرح‌واره‌ی مرتبط آن، به جنبه‌های قانونی و مقرراتی زیر از مدیریت رخداد امنیت اطلاعات تاکید شود:

- **محافظت کافی از داده‌ها و حریم اطلاعات شخصی [1] به عمل می‌آید.** در کشورهایی که قوانین مشخصی وجود دارد که محرمانگی وصحت داده را پوشش می‌دهند، اغلب به کنترل داده شخصی محدود می‌شود. از آنجایی‌که رخدادهای امنیت اطلاعات باید نوعا به فردی نسبت داده شود، بنابراین اطلاعات ماهیت شخصی باید ثبت و مدیریت شود. بنابراین یک رویکرد ساختاری برای مدیریت رخداد امنیت اطلاعات باید محافظت مناسب از محرمانگی را مورد توجه قرار دهد. این موضوع می‌تواند شامل:

- کارکنانی که دسترسی به اطلاعات شخصی دارند، بهتراست تا آنجایی که عملی است، بطور شخصی، فردی (افرادی) را که بررسی شده اند نشناسند.

- بهتراست موافقت‌نامه عدم-افشا با کارکنانی که دسترسی به داده شخصی دارند قبل از اینکه به آن‌ها اجازه دسترسی داده شود، امضا شود.

- بهتراست اطلاعات، تنها در جهت هدفی که برای آن گردآوری شده؛ یعنی، برای بررسی رخداد امنیت اطلاعات مورد استفاده قرارگیرد.

- **نگهداری مناسب از سوابق، اعمال می‌شود.** بعضی قوانین ملی شرکت‌ها را ملزم می‌کنند که سوابق مناسبی از فعالیت‌های خود جهت بازنگری در فرایند ممیزی سالیانه سازمان، برقرار کنند. الزامات مشابهی جهت سازمان‌های دولتی نیز وجود دارد. در برخی کشورهای معین، سازمان‌ها ملزم به گزارش‌دهی یا ایجاد بایگانی‌هایی جهت نهادهای قانونی هستند (برای مثال در خصوص هر مورد که ممکن است شامل یک جرم جدی یا نفوذ به یک سامانه حساس دولت شود).

- **کنترل‌ها برای حصول اطمینان از ایفای تعهدات قرارداد تجاری [2] به‌کار برده می‌شوند.** درجایی‌که الزامات مقیدکننده در ارایه خدمات مدیریت یک رخداد امنیت اطلاعات وجود دارد، برای مثال برای پوشش‌دادن به زمان‌های پاسخگویی مورد نیاز، یک سازمان بهتراست اطمینان پیدا کند

1- Privacy of Personal Infotmation
2- Commercial Contractual

که امنیت اطلاعات مناسب برای حصول اطمینان از ایفای چنین تعهداتی در تمام شرایط، ارایه می‌شود (در این ارتباط، اگر سازمانی با طرف خارجی برای پشتیبانی، قراردادی منعقد نماید، برای مثال یک ISIRT خارجی، پس بهتراست اطمینان حاصل نماید که تمام الزامات، ازجمله زمان‌های پاسخگویی، در قرارداد با طرف خارجی از سازمان گنجانده شده‌است).

- **مسایل قانونی مربوط به خطمشی‌ها و روش‌های اجرایی لحاظ می‌شوند**. بهتراست خطمشی‌ها و روش‌های اجرایی مرتبط با طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات از نظر امور قانونی و مقرراتی بالقوه وارسی شوند. برای مثال اگر بیانیه‌هایی در مورد اقدام انضباطی و/یا قانونی، علیه آن‌هایی که موجب رخدادهای امنیت اطلاعات می‌شوند، وجودداشته باشد. در برخی کشورها خاتمه بخشیدن به رابطه استخدامی آسان نیست.

