INSO
16300-7

1st. Edition
May.2013

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

استاندارد ملی ایران
۱۶۳۰۰-۷
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات - اتصال متقابل سامانه‌های باز - چارچوب‌های کاری امنیتی برای سامانه‌های باز: چارچوب کاری ممیزی امنیت و هشدارها

Information technology - open systems Interconnection - security frameworks for open systems: security audit and alarms framework

ICS 35.100.01

به‌نام 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 حوزه‌های مختلف در کمیسیون‌های 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، سازمان‌های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع 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 به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان‌های 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 نیازمندی‌های خاص کشور ، از آخرین پیشرفت‌های 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 سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این 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- اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز: چارچوب کاری ممیزی امنیت و هشدارها»

رئیس:	**سمت و/یا نمایندگی**
فولادیان، مجید (فوق لیسانس مهندسی مخابرات)	مشاور سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم افزار)	مدیرکل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (لیسانس مهندسی برق کنترل)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
صوفی زاده، جلیل (دکترای مهندسی مخابرات)	نماینده سازمان فناوری اطلاعات
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت مهندسی کاربرد سیستم
عبداللهی ازگمی، محمد (دکتری مهندسی کامپیوتر - نرم‌افزار)	استادیار و عضو هیات علمی دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران

فیاضی، مهدی (لیسانس مهندسی الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات، لیسانس مهندسی الکترونیک)	کارشناس سازمان فناوری اطلاعات ایران
کبیری، پیمان (دکترای مهندسی کامپیوتر)	استادیار و عضو هیات علمی دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران
معروف، سینا (لیسانس مهندسی کامپیوتر سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران
مشکی، محسن (فوق لیسانس مهندسی کامپیوتر هوش مصنوعی)	نماینده دانشگاه علم و صنعت ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استانداردها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات - اتصال متقابل سامانه‌های باز - چارچوب‌های کاری امنیتی برای سامانه‌های باز: چارچوب کاری ممیزی امنیت و هشدارها» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در دویست و چهارمین اجلاس کمیته‌ی ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۰/۳ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

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

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

ISO/IEC 10181-7:1996, Information technology-open systems Interconnection-security frameworks for open systems: security audit and alarms framework.

مقدمه

این استاندارد ملی مفهوم امنیت ممیزی را که در ITU-T Rec. X.810 | ISO/IEC 1018 l-l توصیف شده، پالایش[1] می‌کند. این امر شامل تشخیص رویداد[2] و عمل‌های حاصله از این رویدادها است. بنابراین، چارچوب کاری هم ممیزی امنیت[3] و هم هشدارهای امنیتی را مخاطب قرار می‌دهد.

ممیزی امنیت، بازبینی و رسیدگی مستقل رکوردها و فعالیت‌های[4] سیستم است. اهداف یک ممیزی شامل موارد زیر است:

- مساعدت در شناسایی[5] و تحلیل عمل‌های غیرمجاز[6] یا حمله‌ها؛
- کمک کردن برای حصول اطمینان از اینکه عمل‌ها می‌توانند به عنوان صفت موجودیت‌ها مسئول آن عمل‌ها به آن‌ها نسبت‌دهی شوند؛
- مشارکت در توسعه روال‌های کنترل خسارت بهبودیافته؛
- تأیید مطابقت با سیاست امنیتی برقرارشده؛
- گزارش‌کردن اطلاعاتی که ممکن است عدم کفایت‌ها در کنترل‌های سیستم را مشخص می‌کنند؛ و
- شناسایی تغییرات مورد نیاز در کنترل‌ها، سیاست و روال‌ها.

در این چارچوب، یک ممیزی امنیت شامل تشخیص، جمع‌آوری و ثبت، رویدادهای مرتبط با امنیت[7] گوناگون در یک دنباله ممیزی امنیت[8] و تحلیل آن رویدادها است.

هم ممیزی و هم پاسخ‌گویی[9] نیازمند آن هستند که اطلاعاتی ثبت شده باشد. یک ممیزی امنیت اطمینان می‌دهد که اطلاعات کافی هم در باره رویه هم رویدادهای استثنایی ثبت شده است، طوری که رسیدگی‌های بعدی بتواند تعیین کند که آیا نقض امنیتی[10] رخ داده است یا نه، و اگر این طور است، چه اطلاعات یا منابع دیگری به مصالحه[11] در آمده‌اند. پاسخ‌گویی، اطمینان می‌دهد که اطلاعات مرتبط در باره عمل‌های اجرا شده توسط کاربران، یا فرآیندهای عمل‌کننده از طرف آن‌ها ثبت شده است، طوری که تبعات آن عمل‌ها می‌تواند بعداً به کاربر(ان) مورد پرسش پیوند داده شود، و کاربر(ان) بتوانند به عمل‌های‌شان پاسخ‌گو نگهداشته شوند. فراهم‌سازی خدمت ممیزی امنیت می‌تواند در فراهم‌سازی پاسخ‌گویی مشارکت داشته باشد.

یک هشدار امنیتی[12] یک اخطار صادر شده برای یک فرد یا فرآیند است که تعیین می‌کند یک وضعیت حادث‌شده ممکن است نیازمند عمل فوری باشد. اهداف خدمت هشدار امنیتی شامل موارد زیر است:

- گزارش کردن تلاش‌های واقعی و آشکار برای نقض امنیت؛

---

1 - Refine
2 - Event detection
3 - Security audit
4 - Activities
5 - Identification
6 - Unauthorized actions
7 - Security-related events
8 - Security audit trail
9 - Accountability
10 - Security violation
11 - Compromise
12 - Security alarm

- گزارش رویدادهای مرتبط با امنیت گوناگون، شامل رویدادهای «عادی»؛ و
- گزارش رویدادهای فعال‌شده به وسیله محدوده‌های آستانه[1] نایل‌شده.

1 - Threshold limits

فناوری اطلاعات - اتصال متقابل سامانه‌های باز - چارچوب‌های کاری امنیتی برای سامانه‌های باز: چارچوب کاری ممیزی امنیت و هشدارها

۱ هدف و دامنه‌ي کاربرد

هدف از تدوین این استاندارد، کاربرد سرویس‌های امنیتی در محیط سامانه‌های باز است، جایی که اصطلاح سامانه‌ی باز حوزه‌هایی از جمله پایگاه داده، کاربردهای توزیع‌شده، پردازش توزیع‌شده باز و OSI را شامل می‌شود. چارچوب‌های کاری امنیتی به تعریف ابزارهای فراهم‌سازی محافظت برای سامانه‌ها و موارد درون سامانه‌ها و به روابط متقابل بین سامانه‌ها مربوط می‌شوند. چارچوب‌های کاری امنیتی روش‌های ساخت سامانه‌ها یا سازوکارها را مد نظر قرار نمی‌دهند.

چارچوب‌های کاری امنیتی عناصر داده‌ای و دنباله‌های عملیاتی (اما نه عناصر قرارداد) را هدف قرار می‌دهند که برای بدست آوردن خدمات امنیتی خاص مورد استفاده قرار می‌گیرند. این خدمات امنیتی ممکن است هستارهای[1] سامانه، داده‌های مبادله شده بین سامانه‌ها و داده‌های مدیریت شده به‌وسیله‌ی سامانه‌ها را درخواست کنند.

هدف هشدارها و ممیزی امنیت همانگونه که در این استاندارد ملی توضیح داده می‌شوند، برای حصول اطمینان از آن است که با رویدادهای امنیتی سامانه بر طبق خط مشی امنیتی مرجع امنیتی[2] کاربردپذیر[3] برخورد می‌شود.

به‌طور خاص، این چارچوب:

الف- مفاهیم پایه هشدارها و ممیزی امنیت را تعریف می‌کند؛

ب- یک مدل کلی برای هشدارها و ممیزی امنیت را فراهم می‌کند؛

پ- روابط خدمات هشدارها و ممیزی امنیت را با سایر خدمات امنیتی مشخص می‌کند.

همانند سایر خدمات امنیتی، یک ممیزی امنیت می‌تواند تنها در چارچوب کاری یک خط مشی امنیتی تعریف شده فراهم شود.

مدل هشدارها و ممیزی امنیت که در بند ۶ مطرح می‌شود، اهداف مختلفی را پشتیبانی می‌کند که ممکن است همگی آن‌ها در یک محیط خاص لازم یا مورد نیاز نباشند. خدمات ممیزی امنیت یک مرجع ممیزی[4] را ایجاد کرده که می‌تواند رویدادهایی که نیاز به ثبت در دنباله‌ی ممیزی امنیت دارند را تشخیص دهد.

شماری از انواع مختلف استاندارد می‌توانند از این چارچوب کاری استفاده کنند که عبارتند از:

۱- استانداردهایی که مفاهیم ممیزی و هشدارها را به‌کار می‌گیرند؛

---

1 - Entities
2 - Security authority
3 - Applicable
4 - Audit authority

۲- استانداردهایی که خدمات مجازی که شامل ممیزی و هشدارها هستند را تعیین می‌کنند؛

۳- استانداردهایی که استفاده از ممیزی و هشدارها را مشخص می‌کنند؛

۴- استانداردهایی که ابزارهای فراهم‌سازی ممیزی و هشدارها را در یک معماری سامانه باز مشخص می‌کنند؛ و

۵- استانداردهایی که سازوکارهای ممیزی و هشدارها را مشخص می‌کنند.

این چنین استانداردهایی به‌صورت زیر می‌توانند از این چارچوب کاری استفاده کنند:

- انواع استانداردهای ۱، ۲، ۳، ۴، ۵ می‌توانند از واژگان این چارچوب کاری استفاده کنند؛

- انواع استانداردهای ۱، ۲، ۳، ۴، ۵ می‌توانند از تسهیلات معرفی شده در بند ۸ استفاده کنند؛

- انواع استانداردهای ۵ می‌تواند مبتنی بر خصوصیات سازوکارهای معرفی شده در بند ۹ باشد.

