INSO-ISO-IEC

27039

1st.Edition
2016
Identical with
ISO/IEC 27039: 2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران-ایزو-آی ای سی

۲۷۰۳۹

چاپ اول
۱۳۹۵

فناوری اطلاعات- فنون امنیتی- انتخاب، استقرار و عملیاتِ سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)

Information technology — Security techniques —selection, deployment and operations of intrusion detetcion and prevention systems (IDPS)

ICS: 35.040

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.org

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.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه 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 زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات- فنون امنیتی-انتخاب، استقرار و عملیاتِ سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)»

رئیس:	**سمت و/ یا محل اشتغال:**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	رئیس اداره تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
دبیر:	
کیامهر، بیتا (فوق لیسانس مدیریت تکنولوژی)	معاون اداره کل نظام مدیریت امنیت اطلاعات سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
ناظمی، اسلام (دکترای مهندسی کامپیوتر)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
یعقوبی رفیع، کمال الدین (کارشناسی ارشد فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی
دوست‌محمدی، وحید (کارشناسی ارشد مهندسی صنایع گرایش فناوری اطلاعات)	کارشناس مرکز مدیریت راهبردی افتا
ابوالقاسمی، پیمان (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
ارجمند، مهدی (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
رادمهر، وحید (کارشناسی مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)
جوادزاده، غزاله (کارشناسی ارشد مهندسی کامپیوتر)	پژوهش‌گر پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

اعضاء: (اسامی به ترتیب حروف الفبا)	**سمت و/ یا محل اشتغال:**
مغانی،مهدی (فوق لیسانس ریاضی کاربردی)	کارشناس تدوین استانداردهای حوزه فناوری اطلاعات سازمان فناوری اطلاعات ایران
ویراستار:	
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	مشاور رئیس مرکز آپا دانشگاه تربیت مدرس

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- انتخاب، استقرار و عملیاتِ سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است، در چهارصد و سی و هفتمین اجلاسیه کمیتهٔ ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۵/۰۷/۱۳ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان 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.

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

ISO/IEC 27039: 2015, Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

مقدمه

توصیه می‌شود سازمان‌ها نه تنها زمان، بلکه چگونگی وقوع نفوذ به شبکه، سامانه یا برنامه‌های کاربردی را بدانند. همچنین توصیه می‌شود که آن‌ها از آسیب‌پذیری‌هایی که مورد بهره‌جویی قرار گرفته‌اند آگاهی داشته باشند و توصیه می‌شود حفاظت‌ها یا گزینه‌های مواجهه مناسب با مخاطره (یعنی اصلاح مخاطره، حفظ مخاطره، اجتناب از مخاطره[1]، به اشتراک‌گذاری مخاطره) برای جلوگیری از نفوذهای مشابه در آینده پیاده-سازی شوند. توصیه می‌شود سازمان‌ها، نفوذهای سایبری را تشخیص دهند و مانع آن‌ها شوند. این امر نیاز به تحلیل میزبان و ترافیک شبکه و/یا ردّ [2] ممیزی برای نشانه‌های حمله یا الگوهای مخصوصی دارد که معمولا نیت سوء و مشکوک را نشان می‌دهد. در اواسط دهه‌ی ۹۰ میلادی، سازمان‌ها شروع به استفاده از سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS) کردند تا این نیازها را تامین نمایند. استفاده‌ی عمومی از IDPS با در دسترس قرار دادنِ گستره‌ی وسیع‌تری از محصولات IDPS گسترش می‌یابد، تا سطح فزاینده‌ی تقاضاهای سازمانی برای توانایی کشف پیشرفته نفوذ برآورده نماید.

توصیه می‌شود به منظور اینکه سازمانی به بیشینه منافع از IDPS برسد، فرآیند انتخاب، استقرار و عملیات توسط کارمندان باتجربه و آموزش‌دیده، به‌دقت طرح‌ریزی و پیاده‌سازی شود. در موردی که این فرآیند اجرا شده است، محصولات IDPS می‌تواند به منظور کسب اطلاعات نفوذ به سازمان کمک کند و به عنوان افزاره‌ی مهم امنیتی درون زیرساخت فناوری اطلاعات و ارتباطات (ICT) خدمت‌رسانی کند.

این استاندارد ملی رهنمودهایی برای انتخاب، استقرار و عملیات موثر IDPS و همچنین دانش بنیادی در مورد IDPS فراهم کرده است. این استاندارد همچنین برای سازمان‌هایی که در حال در نظر گرفتن برون‌سپاری توانایی‌های کشف نفوذ هستند، کاربست‌پذیر است. اطلاعاتی در مورد توافقات سطح خدمت برون‌سپاری را می‌توان در فرآیندهای مدیریت خدمات فناوری اطلاعات (ITSM) [3] برمبنای مجموعه‌ی استاندارد ISO/IEC 20000 یافت.

این استاندارد ملی سعی دارد که در موارد زیر مفید باشد:

الف- کمک به سازمان در برآورده نمودن الزامات زیر از استاندارد ISO/IEC 27001:

- سازمان باید روش‌های اجرایی و دیگر واپایش‌های توانمندساز برای کشف سریع و پاسخ به رخدادهای امنیتی را پیاده‌سازی کند.
- سازمان باید روش‌های اجراییِ پایش و بازنگری و دیگر واپایش‌ها را به منظور شناسایی مناسب سوء قصدها، نقض‌ها و نفوذهای موفقیت‌آمیز و رخدادهای امنیتی انجام دهد.

ب- کمک به سازمان در پیاده‌سازی واپایش‌هایی که اهداف امنیتی زیر از استاندارد ISO/IEC 27002 را برآورده می‌سازند:

1- Risk retention
2- Trail
3- Information Technology Service Management

- کشف کردن فعالیت‌های احراز هویت نشده‌ی پردازنده‌ی اطلاعات
- توصیه می‌شود سامانه‌ها پایش شوند و توصیه می‌شود رویدادهای امنیت اطلاعات ثبت شوند. توصیه می‌شود به منظور کسب اطمینان از اینکه مسائل سامانه‌ی اطلاعاتی شناسایی شده است، ورود به سامانه توسط کاروَر[1] و خطاهای ورود به سامانه ثبت شود.
- توصیه می‌شود سازمان با تمامی الزامات کاربردی قانونی در مورد فعالیت‌های پایشی و ورود به سامانه‌ها، مطابقت داشته باشد.
- توصیه می‌شود پایش سامانه به منظور بازرسی کردن تاثیر واپایش‌های سازگار و تصدیق مطابقت با مدل دسترسی خط‌مشی استفاده شده باشد.

توصیه می‌شود سازمان تشخیص دهد که استقرار IDPS ها تنها راه‌حل و/یا راه‌حل جامع به منظور برآورده کردن یا ارضای الزامات بالا نیست. علاوه بر این، این استاندارد ملی به عنوان معیاری برای هر نوع ارزیابی انطباقی به عنوان مثال گواهی سامانه‌ی مدیریت امنیت اطلاعات (ISMS)، خدمات IDPS یا گواهی محصولات نیست.

1- Operator

فناوری اطلاعات- فنون امنیتی-انتخاب، استقرار[1] و عملیات سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)[2]

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین ارائه راهنماهایی برای کمک به سازمان‌ها در جهت آماده‌سازی برای استقرار سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS) است. این استاندارد به‌طور ویژه، به انتخاب، استقرار و عملیاتِ IDPS می‌پردازد. همچنین اطلاعات پس‌زمینه‌ای که این راهنماها از آن‌ها مشتق شده است را فراهم می‌سازد.

۲ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین شده در استاندارد ISO/IEC 27000 [3]، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۲-۱

حمله

attack

تلاش‌هایی جهت نابودی، افشا، تغییر یا از کار انداختن سامانه‌های اطلاعاتی و یا اطلاعات آن‌ها و یا در غیر این صورت نقض خط‌مشی امنیتی است.

۲-۲

نشانه حمله

attack signature

دنباله‌ای از فعالیت‌های رایانش[4] و یا تغییرات که برای اجرای حمله استفاده می‌شود و همچنین توسط IDPS برای کشف وقوع حمله مورد استفاده قرار می‌گیرد. و اغلب از طریق آزمودن ترافیک شبکه یا وقایع ثبت شده‌ی میزبان مشخص می‌شود.

1- Deployment

2 - Intrusion detection systems

۳ - استاندارد ملی ایران با شماره ۲۷۰۰۰ INSO-ISO-IEC در سال ۱۳۹۴ با منبع بین‌المللی ISO/IEC 27002:2015 منتشر شده است.

4- Computing

یادآوری ۱- به نشانه حمله تحت عنوان الگوی حمله نیز ارجاع می‌شود.

۳-۲

تصدیق امضا

attestation

گونه‌ای از رمزگذاری کلید عمومی که به برنامه‌های نرم‌افزاری و افزاره‌های IDPS امکان می‌دهد شناسه خود را به طرف‌های دوردست[1] معرفی کنند.

یادآوری ۱- به تصدیق امضا از دور (۲-۲۳) مراجعه شود.

۴-۲

پل

bridge

از تجهیزات شبکه است که یک شبکه محلی[2] (LAN) را به‌صورت شفاف در لایه‌ی دوم مدل OSI به شبکه‌ی محلی دیگری که از همان قرارداد استفاده می‌کند، متصل می‌سازد.

۵-۲

مقدار چکیده‌ساز رمزنگاشتی

cryptographic hash value

مقدار ریاضی که به یک پرونده[3] اختصاص داده می‌شود و به‌منظور «آزمون» آن پرونده در زمان‌های بعدی برای بررسی اینکه داده‌های موجود در آن پرونده به‌صورت بدخواهانه تغییر نکرده باشند، مورد استفاده قرار می‌گیرد.

۶-۲

انکار خدمت

denial-of-service (DoS)

دسترسی غیرمجاز به یک منبع سامانه و یا به تأخیر انداختن عملیات و کارکردهای سامانه که منجر به کاهشِ دسترس‌پذیری برای کاربران مجاز می‌شود.

[منبع: ISO / IEC 27033-1: 2009]

1- Remote parties
2- Local area network
3- File

۷-۲

حمله‌ی توزیع‌شده انکار خدمت

distributed denial-of-service attack (DDoS)

دسترسی غیرمجاز به یک منبع سامانه و یا به تأخیر انداختن عملیات و کارکردها سامانه با روش مصالحه با چندین سامانه‌ی دیگر برای پر کردن پهنای باند و یا منابع سامانه هدف که منجر به کاهش دسترس‌پذیری برای کاربران مجاز می‌شود.

۸-۲

ناحیه‌ی غیرنظامی

demilitarized zone (DMZ)

فضای منطقی و فیزیکی شبکه بین مسیریاب مرزی و دیوار آتش بیرونی[1] است.

یادآوری ۱- ناحیه DMZ می‌تواند بین شبکه‌ها و تحت نظارت دقیق باشد، اما نیازی نیست چنین باشد.

یادآوری ۲- نواحی DMZ عموماً مناطق ناامنی شامل میزبان‌های سنگر[2] می‌باشند که خدمات عمومی را فراهم می‌سازد.

۹-۲

بهره‌جویی

exploit

روش تعریف‌شده برای نقض امنیت سامانه‌های اطلاعاتی از طریق آسیب‌پذیری است.

۱۰-۲

دیوار آتش

firewall

نوعی مانع که بین محیط شبکه‌ها قرار داده شده است - متشکل از یک افزاره‌ی اختصاصی یا ترکیبی از اجزا و فنون مختلف- که همه ترافیک محیط یک شبکه از طریق آن به شبکه دیگر منتقل می‌شود و بالعکس، و تنها ترافیک مجاز که توسط خط‌مشی امنیتی محلی تعریف شده است، اجازه عبور دارد.

[منبع: ISO / IEC 27033-1: 2009]

1- Exterior firewall
2- Bastion hosts

۱۱-۲

مثبت کاذب

false positive

هشدار IDPS زمانی که هیچ حمله‌ای وجود ندارد.

۱۲-۲

منفی کاذب

false negative

عدم هشدار IDPS زمانی که حمله وجود دارد.

۱۳-۲

هانی پات (ظرف عسل)

honeypot

اصطلاح عمومی برای سامانه‌ی طعمه که برای فریب دادن، اغفال، انحراف، و تشویق[1] مهاجم به‌صرف زمان روی اطلاعاتی که به نظر می‌رسد بسیار ارزشمند است استفاده می‌شود، اما درواقع ساختگی است و موردعلاقه‌ی یک کاربر مشروع[2] نیست.

۱۴-۲

میزبان

host

سامانه یا رایانه‌ی قابل آدرس‌دهی در شبکه‌های مبتنی بر TCP / IP مانند اینترنت است.

۱۵-۲

مهاجم

intruder

فردی که نفوذ و یا حمله را به میزبان، وب‌سایت، شبکه و یا سازمان قربانی انجام داده و یا در حال انجام است.

1- Encourage
2- Legitimate user

۱۶-۲

نفوذ

intrusion

دسترسی غیرمجاز به یک سامانه شبکه و یا سامانه شبکه متصل که آگاهانه یا اتفاقی به سامانه‌های اطلاعاتی دسترسی غیرمجاز پیدا می‌کند و شامل فعالیت‌های مخرب در سامانه‌های اطلاعاتی و یا استفاده غیرمجاز از منابع در سامانه‌های اطلاعاتی است.

۱۷-۲

آشکارسازی نفوذ

intrusion detection

فرآیند رسمی آشکارسازی نفوذها، که مشخصه‌ی عمومی آن جمع‌آوری دانش در مورد الگوهای کاربری غیرطبیعی است و همچنین اینکه چه آسیب‌پذیری‌هایی و چگونه مورد بهره‌جویی قرارگرفته‌اند و این بهره‌جویی چگونه و چه زمانی به وقوع پیوسته است.

۱۸-۲

سامانه‌ی آشکارسازی نفوذ

intrusion detection system (IDS)

سامانه‌های اطلاعاتی که به‌منظور شناسایی تلاش برای یک نفوذ، وقوع نفوذ و یا نفوذ در حال رخداد، مورد استفاده قرار می‌گیرد.

۱۹-۲

سامانه‌ی پیش‌گیری از نفوذ

intrusion prevention system (IPS)

نوعی از سامانه‌های آشکارسازی نفوذ که به‌طور ویژه برای ارائه‌ی قابلیت پاسخ فعال طراحی شده است.

۲۰-۲

سامانه‌ی آشکارسازی و پیش‌گیری نفوذ

intrusion detection and prevention system (IDPS)

برنامه‌های کاربردی نرم‌افزار یا ابزارهای سامانه‌های آشکارسازی نفوذ (IDPS) و سامانه‌های پیشگیری از نفوذ (IPS) که سامانه‌ها را برای فعالیت‌های مخرب پایش می‌کنند، تمرکز IDS تنها بر هشدار در هنگام کشف

چنین فعالیت‌هایی است درحالی‌که IPSها دارای قدرت پیش‌گیری از برخی نفوذها پیش از آشکارسازی می‌باشند.

یادآوری ۱- درصورتی‌که پیش‌گیری از حمله مد نظر باشد، IPS به‌طور فعال در شبکه مستقر می‌شود. اگر در حالت غیر فعال مستقر شود، قابلیت‌های این‌چنین را ارائه نمی‌دهد و به‌طور مؤثر به عنوان یک IDS معمولی با ارائه‌ی هشدار عمل می‌کند.

۲-۲۱

نفوذ

penetration

اقدام غیرمجاز دور زدن سازوکارهای امنیتی سامانه‌های اطلاعاتی است.

۲-۲۲

تأمین

provisioning

فرآیند بارگذاری نرم‌افزار، خط‌مشی امنیتی، و داده‌های پیکربندی صحیح برای افزاره‌های فناوری اطلاعات (IT) است.

۲-۲۳

تصدیق امضا از دور

remote attestation

فرآیندهای استفاده از گواهی‌های رقمی (دیجیتال) برای حصول اطمینان از شناسه، و همچنین پیکربندی سخت‌افزار و نرم‌افزار IDPS و به‌منظور انتقال امن این اطلاعات به یک مرکز عملیات معتمد.

۲-۲۴

رویارویی با پیشامدها یا رویارویی بانفوذ (پاسخ)

incident response or intrusion response (response)

اقدام صورت گرفته برای محافظت و بازگرداندن شرایط عملیاتی عادی سامانه‌های اطلاعاتی و اطلاعات ذخیره شده در آن زمانی که یک حمله‌یا نفوذ رخ می‌دهد.

۲-۲۵

مسیریاب

router

افزاره‌ی شبکه است که برای ایجاد و واپایش جریان داده‌ها بین شبکه‌های مختلف از طریق انتخاب راه‌ها یا مسیرها مبتنی بر الگوریتم‌ها و سازوکارهای قرارداد مسیریابی، استفاده می‌شود.

یادآوری ۱- خود شبکه‌ها می‌توانند مبتنی بر قراردادهای مختلف باشند.

یادآوری ۲- اطلاعات مسیریابی در یک جدول مسیریابی نگهداری می‌شود.

[منبع: ISO / IEC 27033-1: 2009]

۲-۲۶

کارساز

server

سامانه یا برنامه رایانه‌ای که خدماتی را برای رایانه‌های دیگر فراهم می‌سازد.

۲-۲۷

توافقنامه سطح خدمت

Service Level Agreement (SLA)

سندی که پشتیبانی فنی یا اهداف عملکرد کسب‌وکار را تعریف می‌کند و شامل سنجه‌هایی برای عملکرد و همچنین پیامدهای شکست که فراهم کننده خدمت می‌تواند برای کارخواه‌های خود فراهم کند، است.

۲-۲۸

حسگر

sensor

جزء یا عاملی از IDPS که داده‌های رویداد را از سامانه‌های اطلاعاتی یا از شبکه‌ی تحت نظارت جمع‌آوری می‌کند.

یادآوری ۱ به مدخل- به حسگر، همچنین پایشگر نیز گفته می‌شود.

۲-۲۹

زیرشبکه

subnet

بخشی از یک شبکه است که از مولفه‌ی مشترک آدرس بهره می‌برد.

۲-۳۰

سوده

switch

افزاره‌ای است که اتصال بین افزاره‌های اتصال شبکه‌ها را از طریق سازوکارهای توزیع داخلی و با فناوری سودهی که به‌طور معمول در لایه ۲ و یا لایه ۳ از مدل مرجع OSI پیاده سازی می‌شود، فراهم می‌سازد.

یادآوری ۱- سوده‌ها از دیگر افزاره‌های اتصال شبکه‌های محلی (به‌طور مثال ناف (هاب) [1]) متمایز می‌باشند. فناوری مورد استفاده در سوده‌ها اتصالات را بر اساس نقطه به نقطه برپا می‌کند.

[منبع: ISO / IEC 27033-1: 2009]

۲-۳۱

درگاه دسترسی آزمون

test access port (TAP)

نوعا افزاره‌های غیر فعال که نه تنها سربار روی بسته‌های شبکه ندارند بلکه سطح امنیتی را افزایش می‌دهند چون واسط جمع‌آوری داده‌ها را برای شبکه نامرئی می‌سازد، به طوری که سوده هنوز هم می‌تواند اطلاعات لایه ۲ درباره‌ی درگاه را نگهداری کند.

یادآوری ۱- درگاه TAP کارکرد چندین درگاهی را نیز می‌دهد درنتیجه مسائل مربوط به شبکه می‌تواند بدون از دست دادن توانایی IDPS اشکال زدایی شود.

۲-۳۲

اسب تروآ

trojan horse

بدافزاری که خود را نرم‌افزاری بی‌خطر جلوه می‌دهد.

1- Hub

۳۳-۲

ویروس

virus

نوعی بدافزار که نرم‌افزاری است که با قصد بدخواهانه طراحی شده است و حاوی ویژگی‌ها و توانمندی‌هایی است که به‌طور بالقوه می‌تواند باعث آسیب‌رساندن، مستقیم یا غیر مستقیم، به کاربر و یا سامانه‌ی کاربر شود.

۳۴-۲

شبکه‌ی خصوصی مجازی

virtual private network (VPN)

شبکه رایانه‌ای منطقی با کاربری محدود که از منابع سامانه‌ی شبکه‌ی فیزیکی با استفاده از رمزگذاری و/یا تونل زدن لینک‌های شبکه‌ی مجازی در سراسر شبکه ی واقعی ساخته شده است.

[منبع: ISO / IEC 18028-3: 2005]

۳۵-۲

آسیب‌پذیری

vulnerability

ضعف دارایی یا واپایش که می‌تواند توسط یک یا چند تهدید مورد بهره جویی قرار گیرد.

[منبع: ISO / IEC 27000: 2012]

۳ پس‌زمینه[1]

هدف سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)، پایش غیرفعالانه، آشکارسازی و ثبت فعالیت‌های نابجا، ناصحیح، مشکوک و یا ناهنجار است که ممکن است نشان‌دهنده‌ی نفوذ باشد. این سامانه به هنگام آشکار شدن این فعالیت‌ها یک هشدار را فراهم می‌سازد و یا پاسخ خودکار می‌دهد. بازنگری فعال هشدارهای IDPS و وقایع مرتبط آن‌ها به‌منظور اخذ تصمیمات برای پاسخ‌های مناسب، مسئولیت کارکنان تعیین شده‌ی امنیت IT است. وقتی سازمان نیازمند آشکارسازی آنی نفوذها به سامانه‌ی اطلاعاتی سازمان و پاسخ به‌جا به آن‌ها است، توصیه می‌شود استقرار IDPS را در نظر داشته باشد. سازمان می‌تواند IDPS را با در اختیار گرفتن محصولات نرم‌افزاری و یا سخت‌افزاری IDPS و یا از طریق برون‌سپاری توانمندی‌های IDPS به ارائه-کننده‌ی خدمت IDPS، مستقر کند.

1- Background

محصولات و خدمات IDPS بسیاری به‌صورت تجاری‌سازی شده در دسترس و یا متن باز موجود است که مبتنی بر فناوری‌ها و رویکردهای متفاوت می‌باشند. علاوه بر این، IDPS یک فناوری «اتصال و اجرا[1]» نیست. بنابراین زمانی که سازمان برای استقرار IDPS آماده می‌شود، توصیه می‌شود که در حد کمینه با راهنماها و اطلاعات فراهم‌شده در این استاندارد آشنا باشد.

دانش بنیادی در مورد IDPS به‌طور عمده در پیوست الف ارائه شده است. این پیوست مشخصه‌های انواع مختلف IDPS را شرح می‌دهد:

- مبتنی بر شبکه، که ترافیک شبکه را برای بخش‌ها و یا افزاره‌های ویژه‌ی شبکه پایش کرده و فعالیت قرارداد برنامه کاربردی و شبکه را برای شناسایی فعالیت مشکوک تحلیل می‌نماید.
- مبتنی بر میزبان، که مشخصه‌های میزبان و رویدادهایی که در آن میزبان رخ داده برای فعالیت‌های مشکوک پایش می‌کند و همچنین سه رویکرد برای تحلیل آشکارسازی وجود دارد. به عنوان مثال، آشکارسازی مبتنی بر نشانهء، آشکارسازی مبتنی بر ناهنجاری‌های آماری و آشکارسازی مبتنی بر تحلیل قرارداد دارای حالت.

تحلیل رفتاری برای هر دو IDPS مبتنی بر شبکه و مبتنی بر میزبان اعمال می‌شود. این رویکرد ترافیک شبکه و فعالیت‌های میزبان را بررسی می‌کند تا ریسه‌هایی را که رفتارهای ناهنجار تولید می‌کنند شناسایی کند، مانند حملات توزیع‌شده انکار خدمت (DDOS)، حملات جستجوی فراگیر، شکل‌های خاصی از بدافزارها و نقض‌کننده‌های خط‌مشی(به‌طور مثال فراهم کردن خدمات شبکه توسط سامانه‌ی کارخواه برای سامانه‌های دیگر).

سامانه‌ی آشکارسازی و پیش‌گیری از نفوذ مبتنی بر میزبان(HIDPS)[2] منبع اطلاعات خود را از یک یا چند میزبان مشتق می‌کند، درحالی‌که سامانه‌ی آشکارسازی و پیش‌گیری از نفوذ مبتنی بر شبکه(NIDPS) اطلاعات خود را از یک یا چند بخش شبکه استخراج می‌کند. رویکرد مبتنی بر سوءاستفاده حملات روی سامانه‌ی اطلاعاتی را به‌صورت نشانه‌های مشخص حمله مدل‌سازی کرده و سپس به‌صورت سامانمند، سامانه را برای رخداد این نشانه‌های حمله پویش می‌کند. این فرآیند شامل کدبندی مشخص رفتارهای قبلی و اقداماتی که نفوذی و یا مخرب فرض شده‌اند، است.رویکرد مبتنی بر ناهنجاری تلاش می‌کند تا نفوذها را با کشف انحراف مهم نسبت به رفتار عادی آشکارسازی کند. با فرض این‌که نفوذها از رفتار معمولی و یا مشروع متفاوت هستند و بنابراین می‌توان آن‌ها را با سامانه‌ای که این اختلاف‌ها را شناسایی می‌کند، آشکارسازی نمود.

توصیه می‌شود که یک سازمان بداند که منبع اطلاعات و رویکردهای متفاوت تحلیل به مزیت‌ها و یا ضررها و محدودیت‌هایی می‌انجامند که روی توانایی و یا ناتوانی آشکارسازی حملات مشخص تأثیرگذار می‌باشند و درجه‌ی سختی مرتبط با نصب و نگهداری IDPS را تحت تأثیر قرار می‌دهند.

1- Plug and play

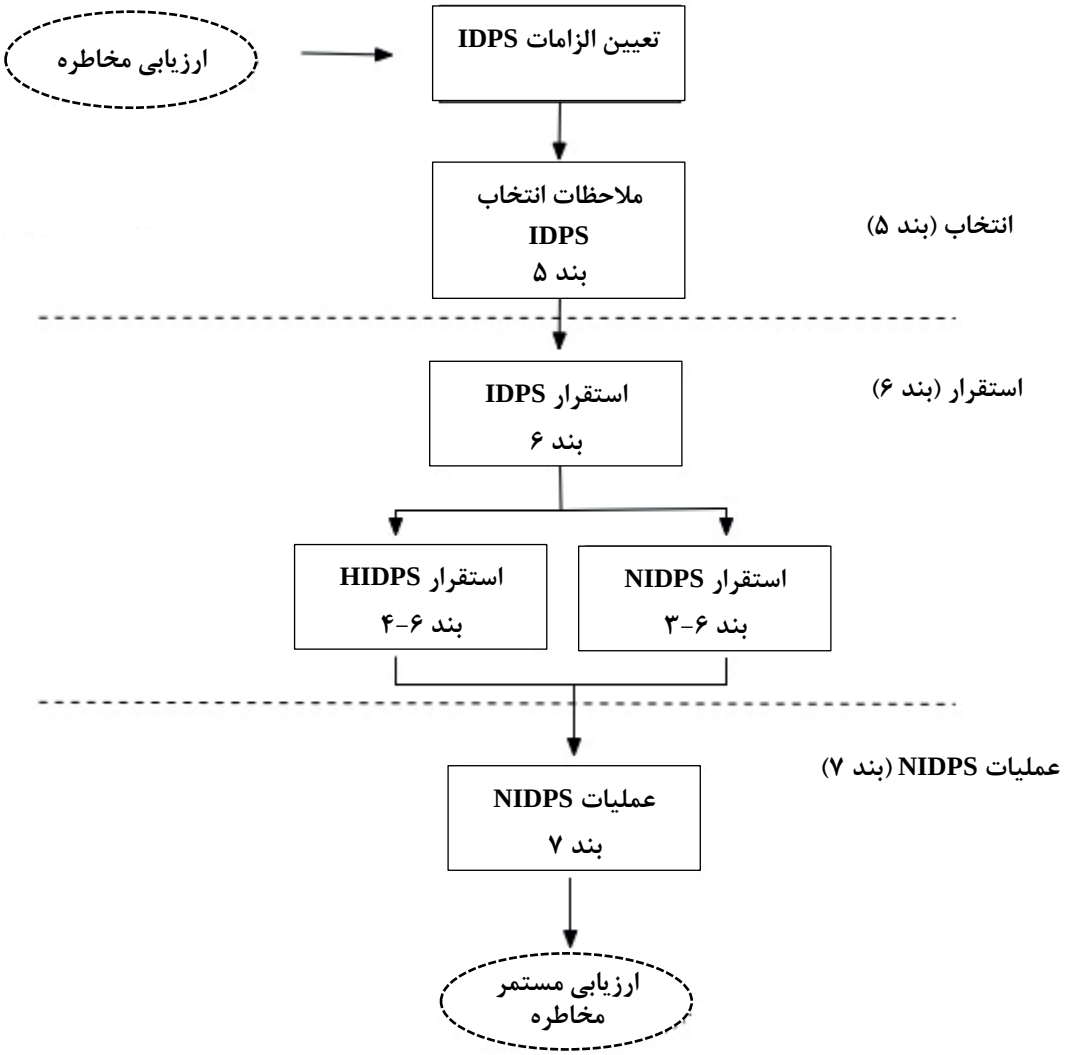
2- Host-based Intrusion Detection and Prevention System

۴ کلیات

کارکردها و محدودیت‌های IDPS، ارائه شده در پیوست الف، نشان می‌دهد که بهتر است سازمان رویکردهای مبتنی بر میزبان(شامل پایش برنامه کاربردی) و مبتنی بر شبکه برای دستیابی به پوشش کامل معقولانه‌ی نفوذهای بالقوه ترکیب کند. هر نوع IDPS نقاط قدرت و محدودیت‌های خود را دارد و در کنارهم می‌توانند پوشش رویدادهای امنیتی و تحلیل هشدار بهتری را فراهم سازند.