- **تکذیب‌نامه‌ها[1] برای داشتن اعتبار قانونی وارسی می‌شوند**. بهتراست تمام تکذیب‌نامه‌ها در خصوص اقدامات انجام‌شده توسط گروه مدیریت رخداد اطلاعات، و هرفرد پشتیبانی خارجی، ازنظر داشتن اعتبار قانونی وارسی شوند.

- **کارکنان پشتیبانی مربوط به قراردادهای برون‌سپاری، تمام جنبه‌های الزامی را پوشش می‌دهند.** بهتراست قراردادهای مشتمل بر هرگونه پشتیبانی کارکنان خارجی، برای مثال از یک ISIRT خارجی، به‌طور کامل از لحاظ مواردی مانند فرار از مسئولیت، عدم- افشا، دسترسی‌پذیری خدمات و عواقب مشاوره‌های نادرست، وارسی شوند.

- **موافقت‌نامه‌های عدم-افشا قابل اجرا هستند.** اعضای گروه مدیریت رخداد امنیت اطلاعات ممکن است ملزم به امضای موافقت‌نامه عدم-افشا، هم در آغاز و هم در پایان استخدام شوند. در بعضی کشورها، الزام به امضای موافقت‌نامه عدم-افشا از نظر قانون موثر نیست؛ بهتراست این مسئله وارسی شود.

- **الزامات اجرای قانون مورد تاکید قرار می‌گیرند.** موضوعات مرتبط با امکان اینکه نمایندگان اجرای قانون بتوانند بطور قانونی از یک طرح‌واره‌ی مدیریت رخداد امنیت اطلاعات، درخواست اطلاعات نمایند، باید روشن شود. ممکن است روشن‌گری در مورد اینکه رخدادها بهتراست مستند شوند، و مستند بهتراست چه مدت نگهداری شود، در سطح کمینه، بطور قانونی الزامی شود.

1- Disclaimers

- **جنبه‌های مسئولیتی روشن هستند.** مسائل مسؤولیتی بالقوه، و کنترل‌های مربوط مورد نیاز برای به‌کاربردن آن‌ها، باید روشن شوند. مثال‌هایی از رویدادهایی که ممکن است با مسائل مسؤولیت مرتبط باشند، عبارتند از:

- اگر یک رخداد بتواند بر سازمان دیگری تأثیر گذارد (برای مثال افشای اطلاعات اشتراکی) و به موقع مطلع نشود و آن سازمان از یک اثر نامطلوب لطمه ببیند.

- اگر آسیب‌پذیری جدیدی در یک محصول کشف شود، و فروشنده مطلع نشود و بعدا یک رخداد اصلی جدی مربوط به آن با اثر اصلی در یک یا چند سازمان دیگر، به وقوع به‌پیوندد.

- یک گزارش تهیه نمی شود، مگر درجایی که، در کشور خاص، سازمان‌ها ملزم شوند در خصوص هر مورد که ممکن است شامل یک جرم جدی، یا نفوذ به یک سامانه حساس دولتی یا قسمتی از زیرساخت حیاتی ملی، گزارش ارایه یا برای موسسات مجری قانون، بایگانی تشکیل دهند.

- اطلاعاتی افشا شود که نشان میدهد ممکن است فرد، یا سازمانی، در یک حمله دخیل باشد. این امر می‌تواند به شهرت و کسب‌وکار شخص یا سازمان دخیل، صدمه بزند.

- اطلاعاتی افشا شود که ممکن است مشکلی با آیتم ویژه‌ای از نرم‌افزار وجود داشته باشد و مشخص شود که این امر حقیقت نداشته است.

- **الزامات مشخص مقرراتی نشان‌دهی می‌شوند.** در جائی‌که الزامات مقرراتی مشخص ایجاب می‌کند، بهتراست رخدادها به یک نهاد تعیین شده گزارش شوند، برای مثال همان‌طور که در صنعت نیروگاه اتمی، شرکت‌های مخابراتی و ارایه‌کنندگان خدمات اینترنتی در بسیاری از کشورها، مورد نیاز است.