۲ مراجع الزامي

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ توصیه‌ها و استانداردهاي بين‌المللي يكسان

2-1-1 ITU-T Recommendation X.200 (1994) | ISOLIEC7 498-l: 1994, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

2-1-2 CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1993, Information technology - Open Systems Interconnection - Systems management: Event report management function.

2-1-3 CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:993, Information technology - Open Systems Interconnection - Systems management: Log control function.

2-1-4 CCITT Recommendation X.736 (1992) | ISO/IEC 10164-7:1992, Information technology - Open Systems Interconnection - Systems management: Security alarm reporting function.

2-1-5 CCITT Recommendation X.740 (1992) | ISO/IEC 10164-81:1993, Information technology - Open Systems Interconnection - Systems management: Security audit trail function.

2-1-6 ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview.

۲-۲ زوج توصیه‌ها و استانداردهاي بين‌المللي معادل در محتوي فني

2-2-1 CCITT Recommendation X.700 (1992), Management framework for Open Systems Interconnection (OSZ) for CCITT applications.

ISO/IEC 7498-4:1989, Information processing systems - Open Systems Interconnection – Basic Reference Model - Part 4: Management framework.

2-2-3 CCITT Recommendation X.80 (1991), Security Architecture for Open Systems Interconnection for CCITT applications.

IS0 7498-2:1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌روند:

۳-۱ تعاریف مدل مرجع پایه

این استاندارد ملی از اصطلاحات زیر که در استاندارد ISO/IEC 7498-1| ITU-T Rec. X.200 تعریف شده‌اند بهره می‌برد:

الف- هستار؛

ب- تسهیلات[1]؛

پ- کارکرد؛

ت- خدمات.

۳-۲ تعاریف مربوط به معماري امنيتي

این استاندارد ملی از اصطلاحات زیر که در ISO/IEC 7498-2 | CCITT Rec. X.800 تعریف شده‌اند، استفاده می‌کند:

الف- پاسخ‌گویی؛

ب- دسترس‌پذیری[2]؛

پ- ممیزی امنیت؛

ت- دنباله ممیزی امنیت؛

ث- خط مشی امنیتی[3]؛

۳-۳ تعاریف چارچوب كاري مديريتي

این استاندارد ملی از اصطلاحات زیر که در ISO/IEC 7498-4 | CCITT Rec. X.700 تعریف شده‌اند، بهره می‌برد:

1 - Facility
2 - Availability
3 - Security policy

- مورد مدیریت‌شده[1].

۳-٤ مرور کلي تعاريف چارچوب کاري امنيتي

این استاندارد ملی از عبارات زیر که در ITU-T Rec. X.810 | ISO/IEC 10181-1 تعریف شده‌اند، استفاده می‌کند:

- دامنه امنیتی[2]

۳-٥ تعاريف افزوده

از تعاریف زیر برای برآوردن اهداف این استاندارد ملی استفاده می‌شود:

۳-٥-۱

پردازنده‌ي هشدار[3]

کارکردی که عملی مناسب در پاسخ به یک هشدار امنیتی انجام می‌دهد و یک پیام ممیزی امنیت را تولید می‌کند.

۳-٥-۲

مرجع ممیزي

مدیر مسؤول تعریف آن جنبه‌هایی از یک خط مشی امنیتی است که برای استفاده از یک ممیزی امنیت کاربردپذیر می‌باشند.

۳-٥-۳

تحليل‌گر ممیزي[4]

کارکردی که دنباله‌ی ممیزی امنیت را به منظور تولید هشدارها و پیام‌های ممیزی امنیت بررسی می‌کند.

۳-٥-٤

بايگاني‌کننده ممیزي[5]

کارکردی که قسمتی از دنباله‌ی ممیزی امنیت را بایگانی می‌کند.

۳-٥-٥

توزيع‌کننده ممیزي[6]

کارکردی که قسمت‌هایی از یا کل یک دنباله‌ی ممیزی امنیت توزیع‌شده را به کارکرد جمع آوری کننده دنباله‌ی ممیزی منتقل می‌کند.

---

1 - Managed Object
2 - Security domain
3 - Alarm processor
4 - Audit analyzer
5 - Audit archiver
6 - Audit dispatcher

۳-۵-۶

آزماينده دنباله‌ي مميزي[1]

کارکردی که گزارش‌های امنیتی را از روی یک یا بیشتر از یک دنباله‌ی ممیزی تهیه می‌کند.

۳-۵-۷

ثبت‌کننده‌ي مميزي[2]

کارکردی که سوابق ممیزی امنیت را ایجاد کرده و آن‌ها را در دنباله‌ی ممیزی امنیت ذخیره می‌کند.

۳-۵-۸

فراهم‌کننده مميزي[3]

کارکردی که سوابق ممیزی امنیت را بر طبق برخی معیارها فراهم می‌کند.

۳-۵-۹

گردآورنده دنباله‌ي مميزي[4]

کارکردی که سوابق را از دنباله ممیزی توزیع‌شده درون دنباله ممیزی امنیت جمع‌آوری می‌کند.

۳-۵-۱۰

تفکیک‌کننده‌ي رويداد[5]

کارکردی که بررسی اولیه رویداد مربوط به امنیت را انجام داده و در صورت نیاز یک ممیزی امنیت و یا یک هشدار ایجاد می‌کند.

۳-۵-۱۱

هشدار امنيتي

پیامی که با تشخیص یک رویداد مرتبط با امنیت که به‌وسیله‌ی خط مشی امنیتی به‌عنوان شرط یک هشدار تعریف شده است تولید شود. یک هشدار امنیتی برای آن است که به موقع مورد توجه هستارهای مناسب قرار گیرد.

۳-۵-۱۲

مدير هشدار امنيتي

یک فرآیند یا هستار یکتا که رفتار هشدارهای امنیتی را تعیین می‌کند.

---

1 - Audit trail examiner
2 - Audit recorder
3 - Audit provider
4 - Audit trail collector
5 - Event discriminator

۳-۵-۱۳

رویداد امنیتي[1]

هر رویدادی که به‌وسیله‌ی خط مشی امنیتی به‌عنوان یک حفره امنیتی بالقوه تعریف شده باشد و یا این که ارتباط امنیتی خاصی داشته باشد. دستیابی به یک میزان آستانه از پیش تعیین شده نمونه‌ای از یک رویداد مرتبط با امنیت است.

۳-۵-۱٤

پیام ممیزي امنیت

پیامی که در نتیجه یک رویداد امنیتی قابل ممیزی تولید می‌شود.

۳-۵-۱۵

سابقه ممیزي امنیت

یک تک سابقه در دنباله ممیزی امنیت.

۳-۵-۱٦

ممیز امنیت[2]

یک هستار منفرد یا یک فرآیند که اجازه‌ی دسترسی به دنباله‌ی ممیزی امنیت را برای ساخت گزارش‌های ممیزی دارد.

۳-۵-۱۷

گزارش امنیتي[3]

گزارشی که نتیجه بررسی دنباله‌ی ممیزی امنیت بوده و می‌توان برای تعیین این که آیا یک حفره امنیتی رخ داده است یا خیر از آن استفاده کرد.

٤ کوته‌نوشت‌ها

OSI	Open System Interconnection	اتصال متقابل سامانه‌های باز

۵ نشانه‌گذاري[4]

اصطلاحات «خدمت» و «سازوکار» به ترتیب برای ارجاع به «خدمت ممیزی امنیت» و «سازوکار ممیزی امنیت» به کار می‌روند مگر آنکه معنی دیگری مد نظر باشد. اصطلاح «ممیزی» به «ممیزی امنیت» ارجاع دارد مگر آنکه معنی دیگری مد نظر باشد. و اصطلاح «هشدار» به «هشدار امنیتی» ارجاع دارد مگر آنکه معنی دیگری مد نظر باشد.

1 - Security related event
2 - Security auditor
3 - Security report
4 - Notation

٦ بحث کلي در مورد ممیزي امنیت و هشدارها

این بند مدلی برای برخورد با هشدارهای امنیتی و ساخت یک ممیزی امنیت برای سامانه‌های باز را توضیح می‌دهد.

یک ممیزی امنیت این اجازه را می‌دهد که میزان کفایت خط مشی امنیتی ارزیابی شود، در تشخیص تخلف‌های امنیتی کمک کرده و به افراد کمک می‌کند تا پاسخ گوی اعمال خود باشند (و یا اعمالی که به‌وسیله‌ی سایر هستارها اما از جانب آن‌ها انجام می‌شوند)، به تشخیص استفاده نادرست از منابع کمک کرده و در مقابل افرادی که در تلاشند به سامانه آسیب برسانند نقش بازدارنده را ایفا می‌کند. سازوکارهای ممیزی امنیت به‌طور مستقیم در جلوگیری از تخلف‌ها از امنیت مورد استفاده قرار نمی‌گیرند: این سازوکارها به تشخیص، ثبت و تحلیل رویدادها می‌پردازند. این امر اجازه تغییر به روال‌های عملیاتی را می‌دهد تا در جواب رویدادهای نامتعارف مانند تخلف‌های امنیتی پیاده‌سازی شوند.

یک هشدار امنیتی در پی تشخیص هر رویداد امنیتی که به‌وسیله‌ی خط مشی امنیتی یک شرط هشدار محسوب می‌شود، تولید می‌شود. این می‌تواند شامل دسترسی به یک آستانه از پیش تعیین شده باشد. برخی از این رویدادها ممکن است نیازمند عملیات بازیابی[1] سریع باشند در حالی که سایر رویدادها نیازمند تحقیقات بیشتری برای تعیین این که چه عملی باید انجام شود، هستند.

یک پیاده‌سازی مدل هشدار و ممیزی امنیت ممکن است از سایر خدمات امنیتی برای پشتیبانی از خدمات ممیزی و هشدارهای امنیتی و همچنین برای اطمینان از صحت عمل، استفاده کند. این موضوع در بند ۱۰ بیشتر مورد بررسی قرار گرفته است.