ترکیب فناوری‌های IDPS به در دسترس بودن موتور همبستگی روی سامانه‌ی مدیریت هشدار بستگی دارد. پیوند دستی هشدارهای HIDPS و NIDPS بدون هیچ فایده‌ی بیشتری ممکن است به کار اضافه در IDPS منجر شود و نتیجه ممکن است از انتخاب مناسب‌ترین خروجی از یک نوع IDPS بدتر باشد.

در شکل ۱، فرآیند انتخاب، استقرار و عملیات IDPS در یک سازمان به همراه بندهایی که به قدم‌های کلیدی در این فرآیند می‌پردازند، نشان داده شده است.



شکل ۱- انتخاب، استقرار و عملیات IDPS

۵ انتخاب

۵-۱ مقدمه

محصولات و خانواده‌های محصولات IDPS متنوعی در دسترس است. گستره‌ی آن‌ها از ارائه‌ی رایگان‌افزارهایی[1] که روی میزبان با هزینه‌ی پایین مستقر می‌شوند تا سامانه‌های تجاری بسیار گران قیمت که نیازمند جدیدترین سخت‌افزارهای در دسترس می‌باشند، است. ازآنجایی‌که تعداد زیادی محصولات متنوع IDPS برای انتخاب وجود دارد، فرآیند انتخاب IDPS که بیشترین تطابق را با نیازمندی‌های سازمان داشته باشد، مشکل است. علاوه بر این ممکن است سازگاری محدودی بین محصولات متنوع IDPS که در بازار ارائه می‌شود، وجود داشته باشد. همچنین به دلیل ادغام‌ها و توزیع بالقوه گسترده‌ی جغرافیایی یک سازمان،

1- Freeware

سازمان‌ها ممکن است مجبور به استفاده از IDPSهای مختلف باشند و یکپارچه‌سازی این IDPSهای پراکنده بسیار چالش‌برانگیز است. دفترک[1]های فروشنده‌ها ممکن است به‌طور کامل توضیح ندهند که IDPS چقدر خوب می‌تواند نفوذها را آشکار کند و استقرار، عملیات و نگهداری آن در یک شبکه‌ی عملیاتی با حجم عظیمی از ترافیک چقدر مشکل است. فروشنده‌ها ممکن است به این‌که چه حمله‌هایی می‌توانند آشکار شوند، اشاره کنند اما بدون دسترسی به ترافیک شبکه‌ی سازمان، توضیح این‌که IDPS چقدر خوب می‌تواند عمل کند و از مثبت کاذب و منفی کاذب جلوگیری کند بسیار مشکل است. همچنین توانایی‌های پیش‌بینانه و واکنشیِ IDPS، نیازمند ارزیابی مستقل است و نگاشت به نیازمندی‌های سازمان است این امر شامل نیاز به بازرسی عمیق بسته‌ها و بازهم گذاردن آن‌ها در مقابل نیازهای عملکردی شبکه و ملاحظات هزینه‌ای است. درنتیجه، تکیه بر اطلاعات فراهم شده توسط فروشنده در مورد توانایی‌های IDPS نه کافی است و نه توصیه می‌شود.

استاندارد ISO/IEC 15408 (همه قسمت‌ها) می‌تواند برای ارزیابی یک IDPS مورد استفاده قرار گیرد. در چنین موردی سندی به نام «هدف امنیت» شامل توضیحاتی دقیق‌تر و قابل‌اطمینان‌تر از دفترک‌های فروشنده در مورد عملکرد IDPSها است. توصیه می‌شود سازمان از این سند در فرآیند انتخاب استفاده کند.

در بندهای ارائه شده در ادامه، عامل‌های مهم که توصیه می‌شود یک سازمان در فرآیند انتخاب IDPS خود استفاده کند فراهم شده است.

۲-۵ ارزیابی مخاطره امنیت اطلاعات

قبل از انتخاب IDPS، توصیه می‌شود سازمان ارزیابی مخاطره امنیت اطلاعات را با هدف شناسایی حملات و تهدیدها به سامانه‌های اطلاعاتی ویژه‌ی سازمان که آسیب‌پذیرتر می‌باشند و با در نظر گرفتن عواملی مانند ماهیت اطلاعات که توسط سامانه استفاده می‌شود، چگونگی حفاظت آن، نوع ارتباطات مورد استفاده‌ی سامانه و عوامل محیطی و عملیاتی دیگر انجام دهد. با در نظر گرفتن این تهدیدهای بالقوه درزمینه‌ی اهداف ویژه‌ی امنیت اطلاعات، سازمان می‌تواند واپایش‌های مقرون به‌صرفه‌ای را شناسایی کند. وارسی‌های شناسایی شده اساس نیازمندی‌های کارکردهای فراهم شده توسط IDPS آن‌ها را فراهم می‌کند.

یادآوری- ارزیابی و مدیریت مخاطره امنیت اطلاعات موضوع استاندارد ISO /IEC 27001[2] است.

هنگامی که یک IDPS نصب و عملیاتی شد، توصیه می‌شود یک فرآیند مستمر مدیریت مخاطره پیاده سازی شود تا به‌صورت دوره‌ای تأثیر واپایش‌ها را در رخداد تغییرات در عملیات سامانه و محیط تهدیدآمیز بازنگری کند.

1- Brochures

۲ - استاندارد ملی ایران با شماره ۲۷۰۰۱ INSO-ISO-IEC در سال ۱۳۹۴ با منبع بین المللی ISO/IEC 27001: 2013 منتشر شده است.

۵-۳ IDPSهای میزبان یا شبکه

۵-۳-۱ مرور کلی

توصیه می‌شود استقرار IDPS بر مبنای برآورد خطرسازمانی و اولویت‌های حفاظت دارایی صورت گیرد. در هنگام انتخاب IDPS توصیه می‌شود مؤثرترین روش برای پایش رویدادها بررسی شود. هر دوی IDPSهای مبتنی بر میزبان (HIDPS) و مبتنی بر شبکه می‌توانند در کنار هم استقرار یابند. با انتخاب یک روش پایش IDPS توصیه می‌شود سازمان پیاده سازی آن را در مراحلی با شروع با NIDPS انجام دهد،زیرا آن‌ها معمولاً از نظر نصب و نگهداری ساده‌ترین می‌باشند. سپس HIDPS باید روی کارسازهای بحرانی مستقر شود.

هر گزینه فواید و ضررهای مخصوص به خود را دارد. به‌طور مثال در موردی که IDPS بیرون یک دیوار آتش خارجی مستقر شده است، IDPS تعداد زیادی هشدار تولید می‌کند که به تحلیل دقیق نیازی ندارد. زیرا حجم زیادی از رویدادهای هشداردهنده را نشان می‌دهند که قبلاً توسط دیوار آتش خارجی به‌طور مؤثر پیش‌گیری شده‌اند.

۵-۳-۲ IDPS مبتنی بر میزبان[1] (HIDPS)

انتخاب HIDPS شناسایی میزبان‌های هدف را طلب می‌کند. به دلیل ماهیت گران قیمت استقرار HIDPS روی تمامی میزبان‌های سازمان، معمولاً به استقرار HIDPS تنها روی میزبان‌های بحرانی منجر می‌شود.بنا براین استقرار HIDPS باید به‌منظور تحلیل نتایج خطر و فرضیات سود-فایده اولویت دهی شود. هنگامی که سازمان HIDPS را روی همه یا تعداد زیادی از میزبان‌ها مستقر کرد، باید یک IDPS با توانایی مدیریت متمرکز و گزارش‌دهی کارکردها نیز مستقر کند.

۵-۳-۳ IDPS مبتنی بر شبکه[2] (NIDPS)

عامل اصلی قابل ملاحظه در زمان استقرار NIDPS مکان حسگرهای سامانه است که شامل گزینه‌های زیر است:

- داخل دیوارهای آتش بیرونی
- خارج دیوارهای آتش بیرونی
- روی مازه[3] اساسی شبکه
- بین مرزهای مطمئن

1- Host-based IDPS
2- Network-based IDPS
3- Backbone

۵-۴ ملاحظات

۵-۴-۱ محیط سامانه

بر مبنای ارزیابی مخاطره امنیت، توصیه می‌شود سازمان به‌منظور تعیین اولویت تعیین کند که چه دارایی‌هایی باید حفاظت شده و سپس IDPS را به محیط اضافه نماید. در حد کمینه، اطلاعات محیط سامانه که در ادامه آورده شده است، باید برای به انجام رساندن این هدف جمع‌آوری شود:

- نمودارها و نقشه‌های شبکه مشخص‌کننده‌ی تعداد و مکان میزبان‌ها، نقاط ورودی شبکه و اتصالات به شبکه‌های خارجی
- توصیف سامانه‌ی مدیریت شبکه‌ی تشکیلات
- سامانه‌ی عامل برای هر میزبان
- تعداد و نوع افزاره‌های شبکه مانند مسیریاب‌ها، پل‌ها و سوده‌ها
- تعداد و نوع کارسازان و اتصالات شماره‌گیری[1]
- توصیف‌گرهای هر کارساز شبکه شامل انواع پیکربندی‌ها، نرم‌افزارهای کاربردی و نسخه‌ی در حال اجرا روی هر یک
- اتصالات به شبکه‌های خارجی شامل پهنای باند اسمی و قراردادهای قابل پشتیبانی
- مسیرهای بازگشت که مسیر اتصال ورودی نباشند به‌طور مثال جریان داده‌ی غیرمتقارن

۵-۴-۲ سازوکارهای محافظت امنیت

پس از مستندسازی شاخصه‌های فنی محیط سامانه، سازوکارهای حمایتی امنیت که به‌زودی نصب می‌شوند، باید شناسایی شوند.در حد کمینه اطلاعاتی که در ادامه آمده است موردنیاز است:

- ناحیه غیرنظامی (DMZ)
- تعداد، نوع و مکان دیوارهای آتش و مسیریاب‌های پالاینده[2]
- شناسایی کارسازان اصالت‌سنجی
- رمز گذاری[3] داده و پیوند
- بسته‌های ضد ویروس /بد افزارها
- محصولات واپایش دسترسی
- سخت‌افزارهای اختصاصی امنیت مانند سخت‌افزار رمزنگاشتی [1]

1- Dialup connections
2- Filtering routers
3- Encryption

- شبکه‌های مجازی خصوصی (VPN) [۲]
- هرگونه سازوکار امنیتی نصب شده‌ی دیگر

۵-۴-۳ خط‌مشی امنیتی IDPS

پس از شناسایی سامانه و محیط امنیت عمومی، خط‌مشی امنیتی IDPS باید شناسایی شود.در حد کمینه خط‌مشی نیازمند پاسخ به سؤالات زیر است:

- چه دارایی‌های اطلاعاتی باید واپایش شود؟
- خط‌مشی برای شرایط شکست باز و شکست بسته چیست؟
- چه نوعی از IDPS مورد نیاز است؟
- IDPS کجا می‌تواند قرار گیرد؟
- چه نوعی از حمله‌ها باید آشکارسازی شوند؟
- چه نوعی از اطلاعات باید ثبت شوند؟
- هنگامی که یک حمله آشکار می‌شود چه نوع پاسخ یا هشدار باید فراهم شود؟

خط‌مشی امنیتی IDPS اهداف سازمان را برای سرمایه گذاری IDPS نشان می‌دهد. این مرحله، اولین مرحله در تلاش برای بدست آوردن بیشینه‌ی ارزش از دارایی IDPS است.

به‌منظور تعیین اهداف و مقاصد خط‌مشی امنیت IDPS، سازمان ابتدا باید خطرهای ممکن از منابع داخلی و خارجی را مشخص نماید. همچنین توصیه می‌شود سازمان بداند که تعدادی از فروشنده‌های IDPS خط‌مشی امنیتی IDPS را به عنوان مجموعه‌ای از قوانین که IDPS برای تولید هشدارها استفاده می‌کند، تعریف می‌کنند.

بازنگری خط‌مشی امنیتی موجود در سازمان الگویی را فراهم می‌آورد که در آن چه نیازمندی از IDPS برحسب اهداف امنیت استاندارد، محرمانگی، یکپارچه‌سازی، دسترس‌پذیری،عدم انکار و همچنین اهداف عمومی‌تر مدیریت مانند حفاظت از حریم خصوصی، مسئولیت و قابلیت اداره تعیین شده است.

هنگامی که IDPS آشکار می‌کند که یک خط‌مشی امنیتی نقض شده است، سازمان چگونه باید واکنش نشان دهد. به خصوص در مواردی که سازمان مایل است که به‌طور فعال به انواع خاصی از تخطی‌ها پاسخ دهد، IDPS باید برای انجام این مورد پیکربندی شده و کارکنان مؤثر و عملیاتی باید از خط‌مشی پاسخ سازمان آگاهی یابند. درنتیجه آن‌ها می‌توانند به شیوه‌ای مناسب با هشدارها روبرو شوند.

به‌طور مثال، برای کمک به نتیجه مؤثر دریک رویداد امنیتی ممکن است رسیدگی اجرای قانون نیاز باشد.

1- Cryptographic
2- Virtual Private Networks

اطلاعات مرتبط شامل گزارش‌های ثبت‌شده‌ی IDPS ، ممکن است نیاز باشد تحویل به بدنه‌ی اجـرای قـانون برای اهداف دلالت کننده داده شود.

اطلاعات بیشتر درباره مدیریت رخداد امنیتی در استاندارد ISO /IEC 27035 یافت می‌شود.

۵-۴-۴ عملکرد

عامل دیگری که هنگام انتخاب IDPS باید ملاحظه شود، عملکرد است. توصیه می‌شـود در حـد کمینـه بـه سؤالات زیر پاسخ داده شود:

- چه پهنای باندی مورد نیاز است که توسط IDPS پردازش شود؟
- هنگام عملیات در آن پهنای باند، چه سطحی از هشدارهای نادرست قابل رواداری است؟
- آیا هزینه یک IDPS با سرعت بالا قابل توجیه است یا یک IDPS با سـرعت متوسـط یـا بـا سـرعت پایین کافی است؟
- پیامدِ از دست رفتن یک نفوذ بالقوه به دلیل محدودیت‌های عملکرد IDPS چیست؟
- زمانی که بازرسی عمیق بسته[1] و یا بازهم‌گذاری[2] آن رخ می‌دهـد چـه تـأثیری بـر عملکـرد خواهـد داشت؟

عملکرد پایدار به عنوان توانایی تشخیص حملات به‌طور مـداوم در یـک پهنـای بانـد مـورد اسـتفاده تعریـف می‌شود. در اغلب محیط ها، از دست رفتن و یا حذف بسته‌ها در ترافیک توسط IDPS که می‌تواند بخشـی از یک حمله باشد، کمتر قابل رواداری است. در برخی موارد، با افزایش پهنای باند و یا ترافیک شـبکه افـزایش، بسیاری از IDPSها دیگر قادر به تشخیص نفوذ طور مؤثر و مداوم نمی‌باشند.

ترکیبی از تعادل و میزان سازی بار می‌تواند عملکرد را افزایش دهد. به عنوان مثال:

- دانشی از شبکه سازمان و آسیب‌پذیری‌های آن مورد نیاز است: هر شبکه متفاوت است؛ توصیه مـی-شود سازمان تعیین کند که کدام دارایی‌های شبکه نیاز به حفاظت دارند و بـه احتمـال زیـاد کـدام تنظیمات نشانه حمله به این دارایی‌ها مرتبط است. این مورد به‌طورکلی از طریق انجام یـک فرآینـد ارزیابی مخاطره صورت می‌گیرد.
- عملکرد اغلب IDPSها می‌تواند در موردی که آن‌ها برای رسیدگی به حجـم محـدودی از ترافیـک و خدمات شبکه پیکربندی شده‌اند، به نسبت بهتر باشد. به عنـوان مثـال، سـازمانی کـه زیـاد تجـارت الکترونیکی انجام می‌دهد، ممکن است به پایش همه ترافیـک قـرارداد انتقـال ابـرمتن (HTTP) [3] و میزان کردن یک یا چند IDPS فقط برای جستجوی نشانه‌های حملـه مـرتبط بـا ترافیـک وب نیـاز

1- Deep packet inspection
2- Reassembly
3- Hypertext Transfer Protocol

داشته باشد.

- پیکربندی مناسب تعادل بار می‌تواند اجازه‌ی کار بسیار سریع‌تر و کامل‌تر را به IDPS مبتنی بر نشانه بدهد زیرا IDPS مبتنی بر نشانه تنها به یک دادگان کوچک‌تر بهینه‌سازی شده از نشانه حمله برای اجرا نیاز دارد و نه یک دادگان از همه نشانه‌های احتمالی حمله.

در استقرار IDPS، تعادل بار برای تقسیم پهنای باند در دسترس مورد استفاده قرار می‌گیرد. اگرچه تقسیم پهنای باند مشکلاتی از قبیل موارد زیر را محتمل می‌سازد:

هزینه‌های اضافی، سربار مدیریت، ناهمزمان‌سازی ترافیک، هشدار تکراری و منفی کاذب. علاوه بر این، فناوری فعلی IDPS در حال رسیدن به سرعت گیگابیت است و درنتیجه مزایا در مقابل هزینه‌های تعادل بار ممکن است کمینه باشد.

۵-۴-۵ درستی‌سنجی قابلیت‌ها

تکیه بر اطلاعات ارائه شده توسط فروشنده در مورد قابلیت‌های IDPS معمولاً کافی نیست. درخواست اطلاعات اضافی توسط سازمان و شاید نمایش شایستگی‌های یک IDPS ویژه برای محیط سازمان و اهداف امنیتی توصیه می‌شود. اکثر فروشندگان IDPS در مطابقت دادن محصولات خود به عنوان رشد دهنده‌ی شبکه‌های هدف تجربه دارند و برخی از آن‌ها به حمایت از استانداردهای جدید قرارداد، انواع سکوها، و تغییرات در محیط تهدید متعهد می‌شوند. توصیه می‌شود سازمان کمینه سؤالات زیر را از فروشنده‌ی IDPS بپرسد:

- چه فرضیاتی در ارتباط با کاربرد IDPS در محیط‌های ویژه ایجاد شده است؟
- جزئیات آزمون‌هایی که برای وارسی ادعاهای قابلیت‌های IDPS انجام شده است، چیست؟
- چه فرضیاتی مربوط به عملگرهای IDPS ایجاد شده است؟
- چه واسط‌های IDPS ای فراهم می‌شوند؟ (به‌طور مثال واسط‌های فیزیکی، قراردادهای ارتباطی، قالب گزارش‌دهی برای واسط بودن با موتورهای همبستگی انواع واسط‌های مهم می‌باشند)
- سازوکارهای صادرکردن هشدار یا قالب‌ها چیست و اینکه آیا به درستی مستند شده‌اند؟ (به‌طور مثال قالب و یا پیام‌های syslog و یا MIB برای پیام‌های SNMP)
- آیا واسط کاربری IDPS با استفاده از کلیدهای میانبر، ویژگی‌های هشدار قابل سفارشی سازی و نشانه حمله‌ها، در حین کار قابل پیکربندی است؟
- در موردی که IDPS در پرواز قابل پیکربندی است، آیا ویژگی‌هایی که این قابلیت را تأمین می‌کنند، مستند و پشتیبانی شده‌اند؟
- آیا محصول با رشد و تغییرات زیرساخت‌های سامانه‌های سازمان قابل انطباق است؟

- آیا محصول IDPS با شبکه ای گسترده و به‌طور فزاینده ای متنوع قابل انطباق است؟
- آیا IDPS قابلیت‌های شکست امن و عدم شکست را فراهم می‌کند و چگونه این قابلیت‌ها با قابلیت‌های مشابه در لایه پیوند شبکه یکپارچه می‌شوند؟
- آیا IDPS از یک شبکه اختصاصی برای هشدارها استفاده می‌کند و یا آن‌ها در همان شبکه‌ای که IDPS پایش می‌کند، انتقال داده می‌شوند؟
- اعتبار فروشنده از نظر تضمین کیفیت، پاسخ به آسیب‌پذیری‌های کشف شده و سابقه‌ی عملکرد محصولاتش چگونه است؟

۶-۴-۵ هزینه

اکتساب IDPS تنها هزینه‌ی مالکیت آن نیست. هزینه‌های اضافی شامل: استفاده از سامانه‌ای که نرم‌افزار IDPS را اجراکند، کمک اختصاصی در نصب و پیکربندی IDPS، آموزش کارکنان و هزینه‌های نگهداری است.کارکنان مدیریت سامانه و تحلیل نتایج بیشترین هزینه را در بردارند. یک روش فنی برای سنجش هزینهIDPS بازگشت سرمایه‌گذاری (ROI) یا تحلیل هزینه در مقابل سود است. در این مورد، ROI بر مبنای صرفه‌جویی‌هایی که در هنگام مدیریت حملات توسط سازمان محقق شده است، محاسبه می‌شود. هزینه‌ی اکتساب و عملکرد باید با هزینه کارکنان موردنیاز برای کمک به رفع هشدارها و سربار ناشی از هشدارهای منفی و پاسخ‌های نامناسب مانند نصب مجدد یک سامانه‌ی اطلاعاتی به دلیل عدم توانایی در تعیین اینکه چه مواردی به خطر افتاده است، متعادل گردد.

مزایای عملکردی IDPS شامل موارد زیر است:

- شناسایی تجهیزات معیوب و یا بد پیکربندی شده.
- درستی‌سنجی پیکربندی‌ها در هنگام بهره‌برداری.
- فراهم سازی آمار اولیه‌ی کاربری سامانه.

به‌منظور تصمیم‌گیری‌های مالی در مورد IDPS، سؤال‌هایی درباره‌ی هزینه کل مالکیت IDPS باید پاسخ داده شود. برای این کار، توصیه می‌شود هزینه استقرار IDPS در سراسر سازمان تحلیل شود. به عنوان یک کمینه، هزینه‌ی تحلیل IDPS برمبنای پاسخ به سؤالات زیر است:

- بودجه برای هزینه‌های سرمایه‌گذاری اولیه برای خرید IDPS چقدر است؟
- مدت زمان مورد نیاز برای کارکردهای IDPS چقدراست، به عنوان مثال ۷/۲۴ (۲۴ ساعت شبانه روز و ۷ روز هفته) یا کمتر؟
- چه زیرساخت هایی برای پردازش، تحلیل و گزارش خروجی‌های IDPS مورد نیاز است و چه هزینه‌ای در بر خواهد داشت؟

- آیا سازمان منابع انسانی و دیگر منابع مورد نیاز برای پیکربندی IDPS با خط‌مشی امنیتی سازمان برای عملکرد، نگهداری، به‌روزرسانی و پایش خروجی‌های IDPS و پاسخ به هشدارها در اختیار دارد؟ اگر نه، چگونه این کارکردها می‌تواند انجام شود؟
- آیا منابع مالی برای آموزش IDPS در دسترس است؟
- مقیاس استقرار چیست و اگر HIDPSها استفاده می‌شوند، چه تعدادی از میزبان‌ها حمایت خواهند شد؟

هزینه‌های یک سازمان ممکن است با به اشتراک گذاشتن هزینه‌های سربار از طریق برون‌سپاری کارکردهای پایش و نگهداری IDPS به یک تأمین‌کننده‌ی خدمات آشکارسازی نفوذ با مدیریت از دور کاهش یابد.
گران‌قیمت ترین بخش استقرار IDPS، بخش پاسخ است. دانستن اینکه چه پاسخی باید داده شود، ساختن گروه‌های پاسخ، توسعه و استقرار خط‌مشی پاسخ و آموزش و تمرین، هزینه‌های قابل‌توجهی دارد که باید ذکر شود.

۵-۴-۷ به‌روزرسانی‌ها

۵-۴-۷-۱ مرور کلی

اکثر IDPSها مبتنی بر نشانه حمله می‌باشند و ارزش IDPS به خوب بودن دادگان نشانه حمله که رویدادها با آن تحلیل می‌شوند وابسته است. آسیب‌پذیری‌ها و حملات جدید به‌صورت مکرر در حال کشف شدن می‌باشند. درنتیجه، دادگان نشانه حمله‌ی IDPS باید به‌طور مرتب به‌روز شود.
بنابراین، توصیه می‌شود یک سازمان عوامل زیر به عنوان کمینه در نظر بگیرد:

- به موقع بودن به‌روزرسانی‌ها؛
- اثربخشی توزیع داخلی.
- پیاده سازی؛
- تاثیر سامانه.

۵-۴-۷-۲ به موقع بودن به‌روزرسانی‌ها برای IDPS مبتنی بر نشانه

نگهداری از نشانه‌های حمله کنونی برای آشکارسازی حملات شناخته شده ضروری است. پاسخ به سؤالات کمینه زیر به‌منظور اطمینان از اینکه نشانه‌های حمله به موقع به‌روزرسانی شده‌اند، توصیه می‌شود:

- زمانی که یک بهره‌جویی و یا آسیب‌پذیری ویژه کشف شده است، فروشنده IDPS چقدر سریع به‌روزرسانی نشانه حمله را صادر می‌کند ؟

- آیا فرآیند اطلاع رسانی قابل اطمینان است؟

- آیا صحت و یکپارچگی به‌روزرسانی‌های نشانه حمله تضمین شده است؟

- آیا مهارت‌های کافی در موردی که نشانه‌های حمله باید برای سازمان سفارشی سازی شوند در دسترس

است؟

- آیا امکان نوشتن و دریافت نشانه‌های حمله سفارشی سازی شده به‌منظور پاسخ بی‌درنگ به یک آسیب‌پذیری در معرض مخاطره و یا حمله درحال پیشرفت وجود دارد؟

۵-۴-۷-۳ اثربخشی توزیع داخلی و پیاده‌سازی

آیا سازمان قادر به توزیع سریع و پیاده‌سازی به‌روزرسانی‌های ویژه‌ی محل در یک بازه زمانی مناسب برای تمام سامانه‌های مربوطه است؟ در بسیاری از موارد، به‌روزرسانی نشانه‌های حمله باید اصلاح شده تا آدرس‌های IP و درگاهی‌های ویژه‌ی محل را در برگیرد. به‌طور خاص، سؤالات کمینه زیر باید در سراسر مرزهای اعتماد شبکه‌ی شرکت پاسخ داده شوند:

- درصورتی‌که فرآیندهای توزیع دستی در محل وجود دارد، آیا مدیران یا کاربران نشانه حمله را در یک بازه زمانی قابل قبول پیاده سازی می‌کنند؟
- آیا اثربخشی فرآیندهای توزیع خودکار و نصب، قابل سنجش است؟
- آیا سازوکاری برای پیگیری مؤثر تغییرات در به‌روز رسانی‌های نشانه حمله وجود دارد؟

۵-۴-۷-۴ تاثیر سامانه

به‌منظور به کمینه رساندن اثر به‌روزرسانی‌های نشانه حمله روی عملکرد سامانه، سؤالات کمینه زیر باید پاسخ داده شوند:

- آیا به‌روزرسانی، نشانه حمله عملکرد خدمات و یا برنامه‌های کاربردی مهم را تحت تأثیر قرار می‌دهد؟
- آیا ممکن است در مورد به‌روزرسانی‌های نشانه حمله، انتخابی عمل کرد؟ این مورد ممکن است برای جلوگیری از برخوردها و یا اثرات عملکرد خدمات و یا برنامه‌های کاربردی ضروری باشد.

۵-۴-۸ راهبردهای هشدار

پیکربندی و بهره‌برداری IDPS باید بر مبنای خط‌مشی پایش سازمان باشد. توصیه می‌شود سازمان در حد کمینه اطمینان حاصل کند که IDPS می‌تواند از روش‌های ویژه‌ی هشداردهی که توسط زیرساخت‌های موجود سازمان استفاده می‌شود پشتیبانی کند. ویژگی‌های هشدار که ممکن است پشتیبانی شود عبارت‌اند از رایانامه، صفحه بندی، سامانه پیام کوتاه (SMS) [1]، رویداد قرارداد مدیریت شبکه ساده (SNMP) [2]، و حتی انسداد خودکار منابع حمله.

