INSO-ISO-IEC

27010
1st. Revision
2017

Identical with
ISO/IEC 27010:2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران
ایزو- آی ای سی
۲۷۰۱۰
تجدید نظر اول
۱۳۹۶

فناوری اطلاعات-
فنون امنیتی- مدیریت امنیت اطلاعات برای ارتباطات بین‌بخشی و بین‌سازمانی

Information technology — Security techniques — information security management for inter-sector and inter-organizational communications

ICS: 03.100.70; 35.030

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

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 عهده‌دارد.

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

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

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

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

---

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

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات– فنون امنیتی– مدیریت امنیت اطلاعات برای ارتباطات بین‌بخشی و بین‌سازمانی»

«تجدید نظر اول»

رئیس:	سمت و/ یا محل اشتغال:
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات- سیستم‌های اطلاعاتی)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون مدیر کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
تهرانی، محمد (کارشناسی ارشد فناوری اطلاعات)	مدیر کارت و خدمات نوین– بانک قوامین
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
رادمهر، وحید (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	پژوهش‌گر- پژوهشگاه ارتباطات و فناوری اطلاعات - مرکز تحقیقات مخابرات ایران
عباسپور، مقصود (دکتری مهندسی کامپیوتر- معماری)	دانشیار– معاون مرکز فناوری دانشگاه شهید بهشتی
طی نیا، رضا (کارشناسی ارشد فناوری اطلاعات)	مدیر عامل– شرکت مهندسی کاربرد سیستم (کاسیس)
مطلق، کامبیز (کارشناسی ارشد فناوری اطلاعات)	معاون فناوری اطلاعات– بانک قوامین
مغانی، مهدی (کارشناسی ارشد ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران
ناظمی، اسلام (دکتری مهندسی کامپیوتر)	دانشیار- دانشگاه شهید بهشتی

اعضاء : (اسامی به ترتیب حروف الفبا)

سمت و/ یا محل اشتغال:

نصیری آسایش، حمیدرضا
(کارشناسی ارشد فناوری اطلاعات معماری سازمانی)
پژوهش‌گر- دانشگاه شهید بهشتی

یعقوبی رفیع، کمال الدین
(کارشناسی ارشد فناوری اطلاعات معماری سازمانی)
پژوهش‌گر- دانشگاه شهید بهشتی

ویراستار:

سمت و/ یا محل اشتغال:

معروف، سینا
(لیسانس مهندسی کامپیوتر، سخت‌افزار)
کارشناس تدوین استانداردهای حوزه فناوری اطلاعات- سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات– فنون امنیتی– مدیریت امنیت اطلاعات برای ارتباطات بین‌بخشی و بین-سازمانی» که نخستین بار در سال ۱۳۹۲ بر مبنای پذیرش استانداردهای بین‌المللی به‌عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تدوین و منتشر شد، بر اساس پیشنهادهای دریافتی و بررسی و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدیدنظر قرار گرفت و در چهارصد و نود و پنجمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۶/۰۲/۰۳ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ایران-ایزو-آی ایی سی ۲۷۰۱۰: سال ۱۳۹۲ است.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 27010: 2015, Information technology – Security techniques — Information security management for inter-sector and inter-organizational communications

مقدمه

این استاندارد مکملِ بخش خاص برای استاندارد ملی ایران به شماره ایران- ایزو- آی ای سی ۲۷۰۰۱: سال ۱۳۹۴ و استاندارد ملی ایران به شماره ایران- ایزو- آی ای سی ۲۷۰۰۲: سال ۱۳۹۴ است که به منظور استفاده جوامع اشتراک اطلاعات است. رهنمودهای گنجانده شده در این استاندارد، متمم و افزون بر راهنمایی‌های کلی ارائه شده در سایر مجموعه استانداردهای ۲۷۰۰۰ است.

استاندارد ملی ایران به شماره ایران- ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴ و استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲: سال ۱۳۹۴ به تبادل اطلاعات بین سازمان‌ها می‌پردازند، اما این کار را به روش کلی انجام می‌دهند. زمانی که سازمان‌ها قصدِ انتقال اطلاعات حساس به چندین سازمان دیگر را دارند، ایجادکنندهٔ پیام[1] باید اطمینان داشته باشد که استفاده از آن در سازمان‌های دیگر در معرض واپایش‌های امنیتی کافی که به وسیله سازمان‌های پذیرنده پیاده‌سازی شده قرار خواهد گرفت. از طریق ایجاد جامعه اشتراک اطلاعات می‌توان به این مهم دست یافت، که در آن هرعضو در مورد حفاظت از اطلاعات اشتراکی، به دیگر اعضا اعتماد می‌کند حتی اگر ممکن است سازمان‌ها در رقابت با یکدیگر باشند.

جامعه اشتراک اطلاعات نمی‌تواند بدون وجود اعتماد، کار کند. آن‌هایی که تامین‌کننده اطلاعات هستند باید بتوانند به دریافت‌کنندگان اطلاعات اعتماد کنند که به گونه‌ای نامناسب داده را افشا[2] نکنند یا به گونه‌ای نامناسب از آن استفاده نکنند. آن‌هایی که پذیرنده اطلاعات هستند باید بتوانند اطمینان حاصل کنند که منوط به هر گونه وضعیت اطلاع داده شده توسط ایجادکنندهٔ پیام، اطلاعات درست است. هر دو جنبه مهم است و باید آشکارا توسط خط‌مشی‌های اثربخش و با استفاده از شیوه‌ای خوب پشتیبانی شوند. بدین منظور، اعضای جامعه باید همگی سامانه مدیریت مشترک پیاده‌سازی کنند که امنیت اطلاعات اشتراکی را پوشش دهد. این سامانه مدیریت امنیت اطلاعات (ISMS)[3] برای جامعه اشتراک اطلاعات است.

به علاوه، اشتراک اطلاعات می‌تواند بین جوامع اشتراک اطلاعات رخ دهد، جای‌که همهٔ گیرندگان، برای ایجادکنندهٔ پیام شناخته شده نیستند. این امر تنها زمانی عملی خواهد شد که اعتماد کافی بین جوامع و توافقات اشتراک اطلاعات آن‌ها وجود داشته باشد. به ویژه، این موضوع مربوط به اشتراک اطلاعات حساس بین جوامع متنوع از قبیل بخش‌های مختلف صنعت یا بازار است.

1- Originator
2 - Disclose
3 - Information Security Management System

فناوری اطلاعات– فنون امنیتی– مدیریت امنیت اطلاعات برای ارتباطات بین‌بخشی و بین‌سازمانی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین رهنمودهایی افزون بر راهنمایی‌های مجموعه استانداردهای ۲۷۰۰۰ برای پیاده‌سازی مدیریت امنیت اطلاعات در جوامع اشتراک اطلاعات است.

این استاندارد به‌طور مشخص، واپایش‌ها و راهنمایی مربوط به آغاز، پیاده‌سازی، نگهداری و بهبود امنیت اطلاعات را در ارتباطات بین‌سازمانی و بین‌بخشی ارائه می‌کند. این استاندارد راهنمایی‌ها و اصول کلی را در مورد چگونگی برآورده ساختن الزامات مشخص با استفاده از پیام‌رسانی و دیگر روش‌های فنی، ارائه می‌کند.

این استاندارد در تمامی شکل‌های تبادل و اشتراک اطلاعات حساس، هم عمومی و هم حریم خصوصی، ملی و بین‌المللی، در بخش یکسانی از صنعت یا بازار یا بین بخش‌ها، کاربردپذیر است. به خصوص ممکن است این استاندارد در تبادل و اشتراک اطلاعات مربوط به تامین، نگهداری و حفاظت از زیرساخت حیاتی سازمان یا دولت، کاربردپذیر باشد. این استاندارد برای پشتیبانی از ایجاد اعتماد هنگام تبادل و اشتراک اطلاعات حساس طراحی شده است، بنابراین، مشوقِ رشد بین‌المللی جوامع اشتراک اطلاعات است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده‌شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن موردنظر این استاندارد ملی ایران نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۰: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سیستم های (سامانه‌های) مدیریت امنیت اطلاعات-مرور کلی و واژگان

۲-۲ استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات

۲-۳ استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲: سال ۱۳۹۴، فناوری اطلاعات- فنون امنیتی- آیین کار برای واپایش‌های امنیت اطلاعات

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۰: سال ۱۳۹۴، به کار می‌رود.

۴ مفاهیم و توجیه

۴-۱ مقدمه

راهنمای ISMS، مخصوصِ ارتباطات بین‌بخشی و بین‌سازمانی، در بندهای ۵ تا ۱۸ این استاندارد شناسایی شده است.

استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، واپایش‌هایی را تعریف می‌کند که تبادل اطلاعات دوجانبه بین سازمان‌ها را پوشش می‌دهد و همچنین برای توزیعِ کلی اطلاعاتِ در دسترس عموم، واپایش‌هایی را تعریف می‌کند. با این وجود، در بعضی شرایط نیازی برای اشتراک اطلاعات در جامعه‌ای از سازمان‌ها وجود دارد، جایی که اطلاعات به طریقی حساس بوده و نمی‌توان آن‌ها را در دسترس اعضایی غیر از اعضای جامعه و در دسترس عموم قرار داد. اغلب اطلاعات را می‌توان تنها در دسترس افرادی معین از هر سازمان عضو قرار داد یا ممکن است اطلاعات دارای الزامات امنیتی دیگری از قبیل گمنامی اطلاعات باشد. این استاندارد، واپایش‌های بالقوه افزوده‌ای را تعریف کرده و راهنمایی و تفسیری افزون بر استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴ و استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به منظور برآورده ساختن این الزامات ارائه می‌کند.

چهار پیوست آگاهی‌دهنده وجود دارد. پیوست الف مزیت‌های بالقوه اشتراک اطلاعات حساس بین سازمان‌ها را توصیف می‌کند. پیوست ب راهنمایی‌هایی در مورد این‌که چگونه اعضای جامعه اشتراک اطلاعات می‌توانند میزان اعتماد که می‌تواند در اطلاعات قرار داده شده توسط اعضا را ارزیابی کند، ارائه می‌کند. پیوست پ پروتکل چراغ راهنمایی رانندگی[1] را توصیف می‌کند، سازوکاری که به طور گسترده برای نشان دادن توزیع مجاز اطلاعات در جوامع اشتراک اطلاعات استفاده می‌شود. پیوست ت دربردارندهٔ چند نمونه الگو برای سازمان‌دهی جامعه اشتراک اطلاعات است.

۴-۲ جوامع اشتراک اطلاعات

جوامع اشتراک اطلاعات، برای اثربخش بودن، باید برای تعریف محدوده اطلاعات حساس به اشتراک گذاشته شده، منافعی مشترک یا روابط دیگری داشته باشند. به عنوان مثال، جوامع ممکن است بخش خاصی از بازار باشند و عضویت را در سازمان‌های داخل آن بخش محدود سازند. البته ممکن است مبناهای دیگری برای منافع مشترک وجود داشته باشد، برای مثال، مکان جغرافیایی یا مالکیت مشترک.

1 - Traffic Light Protocol

همچنین باید بین اعضا، اعتماد وجود داشته باشد، به ویژه این‌که همه‌ی اعضا از توافق‌نامه اشتراک اطلاعات پیروی خواهند کرد.

۴-۳ مدیریت جامعه

جوامع اشتراک اطلاعات از سازمان‌ها یا قسمت‌های مستقل سازمانی ایجاد خواهد شد. بنابراین نمی‌تواند ساختارهای سازمانی و کارکردهای مدیریتی واضح یا یکنواختی برای تمامی اعضا به کار رود. برای اثربخشی مدیریت امنیت اطلاعات، تعهد مدیریتی ضروری است. بنابراین توصیه می‌شود، ساختارهای سازمانی و کارکردهای مدیریتی به کار برده شده در مدیریت امنیت اطلاعات جامعه، به طور واضح تعریف شوند.

همچنین توصیه می‌شود تفاوت‌ها میان سازمان‌های عضو جامعه اشتراک اطلاعات در نظر گرفته شوند. این تفاوت‌ها می‌تواند شامل موارد زیر باشد:

- تفاوت‌گذاری بین محیط‌های مقرراتی[1] یا قانونی[2]،
- این که آیا سازمان‌های عضو، از قبل ISMS خود را به کار می‌برند، و
- قواعد[3] عضو در مورد حفاظت از دارایی‌ها و حفاظت از افشای اطلاعات.

۴-۴ هستار[4]های پشتیبانی‌کننده

بسیاری از جوامع اشتراک اطلاعات، جهت سازمان‌دهی و پشتیبانی اشتراک اطلاعات، اقدام به ایجاد یا گماردن[5] یک هستار پشتیبانی‌کننده متمرکز خواهند کرد. چنین هستاری می‌تواند واپایش‌های پشتیبانی‌کننده بسیاری را ارائه کند، از قبیل ساده‌تر و کاراتر کردن گمنامی منبع و دریافت‌کننده نسبت به جایی که اعضا به صورت مستقیم ارتباط دارند.

الگوهای سازمانی متفاوتی وجود دارند که می‌توان آن‌ها را جهت ایجاد هستارهای پشتیبانی‌کننده مورد استفاده قرار داد. پیوست ت این استاندارد، دو الگوی مشترک را توصیف می‌کند، هستار ارتباطی اطلاعات مورد اعتماد (TICE) [6] نقطه اعلام هشدار، مشاوره و گزارش‌دهی (WARP) [7].

۴-۵ ارتباط بین‌سازمانی

بسیاری از جوامع اشتراک اطلاعات مبتنی بر بخش خواهند بود، چرا که محدوده طبیعی برای منافع مشترک را فراهم می‌سازد. با این وجود، ممکن است اطلاعات به خوبی به اشتراک گذاشته شده توسط چنین جوامعی وجود داشته باشد که مورد نظر دیگر جوامع اشتراک اطلاعات تاسیس شده در بخش‌های دیگر باشد. در

---

[1] - Regulatory
[2] - Legal
[3] - Rule
[4] - Entity
[5] - Appoint
[6] - Trusted Information Communication Entity
[7] - Warning. Advice And Reprting Point

چنین مواردی، ممکن خواهد بود که ایجاد جوامع اشتراک اطلاعات از جوامع اشتراک اطلاعات، باز هم مبتنی بر برخی منافع مشترک مانند طبیعتِ اطلاعات به اشتراک گذاشته شده، باشد. به این مسأله به عنوان ارتباط بین‌بخشی اشاره می‌کنیم.