اگر چه دنباله ممیزی امنیت و ممیزی‌های امنیتی خصوصیات منحصر به فردی دارند، دیگر دنباله‌های ممیزی (غیر امنیتی) و ممیزی‌ها ممکن است از سازوکارها و تسهیلات توضیح داده شده در این چارچوب کاری بهره ببرند.

با توجه به سایر جنبه‌های امنیت، بیشینه کارایی با اطمینان از این که الزامات ممیزی امنیت خاص در سامانه طراحی شده است یا خیر، حاصل می‌شود. بنابراین تولیدکنندگان سامانه‌ها باید به ممیزی‌پذیری[2] (یعنی آماده‌ی آزمون و تحلیل بودن) فرآیند طراحی و سامانه در دست توسعه، توجه داشته باشند.

یادآوری- مدل ممیزی و هشدارهای امنیتی چگونگی ارتباط سایر تسهیلات عملیاتی و مدیریتی با این مدل را نشان نمی‌دهد.

٦-١ مدل و کارکردها

مدلی که در زیر نشان داده می‌شود کارکردهایی را نشان می‌دهد که برای تامین یک ممیزی امنیت و خدمت هشدارها مورد استفاده قرار می‌گیرد.

1 - Recovery
2 - Auditability

۶-۱-۱ کارکردهاي ممیزي و هشدارهاي امنیتي

عملیات مختلفی برای پشتیبانی از ممیزی امنیت و خدمت هشدار، ضروری هستند که عبارتند از:

- **تفکیک‌کننده رویداد،** که تحلیل اولیه رویداد را فراهم کرده و تشخیص می‌دهد که آیا رویداد را به ثبت‌کننده ممیزی یا پردازنده هشدار بفرستد یا خیر؛
- **ثبت‌کننده ممیزی،** که سوابق ممیزی را از پیام‌های رسیده تولید می‌کند و در دنباله ممیزی امنیت آن‌ها را ذخیره می‌کند؛
- **پردازشگر هشدار،** که هم پیام ممیزی و هم عمل مناسب در پاسخ به یک هشدار امنیتی را تولید می‌کند؛
- **تحلیل‌گر ممیزی،** که دنباله ممیزی امنیت را بررسی کرده و در صورت نیاز هشدارها و پیام‌های ممیزی امنیت را ایجاد خواهد کرد؛
- **آزمون‌گر دنباله ممیزی،** که گزارش‌های امنیتی را از روی یک یا بیش از یک دنباله ممیزی امنیت تهیه می‌کند؛
- **فراهم‌کننده ممیزی،** که سوابق ممیزی را مطابق با ضوابط خاص تولید می‌کند؛ و
- **بایگانی‌کننده ممیزی،** که بخش‌هایی از یک دنباله ممیزی را بایگانی می‌کند.

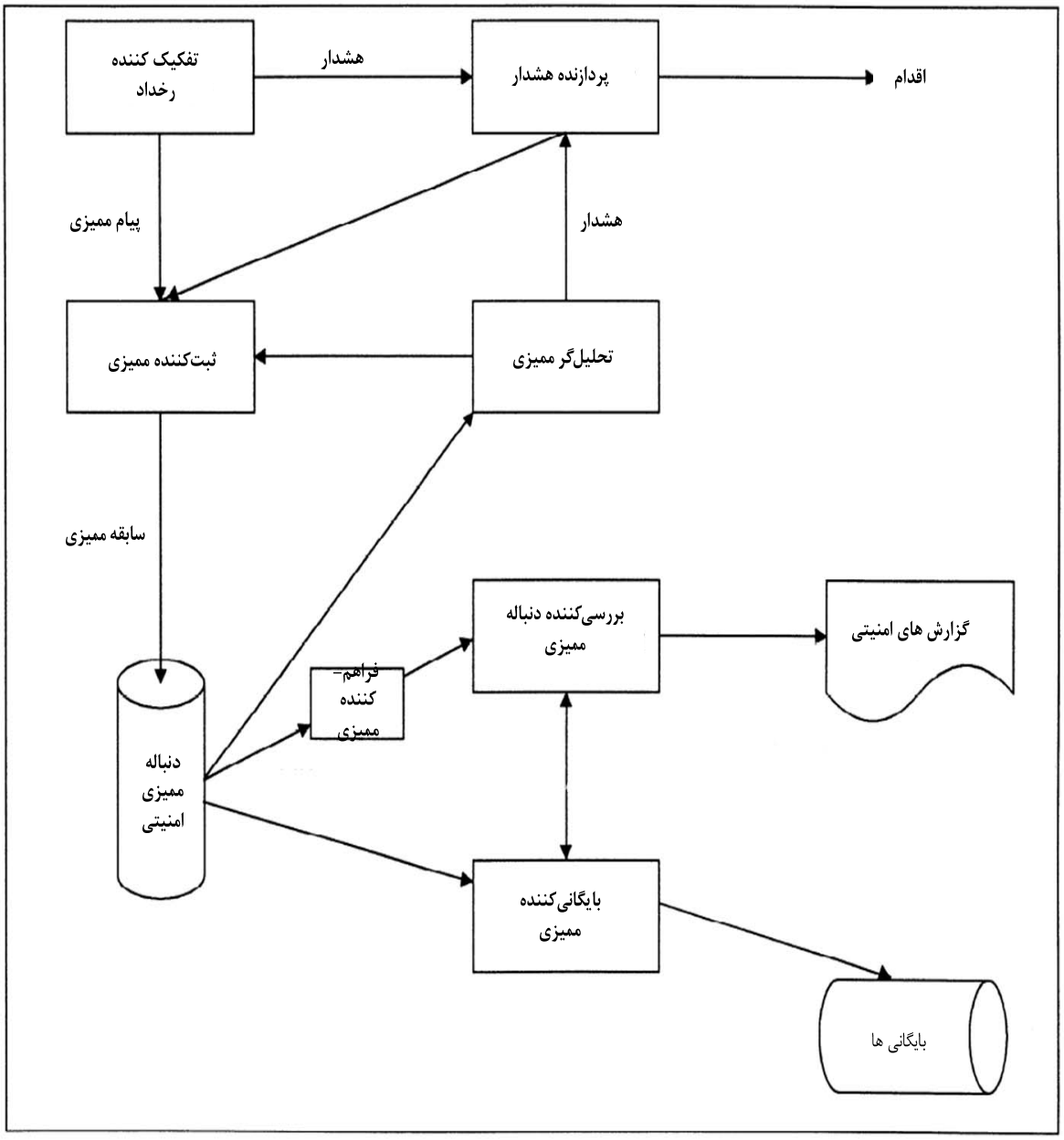
ممکن است کارکردهای بیشتری نیز برای پشتیبانی از دنباله‌های ممیزی و هشدارهای امنیتی توزیع‌شده مورد نیاز باشند که عبارتند از:

- **جمع‌آوری کننده دنباله ممیزی،** که سوابق را از دنباله ممیزی توزیع‌شده به درون یک دنباله ممیزی امنیت می‌آورد؛
- **توزیع‌کننده ممیزی،** که بخش‌هایی یا همه یک دنباله ممیزی امنیت توزیع‌شده را به کارکرد جمع‌آوری کننده دنباله ممیزی منتقل می‌کند.

۶-۱-۲ مدل ممیزي و هشدارهاي امنیتي

مدل ممیزی و هشدارهای امنیتی که در زیر رسم شده است شامل چندین گام است. پس از تشخیص یک رویداد، این مهم که آیا رویداد امنیتی است یا خیر، باید تعیین شود. *تفکیک‌کننده رویداد*، رویداد را ارزیابی می‌کند تا تعیین نماید که آیا یک پیام ممیزی امنیت و/یا یک پیام هشدارهای امنیتی باید تولید شود یا خیر. پیام‌های ممیزی امنیت به *ثبت‌کننده‌ی ممیزی* ارسال می‌شوند: هشدارهای امنیتی به *پردازنده هشدار* برای ارزیابی و عملیات بیشتر فرستاده می‌شوند. سپس پیام‌های ممیزی امنیت برای قرار گرفتن در دنباله ممیزی امنیت، به قالبی خاص در آمده و به سوابق ممیزی امنیت تبدیل می‌شوند. بخش‌های قدیمی‌تر دنباله ممیزی امنیت ممکن است بایگانی شده و سپس هر دوی دنباله ممیزی امنیت و بایگانی‌های دنباله ممیزی امنیت ممکن است برای تهیه گزارش‌های ممیزی مورد استفاده قرار گیرند که این کار با انتخاب سوابق خاصی از دنباله ممیزی امنیت مطابق با معیارهایی مشخص انجام می‌شود. به این معنی که دنباله ممیزی امنیت ممکن است

تحلیل شده و گزارش‌های ممیزی امنیت و/یا هشدارهای امنیتی تولید شوند. مدل ممیزی و هشدارهای امنیتی در شکل ۱ نشان داده شده است.