- **پی‌گردهای قانونی، یا روش‌های اجرایی انضباطی داخلی، می‌تواند موفق باشد.** بهتراست کنترل‌های مناسب جهت امنیت اطلاعات به‌کار برده شوند، ازجمله با ردّ ممیزی ضد - مداخله[1] به نحو قابل اثبات، تا بتوان پی‌گرد موفقیت‌آمیزی انجام داد، یا روش‌های اجرایی انضباطی داخلی علیه «حمله‌کنندگان» اعم از حمله‌های فنی یا فیزیکی آورده شود. جهت پشتیبانی از این امر، باید شواهد نوعاً قابل قبولی برای ارائه به دادگاه‌های قانونی ملی مرتبط یا دیگر مراجع انضباطی جمع آوری شود. بهتر است، امکان نشان‌دادن موارد زیر وجود داشته باشد:

- سوابق کامل هستند و درمورد آن‌ها به هیچ وجه مداخله‌ای صورت نگرفته است،

- رونوشت‌های شواهد الکترونیکی به صورت قابل اثباتی برابر اصل هستند،

1-Tamper-proof

- هر سامانه IT در زمانی که برای گردآوری شواهد استفاده شده‌است، درست عمل کرده‌است.

- **جنبه‌های قانونی مرتبط با فنون پایش نشان‌دهی می‌شوند.** عواقب استفاده از فنون پایش اطلاعات باید در مقوله قانون ملی مرتبط، نشاندهی می‌شوند. قانونی بودن فنون مختلف از کشوری به کشور دیگر فرق می‌کند. برای مثال، دربرخی از کشورها لازم است که به اشخاص در مورد پایش فعالیت‌ها، از جمله از طریق فنون مراقبت، اطلاع رسانی شود. عواملی که باید مورد توجه قرارگیرند عبارتند از چه کسی/چه چیزی پایش می‌شود، چطور آنها/آن پایش می‌شوند و چه موقع پایش به وقوع می‌پیوندد. بهتراست یادآوری کرد پایش/نظارت در مقوله IDS به طور خاص در استاندارد ملی ایران شماره ۱۸۰۴۳: سال ۱۳۸۸، مورد بحث قرارگرفته است.

- **خط‌مشی استفاده قابل قبول، تعریف و مبادله می‌شود.**

بهتراست در سازمان تمرین/استفاده[1] قابل قبول تعریف، مستندسازی‌شده و با همه کاربران مورد نظر مبادله شود (برای مثال، کاربران باید از خط‌مشی استفاده قابل قبول مطلع شوند و از آن‌ها اقرار مکتوب مبنی بر درک و قبول آن خط‌مشی هنگام پیوستن به یک سازمان یا اجازه دسترسی به اطلاعات سامانه ها را دریافت کرده اند، اخذ شود.

1- practice/use

کتاب‌نامه

[۱] استاندارد ملی ۱۸۰۴۳: سال ۱۳۸۸- فناوری اطلاعات - فنون امنیت – انتخاب، استقرار و عملیات سامانه‌های تشخیص نفوذ

[2] ISO/IEC 20000 (all parts), *Information technology — Service management*

[3] ISO/PAS 22399, *Societal security — Guidelines for incident preparedness and operational continuity management*

[۴] استاندارد ملی ۲۷۰۰۱: سال ۱۳۸۷- فنون امنیت – سامانه‌های مدیریت امنیت اطلاعات – الزامات

[۵] استاندارد ملی ۲۷۰۰۲: سال ۱۳۸۷- فناوری اطلاعات- فنون امنیت – آیین‌کار مدیریت امنیت اطلاعات

[6] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

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

[۸] استاندارد ملی ۲۷۰۰۵: سال ۱۳۸۸- فناوری اطلاعات - فنون امنیت – مدیریت ریسک امنیت اطلاعات

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

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

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

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

[13] Internet Engineering Task Force (IETF) Site Security Handbook, http://www. ietf. org/rfc/rfc2196- txt?number=2196