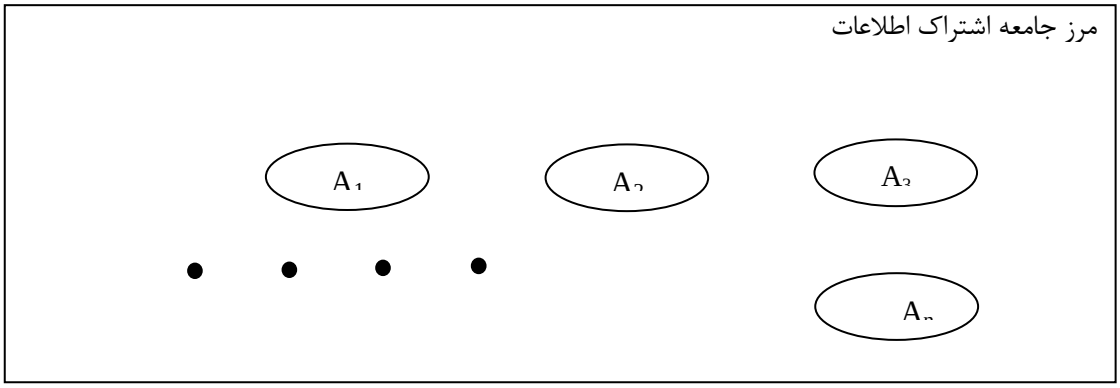
ارتباط بین‌بخشی در جایی که هستارهای پشتیبانی‌کننده درون هر جامعه اشتراک اطلاعات وجود دارد، بسیار تسهیل می‌شود، چراکه توافقات و واپایش‌های تبادل ضروری اطلاعات را می‌توان بین هستارهای پشتیبانی‌کننده، به جای تمامی اعضای تمامی جوامع، برقرار کرد. بعضی جوامع بین‌بخشی نیازمند گمنامی منبع یا سازمان‌های پذیرنده است؛ این امر همچنین از طریق استفاده از هستارهای پشتیبانی‌کننده قابل دستیابی است.

۴-۶ انطباق[1]

در برخی مواقع زمانی که استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴، برای جامعه اشتراک اطلاعات (یا ارتباطات بین‌بخشی و یا جامعه‌ای از جوامع) به کار می‌رود، نیاز به تفسیر خواهد داشت.

اولین ناحیه‌ای که در آن نیاز به تفسیر است، تعریف سازمان مورد نظر است.

استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴ نیازمند آن است که ISMS توسط سازمان برقرار، پیاده‌سازی، نگهداری شود و به طور مستمر بهبود داده شود (طبق بند ۴-۴، استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴). در این زمینه، سازمان مربوطه، جامعه اشتراک اطلاعات است. با این وجود، اعضای جامعه اشتراک اطلاعات، خودشان سازمان هستند- به شکل۱ مراجعه شود.



راهنما

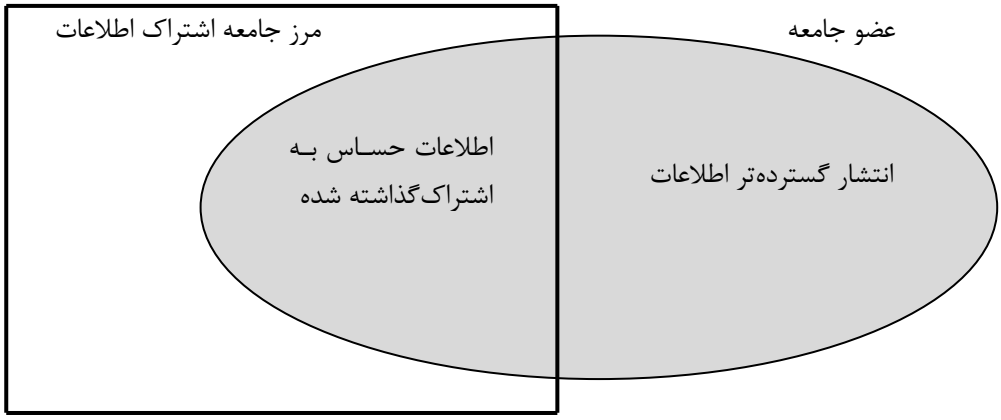
A_k سازمان عضو **k**ام از جامعه (**k=1 . . . n**)، شامل هر هستار پشتیبانی‌کننده.

شکل ۱- جوامع و سازمان‌ها

[1] - Conformity

دوم آن که، در بسیاری از جوامع اشتراک اطلاعات، همه افراد در سازمان‌های عضو اجازه دسترسی به اطلاعات حساس به اشتراک گذاشته شده بین اعضا را ندارند. در این حالت، قسمتی از سازمان عضو در محدوده ISMS جامعه خواهد بود و بخشی خارج آن خواهد بود. قسمت خارج از محدوده جامعه تنها به اطلاعاتی از جامعه دسترسی خواهد داشت که برای انتشار گسترده‌تری مشخص شده است- به شکل ۲ مراجعه شود.

ممکن است اعضای جامعه اشتراک اطلاعات، سامانه‌های مدیریت امنیت اطلاعات خود را داشته باشند، در نتیجه بعضی فرایندها ممکن است بین محدوده جامعه و سامانه‌های مدیریت اعضا قرار گیرد. در این حالت، کمینه یک احتمال نظری وجود دارد که ممکن است الزامات معارض و ناسازگار بین آن فرایندها وجود داشته باشد. این حالتی خواهد بود که حذف از محدوده ISMS اعضا توجیه‌پذیر خواهد بود به زیربند ۴-۳ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴، مراجعه شود.



شکل ۲- عضو ISMS به صورت جزئی در محدوده

هنگام تعریف فرایند ارزیابی مخاطره (بند ۶-۱-۲ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۱ : سال ۱۳۹۴)، جامعه اشتراک اطلاعات نیازمند آن خواهد بود تا تاثیرات مخرب مخاطرات را که ممکن است برای اعضای مختلف جامعه، متفاوت باشد، تشخیص دهد. بنابراین جامعه نیازمند انتخاب شیوه ارزیابی مخاطره است که بتواند تاثیرات غیریکنواخت را شبیه به معیار ارزیابی مخاطره[1] آن اداره کند.

۴-۷ الگوی ارتباطات

تبادل اطلاعات حساس همان‌گونه که در این استاندارد نیز پوشش داده شده، می‌تواند هر شکلی به خود بگیرند- نوشتاری، شفاهی یا الکترونیکی مشروط بر این که الزامات واپایش منتخب برآورده شود.
در ادامه این استاندارد، ارتباطات حساس فردی از نظر شرکت‌کنندگان ذیل توصیف می‌شود:

[1] - Risk assessment criteria

- *منبعِ قلم اطلاعاتی*[1]، شخص یا سازمانی است که قلم اطلاعات را می‌سازد؛ منبع نیازی به عضویت در جامعه ندارد.
- *ایجادکنندهٔ پیام* عضوی از جامعه اشتراک اطلاعات است که توزیع آن در جامعه را آغاز می‌کند. ایجادکنندهٔ پیام ممکن است اطلاعات را به طور مستقیم توزیع کند و یا آن را به منظور توزیع برای هستار پشتیبانی- کننده‌ای بفرستد. ایجادکنندهٔ پیام به طور احتمالی، ولی نه به طور الزامی، شبیه منبع اطلاعات است؛ ایجادکنندهٔ پیام ممکن است هویت منبع را مخفی نگه دارد. جوامع ممکن است تسهیلاتی فراهم سازند که هر عضو را قادر سازد تا هویت خود را به عنوان ایجادکنندهٔ پیام مخفی نگه دارند.
- *پذیرنده*، دریافت‌کننده اطلاعات توزیع شده در جامعه است. اگر اطلاعات برای توزیع گسترده در دسترس باشند، نیازی نیست پذیرنده‌ها عضو جامعه باشند. جوامع ممکن است تسهیلاتی فراهم سازند تا پذیرنده‌ها قادر به مخفی کردن هویت‌هایشان از ایجادکنندهٔ پیام اطلاعات باشند.

۵ خط‌مشی‌های امنیت اطلاعات

۵-۱ هدایت مدیریت برای امنیت اطلاعات

۵-۱-۱ خط‌مشی‌های امنیت اطلاعات

واپایش ۵-۱-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود خط‌مشی اشتراک اطلاعات چگونگی همکاری اعضا با یکدیگر را به منظور تنظیم خط‌مشی‌های مدیریت امنیت و هدایت جامعه اشتراک اطلاعات، تعریف کند. توصیه می‌شود این امر برای تمامی کارکنان درگیر با اشتراک اطلاعات در جامعه، در دسترس باشد.
توصیه می‌شود خط‌مشی اشتراک اطلاعات، علامت‌گذاری اطلاعات و قواعد توزیع مورد استفاده درون جامعه را تعریف کند.

۵-۱-۲ بازنگری خط‌مشی‌های امنیت اطلاعات

واپایش ۵-۱-۲ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

[1] - Item of information

توصیه می‌شود، بازنگری، شامل اطلاعاتی از تغییرات مهم برای عضویت جامعه اشتراک اطلاعات باشد.

۶ سازمان امنیت اطلاعات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۷ امنیت منابع انسانی

۷-۱ پیش از اشتغال

۷-۱-۱ گزینش

واپایش بند ۷-۱-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

احتمال آن بسیار کم است که قواعد گزینشی در میان تمامی اعضای جامعه اشتراک اطلاعات منطبق باشد، توصیه می‌شود جوامع تعریف کمینه سطوحی از بازبینی‌های درستی‌سنجی را برای اعمال به همه کارکنان یا پیمانکاران اعضا که اجازه دسترسی به اطلاعات به اشتراک گذاشته‌شده جامعه به آن‌ها داده خواهد شد، در نظر بگیرند.

۷-۱-۲ ضوابط و شرایط اشتغال

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۷-۲ در زمان اشتغال

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۷-۳ خاتمه و تغییر شغل

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸ مدیریت دارایی

۸-۱ مسئولیت دارایی‌ها

۸-۱-۱ فهرست دارایی‌ها

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۱-۲ مالکیت دارایی‌ها

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۱-۳ استفاده پسندیده[1] از دارایی‌ها

واپایش بند ۸-۱-۳ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

اطلاعات فراهم شده توسط دیگر اعضای جامعه اشتراک اطلاعات، دارایی است و توصیه می‌شود مطابق با هر قاعده‌ای که توسط جامعه اشتراک اطلاعات یا ایجادکنندهٔ پیام تنظیم شده است، حفاظت، استفاده و منتشر شود.

۸-۱-۴ بازگرداندن دارایی‌ها

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۲ طبقه‌بندی اطلاعات

۸-۲-۱ طبقه‌بندی اطلاعات

واپایش بند ۸-۲-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر اصلاح شده است:

واپایش

توصیه می‌شود اطلاعات از نظر الزامات قانونی، ارزش، اعتبار، اولویت، حیاتی بودن و حساسیت نسبت به افشا یا اصلاح غیر مجاز، طبقه‌بندی شوند.

راهنمای پیاده‌سازی

همانند معیارهای داده شده در استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، توصیه می‌شود اطلاعات از نظر اعتبار و اولویتشان طبقه‌بندی شود. رده‌بندی آن اعتبار و اولویت است. توصیه می‌شود، اعتبار از نظر شهرت منبع آن محتوای فنی و کیفیت توصیف ارزیابی شود. توصیه می‌شود، اولویت، نیاز به اقدام ضروری و فوری را نشان دهد، مانند توزیع بیشتر.

به همین ترتیب، حساسیت می‌تواند به بسیاری از جنبه‌های اطلاعات، فراتر از نیاز به حفظ محرمانگی بستگی داشته باشد، مانند تاثیر افشا یا پتانسیلِ نقض گمناميِ منبع آن.

1- Acceptable

توصیه می‌شود در تفسیرِ نشانه‌گذاری‌های طبقه‌بندی که توسط دیگر اعضای جامعه اشتراک اطلاعات تعیین شده است، توجه کرد.

مثال: یک کارخواه رایانامه[1] شناخته‌شده پیغامِ «لطفا با این پیام به عنوان پیامی محرمانه رفتار کنید» را نمایش می‌دهد زمانی که رایانامه‌های نمایشی قسمت سرآیند حساس به‌صورت «محرمانه شرکتی» (RFC 4021[1]) تنظیم شده باشد. در این مورد شفاف نیست که مقصودِ ایجادکنندهٔ پیام «محرمانه شرکتی» بوده (و پیام با خطا ارسال شده است) یا مقصودِ او «محرمانه برای شما، پذیرنده» بوده است.

۸-۲-۲ علامت‌گذاری اطلاعات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۲-۳ اداره کردن دارایی‌ها

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۳ اداره کردن رسانه‌های ذخیره‌سازی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۸-۴ حفاظت از تبادلات اطلاعات

هدفِ واپایشیِ افزون بر بند ۸، مدیریت دارایی، از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، به صورت زیر است:

هدف: حصول اطمینان از حفاظت کافی از مبادلات اطلاعات درون جامعه اشتراک اطلاعات است. توصیه می‌شود اطلاعات مبادله شده بین اعضای جامعه اشتراک اطلاعات به شیوه‌ای سازگار حفاظت شود، حتی اگر اعضا هستارهای مستقل یا قسمتی مستقل از هستارها باشند که ممکن است اطلاعات خود را به طریق مختلف علامت‌گذاری، توزیع و حفاظت کنند. در جایی که گمنامی درخواست شده باشد، توصیه می‌شود هرگونه اطلاعات که منبع تبادل اطلاعات را می‌شناساند، حذف شود. به همین ترتیب، توصیه می‌شود دریافت اطلاعات به اشتراک گذاشته شده بدون آشکار شدن هویت پذیرنده امکان‌پذیر باشد. توصیه می‌شود انتشار اطلاعات به اشتراک گذاشته شده در خارج از جامعه واپایش شود.

۸-۴-۱ انتشار اطلاعات

<u>واپایش</u>

توصیه می‌شود انتشار اطلاعات درون اعضای پذیرنده محدود و بر اساس نشانه‌گذاری از پیش تعریف‌شده انتشار که توسط جامعه تعریف شده است باشد.

1 - Email client

راهنمای پیاده‌سازی

توصیه می‌شود اطلاعاتی که هیچ‌گونه نشانه‌گذاری انتشار به آن‌ها منتسب نشده است، نشانه‌گذاری انتشار پیش‌فرض که توسط جامعه اشتراک اطلاعات تعریف‌شده است، به آن‌ها داده شود. اگر شکی وجود دارد، یا در مواقعی که هیچ‌گونه توافق کلی پذیرفته شده روی انتشار پیش‌فرض وجود ندارد، توصیه می‌شود با اطلاعات به صورت محافظه کارانه رفتار شود. در صورت امکان، توصیه می‌شود پذیرنده، انتقال مجدد را با نشانه‌گذاری صریح انتشار از ایجادکنندهٔ پیام درخواست کند.

محدودیت انتشار ممکن است شامل محدودیت در استفاده باشد: مانند واپایش رونوشت و چسباندن الکترونیکی، جلوگیری از گرفتن عکس از صفحه نمایش و یا جلوگیری از چاپ و برون‌بُرد[1].

اطلاعات دیگر

ممکن است ویژگی‌ها یا مولفه‌های مختلف اطلاعاتِ به اشتراک گذاشته‌شده، حساسیت‌های متفاوتی داشته باشد. به طور خاص، دانشِ وجود پیام و یا دیگر اطلاعات به اشتراک گذاشته‌شده ممکن است حساسیت‌های متفاوتی برای محتویات آن داشته باشد.

کارکرد مدیریت حقوق اطلاعات اغلب برای اعمال محدودیت‌های هنگامِ استفاده، استفاده می‌شود. در این صورت، الگو یا خط‌مشی روشن حقوق کاربر مورد نیاز است تا بدانند که سامانه اجازه انجام چه کاری را می‌دهد و در چه مواقعی آن‌ها را مسدود می‌کند.