شکل ۱ - مدل ممیزی امنیت و هشدارها

۶-۱-۳ گروه‌بندي كاركردهاي ممیزي و هشدارهاي امنیتي

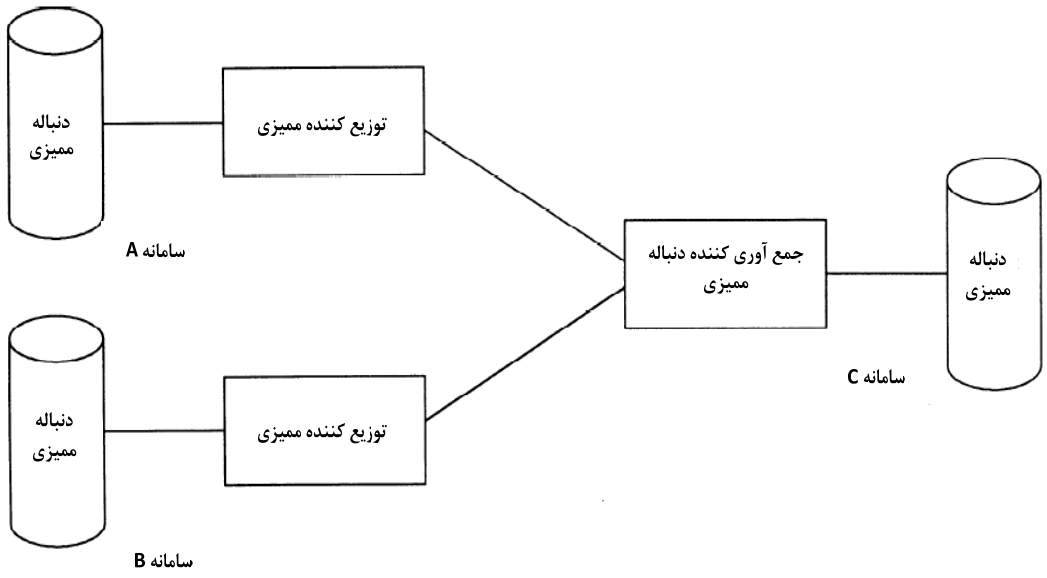
کارکردهایی که در مدل نشان داده شده‌اند، ممکن است در یک جزء از یک سامانه و یا به‌صورت توزیع‌شده بین چ ... سامانه بکار روند. این کارکردها همچنین ممکن است در سامانه‌های انتهایی متفاوتی قرار داده

شده و تکثیر شوند. در برخی موارد، از جمله برای ملاحظات کارایی، گروه‌بندی این عملیات مفید خواهد بود. به خصوص، یک *ثبت‌کننده ممیزی*، یک *توزیع‌کننده ممیزی*، یک *فراهم‌کننده ممیزی* و یک *تحلیل‌گر ممیزی* که همگی بر روی یک دنباله‌ی ممیزی امنیت کار می‌کنند ممکن است بخشی از یک سامانه‌ی انتهایی بدون مراقبت را تشکیل دهند.

گروه‌بندی دیگر می‌تواند یک *بررسی‌کننده دنباله ممیزی* و یک *تحلیل‌گر ممیزی* باشد که برای ممیز امنیتی سودمند هستند.

ممکن است یک زنجیره از کارکردها که به‌صورت سلسله‌مراتبی، مرتب[1] شده‌اند، به‌خصوص در یک دنباله ممیزی امنیت توزیع‌شده وجود داشته باشد. (به شکل ۲ مراجعه شود). در اینجا یک *جمع‌آوری‌کننده دنباله ممیزی* از یک جزء، پیام‌های ممیزی را از *توزیع‌کننده ممیزی* یک جزء دیگر جمع‌آوری می‌کند. این زنجیره زمانی به پایان می‌رسد که یک جزء از یک *توزیع‌کننده ممیزی* پشتیبانی نکند: در این مورد، آن جزء باید از یک *بایگانی‌کننده ممیزی* پشتیبانی کند تا بتواند دنباله ممیزی امنیت خود را بایگانی کند.

تصمیم در مورد این که چه کارکردهایی گروه‌بندی شوند موضوعی در رابطه با پیاده‌سازی است. مثال‌های فوق، تنها به‌عنوان نمونه‌هایی جهت یادگیری معرفی می‌شوند.



شکل ۲ - مدل دنباله‌ی ممیزی توزیع‌شده

۲-۶ مراحل مربوط به روال‌هاي ممیزي امنیت و هشدارها

خدمت ممیزی امنیت یک مرجع ممیزی را ایجاد می‌کند که توانایی تعیین و انتخاب رویدادهای نیازمند تشخیص و ثبت در یک دنباله ممیزی امنیت و رویدادهایی که نیازمند فعال کردن یک هشدار امنیتی و پیام‌های ممیزی امنیت هستند را دارد.

1 - Arrange

مراحل زیر ممکن است در روال‌های ممیزی به وجود آیند:

- مرحله تشخیص، که در آن یک رویداد امنیتی تشخیص داده می‌شود؛
- مرحله تفکیک، که در آن یک تعیین اولیه برای این که آیا ثبت یک رویداد در دنباله ممیزی امنیت یا فعال‌کردن یک هشدار ضروری است یا خیر، انجام می‌پذیرد؛
- مرحله پردازش هشدار، که در آن یک هشدار امنیتی یا پیام ممیزی امنیت ممکن است صادر شود؛
- مرحله تحلیل، که در آن یک رویداد امنیتی با توجه به رویدادهای از قبل تشخیص داده شده که سابقه آن‌ها در دنباله ممیزی ثبت شده و عملیاتی که برای آن‌ها تعیین شده است، ارزیابی می‌شود؛
- مرحله انبوهش[1]، (جمع‌آوری) که در آن سوابق دنباله ممیزی امنیت توزیع‌شده درون یک دنباله ممیزی امنیت جمع‌آوری می‌شوند؛
- مرحله گزارش‌گیری، که در آن گزارش‌های ممیزی از روی سوابق دنباله ممیزی امنیت تهیه می‌شوند؛ و
- مرحله بایگانی، که در آن سوابق از دنباله ممیزی امنیت به بایگانی دنباله ممیزی امنیت منتقل می‌شوند.

مراحل توصیف شده در بالا، در یک زمان در صورت لزوم از یکدیگر مجزا نیستند به این معنی که ممکن است با یکدیگر هم‌پوشانی داشته باشند.

٦-٢-١ مرحله تشخیص[2]

مرحله تشخیص، تعیین آن که یک رویداد امنیتی ممکن است رخ داده شده باشد را در بردارد. تعیین این که چه عملی در پاسخ به این رویداد باید انجام شود، وظیفه *تفکیک‌کننده رویداد* (به بند ۶-۲-۲ مراجعه شود) بوده اما در برخی موارد، همانطور که به‌وسیله‌ی خط مشی امنیتی تعیین شده، ممکن است یک هشدار آنی ایجاد شود.

٦-٢-٢ مرحله تفکیک

هنگامی که یک رویداد امنیتی تشخیص داده می‌شود، تفکیک‌کننده رویداد عمل اولیه متناسب با آن را تعیین می‌کند. این عمل یکی از موارد زیر خواهد بود:

الف- هیچ اقدامی انجام نشود؛

ب- یک پیام ممیزی امنیت تولید شود؛ یا

پ- یک پیام ممیزی امنیت و یک هشدار امنیتی تولید شود؛

تصمیم در مورد این که کدام یک از اقدامات فوق باید برای هر رویدادی انجام شود، به خط مشی امنیتی استفاده شده وابسته است.

٦-٢-٣ مرحله پردازش هشدار

در مرحله پردازش هشدار، پردازنده هشدار، هشدار را برای تعیین عمل مناسب برای رویداد تحلیل می‌کند. عمل انجام شده یکی از موارد زیر است:

1 - Aggregation phase
2 - Detection phase

الف- هیچ اقدامی انجام نشود؛
ب- یک عمل بازیابی شروع شود؛ یا
پ- یک عمل بازیابی شروع شود و یک پیام ممیزی امنیت تولید شود.
تصمیم در مورد این که برای هر رویداد کدام یک از اقدامات فوق انجام شود، به خط مشی امنیتی در عملیات وابسته است.

یادآوری- موارد ب و پ ممکن است شامل قراردادن رویداد در معرض توجه یک شخص مانند یک کارمند امنیتی یا مدیر ممیزی باشد.

٦-٢-٤ مرحله تحلیل

در مرحله تحلیل، یک رویداد امنیتی برای تعیین عمل مناسب پردازش می‌شود. این پردازش همچنین می‌تواند از اطلاعات رویدادهای امنیتی قبلی که در دنباله ممیزی امنیت ثبت شده است استفاده کند. این اقدام شامل یکی از موارد زیر خواهد بود:
الف- هیچ اقدامی انجام نشود؛
ب- یک هشدار امنیتی تولید شود؛
پ- یک سابقه ممیزی امنیت تولید شود؛ یا
ت- یک هشدار امنیتی و یک سابقه ممیزی امنیت تولید شود؛
تصمیم در مورد این که کدام یک از اقدامات فوق باید برای هر رویدادی انجام شود، به خط مشی امنیتی استفاده شده وابسته است.
به‌عنوان قسمتی از فرآیند تحلیل، ممکن است با بررسی سوابق در دنباله ممیزی امنیت و بایگانی دنباله ممیزی امنیت به رویدادهای قبلی ارجاع داده شود.

٦-٢-٥ مرحله انبوهش

هر یک از سوابق ممیزی امنیت از یک دنباله ممیزی توزیع‌شده، باید به‌صورت دوره‌ای درون یک دنباله ممیزی جمع‌آوری شوند. این فرآیند که شامل استفاده از یک *جمع‌آوری‌کننده دنباله ممیزی* (در نقطه جمع‌آوری) و یک کارکرد توزیع‌کننده *ممیزی* (در سامانه‌های راه دور[1]) است انبوهش خوانده می‌شود (همان گونه که در ۶-۱-۳ بیان شد، این فرآیند می‌تواند به‌صورت سلسله‌مراتبی باشد).

٦-٢-٦ مرحله گزارش‌گیری

هنگامی که مطابق با خط مشی امنیتی نیاز یا اجبار وجود داشته باشد، دنباله ممیزی امنیت پردازش می‌شود. این پردازش عنصری از تحلیل و دست‌کاری سوابق دنباله ممیزی امنیت به قالب مناسب را شامل می‌شود. خروجی تحلیل یک دنباله ممیزی امنیت یک گزارش امنیتی است که ممکن است بیان کند که تلاشی برای سوء استفاده از حفره امنیتی انجام شده، به‌طوری که اعمال بازیابی مورد نیاز ممکن است انجام شوند. تحلیل

1 - Remote systems

دنباله ممیزی امنیت می‌تواند برای ارزیابی وسعت حمله و تعیین روال‌های کنترل خسارت مورد استفاده قرار گیرد.