در موردی که داده IDPS برای مقاصد قانونی شامل تعقیب قانونی و گواهی برای نظم داخلی استفاده

1- Short Message System
2- Simple Network Management Protocol

می‌شود، داده IDPS باید کمینه در انطباق با الزامات قانونی و مقرراتی ارائه شده و اعمال شده توسط حوزه‌های قضایی محلی مدیریت و بکارگرفته شود.

۵-۴-۹ مدیریت شناسه

۵-۴-۹-۱ مرور کلی

مدیریت شناسه، شالوده‌ی حیاتی برای تحققِ تأمین و تصدیق امضا از دور IDPS بدون دخالت انسان است. هر یک از این قابلیت‌ها نیازمند ایجاد و استفاده از طرف‌های سوم مورد اعتماد به عنوان مرجع می‌باشند که با وجود برخی تفاوت‌ها، مشابه مرجعی هستند که اغلب به عنوان بخشی از یک زیرساخت کلید عمومی درنظر گرفته می‌شود. این قابلیت‌ها همچنین برای تغییرات شناسه و داده‌ی بدون درز، امن و وارسی شده IDPS در سراسر مرزهای اعتماد شبکه‌ی شرکت مهم است.

۵-۴-۹-۲ تصدیق امضا از دور

ممکن است IDPS میلیون‌ها خط کد داشته باشد. کشف درج عمدی نرم‌افزارهای مخرب در این پایگاه کد بزرگ دشوار است و می‌تواند به مهاجم اجازه دهد تا خروجی IDPS را وارسی کند. درنتیجه، وارسی شدید دسترسی اصالت‌سنجی شده روی سخت‌افزار و نرم‌افزار IDPS بسیار مهم است و باید مبتنی بر بخشی از شناسه موجودیت که درخواست دسترسی را می‌سازد صورت گیرد. تصدیق امضا از دور می‌تواند این قابلیت وارسی دسترسی را بدون حضور انسان در حلقه فراهم سازد.

تصدیق امضا از دور، در سخت‌افزار، یک گواهی رمزنگاشتی و یا تصدیق مقدار چکیده‌ساز برای شناسه‌ی یک افزاره یا نرم‌افزار در حال اجرا بر روی افزاره بدون دخالت کاربر تولید می‌کند. در ساده‌ترین شکل، شناسه توسط یک چکیده‌ساز رمزنگاشتی نمایش داده می‌شود، که اجازه می‌دهد برنامه‌های نرم‌افزاری و یا افزاره‌های مختلف از یکدیگر تمیز داده شده یا تغییرات در نرم‌افزار کشف شود. این گواهی ممکن است، در درخواست کاربر IDPS، برای هر طرف راه دور فراهم شده، و در اصل تأثیر اثبات کننده به آن طرف خواهد داشت که IDPS از نرم‌افزار مورد انتظار و بدون تغییر استفاده می‌کند. اگر نرم‌افزار بر روی IDPS تغییر یافت، گواهی تولیدشده تغییر پایگاه کد IDPS را منعکس خواهد کرد.

در مورد IDPS، هدف از تصدیق امضا از دور این است که تغییرات غیرمجاز در نرم‌افزار IDPS آشکارسازی شود. به عنوان مثال، اگر یک مهاجم یکی از برنامه‌های کاربردی IDPS یا بخشی از سامانه‌ی عامل IDPS به یک نسخه‌ی تغییریافته‌ی از روی بدخواهی را جایگزین‌کرده و یا تغییر دهد، مقدار چکیده‌ساز توسط خدمات از دور و یا نرم‌افزار دیگر به رسمیت شناخته نخواهد شد. درنتیجه، انحراف نرم‌افزار IDPS توسط ویروس و یا تروا می‌تواند توسط یک طرف راه دور آشکارسازی شود (به‌طور مثال مرکز عملکرد شبکه)، که پس از آن می‌تواند بر مبنای این اطلاعات عمل کند. به این دلیل که تصدیق امضا «از دور» است، باید به دیگران که IDPS با آن‌ها ارتباط دارد نیز گفته شود که یک IDPS ویژه به خطر افتاده است. بنابراین، آن‌ها می‌توانند تا زمان رفع این خطر از ارسال اطلاعات به آن جلوگیری نمایند.

به دلایل فوق، توصیه می‌شود IDPS وضعیت خود، پیکربندی، و دیگر اطلاعات مهم را به مرکز کارکردهای شبکه (NOC) از دور تصدیق امضا و یا گزارش بدهد. این قابلیت تصدیق امضا و یا اصالت‌سنجی IDPS برای توانایی ارزیابی سلامت IDPS و برای انجام پیکربندی‌ها و عملکردهای به‌روزرسانی متعدد IDPS مهم است. مخصوصاً، تصدیق امضا، توانایی آزمون یکپارچگی IDPS از دور است. با جمع شدن این گزارش‌های تصدیق امضای IDPS آگاهی موقعیتی در مورد وضعیت دفاعی شبکه فراهم شده و بخش مهمی از قابلیت آگاهی موقعیتی سراسری شبکه است.

۵-۴-۹-۳ تأمین

هنگامی که تصدیق امضا از دور مشکلی را در IDPS آشکارسازی می‌کند، اقدام اصلاحی برای کاهش مشکل مورد نیاز است. این مورد را می‌توان با اجازه دادن به NOC (مرکز کارکردهای شبکه) برای نشاندن پیکربندی اصالت‌سنجی شده، به‌روزرسانی‌های نرم‌افزار و وصله‌ها به IDPS به دست آورد. صنعت، اصطلاح «تأمین» را برای پوشش فرآیند بارگذاری نرم‌افزار مناسب، خط‌مشی امنیتی و داده‌ی پیکربندی برای افزاره‌های IT شامل IDPS اتخاذ کرده است. هدف از تأمین، عمل کردن تا حد امکان از دور است. هر دوی این موارد موجب صرفه جویی در هزینه نیروی انسانی برای بازدید فیزیکی IDPS شده و اجازه‌ی کاهش به موقع تر مشکلات و به خصوص به روزرسانی‌های نشانه حمله را فراهم می‌سازد. برای مؤثر بودن، قابلیت تأمین IDPS باید به‌صورت امن از جانب NOC تحت فشار قرار گرفته و همچنین به‌صورت امن توسط IDPS کشیده شود. در وضعیت دوم، IDPS باید یک قابلیت امن و خودکار برای جستجوی از دور به‌روزرسانی‌های جدید نرم‌افزار از وبگاه فروشنده و بارگیری به‌روزرسانی‌های اصالت‌سنجی شده بر اساس زمان داشته باشد.

۵-۵ ابزارهای مکمل IDPS

۵-۵-۱ مرور کلی

توصیه می‌شود سازمان نفوذ را به‌صورت بی‌درنگ آشکارسازی نموده و آسیب‌های ناشی از نفوذ را کاهش دهد. همچنین توصیه می‌شود سازمان درک کند که IDPS یک راه‌حل تنها و یا جامع برای تحقق این نیست. برخی از افزاره‌های شبکه و ابزارهای فناوری اطلاعات ممکن است قابلیت‌هایی که IDPS فراهم می‌کند را تأمین کنند. توصیه می‌شود سازمان استقرار چنین افزاره‌ها و ابزارهایی را برای تقویت و تکمیل قابلیت IDPS در نظر داشته باشد.

نمونه‌هایی از این افزاره‌ها و ابزارها عبارت‌اند از:

- وارسی کننده‌های یکپارچگی پرونده
- دیوار آتش و یا دروازه امنیتی
- هانی‌پات ها
- ابزارهای مدیریت شبکه

- ابزارهای امنیت اطلاعات و مدیریت رویداد (SIEM) [1]

- ابزارهای حفاظت از ویروس/محتوا

- ابزارهای ارزیابی آسیب‌پذیری

۲-۵-۵ وارسی کننده‌های یکپارچگی پرونده

وارسی کننده‌های یکپارچگی پرونده رده‌ی دیگری از ابزارهای امنیتی مکمل IDPS می‌باشند. آن‌ها از خلاصه‌ی پیام یا دیگر جمع‌های واپایشی [2] رمزنگاشتی برای پرونده‌ها و اشیاء مهم، مقایسه آن‌ها با مقادیر مرجع و پرچم زدن به تفاوت‌ها و یا تغییرات استفاده می‌کنند. استفاده از وارسی‌های رمزنگاشتی مهم است، از آن‌جایی‌که مهاجمان اغلب پرونده‌های سامانه را در سه مرحله از حمله تغییر می‌دهند. نخست، آن‌ها پرونده‌های سامانه را به عنوان هدف حمله تغییر می‌دهند (به عنوان مثال، قرار دادن اسب تروا). دوم، آن‌ها تلاش می‌کنند درب‌های تماس پشتی سامانه را باقی بگذارند تا در زمان‌های بعدی از طریق آن‌ها دوباره وارد شوند. در نهایت آن‌ها در تلاش برای پوشش ردیابی‌های خود می‌باشند به‌طوری‌که صاحبان سامانه از حمله بی‌اطلاع باشند.

مزایا:

- تعیین اینکه آیا وصله‌های اشکال عرضه شده‌ی فروشنده و یا دیگر تغییرات مطلوب به پرونده‌های باینری سامانه اعمال شده‌اند.

- اجازه تشخیص سریع و قابل اعتماد رد پای یک حمله، به ویژه هنگامی که یک بازرسی قانونی سامانه هایی که مورد حمله قرارگرفته‌اند، انجام شده است.

- مهاجمان اغلب پرونده‌های سامانه را تغییرداده یا جایگزین می‌کنند و از فنونی برای حفظ ویژگی‌های پرونده که به‌طور معمول توسط مدیران سامانه بررسی می‌شود، استفاده می‌کنند. ابزارهای وارسی یکپارچگی که از وارسی‌های رمزنگاشتی استفاده می‌کنند، بااین‌وجود می‌توانند هرگونه تغییرات و یا اصلاحات را آشکارسازی نمایند؛

- شناسایی اصلاحات پرونده‌های داده را اجازه می‌دهند.

معایب:

- ممکن است نیاز باشد در طول تحلیل، سامانه‌های اطلاعاتی و یا کمینه سامانه در حال وارسی، برون خط شده و یا خاموش شود.

1- Security Information and Event Management
2- Checksums

۵-۵-۳ دیوار آتش

نقش اصلی یک دیوار آتش (به عنوان مثال، به استاندارد ISO / IEC 27033-2 مراجعه شود) محدود کردن دسترسی بین شبکه‌ها است. دیوارآتش‌های ساده برای پالایش ترافیک شبکه مبتنی بر آدرس‌های قرارداد اینترنت (IP) منبع و مقصد و شماره درگاهی هایی که سازمان می‌خواهد دسترسی پذیر باشد، طراحی شده‌اند. به عنوان مثال، یک سازمان ممکن است تنها بخواهد ترافیک یک کارساز رایانامه (درگاهی شماره ۲۵) و یا یک کارساز وب (درگاهی شماره ۸۰) را بپذیرد. اگرچه، دیوارآتش در سطح برنامه کاربردی از اطلاعات قرارداد برنامه کاربردی برای فراهم سازی پالایه‌های پیچیده‌تر استفاده می‌کند. در صورتی دیوار آتش است در داخل یک قلمرو واقع شود، میزان ترافیکی که نیاز است NIDPS بررسی کند را کاهش می‌دهد.

بیشتر دیوارهای آتش دارای قابلیت‌های محدود برای پایش محتوای پیام‌های شبکه و اعلان هشدار در زمان تلاش ترافیک ممنوعه برای گذر از طریق دیوار آتش می‌باشند. در مقایسه، یک NIDPS به‌طور خاص برای بررسی بسته‌های شبکه، برای آشکارسازی آنچه که به منزله‌ی ترافیک قانونی و غیر قانونی است، طراحی شده است و می‌تواند هشداری را زمانی‌که محتوای مخرب در بسته‌های شبکه آشکارسازی می‌کند، اعلان نماید. در بسیاری از موارد، هشدار NIDPS می‌تواند برای تولید یک تغییر در پارامترهای فیلترکردن دیوار آتش در صورت مطلوب بودن استفاده شود.

درصورتی‌که NIDPS در سمت سازمان دیوارآتش مستقر شود، یک پیکربندی مناسب دیوار آتش به‌طور قابل‌توجهی حجم بسته‌های اطلاعاتی که باید توسط NIDPS مورد بررسی قرار گیرند را کاهش می‌دهد. این پیکربندی NIDPS تا حد زیادی می‌تواند دقت NIDPS را بالا ببرد زیرا درحالی‌که ترافیک ورودی وارسی می‌شود، خش پس زمینه اینترنت به دلیل فعالیت پویش می‌تواند حذف شود.

۵-۵-۴ هانی‌پات‌ها

هانی‌پات یک اصطلاح عمومی برای یک سامانه طعمه برای فریب، حواس پرتی، منحرف کردن و تشویق مهاجم برای صرف زمان روی اطلاعاتی است که بسیار ارزشمند به نظر می‌رسد، اما در واقع ساختگی است و موردعلاقه‌ی یک کاربر مشروع نیست. هدف اصلی هانی‌پات جمع‌آوری اطلاعات در مورد تهدیدها به یک سازمان و فریب و دور کردن مزاحمان از سامانه‌های حیاتی است.

هانی‌پات یک سامانه عملیاتی نیست و به عنوان یک سامانه اطلاعاتی طراحی شده که قادر است با تشویق مهاجمان به باقی ماندن روی خط برای مدت به اندازه کافی طولانی به خطر بیافتد تا سازمان بتواند هدف مهاجمان، سطح مهارت مهاجم و روش کارکرد او را ارزیابی کند.

اطلاعات به دست آمده از تحلیل فعالیت‌های مزاحمان در هانی پات اجازه می‌دهد تا سازمان تهدیدها و آسیب‌پذیری‌های سامانه‌ی خود را بهتر متوجه شده و درنتیجه عملیات IDPS سازمان را بهبود بخشد. با تحلیل اقدامات یک مزاحم در سامانه‌ی هانی‌پات، این اطلاعات می‌تواند به توسعه خط‌مشی IDPS سازمان،

دادگان نشانه‌های حمله و رویکردهای کلی سازمان در جهت بهترین شیوه‌های IDPS در حفاظت در برابر انواع تحلیل شده‌ی تهدیدات مهاجم کمک کند.

در تمام شرایط، توصیه می‌شود سازمان از هانی‌پات‌ها تنها پس از گرفتن راهنمایی از مشاور حقوقی استفاده کند. داده‌ی هانی‌پات ها، ممکن است به عنوان یک شکل از یک فن به دام انداختن در نظر گرفته شده و درنتیجه در برخی از حوزه‌های قضایی از نظر قانونی غیر قابل قبول باشد .

برخی از مزایا و معایب هانی‌پات‌ها عبارت‌اند از:

مزایا:

- مهاجمان را می‌توان به اهداف سامانه که نمی‌توانند به آن‌ها آسیب برسانند، منحرف کرد؛

- هانی‌پات‌ها فعالیت‌های مجاز انجام نمی‌دهند و درنتیجه هرگونه فعالیت گرفته شده توسط یک هانی‌پات مشکوک به نظر می‌رسد.

- مدیران زمان بیشتری برای تصمیم‌گیری اینکه چگونه به یک مهاجم پاسخ دهند، دارند؛

- اقدامات مهاجمان به راحتی و به‌طور گسترده‌تر با نتایج مورد استفاده برای اصلاح مدل‌های تهدید پایش شده و حفاظت سامانه را بهبود می‌بخشد.

- ممکن است در گرفتن یک خودی که در حال جاسوسی در اطراف یک شبکه است، مؤثر واقع شود.

معایب:

- مفاهیم حقوقی استفاده از چنین افزاره‌هایی به خوبی مشخص نشده است؛

- مهاجمی که یک بار به یک سامانه فریب منحرف می‌شود، ممکن است عصبانی شده و برای راه‌اندازی حمله خصمانه علیه سامانه‌های سازمان تلاش نماید.

- سطح بالایی از تخصص برای سرپرست‌ها و مدیران امنیتی به‌منظور استفاده از این سامانه‌ها مورد نیاز است.

۵-۵-۵ ابزارهای مدیریت شبکه

ابزارهای مدیریت شبکه از فنون مختلف کاوش فعال و غیر فعال برای پایش دسترس پذیری و عملکرد افزاره‌های شبکه استفاده می‌کنند. این ابزارها به عنوان یک کارکرد برای پیکربندی و مدیریت زیرساخت‌های شبکه با جمع‌آوری اطلاعات اجزاء و هم‌بندی شبکه در خدمت هستند.

همبستگی ابزارهای مدیریت شبکه یا سامانه با هشدارهای IDPS ممکن است به IDPS کمک کند تا به‌طور مناسب هشدارها را پردازش کرده و تأثیر آن‌ها بر سامانه‌های مورد پایش را ارزیابی نماید.

۵-۵-۶ ابزارهای مدیریت رویداد امنیت اطلاعات (SIEM)

سازمان‌ها از SIEM برای یکی کردن گزارش‌دهی از طریق پیشانه[1] مدیریت و هشدار استفاده می‌کنند. یک SIEM می‌تواند اطلاعات را از IDPS، دیوارهای آتش، شنودگرها و غیره جمع‌آوری کرده، سربار اطلاعات را کاهش داده و حجم عظیمی از اطلاعات را برای وارسی تحلیلگر قابل مدیریت سازد. دومین دلیل اصلی این است که این مجموعه داده از یک نظر می‌تواند همبستگی چندین حمله‌ی کوچک با یک بسته واحد، از منبع‌های متعدد، در طول زمان طولانی و تحت رادار را که ممکن است برای یک IDPS منفی کاذب شود، ایجاد کند.

ابزارهای امنیت اطلاعات و مدیریت رویداد (SIEM) نیز ممکن است برای پردازش داده‌های به دست آمده توسط IDPS مورد استفاده قرار گیرند. به‌طور معمول، ابزارهای SIEM برای اجرای قابلیت‌های زیر استفاده می‌شوند:

- جمع‌آوری و نگهداری داده‌های رویداد مربوط به امنیت از منابع مختلف در یک دادگان مرکزی. این مورد می‌تواند شامل داده‌هایی از یک یا چند IDPS، پرونده‌های ثبت رویداد از افزاره‌های شبکه و میزبان‌ها و همچنین داده‌ی رویداد از ابزارهای ضد ویروس باشد.

- پردازش بیشتر داده‌ی جمع‌آوری شده، به خصوص ارائه پالایه‌ی گسترده، قابلیت‌های تجمع و همبستگی؛

- همبستگی رویداد با ساختن زمینه‌ی بین رویدادهای امنیتی و حتی غیرامنیتی برای آشکارسازی نقض‌های امنیتی که به الگوها مربوط نمی‌باشند.

- پالایش رویداد با کاهش سطح هشدار مبتنی بر همبستگی با توجه به ارتباط، به‌طور مثال هشدارهای IDPS و سطح وصله‌های امنیتی.

- تجمع رویداد با جمع‌آوری و بهنجارسازی رویدادها بر اساس به‌طور مثال منبع، مقصد، زمان، توصیف رویداد و غیره برای کاهش سرریزهای هشدار IDPS؛

- ارائه‌یک واسط ساده و مفید برای گزارش‌دهی هشدارهای مربوطه و ارائه کمک برای تحلیل بیشتر و عمیق‌تر این هشدارها مبتنی بر داده‌ی جمع‌آوری شده.

هدف اصلی ابزارهای SIEM فراهم کردن یک روش خودکار برای تمایز بین هشدارهای مربوطه، وانمودکننده‌ی یک تهدید با احتمال بالا و هشدارهای غیر مرتبط و یا حتی مثبت کاذب که وانمود کننده‌ی هیچ تهدیدی نیستند، است. پیکربندی مناسب ابزارهای SIEM پیش نیاز ضروری برای رسیدن به این هدف است و توصیه می‌شود سازمان آن را به عنوان یک کار مهم در هنگام برنامه ریزی معرفی ابزار SIEM در نظر بگیرد. مشابه سامانه‌های IDPS، پیکربندی نیاز به درجه بالایی از تخصص و مقدار کار قابل‌توجهی دارد. با تنظیم و پیکربندی مناسب، ابزارهای SIEM می‌توانند ارزش افزوده‌ی بالایی فراهم کنند، و به خصوص می‌توانند اطلاعات با ارزشی برای راه‌اندازی فرآیندهای بیشتر و فعالیت‌هایی مانند مدیریت رویداد فراهم

1- Console

سازند.

۵-۵-۷ ابزارهای حفاظت از محتوی/ویروس

ابزارهای حفاظت از محتوا یا ویروس ممکن است IDPS را با تأمین داده‌های اضافی برای تحلیل متقابل ترافیک و اطلاعات ویژه در مورد منشأ ویروس‌ها تکمیل کنند.

۵-۵-۸ ابزارهای ارزیابی آسیب‌پذیری‌ها

ارزیابی آسیب‌پذیری‌ها بخش جدایی‌ناپذیر از ارزیابی مخاطره و یک مولفه باارزش از راهبردهای وارسی و پایش ممیزی/انطباق امنیتی مناسب است. این نوع ارزیابی اجازه می‌دهد تا یک سازمان آسیب‌پذیری‌ها را بیابد و در اغلب موارد اقدامات اصلاحی به‌منظور کاهش فرصت یک مزاحم برای بهره‌جویی توصیه می‌کند. بنابراین، استفاده از ارزیابی آسیب‌پذیری می‌تواند به‌طور قابل‌توجهی تعداد حملاتی که IDPS باید به دنبال آن‌ها باشد کاهش دهد.

ارزیابی آسیب‌پذیری بر ارزیابی مواجهه‌ی یک میزبان داده شده به یک آسیب‌پذیری داده شده متمرکز شده است. این فرآیند ارزیابی همان اجرای اسکریپت[1] حمله نیست. درنتیجه، خرابی IDPS در آشکارسازی فعالیت ارزیابی آسیب‌پذیری نشان نمی‌دهد که IDPS نمی‌تواند حمله را آشکارسازی کند. در مقابل، آشکارسازی فعالیت پویش آسیب‌پذیری‌ها توسط IDPS به این معنا نیست که همان IDPS می‌تواند حمله را به درستی آشکارسازی کند.

ابزارهای ارزیابی آسیب‌پذیری برای آزمون آمادگی یک میزبان شبکه برای مصالحه استفاده شده است. استفاده از ابزارهای ارزیابی آسیب‌پذیری در ترکیب با IDPS یک روش بسیار گران‌بها برای بررسی اثربخشی IDPS در هر دو مورد آشکارسازی و واکنش به حملات فراهم می‌کند. ابزارهای ارزیابی آسیب‌پذیری به عنوان یکی از دو حالت مبتنی بر میزبان یا شبکه طبقه‌بندی شده‌اند. ابزارهای آسیب‌پذیری مبتنی بر میزبان امنیت یک سامانه اطلاعات را توسط پرس و جوی منابع داده‌ها مانند محتویات پرونده‌ها، جزئیات پیکربندی و دیگر اطلاعات وضعیت ارزیابی می کنند. یک ابزار مبتنی بر میزبان اجازه دسترسی به میزبان هدف که در آن از طریق یک اتصال از دور در حال اجرا است، دارد. ابزارهای آسیب‌پذیری مبتنی بر شبکه برای پویش تعدادی از میزبان برای آسیب‌پذیری‌های مربوط به خدمات شبکه استفاده می‌شوند. به‌منظور انجام ارزیابی آسیب‌پذیری میزبان یا شبکه، سطح مناسبی از مدیریت در سازمان باید آزمون را تائید کند. تأکید این نکته مهم است که استفاده از ابزارهای ارزیابی آسیب‌پذیری مکمل استفاده از IDPS است و نمی‌تواند به عنوان یک جایگزین در نظر گرفته شود.

مزایا و معایب استفاده از ابزارهای ارزیابی آسیب‌پذیری عبارت‌اند از:

مزایا:

1- Script

- ابزارهای ارزیابی آسیب‌پذیری یک روش مؤثر برای مستندسازی وضعیت امنیتی سامانه اطلاعات و موردی که برقراری مناسب دوباره‌ی یک پایه امنیتی برای بازگشت به آن بعد از تغییرات سامانه صورت می‌گیرد، فراهم می‌سازند.

- ابزارهای ارزیابی آسیب‌پذیری درصورتی‌که بر اساس یک قاعده استفاده شوند، می‌توانند تغییرات در وضعیت امنیتی یک سامانه اطلاعاتی را به‌طور قابل اعتماد شناسایی کنند.

- بزرگ‌ترین مزیت ابزارهای ارزیابی آسیب‌پذیری کمک در شناسایی آسیب‌پذیری‌ها است؛

- به سازمان‌ها اجازه می‌دهد تا داده‌ی حمله را با آسیب‌پذیری‌های شناخته شده برای تعیین اینکه آیا حمله موفقیت‌آمیز بوده مطابقت دهند؛

معایب و مسائل:

- ابزارهای ارزیابی آسیب‌پذیری مبتنی بر میزبان، بستره و نرم‌افزار خاص دارند و معمولاً ساخت، مدیریت و نگهداری آن‌ها پرهزینه‌تر از ابزارهای مبتنی بر شبکه است؛

- ابزارهای ارزیابی آسیب‌پذیری مبتنی بر شبکه مستقل از بستر هستند و به نسبت ابزارهای مبتنی بر میزبان کمتر خاص می‌باشند.

- ارزیابی آسیب‌پذیری یک فعالیت مصرف‌کننده‌ی منابع است و ممکن است غیرعملی باشد و یا ممکن است تنها در قبال هزینه‌ی کاهش عملکرد سامانه و یا شبکه عمل کند و یا ممکن است تنها با محدودیت‌های تاریخ و زمان عمل کند.
- در بسیاری از موارد، ارزیابی آسیب‌پذیری یک فعالیت تناوبی است که در مقابل پیوسته بودن، به‌صورت هفتگی، ماهانه و یا حتی به‌صورت تصادفی انجام می‌شود و درنتیجه آشکارسازی به موقع مسائل امنیتی ممکن است در بهترین حالت یک چالش باشد و گاهی اوقات غیرممکن شود.
- مشابه IDPS، ابزارهای ارزیابی آسیب‌پذیری در معرض مثبت‌های کاذب و یا منفی‌های کاذب قرار دارند و توصیه می‌شود به‌دقت مورد تحلیل قرار گیرند؛
- ارزیابی آسیب‌پذیری مکرر می‌تواند بسیاری از IDPSهای مبتنی بر ناهنجاری را آموزش داده تا از حملات واقعی چشم‌پوشی نمایند؛
- نیاز برای به‌روزرسانی نشانه حمله؛
- ابزار ارزیابی آسیب‌پذیری مبتنی بر میزبان، سامانه‌های غیرمجاز را در شبکه شما آشکارسازی نخواهد کرد.

آزمون ارزیابی آسیب‌پذیری شبکه باید به سامانه‌های هدف محدودشده و باید برای حفظ حریم خصوصی هرگونه اطلاعات جمع‌آوری شده در طول این فرآیند مراقبت صورت گیرد. داده‌های جمع‌آوری شده توسط

ابزارهای آسیب‌پذیری، به اطلاعاتی که می‌تواند توسط یک مزاحم برای بهره‌جویی از سامانه‌های سازمان مورد استفاده قرار گیرد نفوذپذیر است و درنتیجه باید محافظت شود.

۵-۶ مقیاس‌پذیری

توصیه می‌شود سازمان قبل از متعهد شدن به استفاده از یک IDPS خاص مقیاس‌پذیری آن را بررسی کند. کارکرد مناسب بسیاری از IDPSها در نرخ‌های پایین داده است، اما با افزایش پهنای باند از تنزل عملکرد رنج می‌برند. تنزل عملکرد به‌طور معمول منجر به افزایش قابل‌توجه خطاها می‌شود که با دور ریخته شدن بسته‌های بیشتر و بیشتر و خطا در پردازش آن، هشدارهای منفی کاذب (زمانی که یک حمله به وقوع پیوسته است هشداری را تولید نمی‌کند) و مثبت کاذب (تولید هشدار زمانی که هیچ حمله‌ای وجود ندارد) تولید می‌شوند. به عبارت دیگر، بسیاری از IDPSها قادر به مقیاس‌پذیری در محیط شبکه‌های بزرگ و دارای توزیع گسترده‌ی شرکت‌ها نمی‌باشند.

نگرانی‌های مقیاس‌پذیری عمدتاً در استقرار NIDPS قابل اعمال است، اما به HIDPS نیز در مورد دستگاه‌های میزبان که به عملکرد بالا نیاز دارند اعمال می‌شود.

۵-۷ پشتیبانی فنی

مانند سامانه‌های دیگر، سامانه IDPS نیز نیاز به پشتیبانی و نگهداری دارد. سامانه‌های IDPS فناوری‌های «اتصال و اجرا» نیستند. بسیاری از فروشندگان کمک تخصصی به مشتریان را در نصب و پیکربندی IDPS تأمین می‌کنند. دیگران انتظار دارند که کارکنان سازمان این کارکردها را اداره کنند و تنها کارکردهای شماره تلفن یا رایانامه میز کمک را فراهم می‌سازند.