۸-۴-۲ بیانیه‌های سلب مسئولیت اطلاعات

واپایش

توصیه می‌شود هر تبادل اطلاعات با بیانیه سلب مسئولیت آغاز شود، که این بیانیه هرگونه الزامات خاص را که لازم است گیرندگان افزون بر علامت‌گذاری عادی اطلاعات از آن‌ها پیروی کنند، فهرست می‌کند.

راهنمای پیاده‌سازی

توصیه می‌شود در صورتی که بیانیه سلب مسئولیت برای پذیرنده به طور کامل قابل فهم نیست یا نمی‌تواند پیاده‌سازی شود، پذیرنده از ایجادکنندهٔ پیام درخواست کند که آن را شفاف‌سازی کند.

۸-۴-۳ اعتبارپذیری اطلاعات

واپایش

توصیه می‌شود هر تبادل اطلاعات، درجه اعتماد ایجادکنندهٔ پیام از دقت و اعتبارپذیری اطلاعات منتقل شده را نشان دهد.

1 - Export

راهنمای پیاده‌سازی

بر اساس ضرورت، پیامدهای بالقوه و محدودیت‌های فنی، ممکن است اعتبارسنجیِ همه اطلاعات قبل از انتقال امکان‌پذیر نباشد. در مواقعی که محدودیت وجود داشته باشد، توصیه می‌شود این محدودیت‌ها عنوان قسمتی از پیام نشان داده شود.

نشان دادن ذخیره‌ها[1] در اعتبارپذیری اطلاعات در مواقعی که منبع گمنام و یا ناشناخته است، اهمیت ویژه‌ای دارد. همچنین مهم است که نشان داده شود چه مواقعی ایجادکنندهٔ پیام قادر بوده که مستقیما اطلاعات داده شده را اعتبارسنجی کند و می‌تواند صحت آن را تایید کند.

۸-۴-۴ کاهش حساسیت اطلاعات

واپایش

توصیه می‌شود ایجادکنندهٔ پیام تبادل اطلاعات، نشان دهد که آیا حساسیت اطلاعات عرضه‌شده پس از برخی از رویدادهای بیرونی، یا گذشت زمان کاهش می‌یابد.

راهنمای پیاده‌سازی

حتی اگر حساسیت اطلاعات عرضه شده با گذشت زمان کاهش می‌یابد، هنوز هم ممکن است نیاز به محافظت داشته باشد. ممکن است نیاز باشد که راهنمایی‌های رده‌بندی (به بند ۸-۲-۱ مراجعه شود)، برای کاهش حساسیت پیش‌فرض‌هایی را در بر گیرند.

۸-۴-۵ حفاظتِ منبع گمنام

واپایش

توصیه می‌شود در مواقعی که گمنام ماندن درخواست شده باشد، عضو جامعه در هر گونه ارتباط که آغاز یا دریافت می‌کند، هرگونه اطلاعات شناسایی منبع را از بین ببرد.

راهنمای پیاده‌سازی

ایجادکنندهٔ پیام اطلاعات مسئول دریافت تایید از منبع (اگر متفاوت باشد) قبل از ابلاغ اطلاعات به دیگر اعضای جامعه اشتراک اطلاعات است. همچنین توصیه می‌شود ایجادکنندهٔ پیام از منبع بپرسد که آیا می‌توان آن را به عنوان ارائه‌کننده اصلی اطلاعات شناخت.

این موضوع مهم است که فرایند محافظت منبع به محتوای پیام و همچنین به منشاء پیام نگاه می‌کند، چون تحلیل محتوا ممکن است هویت منبع را آشکار کند. در صورت امکان، توصیه می‌شود ایجادکنندهٔ پیام از منبع بخواهد تا اطلاعات گمنام‌شده و فهرست گیرندگان در نظر گرفته شده را قبل از توزیع بازنگری کند.

[1] - Reservations

مثال: پیامی مانند « امروز دستگاه‌های ATM ما غیرفعال بود، این به این دلیل بود که عامل ویروس جدیدی بود که به‌وسیله دیوارآتش ما آشکارسازی نشد، اما به‌وسیله کارسازِ خط‌مشی ما آشکارسازی شد»، می‌تواند منبع را آشکار کند، اگر در روز درخواست تنها یک بانک متحمل قطع خدمت عمومی شده باشد.

سازوکارهای فنی وجود دارد که می‌تواند بدون به خطر انداختن گمنامی، برای ارائه اعتبار استفاده شود. به عنوان مثال، اسرار رمزنگاشتی به اشتراک گذاشته شده می‌تواند برای تایید این که ارتباط، از طرف عضو جامعه آغاز شده است، استفاده شود و این امر بدون آشکار ساختن هویت واقعی ایجادکنندهٔ پیام باشد.

۸-۴-۶ حفاظت پذیرنده گمنام

واپایش

با تایید ایجادکنندهٔ پیام، توصیه می‌شود اعضای جامعه قادر به دریافت ارتباطات بدون آشکار ساختن هویت-های خود باشند.

راهنمای پیاده‌سازی

رسید گمنام می‌تواند از طریق وسیله فنی (برای مثال، رمزنگاری) و هم از طریق وسیله رویه‌ای (برای مثال، مسیریابی از طریق هستار پشتیبان) پیاده‌سازی شود. باید توجه داشت که اطمینان حاصل شود که گمنامی، محدودیت‌های قانونی را نقض نکند یا سطح کلی اعتماد درون جامعه را نکاهد.

رسید گمنام، اغلب برای ارتباطات بین سازمانی موثر است چون جوامعِ بخشی تمایل دارند که جزییات عضویت خود را خصوصی نگه دارند.

۸-۴-۷ اختیار انتشار بعدی

واپایش

توصیه می‌شود بدون تایید رسمی از طرف ایجادکنندهٔ پیام، اطلاعات فراتر از جامعه اشتراک اطلاعات توزیع نشود، مگر در مواردی که برای انتشار وسیع‌تر علامت‌گذاری شده باشد.

راهنمای پیاده‌سازی

توصیه می‌شود هر پذیرنده، مسئول به دست آوردن مجوزهای ضروری برای انتشار وسیع‌تر از ایجادکنندهٔ پیام، قبل از توزیع بعدی باشد.

در ارتباطات بین بخشی، ایجادکنندهٔ پیام نمی‌تواند تمامی سازمان‌هایی را که اطلاعات دریافت خواهند کرد، بداند. در چنین مواردی، لازم است تایید انتشار عمومی یا خاص بخش اعطا شود.

اطلاعات دیگر

پروتکل چراغ راهنمایی رانندگی (به پیوست پ مراجعه شود) اغلب استفاده می‌شود تا نشان دهد که چگونه

اطلاعات می‌توانند بدون طلب کردن تایید اضافی، توزیع شوند.

۹ واپایش دسترسی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۰ رمزنگاری

۱-۱۰ واپایش‌های رمزنگاشتی

۱-۱-۱۰ خط‌مشی استفاده از واپایش‌های رمزنگاشتی

واپایش بند ۱۰-۱-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

فنون رمزنگاشتی می‌توانند برای پیاده‌سازی قواعد انتشارِ اشتراک اطلاعات استفاده شوند، برای مثال، از طریق مدیریت حقوق اطلاعات.

۲-۱-۱۰ مدیریت کلید

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۱ امنیت فیزیکی و محیطی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲ امنیت عملیات

۱-۱۲ مسئولیت‌ها و روش‌های اجرایی عملیاتی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۲-۱۲ حفاظت در برابر بدافزار

۱-۲-۱۲ واپایش‌ها در برابر بدافزار

واپایش بند ۱۲-۲-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود اطلاعات دریافتی از دیگر اعضای جامعه اشتراک اطلاعات از جهت حضور بدافزار پویش شود، بدون در نظر گرفتن این که خدمت ارتباطاتی بین اعضای جامعه، پویش پیام را ارائه می‌کند یا خیر.

۱۲-۳ نسخه‌های پشتیبان

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۴ واقعه‌نگاری[1] و پایش

۱۲-۴-۱ واقعه‌نگاری رویداد

واپایش بند ۱۲-۴-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

زمانی که جامعه اشتراک اطلاعات لازم می‌داند، توصیه می‌شود اعضا انتشار داخلی اطلاعات به اشتراک گذاشته شده را ثبت کنند.

۱۲-۴-۲ حفاظت از اطلاعات ثبت‌شده وقایع

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۴-۳ ثبت وقایع سرپرست و کاروَر سامانه

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۴-۴ هم‌زمان‌سازی ساعت‌ها

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۵ واپایش نرم‌افزارهای عملیاتی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۶ مدیریت آسیب‌پذیری فنی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

[1] - Logging

۱۲-۷ ملاحظات ممیزی سامانه‌های اطلاعاتی

۱۲-۷-۱ واپایش‌های ممیزی سامانه‌های اطلاعاتی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۲-۷-۲ حقوق ممیزی جامعه[1]

واپایش افزون بر بند ۱۲-۷، ملاحظات ممیزی سامانه‌های اطلاعاتی، از استاندارد ملی ایران به شماره ایزو-آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت است:

واپایش

توصیه می‌شود هر جامعه اشتراک اطلاعات، حقوق اعضا را برای ممیزی سامانه‌های دیگر اعضا و هر ارائه‌کننده مورد اعتماد خدمت، مشخص کند.

راهنمای پیاده‌سازی

اختیار برای ممیزی سامانه‌های اعضا می‌تواند محدود به طرف سوم مورد اعتماد باشد، از قبیل، TICE یا WARP.

۱۳ امنیت ارتباطات

۱۳-۱ مدیریت امنیت شبکه

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۳-۲ انتقال اطلاعات

۱۳-۲-۱ خط‌مشی‌ها و روش‌های اجرایی انتقال اطلاعات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۳-۲-۲ توافق‌نامه‌های انتقال اطلاعات

واپایش بند ۱۳-۲-۲ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود تمامی جوامع اشتراک اطلاعات توافق‌نامه‌های انتقال اطلاعات را تعریف کنند و توصیه می‌شود

[1] - Community audit rights

تنها به اعضایی اجازه پیوستن به جامعه را بدهند که چنین توافق‌نامه‌هایی را امضا کرده و پذیرفته‌اند.

۱۳-۲-۳ پیام‌رسانی الکترونیکی

واپایش بند ۱۳-۲-۳ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود تمامی جوامع اشتراک اطلاعات قواعدی برای حفاظت اطلاعات در حین انتقال تعریف کنند و تنها به اعضایی اجازه پیوستن به جامعه بدهند که چنین قواعدی را پذیرفته و پیاده‌سازی کرده‌اند. توصیه می‌شود هر گونه هستار پشتیبانی‌کننده، چنین قواعدی را به صورت داخلی پیاده‌سازی کند.

توصیه می‌شود جوامع اشتراک اطلاعات، پیاده‌سازی سازوکارهای جایگزین برای اشتراک اطلاعات را در نظر داشته باشند که متکی بر پیام‌رسانی الکترونیکی نباشد و اعضا را قادر سازد که مشخص کنند پیام‌های خاص، از طریق چنین مسیرهایی توزیع می‌شود.

۱۳-۲-۴ توافق‌نامه‌های محرمانگی یا عدم افشاء

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۴ اکتساب، توسعه و نگهداری سامانه

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۵ ارتباط با تأمین‌کنندگان

۱۵-۱ امنیت اطلاعات در ارتباط با تأمین‌کنندگان

۱۵-۱-۱ خط‌مشی امنیت اطلاعات برای ارتباط با تأمین‌کنندگان

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۵-۱-۲ پرداختن به امنیت درون توافقنامه‌های تأمین‌کننده

واپایش بند ۱۵-۱-۲ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود تمامی اعضای جامعه در مورد هویت تمامی طرف‌های سوم درگیر در فراهم‌سازی خدمات

جامعه، آگاه شده باشند، برای مواردی که نسبت به طرف‌های خاص درگیر در اداره کردن اطلاعاتی که ارائه می‌کنند، اعتراضاتی دارند.

توصیه می‌شود توافق‌نامه‌ها با تامین‌کنندگان مرتبط با فراهم‌سازی خدمات جامعه، قادر سازد تا بازنگری‌ها و ممیزی‌های امنیتی خدمات خود را به طور منظم اجرا کنند.

۱۵-۱-۳ زنجیره تأمین فناوری اطلاعات و ارتباطات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۵-۲ مدیریت تحویل خدمت تأمین‌کننده

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۶ مدیریت رخداد امنیت اطلاعات

۱۶-۱ مدیریت رخدادهای امنیت اطلاعات و بهبودها

۱۶-۱-۱ مسئولیت‌ها و روش‌های اجرایی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۶-۱-۲ گزارش‌دهی رویدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۲ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود اعضای جامعه اشتراک اطلاعات درنظر داشته باشند که آیا رویدادهای شناسایی شده بهتر است به اعضای دیگر جامعه گزارش شوند. توصیه می‌شود جامعه برای انواع رخدادی که مورد علاقه اعضای دیگر خواهند بود توافق کرده و راهنما منتشر کند. توصیه می‌شود، اعضا برای اطمینان از این که تنها رویدادهای به طور بالقوه مورد علاقه اعضای دیگر گزارش می‌شود از قضاوت بهره گیرند.

به منظور حفاظت از شهرت ایجادکنندهٔ پیام، گرایش فراوان برای محرمانه نگه داشتن رخدادها و فاش نکردن اطلاعات رخداد از طریق عضو جامعه وجود دارد. با این وجود، انتقال اطلاعات رخداد به دیگران، همکاری و هماهنگی آتی در پیشگیری رخداد را تقویت خواهد کرد، موجب واکنش سریع به رخدادها شده و امنیت کلی در داخل جامعه را بهبود خواهد بخشید. رویدادها و رخدادها می‌توانند بدون نیاز به آشکارسازی تمامی پیامدهایشان گزارش شوند.

همچنین بهتر است، اعضا تمام رویدادهای گزارش شده را بی‌درنگ بررسی کنند تا دریابند که آیا آن‌ها

تاثیری بر عملیات خودشان دارند. برای مثال، یک اعلام روزمره به وسیله یک عضو تامین‌کننده خدمتی به - اشتراک گذاشته‌شده از یک عملیات نگهداری طرح‌ریزی شده ممکن است اعضای دیگر را ملزم سازد که اطمینان‌پذیری تامین‌کنندگان جایگزین را قبل از شروع فعالیت نگهداری، بازنگری کنند.

۱۶-۱-۳ گزارش‌دهی ضعف‌های امنیتی

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۶-۱-۴ ارزیابی و تصمیم برای رویدادهای امنیت اطلاعات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۶-۱-۵ پاسخ به رخدادهای امنیت اطلاعات

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۶-۱-۶ یادگیری از رخدادهای امنیت اطلاعات

واپایش بند ۱۶-۱-۶ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲: سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود بررسی‌ها بر اساس اطلاعات توزیع شده توسط جامعه اشتراک اطلاعات انجام شود، تا مخاطرات ناشی از رخدادهای مشابه را کاهش دهد و فهم بهتری از مخاطرات پیش روی جامعه و هر زیرساخت اطلاعاتی مهم مربوط را ایجاد کند. این‌گونه بررسی‌ها می‌تواند از طریق اعضای درگیر جامعه و یا توسط یک هستار حمایتی، در صورت وجود، انجام شود.