یک گزارش امنیتی ممکن است به‌وسیله‌ی بازیابی امنیتی برای شناسایی وسعت خسارت ناشی از یک مشکل امنیتی مورد استفاده قرار گیرد. به خصوص ممکن است بتوان از آن برای شناسایی منابع استفاده شده به‌وسیله‌ی یک کاربر مجاز که به گونه‌ای ناهنجار از حق دسترسی خود بهره می‌برده است، استفاده نمود. همچنین، می‌توان برای ارزیابی هر نوع خسارت به گونه‌ای از آن استفاده نمود که فعالیت بازیابی مورد نیاز قابل انجام باشد.

٦-٢-٧ مرحله بایگانی

دنباله‌ی ممیزی امنیت ممکن است نیازمند به نگهداری طولانی مدت باشد. در مرحله بایگانی، قسمتی از یک دنباله‌ی ممیزی امنیت به یک فضای ذخیره‌سازی طولانی مدت منتقل می‌شود. حافظه مورد استفاده برای بایگانی باید یکپارچگی[1] سوابق اولیه را حفظ کند. بایگانی دنباله‌های ممیزی امنیت به‌صورت محلی و یا دور از منبع اولیه دنباله ممیزی انجام پذیرد. ممکن است مقرراتی برای بایگانی راه دور[2] ایجاد شود.

٦-٣ همبستگي اطلاعات ممیزي

سوابق ممیزی موجود در یک یا چند دنباله ممیزی امنیت ممکن است به هم وابسته باشند. برای مثال، یک درخواست اتصال ممکن است از تعدادی از سامانه‌های میانی عبور کرده و در نتیجه چندین سابقه ممیزی امنیت در دنباله‌های ممیزی امنیت مختلف تولید کند. مهم است که به این سوابق ممیزی امنیت به درستی برچسب زمانی زده شود و یا این که ارتباط درونی آن‌ها با یکدیگر مشخص گردد. مثالی دیگر، ثبت دو رویداد متفاوت در دو دنباله ممیزی امنیت است؛ که در آن تعیین این که کدام رویداد اول اتفاق افتاده است اهمیت دارد. بحثی در مورد مسائل مربوط به همبستگی زمان‌های رویدادها از تولیدکنندگان رویداد متفاوت در پیوست ت وجود دارد.

٧ خط مشي و سایر جنبه‌هاي ممیزي و هشدارهاي امنیتي

٧-١ خط مشي

یک خط مشی ممیزی امنیت، رویدادهای امنیتی را تعریف و قواعدی را برای اعمال بر روی مجموعه، ثبت (در یک دنباله‌ی ممیزی) و تحلیل رویدادهای مختلف امنیتی شناسایی می‌کند. ملاحظاتی وجود دارند که ممکن است در خط مشی‌های ممیزی و نمایش آن‌ها به‌صورت قواعد وجود داشته باشند. یک یا بیش از یکی از این ملاحظات ممکن است به خط مشی امنیتی ویژه‌ای قابل اعمال باشد.

یک خط مشی ممیزی امنیت باید الزاماتی را برای اجرای ممیزی امنیت در سطوح و گونه‌های مختلف تعریف کرده و باید علاوه بر این، معیارهایی را نیز برای تولید هشدارهای امنیتی تعریف کند. آزمایش کفایت کنترل‌های

1 - Intgrity
2 - Remote archiving

سامانه، تایید انطباق با خط مشی امنیتی، و تعیین تغییرات مشخص در خط مشی، کنترل‌ها و روال‌ها نیازمند تحلیل سوابق دنباله‌ی ممیزی امنیت و بسیاری از جنبه‌های طراحی، پیکربندی و عملکرد سامانه‌ها است.

یادآوری- روش تعریف رویدادهای امنیتی در یک خط مشی امنیتی خارج از حوزه این توصیه‌نامه | استاندارد ملی است.

۲-۷ جنبه‌هاي قانوني

در بسیاری از کشورها، قوانینی برای محافظت از حریم خصوصی[1] شهروندان طراحی شده است. در برخی موارد این بدان معنی است که یک سابقه دنباله ممیزی که شامل اطلاعاتی درباره ماهیت شخصی است، در چارچوب کاری قوانین ملی از جمله آنهایی که با حریم خصوصی و دسترسی به اطلاعات درباره ماهیت شخصی مربوط است قرار می‌گیرد، این سوابق نیازمند محافظت در برابر فاش سازی‌های غیر مجاز هستند.

جایی که سوابق ممیزی امنیت به‌عنوان مدارک قانونی قابل پذیرش مورد استفاده قرار می‌گیرند، الزامات خاصی ممکن است با توجه به استفاده، ذخیره و محافظت از سوابق ممیزی امنیت وجود داشته باشد.

۳-۷ الزامات محافظتي

دو جنبه از محافظت ممکن است مد نظر باشد:

- محافظت از دنباله ممیزی امنیت و اطلاعات ممیزی؛ و
- محافظت از خدمات ممیزی امنیت.

۱-۳-۷ محافظت از اطلاعات ممیزي

اطلاعات جمع‌آوری شده در دنباله ممیزی امنیت ممکن است مستقیما از پیام‌های ممیزی یا از سایر دنباله‌های ممیزی امنیت بدست آمده باشند. از این رو یک دنباله ممیزی امنیت ممکن است مجموعه‌ای[2] از سوابق ممیزی امنیت تولید شده به‌وسیله‌ی یک یا چند منبع باشد. در ساده‌ترین مورد، یک دنباله ممیزی امنیت شامل تمامی سوابق ممیزی امنیت تولید شده به‌وسیله‌ی یک سامانه است.

دنباله ممیزی امنیت باید در برابر انتشار غیرمجاز و/یا تغییر غیرمجاز محافظت شود. سازوکارهای کنترل دسترسی، محرمانگی، یکپارچگی و احراز هویت ممکن است برای محافظت از آن، مورد نیاز باشد. به علاوه، مهم است که فرستنده و گیرنده اطلاعات مطمئن باشند که مبدأ و مقصد داده‌ها همان‌هایی هستند که ادعا شده است و به اطلاعات هیچ گونه خدشه‌ای وارد نشده است.

محرمانگی ممکن است برای حداقل برخی از اطلاعات مورد نیاز باشد. این می‌تواند به چند دلیل باشد:

- جنبه‌های قانونی با توجه به حریم خصوصی؛
- مخفی کردن این که چه رویدادهای ممیزی ثبت شده یا نشده‌اند؛
- مخفی کردن هویت دریافت کنندگان (یا آن‌ها که دریافت کننده نیستند) اقدامات ناشی از هشدارها.

1 - Privacy
2 - Set

۷-۳-۲ محافظت از خدمت هشدارها و ممیزي

خدمت هشدارها و ممیزی امنیت وابسته به سطحی بالا از دسترس‌پذیری است. انکار خدمت مخاطره‌ای است که متوجه خدمت هشدارها و ممیزی می‌شود. اطلاعات مورد توجه یک مدیر هشدار امنیتی یا ممیز امنیتی می‌تواند تا جایی که اطلاعات دیگر ارزشی نداشته باشند، به تعویق بیافتند. بسیار مهم است که اطلاعات به مخاطب مورد نظر به موقع برسد.

بحث بیشتر در مورد این جنبه‌ها از محافظت ممکن است در بند۱۰ یافت شود.

۸ تسهیلات و اطلاعات مربوط به هشدارها و ممیزي امنیت

برای پردازش اطلاعات هشدارها و ممیزی امنیت دو دیدگاه در نظر گرفته می‌شود:

- پردازش پیام‌های تولید شده در پاسخ به یک رویداد غیرمترقبه (یعنی اطلاعات هشدارها و ممیزی امنیت ناخواسته)؛ و

- پردازش درخواست‌ها برای اطلاعات هشدارها و ممیزی امنیت مشخص (یعنی اطلاعات درخواست شده).

مدیریت خدمات برای کنترل جنبه‌های مختلف پردازش هشدارها و ممیزی امنیت شامل سازوکارهای دنباله‌ی ممیزی امنیت، معیارهایی برای انجام عملیات خاصی پس از تشخیص یک رویداد امنیتی و فرآیندهایی که شامل برخورد با اطلاعات هشدارها و ممیزی هستند مورد نیاز است.

۸-۱ اطلاعات هشدارها و ممیزي

اطلاعات هشدارها و ممیزی شامل هشدارهای امنیتی، پیام‌های ممیزی امنیت، سوابق ممیزی امنیت و گزارش‌های امنیتی هستند.

۸-۱-۱ پیام‌هاي ممیزي امنیت

یک *پیام ممیزی امنیت*، پیامی است که در نتیجه‌ی یک رویداد امنیتی قابل ممیزی تولید می‌شود. یک پیام ممیزی امنیت ممکن است به‌عنوان مثال از تحلیل اولیه‌ی یک رویداد امنیتی به‌وسیله‌ی تفکیک‌کننده‌ی رویداد یا در نتیجه‌ی ارزیابی انجام شده به‌وسیله‌ی پردازنده هشدار یا تحلیل‌گر ممیزی تولید شود.

۸-۱-۲ سوابق ممیزي امنیت

اصطلاح «*سابقه امنیتی*» برای توصیف یک تک سابقه در دنباله‌ی ممیزی امنیت بکار می‌رود. در بسیاری از موارد، معادل یک رویداد امنیتی بوده اما در برخی پیاده‌سازی‌ها نیز که یک سابقه ممیزی امنیت در نتیجه‌ی بیش از یک رویداد امنیتی تولید می‌شود، قابل درک است. یک سابقه دنباله‌ی ممیزی امنیت معمولی شامل اطلاعاتی درباره‌ی مبدأ و دلیل پیام بوده و ممکن است شامل اطلاعاتی درباره‌ی هستارهای درگیر در تشخیص و پردازش پیام نیز باشد.

۸-۱-۳ هشدارهاي امنیتي

یک *هشدار امنیتی* پیامی است که در پی تشخیص یک رویداد امنیتی که معلوم شده به‌صورت بالقوه یک حفره‌ی امنیتی است و شرایط یک هشدار را دارد، تولید می‌شود. این امر ممکن است یک رویداد یا نتیجه‌ی

رسیدن به یک آستانه باشد. در هر یک از موارد مذکور، تعریف آنچه که یک شرط هشدار را دارد در خط مشی امنیتی مشخص می‌شود.