[14] Internet Engineering Task Force (IETF) RFC 2350, Expectations for Computer Security Incident Response, http://www. ietf. org/rfc/rfc2350. txt?number=2350

[15] NIST Special Publication 800-61, Computer Security Incident Handling Guide (2004), http://csrc. nist. gov/publications/nistpubs/800-61-rev1/SP800-61rev1-pdf

[16] TERENA's Incident Object Description Exchange Format Data Model and XML Implementation (IODEF) (produced by IETF), RFC 5070

[17] Internet Engineering Task Force (IETF) RFC 3227, Guidelines for evidence collection and archiving

[18] CESG GOVCERTUK, Incident Response Guidelines (2008), http://www. govcertuk. gov. uk/pdfs/incident_response_guidelines.pdf

[19] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Capability Metrics Version 0.1 (2007), http://www. cert. org/archive/pdf/07tr008-pdf

[20] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Incident Management Mission Diagnostic Method Version 1.0, http://www. cert. org/archive/pdf/08tr007-pdf

[21] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Defining Incident Management Processes for CSIRTs: A Work in Progress, http://www. cert. org/archive/pdf/04tr015-pdf

[22] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Handbook for Computer Security Incident Response Teams (CSIRTs), http://www. cert. org/archive/pdf/csirthandbook.pdf

[23] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", State of the Practice of Computer Security Incident Response Teams, http://www. cert. org/archive/pdf/03tr001-pdf

[24] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", CSIRT Services, http://www. cert. org/csirts/services. html

[25] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Action List for Developing a Computer Security Incident Response Team (CSIRT), http://www. cert. org/csirts/action_list. Html

[26] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed? http://www. cert. org/csirts/csirt-staffing. html

[27] Software Engineering Institute at Carnegie Mellon "CERT Coordination Centre", Steps for Creating National CSIRTs, http://www. cert. org/archive/pdf/NationalCSIRTs.pdf

[28] SANS Institute, An approach to the ultimate in-depth security event management framework (2008)

[29] SANS Institute, Mining gold, A primer on incident handling and response (2008)

[30] SANS Institute, Incident Handling for SMEs (Small to Medium Enterprises) (2008)

[31] SANS Institute, Breach Notification in Incident Handling (2008)

[31] SANS Institute, Breach Notification in Incident Handling (2008)

[32] SANS Institute, Baselines and Incident Handling (2008)

[33] SANS Institute, Documentation is to Incident Response as an Air Tank is to Scuba Diving (2007)

[34] SANS Institute, Creating and Managing an Incident Response Team for a Large Company (2007)

[35] SANS Institute, An Incident Handling Process for Small and Medium Businesses (2007)

[36] SANS Institute, Incident Management 101 Preparation & Initial Response (aka Identification) (2005)

[37] SANS Institute, Building an Incident Response Program To Suit Your Business (2003)

[38] ISACA, COBIT 4- 1 (Section DS5- 11), www.isaca.org/cobit

[39] ENISA, A step-by-step approach on how to set up a CSIRT, http://www.enisa.europa.eu/act/cert/support/guide

[40] ENISA, CERT cooperation and its further facilitation by relevant stakeholders, http://www.enisa.europa.edu/act/cert/background/coop

[41] ENISA, A basic collection of good practices for running a CSIRT, http://www.enisa.europa.edu/act/cert/support/guide2

[42] TERENA's Incident Object Description and Exchange Format Requirements (IODEF) (produced by IETF), RFC 3067

[43] CVSS — A complete Guide to the Common Vulnerability Scoring System (Version 2.0), FIRST, 20 June 2007, http://www.first.org/cvss/cvss-guide.html

[44] SWIF — Structured Warning Information Format (Version 2.3), ITsafe, 9 May 2008

[45] ITIL, ITIL framework document, http://www.itil-officialsite.com/home/home.asp