توصیه می‌شود پیروِ رخدادهای گزارش شده، بازنگری‌های بعدی رخداد توسط اعضای جامعه اشتراک اطلاعات انجام شود تا به‌روز رسانی‌های طرح‌های پاسخ به رخداد امنیت، رویه‌های مربوطه و رخ‌نمون مخاطره کسب‌وکار را چکانش[1] کند، حتی اگر عضو تحت تاثیر رخداد مورد نظر نباشد. توصیه می‌شود هر عضو اطمینان حاصل کند که پاسخ‌ها به رخداد امنیت ارزیابی می‌شود و هر گونه درس و یا بهبود ممکن برای فرایندهای آن عضو شناسایی شده و به آن‌ها عمل می‌شود تا فرایندهای پاسخ خود را به طور مداوم بهبود بخشد.

۱۶-۱-۷ جمع‌آوری شواهد

برای ارتباطات بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

1 - Trigger

۱۶-۱-۸ سامانه اعلام هشدار اولیه

واپایشی افزون بر بند ۱۶-۱، استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، ۱۳-۱، مدیریت رخدادهای امنیت اطلاعات و بهبودها، به صورت زیر است:

واپایش

سامانه اعلام هشدار اولیه بهتر است در داخل جامعه اشتراک اطلاعات استقرار یابد تا اطلاعات اولویت‌دار را به محض این که در دسترس قرار گرفتند، به گونه‌ای اثربخش منتقل کند.

راهنمای پیاده‌سازی

اطلاعات اولویت‌دار، اطلاعاتی هستند که ممکن است اعضای دیگر جامعه را قادر سازند که رویدادهای ناخوشایند مشابه را کم یا از آن‌ها جلوگیری کنند. مهم است که چنین اطلاعاتی فوری به اشتراک گذاشته - شوند، حتی اگر کاملا تحلیل یا تایید نشده باشند.

۱۷ جنبه‌های امنیت اطلاعات مدیریت تداوم کسب‌وکار

۱۷-۱ تداوم امنیت اطلاعات

۱۷-۱-۱ طرح‌ریزی تداوم امنیت اطلاعات

واپایش بند ۱۷-۱-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

توصیه می‌شود طرح‌های تداوم کسب‌وکار بازیابی از فاجعه که به وسیله اعضای جامعه اشتراک اطلاعات تدوین شده است، به نیاز برای تبادل اطلاعات حساس به طور امن با دیگر اعضا، به عنوان قسمتی از فرایند بازیابی بپردازد.

۱۷-۱-۲ پیاده‌سازی تداوم امنیت اطلاعات

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۷-۱-۳ درستی‌سنجی، بازنگری و ارزشیابی تداوم امنیت اطلاعات

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۷-۲ افزونگی‌ها

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۱۸ انطباق

۱-۱۸ انطباق با الزامات قانونی و قراردادی

۱-۱-۱۸ شناسایی الزامات قانونی و قراردادی قابل‌اجرا

واپایش بند ۱۸-۱-۱ از استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ به صورت زیر افزوده شده است:

راهنمای پیاده‌سازی

بهتر است جامعه اشتراک اطلاعات هرگونه توافقات، قوانین، مقررات مرتبط با اشتراک اطلاعات، مانند قوانین و مقررات ضد-کارتل [۱]، را به خوبی در نظر بگیرد. این مورد می‌تواند از پیوستن سازمان‌های معین به جامعه، یا محدودسازی‌های مکانی بر نمایندگی آن‌ها پیشگیری کند.

۲-۱-۱۸ حقوق دارایی فکری [۲]

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۳-۱-۱۸ حفاظت از سوابق

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۴-۱-۱۸ حریم خصوصی و حفاظت از اطلاعات شخصی قابل‌شناسایی

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۵-۱-۱۸ مقررات واپایش‌های رمزنگاشتی [۳]

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

۶-۱-۱۸ تعهد به جامعه اشتراک اطلاعات

واپایش افزون بر استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴، بند ۱۸-۱ انطباق با الزامات قانونی و قراردادی، به صورت زیر است:

واپایش

بهتر است مسائل الزامی و روش حل‌وفصل [۴] به وسیله تمامی اعضای جامعه اشتراک اطلاعات روشن، درک و

۱- ضد اتحادیه شرکت‌های تولید و عرضه‌کننده کالا که به منظور قبضه کردن بازار کشور یا حتی جهان قیمت‌ها را به میل خود تعیین می‌کنند، عمل می‌کند.

[2] - Intellectual Property Rights

[3] - Regulation of cryptographic controls

[4] - Remediation

اثبات شوند تا به موقعیت‌هایی که در آن‌ها اطلاعات به طور عمدی یا سهوی فاش شوند، پرداخته شود.

راهنمای پیاده‌سازی

روش حل‌وفصل بهتر است کمینه شامل اطلاع هر گونه افشای مجاز نشده به ایجادکنندهٔ پیام با جزئیات کافی، برای شناسایی اطلاعات فاش شده باشد.

در مواقعی که امکان‌پذیر است، بهتر است اطلاع‌رسانی به منبع ارائه شود، حتی اگر اطلاعات تصدیق شده و اصل خود را آشکار نمی‌سازد. این می‌تواند به وسیله وساطت طرف سوم مورد اعتمادی، مانند یک TICE ، به دست آید. پیامدهای افشای غیرمجاز می‌تواند به طور مستقیم طرف‌های مسئول را تحت تاثیر قرار داده و به طور احتمالی موجب حذف یا محدودسازی دسترسی بعضی اعضا برای چند دوره زمانی، به منظور برقراری مجدد اعتماد جامعه، خواهد شد.

۱۸-۲ بازنگری‌های امنیت اطلاعات

برای جوامع بین‌بخشی و بین‌سازمانی اطلاعات افزوده مشخصی وجود ندارد.

پیوست الف

(آگاهی‌دهنده)

اشتراک اطلاعات حساس

الف-۱ مقدمه

اطلاعات حساس، دارایی‌های با ارزش بسیار مهم هستند که باید زمانی که بین سازمان‌ها به اشتراک گذاشته می‌شوند، به صورت امن مدیریت گردند. این اطلاعات چنانچه برای سازمان حیاتی باشند باید به موقع برای پرداختن به مسائل کسب‌وکار و اتخاذ تصمیمات بهتر و حتی بیشتر از آن تحویل گردند.

جوامع اشتراک اطلاعات ممکن است نمایندهٔ انواع بسیاری از سازمان‌ها و حتی افراد باشند. جوامع ممکن است از نظر عضویتشان فوق‌العاده متنوع باشند، یا به شکلی از فعالیت کسب‌وکار، از قبیل یک صفت یا بخش بازار خاص، بسیار نزدیک تراز شوند. جوامع ممکن است در هر دو بخش عمومی و حریم خصوصی قرار گیرند یا ممکن است شامل اعضای هر دو نوع باشند. الزامات، تمایلات مشترکی هستند برای به اشتراک گذاشتن برخی از گونه‌های حساس اطلاعات و پذیرش واپایش‌ها و فرایندهای اداره‌کننده استفاده از آن اطلاعات است.

برای تبادلِ امنِ اطلاعات حساس در داخل جامعه اشتراک اطلاعات، ضروری است که فرایندهایی برای تامین جریان امن اطلاعات بر پایهٔ زمان، طراحی، پیاده‌سازی و پایش شود. فرایندها بهتر است اطمینان یابند که اطلاعات بین افراد مقتضی پخش شده است، در جایی که اطمینان معقولی فراهم می‌سازند که اطلاعات نمی‌توانند برای اهداف مورد استفاده قرار گیرند و برای آن که به طور ضروری اطلاعات عمومی شوند، به طور تصادفی دوباره توزیع شده نیستند.

اثربخشیِ توزیع به وسیله درجه اطمینان که اعضا در ارتباطاتِ برقرارشده از طریق جامعه اشتراک اطلاعات برخوردارند، تعیین می‌شود. هم‌زمان، سازوکارهای امنیتی مرتبط با ارتباطات بهتر است از توزیع اطلاعات به افراد یا سازمان‌هایی مانند زیر جلوگیری کنند:

- استفاده یا انباشتن داده برای انجام فعالیت‌های مخرب؛
- پخش عمومی اطلاعات بدون اجازه از ایجادکنندهٔ پیام اطلاعات؛
- تامین اطلاعاتی که به اندازه کافی تحلیل نشده‌اند و بنابراین موجب فعالیت‌های نامناسبی که می‌تواند منابع و تاثیر بر سازمان‌ها را اتلاف کرده یا منحرف سازند.

برای آن که عملکرد جوامع اشتراک اطلاعات به گونه‌ای اثربخش باشد، پذیرنده‌های اطلاعات باید به وسیله سازمان‌های عضوشان برای استفاده از اطلاعات دریافتی، تقویت شوند و نباید برای سوء استفاده از آن اطلاعات، برای مثال منفعت تجاری، تشویق شوند.

الف-۲ چالش‌ها

برای مواجهه با چالش‌های زیر، توصیه اکید می‌شود که مدیریت امنیت اطلاعات کافی برای ارتباطات بین-بخشی و بین‌سازمانی باشد؛ شکست در انجام این کار می‌تواند شرایط عادیِ کسب‌وکار را تحت تاثیر قرار دهد و موجب اختلال در طول رخدادها شود:

- تهدیدهای و آسیب‌پذیری‌های امنیتی جدید
- وابستگی‌های رو به افزایش سامانه و شبکه
- تحول و محدودیت‌های کسب‌وکاری، پیمانی، قانونی و مقرراتی
- ایجاد الگوهای ارتباطی کافی
- هماهنگی فرایندهای حمله و واکنش
- حاکمیت مداوم

ارتباطات امن و مقاوم بین اعضای جامعه بهتر است شامل عناصر زیر باشد:

- دانش و مدیریت مخاطره
- اشاعه[1] و ارتباط
- پایش

در حالی که این سه عنصر بهتر است برای ارزش مشخص خودشان در نظر گرفته شوند، آن‌ها به صورتی نزدیک هم مرتبط به هم و مکمل یکدیگر هستند. ایجاد امنیت بین اعضای جامعه اشتراک اطلاعات بدون روابط فردی با نمایندگان دیگر اعضا، مشکل است. مردم برای ساختن روابط و ایجاد اطمینان در اعتبار و اختیار یکدیگر، نیاز به ملاقات رو در رو دارند. خلق اعتماد تنها با استفاده از فناوری‌های ارتباط از راه دور مشکل است .همچنین برقراری سازوکارهایی که اطمینانی به اعتبار منبع اطلاعات می‌دهند، در حالی که گمنامی آن منبع را حفظ می‌کنند، مشکل است.

مردم اغلب اگر اطمینان داشته باشند که هویت آن‌ها محرمانه خواهد بود، آزادانه‌تر صحبت می‌کنند. جامعه

اشتراک اطلاعاتی می‌تواند اثربخش باشد، حتی اگر تمامی اعضای کلیدی اطلاعات خود را با تمام دیگر اعضا به اشتراک نگذارند. سازوکارهای توزیع باید به اندازه کافی منعطف باشند تا توزیع بتواند به اعضای مشخصی از جامعه و یا بر اساس موضوع ، محدود شود.

سرانجام، هنگام اشتراک اطلاعات بین جوامع)برای مثال در جوامع بین‌بخشی(درگاه‌بان‌های میان جوامع با مشکلات خاصی مواجه می‌شوند. منابع اطلاعاتی به طور ضروری دانش عضویت جوامع دیگر را ندارند و باید برای حفاظت از گمنامی و دیگر شرایط انتشار، متکی بر رابط‌ها باشند. درگاه‌بان‌ها ممکن است فاقد دانش

[1] - Dissemination

تخصصی برای تشخیص آن باشند که چه زمانی ارتباطات اجتماعی قطعی نباید بیش از این برقرار باشد. این مشکلات به طور معمول حتی در ارتباطات بین‌المللی بدتر از ارتباطات بین‌بخشی است.

الف-۳ منافع بالقوه

اشتراک اطلاعات حساس با دیگران، مخاطره بالقوه افشاگری نامناسب را به گونه‌ای اجتناب‌ناپذیر افزایش می‌دهد. به منظور اثربخشی جامعه، این مخاطرات باید مدیریت و کمینه شوند و منافع بر مخاطرات پذیرفته‌شده باقیمانده رجحان داده شوند.

منافع احتمالی اشتراک اطلاعات حساس عبارتند از:

- اعلام هشدار اولیه هر تغییر قابل ملاحظه در موقعیت مخاطره، مانند تهدیدهای جدید، احتمال به روز شده حمله، آسیب‌پذیرهای تازه کشف شده و غیره.
- بهبود امنیت از طریق بهترین عمل به اشتراک گذاشته شده
- ارزیابی اطلاعات مفیدی که از هر منبع عمومی در دسترس نباشد
- صرفه‌جویی‌های هزینه از طریق حذف تلاش تکراری
- ارزیابی‌های مخاطره بهتر، از طریق درک بیشتر از تهدیدها و آسیب‌پذیری‌ها
- سازمان‌دهی بهتر نگهداری و مداخله در اطلاعات درباره فعالیت‌های مشابه در سازمان‌های دیگر
- آمادگی بهتر برای رخدادهای امنیتی
- محک‌زنی سنجه‌های امنیتی علیه سازمان‌های مشابه
- مسئولیت اجتماعی شرکت
- انطباق با الزامات قانونی یا حقوقی‌سازی خط‌مشی

ضروری است که پایش جامعه و بازنگری فرایندها، منافع (و معایب) ملموسی را از عضویت جامعه، برای استفاده به وسیله اعضا در ارزیابی عضویت مداوم آن‌ها در جامعه شناسایی کند.

الف-۴ کاربردپذیری

اطلاعات می‌توانند بین انواع بسیاری از سازمان‌ها تبادل شوند، بزرگ یا کوچک، دولتی یا خصوصی، همسان یا متنوع. با این وجود، بزرگ‌ترین منافع، ممکن است اغلب به وسیله سازمان‌هایی کسب شود که در داخل بخش یکسان یا با اهداف حقوقی یکسان عمل می‌کنند که دسته‌های بخش مشخصی از مخاطره امنیت اطلاعات را به اشتراک می‌گذارند. استاندارد ISO/IEC 27006 [1] چنین بخش‌هایی را شناسایی می‌کند.

۱ـ استاندارد ملی ایران به شماره ۲۷۰۰۶: سال ۱۳۹۶، فناوری اطلاعات– فنون امنیتی– الزامات برای نهادهای ممیزی و صدور گواهینامه سامانه‌های مدیریت امنیت اطلاعات، با منبع ISO/IEC 27006: 2015 تدوین شده است.

همچنین ممکن است منافع بزرگی در اشتراک اطلاعات میان بخش‌ها یا به وسیله تعریف جوامع بر اساس دیگر خصوصیات (مانند مکان جغرافیایی) یا به وسیله اشتراک اطلاعات با دیگر جوامع اشتراک اطلاعات مبتنی بر بخش در یک ساختار سلسله مراتبی از جوامع، وجود داشته باشد.