هشدارهای امنیتی ممکن است به وسیله تفکیک‌کننده‌ی رویداد (در نتیجه‌ی بررسی اولیه‌ی یک رویداد امنیتی) یا به‌وسیله‌ی یک تحلیل‌گر ممیزی، در هر زمانی، در صورت وجود یک شرط هشدار شروع شود.

۸-۱-٤ گزارش‌هاي امنيتي

گزارش‌های امنیتی اطلاعاتی هستند که در نتیجه‌ی تحلیل دنباله‌ی ممیزی امنیت تولید می‌شوند. *بررسی‌کننده‌ی دنباله‌ی ممیزی* برای تولید گزارش از یک یا چند دنباله‌ی ممیزی امنیت مورد استفاده قرار می‌گیرد.

۸-۱-٥ نمونه‌اي از تركيب اطلاعات هشدارها و ممیزي

اطلاعات هشدارها و ممیزی به‌طور معمول شامل موارد زیر است:

- نوع پیام/اطلاعات (یعنی هشدار امنیتی، پیام ممیزی امنیت یا گزارش امنیتی)؛
- شناسه تشخیص عناصر (مانند شروع‌کننده/هدف رویداد امنیتی، موضوع/شئ[1] اقدام)؛
- علت پیام؛
- شناسه‌های تشخیص مربوط به *تفکیک‌کننده‌ی رویداد*، *فراهم کننده‌ی ممیزی* و یا *ثبت‌کننده‌ی ممیزی*.

۸-۲ تسهیلات هشدارها و ممیزي امنیت

به منظور اعمال ممیزی و اجازه دادن به انجام تحلیل رویداد به‌صورت کارا، روشی برای تعیین این که کدام رویدادها امنیتی است و چگونه باید پردازش شوند، مورد نیاز است. تحلیل پیام‌ها به‌وسیله‌ی یک سازوکار پالایش انجام می‌شود که اعمال مناسب پس از دریافت یک پیام ممیزی برای انجام دادن را مشخص می‌کند. پالایه[2] بر طبق معیارهایی (که به‌وسیله مرجع امنیتی تعیین می‌شوند) انجام می‌پذیرد که عملیات مربوط به هر نوع پیام را مشخص می‌کنند. معیارهایی که ممکن است مورد استفاده باشند، عبارتند از:

- زمان وقوع در طول روز؛
- یک شمارنده‌ی آستانه؛
- نوع رویداد؛ و
- هستار پدید آورنده‌ی رویداد.

برای نیل به اهداف مدیریتی، پالایه به‌عنوان یک مورد مدیریت شده با رفتار و پارامترهای خاص تعریف می‌شود. تسهیلات مدیریتی هشدارها و ممیزی، ابزاری برای پیاده‌سازی و انتخاب معیارها فراهم می‌سازند که به کاربر اجازه می‌دهد اطلاعات مورد نیاز برای فراهم کردن خدمات هشدارها و ممیزی را پردازش کند. به‌طور کلی این تسهیلات عبارتند از:

الف- ایجاد، تغییر و حذف معیارها برای پردازش رویدادهای مرتبط با امنیت؛

1 - Subject/object
2 - Filter

ب- فعال و غیرفعال‌سازی تولید پیام‌های ممیزی امنیت مشخص‌شده؛
پ- فعال و غیرفعال‌سازی تولید دنباله‌های ممیزی امنیت؛
ت- فعال و غیرفعال‌سازی تولید و پردازش هشدارها.
تسهیلات عملیاتی هشدارها و ممیزی عبارتند از:
الف- تولید اطلاعات هشدارها و ممیزی (مانند تولید هشدار، تولید پیام ممیزی، تولید گزارش ممیزی)؛
ب- ثبت اطلاعات هشدارها و ممیزی؛
پ- جمع‌آوری اطلاعات هشدارها و ممیزی؛
ت- تحلیل اطلاعات هشدارها و ممیزی؛ و
ث- بایگانی اطلاعات هشدارها و ممیزی.

۸-۲-۱ تعیین و تحلیل رویدادهاي امنیتي- معیارهایي براي عملیات هشدارها و ممیزي

هم یک هشدار امنیتی و هم یک پیام ممیزی امنیت نوع رویداد، مسبب رویداد، زمان تشخیص رویداد، هویت تشخیص دهنده‌ی رویداد و هویت هستارهای مرتبط با رویداد (یعنی موضوع و شئ، عملی که منجر به وقوع رویداد می‌شوند) را مشخص می‌کنند. معیارها برای تعیین عملی که هنگام پردازش انواع مختلفی از اطلاعات باید انجام شود، مشخص می‌شود. معیارهای تعریف شده عبارتند از:

معیار ۱ - تفکیک رویداد

این معیارها عملی را که پس از تشخیص یک رویداد امنیتی باید انجام شود، تعیین می‌کنند.

پارامترهای ورودی کاندید[1]:

- نوع رویداد امنیتی؛
- زمان وقوع؛
- هستار مسبب رویداد.

پارامتر خروجی کاندید:

- عملی که باید انجام شود؛
- هشدار امنیتی که باید تولید شود؛
- پیام ممیزی امنیت که باید تولید شود.

معیار ۲- بررسی دنباله‌ی ممیزی

این معیارها مبنایی برای انتخاب اطلاعات موجود در یک یا چند دنباله‌ی ممیزی امنیت را برای ترجمه گزارش‌های امنیتی مهیا می‌کنند.

پارامترهای ورودی کاندید:

- نوع سابقه ممیزی؛

1 - Candidate input parameters

- نوع رویداد امنیتی؛
- زمان رویداد تحت بازنگری؛
- هستاری که اطلاعاتی در مورد آن درخواست می‌شود.

پارامترهای خروجی کاندید:

- فهرستی از سوابق انتخاب شده؛

معیار ۳- معیار تحلیل دنباله‌ی ممیزی

این معیارها چگونگی پردازش دنباله‌ی ممیزی به‌وسیله‌ی تحلیل‌گر ممیزی را مشخص می‌کند. دنباله‌های ممیزی با ارزیابی وقوع و فراوانی رویداد قبل از تعیین عملی که باید انجام شود، تحلیل خواهند شد.

پارامترهای ورودی کاندید:

- نوع رویداد؛
- تعداد دفعات وقوع؛
- دوره‌ی زمانی؛

پارامترهای خروجی کاندید:

- اقدامی که باید انجام شود

یادآوری- برای ثبت ممیزی امنیت یا بایگانی ممیزی امنیت، معیارها مورد نیاز نمی‌باشند.

۹ سازوکارهاي هشدارها و ممیزي امنیت

خدمت هشدارها و ممیزی امنیت با سایر خدمات امنیتی توصیف شده در این خانواده از استانداردهای ملی فرق دارد. به این دلیل که هیچ سازوکار امنیتی خاصی وجود ندارد که برای فراهم کردن این خدمت مورد استفاده قرار گیرد. سازوکارهای ممیزی ممکن است به‌عنوان روال‌هایی مبتنی بر تعدادی رهیافت[1] عملیاتی و مدیریتی مشخص شوند. اما به‌عنوان مثالی از انواع رهیافت‌های مورد استفاده برای ممیزی، سازوکارهای مورد استفاده برای تحلیل رویداد امنیتی ممکن است شامل موارد زیر باشد:

- مقایسه‌ی فعالیت یک هستار با یک نمایه[2] شناخته شده مانند دسترسی غیرمتعارف مبتنی بر زمان و جغرافیا، استفاده‌ی نامتعارف از منابع و غیره؛
- تشخیص انباشتگی یک یا چند نوع رویداد در برخی بازه‌های زمانی؛
- مشاهده‌ی عدم وقوع یک یا چند نوع رویداد در برخی بازه‌های زمانی.

نمونه‌های فوق نمونه‌های کاملی نیستند.

1 - Approach
2 - Profile

۱۰ تعامل با سایر خدمات و سازوکارهاي امنيتي

۱۰-۱ احراز هویت هستار

انتقال دنباله‌ی ممیزی بین یک *توزیع‌کننده‌ی ممیزی* و یک *جمع‌آوری کننده‌ی ممیزی* نیازمند احراز هویت متقابل است به‌طوری که توزیع‌کننده‌ی ممیزی دنباله‌ی ممیزی را برای یک *جمع‌آوری کننده‌ی* مورد نظر فرستاده و *جمع‌آوری کننده‌ی ممیزی* دنباله‌ی ممیزی را از یک توزیع‌کننده‌ی مورد نظر دریافت می‌کند.

۱۰-۲ احراز هویت مبدأ داده‌ها

احراز هویت مبدأ داده‌ها برای این که مبدأ پیام‌های ممیزی امنیت و هشدارهای امنیتی شناخته شود، مورد استفاده قرار می‌گیرد. این خدمات همچنین به‌وسیله‌ی تحلیل‌گر ممیزی نیز برای اطمینان از این که پیام‌های یک تولیدکننده‌ی رویداد ناشناخته یا تحلیل‌گر ممیزی ناشناخته، رد می‌شوند، مورد استفاده قرار می‌گیرد.

۱۰-۳ کنترل دسترسي

خدمات کنترل دسترسی باید برای ذخیره و انتقال سوابق دنباله‌ی ممیزی امنیت استفاده شوند. کنترل دسترسی می‌تواند برای جلوگیری از دسترسی‌های غیرمجاز به دنباله‌ی امنیتی نیز مورد استفاده قرار گیرد.

۱۰-٤ محرمانگي

خدمات محرمانگی در طول انتقال دنباله‌های امنیتی، انتخاب سوابق ممیزی امنیت، پیام‌های ممیزی امنیت و هشدارهای امنیتی مورد استفاده هستند. خدمات محرمانگی همچنین می‌تواند برای محافظت از سوابق ممیزی ذخیره شده نیز مورد استفاده قرار گیرد.