درجه پشتیبانی فنی به ماهیت مقدمات قراردادی سازمان با فروشنده‌ی IDPS وابسته است و به‌صورت مورد به مورد اجرا می‌شود. در حد کمینه، پشتیبانی فنی باید شامل کمک فروشنده در تنظیم یا تطبیق IDPS برای وفق دادن آن با نیازهای ویژه‌ی سازمانی، اینکه آیا آن‌ها در حال پایش سامانه‌های سفارشی و یا میراثی در یک شرکت می‌باشند، یا گزارش نتایج IDPS در یک قرارداد یا قالب سفارشی باشد.

سازمان باید ابزارهایی را برای تماس با پشتیبانی فنی (به عنوان مثال، رایانامه، شماره تلفن، گپ‌زدن برخط[1]، گزارش مبتنی بر وب، پایش از دور یا خدمات پاسخ) تعیین کند. مفاد قرارداد به‌طور معمول می‌تواند این خدمات پشتیبانی فنی و زمان‌های پاسخ را مشخص کند. قرارداد با فروشنده باید برای چنین خدماتی در یک اسلوب به اندازه‌ی کافی دسترس‌پذیر برای پشتیبانی رسیدگی به رخداد و یا دیگر نیازهای نفوذپذیر به زمان فراهم شود.

۵-۸ آموزش

فناوری به تنهایی برای آشکارسازی نفوذهای سامانه کافی نیست. یک سازمان به کارکنان فنی واجد شرایط

1- Online chat

برای ارزشیابی، انتخاب، نصب، کارکرد، و نگهداری IDPS نیازمند است. تقاضا برای کارکنان واجد شرایط IDPS بسیار زیاد است و در بسیاری از شرایط گرفتن نیروی تازه، استخدام، و حفظ کارکنانی که دارای تجربه و دانش مورد نیاز برای تحقق مسئولیت‌های IDPS بسیار دشوار است. با توجه به این وضعیت، بسیاری از سازمان‌ها تصمیم به برون‌سپاری کارکردهای IDPS به یک خدمت مدیریت امنیت می‌گیرند. این گزینه خود مسائل و مخاطرات آموزش سازمانی را معرفی می‌کند. به‌طور مثال، حتی در موردی که اغلب کارکردهای در حال اجرا برون‌سپاری شده‌اند، سازمان باید کارکنان را با دانش قابل‌توجهی در مورد مسائل و کارکردهای IDPS آموزش داده و یا می‌تواند واپایش فرآیند IDPS را به دیگران بدهد. برای این‌که سازمان از IDPS استفاده بهینه داشته باشد، کارکنان سازمان مسئول پایش کارکردهای برون‌سپاری شده‌ی IDPS باید با کارکردها و روال‌های IDPS آشنا شوند. این نوع آموزش عموماً از جانب فروشندگانی که محصولات IDPS را فراهم می‌کنند، در دسترس است. توصیه می‌شود سازمان این نوع آموزش فروشنده را به عنوان بخشی از هزینه خرید IDPS به حساب آورد.

درصورتی‌که فروشنده IDPS آموزش را به عنوان بخشی از بسته IDPS تأمین نکند، سازمان باید بودجه‌ی مناسبی را برای آموزش کارکنان عملیاتی درنظر بگیرد. این آموزش باید به‌صورت مستمر ارائه شود تا امکان تعویض و تغییرات کارکنان را به IDPS و محیط آن فراهم سازد.

۶ استقرار

۶-۱ مرور کلی

بر اساس ضوابطی که پیش از این در این سند فراهم شده است، استقرار موفقیت‌آمیز HIDPS یا NIDPS را تنها می‌توان با موارد زیر به دست آورد:

- تحلیل کامل نیازمندی‌ها، شامل نیازهای امنیتی IDPS ، بر اساس یک ارزیابی مخاطره،
- انتخاب دقیق یک راهبرد استقرار IDPS؛
- شناسایی یک راه‌حل که با زیرساخت‌های شبکه سازمان،خط‌مشی‌ها و سطح منابع سازگار باشد؛
- تعمیر و نگهداری تخصصی IDPS و آموزش کارکردها.
- مستندسازی آموزش و روال‌های تکرار برای رسیدگی و پاسخ به هشدارهای IDPS.

با توجه به مزایا و محدودیت‌های دو نوع عمده از IDPSها، سازمان باید ترکیبی از IDPS مبتنی بر شبکه و IDPS مبتنی بر میزبان را برای حفاظت از شبکه‌ی گسترده در سطح شرکت در نظر داشته باشد.

۶-۲ استقرار مرحله‌ای

سازمان‌ها باید یک استقرار مرحله‌ای برای IDPS در نظر بگیرند. این رویکرد می‌تواند به کارکنان اجازه دهد تا با کسب تجربه، معین کنند که چه تعداد منابع پایش و نگهداری برای پشتیبانی از کارکردهای IDPS

می‌تواند مورد نیاز باشد. منابع مورد نیاز برای هر نوع از IDPS به‌طور گسترده‌ای متفاوت بوده و به‌شدت به سامانه‌های سازمان و محیط‌های امنیتی آن وابسته است.

در یک استقرار مرحله‌ای، توصیه می‌شود سازمان با IDPS مبتنی بر شبکه شروع کند. معمولاً NIDPS ساده‌ترین مورد برای نصب و نگهداری است. گام بعدی محافظت از کارسازهای بحرانی با IDPS مبتنی بر میزبان است. علاوه بر این، سازمان باید ابزارهای ارزیابی آسیب‌پذیری را نیز در یک برنامه منظم برای آزمون IDPS و دیگر سازوکارهای امنیتی برای عملکرد و پیکربندی مناسب، مورد استفاده قرار دهد.

۶-۳ استقرار NIDPS

۶-۳-۱ مرور کلی

همان‌طور که با یک HIDPS، یک سازمان اطمینان حاصل می‌کند که کاروَرها با NIDPS در یک محیط واپایش شده اما با آزمون و آموزش فعال آشنا شده‌اند. موقعیت‌های مختلف حسگرهای NIDPS را می‌توان قبل از استقرار در مقیاس کامل در یک شبکه عملیاتی آزمایش کرد. موقعیت متعارف حسگرهای NIDPS در ادامه شرح داده شده و در شکل ۲ نمایش داده شده است. در استقرار حسگرهای شبکه، سازمان باید هزینه‌های استقرار و کارکردهای در حال انجام را در مقابل سطح واقعی حفاظت مورد نیاز متعادل سازد.

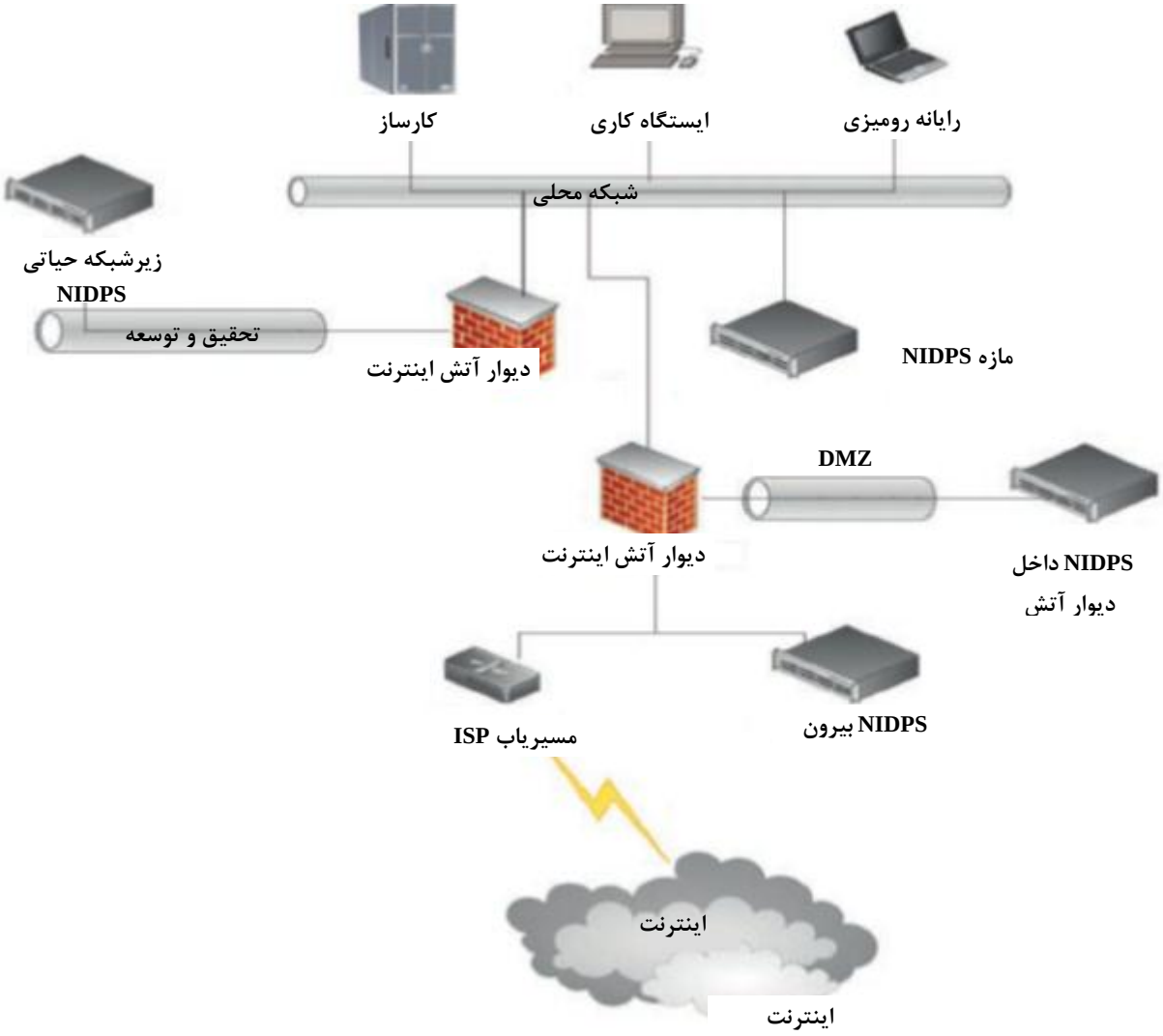
علاوه بر این، به‌ویژه در محیط شبکه‌های با سرعت بالا، مشاهده‌ی سطح بسته‌های IP از دست رفته مورد نیاز است زیرا نرخ‌های افت سطح بالا می‌تواند به‌شدت مقدار عدم هماهنگی الگو را افزایش داده و به افزایش مثبت کاذب و یا حتی منفی کاذب می‌انجامد. به عنوان یک راه چاره کارت‌های واسط مناسب شبکه با ارائه‌ی نرخ جذب بالاتر و یا فناوری‌های مشابه برای کاهش افت بسته ممکن است برای اطمینان از اثربخشی مورد نیاز باشد.

در هنگام استقرار NIDPS برای پایش شبکه، روش ضبط داده‌ها باید در نظر گرفته شود. به خصوص، در موردی که سوده یا TAP (آزمون دسترسی درگاهی) مورد استفاده قرار می‌گیرد. سازمان باید در هنگام استقرار NIDPS از یک سوده مجزا از نظر فیزیکی استفاده کند و VLANو یا فناوری مشابهی بر روی سوده مرکزی قرار نگیرد. سوده‌ها به‌طور معمول در هر زمان، تنها می‌توانند اجازه دهند یک درگاهی به منظور تحلیلگر درگاهی سوده[1] (SPAN) عملیاتی باشد. درگاهی SPAN همچنین کاربری پردازنده سوده را افزایش می‌دهد، و به‌طور معمول برای متوقف کردن تکرار داده‌ها درصورتی‌که CPU به آستانه بهره‌برداری رسیده باشد، طراحی شده است.

به طور مشابه، در موردی که این درگاهی برای اشکال زدایی شبکه استفاده شود، IDPS غیر کارکردی می‌شود. سازمان باید این درگاهی را به کارکرد NIDPS اختصاص دهد. برای رسیدگی به این موضوع، سازمان باید یک شبکه TAP (آزمون دسترسی درگاهی) به خصوص یک TAP متراکم در نظر بگیرد که جریان‌های بالا خطی و پایین خطی را ترکیب نماید. این افزاره‌ها به‌طور معمول افزاره‌های غیر فعال هستند

1- Switch Port Analyser

که هیچ سرباری را به بسته متصل نمی‌کنند. آن‌ها همچنین سطح امنیتی را کـه واسـط مجموعـه داده‌هـا را برای شبکه قابل‌دیدن می‌سازد، افزایش می‌دهند که در آن یک سوده هنوز هم می‌تواند اطلاعات لایه‌ی ۲ در مورد درگاهی را نگهداری کند. یک TAP همچنین قابلیت‌های چندین درگاهی متعدد را مـی‌دهـد درنتیجـه مسائل مربوط به شبکه را می‌توان بدون از دست دادن قابلیت IDPS اشکال زدایی نمود.



شکل ۲- موقعیت‌های عادی NIDPS

۲-۳-۶ موقعیت NIDPS داخل دیوار آتش اینترنت

مزایا:

- شناسایی حملات نشات گرفته از شبکه‌های بیرونی که از دفاع‌های پیرامون به داخل نفوذ کرده‌اند.
- می‌تواند به آشکارسازی خطاها در خط‌مشی‌های پیکربندی دیوار آتش کمک کند؛
- پایش حملات با هدف سامانه‌های موجود در DMZ (ناحیه‌ی غیرنظامی)؛

- می‌تواند برای آشکارسازی حملات علیه اهداف خارجی نشات گرفته از درون سازمان، پیکربندی شود.

معایب:

- با توجه به نزدیکی آن به شبکه‌های خارجی با قدرت محافظت نمی‌شود؛

- قادر به پایش حملاتی که توسط دیوار آتش مسدود شده‌اند (پالایش شده‌اند) نیست.

۶-۳-۳ موقعیت NIDPS خارج دیوار آتش اینترنت

مزایا:

- اجازه‌ی مستندسازی تعداد و نوع حملات نشات گرفته از شبکه‌های خارجی را فراهم می‌سازد؛

- قابلیت دیدن حملاتی که توسط دیوار آتش مسدود شده‌اند (پالایش شده‌اند).

- توانایی کاهش اثر حملات انکار خدمت.

- در صورتی در ترکیب با IDPS واقع شده در داخل دیوار آتش خارجی استفاده شود، پیکربندی این IDPS می‌تواند اثربخشی دیوار آتش را ارزیابی کند.

معایب:

- ازآنجایی‌که حسگر خارج از محدوده‌ی امنیتی شبکه واقع شده است، در معرض حمله به خود قرار گرفته و درنتیجه نیاز است یک افزاره‌ی مقاوم و پوشیده باشد؛

- مقدار زیادی از اطلاعات تولیدشده در این مکان باعث می‌شود تحلیل داده‌های جمع‌آوری شده‌ی IDPS بسیار دشوار باشد.

- تعامل بین حسگر IDPS و پیشانه‌ی مدیریت ممکن است نیازمند حفره‌های اضافی در دیوار آتش باشد که به دسترسی خارجی احتمالی به پیشانه مدیریت منجر می‌شود.

۶-۳-۴ موقعیت NIDPS روی مازه‌ی اصلی شبکه

مزایا:

- پایش حجم زیادی از ترافیک شبکه، درنتیجه احتمال حملات تشخیص[1] را افزایش می‌دهد.

- در موردی که IDPS از مازه‌ی اصلی شبکه پشتیبانی می‌کند، قابلیت مسدود کردن حملات انکار خدمت وجود دارد، قبل از اینکه آن‌ها بتوانند به زیرشبکه‌های حیاتی آسیبی را تحمیل کنند.

- فعالیت‌های غیرمجاز توسط کاربران مجاز را در محدوده‌ی امنیتی سازمان آشکارسازی می‌کند.

معایب:

1- Spotting attacks

- مخاطره‌ی ضبط و ذخیره سازی داده‌های نفوذپذیر یا محرمانه؛

- IDPS باید مقادیر زیادی از داده را پردازش کند؛

- حملاتی که از مازه عبور نمی‌کنند آشکارسازی نخواهند شد.

- حملات میزبان به میزبان بر روی یک زیرشبکه شناسایی نخواهد شد.

۶-۳-۵ موقعیت NIDPS روی زیرشبکه‌های بحرانی

مزایا:

- پایش حملاتی که در سامانه‌های بحرانی، خدمات و منابع هدفمند شده‌اند.

- تمرکز بر منابع محدود به دارایی‌های شبکه با در نظرگرفتن بیشترین ارزش را مجاز می‌داند.

معایب:

- با همبستگی رویدادهای امنیتی بین زیرشبکه‌ها دارای مشکل است.

- اگر هشدارها بر روی یک شبکه اختصاصی منتقل نشوند، ترافیک مربوط به IDPS ممکن است بار شبکه را روی زیرشبکه‌های بحرانی افزایش دهد.

- اگر به‌طور نادرست پیکربندی شود، IDPS ممکن است اطلاعات نفوذپذیر را ضبط و ذخیره سازی نموده و به این اطلاعات به شیوه‌ای نامشخص دسترسی دهد.

۶-۴ استقرار HIDPS

پیش از استقرار عملیاتی یک HIDPS سازمان باید اطمینان حاصل کند که کاروَرها با ویژگی‌ها و قابلیت‌های در یک محیط محافظت شده، اما فعال، آشنا شده‌اند. اثربخشی هر IDPS، و به خصوص HIDPS، بستگی به توانایی کاروَر آن در تشخیص تمایز بین هشدار واقعی و کاذب است که نیازمند دانشی درباره‌ی هم‌بندی شبکه‌ی سازمان، آسیب‌پذیری‌ها، و دیگر جزئیات مرتبط با حل‌وفصل هشدارهای کاذب است. تجربه عملیاتی در طول زمان می‌تواند انواع فعالیت‌های بهنجار و یا پایه را در محیطی که توسط HIDPS تحت پایش است، شناسایی کند. ازآنجایی که معمولاً HIDPS به‌طور مداوم تحت پایش نیست، توصیه می‌شود سازمان یک برنامه‌ی زمان‌بندی برای وارسی خروجی‌های IDPS ایجاد کند. این حالت از عملکرد HIDPS به‌طور قابل‌توجهی مخاطره‌ی مداخله‌ی مهاجم در HIDPS را در این دوره از یک حمله کاهش می‌دهد.

استقرار تمام مقیاس HIDPS باید با کارسازهای مهم آغاز شود. زمانی که عملیات HIDPS به‌صورت عادی درآمد، کارسازهای دیگر می‌توانند برای استقرار HIDPS در نظرگرفته شوند. نصب HIDPS در هر میزبان در سازمان می‌تواند گران قیمت و زمان بر باشد، زیرا هر IDPS باید برای هر میزبان ویژه نصب و پیکربندی شود. بنابراین، سازمان باید اول HIDPS را تنها در کارسازهای بحرانی نصب کند. این رویکرد می‌تواند هزینه‌های کلی استقرار را کاهش داده و اجازه می‌دهد کارکنان بی‌تجربه بر روی هشدارهایی که از مهم‌ترین

دارایی‌ها تولید می‌شوند، تمرکز کنند. هنگامی که این بخش از عملیات HIDPS به حالت عادی درآمد، سازمان ممکن است بخواهد دوباره نتایج ارزیابی مخاطره امنیتی اطلاعات اولیه را بررسی کرده و نصب HIDPSهای بیشتر را در نظر داشته باشد. توصیه می‌شود سازمان سامانه‌ی HIDPS را به کار بگیرد که این سامانه دارای مدیریت متمرکز و کارکردهای گزارش‌دهی است. این ویژگی‌ها به‌طور قابل‌توجهی می‌تواند پیچیدگی مدیریت هشدارهای HIDPS هایی که در سراسر سازمان مستقر شده‌اند، را کاهش دهد. درصورتی‌که تعداد قابل‌توجهی از HIDPSها مستقر شده‌اند، سازمان ممکن است بخواهد عملیات و نگهداری HIDPS را به یک خدمت مدیریت امنیت اطلاعات برون‌سپاری نماید.

۵-۶ حراست و حفاظت امنیت اطلاعات IDPS

دادگان IDPS تمام داده‌های مربوط به فعالیت‌های مشکوک و حملات در داخل زیرساخت‌های اطلاعات سازمان را ذخیره سازی می‌کند درنتیجه نفوذپذیر به امنیت است. بنابراین حفاظت از داده‌ها مورد نیاز است و واپایش‌های کمینه زیر یا معادل آن‌ها توصیه می‌شود:

- استفاده از جمع واپایشی به‌منظور درستی‌سنجی یکپارچگی داده‌های ذخیره شده.

- رمزگذاری داده‌ی IDPS ذخیره شده.

- پیکربندی مناسب دادگان، به خصوص از طریق استفاده از سازوکارهای واپایش دسترسی.

- فنون نگهداری مناسب دادگان شامل روش‌های اجرایی پشتیبان گیری؛

- به اندازه کافی سخت شدن سامانه‌هایی که در حال اجرای دادگان IDPS هستند، برای مقاومت در برابر نفوذها؛

- شنود[1] بافه[2]ها (فقط دریافت) برای اتصال IDPS به هاب و یا سوده اترنت.

- پیاده سازی یک شبکه مدیریت IDPS جداگانه.

- ارزیابی آسیب‌پذیری به‌طور منظم و آزمون نفوذ در IDPS و سامانه‌های متصل.

ثبت رویدادها[3] همچنین باید بر روی یک میزبان مجزای ثبت رویداد و نه بر روی سامانه محلی ذخیره شود. ثبت رویدادهای مربوط به IDPS، پیکربندی، نشانه حمله و اطلاعات ردوبدل شده بین حسگرهای IDPS و جمع کننده‌ها، باید در برابر تغییر غیرمجاز و یا حذف شدن محافظت شوند.

ثبت رویدادهای مربوط به IDPS ممکن است شامل اطلاعات نفوذپذیر و یا مربوط به حریم خصوصی باشد و باید در ذخیره سازی و انتقال محافظت شود. افراد مجاز مسئول برای تحلیل اطلاعات حسگرهای IDPS و یا جمع‌کننده‌ها باید از اطلاعات حراست کنند.

1- Sniff
2- Cable
3- Logs

۷ عملیات

۷-۱ مرور کلی

قبل از مرحله کارکردهای IDPS، توصیه می‌شود سازمان:

- فرآیندها، روش‌های اجرایی و سازوکارهایی که اطمینان می‌دهند IDPS توسط فرآیند مدیریت آسیب‌پذیری سازمان تحت پوشش قرار گرفته، برپا شوند.

- آماده سازی یک فرآیند مدیریت رخداد مطابق با ISO / IEC 27035.

- تعریف اقداماتی که زمانی که یک IDPS یک هشدار تولید می‌کند باید انجام شوند؛

- شناسایی شرایطی که تحت آن پاسخ‌های خودکار و نیمه خودکار مجاز هستند و چگونه نتیجه این نوع پاسخ را می‌توان پایش کرد برای اطمینان از اینکه یک اقدام امن و مناسب اجرا شده است.

- توضیح دادن و آماده‌سازی ملاحظات قانونی.

۷-۲ تنظیم IDPS

به دنبال استقرار IDPS، توصیه می‌شود سازمان تصمیم‌گیری کند که کدام ویژگی‌های هشدار IDPS، چه زمانی و چگونه می‌تواند مورد استفاده قرار گیرد و اطمینان حاصل شود که این ویژگی‌ها به‌طور معمول تنظیم می‌شود.

اغلب IDPSها با ویژگی‌های هشدار قابل تنظیم ارائه می‌شوند، که اجازه می‌دهد طیف گسترده‌ای از گزینه‌های هشدار شامل رایانامه، سامانه پیام کوتاه، صفحه بندی، تله‌های قرارداد مدیریت شبکه، و حتی مسدود کردن خودکار منابع حمله می‌باشند.

با اینکه بسیاری از این ویژگی‌های هشدار ممکن است خوشایند باشند، سازمان باید در مورد استفاده از آن ها محافظه‌کار باشد تا زمانی که به نصب و راه‌اندازی یک IDPS پایدار و به خوبی درک شده و پی بردن به رفتار IDPS در محیط سازمان دست یابد.

همان‌طور که قبلاً اشاره شد، استفاده از فناوری SIEM دارای ارزش بالایی در اولویت‌بندی و کاهش هشدارهای IDPS است. به‌طور مثال، مقایسه ارزیابی آسیب‌پذیری داده و سطوح وصله‌های سامانه با پیکربندی هشدار IDPS. در این زمینه استفاده از ابزارهای اکتشاف شبکه و تحلیل ترافیک ممکن است ارزش بیشتری را اضافه کرده و اجازه تنظیم بیشتر قوانین هشدار را صادر می‌کند.

در برخی شرایط، سازمان باید فعال‌سازی مجموعه کامل ویژگی‌های هشدار را به تأخیر بیندازد تا زمانی که دوره آزمایشی مناسب، بهترین تعادل نیازمندی‌های عملیاتی و امکان هشدارها را آشکار سازد و درنهایت برای

سفارشی کردن قوانین هشدار و قابلیت‌های پاسخ اجازه صادر شود. سازمان پس‌ازآن می‌توانید تصمیم بگیرد که کدام ویژگی‌ها غیرضروری هستند، کدام ویژگی‌ها از بقیه مفیدتر هستند، و کدام ویژگی‌ها می‌توانند بیشترین بهره را به سازمان خود برسانند. در مواردی که ویژگی‌های هشدار و پاسخ شامل پاسخ خودکار به حملات می‌باشند، به‌ویژه مواردی که اجازه می‌دهند IDPS دیوار آتش را برای مسدودکردن ترافیک منابع متفاوت حملات هدایت کند، سازمان باید بسیار مراقب باشد که مهاجم از این ویژگی IDPS برای منع دسترسی به کاربران مشروع استفاده می‌کند، یعنی حمله‌ی انکار خدمت خود-وارد[1]. در ابتدا، این نوع از ویژگی‌های IDPS باید در یک حالت نیمه خودکار قرار داده شود که یک انسان تصمیم بگیرد که پاسخ IDPS باید فعال شود.

۳-۷ آسیب‌پذیری‌های IDPS

پیاده‌سازی ناامن یک حسگر IDPS مانند هر افزاره دیگر در شبکه به‌طور بالقوه مستعد برای حمله است. درصورتی‌که یک مهاجم از وجود آسیب‌پذیری آگاه شود، آن‌ها بیشتر به تلاش و بهره‌جویی از هرگونه آسیب‌پذیری‌های شناخته شده در IDPS متمایل می‌شوند. مهاجمان به احتمال زیاد درجهت غیر فعال کردن IDPS و یا وادار کردن آن به ارائه اطلاعات نادرست تلاش می‌کنند. علاوه بر این، بسیاری از IDPSها نقاط ضعف امنیتی مانند ارسال پرونده‌های ثبت رویداد رمزگذاری نشده، وارسی دسترسی محدود و عدم بررسی یکپارچگی پرونده‌های ثبت رویداد می‌باشند. ضروری است که حسگرها و پیشانه‌ی IDPS در یک اسلوب امن پیاده سازی شده و به نقاط ضعف بالقوه IDPS باید رسیدگی شود.

۴-۷ اداره کردن هشدارهای IDPS

۱-۴-۷ مرور کلی

به‌طور معمول، IDPS مقدار زیادی خروجی تولید می‌کند. به‌منظور جداسازی هشدارهای بی‌اهمیت از آن‌هایی که ماهیت جدی‌تری دارند، توصیه می‌شود سازمان خروجی IDPS را به‌طور کامل تحلیل نماید. هشدارها به‌طور معمول شامل خلاصه‌ای کوتاه از حمله‌ی آشکارسازی شده می‌باشند و کمینه باید شامل موارد زیر باشند:

- زمان یا تاریخ حمله آشکارشده؛
- آدرس IP حسگری که این حمله را آشکارکرده است؛
- نام حمله مخصوص فروشنده ؛
- نام استاندارد حمله (در صورت وجود).
- آدرس IP مبدأ و مقصد ؛

1-Self-inflicted

- شماره درگاهی منبع و مقصد ؛

- قرارداد شبکه مورد استفاده در حمله.

چند IDPS جزئیات عمومی بیشتری از روش‌های مورد استفاده‌ی حمله فراهم می‌کنند. این اطلاعات اجازه می‌دهد تا کاروَرها شدت حمله را اندازه گیری کنند و باید حاوی موارد زیر باشد:

- توصیف متنی از حمله؛

- سطح شدت حمله.

- نوع زیان تجربه شده به عنوان نتیجه‌ی حمله‌ای؛

- نوع آسیب‌پذیری که حمله مورد بهره‌جویی قرار داده است.

- فهرستی از انواع نرم‌افزارها و شماره نسخه‌ای که در معرض حمله است.