الف-۵ تعریف و عملیاتی کردن یک جامعه اشتراک اطلاعات

جامعه اشتراک اطلاعات بهتر است قوانین و شرایطی را تعریف کند که عملیات آن را اداره کنند. چنین قوانین و شرایطی بهتر است شامل موارد زیر باشند:

- قوانین و شرایط اداره‌کننده عضویت جامعه اشتراک اطلاعات و سازمان داخلی آن
- اهداف جامعه اشتراک اطلاعات و منافع مورد نظر برای اعضا
- رویه‌ها برای اعضایی که به جامعه اشتراک اطلاعات پیوسته یا آن را ترک کردند
- قوانین و شرایط اداره‌کننده هر گونه فرایند جامعه متمرکز یا هستارهایی از قبیل TICE یا WARP
- قوانین و شرایط در خصوص تعهدات اعضای جامعه ، فرایندها و معیارهای انضباطی و اخراجی
- قوانین واضح برای آنکه چگونه اعضا ممکن است اطلاعات به اشتراک گذاشته شده را استفاده یا عبور دهند
- دیگر تعهدات قانونی و مالی و شرایط عضویت جامعه

همچنین قوانین و شرایط جامعه اشتراک اطلاعات بهتر است:

- اطمینان یابند که اطلاعات به روش امن و کارا منتقل می‌شوند تا اطمینان یابند مخاطبان هدف آن به‌درستی و در زمان مناسب داده را دریافت می‌کنند.
- کانال‌های ارتباطی انتخابی و احتمالی را از نظر اولویت استفاده برای انتقال داده به هر نوع اطلاعاتی شناسایی شده مشخص و اولویت‌بندی کنند.
- شرایط مجازی که تحت آن‌ها اطلاعات به اعضای جامعه فرستاده می‌شود را مشخص کنند.
- حفاظت داده اختیاری و اجباری و صفات توزیع مرتبط با ارتباطات جامعه را مشخص کنند.
- قوانین واضحی برای تفسیر حفاظت داده و صفات توزیع راجع به اشاعه اطلاعات را مشخص کنند.
- اعضا را ملزم سازند تا بازخوردی بر اساس روابط داشتن، به موقع بودن و درستی اطلاعات دریافتی فراهم سازند.
- آنجا که امکان‌پذیر است، استانداردهای پیام‌رسانی موجود را برای تبادل اطلاعات شخصی و سازگار سازند.

قواعد ارتباطی باید بسامد ارتباط، هرگونه الزاماتی برای تایید پذیرنده و هرگونه اولویت یا معیار صعود را تعریف

کنند. قوانین بهتر است تشخیص دهند که اعضای جامعه اشتراک اطلاعات ممکن است سطوح متغیری از اعتماد در دیگر اعضای جامعه داشته باشند. درجه اعتماد ممکن است در طول زمان و بسته به موقعیت متغیر باشد.

کانال‌های ارتباطی مناسب بهتر است به وسیله ارزیابی نقاط قوت و ضعف آن‌ها زمانی که انواع اطلاعات شناسایی شده را بر اساس معیارهایی از قبیل مخاطبان هدف ، صفات اطلاعات برای تحویل شدن، وسعت و بسامد کانال و هزینه تحویل می‌دهند، انتخاب شوند. مثال‌های کانال‌های ارتباطی احتمالی، پیام‌رسانی الکترونیکی، جایگاه‌های عمومی یا مختص اعضاء اجلاس یا تماس‌های تلفنی دوطرفه، نامه‌های فرستاده شده به وسیله خدمات پست عمومی یا ملاقات رو در رو هستند. تاثیری که یک ارتباط بر روی مخاطبان هدف خود دارد، به اثربخشی کانال در رسیدن به مخاطب، اعتبار آن برای مخاطبان و تناسب آن با موضوع اطلاعات یا مساله بستگی دارد.

تمامی اطلاعات نیاز نیست که بی‌درنگ منتقل شوند؛ خیلی خوب است که بعضی اطلاعات از طریق تماس روزمره به اشتراک گذاشته شوند.

مثال‌های احتمالی از این که چه زمانی اطلاعات برای اعضای جامعه فرستاده می‌شوند، شامل گزارش دهی فوری رخدادهای تشخیص داده شده متناسب با رخنمون‌های از پیش تعریف شده، گزارش‌دهی روزمره براساس زمان، یا پاسخگویی به درخواست‌ها برای اطلاعات از دیگر اعضا هستند. مثال‌های احتمالی از حفاظت داده و صفات توزیع، یک نیازی برای پنهان کردن اصل اطلاعات، حساسیت اطلاعات یا ارزیابی ایجادکنندهٔ پیام از قابلیت اعتماد اطلاعات هستند. یک مثال از مجموعه‌ای از قوانین برای تفسیر حفاظت داده و صفات توزیع، پروتکل چراغ راهنمایی رانندگی است به پیوست پ مراجعه شود. صفات ممکن است بسته به کانال ارتباطی متغیر باشند. برای مثال، صفات اجباری برای توزیع پستی ممکن است از رایانامه متفاوت باشد.

هر آنچه از راه‌حل‌های فنی انتخاب و پیاده‌سازی شوند، بهتر است برای انواع اطلاعات به اشتراک گذاشته شده در داخل جامعه مناسب و با اهداف تعریف شده جامعه سازگار باشند. تماس رو در رو اعتماد می‌سازد و ممکن است یک راه ضروری برای رشد جوامع به وسیله دعوت از اعضای جدید باشد. با این حال وجود یک بستر یا زیرساخت اشتراکی دیگر مورد اعتماد ممکن است خود تشویقی برای عضویت باشد.

الف-۶ توافقات تبادل اطلاعات

جامعه اشتراک اطلاعات بهتر است در یک توافق تبادل اطلاعات، سازوکارها و فرایندها اداره‌کننده ارتباطات جامعه را تعریف کنند. اطلاعات می‌توانند به وسیله نامه، یا به صورت شفاهی در ملاقات‌های رو در رو و همچنین الکترونیکی تبادل شوند. اطلاعات می‌توانند به صورت رسمی و یا با استفاده از قالب‌ها و قراردادهای از پیش تعریف شده یا به صورت غیررسمی و به طریق غیرساختار یافته، تبادل شوند. اطلاعات می‌توانند براساس معمولی یا ویژه تبادل شوند. اطلاعات می‌توانند به وسیله ارتباطات نظیر به نظیر، به صورت سلسله مراتبی یا از طریق یک هستار پشتیبانی‌کننده متمرکز از قبیل یک TICE یا یک WARP تبادل شوند. توافق تبادل

اطلاعات ممکن است به اطلاعات اجازه دهد تا تنها بین اعضای انتخاب شده جامعه اشتراک اطلاعات به اشتراک گذاشته شوند یا تنها به صورت گمنام به اشتراک گذاشته شوند. همچنین حتی وقتی تسهیلات گزارش‌دهی متمرکز وجود دارد. ممکن است اطلاعات اجازه یابند مستقیم در بین اعضا عبور داده شوند.

توافق تبادل اطلاعات بهتر است انواع اطلاعاتی که ممکن است بین اعضای جامعه تبادل شوند را مشخص کند تا از درکی مشترک میان اعضای جامعه اطلاعات منتقل شده و این که اعضا سنجه‌های امنیتی مناسبی برای سطح حساسیت اطلاعات به اشتراک گذاشته شده طراحی و پیاده‌سازی می‌کنند، اطمینان یابند.

مثال‌های انواع احتمالی اطلاعات به صورت زیر هستند:

- «اعلامیه[1]ها» متناظر با رویدادهای توضیح داده شده اطلاعاتی؛
- «هشدارها و اخطارها» متناظر با رویدادهای توضیح داده نشده فیزیکی یا مرتبط با فناوری اطلاعات، حمله‌های انکار خدمت، پویش[2] و تقلید[3]؛
- «اداره کردن رخداد[4]» متناظر با تحلیلی، پشتیبانی و هماهنگی پاسخ مرتبط با رخدادهای واقعی؛
- «درخواست‌های اطلاعاتی» متناظر با درخواست‌هایی برای اطلاعات از یک عضو جامعه‌ای که به همه یا بعضی اعضای دیگر جامعه می‌پردازد؛
- « پیش‌بینی‌هایِ کیفیت خدمات[5]» که اطلاعاتی برای اثربخشی و اطمینان‌پذیری پیش‌بینی شده کانال‌های گوناگون ارتباطات جامعه فراهم می‌سازد.

اشتراک بیش از اندازه اطلاعات می‌تواند به همان اندازه بد باشد که اشتراک کم آن است، مگر آنکه روشی مناسب از پالایش داده را شامل شود. اگر ساخت اطلاعات روند به عنوان اصلی‌ترین مزیت اشتراک باشد، باید روشی برای تفاوت قائل شدن بین اطلاعات اولویت بالا «اکنون اقدام شود» از اطلاعات اولویت پایین «برای ثبت[6]»، وجود داشته باشد.

الف-۷ عوامل موفقیت

اگر چه تمامی اعضا ممکن است به تمامی جنبه‌های علاقه‌مند نباشند، جوامع اثربخش منافع مشترک خالصی خواهند داشت. به عنوان مثال، شرکت‌های ارتباطات راه دور خطوط ثابت به مشکلات بی‌سیم علاقه‌ای نخواهند داشت. اما به اندازه شرکت‌های ارتباط سیار به شناسایی مزاحمت‌های تلفنی علاقه‌مند هستند.

اعضایِ جوامع اثربخش از نمایندگی‌های صاحب‌اختیار، استفاده خواهند کرد که می‌توانند کارها را به صورت داخلی انجام دهد.

---

[1] - Announcement
[2] - Scanning
[3] - Spoofing
[4] - Incident handling
[5] - Quality of service predictions
[6] - For the record

جوامع اثربخش ممکن است عضویت را محدود یا مقید سازند، به عنوان مثال برای اطمینان از نمایش عادلانه در تصمیم‌گیری.

الف-۸ گستره ISMS برای جامعه اشتراک اطلاعات

محدوده ISMS برای جامعه اشتراک اطلاعات بهتر است شامل موارد زیر باشند:

- تمامی فرایندهای مورد استفاده برای ارتباط اطلاعات بین اعضای جامعه، شامل واسطه‌ها
- ذخیره اطلاعات درست در طول ارتباط
- فرایندهای پیاده‌سازی شده به وسیله اعضای مرتبط برای فرستادن و دریافت اطلاعات
- فرایندهای پیاده‌سازی شده به وسیله اعضای جامعه برای تخریب اطلاعات به اشتراک گذاشته شده

توصیه نمی‌شود محدوده شامل فرایندهای مدیریت امنیت اطلاعات باشد، جدا از محدودسازی‌های واقع بر طبیعت اطلاعات برای اشتراک گذاشتن و رابطه‌ها برای سامانه اشتراک اطلاعات، چه به وسیله اعضای مرتبط جامعه به منظور مدیریت امنیت اطلاعات خودشان پیاده‌سازی شده باشد و یا به وسیله دیگر سامانه‌های مدیریت امنیت اطلاعات پوشش داده شده باشد.

سامانه مدیریت امنیت اطلاعات (ISMS) می‌تواند به وسیله یک هستار پشتیبانی‌کننده مانند TICE یا WARP به صورت مرکزی مدیریت شود و یا می‌تواند به وسیله اعضای جامعه به وسیله گروهی مدیریت شود.

پیوست ب

(آگاهی‌دهنده)

برقراری اعتماد در تبادلات اطلاعات

ب-۱ بیانیه اعتماد

درجه اعتماد پذیرنده در بیانیه دریافتی به طور عمده براساس درجه‌ای که منبع پیام مورد اعتماد است و اعتماد خود منبع در بیانیه پیش‌بینی می‌شود. این مهم شاید به بهترین نحو در الگوی «۵ در ۵» مورد استفاده در داخل اعمال قانون و جوامع هوشمند پوشینه‌سازی شده است:

- {A-E} درجه کاهشی[1] اعتماد در منبع؛
- { 1-5 } درجه کاهشی اعتماد که توسط منبع در اطلاعات قرار داده شده است؛

بنابراین انتظار می‌رود اطلاعات «A-1» به صورت ضمنی مورد اعتماد باشند. در حالی که اطلاعات «E-5» به طور معمول دور ریخته خواهند شد.

اما در حقیقت در دنیای واقعی اطلاعات «A-1» بسیار کم هستند. شاید بهترین مثال شناخته شده آنجا باشد که هم منبع هم اطلاعات به صورت ضمنی مورد اعتماد باشند، اما چیزی که برای آن خطاهای اتفاقی باید مورد انتظار باشند. استفاده از سامانه موقعیت‌یاب جهانی (GPS) [2] بر اساس سامانه‌های ناوش ماهوارهای آنجا که نمونه‌های نگاشت یا خطاهای سامانه طرح‌ریزی مسیر به صورت تصادفی منحرف شده‌اند که سبب می‌شود وسایل انتقال بزرگ مسیرهای کوتاه که اغلب موارد تغییردهنده فضای جدی در مطبوعات هستند، را به اشتباه بیندازند.

مساله بعدی با توجه به اعتماد در بیانیه، مخاطرهٔ خوش‌ظاهر بودن است. گرایش درونی یا فرضیه نهفته، وجود دارد که چندین نمونه اطلاعات از منابع به ظاهر متفاوت تاییدبخش است.

این مساله از بعضی جهات در واقع درست است. اما چنین اعتمادی نباید بسیار دقیق در نظر گرفته شود و به خصوص توصیه نمی‌شود هرگونه الگوی ریاضی، چنین اعتمادی نمونه‌های افزوده را بر وزن‌دهی خطی نسبت دهد.

ب-۲ پشتیبانی فنی

ب-۲-۱ مقدمه

به تازگی برای پشتیبانی از اعتماد در اطلاعات ذخیره شده به صورت الکترونیکی که به وسیله هستارهای ناشناخته و ناآشنا ساخته شده‌اند، فناوری‌های متعددی ایجاد شده است.

[1] - Decreasing degree
[2] - Global Positioning System

چنین فناوری‌های بسیار مرتبط با مفهوم «Web 2.0» هستند. مفهوم Web 2.0 مجموعه‌ای از فناوری‌ها نیست، بلکه فلسفه یا مفهومی است که مرتبط با رسانه‌های جمعی است و شامل ایده‌هایی همچون استفاده از وب به عنوان بستر است که هوش جمعی، محتوای تولید شده توسط کاربر، استفاده اجتماعی از وب و غیره را به خدمت گرفته است.

دو جنبه از Web 2.0 به صورت خاصی با این استاندارد مرتبط هستند:

- شبه گمنامی؛
- سامانه‌های شهرت، موتورهای شهرت نیز نامیده می‌شوند.

ب-۲-۲ گمنامی و شبه گمنامی

منابع و پذیرنده‌های اطلاعات ممکن است به دلایل متنوع تمایل داشته باشند تا گمنام باقی بمانند. نقطه قوتی که در واقع از طریق آن گمنامی قابل دستیابی است به دانش بافت بستگی دارد. برای مثال این که کل سامانه پیام‌رسانی چقدر خوب درک می‌شود. در سامانه‌های بزرگ و غیرمتمرکز، ممکن است سامانه پیام‌رسانی به طور کامل برای هر شرکت‌کننده‌ای شناخته شده نباشد و در بسیاری موارد بافت پیام در طول زمان تغییر خواهد کرد.

مفهوم گمنامی بسته به مفهوم **عدم پیوندپذیری**[1] است، آنجا که موارد مورد علاقه کم‌وبیش وابسته به هرگونه مشاهده‌ای هستند به جای وابستگی به دانش مقدم هستند.