۱۰-۵ یکپارچگي

مهم است که تغییرات غیرمجاز در دنباله‌ی ممیزی امنیت، یک مجموعه از سوابق ممیزی امنیت انتخاب شده، یک پیام ممیزی امنیت یا هشدار امنیتی تشخیص داده شود. می‌توان خدمت یکپارچگی را برای این منظور استفاده کرد.

۱۰-٦ انکارناپذیري[1]

از آنجا که انتقال دنباله‌های ممیزی امنیت به‌طور معمول در همان دامنه‌ی امنیتی انجام می‌شود، خدمت انکارناپذیری به طور معمول مورد استفاده قرار نخواهد گرفت.

1 - Non-repudiation

پیوست الف

اصول کلي هشدارها و ممیزي امنیت در OSI
(اطلاعاتي)

توصیه می‌شود که انواع ذیل از رویدادهای امنیتی همواره ممیزی شوند:
- عملیات مربوط به مدیریت اطلاعات امنیتی؛
- عملیاتی که مجموعه‌ی رویدادهایی که باید ممیزی شوند را تغییر می‌دهند؛ و
- عملیاتی که شناسایی موارد ممیزی شده را تغییر می‌دهند.

این پیوست رویدادهای OSI که بالقوه یک رویداد امنیتی هستند را مشخص می‌کند. هر دو شرایط عادی و غیرعادی ممکن است نیازمند آن باشند که ممیزی شوند، برای نمونه هر درخواست اتصال ممکن است بدون این که تشخیص داده شود درخواست غیرعادی بوده یا خیر و این که آیا درخواست مورد پذیرش واقع شده یا خیر، پدید آورنده‌ی یک سابقه دنباله‌ی امنیتی باشد.

رویدادهای ذیل ممکن است هدف ممیزی شدن باشند. این فهرست کامل نبوده و تنها برای راهنمایی ارائه شده است:

رویدادهای امنیتی مربوط به یک اتصال خاص:
- درخواست‌های اتصال؛
- تایید اتصال؛
- درخواست‌های قطع اتصال؛
- آمارهای وابسته به اتصال.

رویدادهای امنیتی مربوط به استفاده از خدمات امنیتی:
- درخواست‌های خدمات امنیتی؛
- استفاده از راه‌کارهای امنیتی؛
- هشدارهای امنیتی.

رویدادهای امنیتی مربوط به مدیریت:
- عملیات مدیریتی؛
- اعلان[1] امنیتی.

فهرست رویدادهای قابل ممیزی حداقل باید شامل موارد زیر باشد:
- رد دسترسی؛

1 - Notification

- احراز هویت؛
- تغییر صفات؛
- ساخت موارد؛
- حذف موارد؛
- اصلاح موارد؛
- استفاده از حقوق ویژه.

از نظر خدمات امنیتی تک، رویدادهای امنیتی زیر حائز اهمیت هستند:

- احراز هویت: درستی‌سنجی موفقیت؛
- احراز هویت: درستی‌سنجی شکست؛
- کنترل دسترسی: تصمیم در مورد موفقیت دسترسی؛
- کنترل دسترسی: تصمیم در مورد شکست دسترسی؛
- انکارناپذیری: انکارناپذیری مبدأ پیام؛
- انکارناپذیری: انکارپذیری دریافت‌کننده‌ی پیام؛
- انکارناپذیری: انکار ناموفق رویداد؛
- انکارناپذیری: انکار موفق رویداد؛
- یکپارچگی: استفاده با حفاظ[1]؛
- یکپارچگی: استفاده بی حفاظ؛
- یکپارچگی: اعتبارسنجی موفقیت؛
- یکپارچگی: اعتبارسنجی شکست؛
- محرمانگی: استفاده از پوشش[2]؛
- محرمانگی: استفاده از فاش‌سازی[3]؛
- ممیزی: انتخاب رویداد برای ممیزی؛
- ممیزی: عدم انتخاب رویداد برای ممیزی.
- ممیزی: تغییر معیار انتخاب رویداد ممیزی

یادآوری- هنگامی که از کنترل دسترسی به‌عنوان مبنای سازوکارهای یکپارچگی و محرمانگی استفاده می‌شود، سوابق ممیزی مربوط به «تصمیم در مورد شکست دسترسی» می‌توانند به‌صورت یک شناسه صریح برای نشان‌دادن تلاش انجام شده برای تخطی از یکپارچگی یا محرمانگی درآیند.

1 - Shield
2 - Hide
3 - Reveal

تمامی سوابق دنباله‌ی ممیزی که به یک نمونه‌ی ویژه از ارتباط مربوط می‌شوند، باید برای اطمینان از این که سوابق ردگیری می‌شوند، بدون ابهام تشخیص داده شوند.

خدمات توصیه‌نامه CCITT X.734 | ISO/IEC 10164-5 برای مدیریت رویدادهایی که پس از تفکیک‌کننده‌هایی رخ می‌دهند که معیارهای انتخاب رویدادهای امنیتی را مشخص می‌کنند و به یک ممیزی امنیت مرتبط هستند، مورد استفاده قرار می‌گیرند.

خدمات تولید گزارش از دنباله‌ی امنیتی موجود در توصیه‌نامه CCITT X.740 | ISO/IEC 10164-8 ممکن است به‌وسیله‌ی هستارهایی که پیام‌های ممیزی امنیت را تولید می‌کنند، استفاده شوند.

خدمات توصیه‌نامه CCITT X.735 | ISO/IEC 10164-6 برای تعیین انتخاب پیام‌های ممیزی امنیت که در دنباله‌های ممیزی ذخیره شده‌اند، استفاده می‌شوند.

خدمات تولید گزارش از هشدارهای موجود در توصیه‌نامه CCITT X.736 | ISO/IEC 10164-7 ممکن است به‌وسیله‌ی یک کاربرد دنباله‌ی ممیزی امنیت برای تولید هشدارهای امنیتی مورد استفاده قرار گیرد.

پیوست ب

تحقق مدل هشدارها و ممیزي امنیت
(اطلاعاتي)

عملیات مدل هشدارها و ممیزی امنیت در شکل ۱ نشان داده شده است. تمامی روال ممکن است بین سامانه‌های باز مجزا و زیادی توزیع شود، به این صورت که هر سامانه مسؤول یک یا چند جنبه از این روال است. نمونه‌ای از این در شکل ب-۱ نشان داده شده است.

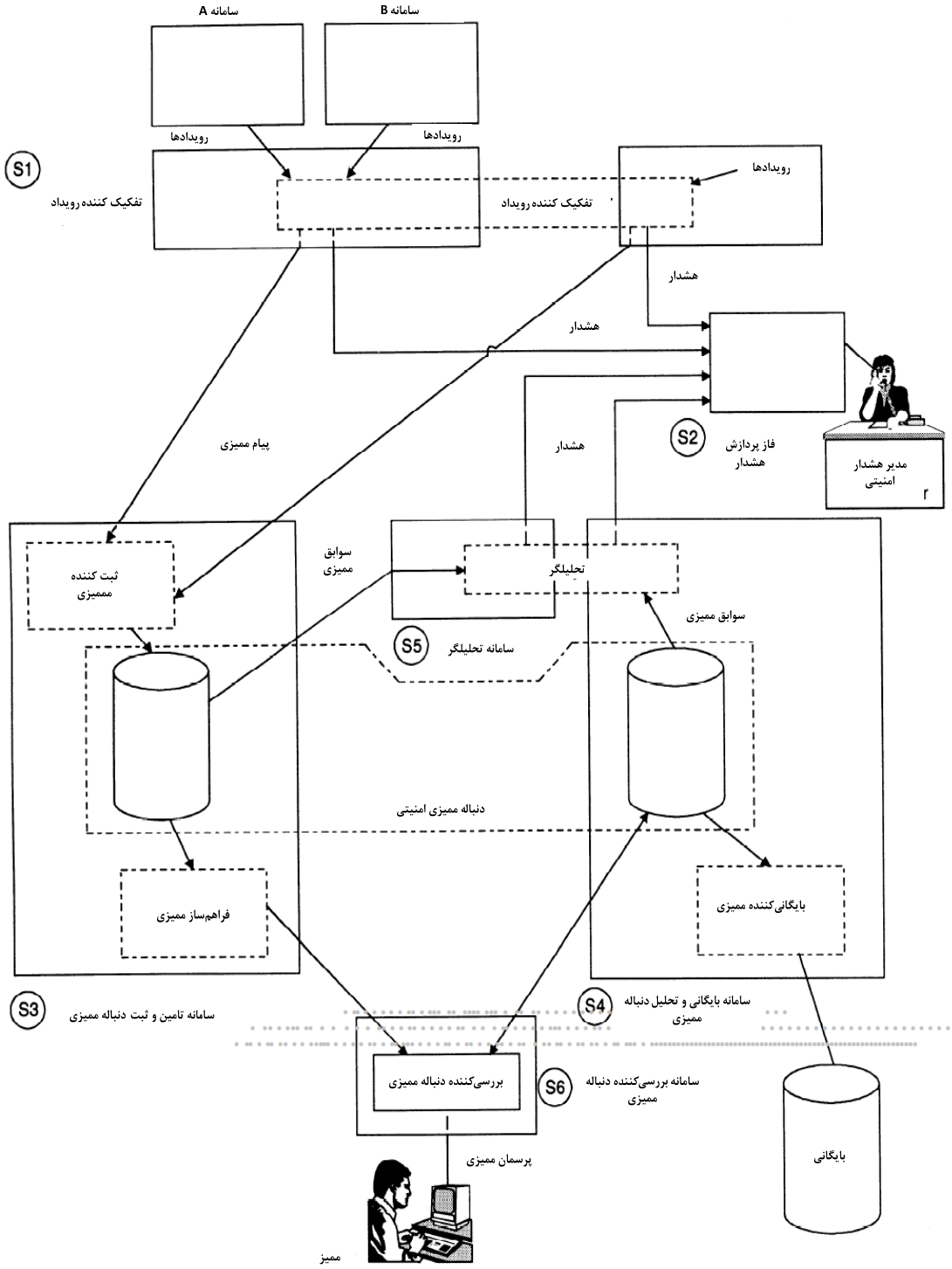
نمونه‌ای از یک رویداد امنیتی می‌تواند تلاش برای ورود به یک سامانه باشد که با استفاده از یک رمز عبور نامعتبر انجام شود. تحلیل دنباله‌ی ممیزی ممکن است افشا سازد که این یکی از مجموعه تلاش‌هایی است که برای ورود به حساب کاربری با یک رمزعبور نامعتبر انجام شده است و در صورت رسیدن به یک آستانه، هشداری فعال خواهد شد.

در شکل۱،S1 توانایی تشخیص رویدادهای امنیتی و تحلیل آن‌ها بر طبق معیارهای تعریف شده (معیار ۱) را داراست، اما هیچ عملی مربوط به دنباله‌ی ممیزی امنیت را ندارد، در نتیجه هشدارهای امنیتی‌اش به S2 و پیام‌های امنیتی‌اش به S3 فرستاده می‌شوند، تا در دنباله‌ی ممیزی امنیت قرار گیرند.

در این شکل، S3 مسؤول بروزرسانی دنباله‌ی ممیزی امنیت است و همچنین به S6 اجازه‌ی دسترسی به دنباله‌ی ممیزی امنیت و بایگانی‌های دنباله‌ی ممیزی امنیت را می‌دهد، به‌طوری که سوابق دنباله‌ی ممیزی امنیت بر طبق معیار تعریف شده (معیار ۲) انتخاب و درون یک گزارش امنیتی جمع می‌شوند.

قسمت S4 مسؤول بایگانی و بازیابی سوابق دنباله‌ی ممیزی است.

قسمت S5 کاربردی دارد که سوابق دنباله‌ی ممیزی را بر طبق معیار تعریف شده (معیار ۳) تحلیل کرده و هشدارها را به S2 هنگامی که حدود آستانه نقض گردیده یا سایر شرایط هشدار تشخیص داده شده است، می‌فرستد.



شکل ب-۱- مثالی از تحقق یک خدمت هشدار و ممیزی امنیت

پیوست پ

فهرست هشدارها و ممیزي امنیت (اطلاعاتي)

طرح کلی تسهیلات امنیتی			هستار ها: مرجع ممیزی؛ مدیر هشدار؛ ممیزی امنیتی.	عنصر
			کارکردها: تفکیک‌کننده‌ی رویداد؛ ثبت کننده‌ی ممیزی؛ پردازنده هشدار؛ تحلیلگر ممیزی؛ بررسی کننده‌ی دنباله‌ی ممیزی؛ فراهم کننده ممیزی؛ توزیع کننده‌ی ممیزی؛ جمع‌کننده‌ی دنباله‌ی ممیزی	
			موارد اطلاعاتی: پیام‌های ممیزی امنیت؛ سوابق ممیزی امنیت؛ گزارش‌های امنیتی.	
			هدف خدمت: برای این که سامانه‌های باز اطلاعاتی از ثبت اطلاعات امنیتی و گزارش آن‌ها در زمان مناسب مطمئن شوند.	
تسهیلات	هستار		مرجع ممیزی	
	کارکرد		تعیین و تحلیل رویدادهای امنیتی	
	فعالیت‌های مدیریتی		معیار ۱: تفکیک دادن رویداد معیار ۲: بررسی دنباله‌ی ممیزی معیار ۳: تحلیل دنباله‌ی ممیزی	
	هستار	مدیر هشدار	ممیز امنیتی	آغازگر/هدف موضوع/شئ
	کارکرد	تفکیک‌کننده‌ی رویداد پردازشگر هشدار تحلیل‌گر ممیزی	رویداد تفکیک‌کننده تحلیل‌گر ممیزی ثبت کننده ممیزی دنباله ممیزی بررسی کننده فراهم کننده ممیزی بایگانی کننده ممیزی	
	تسهیلات عملیاتی	تولید INFO. جمع‌آوری INFO. (INFO به‌معنی هشدار است)	تولید INFO. جمع‌آوری INFO. تحلیل INFO. (INFO به‌معنی هشدار است)	

اطلاعات	عناصر داده مدیریت‌شده با استفاده از مرجع ممیزی	معیار ۱ - نوع رویداد - زمان - هستار	معیار ۲ - نوع ثبت - نوع رویداد	معیار ۳ - نوع رویداد - تعداد وقوع - دوره زمانی
		- عملی که باید انجام شود. - اطلاعات امنیتی که باید تولید شود.	- فهرست سوابق	- عملی که باید انجام شود.
	نوع اطلاعات استفاده شده در عملیات	- نوع پیام/اطلاعات - شناسه تمیزدهنده عناصر - علت پیام - شناسه تمیزدهنده‌ی تفکیک‌کننده، فراهم‌کننده یا ثبت کننده رویداد		
	کنترل اطلاعات	- زمان، تعداد وقوع		

پیوست ت

ثبت زمان رویدادهاي ممیزي
(اطلاعاتي)

ایجاد هماهنگی کامل بین به‌وجود آورندگان یا ثبت‌کنندگان متفاوت رویداد در عمل امکان‌پذیر نیست. در چنین مواردی، به ابزاری جهت مرتبط کردن زمان به رویدادهای موجود در دنباله‌ی ممیزی امنیت نیاز است. یک سابقه ممیزی امنیت از روی یک پیام ممیزی امنیت ساخته می‌شود که ممکن است شامل یک برچسب زمانی باشد و یا این که برچسب زمانی نداشته باشد. در صورت داشتن برچسب زمانی، یک سابقه ممیزی امنیت با استفاده از نشانه‌ی زمانی[1] موجود در پیام ممیزی امنیت ایجاد می‌شود. در مورد اخیر، سابقه امنیتی ایجاد شده در پی دریافت رویداد امنیتی، شامل یک برچسب زمانی است که از مرجعی زمانی[2] برای ثبت‌کننده‌ی ممیزی استفاده می‌کند. در هر دو مورد، باید یک سابقه ممیزی ایجاد شود که به رابطه‌ی زمانی بین پدید آورنده‌ی رویداد و ثبت‌کننده‌ی ممیزی مربوط می‌شود.

در مورد قبلی، تفاوت بین مرجع زمانی پدید آورنده‌ی رویداد و مرجع زمانی *ثبت‌کننده‌ی ممیزی* باید ارزیابی شود. سابقه ممیزی باید شناسایی *پدید آورنده‌ی رویداد*، مرجع زمانی آن، مرجع زمانی ثبت‌کننده‌ی ممیزی، تأخیر بین مراجع زمانی و حاشیه رواداری در برابر تأخیر[3] را شامل شود. در مورد اخیر، سابقه ممیزی باید به نمایان ساختن پدیدآورنده‌ی رویداد، مرجع زمانی *ثبت‌کننده‌ی ممیزی* و ارزیابی تأخیر بین پدید آورنده‌ی رویداد و *ثبت‌کننده‌ی ممیزی* و آستانه‌ی تحمل در برابر تأخیر دلالت داشته باشد.

ایجاد چنین سوابقی برای هر رویداد در عمل امکان‌پذیر نیست. بسته به ماهیت رابطه یا شناوری بین مراجع زمانی، چنین سوابقی ممکن است ایجاد شوند. اگر پس از دوره‌ی مشاهده، معلوم شود که تأخیر ناچیز است، آن‌گاه چنین سوابقی نادیده گرفته می‌شوند. در صورت عدم وجود اندازه‌گیری‌های[4] تأخیر، از درون‌یابی خطی استفاده می‌شود.

این چنین مشکلی نیز بین مرجع زمانی یک *ثبت‌کننده‌ی ممیزی* و مرجع زمانی یک توزیع‌کننده‌ی ممیزی موجود در سامانه‌ی پایانی[5] دیگر، پدید می‌آید. اما در این مورد، هر دو سامانه یک مرجع زمانی خواهند داشت. اندازه‌گیری اختلاف زمانی ممکن است در هر زمان بین طرفین یا در هر زمان که انتقال دنباله‌ی ممیزی امنیت رخ می‌دهد، انجام شود. سابقه باید شامل شناسایی پدیدآورنده‌ی رویداد، شناسایی *توزیع‌کننده‌ی ممیزی*، *مرجع*

1 - Time indication
2 - Time reference
3 - Tolerance margin of the delay
4 - Measurements
5 - End system

زمانی ثبت‌کننده‌ی ممیزی، *ارزیابی تأخیر بین ثبت‌کننده‌ی ممیزی* و *توزیع‌کننده‌ی ممیزی* و آستانه‌ی تحمل در برابر تأخیر خواهد بود.

تشخیص این که کدام رویداد نخست واقع شده ممکن است با اضافه یا کم کردن تأخیرهای بین یک سری از مراجع زمانی و اضافه کردن تمامی آستانه‌های تحمل انجام شود. اگر تأخیر حاصل کمتر از آستانه‌ی تحمل باشد، آن‌گاه جداسازی[1] امکان‌پذیر نیست.

هنگام نیاز به تولید گزارش ممیزی امنیت، بحثی مشابه وجود دارد. با استفاده از اطلاعاتی که در دنباله‌ی ممیزی امنیت وجود دارد، مرتب کردن رویدادها بر طبق اختلاف مراجع زمانی امکان‌پذیر است. اما مرتب کردن یک رویداد تنها زمانی تضمین می‌شود که آستانه‌ی تحمل در برابر تأخیر کوتاه‌تر از اختلاف زمانی به علاوه‌ی آستانه‌ی تحمل رویداد بعدی باشد. برای این منظور، محاسبه‌ی آستانه‌ی تحمل تجمعی[2] با هر رویداد، باید امکان‌پذیر باشد.

1 - Distinction
2 - Cumulative tolerance margin