- یک فهرست از وصله‌های مربوطه؛

- مرجع‌ها به مشاوران عمومی که در آن‌ها جزئیات حمله‌یا آسیب‌پذیری را می‌توان یافت.

۷-۴-۲ گروه پاسخگویی به رخدادهای امنیت اطلاعات[1] (ISIRT)

زمانی که یک هشدار دریافت می‌شود، سازمان باید یک گروه پاسخگویی به رخدادهای امنیت اطلاعات (ISIRT) در محل داشته باشد. طرح ISIRT باید روش‌های اجرایی پیش روی این سازمان را برای ساماندهی رخدادهای امنیتی، مانند ویروس‌ها، سوءاستفاده خودی از سامانه‌ها و انواع دیگر حملات تعیین کند. این طرح کلی اقداماتی را که در این رویداد از یک حادثه امنیتی در نظر گرفته شده و ایجاد برنامه‌ها و محتوا برای آموزش کارکنان در مورد مسئولیت‌هایشان در فرآیند ساماندهی رخداد مشخص می‌کند. اطلاعات بیشتر در گزارش رخداد امنیتی و ساماندهی در استاندارد ISO / IEC 27035 مورد بحث قرار گرفته است.

۷-۴-۳ برون‌سپاری

علاوه بر محصولات IDPS، برخی از تأمین‌کنندگان خدمات امنیتی خدمات مدیریت IDPS را پیشنهاد می‌کنند که شامل مدیریت مرکز مشاوره و عملکردها است. بسیاری از سازمان‌ها ترجیح می‌دهند نقش‌های اصلی پشتیبانی را برون‌سپاری کنند. ازجمله‌ی این نقش‌ها برون‌سپاری خدمت‌های امنیتی به تأمین‌کنندگان خدمات مدیریت است، به‌طوری‌که سازمان‌ها مجبور به آموزش نیستند و کارکنان با مهارت‌های تخصصی را حفظ می‌کنند. همانطورکه با انتخاب محصولات IDPS، پیشنهادهای خدمت مدیریت امنیت باید به‌دقت برای تعیین اینکه آیا آن‌ها از نظر مالی قابل دوام می‌باشند و سطح مناسبی از پشتیبانی را همراه با حفظ محرمانه بودن فراهم می‌سازند، در نظر گرفته شود.

در هنگام برخورد با یک فروشنده IDPS که یک راه‌حل خدمت مدیریت امنیتی پیشنهاد می‌دهد ، کمینه،

1- Information Security Incident Response Team

سازمان باید سؤالات زیر را از فروشنده بپرسد:

- چه توافقات محرمانه‌ای در محل وجود دارند؟

- چه شرایطی از افرادی که IDPSرا پایش می‌کنند مورد نیاز است؟

- شرایط کارکنان نظارت و سرپرستی چیست؟

- ترتیب رابط و ارتباطات بین تأمین کننده‌ی خدمات و کارکنان امنیتی داخلی سازمان چگونه است؟

- آیا فروشنده خدمات پاسخی اضطراری برای تکمیل قابلیت‌های این سازمان پیشنهاد می‌کند؟

- آیا فروشنده خدمات تحقیقات قانونی را پیشنهاد می‌دهد؟

- آیا فروشنده SLA را پیشنهاد می‌دهد؟

- چه گزینه‌های گزارش‌دهی در دسترس هستند، و آیا می‌توان آن‌ها را با نیازهای سازمان سفارشی‌سازی کرد؟

- آیا خط‌مشی‌های آشکارسازی می‌تواند برای محیط یک سازمان سفارشی شود ، و یا شما را مجبور به استفاده از پیش فرض‌های از پیش تنظیم شده‌ی خود می‌سازد؟

- چه سنجه‌های فنی در محل برای تأکید بر این قراردادها وجود دارد؟

- چه روشهای اجرایی برای بررسی امنیتی کارکنان تأمین کننده خدمات تعهد شده است؟

SLA به خوبی مطالعه شده برون‌سپاری شده ممکن است مورد نیاز باشد که الزامات تفضیلی را برای موارد زیر شامل می‌شود:

- محتوای گزارش‌های دوره‌ای (روزانه، هفتگی، و غیره)؛

- سنجه‌هایی برای زمان پاسخ.

- سازوکار برای اطلاعَرسانی به سازمان زمانی که یک حمله رخ می‌دهد (رایانامه، فراخوان[1]، سامانه‌ی پیام کوتاه ، سامانه‌های چندرسانه‌ای، تلفن، و غیره)؛

- روش‌های اجرایی ردیابی و مدیریت رخداد؛

- محرمانگی و توافق‌نامه‌های افشا ناپذیر.

مزایا:

- تأمین کننده‌ی خدمات امنیتی مدیریت شده به‌طور معمول می‌تواند سطح بالاتری از امنیت را نسبت به هزینه معادل تولید برای فراهم شدن آن توسط خود سازمان عرضه کند.

1- Pager

- به‌طورکلی، قابلیت می‌تواند ۲۴ به ۷ بار سریع‌تر، به‌طور مؤثرتر و با اختصاص هزینه‌ی پایین‌تر اجرا شود.

- ازآنجاکه بسیاری از تأمین کنندگان خدمت امنیتی مدیریت شده می‌توانند به اطلاعات مشتریان بسیار متفاوتی دسترسی داشته باشند، آن‌ها ممکن است در موقعیت بهتری برای حل‌وفصل فعالیت‌های مشکوک و شناسایی یک حمله قرار داشته باشند؛

- سازمان می‌تواند زمان مورد نیاز برای کنارهم قرار دادن روش‌های اجرایی مؤثر IDPS و زمان مورد نیاز برای پیگیری تمام جزئیات پیاده سازی را کاهش دهد.

- درحالی‌که نیاز برای آگاهی از قابلیت‌های IDPS در یک سازمان وجود دارد، هیچ الزامی برای فراهم شدن آموزش‌های تخصصی مداوم کارمندان در آخرین ابزارها و قابلیت‌های IDPS وجود ندارد.

معایب:

- برای انطباق با الزامات امنیتی ، محدودیت‌ها و خط‌مشی‌های سازمان، برون سپار باید شنود و پایش شود؛

- افشای پنهانی اطلاعات نفوذپذیر سازمانی به یک سازمان طرف سوم؛

- اگر به‌دقت اجرا نشود، می‌تواند از پشتیبانی در خانه پرهزینه‌تر باشد.

- می‌تواند سازمان را از واپایش داده‌های نفوذپذیر محروم کند.

۷-۵ گزینه‌های پاسخ

۷-۵-۱ اصول

بسیاری از IDPSها از طیف گسترده‌ای از گزینه‌های پاسخ پشتیبانی می‌کنند که می‌تواند به‌صورت فعال یا غیر فعال طبقه‌بندی شود.

۷-۵-۲ واکنش فعال

پاسخ فعال شامل یک کنش خودکار است که توسط IDPS در هنگام آشکارسازی حمله گرفته می‌شود. سامانه‌های آشکارسازی نفوذ طراحی شده برای ارائه پاسخ به صورت فعال به عنوان سامانه‌های پیشگیری از نفوذ(IPS) نیز شناخته می‌شوند. پاسخ‌های فعال به شرح زیر بیشتر طبقه‌بندی می‌شوند:

- جمع‌آوری اطلاعات اضافه درباره حمله مشکوک؛

- تغییر محیط «سامانه» برای متوقف کردن حمله.

- پس از یک هشدار، برای اخذ یک کنش پیشگیرانه بدون کنش ضروری انسان، IPS به‌طور فعال ارتباط را رد کرده و یا به نشست ارتباط پایان می‌دهد.

سامانه‌های IPS و IDPS بسیاری از کارکردهای مشابه مانند بازرسی بسته، اعتبار سنجی قرارداد، تطبیق نشانه حمله و تحلیل وضعیت‌دار را به اشتراک گذاشته‌اند. اگرچه، هر افزاره ممکن است برای اهداف متفاوتی

مستقر شود.

IPS نشان دهنده ترکیب قابلیت‌های حفاظت با قابلیت‌های آشکارسازی نفوذ است و این امکان را فراهم می‌سازد که ابتدا حمله آشکارسازی شده و سپس محافظت در برابر آن به یکی از دو شیوه‌ی ایستا و یا پویا انجام شود.

سامانه IDPS یک افزاره غیر فعال است که فعالیت‌ها را پایش کرده و نشانه‌های حمله شناخته شده و یا شرایط ناهنجار را جستجو می‌کند. سامانه IDPS افزاره‌ای برون خط است که برای بیان اینکه چه فعالیت مخربی روی شبکه اتفاق افتاده، طراحی شده است. با توجه به ماهیت منفعل IDPS، فرصت کمی برای IDPS وجود دارد که موجب بدعمل کردن شبکه شود.

در طرف دیگر، IPS دسترسی به منابع را بر اساس اعتبارات و یا برخی مجموعه قوانین یا خط‌مشی از پیش تعریف شده، اجازه داده و یا رد می‌کند.IPS افزاره‌ای برخط است که برای پایش ترافیک و تصمیم‌گیری از قلم انداختن بسته‌های داده، قطع ارتباطاتی که حاوی داده‌های غیرمجاز می‌باشند و یا پذیرش ترافیک طراحی شده است. به عبارت دیگر، IPS حفاظت از دارایی‌های اطلاعات را با از بین بردن ترافیک مخرب شبکه فراهم می‌کند، درحالی‌که به اجازه دادن به رخداد فعالیت‌های قانونی ادامه می‌دهد. دو نوع IPS اصلی عبارتند از:

- سامانه IPS مبتنی بر میزبان (HIPS) - نرم‌افزار را به‌طور مستقیم بر روی یک ایستگاه کاری یا کارساز اجرا می‌کند و می‌تواند تهدیدات با هدف میزبان محلی را شناسایی و پیشگیری نماید.

- سامانه IPS مبتنی بر شبکه (NIPS) - ویژگی‌های استاندارد IDPS و IPS و دیوار آتش را ترکیب می‌کند. در موردی که ترافیک حالت یک تهدید را دارد، این ترافیک برای تعیین شدن به موتور آشکارسازی ارسال می‌شود. به‌محض آشکارسازی ترافیک‌های مخرب، یک هشدار رخ می‌دهد و ترافیک دور ریخته می‌شود.

مشابه HIDPS، HIPS متکی بر نرم‌افزاری است که به‌طور مستقیم بر روی سامانه محافظت شده نصب شده و به‌دقت ملزم به محافظت از سامانه‌ی عامل و خدمات آن است. این مورد اجازه می‌دهد تا فراخوان‌های سامانه‌ای به سامانه‌ی عامل و یا رابط‌های برنامه کاربردی به‌منظور پیشگیری و ثبت حملات پایش و تفسیر شوند. سامانه NIPS ویژگی‌های IPS،IDPS و دیوار آتش را ترکیب می‌کند. بسته‌ها در هر دو رابط داخلی یا خارجی ظاهر می‌شوند و برای تعیین شدن اینکه آیا بسته حالت تهدید دارد، به موتور آشکارسازی ارسال می‌شود. درصورتی‌که یک بسته مخرب شناسایی، یک هشدار تولید شده و بسته دور انداخته می‌شود و جریان به عنوان مخرب علامت‌گذاری می‌شود. درنتیجه بسته‌های باقی مانده از این نشست ویژه‌ی TCP پس از رسیدن به افزاره‌ی IPS بلافاصله دور ریخته می‌شوند. یک IPS بیشتر پالایش شده می‌تواند بسته‌های تکی را به‌جای کل نشست متوقف کند، آن‌ها می‌توانند به‌صورت پویا قوانین دیوار آتش را بازنشانی کنند، ترافیک را به یک هانی‌پات مسیریابی کرده یا ترکیبی از این دو فعالیت را انجام دهند.

نرم‌افزار HIPS تمامی درخواست‌های ارسالی به سامانه‌ای که از آن محافظت می‌کند را قطع می‌کند[1]. درنتیجه توصیه می‌شود این نرم‌افزار بسیار قابل اعتماد باشد، توصیه نمی‌شود عملکرد را تحت تأثیر قرار دهد و ترافیک قانونی را مسدود کند.

مزایا:

- قابلیت آشکارسازی و مسدود کردن حملات؛

- فراهم کردن محافظت فعال.

- افزایش عملکردهای عملیاتی به دلیل کاهش نیاز به واکنش در مقابل رویدادهای ثبت شده‌ی IDPS.

معایب:

- برای کار در حالت بر خط طراحی شده است، درنتیجه یک نقطه انسداد بالقوه و یک نقطه خرابی واحد را نشان می‌دهد.

- مثبت‌های کاذب می‌توانند به نسبت IDPS به مراتب جدی‌تر و دور از دسترس تر باشند ، یعنی نتایج می‌تواند یک حمله‌ی انکار خدمت خود-وارد باشد.

- تحت بارهای ترافیک پیش بینی شده، تحلیل باید روی هر بسته و بدون هیچ‌گونه اثر قابل‌توجهی بر جریان ترافیک انجام شود؛

- پاسخ‌های فعال ممکن است فقط به یک زیرمجموعه از مجموعه امضا اعمال شود.

- با توجه به یکپارچگی زیاد نرم‌افزار HIPS به هسته سامانه عامل، ارتقاء سامانه عامل می‌تواند مشکلاتی را موجب شود.

۳-۵-۷ واکنش منفعل

پاسخ‌های منفعل اطلاعاتی را برای کاروَرها و یا یک محل از پیش تعیین شده فراهم می‌سازند. آن‌ها به کاروَرهای IDPS تکیه می‌کنند تا اقدام پسینی[2] مبتنی بر اطلاعات فراهم شده اتخاذ کنند. پاسخ‌های منفعل به یکی از شکل‌های زیر است:

- هشدارها و آگاه‌سازی‌ها، هشدارهای معمول روی صفحه، پنجره‌های بازشو و پیام‌هایی به پیجرها یا گوشی‌های تلفن همراه.

- تله‌های SNMP برای پاسخ به یک پیشانه مدیریت مرکزی پیکربندی شده است.

1- Intercept
2- Subsequent

۷-۶ ملاحظات قانونی[1]

۷-۶-۱ مرور کلی

همان‌طور که تمام سامانه‌هایی که اطلاعاتی جمع‌آوری می‌کنند که ممکن است شامل محتویات نفوذپذیر، داده کارمند و یا شواهدی برای تحقیقات مجرمانه‌ی بعدی، داده‌ها باید به‌صورت مسئولانه و در انطباق کامل با قوانین قابل‌اجرا ذخیره و پردازش شوند. سازمان باید اطمینان حاصل کند که کارکنان آن از مسئولیت‌های خود در این زمینه آگاه می‌باشند. این بند به تشریح ملاحظات قانونی مرتبط با استفاده‌ی IDPS می‌پردازد.

۷-۶-۲ حریم شخصی

در این دوره کارکرد هنجار، سامانه‌ی IDPS می‌تواند اطلاعاتی مربوط به افراد را جمع‌آوری کرده و برای پایش فعالیت‌های کارکنان مورد استفاده قرار دهد که ممکن است تابع حریم خصوصی و قانون قابل‌اجرا در بسیاری از حوزه‌های قضایی باشد. توصیه می‌شود سازمان خط‌مشی‌هایی را برای اطمینان از برآوردن حریم خصوصی مرتبط و قانون قابل‌اجرا برای هرگونه استفاده‌ی IDPS توسعه داده و پیاده سازی نماید.

۷-۶-۳ دیگر ملاحظات قانونی و خط‌مشی

اجرا و عملکرد IDPS ممکن است تابع دیگر الزامات قانونی و مقرراتی و همچنین الزامات خط‌مشی سازمانی باشد که IDPS در آن‌جا مستقر شده است. الزامات حقوقی، قانونی و خط‌مشی سازمانی باید بررسی شود و زمان اجرا و عملکرد IDPS مورد خطاب قرارگیرد. جنبه‌های قانونی و حقوقی بیشتر در استاندارد ISO / IEC 27035 مورد بحث قرار گرفته است.

۷-۶-۴ جرم‌شناسی[2]

ثبت رویدادهای IDPS ممکن است برای اهداف قضایی مورد استفاده قرار گیرد. الزامات قضایی حوزه‌های قضایی مربوطه باید درک شده و واپایش‌های مناسب بر روی ذخیره سازی و ساماندهی ثبت رویدادهای IDPS باید به مورد قرار داده شود تا بررسی قضایی قابل قبول اطلاعات را فعال نماید. ممکن است الزامات اضافی در مورد مستندسازی سامانه‌های IDPS و فرآیندهایی مقتضی الزامات قضایی و مبتنی بر مدرک وجود داشته باشد.

1- Legal Considerations
2- Forensics

پیوست الف

(آگاهی‌دهنده)

سامانه‌ی آشکارسازی و پیشگیری نفوذ (IDP): چارچوب و مسائلی که در نظر گرفته می‌شود

الف-۱ مقدمه‌ای بر آشکارسازی نفوذ

یک سازمان به محافظت از سامانه‌های اطلاعاتی خود نیازمند است. زیرا با وجود کسب‌وکار سازمانی دلایلی برای استفاده از سامانه‌های اطلاعاتی و اتصال آن‌ها به اینترنت و شبکه‌های دیگر وجود دارد. این واقعیت وجود دارد که آسیب‌پذیری‌هایی در سامانه‌های اطلاعاتی این سازمان‌ها موجود است که می‌تواند به‌طور تصادفی و یا عمدی مورد بهره‌جویی، نفوذ و حمله قرار گیرد.

روش‌های پیشرفته و سهولت بیشتر در دسترسی به اطلاعات، و همچنین، آسیب‌پذیری‌های جدید، هر هفته در حال کشف شدن است. به‌طور هم‌زمان، حملات در حال توسعه برای بهره‌جویی از این آسیب‌پذیری‌ها می‌باشند.

نفوذگران به‌طور مستمر روش‌های خود را بهبود می‌دهند و اطلاعات برای کمک به آن‌ها راحت و راحت‌تر در دسترس است. به یک درجه‌ی اهمیت، سواد رایانه امری معمولی است، و با توجه به دسترس‌پذیری رخنمون-های حمله‌ها و ابزارهای پیشرفته، مهارت‌های مورد نیاز برای راه‌اندازی حملات در حال کاهش است. به‌تبع آن، حملات را بدون دانش فردی در مورد اینکه دقیقاً چه رخ می‌دهد و یا حمله به چه آسیبی می‌تواند منجر شود می‌توان آغاز کرد.

اولین لایه‌ی دفاعی برای حفاظت از سامانه‌های اطلاعاتی از واپایش‌های فیزیکی، مدیریتی و فنی استفاده می‌کند که شامل شناسایی و اصالت‌سنجی، واپایش دسترسی منطقی و فیزیکی، ممیزی و سازوکارهای رمزگذاری باشد. فهرستی از واپایش‌های توصیه شده در استاندارد ISO / IEC 27002 برای سازمان‌ها یافت می‌شود. بااین‌حال، محافظت کامل از هر سامانه‌ی اطلاعاتی، خدمت و شبکه در تمام زمان‌ها، ازلحاظ اقتصادی غیرممکن است. به‌طور مثال، پیاده سازی سازوکارهای واپایش دسترسی، زمانی که شبکه مورد استفاده‌ی جهانی، بدون هیچ حدومرز جغرافیایی قرار گرفته و تفاوت بین درون و برون واضح نیست، مشکل است. علاوه بر این، از آن‌جایی که سازمان‌ها به‌طور فزاینده ای بر دسترسی از دور توسط کارکنان و شرکای تجاری توسعه یافته تکیه می‌کنند، دفاع از محیط[1] سنتی، کمتر دست‌یافتنی شده است. این محیط IT تنظیمات پیچیده‌ی شبکه را ایجاد کرده است که بسیار پویاست و شامل نقاط دسترسی چندگانه به سامانه‌های IT و خدمات سازمان است. بدین ترتیب، لایه‌ی دوم دفاعی به‌منظور آشکارسازی و پاسخ بی‌درنگ و مؤثر در زمان رخداد نفوذها مورد نیاز است. این لایه‌ی دفاعی عمدتاً توسط سامانه آشکارسازی نفوذ انجام می‌شود (IDPS). علاوه بر این، پس‌خورد از IDPS مستقر می‌تواند دانشی در مورد آسیب‌پذیری‌های

1- Perimeter

سامانه‌های اطلاعاتی سازمان را پالایش کند که برای بهبود کیفیت کلی امنیت اطلاعات به سازمان کمک می‌کند.

یک سازمان می‌تواند با گرفتن محصولات نرم‌افزاری و یا سخت‌افزاری IDPS از بازارها و یا توسط برون‌سپاری توانمندی‌های IDPS به تأمین کننده‌ی خدمات IDPS، IDPS را مستقر کند. در هر دو مورد، سازمان باید بداند که استقرار مؤثر IDPS نیازمند دانش آن سازمان در مورد IDPS است و IDPS یک افزاره‌ی اتصال و اجرا نیست.

مانند هر واپایشی، سازمان به توجیه استقرار IDPS با استفاده از ارزیابی خطر امنیت اطلاعات و یکپارچه‌سازی IDPS مستقر شده با فرآیند مدیریت امنیت اطلاعات سازمان نیازمند است. علاوه بر این، مراقبت‌های مناسب مورد نیاز است با درنظرگرفتن اینکه، درصورتی‌که یک مزاحم یا مهاجم اطلاعات موجود در IDPS مستقر را استراق سمع کند، مزاحم و یا مهاجم می‌تواند آن‌ها را باطل ساخته و سازمان را با مشکلات زیادی مواجه کند. این جنبه‌ها شامل چگونگی شناسایی و توجیه نیاز به پادمان[1]هایی مانند IDPS است. سامانه هوشمند و مرتبط و یا خط‌مشی امنیتی خدمت باید تعیین شود که ایمن‌داشت مناسب برای مدیریت مخاطرات نفوذ انتخاب شود. این ایمن‌داشت‌ها شامل آن‌هایی است که:

- احتمال رخداد نفوذ را کاهش می‌دهند؛ و
- آشکارسازی و پاسخ به‌طور مؤثر به نفوذهایی که ممکن است رخ دهد.

مانند هر واپایشی، سازمان به توجیه استقرار IDPS با استفاده از ارزیابی خطر امنیت اطلاعات و یکپارچه سازی IDPS مستقر شده با فرآیند مدیریت امنیت اطلاعات سازمان نیازمند است. علاوه بر این، مراقبت‌های مناسب موردنیاز است با درنظرگرفتن اینکه، درصورتی‌که یک مزاحم یا مهاجم اطلاعات موجود در IDPS مستقر را استراق سمع کند، مزاحم و یا مهاجم می‌تواند آن را باطل کرده و سازمان را با مشکلات زیادی مواجه کند.

هنگامی که یک سازمان استقرار IDPS را در نظر دارد، باید موارد زیر درک شود:

- انواع نفوذها و حملات به سامانه‌های اطلاعاتی و / یا شبکه‌ها،

- الگوی عمومی IDPS که در این سند ارائه شده است.

الف-۲ انواع نفوذها و حملات

الف-۲-۱ مقدمه

مزاحمان و مهاجمان به سامانه‌های اطلاعاتی می‌توانند از خطاهای پیکربندی، خطاهای اجرا و یا خطاهای مفهومی سامانه‌های اطلاعاتی و یا شبکه‌ها و همچنین از رفتار کاربران غیرطبیعی بهره‌جویی کنند.

آسیب‌پذیری‌ها به مزاحم و مهاجم اجازه‌ی دسترسی به سامانه‌های اطلاعاتی محافظت شده و اطلاعاتی را که

1- Safeguard

در سامانه اطلاعات پردازش و ذخیره‌سازی شده است، می‌دهد و همچنین باعث مخاطره‌ی محرمانگی، یکپارچگی و یا دسترس‌پذیری اطلاعات و سامانه‌های اطلاعاتی می‌شود. این نفوذها و حملات، دانش ارزشمندی درباره‌ی سامانه‌های اطلاعاتی و یا شبکه‌هایی که می‌توانند توسط روش‌های پیچیده‌تر نفوذ یا حمله مورد بهره‌جویی قرار گیرند، فراهم می‌سازند. توصیه می‌شود سازمان تشخیص دهد که نفوذها و حملات نه‌تنها توسط یک نفر خارج از سازمان، بلکه توسط بدخواه داخل سازمان تلاش می‌شوند. به‌طور مثال، کاربران مجاز سامانه اطلاعاتی یک سازمان ممکن است برای به دست آوردن امتیازات اضافی که برای آن‌ها مجاز نیست، تلاش کنند. نفوذها و حملات عمدی ممکن است برای موارد زیر استفاده شوند:

- جمع‌آوری اطلاعات، که نفوذگر برای بازیابی اطلاعات دقیق در مورد سامانه‌های اطلاعاتی هدف تلاش کند.

- تلاش برای به دست آوردن امتیازات غیرمجاز استفاده از سامانه‌ها، منابع و یا داده‌ها،

- به خطر انداختن یک سامانه، که ممکن است استفاده از منابع سامانه برای حملات بیشتر را اجازه دهد،

- افشای اطلاعات، که یک مزاحم تلاش می‌کند از اطلاعات محافظت شده (به‌طور مثال، رمز عبور، اطلاعات کارت اعتباری) به عنوان ابزار غیرمجاز استفاده کند، و / یا

- حملات انکار خدمت (DOS) ، که نفوذگر برای کم کردن سرعت یا ایجاد شرایط خارج از خدمت برای خدمات هدف سامانه اطلاعات تلاش می‌کند.

با توجه به نقاط آسیب‌پذیر محتمل برای نفوذ و حمله، نفوذها و حملات نیز می‌توانند به موارد زیر شکسته شده و در نظر گرفته شوند:

- مبتنی بر میزبان،

- مبتنی بر شبکه، یا

- ترکیب روش‌ها.

الف-۲-۲ نفوذهای مبتنی بر میزبان

نفوذهای مبتنی بر میزبان به‌طورکلی فعالیت‌های نفوذی‌ای در نظر گرفته می‌شوند که کدهای مخرب و مخاطره‌آمیز (به‌طور مثال، حملات با استفاده از اسب‌های تروآ، کرم‌ها، و یا ویروس‌ها) را معرفی می‌کنند.

- لایه کاربرد (SMTP، DNS) (به‌طور مثال، جعل رایانامه، هرزه نگاره، حملات سرریز بافر، حملات شرایط رقابتی[1] ، حملات مرد در میان[2]).

- یک سامانه اصالت‌سنجی (به‌طور مثال، حملات با استفاده از استراق سمع و یا حدس زدن رمز عبور)،

- خدمات مبتنی بر وب (به‌طور مثال، حملات با هدف CGI، اکتیو ایکس[3]، یا جاوا اسکریپت[1])،

1- Race-Condition Attacks
2- Man-in- the- middle Attacks
3- ActiveX

- در دسترس بودن سامانه (به‌طور مثال، حملات DOS)،

- سامانه عامل، و یا

- سامانه‌های مدیریت شبکه و کاربرد (به‌طور مثال، حملات SNMP).