گمنامی رابطه دلالت بر درجه‌ای از عدم ردیابی‌پذیری دارد که چه کسی با چه کسی ارتباط برقرار می‌کند:

بنابراین، پیوند ایجادکنندهٔ پیام به پذیرنده یا پذیرنده‌های امکان‌پذیر نیست.

عدم مشاهده‌پذیری رابطه، قادر نبودن به مشاهده زمانی است که ایجادکنندهٔ پیام، می‌فرستد و پذیرنده دریافت می‌کنند. عدم مشاهده‌پذیری ارتباط به این معناست که مشاهده ارتباط بین ایجادکنندهٔ پیام و پذیرنده ممکن نیست.

شبه‌گمنامی شامل جایگزینی نام و سایر صفات شناساننده فرد به وسیله برچسب است تا از شناسایی موضوع داده جلوگیری کند یا کمینه چنین شناسایی را بسیار مشکل سازد. **شبه‌گمنام** بودن، حالت استفاده از نام مستعار به عنوان برچسب شناسایی است.

با توجه به درجه پیوندپذیری، انواع نام‌های مستعار امکان‌پذیر خواهد بود:

الف- *نام مستعار فردی:* نام مستعار فرد جایگزین برای نام نگهدارنده است که بازنماینده هویت مدنی نگهدارنده این نام ممکن است در تمامی بافت‌ها مورد استفاده قرار گیرد، مانند :تعدادی از کارت‌های شناسایی،

1 - Unlinkability

شماره ملی،DNA [1]، لقب، نام مستعار یک کنشگر یا شماره تلفن همراه.

ب- *نام مستعار نقش* : استفاده نام مستعارهای نقش محدود به نقش‌های مشخص است، مانند: نام مستعار مشتری، یا حساب اینترنتی مورد استفاده برای نمونه سازی نقش مشابه «کاربر اینترنتی» ممکن است نام مستعار نقش مشابهی توسط شرکای ارتباطی متفاوتی استفاده شود.

پ- *نام مستعار رابطه:* برای هر شریک ارتباطی، شبه‌گمنامی متفاوتی استفاده می‌شود. این بدان معناست که شرکای ارتباطاتی نمی‌توانند بگویند که با کاربر یکسانی در ارتباط هستند.

ت- *نام مستعار نقش-رابطه:* برای هر نقش و برای هر شریک ارتباطی، نام مستعار نقش-رابطه متفاوتی مورد استفاده قرار می‌گیرد. این بدان معناست که شریک ارتباطی ضرورتا نمی‌داند که آیا دو نام مستعار مورد استفاده در نقش‌های مختلف متعلق به کاربری در نقش یکسان در ارتباط هستند، تنها از طریق نام مستعار نمی‌دانند که آیا این کاربر یکسانی است یا خیر.

مثال: منبعی از اطلاعات را در نظر بگیرید که وقتی در غیر دامنه عمومی به Berstein اطلاعات منتقل می‌کند، به طور مرتب از نام « Wool » و وقتی اطلاعات یکسانی را به Woodward منتقل می‌کند از «Touched» استفاده می‌کند. Berstein سپس اطلاعاتی درباره موضوع جدیدی از «Deep Throat» دریافت می‌کند و Woodward از «Watergate» دریافت می‌کند، Berstein و Woodward نمی‌دانند که آیا «Deep Throat» همان فرد « Wool » یا «Touched» است یا هر دوی آن‌ها.

ث- *نام مستعار تراکنش* : برای هر تراکنش، شبه‌گمنامی تراکنش غیرقابل پیوند با هر شبه‌گمنامی تراکنش دیگری (و کمینه در آغاز غیرقابل پیوند با هر گونه شبه‌گمنامی تراکنش دیگر) مورد استفاده است، مانند اعداد تراکنش تصادفی تولید شده برای بانکداری برخط. بنابراین، شبه‌گمنامی تراکنش می‌تواند مورد استفاده قرار گیرد تا گمنامی قوی را تا آنجا که امکان دارد تشخیص دهیم.

به صورت کلی، گمنامی نقش نام‌های مستعار نقش و نام‌های مستعار رابطه از گمنامیِ نام‌های مستعار فردی قوی‌تر است. قدرتِ گمنامی با کاربردِ نام‌های مستعار نقش-رابطه افزایش می‌یابد که استفاده از آن محدود به هر دو نقش یکسان و رابطه یکسان می‌شود.

اگر اطلاعات فردی کمتری از صاحب نام مستعار به نام مستعار پیوند داده شود، گمنامی قوی‌تر خواهد بود.

ب-۲-۳ موتورهای شهرت

مفهوم موتور اعتبار، اساس بسیاری از رسانه‌ها و شبکه‌های جامعه‌ای بر روی وب را تشکیل می‌دهد. موتورهای شهرت برای پایش اطلاعات مرتبط مورد استفاده قرار می‌گیرند و همچنان که کمیت و تنوع اطلاعات به طور چشم‌گیری افزایش می‌یابد این موتورها مرتبط‌تر می‌شوند.

یک موتور شهرت به عنوان مجموع شکل گرفته‌ای از خطوط‌مشی و رویه‌ها که برای محاسبه امتیاز شهرت برای فرد بر اساس فعالیت‌های گذشته آن‌ها مورد استفاده قرار می‌گیرد. در دنیای برخط، موتور شهرت به

2- Deoxyribonucleic Acid

ایده ردپای رقمی(دیجیتالی)[1] بستگی دارد. ردپاهای رقمی، اثری از فعالیت یک نفر در محیط رقمی هستند.

گزارش‌های شهرت و دیگر سازوکارها همواره وسیله‌ای برای کمّی کردن شهرت فراهم آورده‌اند اما مقایسه بین سازوکارهای شهرت وب (مانند درجه‌بندی‌های حراجی اینترنتی) و گزارش‌های شهرت سنتی، جالب است. همان‌گونه که ما در وب، تراکنشی (خرید، فروش، قرض، بازپرداخت) انجام می‌دهیم، داده رقمی خلق می‌کنیم.

این داده به وسیله دیگران گرفته می‌شود (مانند بنگاه‌های ارزشیابی اعتبار) و اگر چه این داده متعلق به ما است- به وسیله بنگاه ارزشیابی شهرت تصاحب شده است (و البته ممکن است ما مسئول ارزیابی آن باشیم). شکل‌های شیک‌تری از موتورهای شهرت نیز وجود دارد از قبیل موتور اعتبارeBay [2] موتور eBay از یک امتیاز شهرت متمایز است چرا که شفافیت دارد. هر بازخوردی (شام بازخوردهای منفی) به شخصی که آن نظر درباره او داده شده است برمی‌گردد- بنابراین فرصتی برای جذابیت به دست می‌دهد.

یک موتور شهرت می‌تواند برای افزایش اعتماد به وسیله گنجاندن بینش‌هایی از منابع گسترده‌تر جامعه مورد استفاده قرار گیرد، این کار از طریق وظایفی مانند اعتبارسنجی منابع جدید اطلاعاتی، اعتبارسنجی منبع محتوایی، هشدارهای آنی مانند جستجوی توییتر[3] (شبکه اجتماعی) و هشدارهای وبگاه گوگل[4]، تقویت اعتماد از منابع ناشناخته، تکمیل جستجو به وسیله بینش‌های خارجی، آوردن ایده‌های جدید/ خارجی به محدوده اشتراکی مورد اعتماد، پیش‌بینی فرصت‌ها و تهدیدها از منابع خارجی، غیره صورت می‌گیرد. با این وجود، بسیاری از فناوری موجود Web 2.0 (مانند ویکی ها) محدودیت‌هایی برای ساخت اعتماد دارند چرا که آن‌ها الگوی اعتماد مستحکم داخلی ندارند.

ب-۳ ارزیابی قابلیت اعتماد اطلاعات

مفاهیم زیربنایی برای اعتماد به صورت ذاتی دارای طبیعت ذهنی به جای عینی هستند و ضرورتا پذیرای باز نمایش مکانیکی نیستند. با این وجود، دیدگاه[5] Pareto برای این مشکل در نظر گرفته می‌شود: با وجود هرگونه تلاش برای کامل کردن الگوی آنجا که اکثریت نتایج مطلوب نسبتا با میزان کمی تلاش قابل دستیابی است. یک راه‌حل نیازمند میزان نامناسبی از تلاش خواهد بود. اجرای ممکن چنین دیدگاهی عبارتند از:

الف- ایجادکنندهٔ پیام‌های اطلاعات درجه‌ای از اعتماد به اطلاعاتی که منتشر کرده‌اند نسبت دهند. فایده‌ی چنین دیدگاهی توسط زیرساخت ملی مرکز حفاظت انگلستان اعتبارسنجی شده است که در آنجا برای نوشتن شرح و اشاعه‌ی اطلاعات هشدار دهنده به طور خودکار و برای جوامع اشتراک اطلاعات گوناگونی مورد استفاده

---

1 - Digital footprint

۲ـ اسامی محصولات مورد استفاده در پاراگراف ذیل ، مثال‌هایی از کالاهای مرتبطی هستند که از نظر تجاری در دسترسند. این اطلاعات برای راحتی کاربر در این سند داده میشود و معادل حمایت ISO یا IEC از این محصولات نیست.

3- Twitter

4- Google

۴- اساس این معیار اساس این معیار که در اقتصاد رفاه به کار برده می‌شود این است که تغییر وضعیت نسبت به قبل بهتر خواهد بود که بتوان حداقل وضعیت یک فرد را بهبود بخشید بدون اینکه به دیگران صدمه‌ای وارد آید.

قرار می‌گیرد.

ب - این که تمامی اطلاعات به گونه‌ای واضح از طریق منبع خود، به طور مطلوب با استفاده از یک شکل ساختاریافته داده شناسایی می‌شوند.

پ - با وجود مفهوم شناسایی منبع، بهتر است پشتیبانی برای گزارش‌دهی گمنام نیز وجود داشته باشد، همانگونه که تجربه‌ها از دنیای امنیت نشان می‌دهد که تامین گمنامی به گونه‌ای چشمگیر، اشتراک اطلاعات را افزایش می‌دهد.

ت - این که مفهوم یک شیء مرزی برای پوشینه‌سازی اساس هرگونه اطلاعات تبادل‌یافته‌ای مورد استفاده قرار می‌گیرد. اشیاء مرزی، تجمعات ساختاریافته‌ای از اطلاعات هستند که درجه‌ای از شناخت دوسویه در داخل جامعه مورد علاقه دارند و بنابراین هر دو ارتباط در طول مرزهای دامنه‌ای و زبانی را ممکن می‌سازند:

موفقیت ابتکارات عملی چون علائم برشماری آسیب‌پذیری رایج میتر (Mitre's CVE)[1]، همان گونه که برای اشیا مرزی گفته شد، تا حدی به انتخاب موجود آن‌ها نسبت داده می‌شود.

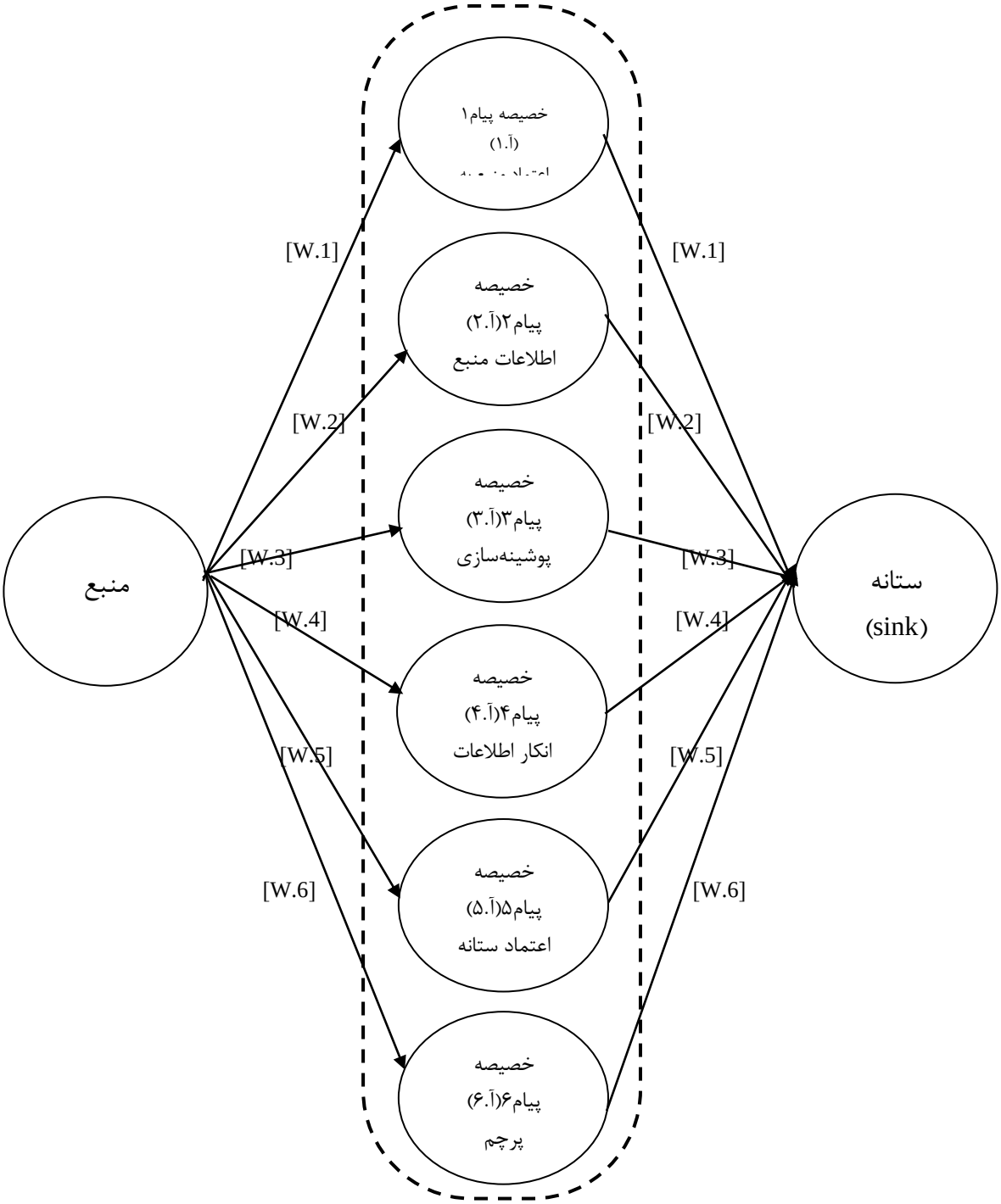
ث - بهتر است ایجادکنندهٔ پیام و پذیرنده یک تبادل اطلاعات مورد اعتماد، هر دو ارزیابی کنند که آیا اطلاعات، پشتیبان محتوای از پیش دریافت شده هستند و چندین بار بوده‌اند: اگرچه بدین منظور حوزه‌هایی برای تجزیه خودکار اطلاعات وجود دارد، باید تشخیص داده شود که تجزیه خودکار پیام‌ها برای چنین اهدافی در حالت بسیار پیشرفته جاری، اطمینان‌پذیر نیست. برای کمینه کردن مخاطرات تقویت به ظاهر درست، تابع توزیع تجمعی بازگشت کاهنده مورد نیاز خواهد بود تا بر روی شماره تعداد نمونه‌های قبلی اعمال شود، که در نتیجه این بدان معنا خواهد بود که مقدار وزن‌دار اطلاعات افزوده با افزایش شماره، کاهش می‌یابد.