الف-۲-۳ نفوذهای مبتنی بر شبکه

نفوذهای مبتنی بر شبکه به‌طورکلی فعالیت‌های مزاحم در موارد زیر در نظر گرفته می‌شوند:

- قراردادهای ارتباطی فیزیکی و پیوند-داده و سامانه‌هایی که آن‌ها را اجرا می‌کنند (به‌طور مثال جعل آرپ[۲]، شبیه سازی آدرس واد[۳])، و یا

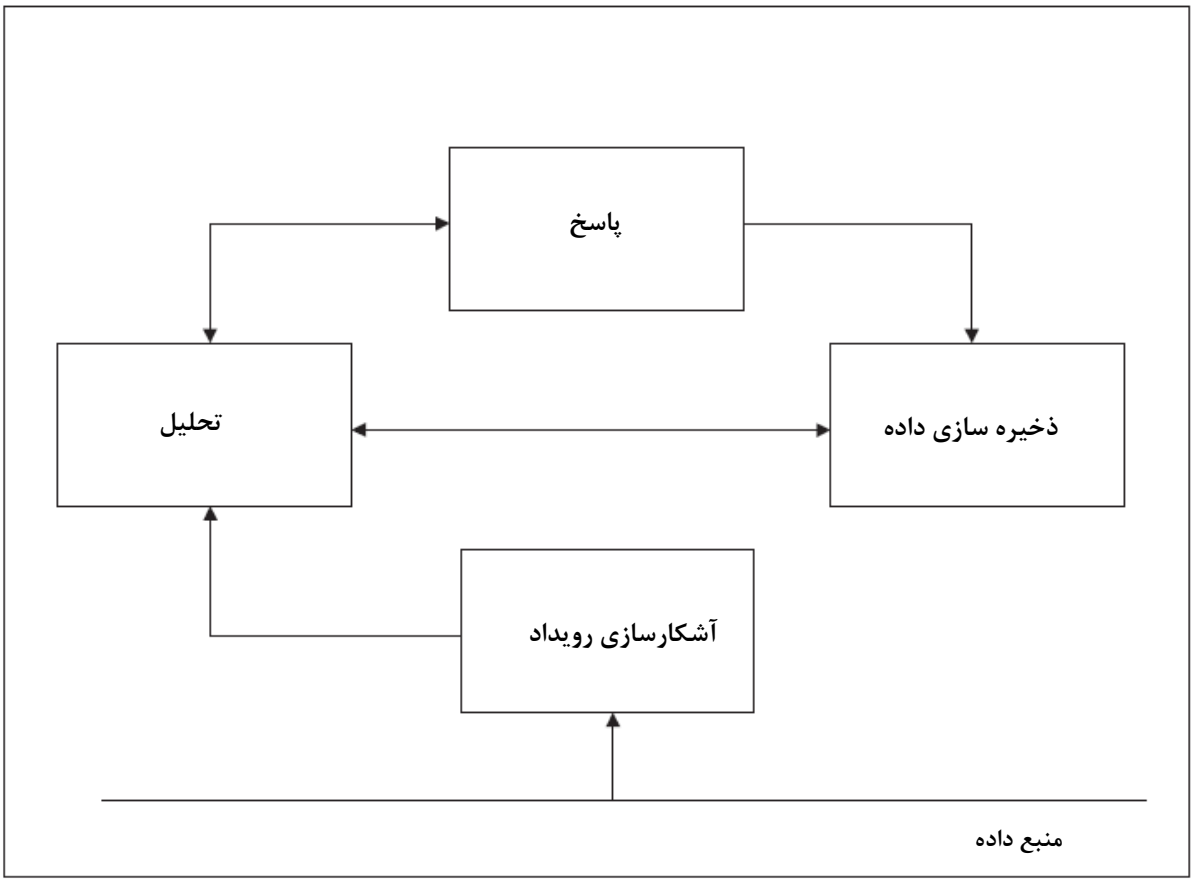
- قراردادهای شبکه و حمل‌ونقل ارتباطات و سامانه‌های اجراکننده (IP، ICMP، TCP،UDP) (به‌طور مثال جعل IP، حملات قطعه‌قطعه کردن IP، حملات طغیان SYN ، حملات سرآیند اطلاعاتی ناقص TCP).

الف-۳ الگوی عمومی فرآیند آشکارسازی نفوذ

الف-۳-۱ مقدمه

IDPS شامل محصولات نرم‌افزاری و یا سخت‌افزاری است که به‌طور خودکار رویدادهای مشکوک در سامانه‌های اطلاعاتی و یا شبکه‌ها را برای نشانه‌هایی از نفوذها، پایش، جمع‌آوری و تحلیل می‌کند. الگو عمومی آشکارسازی نفوذ را می‌توان با مجموعه‌ای از توابع تعریف نمود. این توابع عبارت‌اند از: یافتن منابع داده‌های خام، آشکارسازی رویداد، تحلیل، ذخیره سازی داده و پاسخ. این توابع را می‌توان به‌صورت قطعات مجزا و یا بسته‌های نرم‌افزاری به عنوان بخشی از یک سامانه‌ی بزرگ‌تر اجرا نمود. شکل الف-۱ شیوه‌ای که این توابع به یکدیگر مرتبط می‌شوند را نمایش می‌دهد.

1- JavaScript
2- ARPspoofing
3- Mac Address



شکل الف-۱- الگو عمومی آشکارسازی نفوذ

الف-۳-۲ منابع داده

موفقیت فرآیند آشکارسازی نفوذ به منابع داده‌ای وابسته است که اطلاعات آشکارسازی تلاش‌های نفوذ از آن‌ها گرفته شده است. این منابع به‌صورت زیر تعریف می‌شوند:

- داده‌های ممیزی[1] از منابع مختلف سامانه: سوابق داده ممیزی حاوی پیام‌ها و وضعیت اطلاعات اعم از دارای سطح انتزاع بالا تا داده‌هایی در سطح بسیار تفصیلی نشان‌دهنده‌ی جریان زمانی از رویدادها می‌باشند. منابع مفید برای داده‌های ممیزی پرونده‌های ثبت رویداد سامانه‌های عامل است که شامل ثبت رویدادهای سامانه و فعالیت‌های تولید شده توسط سامانه عامل مانند دنباله‌ها یا ثبت رویدادهای ممیزی است. برنامه‌های کاربردی که اطلاعاتی درباره‌ی سامانه پرونده‌ها، خدمات شبکه، تلاش‌های دسترسی و غیره نیز منابع خوبی برای داده‌های خام هستند.

- تخصیص منابع سامانه توسط سامانه عامل: پارامترهای پایش سامانه مانند حجم کار CPU، استفاده ی حافظه، نبود منابع سامانه، نرخ ورودی و خروجی، تعداد اتصالات فعال شبکه و غیره برای کمک به آشکارسازی نفوذها جالب است.

1- Audit data

- ثبت رویدادهای مربوط به مدیریت شبکه: ثبت رویدادهای مدیریت شبکه، سلامت افزاره‌های شبکه، وضعیت و اطلاعات انتقال حالت افزاره را فراهم می‌سازد.

- ترافیک شبکه: ترافیک شبکه پارامترهایی مانند آدرس منبع و مقصد و همچنین درگاهی‌های منبع و مقصد که مربوط به امنیت می‌باشند را فراهم می‌کند. را فراهم می‌کند. گزینه‌های مختلف قراردادهای ارتباطی (به‌طور مثال، پرچم‌های وضعیت IP و TCP، که مسیریابی منبع و یا تلاش‌های اتصال و تصدیق وصول را نشان می‌دهد) نیز برای IDPS مفید هستند. جمع‌آوری این داده‌ی خام در سطح پایین با توجه به الگو OSI مفید است زیرا فرصت‌های کمتری برای دست‌کاری این داده‌ها قبل از جمع‌آوری وجود دارد. در مورد داده‌های خام که در سطح بالاتری از انتزاع به‌طور مثال، از یک کارساز وکالتی، جمع‌آوری می‌شوند، اطلاعات نمایش داده شده در سطح پایین‌تر ممکن است از دست بروند.

- دیگر منابع داده‌ها: دیگر منابع داده‌ها شامل دیوارهای آتش، سوده‌ها و مسیریاب‌ها، و البته حسگرهای ویژه و عامل‌های پایش IDPS.

محل منابع داده‌های خام را می‌توان به دو رده‌ی میزبان و شبکه تقسیم بندی کرد. ازآنجاکه تمایز مکان در دنیای آشکارسازی نفوذ حکم‌فرماست، IDPS نیز می‌تواند به دو نوع مبتنی بر میزبان و مبتنی بر شبکه رده‌بندی شود. سامانه IDPS مبتنی بر میزبان، دنباله‌ها و یا ثبت رویدادهای ممیزی و همچنین داده‌های دیگر از میزبان‌ها و برنامه‌های کاربردی را مورد بازرسی قرار می‌دهد. سامانه IDPS مبتنی بر شبکه می‌تواند ثبت رویدادهای مدیریت شبکه و همچنین داده‌های دیوارهای آتش، سوده‌ها، مسیریاب‌ها و عوامل حسگرهای ویژه‌ی IDPS را مورد بررسی قرار دهد.

الف-۳-۳ آشکارسازی رویداد

هدف از آشکارسازی رویداد، شناسایی و فراهم کردن داده‌های مربوط به رویداد امنیتی برای استفاده در کارکرد تحلیل است.

رویدادهای آشکارشده ممکن است رویدادهای ساده(متشکل از قطعات حملات و یا رویدادهایی در طول عملیات عادی) یا رویدادهای پیچیده (متشکل از ترکیبی از حوادث ساده است که به احتمال زیاد یک حمله ویژه را نشان می‌دهد) باشند. بااین‌حال، رویداد یا داده‌ی رویداد ممکن است به عنوان شواهدی از نفوذ به‌کار نروند.

کارکرد آشکارسازی رویداد توسط جزء پایش IDPS به دست آید. این کارکرد را می‌توان روی افزاره‌ی شبکه(به‌طور مثال، مسیریاب، پل و یا دیوارآتش) یا روی یک رایانه‌ی خاص(به‌طور مثال، کارساز برنامه کاربردی، کارساز دادگان) بسته به منابع داده‌های خام که داده‌ی رویداد از آن آشکار می‌شود، نصب کرد.

از آن‌جایی‌که فرآیند آشکارسازی رویداد می‌تواند مقدار زیادی داده‌ی رویداد تولید کند، فراوانی آشکارسازی رویداد می‌تواند روی اثربخشی کلی IDPS تأثیرگذار باشد. این وضعیت همچنین می‌تواند در فرآیند تحلیل که در ادامه مطرح می‌شود نیز استفاده شود.

الف-۳-۴ تحلیل

الف-۳-۴-۱ مقدمه

هدف از کارکرد تحلیل، تحلیل و پردازش داده‌ی رویداد است که توسط کارکرد آشکارسازی رویداد به‌منظور یافتن یک تلاش برای نفوذ، نفوذ در حال رویداد و یا نفوذی که به وقوع پیوسته است، فراهم شده است.

علاوه بر داده‌ی مربوط به آشکارسازی رویداد، کارکرد تحلیل می‌تواند اطلاعات و یا داده‌هایی را از منابع مختلف شامل موارد زیر استفاده کند:

- داده هایی که نتایج حاصل از تحلیل قبلی هستند و توسط کارکرد ذخیره‌سازی داده‌ها نگهداری شده‌اند،
- اطلاعات و یا داده‌های تولید شده از دانشی در مورد این‌که چگونه یک فرد یا سامانه قرار است رفتار کند (به‌طور مثال از وظایف شناخته شده‌ای که قرار است انجام شود یا از اقدامات مجاز که باید انجام شود)،
- اطلاعات و یا داده‌های تولید شده از دانشی در مورد این‌که چگونه یک فرد یا سامانه نباید رفتار کند(به‌طور مثال از حملات شناخته شده و یا از اقدامات مضر شناخته شده)
- دیگر اطلاعات و یا داده‌های مربوطه مانند وب‌گاه‌های مشکوک منبع حمله، افراد، و یا مکان مهاجمان.

دو رویکرد کلی برای تحلیل وجود دارد: رویکرد مبتنی بر ناهنجاری و رویکرد مبتنی بر سوءاستفاده. گاهی رویکرد مبتنی بر سوءاستفاده به عنوان مبتنی بر دانش نیز نامیده می‌شود. گاهی رویکرد مبتنی بر ناهنجاری نیز به عنوان مبتنی بر رفتار نامیده می‌شود.

الف-۳-۴-۲ رویکرد مبتنی بر سوءاستفاده

الف-۳-۴-۲-۱ مرور کلی

رویکرد مبتنی بر سوءاستفاده در جستجو برای شواهدی از حملات در داده‌ی رویداد آشکارشده برمبنای دانش انباشته شده از حملات شناخته شده و فعالیت‌های غیرمجاز تمرکز دارد.

رویکرد مبتنی بر سوءاستفاده تلاش‌هایی را برای الگوگذاری و کدبندی حملات شناخته شده در سامانه‌های اطلاعاتی، و همچنین رفتارهای قبلی و اقداماتی که مخرب و یا مزاحم تلقی می‌شده‌اند، به عنوان نشانه‌های حمله خاص انجام می‌دهد. این تلاش‌ها شامل پویش سامانمند سامانه‌های اطلاعاتی برای رخداد این نشانه-های حملات است. از آنجایی‌که الگوهای حملات شناخته شده و یا تغییرات جزئی از حملات شناخته شده، نشانه نامیده می‌شوند، آشکارسازی سوءاستفاده گاهی IDPS مبتنی بر نشانه نامیده می‌شود.

رایج‌ترین روش‌های آشکارسازی حمله مبتنی بر نشانه مورد استفاده در محصولات تجاری، هر الگوی رویداد

متناظر به یک حمله و یا فعالیت غیرمجاز را به عنوان یک نشانه‌ی جداگانه‌ی حمله مشخص می‌کنند. بااین‌حال، برخی سازوکارهای پیچیده‌تر اجازه‌ی استفاده از یک نشانه حمله‌ی واحد را برای آشکارسازی گروهی از حملات شناخته شده و فعالیت‌های غیرمجاز می‌دهند.

زمانی که رویکرد مبتنی بر سوءاستفاده، بر این فرض است که داده‌ی رویداد با نشانه حمله همسان نیست، نفوذها و یا حملات را نشان نمی‌دهد، مراقبت‌هایی نیاز است که در نظر گرفته شوند. برخی داده‌های بی‌بدیل هنوز هم می‌توانند حاوی شواهدی از نفوذ و یا حملات باشند که ممکن است درزمانی که نشانه‌های حملات الگو شده‌اند، ناشناخته بوده‌اند.

روش‌های غالب فعلی استفاده شده توسط کارکرد تحلیل بر اساس سوءاستفاده، عبارت‌اند از:

الف-۳-۴-۲-۲ تحلیل نشانه حمله

این روش که احتمالاً رایج‌ترین روش برای آشکارسازی نفوذها است، مبتنی بر این توقع است که هر اقدام مرتبط با امنیت که در یک سامانه اطلاعاتی آغازشده می‌تواند به یک ورودی متناظر ثبت رویداد ممیزی منجر شود.

فرانامه‌های نفوذ ممکن است به توالی‌هایی از ثبت رویداد ممیزی و یا الگوهای داده ترجمه شده باشد، که می‌تواند در داده‌های تولید شده توسط سامانه‌ی عامل یک رایانه، برنامه‌های کاربردی، دیوارآتش، سوده‌ها و مسیریاب، و یا حسگرها یا پایشگرهای خاص IDPS یافت شود. توالی‌ها یا نشانه‌های حمله‌ی دیگر ممکن است در جریان ترافیک شبکه یافت شوند. تحلیل قرارداد شکلی از تحلیل نشانه حمله خاص شبکه است و از ساختار به خوبی تعریف شده‌ی قراردادهای ارتباطی استفاده می‌کند. تحلیل قرارداد می‌تواند عناصری مانند بسته‌ها، قاب‌ها و اتصالات را پردازش کند.

توصیف معنایی و یا نشانه حمله‌ی حملات شناخته شده توسط فرآیند تحلیل، جمع‌آوری یا فرمول‌بندی شده و در دادگان ذخیره می‌شود. زمانی که توالی خاص و یا نشانه حمله منطبق بر یک نشانه حمله‌ی از پیش تعریف شده‌ی نفوذ در ثبت رویدادهای ممیزی و غیره یافت شود، تلاشی برای یک نفوذ نشان داده می‌شود.

روش‌های تحلیل نشانه حمله می‌تواند با آستانه‌ها یا بدون آن‌ها استفاده شوند. درصورتی‌که هیچ آستانه‌ای تعریف نشده باشد، زمانی که یک نشانه حمله شناخته شد، هشدار تولید می‌شود. زمانی که یک آستانه تعریف شده است، هشدار تنها زمانی تولید می‌شود که تعداد نشانه‌های حمله بیش از مقدار آستانه باشد. آستانه می‌تواند به‌صورت درصد، یا یک عدد، از تعداد رخدادها در دوره زمانی و یا سنجه‌ی دیگری باشد.

اشکال اصلی روش تحلیل نشانه حمله، نیاز به به‌روز رسانی‌های مکرر است تا با جریان آسیب‌پذیری‌ها و یا حملات تازه کشف شده همپا شود.

الف-۳-۴-۲-۳ سامانه‌های خبره

در رویکردهای مبتنی بر سوءاستفاده، سامانه های خبره حاوی قوانینی هستند که نفوذها را توصیف می‌کنند.

در رویکردهای مبتنی بر ناهنجاری، مجموعه‌ای از قوانین توصیف کننده‌ی رفتار کاربران به‌صورت آماری بر اساس سوابق فعالیت‌های آن‌ها در طی یک دوره زمانی معین تولید می‌شود. این قوانین باید به‌طور پیوسته به روز شده تا توصیف‌های جدید نفوذها و یا الگوهای جدید استفاده شده را در خود جای دهد.

رویدادهای ممیزی به واقعیت‌هایی که حامل معانی آن‌ها در سامانه خبره هستند، ترجمه می‌شوند. کارکرد تحلیل نفوذ با استفاده از این قوانین و واقعیت‌ها هم برای آشکارسازی حضور یک نفوذ مشکوک و یا برای آشکارسازی رفتار متناقض نتیجه‌گیری می‌کند .

الف-۳-۴-۲-۴ تحلیل انتقال حالت

این روش یک نفوذ را با مجموعه‌ای از اهداف و انتقال‌ها توصیف می‌کند و آن‌ها را به‌صورت نمودارهای حالت-انتقال نمایش می‌دهد. حالت‌ها در نشانه حمله‌ها، متناظر با حالت‌های سامانه، دارای اعلان‌های بولی مرتبط می‌باشند که این اعلان‌ها برای انتقال به آن حالت‌ها باید برآورده شوند.

الف-۳-۴-۳ رویکرد مبتنی بر ناهنجاری

الف-۳-۴-۳-۱ مرور کلی

رویکرد مبتنی بر ناهنجاری بر پیدا کردن بی نظمی‌های رفتار مشاهده شده در رفتار معمول پیش بینی شده و یا مورد انتظار متمرکز است و بر مبنای مشاهدات قبلی سامانه در طول عملیات عادی یا رخنمون تعریف شده با استفاده از دیگر پارامترهای مورد انتظار است. رخنمون یک الگوی رویداد ویژه و از پیش تعیین شده است که معمولاً به یک دنباله از وقایع مرتبط بوده و برای هدف مقایسه در یک دادگان ذخیره شده است.

زمانی که رویکرد مبتنی بر ناهنجاری، بر این فرض است که داده‌ی رویداد با نشانه حمله همسان نیست، نفوذها و یا حملات را نشان می‌دهد، مراقبت‌هایی نیاز است که در نظر گرفته شوند. برخی داده‌های بی‌بدیل هنوز هم می‌توانند حاوی شواهدی از رفتارهای طبیعی و مجاز باشند که ممکن است درزمانی که نشانه‌های حملات الگو شده‌اند، ناشناخته بوده‌اند.

روش‌های غالب فعلی استفاده شده توسط کارکرد تحلیل مبتنی بر ناهنجاری، عبارت‌اند از:

الف-۳-۴-۳-۲ شناسایی رفتار غیرعادی

این روش الگوهای فعالیت مناسب کاربران را تطبیق می‌دهد، درحالی‌که تحلیل نشانه حمله الگوهای فعالیت نامناسب را مطابقت می‌دهد.

این روش رفتار طبیعی و یا مجاز کاربران را توسط مجموعه‌ای از وظایفی که باید انجام دهند و یا مجاز به انجام آن روی سامانه هستند، با استفاده از روش غیر آماری الگوسازی می‌کند. این وظایف و واقعیت‌ها سپس به عنوان الگوهایی برای عملیات مورد انتظار و یا مجاز مانند دسترسی به پرونده‌های ویژه و یا انواع پرونده‌ها بازنموده می‌شوند.

اقدامات افراد که در دنباله‌های ممیزی یافت شده با الگوهای مورد انتظار و یا مجاز آن‌ها مقایسه می‌شود. هشدار زمانی صادر می‌شود که الگوی عمل با الگوی مورد انتظار و یا مجاز متفاوت باشد.

الف-۳-۴-۳-۳ سامانه‌های خبره

(به الف-۳-۳-۱-۲ مراجعه کنید)

الف-۳-۴-۳-۴ روش‌های آماری

پراستفاده‌ترین روش برای رویکردهای مبتنی بر ناهنجاری به‌منظور آشکارسازی نفوذ روش‌های آماری است.

به‌منظور اندازه گیری، رفتار کاربر یا سامانه توسط تعدادی از متغیرها در طول زمان نمونه‌برداری شده و در یک رخ‌نمون ذخیره می‌شود. در فواصل منظم، رخ‌نمون فعلی با رخ‌نمون ذخیره شده ادغام شده و به عنوان تکامل رفتارهای کاربران به روزرسانی می‌شود.

نمونه‌هایی از این متغیرها شامل زمان ورود به سامانه و خروج از آن در هر نشست ، طول مدت استفاده‌ی منابع و میزان منابع پردازنده، حافظه و دیسک مصرف شده در طول یک نشست و یا در طول مدت زمان داده شده می‌باشند.

رخ‌نمون می‌تواند از انواع مختلفی از سنجه‌ها تشکیل شود. این انواع عبارت‌اند از:

- سنجه‌های شدت فعالیت،

- سنجه‌های توزیع سابقه‌ی ممیزی،

- سنجه‌های رسته ای (به‌طور مثال، فراوانی نسبی ورودها)، و / یا

- سنجه‌های عددی (به‌طور مثال، یک مقدار عددی از مقدار CPU یا I / O برای یک کاربر خاص).

رفتار غیرعادی با بررسی رخ‌نمون جاری با رخ‌نمون ذخیره شده و تعیین اینکه آیا انحراف معیار استاندارد یک متغیر بیش از مقدار آستانه شده است یا نه مشخص می‌شود.

الف-۳-۴-۳-۵ شبکه‌های عصبی

شبکه‌های عصبی الگوریتم‌هایی هستند که درباره‌ی رابطه بین بردارهای ورودی-خروجی آموزش می‌بینند و قانون کلی برای به دست آوردن بردارهای ورودی و خروجی‌های جدید به شیوه‌ای معقول کشف می‌کنند. استفاده اصلی از شبکه‌های عصبی برای آشکارسازی نفوذ در یادگیری رفتار بازیگران در سامانه است. (به‌طور مثال، کاربران، برنامه‌های Daemon). مزیت استفاده از شبکه‌های عصبی نسبت به روش‌های آماری، داشتن روشی ساده برای بیان روابط غیرخطی بین متغیرها، و یادگیری و بازآموزی شبکه عصبی به‌طور خودکار است.

الف-۳-۴-۴ روش‌های ترکیبی

روش‌های مبتنی بر سوءاستفاده و مبتنی بر ناهنجاری می‌توانند برای استفاده از مزیت‌های هردو با هم ترکیب شوند. استقرار IDPS ترکیبی اجازه می‌دهد تا آشکارسازی نفوذ مبتنی بر نشانه‌های حملات شناخته شده و همچنین الگوهای ناشناس مانند تعداد تلاش ورود یک کاربر خاص انجام شود.

همچنین تحقیقات برای بررسی رویکردهای اضافی و یا روش‌هایی برای آشکارسازی نفوذ در حال انجام است. به‌طور مثال، تحقیقات مربوط به استفاده از شبکه‌های پتری وجود دارد. همچنین یک حوزه‌ی تحقیق نسبتاً جدید نیز با عنوان ایمنی شناسی رایانه موجود است.

الف-۳-۴-۵ فراوانیِ تحلیل

الف-۳-۴-۵-۱ مرور کلی

داده‌های خام (به‌طور مثال دفتر پیگیری / ثبت رویداد) به‌طورکلی به‌طور مستمر تولید می‌شوند اما آن‌ها همیشه ممکن است توسط کارکرد آشکارسازی رویداد پردازش نشده یا توسط کارکرد تحلیل مورد تحلیل قرار نگیرند.

فراوانی تحلیل ممکن است پیوسته، دوره‌ای، و یا تحت شرایط خاص باشد.

الف-۳-۴-۵-۲ به‌طور پیوسته / نزدیکی زمان واقعی

هنگامی که کارکرد آشکارسازی رویداد به‌طور پیوسته به دنبال رخداد داده‌ها، شرایط، و یا فعالیت‌های خاص است و داده‌ی رویداد را فراهم می‌سازد، کارکرد تحلیل نیز می‌تواند به‌طور پیوسته انجام شود.

باید دقت شود که نفوذ ممکن است در برخی موارد پیش از آشکارسازی و گزارش آن به پایان برسد. یک تأخیر زمانی ممکن است بین رخداد یک رویداد و زمانی که در آن شناسایی و گزارش می‌شود، وجود داشته باشد.این تأخیر زمانی به پارامترهایی مانند منبع داده‌ی رویداد، روش آشکارسازی، و یا ماهیت نفوذ بستگی دارد که باعث زمان سپری شده بین زمانی که یک نفوذ آغازشده و هنگامی که به سامانه هدف نفوذ کرده است می‌شود.

الف-۳-۴-۵-۳ دوره‌ای / پردازش دسته‌ای

درصورتی‌که داده‌های خام و یا داده‌ی رویداد شناسایی شده به رسانه‌های ذخیره سازی منتقل شوند، احتمال شناسایی و یا تحلیل آن‌ها به‌صورت دوره‌ای یا در زمان مناسب وجود دارد. برای مثال، آشکارسازی و یا تحلیل ممکن است زمانی که بار روی سامانه IT کمتر است، مانند شب، و یا توسط یک زیر سامانه کمکی خارج از خط صورت گیرد.

الف-۳-۴-۵-۴ آغاز نمودن تحت شرایط خاص

گاهی تحلیل تنها ممکن است تحت شرایط خاصی آغاز شود، مانند زمانی که یک حمله گسترده شناسایی شده و باعث آسیب شدید شده است. در این مورد، تلاش متمرکزی ممکن است آغاز شود تا به‌طور کامل تمامی جنبه‌های حمله و عواقب آن را مورد تحلیل قرار دهد. این تلاش‌ها گاهی اوقات تحلیل قانونی نامیده

می‌شوند و ممکن است به‌منظور اقدام قانونی استفاده شوند. در صورت در نظر گرفتن اقدام قانونی، قوانین قابل‌اجرای شاهد باید دنبال شوند.

الف-۳-۵ ذخیره سازی داده

هدف از کارکرد ذخیره سازی داده‌ها ذخیره‌ی اطلاعات مربوط به امنیت و در دسترس قرار دادن آن برای تحلیل در زمان بعد و یا برای گزارش است. داده‌های ذخیره شده ممکن است شامل:

- رویدادهای آشکارشده و دیگر انواع داده‌های لازم؛

- نتایج تحلیل، ازجمله نفوذهای آشکارشده، و رویدادهای مشکوک است که می‌تواند بعداً برای هماهنگی تحلیل رویداد مشکوک مورد استفاده قرارگیرد؛

- مجموعه‌ای از رخ‌نمون‌های حملات شناخته شده و رفتار طبیعی؛ و

- داده‌های خام تفصیلی جمع‌آوری و حفظ شده به عنوان مدرک (به‌طور مثال، برای قابلیت ردیابی)، زمانی که یک هشدار امنیتی مطرح است.

باید خط‌مشی نگهداری و حفاظت داده‌ها وجود داشته باشد، که به نگرانی‌های مختلف مانند تکمیل تحلیل، شرایط قانونی داده ها، و حفظ شواهد، و همچنین حفاظت در برابر استراق سمع اطلاعات مربوط به امنیت بپردازد.

الف-۳-۶ پاسخ

هدف کارکرد پاسخ، ارائه نتایج مناسب تحلیل به کارکنان مسئول (به‌طور مثال، مدیر سامانه، کارشناس امنیتی) است. از آنجایی‌که این نتایج معمولاً بر روی یک پیشانه مدیریت با یک واسط کاربری نگاشتاری ارائه می‌شود، ابزارهای اضافی مانند رایانامه، پیام‌های متنی، تماس‌های تلفنی و غیره برای اطلاع‌رسانی نتایج به کارکنان مربوطه به‌منظور تشدید و سازماندهی پاسخ‌ها به هشدارهای ایجادشده مورد نیاز است.

درحالی‌که یک کارکرد پاسخ منفعل به تولید هشدارها بر روی پیشانه محدود است، یک کارکرد پاسخ فعال نیز می‌تواند پادکنش‌های مناسب برای نفوذ را فراهم کند. سامانه‌های آشکارسازی نفوذ که برای ارائه پاسخ به‌صورت فعال طراحی شده‌اند، به عنوان سامانه‌های پیشگیری از نفوذ (IPS) نیز شناخته می‌شوند. برخی کارکردهای فعال پاسخ می‌توانند چنین سنجه‌های اصلاحی یا پیشگیرانه را برای محدود کردن نفوذ و یا به کمینه رساندن عواقب آن، توسط موارد زیر فراهم سازند:

- پیکربندی دوباره‌ی یک سامانه مورد نفوذ قرار گرفته،

- قفل کردن یک حساب کاربری مورد نفوذ قرار گرفته و / یا

- بستن تطابق قرارداد برای یک نشست.

اطلاعات ارائه شده توسط کارکرد پاسخ می‌تواند به مرجع مناسب سازمان برای ارزیابی شدت نفوذ و تصمیم

برای اجرای پادکنش[1]های مناسب کمک کند. یک سازمان نیاز دارد اطمینان حاصل کند که ارزیابی شدت و اجرای پادکنش‌ها در مسیر خط‌مشی‌ها و روش‌های امنیت اطلاعات سازمان می‌باشند.