ج - این که منبع یا پذیرنده، بر طبق این که آیا اطلاعات به صورت مستقل تایید شده‌اند، پرچمی به آن اختصاص می‌دهند، تا با حفظ به اصطلاح افسانه‌های شهری به عنوان اطلاعات مفید مقابله کند.

این که پذیرنده‌های اطلاعات بهتر است بر اساس برداشت‌های الگوی «۵ در ۵» یک ارزشیابی ذهنی به منبع اختصاص دهند (به بند ب-۱ مراجعه شود).

چنین معیارهایی که به صورت مناسبی وزن‌دار شده‌اند می‌توانند اعضای جامعه اشتراک اطلاعات را قادر به کمی کردن اعتمادی سازند که می‌توانند و بهتر است در اطلاعاتی که از اعضای جامعه دریافت می‌کنند قرار دهند. این مسأله به صورت تصویری در شکل ب-۱ در بالا بازنمایش داده شده است.

1- Mitre's Common Vulnerability Enumeration



کلید

W.n توجیه ایجادکنندهٔ پیام از قابلیت اعتماد اطلاعات در پیام

W.n’ توجیه پذیرنده پیام از قابلیت اعتماد اطلاعات در پیام

شکل ب-۱- ارزیابی اعتماد محتوای پیام

پیوست پ

(آگاهی‌دهنده)

پروتکل چراغ راهنمایی رانندگی

این پیوست پروتکل چراغ راهنمایی رانندگی را تشریح می‌سازد، سازوکاری که به صورت گسترده در جوامع اشتراک اطلاعات برای نشان دادن توزیع مجاز اطلاعات، مورد استفاده قرار می‌گیرد، اگرچه مفهوم اساسی به طور گسترده درک شده است، بعضی تغییرات مختصر مورد استفاده وجود دارد. این شرح از «راهنمای عملی مناسب برای مبادله اطلاعات امنیت شبکه» که به وسیله بنگاه امنیت اطلاعات و شبکه اروپا (ENISA)[1] منتشر شده، گرفته شده است. این مفهوم در اصل به وسیله مرکز حفاظت زیرساخت ملی (CPNI)[2] انگلستان ایجاد شده بود.

پروتکل چراغ راهنمایی رانندگی (TLP) به منظور حمایت از اشتراک اطلاعات حساس بین سازمان‌ها ایجاد شود. نیاز است ایجادکنندهٔ پیام‌ها خبر بدهند که می‌خواهند اطلاعات آن‌ها چقدر گسترده، آن سوی پذیرنده بی واسطه، در صورت وجود، گردش یابند.

پروتکل چراغ راهنمایی رانندگی بر اساس مفهوم برچسب‌گذاری اطلاعات توسط ایجادکنندهٔ پیام با یکی از چهار رنگ زیر است، تا در صورت وجود، نشان دهد که کدام اشاعه دورتری، می‌تواند به وسیله پذیرنده تقبل شود. اگر اشاعه گسترده‌تری مورد نیاز باشد، پذیرنده باید با ایجادکنندهٔ پیام مشورت کند.

چهار رنگ و معانی آن‌ها در زیر آمده است:

قرمز- شخصی تنها برای پذیرنده‌های دارای نام. به عنوان مثال در بافت کلی ملاقات، اطلاعات قرمز محدود به آن‌هایی است که در ملاقات حاضر هستند. در اکثر شرایط، اطلاعات قرمز به صورت کلامی یا حضوری عبور داده خواهند شد.

زرد- توزیع محدود. پذیرنده مجاز است اطلاعات زرد را با دیگرانی که در داخل سازمان آن‌ها هستند، فقط جهت اطلاع ، به اشتراک بگذارد. ممکن است انتظار برود که ایجادکنندهٔ پیام محدودیت‌های مورد نظر این اشتراک را

مشخص کند.

سبز- در گستره جامعه. اطلاعات در این دسته می‌توانند به صورت گسترده‌ای در داخل جامعه خاص گردش یابند. با این وجود، ممکن است اطلاعات نه در اینترنت منتشر یا پست شوند و نه خارج از جامعه.

سفید- نامحدود. مشروط بر قوانین استاندارد حق نشر، اطلاعات سفید مجاز هستند آزادانه و بدون

1- European Network and Information Security Agency

2- Centre for the Protection of National Infrastructure

محدودسازی توزیع شوند.

اطلاعات حساس به هر صورتی که به وسیله ایجادکنندهٔ پیام فراهم شدند، بهتر است در زمان افشا مطابق با پروتکل چراغ راهنمایی رانندگی نشانه‌گیری شوند. تمامی اطلاعات حساس، اطلاعات زرد فرض خواهند شد مگر این که در عوض، اظهار یا نوشته شوند. با این وجود، هویت منبع اطلاعات حساس به صورت پیش‌فرض و مگر این که غیر از زمان افشا به صورت مشخص اظهار شده باشد، قرمز خواهد بود. پروتکل چراغ راهنمایی رانندگی همچنین می‌تواند برای استفاده در داخل سازمان مناسب شود، برای مثال آنجا که تنها به برخی افراد دسترسی کامل به تمامی اطلاعات به اشتراک گذاشته شده، داده شده است (به شکل ۹ مراجعه شود.)

پیوست ت

(آگاهی‌دهنده)

الگوهایی برای سازمان‌دهی جامعه اشتراک اطلاعات

ت-۱ مقدمه

راه‌های بسیاری وجود دارد تا جامعه اشتراک اطلاعات بتواند از اتحادیه نامنسجمی از شرکای متناظر گرفته به هستار رسمی ساختاریافته و به شکل متمرکز قانونی واپایش شده، سازمان‌دهی شود . این پیوست دو شکل از سازمان جامعه‌ای را تشریح می‌کند که ممکن است در عمل قابل یافتن باشند و از مدیریت امنیت اطلاعات اثربخش پشتیبانی می‌کنند.

ت-۲ هستارهای ارتباط ی اطلاعات مورد اعتماد

ت-۲-۱ مقدمه

یک هستار ارتباطی اطلاعات مورد اعتماد (TICE) سازمان خودگردانی است که تبادل اطلاعات بین اعضای جامعه اشتراک اطلاعات را با اجرای نقش درگاه هماهنگی و ارتباطی، پشتیبانی می‌کند.

این هستار می‌تواند عنصر مرکزی سامانه مدیریت امنیت اطلاعات اثربخش ، برای ارتباطات بین‌بخشی یا بین-سازمانی باشد. یک TICE می‌تواند تبادل اطلاعات امن و کارا بین اعضای جامعه اشتراک اطلاعات را تضمین کند و به آن‌ها در قابلیت‌هایی چون پایش ، تحلیل و مدیریت پاسخ‌ها به رخدادها و مخاطرات یاری می‌رساند.

یک هستار ارتباطی اطلاعات مورد اعتماد (TICE) متشکل از گروهی از کارشناسان در حوزه‌های خاص است که کسب‌وکارهای اصلی آن‌ها عبارتند از:

- حصول اطمینان تبادل اطلاعات مناسب بین TICE و اعضای جامعه ؛
- تحلیل و پاسخگویی به رخدادهای امنیت اطلاعات؛
- اداره کردن رخدادها و پشتیبانی از اعضای جامعه برای بازیابی از رخنه‌ها؛
- تامین آگاهی امنیت اطلاعات مرتبط با اعضای جامعه به وسیله:
  - صدور توصیه‌ها در مورد آسیب‌پذیری‌های مولفه‌های مورد استفاده،
  - اطلاع‌رسانی به نمایندگان اعضای جامعه درباره بهره‌جویی‌ها و سوء استفاده ویروس‌ها از این نقاط ضعف، به گونه‌ای که اعضای تصدیق شده بتواند مولفه‌های وصله و به روزرسانی‌های کارا را انجام دهند.

یک TICE می‌تواند به عنوان واسطه مورد اعتماد برای گمنام کردن منبع یا پذیرنده‌های اطلاعات به اشتراک گذاشته شده عمل کند. این مساله اعضا را قادر می‌سازد تا بدون آنکه در مواقع ضروری هویت خودشان را

آشکار کنند یا به اعضای دیگری که هویت آن‌ها مخفی شده اعتماد کنند، اطمینان داشته باشند که اطلاعات از منبعی مورد اعتماد می‌آید.

یک TICE ممکن است براساس یا ایجاد شده از سازمان موجود، مانند گروه پاسخگویی رخداد امنیت اطلاعات (ISIRT)[1] که بیش از این به جامعه مرتبط خدمت کرده است، باشد .بنابراین وجود ISIRT نیازمند بسط داده شدن است تا به تامین خدمات TICE پیش فعال به علاوه خدمات واکنشی که در کل به وسیله ISIRT فراهم شده، بپردازد.

ت-۲-۲ ملاحظات سازمانی TICE

ت-۲-۲-۱ کارشناسان در هر موضوع خاص

این ساختار بهتر است شامل مهارت بخشی و عمومی باشد تا اطمینان یابیم افراد درستی با مهارت‌های متناسب درگیر هستند و همچنین کارشناسان می‌توانند ارتباط هرگونه اطلاعاتی در داخل ارتباط داخلی و یافت زیرساخت‌های اطلاعاتی مرتبط را تعیین کنند.

کارشناسان بهتر است به منظور هدایت تحلیل ، به ویژه در دامنه‌های زیر (اما نه محدود به آن‌ها) به کار گرفته شوند:

- مدیریت کسب‌وکار؛
- امنیت و زیرساخت فناوری اطلاعات؛
- عملیات؛
- تنظیم کنندگان مقررات داخلی؛
- وزارت دادگستری.

کارشناسان می‌توانند به صورت پاره‌وقت یا تمام‌وقت باشند و ممکن است در پایگاه مرکزی، پایگاه‌های عملیاتی یا ترکیبی از هر دو، مستقر شوند.

ت-۲-۲-۲ ساختار سازمانی

یک TICE معمول بهتر است کمینه شامل عملکردهای زیر باشد:

- هیأت مدیره (ضروری؛ کسانی که مسئول مدیریت راهبرد TICE و روابط با اعضای جامعه هستند).
- گروه فنی عملیاتی (ضروری؛ کسانی که مسئول تحلیل کسب‌وکار و مسائل مخاطره فنی و تعیین کننده کاربرد مناسب برای وصله ها و تغییرات به کار برده هستند).
- کارشناسان فنی عملیاتی (اختیاری؛ کسانی که توصیه می‌شود به بهبود درک TICE از محیط عملیاتی یا منابع درگیر در سطح تجمعی اجزا پایگاه محلی بپردازند).

1- Information Security Incident Response Team

- کارشناسان حقوقی (اختیاری؛ اما به ویژه در زمان آغاز مرحلهٔ TICE برای کاهش مسائل قانونی توصیه می‌شود).
- کارشناسان ارتباطات (اختیاری؛ کسانی که توصیه می‌شود برای تمرکز بر ترجمه مشکلات مرتبط با مسائل فنی از آن‌ها استفاده شود تا پیام‌های قابل فهم بیشتری برای اعضا آماده کنند). کارشناسان ارتباطات می‌توانند با اجرای نقش تسهیل‌کننده بین دو گروه از اعضای جامعه گرفته تا گروه فنی عملیاتی، بازخورد جمع‌آوری کنند).

ت-۲-۲-۳ مدیریت عضو جامعه

بهتر است پشتیبانی به وسیله TICE به منظور اصالت‌سنجی، ارزیابی، درک مستمر و مدیریت اعضای جامعه‌ای یا نمایندگان آن‌ها فراهم شود تا از رابطه مورد اعتماد درست اطمینان یابیم.

ت-۲-۲-۴ الگوی سازمانی

الگوی سازمانی مناسب برای TICEبه ساختار کنونی در محل ، طبیعت اعضای جامعه و امکانی برای TICE تا به منظور برآوردن خدمات اظهار شده گسترش یابد، بسیار وابسته است. این الگو همچنین به میزان دسترسی به کارشناسان در هر موضوع خاص بستگی دارد که به صورت داتم یا بر پایه‌ای موقت استخدام شوند.

کمینه سه الگوی ممکن وجود دارد:

- الگوی مستقل: یک TICE مستقل که به اجرای نقش سازمان مستقل، با مدیریت و کارکنان خود می‌پردازد.
- الگوی نهفته :یک TICE نهفته در داخل سازمان تاسیس می‌شود تا از منابع آن برای تامین خدمات خود استفاده کند. تعداد منابع تخصیص داده شده می‌تواند بسته به فعالیت‌های پشتیبانی در طول شرایط عادی و خاصی، متغیر باشد.
- الگوی داوطلبانه :یک TICE داوطلب به وسیله کارشناسانی ساخته شده است که برای یکدیگر و بر پایه داوطلبانه مشاوره و پشتیبانی فراهم می‌آورند. این الگو بهتر است به عنوان جامعه کارشناسان در نظرگرفته شود که بسیار وابسته به انگیزش شرکت‌کنندگان هستند.

ت-۲-۳ خدمات اصلی و اختیاری TICE

انتخاب خدماتی که به وسیله TICE برای اعضای جامعه فراهم شده، فازی حیاتی است و بهتر است براساس عناصر زیر صورت پذیرد:

- محدوده و مخاطرات مرتبط با ارتباطات مطرح شده بین اعضای جامعه اشتراک اطلاعات
- محدوده TICE ، سازمان و طبیعت جامعه اشتراک اطلاعات

افزوده بر این، این مورد بسیار وابسته به نقش‌هایی است به فرض به وسیله TICE در داخل بافت جامعه به عهده گرفته شده است (با اجرای نقش تسهیل‌کننده و یا آغازگر اشتراک اطلاعات بین اعضا) خدمات اصلی

احتمالی TICE عبارتند از:

- خدمات واکنشی[1]: خدمات واکنشی برای شناسایی هرگونه حمله احتمالی به مولفه‌های زیرساخت اطلاعات، تحلیل و گزارش تاثیرات تهدیدها و حملات، پاسخگویی به درخواست های کمک، گزارش‌های رخدادها به اعضای جامعه ، طراحی شده است.
- خدمات پیش‌فعال[2]: خدمات پیش فعال برای اطمینان و تسهیل تبادل اطلاعاتی دربست، به وسیله بهبود فرایندهای امنیتی. جامعه اشتراک اطلاعات و زیرساخت‌های اطلاعاتی مرتبط، پیش از آنکه هرگونه رخداد یا رویدادی اتفاق بیافتد یا شناسایی شود، طراحی شده است. افزون بر این، بعضی خدمات پیش فعال برای بهبود پیشگیری رخداد از طریق آگاهی میان اعضا برای کاهش اثر و محدوده آن‌ها زمانی که اتفاق می‌افتند، طراحی شده است.

خدمات اختیاری بالقوه TICE عبارتند از:

- خدمات بررسی کد مخرب[3]: خدمات بررسی کد مخرب طراحی شده است تا:
  - تحلیل هرگونه پرونده یا شیء یافته شده بر روی مولفه که ممکن است در فعالیت‌های مخرب درگیر شده
  - اداره کردن و اشاعه نتایج به اعضای جامعه ، فروشندگان و دیگر طرح‌های ذینفع، به منظور پیشگیری از شیوع بدافزار و کاستن مخاطرات
- خدمات مدیریت امنیت و کیفیت. خدمات مدیریت امنیت و کیفیت به منظور یاری رساندن به اعضای جامعه در تحلیل مخاطره، مدیریت تداوم کسب‌وکار و آگاهی امنیتی با اهداف بلندمدت تر، طراحی شده است.
- خدمات گمنامی. خدمات گمنامی به منظور قادر ساختن جامعه برای فرستادن یا دریافت اطلاعات بدون آشکارسازی هویت خود آن‌ها به دیگر اعضا، طراحی شده است.

ت-۲-۴ نتیجه‌گیری

الگوی TICE ، الگویی جامع، تحت واپایش و ساختاریافته برای اشتراک اطلاعات بین سازمان‌ها فراهم می‌سازد. این الگو به ویژه برای محیط‌های حیاتی که اشتراک و تحلیل اطلاعات فوری و ارجح اهمیت دارد و اعضا یا دولت می‌توانند از هزینه زیرساخت مورد نیاز پشتیبانی کنند ، مناسب است.

ت-۳ نقاط اعلام هشدار، مشاوره و گزارش دهی

ت-۳-۱ مقدمه

الگوی نقطه اعلام هشدار، مشاوره و گزارش‌دهی (WARP) از سال ۲۰۰۳ مورد استفاده بوده است و سازوکار

1 - Reactive Services
2 - Proactive Services
3 - Malicious Code Investigation Services

اثبات شده‌ای برای اشتراک اطلاعات حساس بین سازمان‌ها در هر دو بخش عمومی و خصوصی فراهم می‌آورد.

نقطه اعلام هشدار، مشاوره و گزارش‌دهی، به طور معمول بر پایه‌ای داوطلبانه، اطلاعات را بین مردم یا سازمان‌هایی با منافع مشترک به اشتراک می‌گذارد.

نقطه اعلام هشدار، مشاوره و گزارش‌دهی (WARP) برپایه روابط شخصی بین مردمی که نماینده اعضای جامعه اشتراک اطلاعات هستند، مستقر است. یک WARP معمولی شامل کاروَر است که تا اندازه‌ای درباره موضوع مورد نظر می‌داند اما به طور عمده به دلیل روابط خوب با اعضا انتخاب می‌شود. به طور معمول بین ۲۰ تا ۱۰۰ عضو وجود دارد، در غیر این صورت WARP ممکن است تماس شخصی و اعضای متعلق به جامعه‌ای از منافع مشترک بارز (کسب‌وکارهای کوچک، دولت محلی، تامین کنندگان خدمات، گروه‌های مورد علاقه و غیره) را از دست بدهد.

اعضای WARP توافق کرده‌اند تا به عنوان بخشی از جامعه با همدیگر کار کنند و اطلاعات را به اشتراک بگذارند تا مخاطرهٔ نقضِ سامانه‌های اطلاعاتی خود را کاهش دهند و در نتیجه، مخاطره سازمان خود را کاهش دهند. این جامعه اشتراک می‌تواند بر پایه بخشی از صنعت یا بازار، مکان جغرافیایی، استانداردهای فناوری، گروه‌های مورد علاقه، گروه‌بندی مخاطره یا هر آنچه از منافع مشترک دیگر که در کسب‌وکار معنا می‌دهد، استوار باشد.

به طور معمولWARP ها کوچک، شخصی و «غیرانتفاعی» هستند.

ت-۳-۲ کارکردهای WARP

کاروَر WARP از وبگاه، رایانامه، تلفن، پیامک و ملاقات اتفاقی (هر جا که ممکن باشد)، استفاده می‌کند تا خدمتی شخصی شده از هشداردهنده‌ها و مشاوره به اعضا بفرستد. این مشاوره به طور معمول از نوع امنیت فناوری اطلاعات است (چرا که مقدار زیادی از آن وجود دارد و به‌سرعت تغییر می‌کند)، اما می‌تواند شامل مطالب دیگری نیز باشد (تهدیدهای دیگر، جرایم الکترونیکی، طرح‌ریزی اقتضایی و غیره). کاروَر همچنین از دانش خود اعضا استفاده می‌کند تا به اعضای دیگری که از تابلوی اعلانات، ملاقات و مهارت‌های کلی ارتباطی استفاده می‌کنند یاری رساند. یک WARP موفق ، برای تشویق اعضا به صحبت کردن درباره رخدادها و مشکلات خودشان، به صورت بی‌نام و برای منفعت بقیه، اعتماد کافی ایجاد می‌کند (کمی شبیه به طرح «شبگردی»).

ت-۳-۳ خدمات WARP

ت-۳-۳-۱ مرور کلی

یک WARP به طور معمول سه خدمت اصلی ارائه می‌دهد:

- یک خدمت هشدار دهنده پالایش شده که در آن اعضا تنها اطلاعات امنیتی مورد نیاز خود را که از طریق یک فهرست علامت‌دار برخط انتخاب شده، دریافت می‌کنند.
- یک خدمت واسطه مشاوره که در آن اعضا می‌توانند از ابتکارات عمل و تجربیات دیگر اعضا، به طور

احتمالی از طریق تابلوی اعلانات یک عضو، بیاموزند.

- یک خدمت اشتراک مورد اعتماد که در آن گزارش‌ها بی‌نام می‌شوند تا اعضا بتوانند از رخدادها و حملات یکدیگر، بدون ترس از گرفتاری یا اتهام متقابل، بیاموزند.

ت-۳-۳-۲ هشداردهنده‌های پالایش‌شده

خدمت هشداردهنده‌های پالایش شده به اعضای WARP اجازه می‌دهد تا هشدارها و مشاوره‌هایی که براساس حوزه مورد علاقه خودشان پالایش شده‌اند را دریافت کنند. نرم‌افزار کاربردی هشداردهنده‌های پالایش شده از یک فهرست علامت‌دار درختی عضویت استفاده می‌کند که به اعضای WARP اجازه می‌دهد به سادگی انتخاب‌هایشان را تعدی و حفظ کنند. این نرم‌افزار همچنین به کاروَران WARP کمک می‌کند تا به سادگی و به روشی به هنگام، هشداردهنده‌ها و مشاوره‌ها را دسته‌بندی و توزیع کنند. این خدمت قسمت هشداردهندگی در نقطه هشدار، مشاوره و گزارش را بر عهده دارد.

ت-۳-۳-۳ کارگزار مشاوره

این خدمت به اعضای جامعه WARP اجازه می‌دهد تا راجع به شیوه‌های مناسب و مسائل امنیت اطلاعات در یک فضای امن به بحث بپردازند. این خدمت همچنین اعضا را قادر می‌سازد تا تجربیات و مهارت‌های خود را به طور احتمالی به صورت تهاتری که در آن یک نفر در حوزه‌ای کار کرده است و دیگری به آن می‌اندیشد، به یکدیگر ارائه دهند. این خدمت، قسمت مشاوره از نقطه هشدار، مشاوره و گزارش را بر عهده دارد.

ت-۳-۳-۴ اشتراک مورد اعتماد

این خدمت محیطی مورد اعتماد فراهم می‌سازد، که در آن اعضای WARP می‌توانند اطلاعات حساس همانند داده تهدید یا رخداد را به اشتراک بگذارند، با علم به این که این مورد موجب آسیب یا دردسر آن‌ها نخواهد بود، گزارش‌دهی می‌تواند از طریق تلفن ، رایانامه یا به صورت رودررو با محافظان امنیتی مناسب به دست آید. زمانی که رخدادی سانسور و بینام شد، در صورت اقتضا، اطلاعات آن نیز ممکن است به WARPهای دیگری که ارتباطی مورد اعتماد با آن‌ها وجود دارد و به دولت، برای تطبیق و پایش گرایش‌های ملی، عبور داده شود. این خدمت، قسمت گزارش‌دهی از نقطه اعلام هشدار، مشاوره و گزارش‌دهی را بر عهده دارد.

ت-۳-۳-۵ خدمات دیگر

نقاط اعلام هشدار، مشاوره و گزارش دهی (WARP) ممکن است خدمات دیگری فراهم سازند که به نفع اعضای جامعه خودشان است. با این وجود، چنین خدماتی عموما بسیار ساده و مستقیم نگه داشته می‌شوند تا زمان و منابع مورد نیاز کاروَر WARP برای پشتیبانی از آن‌ها را کمینه سازند.

ت-۳-۴ منافع

WARPها امنیت اطلاعات اثربخش و کم‌هزینه به اعضا ارائه می‌کنند، با فراهم کردن:

- یک محیط مورداعتماد؛

- پالایش اطلاعات امنیتی؛
- دسترسی به مشاوره‌ی کارشناسان؛
- اعلام هشدار برای تهدیدها؛
- پشتیبانی تصمیم راهبردی؛
- آگاهی امنیت بهبود یافته؛

بعضی از این تعداد منافع احتمالی که مرتبط به تاسیس یک WARP می‌باشند، عبارتند از:

- کارایی کار[1]: WARP ها، اشتراک اطلاعات و هماهنگی وظایف مشترک را ارتقا بخشیدند، که این به نوبه خود، وظایف تکراری را کاهش خواهد داد. این به یک شرکت یا دولتی از طریق کارایی فزاینده فایده خواهد رساند.
- اجتناب از آسیب شهرت[2]: همین‌طور که سازمان‌ها به منظور تراکنش با عموم، بیشتر به سمت دیدگاه‌های برخط حرکت می‌کنند، حضور در وب به عاملی کلیدی تبدیل شده است. اگر یک وب‌سایت غیرقابل دسترسی باشد یا بدشکل و از ظاهر افتاده شده باشد، این مورد می‌تواند موجب مسائل شهرت شود و می‌تواند درک خدمات وب را سست کند. جامعه مورد خدمت با عضویت در WARP بهتر مورد حفاظت قرار خواهد گرفت.
- اعلام هشدار اولیه[3]: دریافتن مشکلات و راه‌حل‌هایی که دیگران تجربه می‌کنند و اشتراک آن‌ها در داخل جامعه WARP ، خدمتی منحصربه‌فرد و شخصی شده را تسهیل خواهد کرد که حتی یک تامین‌کننده تجاری بزرگ نخواهد توانست با آن تطابق یابد.
- پشتیبانی از سوی دولت و دیگرWARP ها: مزیت متعلق بودن به چنین جامعه متمرکزی به معنای توانایی اشتراک و توزیع سودمند مشاوره از یک منبع مورد اعتماد است .پشتیبانی عملیاتی ازWARP های دیگر به خوبی از طریق فرم کاروَران WARP بر قرار شده است. همچنین همکاری نظیر به نظیری از طریق برنامه کاربردی هشداردهنده‌های پالایش شده وجود دارد که توزیع مشاوره‌ها و هشدارهای دیگرWARP ها را به سادگی ممکن می‌سازد.
- کم‌هزینه[4]: این الگو طوری طراحی شده است که از طریق کمینه کردن سطوح کارمندی (یا گروه‌های مجازی) بسیار کم‌هزینه باشد.
- جعبه ابزار رایگان جامع[5]: یک تامین‌کننده WARP به جعبه ابزار WARP دسترسی دارد که از تجربیات موجودWARP ها ایجاد شده است. این جعبه ابزار شامل اطلاعات پیش‌زمینه، چگونگی

1 - Work Efficiency
2 - Avoidance of Reputation Damage
3 - Early warning
4 - Low cost
5 - Comprehensive free Toolbox

آغاز کردن، چگونگی ساخت و اجرای یک WARP و فهرست وسیعی از دانلودها، از مقالات مطبوعات گرفته تا مطالب بازاریابی، است.

- پایداری[1]: WARP ها امروزه به طور گسترده‌ای ایجاد می‌شوند، با بسیاری از سازمان‌های قابل احترام که به صورت موفقیت آمیزی این دیدگاه را با پایداری اثبات شده آن به کار گرفتند.
- نرم‌افزار: تامین‌کنندگان WARP ممکن است به نرم‌افزار متخصصی دسترسی داشته باشند که برای پشتیبانی از تمام سه خدمت WARP ایجاد شده است.
- اعتبارپذیری افزاینده[2]: صفت انسانی «غیرانتفاعی» و ارتباط آن با به‌گزینی موجود، به کسب اعتماد جامعه کمک خواهد کرد و می‌تواند به اعتبار سازمان، به ویژه در بافت فعالیت‌های عمومی یاری رساند.
- انطباق[3]: عضویت WARP به سازمان‌های عضو کمک خواهد کرد تا واپایش‌های تماسی سازمانی شناسایی شده در داخل استاندارد ملی ایران به شماره ایزو- آی ای سی ۲۷۰۰۲ : سال ۱۳۹۴ را برآورده سازند.
- امکان رشد[4]: بسیاری از تامین‌کنندگان WARP در فرایند ایجاد WARPهای بعدی هستند که بر روی مهارت و زیرساخت موجود ساخته می‌شود که هم هزینه کم و هم پایداری را پشتیبانی می‌کند. WARPها هم‌اکنون در بسیاری از بخش‌ها ظاهر می‌شوند و شروع به گسترش بین‌المللی می‌کنند.
- مسئولیت اجتماعیِ شرکت[5]: یک عضو WARP بودن، مسؤولیت جامعه مشارکتی سازمان و در نتیجه کسب اعتماد جامعه و به طور احتمالی پشتیبانی هر دوی کاروَران و اعضای دیگر راهبردهای کسب‌وکار، را بالا می‌برد.

ت-۳-۵ نتیجه‌گیری

الگوی WARP، الگویی ساده و مشارکتی برای اشتراک اطلاعات بین سازمان‌های هم‌فکر فراهم می‌سازد. این الگو به ویژه برای موقعیت‌های مناسب که در آن بودجه محدود و زیرساخت مرکزی باید بر پایه‌های داوطلبانه فراهم و اجرا شود.

1- Sustainability
2 - Increased credibility
3 - Compliance
4 - Growth potential
5 - Corporate Social Responsibility

کتاب‌نامه

[1] Internet Engineering Task Force. RFC 4021: Registration of Mail and MIME Header Fields [online]. March 2005 [viewed October 2014]. http://datatracker.ietf.org/doc/rfc4021/

[۲] استاندارد ملی ایران شمارهٔ ۲۷۰۰۶: سال ۱۳۸۷، فناوری اطلاعات –فنون امنیتی – الزامات برای نهادهای ممیزی‌کننده و گواهی کننده سامانه‌های مدیریت امنیت اطلاعات

[3] O'REILLY. Tim. What Is Web 2.0 - Design Patterns and Business Models for the Next Generation of Software. O'Reilly Web Blog [online]. 30 September 2005 [viewed October 2014]. http://oreilly. com/web2/archive/what-is-web-20.html

[4] Wikipedia, The Free Encyclopedia. Pareto distribution [online]. 25 April 2011 [viewed October 2014]. http://en.wikipedia.org/wiki/Pareto_distribution

[5] European Agency for Network and Information Security. Good Practice Guide on Information Sharing. June 2009 [viewed October 2014]. http://www.enisa.europa.eu/activities/Resilienceand- CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide

[6] Centre for the Protection of National Infrastructure (UK). WARP homepage. April 2010 [viewed October 2014]. Available from: http://www.warp.gov.uk