سازمان می‌تواند فهرستی از واپایش‌های قابل توصیه را در بند ۱۳ استاندارد ISO / IEC 27002 بیابد که شامل گزارش اطلاعات رویدادهای امنیتی، مسئولیت‌ها و روش‌هایی برای بازیابی نقض‌های امنیت و تصحیح خرابی‌های سامانه است. استاندارد ISO / IEC 27035نیز اطلاعات مفیدی در مورد مدیریت اطلاعات رخداد امنیتی فراهم می‌کند.

الف-۴ انواع IDPS

الف-۴-۱ مقدمه

همان‌طور که قبلاً ذکر شد، سه نوع IDPS وجود دارد: سامانه IDPS مبتنی بر نشانه، سامانه IDPS مبتنی بر ناهنجاری، سامانه IDPS تحلیل قرارداد دارای وضعیت. اغلب IDPSها از روش‌های آشکارسازی متعدد، به‌صورت جداگانه و یا یکپارچه برای فراهم سازی آشکارسازی گسترده‌تر و دقیق‌تر استفاده می‌کنند. گروه‌های اصلی روش‌های آشکارسازی عبارت‌اند از:

مبتنی بر نشانه، که برای شناسایی رویدادها، نشانه‌های تهدیدهای شناخته شده را با رویدادهای مشاهده شده مقایسه می‌کند. این روش در آشکارسازی تهدیدات شناخته شده بسیار مؤثر است اما در آشکارسازی تهدیدات ناشناخته و انواع بسیاری از تهدیدات شناخته شده تا حد زیادی بی‌اثر است. آشکارسازی مبتنی بر نشانه نمی‌تواند وضعیت ارتباطات پیچیده را پیگیری و درک کند، بنابراین نمی‌تواند بسیاری از حملات که شامل رویدادهای متعدد هستند را آشکارسازی کند.

در آشکارسازی مبتنی بر ناهنجاری، تعاریف این‌که چه فعالیت‌هایی هنجار در نظر گرفته می‌شود در مقابل رویدادهای مشاهده شده برای شناسایی انحرافات مهم، با هم مقایسه می‌شوند. این روش از رخ‌نمون‌هایی که توسط پایش مشخصات فعالیت معمولی در طی یک دوره‌ی زمانی توسعه داده شده است، استفاده می‌کند. سپس IDPS مشخصات فعالیت‌های جاری را با آستانه‌های مربوط به رخ‌نمون مقایسه می‌کند. روش‌های آشکارسازی مبتنی بر ناهنجاری می‌توانند در آشکارسازی تهدیدات ناشناخته بسیار مؤثر واقع شوند. مشکلات سهوی متداول در آشکارسازی مبتنی بر ناهنجاری شامل فعالیت‌های مخرب در یک رخ‌نمون، ایجاد رخ‌نمون-هایی که به اندازه کافی پیچیده نیستند تا منعکس‌کننده‌ی فعالیت‌های محاسباتی دنیای واقعی باشند، و تولید مثبت‌های کاذب بسیار است.

تحلیل قرارداد دارای وضعیت که رخ‌نمون‌های از پیش تعیین‌شده‌ی تعاریف فعالیت قراردادهای بی‌خطر پذیرفته شده برای هر حالت قرارداد را با رویدادهای مشاهده شده برای شناسایی انحرافات مقایسه می‌کند. بر خلاف آشکارسازی مبتنی بر ناهنجاری، که از رخ‌نمون‌های میزبان و یا خاص شبکه استفاده می‌کند، تحلیل قرارداد دارای وضعیت متکی بر رخ‌نمون‌های جهانی توسعه یافته توسط فروشنده است که بایدونبایدهای

1- Countermeasure

استفاده از قراردادهای خاص را مشخص می‌کنند. این روش قادر به درک و ردیابی وضعیت قراردادهایی است که مفهوم حالت دارند که به آن اجازه می‌دهد تا بـه آشکارسـازی بسـیاری از حمـلات کـه روش‌هـای دیگـر نمی‌توانند، بپردازد. مشکلات روش تحلیل قرارداد دارای وضعیت شامل این است که توسـعه الگوهـای کـاملاً دقیق برای قراردادها اغلب بسیار دشوار یا غیرممکن است، این روش بسیار متمرکز بر منبع است و نمی‌توانـد حملاتی را که ویژگی‌های کلی رفتار قرارداد قابل قبول را نقض نمی‌کنند را آشکارسازی کند.

انواع دیگری از IDPS وجود دارد:

- سامانه IDPS مبتنی بر کاربرد(AIDPS)، اما این نوع یک طبقه خاص از HIDPS است و دارای ویژگی‌های مشابه با HIDPS است.

به‌طورکلی، IDPS قادر به انجام وظایف زیر است:

- پایش و تحلیل رویدادهای سامانه و رفتارهای کاربر،

- تشخیص الگوهای رویدادهای سامانه که با حملات شناخته شده مطابقت دارد،

- تشخیص الگوهای فعالیت که ازلحاظ آماری با فعالیت‌های عادی متفاوت است،

- هشدار به کارکنان مناسب با استفاده از ابزار مناسب هنگامی که حملات آشکارسازی شده‌اند،

- انجام سنجش خط‌مشی‌های امنیتی کدگذاری شده در موتور تحلیل،

- اجازه به خبرگان غیرامنیتی برای اجرای کارکردهای مهم پایش امنیتی،

- افزایش خطرات برداشت شده از کشف و مجازات مهاجمان،

- شناسایی مشکلات بسیاری که توسط افزاره‌های امنیتی دیگر پیش‌گیری نشده‌اند،

- هماهنگی رویدادها با افزاره‌های امنیتی دیگر مانند دیوارهای آتش،

- شناسایی، نوشتن جزء به جزء و توصیف تهدیدات مجازی به سامانه‌های اطلاعاتی یک سازمان و

- ارائه اطلاعات ارزشمند در مورد نفوذها که از بررسی حادثه، ارزیابی آسیب، تلاش‌هـای بازیـابی و عملیـات قانونی در شرایط خاص حمایت می‌کند.

سامانه IDPS محدودیت هایی دارد که باید درک شوند. محدودیت‌های قابل‌توجه عبارت‌اند از:

- نمی‌تواند حملات جدید را آشکارسازی کند، و جدیدترین تغییرات حملات را ضبط کند.

- مشکل در جبران خطاها و اختلال از منابع اطلاعاتی،

- مشکل در برخورد مؤثر با شبکه‌های سوداده[1]،

- مشکل مقیاس‌پذیری برای شبکه‌های بسیار بزرگ و یا توزیع شده،

1- Switched networks

- مشکل در تعیین محل فیزیکی و یا مجازی مزاحم از یک خروجی IDPS،

- مشکل یکپارچه سازی محصولات مختلف IDPS با سامانه‌های مدیریت شبکه،

- عدم توانایی در جبران خط‌مشی امنیتی و یا سازوکارهای امنیتی ضعیف و یا ناموجود در زیرساخت‌های حفاظت، مانند دیوارهای آتش، شناسایی و اصالت‌سنجی، رمزگذاری پیوند، سازوکارهای واپایش دسترسی، و آشکارسازی و ریشه‌کنی ویروس،

- عدم توانایی در آشکارسازی، گزارش، و یا پاسخ به اندازه‌ی کافی سریع به انواع خاصی از حملات،

- عدم توانایی کاهش اغلب حملات DOS، به‌رغم توانایی شناسایی آن‌ها،

- عدم توانایی در آشکارسازی حملات جدید و یا برخی از انواع حمله‌های موجود (این مورد تنها IDPS مبتنی بر نشانه را شامل می‌شود و نه IDPS مبتنی بر ناهنجاری)،

- ناتوانی در انجام تحلیل تفصیلی حملات بدون دخالت انسان،

- عدم توانایی در جبران کاستی‌های قابل‌توجهی در راهبرد امنیت، خط‌مشی، و یا معماری امنیت سازمان

- عدم توانایی در جبران ضعف‌های امنیتی در قراردادهای شبکه،

- احتمال آن‌که خروجی IDPS نوعاً شامل نرخ خطای قابل‌توجهی به خصوص مثبت‌های کاذب باشد، و می‌تواند زمان و منابع زیادی برای حل‌وفصل آن در اختیار بگیرد.

- احتمال غیر فعال شدن به عنوان بخشی از دنباله‌ی یک حمله،

- احتمال بهره‌جویی توسط مهاجمان برای تولید مثبت‌های کاذب برای منحرف کردن توجه از حمله اصلی،

- احتمال ایجاد حجم زیادی اطلاعات ممیزی که ممکن است نیاز به ذخیره‌سازی محلی اضافه بر روی سامانه داشته باشد،

- احتمال این‌که مسدود کردن خودکار بر مبنای هشدارهای IDPS باعث مشکلات امنیتی و دسترس‌پذیری شود.

- نیاز به عمق فنی و دانش سامانه‌ای برای استفاده به‌طور مؤثر.

الف-۴-۲ IDPS مبتنی بر میزبان (HIDPS)

سامانه HIDPS بر روی یک رایانه مستقر شده و حفاظت را برای آن رایانه‌ی خاص فراهم می‌کند. این حالت به HIDPS اجازه می‌دهد تا داده‌ی ثبت رویدادهای (برای مثال دفتر پیگیری یا ثبت رویدادها) سامانه‌ی عامل و داده‌های محلی دیگر را بررسی کند. سامانه HIDPS همچنین ممکن است رخداد رویدادهای برنامه‌های کاربردی را نیز با استفاده از پرونده‌های ثبت رویداد سامانه عامل یا برنامه‌های کاربردی تحلیل کند.

دفتر پیگیری سامانه عامل ، که HIDPS معمولاً استفاده می‌کند معمولاً در درونی‌ترین سطح (هسته‌ی اصلی) سامانه‌ی عامل تولید می‌شود و درنتیجه تفصیلی‌تر بوده و محافظت‌کننده‌ی بهتری نسبت به ثبت رویدادهای سامانه می‌باشند. با این‌که ثبت رویدادهای سامانه کوچک‌تر از دفتر پیگیری است و راحت‌تر درک می‌شود.

برخی HIDPSها برای پشتیبانی از مدیریت متمرکز IDPS و زیرساخت گزارش دهی طراحی شده‌اند که اجازه می‌دهد یک پیشانه مدیریت واحد بسیاری از میزبان‌ها را ردیابی کند. برخی دیگر از HIDPSها پیام‌هایی را در قالب‌های سازگار با سامانه‌های مدیریت شبکه تولید می‌کنند.

برخلاف NIDPS، HIDPS می‌تواند نتیجه یک تلاش حمله را مشاهده کند، همانطورکه به‌طور مستقیم می‌تواند پرونده‌های داده و فرآیندهای سامانه که معمولاً مورد هدف حملات قرار دادند را دسترسی و پایش نماید. به‌طور مثال، HIDPS اجازه آشکارسازی حملات از صفحه کلید یک کارساز مأموریت بحرانی را می‌دهد.

سامانه HIDPS برای موارد زیر طراحی شده است:

- پیوند هویت کاربر خاص با فعالیت‌های مشکوک،

- مشاهده و پیگیری تغییرات رفتاری کاربر،

- مبناسازی حالت امنیتی یک سامانه، و ردیابی تغییرات در آن مبنا،

- مدیریت سازوکارهای ثبت رویدادها و دفتر پیگیری سامانه عامل و داده‌های تولید شده،

- فراهم سازی ثبت رویدادها و پایش در سطح برنامه کاربردی، زمانی که داده‌ها به‌صورت رمزگذاری شده یا غیر رمزگذاری شده منتقل شده و یا ذخیره می‌شوند.

- مشاهده تغییرات داده ناشی از حملات؛

- پایش سامانه‌هایی که روی شبکه‌های با سرعت بالا و در شبکه‌هایی که از رمزگذاری استفاده شده است، مستقر شده‌اند.

- شناسایی حملاتی که توسط IDPS مبتنی بر شبکه دیده نمی‌شود.

سامانه HIDPS محدودیت‌های منحصر به فردی دارد که باید درک شوند. محدودیت‌های قابل‌توجه شامل موارد زیر است:

- احتمال اینکه حملات خاص DOS بتوانند HIDPS را غیر فعال کنند،

- احتمال اینکه HIDPS منابع میزبان، ازجمله نیازمندی‌های ذخیره سازی داده برای ثبت رویدادهای پیگیری میزبان را مصرف کند.

- احتمال نیاز به فرآیندهای پیچیده‌ی نصب و راه‌اندازی و تعمیر و نگهداری به دلیل تعداد زیاد نمونه‌های نصب شده (کمینه یکی برای هر میزبان)،

- عدم توانایی استفاده در حالت مخفیانه[1]، چون میزبان‌ها معمولاً توسط لایه‌های بالاتر شبکه آدرس‌دهی می‌شوند.

- عدم توانایی در تشخیص حملاتی که در میزبان‌های دیگر و یا در شبکه هدایت شده‌اند.

الف-۴-۳ IDPS مبتنی بر شبکه (NIDPS)

سامانه NIDPS ترافیک به مقصد سامانه‌های میزبان شبکه را پایش می‌کند. سامانه NIDPS اغلب شامل مجموعه‌ای از حسگرهای تک هدفی یا میزبان‌هایی است که در نقاط مختلف یک شبکه واقع شده‌اند. این واحدها ترافیک شبکه را پایش کرده، برای این ترافیک تحلیل محلی انجام داده و حملات به پیشانه مدیریت مرکزی را گزارش می‌دهند. ازآنجایی‌که حسگرها به‌طور خاص به عنوان یک جزء IDPS استفاده می‌شوند، می‌توان آن‌ها را به‌راحتی در برابر حمله محافظت نمود. بسیاری از این حسگرها به‌منظور مشکل‌تر شدن تعیین حضور و محل آن‌ها توسط مهاجم، برای لایه‌های بالاتر شبکه پنهان می‌باشند. (به‌طور مثال طراحی شده برای اجرا در حالت «مخفیانه»)

سامانه NIDPS اجازه آشکارسازی و پاسخ زمان واقعی یا نزدیک به زمان واقعی را با فراهم کردن اطلاعات نفوذهای مشکوک، به‌محض رخداد آن‌ها صادر می‌کند (به‌طور مثال حمله‌ی DoS)، درحالی‌که بهنگام بودن پاسخ از جانب HIDPS با فراوانی فاصله‌ی داده‌خواهی[2] در ارتباط مستقیم است.

از ویژگی‌های منحصر به فرد NIDPS، توابع با توانایی‌های زیر است:

- عمل در حالت مخفیانه و پنهان کردن حسگر از قراردادهای لایه‌های سطح بالاتر شبکه (معمولاً لایه ۳ و بالاتر)،

- استفاده از یک حسگر واحد برای پایش ترافیک چندین میزبان در همان بخش شبکه، و

- تشخیص حملات توزیع شده که بسیاری از میزبان‌ها را تحت تأثیر قرار می‌دهد.

سامانه NIDPS محدودیت‌های منحصر به فردی دارد که باید درک شوند. محدودیت‌های قابل‌توجه شامل موارد زیر است:

- عدم توانایی در مقابله مناسب با ترافیک شبکه‌های رمزگذاری شده،

- احتمال نیاز به پهنای باند بسیار بالاتر و توانمندی پردازش سریع تر از HIDPS زیرا، برای به بیشینه رساندن تأثیر NIDPS، ظرفیت کارکرد آن باید با حجم ترافیک آن بخش شبکه که در آن مستقرشده است، برابر باشد.

- احتمال این‌که بسیاری از کارکردهای فراهم شده توسط NIDPS نیاز به تنظیم خاص فنی داشته باشند تا در شبکه‌های نو مبتنی بر سوده در دسترس باشند.(به‌طور مثال حسگرهای شبکه که نیازمند اتصال به

1- Stealth Mode
2- Polling

درگاهی‌های ویژه‌ی سوده‌های شبکه که داده‌های همه‌ی درگاهی‌های دیگر را منعکس می‌کنند، هستند.)

- احتمال اینکه برخی NIDPSها مشکلات روبرو شدن با حملات قطعه‌قطعه شدن بسته‌ها در لایه‌ی شبکه (IP) و یا سطح انتقال (TCP / UDP) داشته باشند که به دلیل مسائل مربوط به رمزگشایی قراردادهای سطح کاربرد (به‌طور مثال HTTP، SMTP) است.

- به‌طور معمول ناتوانی در مشاهده‌ی اینکه آیا یک حمله موفق شده است.

الف-۵ معماری

سامانه IDPS ممکن است به شیوه‌های متفاوت اجرا شده باشد.

در سازمان‌های کوچک‌تر، و یا برای محافظت از یک سامانه‌ی به خوبی تعریف شده و نسبتاً مستقل، سامانه IDPS واحد ممکن است راه‌حل خوبی باشد.

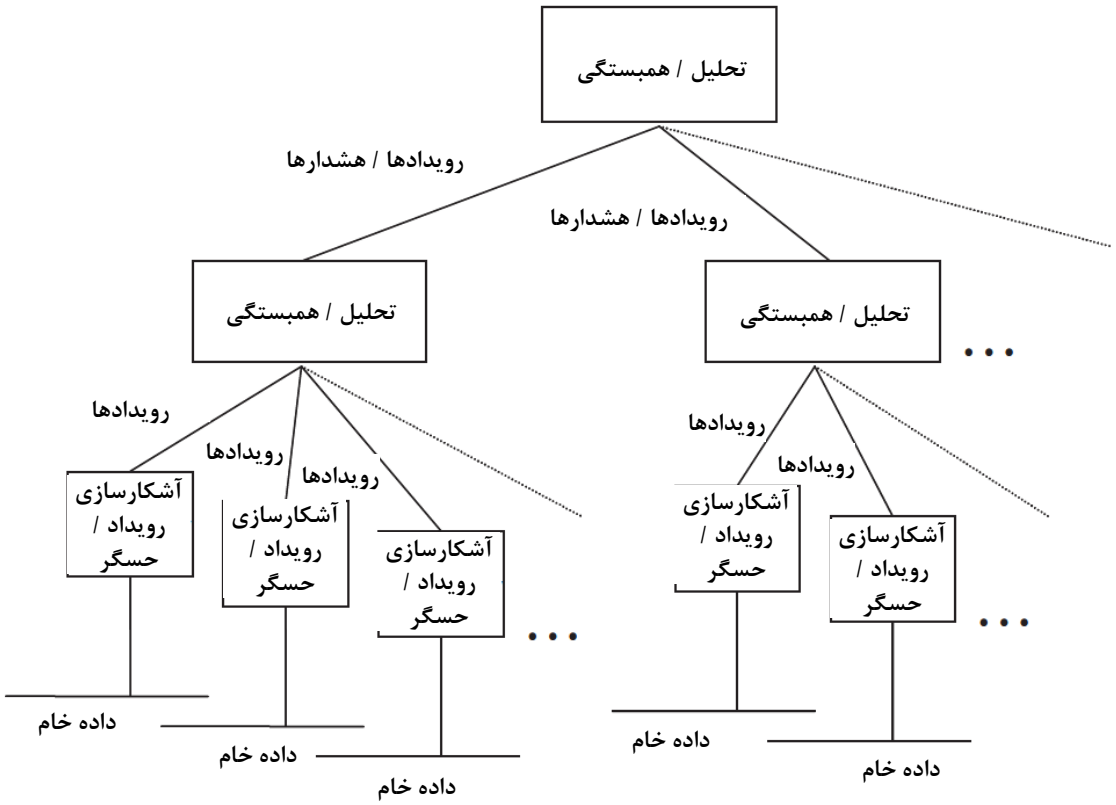
در محیط‌های با زیرساخت‌های بسیار بزرگ و پیچیده برای شبکه‌ها، سامانه‌ها و برنامه‌های کاربردی، سامانه IDPS واحد ممکن است برای تحقق الزامات آشکارسازی نفوذ ناکافی و یا غیرعملی باشد. برای تحقق این الزامات چندین IDPS ممکن است مورد نیاز باشد که هر یک متناسب با یک زیر سامانه تعریف شده یا یک

جزء است. در چنین محیط‌هایی، حملات ممکن است چند زیر سامانه‌یا چند جزء را مورد هدف قرار دهند. فرانامه‌ی دیگر، یک حمله ممکن است یک پیکربندی خاص از زیر سامانه و یا اجزاء را به جای هدف قرار دادن آسیب‌پذیری یک زیر سامانه و یا یک جزء هدف قرار دهد. به‌منظور شناسایی یک حمله در چنین فرانامه‌ای، داده‌ی رویداد از چند IDPS باید ارتباط داده شده و تحلیل شوند.

هدف از معماری IDPS اجرای کارکردهای آشکارسازی نفوذ به روشی کارآمد و مؤثر است. دو مورد از ملاحظات اولیه معماری در این زمینه موارد زیر می‌باشند:

- روشی که در آن چند IDPS به هم پیوسته و مرتبط هستند،

- تمرکز و یا توزیع وظایف در معماری IDPS.



شکل الف-۲- معماری سلسله مراتبی آشکارسازی نفوذ

مثالی از معماری سلسله مراتبی آشکارسازی نفوذ در شکل الف-۲ نشان داده شده است. در شکل الف-۲، خروجی چندین جزء تحلیل و همبستگی برای سطح بالاتری از تحلیل و همبستگی مجتمع شده‌اند. در هر زیرساخت برنامه‌های چند لایه ممکن است، مکان‌های مختلفی برای اجرای کارکردهای مورد نیاز وجود داشته باشد.

در معماری متمرکز، اجزای آشکارسازی رویداد و حسگر ممکن است به سادگی داده‌های خام را جمع‌آوری کرده و آن به یک جزء واحد برای تحلیل بیشتر و همبستگی ارسال نمایند. اگرچه این رویکرد دارای مزیت طراحی ساده است، اما به خوبی مقیاس‌پذیر نیست و تنها ممکن است برای محیط‌های کوچک‌تر مناسب باشد.

راه‌حل‌های مقیاس پذیرتر ممکن است برخی از وظایف IDPS را در اجزای غیرمتمرکز با هدف کاهش داده‌های خام انجام دهند. در مراحل اولیه‌ی فرآیند، تا جایی که ممکن است رویدادها را به لایه‌ی بعدی ارسال می‌کند. زنجیره ای از اجزا ممکن است تحلیل و همبستگی بیشتر داده‌ی رویداد را انجام داده و تنها رویدادهای مرتبط با هشدارها را به یک جزء مرکزی و نهایی انتقال می‌دهد. چنین سامانه‌ای ممکن است تعدادی وظیفه‌ی بسیار پیچیده را معرفی کند. به‌طور مثال، این سامانه نیازمند پیکربندی پالایه‌ها و اجزای درگیر تحلیل و همبستگی به روشی که نشانه‌های حمله راه خود را به جزء مرکزی یافته و هشدار صحیح

صادر شود.

الف-۶ مدیریت IDPS

الف-۶-۱ مقدمه

مدیریت سامانه‌های آشکارسازی نفوذ برای استقرار کارآمد و مؤثر در زیرساخت‌های شبکه شرکت‌ها بسیار حیاتی است.. به‌منظور کارآمدی IDPS زیر سامانه‌ی مدیریت باید توانمندی کافی را فراهم کند. این بخش به جنبه‌های مختلف مدیریت IDPS می‌پردازد.

الف-۶-۲ مدیریت پیکربندی

الف-۶-۲-۱ مرور کلی

مدیریت پیکربندی کارکردهایی را برای اعمال واپایش بر شناسایی، جمع‌آوری داده‌ها و فراهم کردن داده برای موجودیت‌هایی که بخشی از IDPS هستند، فراهم می‌کند. به‌منظور آشکارسازی نفوذ،مدیریت پیکربندی شامل مدیریت کارکرد آشکارسازی و سازوکارهای متناظر استفاده شده است.

الف-۶-۲-۲ کارکرد آشکارسازی

پیکربندی کارکرد آشکارسازی شامل تنظیم معیار برای اینکه چه رویدادها و یا توالی از رویدادها خط‌مشی‌های امنیتی را نقض کرده‌اند، است. این کارکرد همچنین ممکن است شامل توصیف الگوهای سوءاستفاده و رفتار عادی کاربر باشد.

الف-۶-۲-۳ کارکرد پاسخ

مدیریت کارکرد پاسخ رفتار سامانه در قبال یک هشدار امنیتی را تعیین می‌کند. این کارکرد شامل واپایش سازوکارهای مختلف پاسخ مانند هشدارهای شنیداری، هشدارهای مدیر و یا کارشناس امنیتی و پایان نشست است. سامانه IDPS همچنین باید از آغاز هشدارهای غیرمجاز محافظت شود. در موردی که مهاجم راهی را برای فریب سامانه به‌منظور پاسخ به نفوذهای ناموجود می‌یابد، می‌تواند به‌طور بالقوه، بسته به پاسخ‌های پیکربندی شده، باعث آسیب بیشتر نسبت به آسیبی که بدون نصب IDPS محتمل است شود. احتمال پذیر است. مدیریت پاسخ باید مطابق با طرح مدیریت رخداد سازمان مطابقت داشته باشد.

الف-۶-۲-۴ مدیریت خدمات امنیتی

مدیریت خدمات امنیتی شامل مدیریت کردن خدمات امنیتی است که بخشی از IDPS به شمار می‌روند. این مدیریت شامل واپایش اعتبار کاربران، محرمانگی، یکپارچگی، و خدمات واپایش دسترسی است. بسته به اعتبار کاربران، حق دسترسی ممکن است به دسترسی محدود به پارامترهای پیکربندی، دفتر پیگیری و اطلاعات مرتبط با رویدادهای امنیتی منحصر شود.

الف-۶-۲-۵ یکپارچگی با دیگر سامانه‌های مدیریت

سامانه مدیریت IDPS باید واسطی امن یا بخشی جدایی ناپذیر از مدیریت شبکه، مدیریت سامانه و یا سامانه‌های مدیریت امنیت محیط حافظت شده باشد. این یکپارچگی برای پیاده سازی انواع خاصی از کارکردهای آشکارسازی و انواع خاصی از کارکردهای پاسخ ضروری به نظر می‌رسد(به‌طور مثال برای دسترسی به ثبت رویدادها). نکته‌ی کلیدی این است که IDPS نمی‌تواند به تنهایی انتخاب و یا اجرا شود، زیرا کارکرد مدیریت IDPS باید به خوبی با دیگر کارکردهای مدیریت سامانه‌یکپارچه گردد.

الف-۶-۲-۶ امنیت عملیات مدیریت

الف-۶-۲-۶-۱ مرور کلی

امنیت عملیات‌های مدیریت باید برای پیشگیری از دسترسی مهاجم به اطلاعات IDPS و یا منابع واپایش IDPS محافظت گردد. امنیت مدیریت IDPS شامل اصالت‌سنجی، یکپارچگی، محرمانه بودن، و در دسترس بودن خدمات مدیریت است.

سامانه‌ای که مزیت‌های مدیریت IDPS را اجرا می‌کند باید مطابق با خط‌مشی امنیتی پیکربندی شود که نیازمند سطح بالایی از امنیت (قابل مقایسه با آنچه که برای دیگر سامانه‌های مدیریت مورد نیاز است) است. از آن جایی که حسگرهای IDPS مبتنی بر میزبان به‌طور معمول در حالت ممتاز سامانه‌ی عامل اجرا می‌شوند، به خطر انداختن امتیازات مدیریت ممکن است به نقض شدید و گسترده‌ی امنیتی منجر شود و به‌طور بالقوه تمام میزبان‌هایی که در حال اجرای عامل IDPS می‌باشند، می‌توانند به خطر بیافتند. عواقب ناشی از نقض امنیت امتیازات مدیریت IDPS اغلب نادیده گرفته می‌شود. به خصوص با IDPS مبتنی بر میزبان، که بسیاری از عرضه‌های تجاری آن دارای گزینه‌ی پاسخ حمله با اجرای یک فرمان روی میزبان پایش شده می‌باشند.

پایش آشکارسازهای رویداد و حسگرها برای اطمینان از کارکرد و عملیات صحیح برای یک IDPS موفق ضروری است. آشکارسازهای رویداد، اطلاعات را از حسگرها به کارکرد تحلیل آشکارسازی بازپخش می‌کنند. خطا در نگهداری یک کارکرد در حال اجرای پایش این افزاره‌ها ممکن است به امنیت کاذب منجر شود، به‌طور مثال، یک اشکال در حسگر به وجود آمده و سامانه‌ی مرکزی (و درنتیجه سازمان) از این خطای فنی آگاه نمی‌شوند. درنتیجه سامانه‌ی مرکزی هیچ هشدار و یا قرائتی[1] برای ارسال به کارورَ مرکزی که هنوز معتقد است همه چیز به خوبی پیش می‌رود نخواهد داشت.

الف-۶-۲-۶-۲ اصالت‌سنجی

عملیات مدیریت باید توسط موجودیت مناسب مدیریت شناسایی و اصالت‌سنجی محافظت گردد. موجودیت مدیریت ممکن است کاربر انسانی یا یک موجودیت سامانه باشد.

الف-۶-۲-۶-۳ یکپارچگی

1- Reading

عملیات مدیریت باید در برابر حملات یکپارچگی محافظت شوند. اضافه، حذف و یا تغییر یک عملیات مدیریت به شیوه‌ای غیرمجاز امکان‌پذیر نیست.

الف-۶-۲-۶-۲ محرمانگی

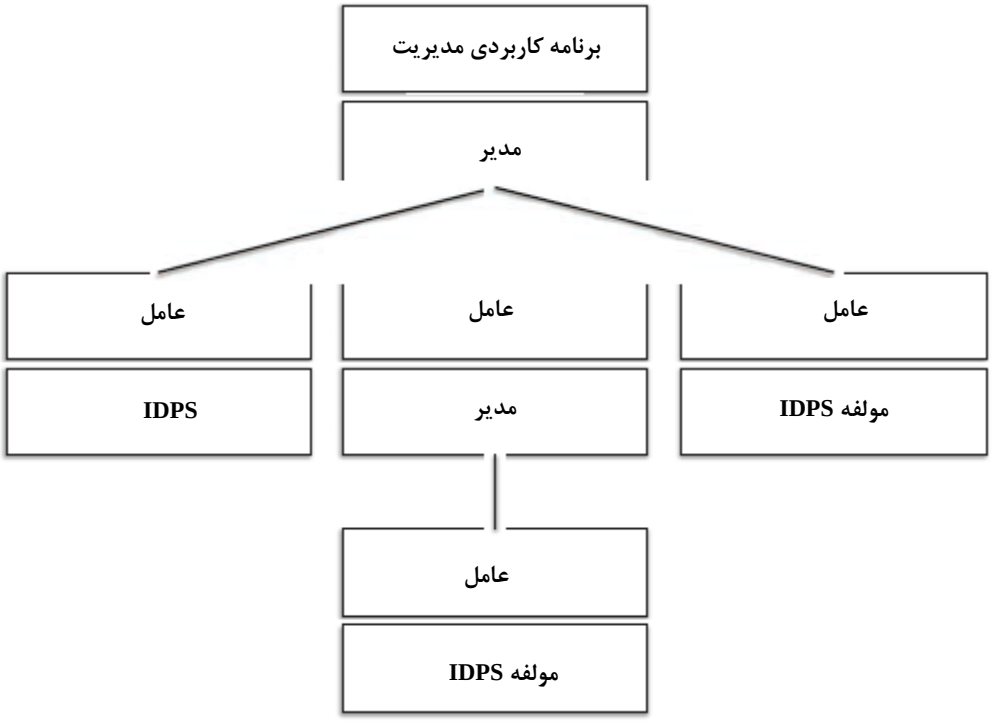
عملیات مدیریت باید در برابر حملات محرمانگی محافظت گردد. استنباط هدف هرگونه عملیات مدیریت با روش‌های غیرمجاز نباید امکان‌پذیر باشد.

الف-۶-۲-۶-۲ دسترس‌پذیری

حمله به زیرساخت‌های شبکه، IDPS خود ، و یا هدف پایش شده نباید دسترس‌پذیری خدمت مدیریت را تحت تأثیر قرار دهد. به‌طور مثال، مدیریت IDPS باید تحت یک حمله‌ی انکار خدمت(DOS) ممکن باشد. مدیریت IDPS باید حتی زمانی که IDPS بد عمل می‌کند نیز ممکن باشد. سامانه IDPS و مدیریت آن باید در فرآیند برنامه‌ریزی تداوم کسب‌وکار عنوان شده باشد.

الف-۶-۳ مدل مدیریت

واپایش و مدیریت برای پیاده سازی موفق آشکارسازی نفوذ ضروری است، به‌ویژه در محیط‌های توزیع شده که در آن تعداد زیادی از اجزاء آشکارسازی نفوذ استفاده شده‌اند. شکل الف-۳ مثالی از پیاده سازی یک مدل مدیریت به شیوه‌ی سلسله مراتبی ارائه نموده است. این مدل به خوبی برای سازمان‌های بزرگ مناسب است. مواقعی وجود دارد که در آن واپایش متمرکز، نقطه‌ی شکست واحد را نشان می‌دهد که در برخی محیط‌ها ممکن است قابل قبول نباشد. این مورد همچنین به مهاجم نقطه‌ی واحد حمله را خواهد داد و می‌تواند فرصت به تأخیر انداختن آشکارسازی را به مهاجم بدهد و از اقدامات مناسب توسط مدیر جلوگیری نماید.



شکل الف-۳- مدل مدیریت آشکارسازی نفوذ

علاوه بر عدد اصلی یک به چند که در مدل سلسله مراتبی مورد استفاده قرار می‌گیرد، عدد اصلی‌های دیگر روابط مدیریت نیز ممکن است مناسب باشند:

- چند-به-چند - چندین پیشانه مدیریت می‌توانند تعداد زیادی عامل توزیع شده را مدیریت کنند.

- یک-به-چند- یک پیشانه مدیریت می‌تواند تعداد زیادی عامل توزیع شده را مدیریت کند.

- یک-به-یک - یک پیشانه مدیریت می‌تواند یک عامل را مدیریت کند.

الف-۷ مسائل پیاده سازی و استقرار

الف-۷-۱ مقدمه

هنگامی که تصمیم گرفته می‌شود که استقرار IDPS مورد نیاز است، مسائل مهم و ملاحظات بسیاری مطرح می‌شوند. همه‌ی IDPS ها مثل هم نیستند، درنتیجه الزامات شرکت ازلحاظ مدیریت مخاطره‌ی IT و خط‌مشی امنیتی در ارزشیابی IDPS برای استقرار باید در نظر گرفته شوند.

الف-۷-۲ کارایی

ملاحظه‌ی مهم در ارزیابی استقرار IDPS کارایی است. برای ارزیابی کارایی IDPS چندین معیار مرتبط وجود دارد:

دقت: عدم دقت زمانی رخ می‌دهد که IDPS به‌صورت نادرست یک فعالیت را به عنوان حمله شناسایی کند (به‌طور مثال مثبت کاذب) یا زمانی که IDPS به‌صورت نادرست یک حمله را به عنوان عمل قانونی تشخیص دهد (به‌طور مثال منفی کاذب) نسبت هر دو نوع شکست به تعداد کل رویدادهای وارسی شده قابلیت استفاده‌ی IDPS را به‌طور قابل‌توجهی تحت تأثیر قرار می‌دهد. نسبت مثبت‌های کاذب به منفی‌های کاذب ممکن است یک پارامتر خط‌مشی امنیتی مهم باشد و نشان‌دهنده‌ی پیش قدر اجرای تحلیل است.

عملکرد: عملکرد IDPS میزانی است که در آن رویدادهای ممیزی جمع‌آوری ذخیره سازی و پردازش می‌شوند. در حالتی که عملکرد IDPS ضعیف است، آشکارسازی زمان واقعی امکان‌پذیر نیست. جنبه‌ی دیگر عملکرد به بار شبکه اشاره می‌کند که IDPS ممکن است تولید کند.

کامل بودن :عدم کامل بودن زمانی رخ می‌دهد که IDPS نتواند حمله را آشکارسازی کند.ارزیابی این سنجه بسیار مشکل‌تر از سنجه‌های دیگر است زیرا داشتن دانش جهانی درباره‌ی حملات و یا سو استفاده از اختیارات غیرممکن است.

رواداری خطا: IDPS باید خودش در مقابل حملات مقاوم باشد به‌ویژه حمله‌ی انکار خدمت و باید با این هدف طراحی شده باشد. این مورد بسیار مهم است زیرا بسیاری از IDPS ها روی سامانه عامل و یا سخت‌افزار در دسترس به‌صورت تجاری اجرا می‌شوند که در مقابل حملات آسیب‌پذیر شناخته شده‌اند.

به موقع بودن: سامانه IDPS باید تحلیل خود را با بیشترین سرعت ممکن انجام داده و منتشر کند تا کارشناس امنیتی را برای نشان دادن واکنش قبل از اینکه آسیب بیشتر ایجاد شود فعال کند.و همچنین مانع مهاجم برای خرابکاری داده‌ها، منابع داده و یا خود IDPS شود.

الف-۷-۳ کارکرد

ملاحظه‌ی مهم دیگر در استقرار IDPS کارکرد و مسائل مربوط به آن است که در بخش‌های پیش‌رو مورد بحث قرار گرفته است. تعدادی از جنبه‌های عملکرد در ادامه مورد بحث قرار می‌گیرند :

استفاده در محیط‌های رمزگذاری یا سودهی شده: IDPS مبتنی بر میزبان می‌تواند به خوبی برای محیط‌های رمزگذاری شده و سودهی شده مناسب باشد. ازآنجایی‌که سامانه‌های مبتنی بر میزبان بر روی میزبان‌های مختلف در سراسر شرکت مقیم شده‌اند، می‌توانند بر برخی از چالش‌های استقرار که IDPS های مبتنی بر شبکه در محیط‌های سودهی شده و رمزگذاری شده با آن مواجه می‌شوند، غلبه کنند.

آشکارسازی حملات به‌محض رخ دادن آن‌ها: منابع داده مبتنی بر شبکه اجازه‌ی آشکارسازی زمان واقعی و پاسخ را با فراهم نمودن داده برای آشکارسازی حملات مخرب و مشکوک به‌محض رخ دادن آن‌ها صادر می‌کنند، (به‌طور مثال یک حمله‌ی انکار خدمت) درنتیجه اطلاع رسانی و پاسخ سریع‌تر را فراهم می‌سازند. سامانه IDPS مبتنی بر شبکه، حملاتی را که سامانه‌های مبتنی بر میزبان از دست داده‌اند، آشکارسازی می‌کند. بسیاری از حملات تکه‌تکه شدن بسته و انکار خدمت مبتنی بر IP تنها با مشاهده‌ی سرآیند[1] بسته

1- Header

ها زمانی که در سراسر شبکه جابجا می‌شوند، می‌توانند شناسایی شوند.

تحلیل ترکیبی داده‌های مبتنی بر میزبان و مبتنی بر شبکه: برخی از IDPS ها داده‌هایی از هر دو منبع میزبان و شبکه استفاده می‌کنند و درنتیجه اجزای میزبان و شبکه را یکپارچه می‌سازند. راه‌حل‌های IDPS مبتنی بر میزبان و شبکه هر کدام نقاط قوت و مزایای منحصر به فردی دارند که هر یک مکمل دیگری است. همان‌طور که در بند ۶-۱ بحث شده است، روش‌های آشکارسازی نفوذ مبتنی بر میزبان و مبتنی بر شبکه می‌توانند در تحلیل با هم ترکیب شده تا یک مدافع قدرتمندتر سامانه‌ی اطلاعاتی را ایجاد کنند.

الف-۷-۴ کارکنان استقرار و عملیات IDPS

سامانه IDPS انتخاب شده ممکن است پیشرفته‌ترین باشد و زیر سامانه‌های آن به خوبی با هم و با سامانه‌های فناوری اطلاعات شما، خدمت و یا شبکه با هم یکپارچه شده باشند. بااین‌حال، بسیاری از کارکردها باید به‌صورت دستی توسط افراد آموزش دیده و آگاه در مورد آشکارسازی نفوذ، امنیت IT شامل امنیت شبکه و IT سازمان (ازجمله همبندی شبکه و پیکربندی).

فرآیند آشکارسازی نفوذ شامل نصب یک IDPS و در اختیار داشتن منابع انسانی است که بتوانند:

- سامانه IDPS را سفارشی سازی کنند به‌طوری‌که به دنبال رویدادهایی مرتبط به محیط IT جایی که در آن مستقر شده، بگردد.

- تفسیر آنچه IDPS به شما می‌گوید زمانی که یک هشدار خاموش می‌شود،

- توسعه خط‌مشی‌ها و روش‌هایی برای پاسخ به هشدارهای IDPS که واقعی به نظر می‌رسند،

- اصلاح آسیب‌پذیری‌هایی که باعث شده‌اند، نفوذ به موفقیت دست یابد.

این عملیات نیروی انسانی بر، فراتر از نصب و راه‌اندازی IDPS است و باید بخشی از فرآیند آشکارسازی نفوذ در نظر گرفته شود.

کارکرد تحلیل داده‌های جمع‌آوری شده از حسگر را برای نشانه‌های فعالیت‌ها و یا رویدادهای غیرمجاز و یا مشکوک تحلیل می‌کند که ممکن است نشان‌دهنده‌ی اینکه رخداد شنود و یا پویش شبکه در حال وقوع است،یک نفوذ به وقوع پیوسته است و یا حمله‌های مخرب در جریان است باشند.

بخش‌های خودکار نمی‌توانند بدون کمک انسانی برای ورودی، پیکربندی، تفسیر، خروجی و یا تنظیم IDPS عمل کنند.

هنگامی که یک IDPS به درستی پیکربندی شده باشد، اطلاعاتی را فراهم می‌کند که باید به‌منظور درک اینکه چه رفتارهای نفوذی ای در شبکه در حال رخداد است، به‌دقت مورد تحلیل قرار گیرند. سامانه IDPS نیازمند تعامل فشرده با انسان است و نمی‌تواند به آرامی بر روی شبکه قرار گرفته و بسته‌های ناخواسته را رد کند. سامانه IDPS نیازمند افراد ماهر است که قادر به درک این باشند که چه زمانی خروجی IDPS چیزی قابل نگرانی است در مقابل اینکه فقط یک مثبت کاذب (فعالیتی که به عنوان نفوذ طبقه‌بندی می‌شود

درحالی‌که قانونی است) و یا منفی کاذب است (فعالیت نفوذی که به وقوع پیوسته است، اما به عنوان فعالیت غیر نفوذی مشخص شده است).

کارکرد پاسخ شامل هر دوی ابزارهای خودکار و عملکردهای دستی است. به‌طور مثال، بسیاری از IDPS های امروزی هشدارها را با توجه به برخی از معیارهای از پیش تعریف شده، دسته‌بندی می‌کنند ، اما کار کمی برای نشان دادن اینکه زمانی که یک هشدار رخ می‌دهد چه باید کرد، انجام می‌دهند. این وضعیت بیشتر پیچیده است چرا که امروز بسیاری از IDPS ها تعداد زیادی مثبت کاذب تولید می‌کنند و در بیشتر مواقع، اولین سطح پاسخ شامل کاروَرهای نسبتاً بدون تجربه است. حتی اگر یک سازمان خوش شانس باشد و کاروَرهای آگاه و با تجربه در اختیار داشته باشد، بعید است که آن‌ها در مورد اینکه چگونه به درستی به هر نوع نفوذ آشکار شده پاسخ دهند، آگاه باشند. از سوی دیگر، واکنش سریع به هشدارهای IDPS در طول دوره‌های تنش که رویدادها به سرعت در حال آشکار شدن هستند، بسیار مهم است. به این دلیل و دلایل دیگر، فراهم کردن کاروَرهایی با درک خوب دستورالعمل‌هایی که مشخص کننده‌ی طرح کلی مراحلی که باید برای انواع خاصی از هشدارهای IDPS در نظر گرفته شود، می‌باشند بسیار ضروری است. در مواردی که این دستورالعمل‌ها در دسترس نیست، پاسخ به یک هشدار IDPS ممکن است ناکافی، سازماندهی نشده ، یا دارای واکنش بیش‌ازحد باشد. اتکای کامل بر سازوکارهای پاسخ خودکار محتاطانه نیست.

در موارد غیرمعمول که در آن IDS ممکن است از طریق تطبیق الگوی بار مشابه برای یک بهره‌جویی شناخته شده، و یا از طریق امضاهای کد بایت مخرب یک روز بدون بهره‌جویی آشکار کند، کارکنان باید با فروشنده مناسب هماهنگ باشند تا از آسیب‌پذیری‌های جدید که یافت شده است و در حال حمله به شبکه ی سازمان شما می‌باشند مطلع شوند.

الف-۷-۵ دیگر ملاحظات پیاده سازی

در زیر فهرستی از ویژگی‌های دیگری وجود دارد که دارای اهمیت هستند هنگامی که پیاده سازی، عملکرد، یکپارچه سازی و انتخاب IDPS مدنظر است.

- رابط‌های کاربری،

- قرار دادن حسگرهای شبکه: حسگرهای شبکه می‌توانند به‌گونه‌ای انعطاف‌پذیر جایگذاری شوند تا از طیف وسیعی از آشکارسازی و راهبردهای پاسخ پشتیبانی نمایند. به‌طور مثال، دیوارهای آتش بیرونی برای آشکارسازی تلاش‌های حمله،

- رواداری خطای سامانه - یکپارچگی سامانه یک نگرانی مهم است. انکار خدمت یک نمونه حمله است. در صورت امکان ارتباطات میان حسگرهای IDPS، پایشگرها، و مدیران باید در یک شبکه مجزا از شبکه ی پایش شده باشد. بدین ترتیب امنیت و در دسترس بودن افزایش می‌یابد.

- اطمینان از IDPS،

- قابلیت استفاده، به‌طور مثال سهولت استفاده،

- مقیاس‌پذیری IDPS،

- قابلیت همکاری با دیگر محصولات امنیتی،

- سطح و کیفیت پشتیبانی فروشنده،

- مدیریت اجرایی- IDPS ها افزاره‌های اتصال و اجرا نیستند؛ عموماً کارکنان ماهر برای تحلیل و تفسیر خروجی‌های IDPS مورد نیاز است،

- الزامات سخت‌افزاری و نرم‌افزاری،

- مستندسازی،

- هزینه‌ها - علاوه بر هزینه‌های نرم‌افزار، سخت‌افزار، نصب و راه‌اندازی، هزینه‌های دیگری برای آموزش، عملکرد و نگهداری وجود دارد.

الف-۸ مسائل آشکارسازی نفوذ

الف-۸-۱ آشکارسازی نفوذ و حریم خصوصی

حریم خصوصی در استفاده از IDPS به یک مسئله تبدیل شده است. . شناسایی و یا منحرف کردن نفوذها نیازمند تحلیل ترافیک شبکه و یا دنباله‌های ممیزی سامانه عامل به دنبال نشانه‌های حمله و یا الگوهای ویژه که معمولاً نشان‌دهنده‌ی هدف‌های مخرب و مشکوک هستند، است.

ترافیک شبکه و یا داده‌ی جمع‌آوری‌شده‌ی رویدادها ممکن است شامل برخی اطلاعات شخصی باشند.به‌طور مثال داده‌ها ممکن است به یک فرد ویژه مرتبط باشند. سخت‌افزار یا آدرس IP ممکن است نمونه‌ای از چنین داده‌هایی باشند. بنابراین، آشکارسازی نفوذ می‌تواند به عنوان یک ابزار برای پایش کاربران و رفتار آن‌ها مورد استفاده قرار گیرد. درصورتی‌که آشکارسازی نفوذ برای تشخیص مزاحمان «داخلی»، به‌طور مثال کارکنان سازمانی به کار برده شود، باید مفاهیمی در نظر گرفته شود.

اگر آشکارسازی نفوذ به کار برده می‌شود، سه اصلی که چالش‌های حریم خصوصی را منعکس می‌کنند باید در نظر گرفته شوند:

- تشخیص نفوذ باید برای هدف حفاظت از داده‌ها و یا سامانه به خدمت گرفته شود،

- جمع‌آوری داده‌ها (بسته‌های شبکه، ثبت رویدادهای ممیزی) باید برای هدف حفاظت کافی باشند.

- الزامات پوشش خط‌مشی برای محافظت از حریم خصوصی اطلاعات کارکنان جمع‌آوری شده در IDPS باید توسعه یافته و اعمال شود.

جنبه اول بدان معنی است که نیازی نیست آشکارسازی نفوذ به عنوان ابزاری برای نظارت بر رفتار کارکنان مورد استفاده قرار گیرد.

جنبه دوم اشاره می‌کند که فقط آن دسته از داده‌هایی باید جمع‌آوری و تحلیل شوند که برای تشخیص حملات ضروری باشند. پس از مقایسه داده رویداد با نشانه حمله IDPS، داده‌هایی که دیگر مورد نیاز نیست و یا هیچ نشانه ای از یک حمله در آن وجود ندارد باید حذف شوند. داده‌های مربوطه، که یک حمله را نشان می‌دهد باید به شیوه‌ای امن ذخیره سازی گردد. اگرچه، حذف داده‌ها ممکن است در برخی موارد کافی نباشد. داده‌ی رویداد ممکن است برای بازرسی‌های بعدی آرشیو شود، به‌طور مثال، برای اهداف قابلیت ردیابی مهاجم و یا برای تحلیل قانونی در زمان‌های بعد. برخی از داده‌ها شاید در ابتدا خوش‌خیم به نظر برسند. پس از تحلیل بیشتر ممکن است اثبات شود که به یک حمله مربوط می‌شوند. ارتباط با داده‌های جمع‌آوری شده بعدی نیز ممکن است اثبات کند که به یک حمله مربوط می‌شود. در هر رویداد داده‌ها باید از دسترسی با اهداف بسیار دیگر شامل حریم خصوصی، به‌شدت محافظت شوند. اقدامات صورت گرفته باید با خط‌مشی‌های امنیتی سازمان سازگار باشد.

داده‌ها باید برای یک دوره زمانی معین و مطابق با خط‌مشی‌ها ذخیره شده، و پس‌ازآن به‌صورت ایمن برای محافظت از حریم خصوصی همه طرف‌های درگیر نابود شوند. این مقدار زمان، زمان زیادی را به قانون و مراجع قانونی برای انجام تحقیقات می‌دهد و داده‌های حساس که دیگر بر روی یک سامانه مورد نیاز نمی‌باشند و می‌توانند مورد دسترسی‌های غیرمجاز در آینده قرار بگیرند را باقی نمی‌گذارد.

نکته سوم بدین معنی است که حریم خصوصی اطلاعات کارکنان مطابق با خط‌مشی حفظ حریم خصوصی کلی سازمان و یا هر قانونی که ممکن است به اطلاعات حساس کارکنان اعمال شود، نیاز به محافظت و مدیریت دارد.

در حال حاضر تعداد بسیار کمی از الزامات خاص قانونی و نظارتی همراه با آشکارسازی نفوذ وجود دارد. انتظار می‌رود قوانین و مقرراتی پدیدار گردد برای ارائه‌ی حفاظت کافی از حریم خصوصی افراد درحالی‌که در همان زمان به IDPS و ثبت رویدادهای مرتبط با آن اجازه‌ی جمع‌آوری و استفاده کافی از داده‌ها برای شناسایی نفوذهایی که به‌طور بالقوه آسیب‌رسان داده شده است. در حال حاضر برخی مقررات ملی شامل معیارهای کفایت و هدف مرتبط با استفاده از اطلاعات شخصی می‌باشند. برخی از کشورها مقرراتی مربوط به حفاظت از داده‌های شخصی کارکنان و حق مشارکت کارکنان در حریم خصوصی اطلاعات شخصی خود دارند. علاوه بر این، مقررات مختلف ملی و معاهداتی در مورد انتقال جریان داده‌ی مرزی ممکن است بر آشکارسازی نفوذ و حریم خصوصی تأثیرگذار باشد.

برخی از قوانین و مقررات ملی مستلزم این است که اگر باید پایش فعالیت‌های مردم که در حال رخداد است صورت گیرد به عنوان مثال، از طریق ثبت داده‌های مربوط به رویداد و یا حسگرهای ویژه‌ی IDPS و یا عوامل پایش، آنگاه کارکنان و پیمانکاران مربوطه باید به‌طور ویژه مطلع شده و قبل از آغاز عملیات تصدیق نمایند. این مورد می‌تواند در قالب قرارداد امضاشده از نظر به‌کارگیری و یا یک برگه‌ی ویژه یا اطلاع رسانی الکترونیکی باشد.

الف-۸-۲ به اشتراک‌گذاری داده‌ها در نفوذ

به اشتراک‌گذاری داده‌ها در مورد نفوذها و تجربه‌های استفاده از IDPS، منافعی را برای تمام سازمان‌هایی که به‌طور جدی از IDPS استفاده می‌کنند در بر دارد. به‌طور مثال، هشدارهای زودهنگام برخی نفوذها برای برخی از سازمان‌ها از تحلیل انجام شده بر روی نفوذهای مشابهی که توسط تعدادی از سازمان‌های دیگر تجربه شده است، امکان‌پذیر خواهد بود و یا اطلاعات در مورد یک نوع نفوذ جدید، برای دیگران بسیار مفید خواهد بود. اطلاعات مربوط به تجارب استفاده از IDPS می‌تواند به سازمان‌های دیگر برای بهبود عملیات IDPS آن‌ها کمک کند.

اگرچه، مشخص شده است که نگرانی‌های قابل‌درکی در بسیاری از سازمان‌ها در مورد ایجاد دانش عمومی از نفوذهایی که سامانه‌هایIT آن‌ها و درنتیجه عملیات کسب‌وکار آن‌ها را تحت تأثیر قرار داده است وجود دارد. چنین دانش عمومی می‌تواند در حد کمینه شرم‌آور باشد و در حد بیشینه می‌تواند بر کسب‌وکار اثر داشته باشد. به‌طور مثال، سودآوری، قیمت سهم. با در نظر گرفتن این موضوع، مناسب‌ترین توصیه برای سازمان‌ها شرکت در طرح‌های مشترک است که در آن منبع اطلاعات روی نفوذها و استفاده از IDPS وجود دارد و بررسی شده است، و درنتیجه سازمان ناشناس باقی می‌ماند. چنین طرحی می‌تواند بر مبنای مجموعه‌ای از دانش ناشناخته و اطلاعات در یک دادگان طراحی شده برای خدمت به جامعه‌ی IDPS باشد. این‌چنین دادگان آشکارسازی نفوذ باید برای موارد زیر طراحی شود:

- هماهنگی اطلاعات دقیق در مورد تنظیمات آسیب‌پذیر، انواع نفوذ و دستورالعمل‌ها برای بهره‌جویی از این تنظیمات،

- رسیدگی به مقادیر زیادی از اطلاعات در مورد یک نمونه ویژه از نفوذ برای ایجاد اظهارات صحیح در مورد یک نوع نفوذ از نظر پیش‌نیازها، تأثیر، ردیابی، مشکل، راه‌حل‌ها، و غیره،

- ذخیره سازی داده‌های فنی در مورد انواع نفوذ و به اشتراک‌گذاری تمایز اصلی بین دو نوع اگر آثار قابل مشاهده‌ی آن‌ها به‌طور قابل‌توجهی با هم متفاوت باشد،

- اطمینان از اینکه اطلاعات ردیابی در قالبی ساختاردهی شده است که از بارگیری توصیف نفوذهای جدید پشتیبانی می‌کند.

- به‌روزرسانی قوانین جدید و / یا تغییر پارامترها، زمانی که انواع جدیدی از آسیب‌پذیری‌ها کشف می‌شوند،

- توانایی استخراج اطلاعات مورد نیاز برای تولید قوانین جدید به‌طور خودکار (امضا،پارامترها، و غیره) که نفوذهای جدید را شناسایی می‌کنند.

دادگان IDPS باید با سامانه‌های جدید تشخیص ویروس‌ها ، که اغلب به‌صورت خودکار کارکرد به‌روزرسانی مبتنی بر شبکه دارند، قابل مقایسه باشد.

دادگان نفوذ به معنای یک دادگان از رویدادهای نفوذ که در آن شواهد موارد حمله نگران کننده ذخیره شده است، نیست.

ملاحظات برای به اشتراک‌گذاری اطلاعات رویداد در استاندارد ISO / IEC 27010:2012 به‌طور تفضیلی وجود دارد. الگوی داده‌ها، قالب‌ها و قراردادهای تبادل امن برای تسهیل در تبادل خودکار اطلاعات نفوذها در IETF توسعه داده شده و استانداردسازی شده است. استانداردهای بین‌المللی خودکارسازی شامل RFC5070 قالب تبادل توصیف شی رویداد (IODEF)، RFC6545 دفاع زمان واقعی داخل شبکه(RID)، و RFC6546 انتقال دفاع زمان واقعی داخل شبکه است.

کتاب‌نامه

[1] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[2] ISO/IEC 18028-3:2005, Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways

[3] ISO/IEC 18028-4:2005, Information technology — Security techniques — IT network security — Part 4: Securing remote access

[4] ISO/IEC 18028-5, Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks

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

[۶] استاندارد ملی ایران شماره ۲۷۰۱۰ : سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – مدیریت امنیت اطلاعات – برای ارتباطات درون‌بخشی و درون‌سازمانی

[7] ISO/IEC 27033-1:2009, Information technology — Security techniques — Network security— Part 1: Overview and concepts

[۸] استاندارد ملی ایران شماره ۲۷۰۳۳-۲ : سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی – امنیت شبکه قسمت ۲: راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه

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

[۱۰] استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۹۴، فناوری اطلاعات – فنون امنیتی – سامانه (سیستم) مدیریت امنیت اطلاعات – الزامات

[۱۱] استاندارد ملی ایران شماره ۲۷۰۰۲ : سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات