

" امنیت شبکه لایه بندی شده "

در این بخش، رویکردی لایه بندی شده برای امن سازی شبکه به شما معرفی می گردد. این رویکرد هم یک استراتژی تکنیکی است که ابزار و امکان مناسبی را در سطوح مختلف در زیر ساختار شبکه شما قرار می دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیأت مدیره تا قسمت فروش را می طلبد. رویکرد امنیتی لایه بندی شده روی نگهداری ابزارها و سیستمهای امنیتی و روال ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می گردد.

۱- پیرامون

۲- شبکه

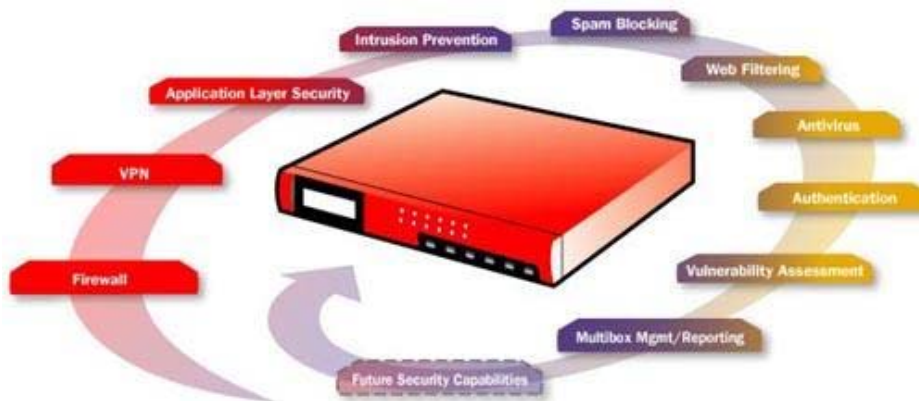
۳- میزبان

۴- برنامه کاربردی

۵- اطلاعات

در این بخش، هریک از این سطوح تعریف می شوند و یک دید کلی از ابزارها و سیستمهای امنیتی گوناگون که روی هریک عمل می کنند، ارائه می شود. هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی های دیجیتال است. مخاطبان این سلسله مقالات متخصصان فناوری اطلاعات، مدیران تجاری و تصمیم گیران سطح بالا هستند.

محافظت از اطلاعات اختصاصی به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسأله، خلق یک طرح امنیتی استراتژیکی و تاکتیکی می تواند تمرینی آسان باشد. بعلاوه، با رویکرد عملی که در اینجا معرفی می شود، می توانید بدون هزینه کردن بودجه های کلان، موانع موثری بر سر راه اخلاص گران امنیتی ایجاد کنید.



افزودن به ضریب عملکرد هکرها:

متخصصان امنیت شبکه از اصطلاحی با عنوان ضریب عملکرد (work factor) استفاده می کنند که مفهومی مهم در پیاده سازی امنیت لایه بندی است. ضریب عملکرد بعنوان میزان تلاش مورد نیاز توسط یک نفوذگر بمنظور تحت تأثیر قراردادن یک یا بیشتر از سیستمها و ابزار امنیتی تعریف می شود که باعث رخنه کردن در شبکه می شود. یک شبکه با ضریب عملکرد بالا به سختی مورد دستبرد قرار می گیرد در حالیکه یک شبکه با ضریب عملکرد پایین می تواند نسبتاً به راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه شما ضریب عملکرد بالایی دارد، که فایده رویکرد لایه بندی شده نیز هست، احتمالاً شبکه شما را رها می کنند و به سراغ شبکه هایی با امنیت پایین تر می روند و این دقیقاً همان چیزی است که شما می خواهید.

تکنولوژی های بحث شده در مجموع رویکرد عملی خوبی برای امن سازی دارایی های دیجیتالی شما را به نمایش می گذارند. در یک دنیای ایده آل، شما بودجه و منابع را برای پیاده سازی تمام ابزار و سیستم هایی که بحث می کنیم خواهید داشت. اما متأسفانه در چنین دنیایی زندگی نمی کنیم. بدین ترتیب، باید شبکه تان را ارزیابی کنید - چگونگی استفاده از آن، طبیعت داده های ذخیره شده، کسانی که نیاز به دسترسی دارند، نرخ رشد آن و غیره - و سپس ترکیبی از سیستم های امنیتی را که بالاترین سطح محافظت را ایجاد می کنند، با توجه به منابع در دسترس پیاده سازی کنید.

مدل امنیت لایه بندی شده

در این جدول مدل امنیت لایه بندی شده و بعضی از تکنولوژی هایی که در هر سطح مورد استفاده قرار می گیرند، ارائه شده اند. این تکنولوژی ها با جزئیات بیشتر در بخش های بعدی مورد بحث قرار خواهند گرفت.

ردیف	سطح امنیتی	ابزار و سیستم های امنیتی قابل استفاده
۱	پیرامون	<input checked="" type="checkbox"/> فایروال <input checked="" type="checkbox"/> آنتی ویروس در سطح شبکه <input checked="" type="checkbox"/> رمزنگاری شبکه خصوصی مجازی
۲	شبکه	<input checked="" type="checkbox"/> سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) <input checked="" type="checkbox"/> سیستم مدیریت آسیب پذیری <input checked="" type="checkbox"/> تبعیت امنیتی کاربر انتهایی <input checked="" type="checkbox"/> کنترل دسترسی / تایید هویت کاربر
۳	میزبان	<input checked="" type="checkbox"/> سیستم تشخیص نفوذ میزبان <input checked="" type="checkbox"/> سیستم ارزیابی آسیب پذیری میزبان <input checked="" type="checkbox"/> تبعیت امنیتی کاربر انتهایی <input checked="" type="checkbox"/> آنتی ویروس <input checked="" type="checkbox"/> کنترل دسترسی / تایید هویت کاربر
۴	برنامه کاربردی	<input checked="" type="checkbox"/> سیستم تشخیص نفوذ میزبان <input checked="" type="checkbox"/> سیستم ارزیابی آسیب پذیری میزبان <input checked="" type="checkbox"/> کنترل دسترسی / تایید هویت کاربر <input checked="" type="checkbox"/> تعیین صحت ورودی
۵	داده	<input checked="" type="checkbox"/> رمزنگاری <input checked="" type="checkbox"/> کنترل دسترسی / تایید هویت کاربر

سطح ۱: امنیت پیرامون

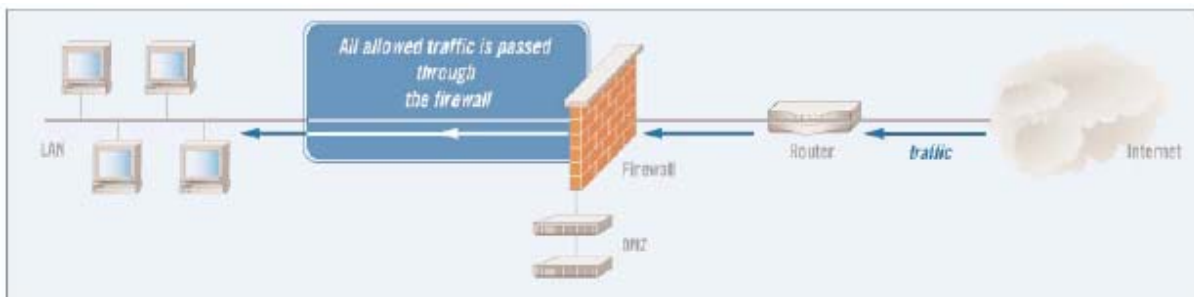
منظور از پیرامون، اولین خط دفاعی نسبت به بیرون و به عبارتی به شبکه غیرقابل اعتماد است. «پیرامون» اولین و آخرین نقطه تماس برای دفاع امنیتی محافظت کننده شبکه است. این ناحیه ای است که شبکه به پایان می رسد و اینترنت آغاز می شود. پیرامون شامل یک یا چند فایروال و مجموعه ای از سرورهای به شدت کنترل شده است که در بخشی از پیرامون قرار دارند که بعنوان DMZ (zone demilitarized) شناخته می شود. معمولاً وب سرور ها، مدخل ایمیل ها، آنتی ویروس شبکه و سرورهای DNS را در بر می گیرد که باید در معرض اینترنت قرار گیرند. فایروال قوانین سفت و سختی در مورد اینکه چه چیزی می تواند وارد شبکه شود و چگونه سرور ها در DMZ می توانند با اینترنت و شبکه داخلی تعامل داشته باشند، دارد.

پیرامون شبکه، به اختصار، دروازه شما به دنیای بیرون و برعکس، مدخل دنیای بیرون به شبکه شماست. تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

☑ فایروال : معمولاً یک فایروال روی سروری نصب می‌گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می‌دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳- نقطه پایانی VPN. فایروال کنترل ترافیک را با سنجیدن مبدا و مقصد تمام ترافیک وارد شونده و خارج شونده انجام می‌دهد و تضمین می‌کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال‌ها به شبکه امن در تبدیل آدرس‌های IP داخلی به آدرس‌های قابل رویت در اینترنت کمک می‌کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می‌کند. یک فایروال همچنین می‌تواند به عنوان نقطه پایانی تونل‌های VPN (که بعداً بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می‌کند.

☑ آنتی ویروس شبکه : این نرم افزار در DMZ نصب می‌شود و محتوای ایمیل‌های وارد شونده و خارج شونده را با پایگاه داده‌ای از مشخصات ویروس‌های شناخته شده مقایسه می‌کند. این آنتی ویروس‌ها آمد و شد ایمیل‌های آلوده را مسدود می‌کنند و آنها را قرنطینه می‌کنند و سپس به دریافت‌کنندگان و مدیران شبکه اطلاع می‌دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می‌کند و جلوی گسترش ویروس توسط شبکه شما را می‌گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضد ویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می‌گیرد. بمنظور کارکرد مؤثر، Database ویروس‌های شناخته شده باید به روز نگه داشته شود.

☑ VPN- یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ‌تاپ‌ها و شبکه مقصد استفاده می‌کند. VPN اساساً یک تونل رمز شده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می‌کند. این تونل VPN می‌تواند در یک مسیر یاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش‌های دور و بی‌سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده‌سازی می‌شود.



مزایا:

تکنولوژی های ایجاد شده سطح پیرامون سالها است که در دسترس هستند، و بیشتر خبرگان IT با توانایی ها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجه اقتصادی هستند. بعضی از فروشندگان راه حل های سفت و سختی برای این تکنولوژیها ارائه می دهند و بیشتر آنها به این دلیل پر هزینه هستند.

معایب:

از آنجا که بیشتر این سیستم ها تقریباً پایه ای هستند و مدتها است که در دسترس بوده اند، بیشتر هکرهای پیشرفته روش هایی برای دور زدن آنها نشان داده اند. برای مثال، یک ابزار آنتی ویروس نمی تواند ویروسی را شناسایی کند مگر اینکه از قبل علامت شناسایی ویروس را در Database خود داشته باشد و این ویروس داخل یک فایل رمز شده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را بر روی کارمندان IT تحمیل می کند، چرا که کلیدهای رمزنگاری و گروه های کاربری باید بصورت مداوم مدیریت شوند.

ملاحظات:

پیچیدگی معماری شبکه شما می تواند تأثیر قابل ملاحظه ای روی میزان اثر این تکنولوژی ها داشته باشد. برای مثال، ارتباطات چندتایی به خارج احتمالاً نیاز به چند فایروال و آنتی ویروس خواهد داشت. معماری شبکه بطوری که تمام این ارتباطات به ناحیه مشترکی ختم شود، به هر کدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

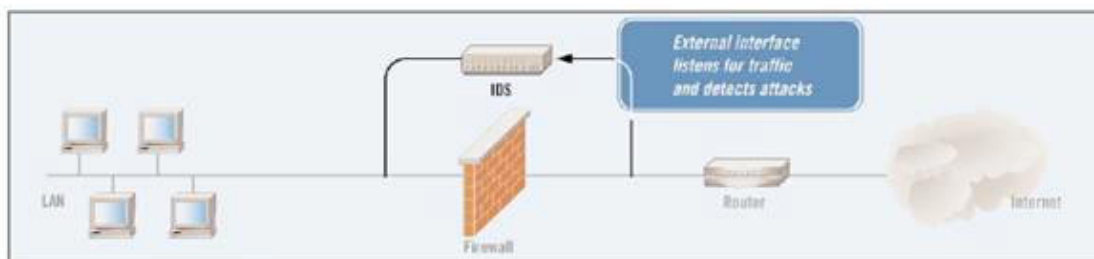
انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

سطح ۲- امنیت شبکه

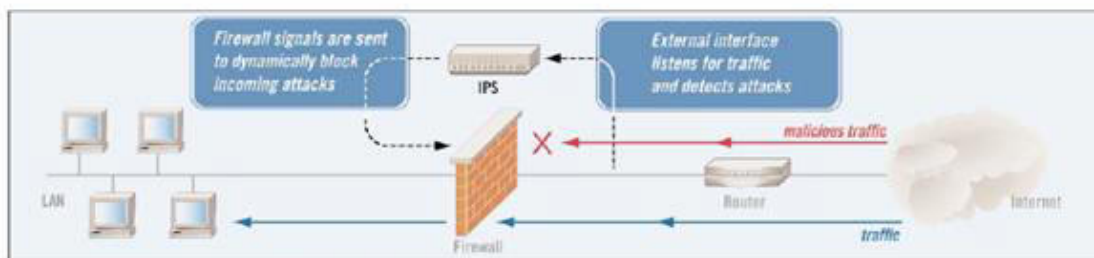
سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی در میان شبکه حرکت کنید. این قضیه بخصوص برای سازمان های کوچک تا متوسط صدق می کند که به این ترتیب این شبکه ها برای هکرها و افراد بداندیش دیگر به اهدافی وسوسه انگیز مبدل می شوند. تکنولوژی های ذیل امنیت را در سطح شبکه برقرار می کنند:

☑️ **IDS**ها (سیستم های تشخیص نفوذ) و **IPS**ها (سیستم های جلوگیری از نفوذ) :

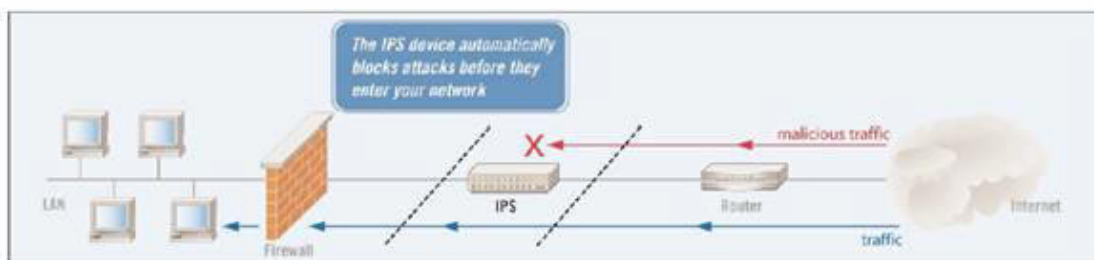
تکنولوژیهای **IDS** و **IPS** ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می‌کنند. مشابه سیستم های آنتی ویروس، ابزارهای **IDS** و **IPS** ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده‌ای از مشخصات حملات شناخته شده مقایسه می‌کنند. هنگامی که حملات تشخیص داده می‌شوند، این ابزار وارد عمل می‌شوند. ابزارهای **IDS** مسؤولین **IT** را از وقوع یک حمله مطلع می‌سازند؛ ابزارهای **IPS** یک گام جلوتر می‌روند و بصورت خودکار ترافیک آسیب رسان را مسدود می‌کنند. **IDS**ها و **IPS**ها مشخصات مشترک زیادی دارند. درحقیقت، بیشتر **IPS**ها در هسته خود یک **IDS** دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می‌شود. محصولات **IDS** تنها ترافیک آسیب رسان را تشخیص می‌دهند، در حالیکه محصولات **IPS** از ورود چنین ترافیکی به شبکه شما جلوگیری می‌کنند. پیکربندی های **IPS** و **IDS** استاندارد در شکل نشان داده شده‌اند:



Intrusion detection system (IDS)



Intrusion prevention system (out-of-band configuration)



Intrusion prevention system (in-line configuration)

مدیریت آسیب پذیری : سیستم های مدیریت آسیب پذیری دو عملکرد مرتبط را انجام می‌دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می‌کنند و (۲) روند مرمت آسیب پذیری یافته شده را مدیریت می‌کنند. در گذشته، این تکنولوژی **VA** (تخمین آسیب پذیری) نامیده می‌شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می‌دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری‌هایی که می‌توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می‌کنند. آنها معمولاً پایگاه

داده‌ای از قوانینی را نگهداری می‌کنند که آسیب پذیری های شناخته شده برای گستره ای از ابزارها و برنامه‌های شبکه را مشخص می‌کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می‌آزماید.

همچنانکه از نامش بر می آید، سیستم مدیریت آسیب پذیری شامل ویژگی‌هایی است که روند بازسازی را مدیریت می‌کند. لازم به ذکر است که میزان و توانایی این ویژگی ها در میان محصولات مختلف، فرق می‌کند.

☑ **تابعیت امنیتی کاربر انتهایی:** روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می‌کنند که تضمین می‌کنند کاربران انتهایی استانداردهای امنیتی تعریف شده را قبل از اینکه اجازه دسترسی به شبکه داشته باشند، رعایت کرده اند. این عمل جلوی حمله به شبکه از داخل خود شبکه را از طریق سیستم‌های ناامن کارمندان و ابزارهای VPN و RAS می‌گیرد.

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می‌دهند، اجازه دسترسی می‌دهند. هدف آنها از این تست ها معمولاً برای بررسی (۱) نرم افزار مورد نیاز، مانند سرویس پک ها، آنتی ویروس های به روز شده و غیره و (۲) کاربردهای ممنوع مانند اشتراک فایل و نرم افزارهای جاسوسی است.

☑ کنترل دسترسی/تأیید هویت:

کنترل دسترسی نیازمند تأیید هویت کاربرانی است که به شبکه شما دسترسی دارند. هم کاربران و هم ابزارها باید با ابزار کنترل دسترسی در سطح شبکه کنترل شوند.

نکته: در این سلسله مباحث، به کنترل دسترسی و تأیید هویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می‌پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می‌افتد. اما به خاطر داشته باشید که کنترل دسترسی و تأیید هویت مراحل پیچیده ای هستند که برای ایجاد بیشترین میزان امنیت در شبکه، باید به دقت مدیریت شوند.

مزایا:

تکنولوژی های IDS، IPS و مدیریت آسیب پذیری تحلیل های پیچیده ای روی تهدیدها و آسیب پذیری های شبکه انجام می‌دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می‌دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می‌کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می‌توانند از فایروال عبور کنند، مشخص خواهند شد و قبل از آسیب رسانی به آنها خاتمه داده خواهند شد.

سیستم های مدیریت آسیب پذیری روند بررسی آسیب پذیری های شبکه شما را بصورت خودکار استخراج می کنند. انجام چنین بررسی هایی به صورت دستی با تناوب مورد نیاز برای تضمین امنیت، تا حدود زیادی غیر عملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاء دادن نرم افزارها و وصله ها، و افزودن و کاستن از کاربران، همگی می توانند آسیب پذیری های جدید را پدید آورند. ابزار تخمین آسیب پذیری به شما اجازه می دهند که شبکه را مرتب و کامل برای جستجوی آسیب پذیری های جدید پیمایش کنید.

روش های تابعیت امنیتی کاربر انتهایی به سازمان ها سطح بالایی از کنترل بر روی ابزاری را می دهد که به صورت سنتی کنترل کمی بر روی آنها وجود داشته است. هکرها بصورت روز افزون به دنبال بهره برداری از نقاط انتهایی برای داخل شدن به شبکه هستند، هم چنانکه پدیده های اخیر چون **Sasser**، **Sobig**، **Mydoom** و **Sasser** گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

معیاب:

IDSها تمایل به تولید تعداد زیادی علائم هشدار غلط دارند، که به عنوان **False Positives** نیز شناخته می شوند. در حالیکه **IDS** ممکن است که یک حمله را کشف و به اطلاع شما برساند، این اطلاعات می تواند زیر انبوهی از هشدارهای غلط یا اطلاعات کم ارزش مدفون شود. مدیران **IDS** ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیر گذاری بالا، یک **IDS** باید بصورت پیوسته بررسی شود و برای الگوهای مورد استفاده و آسیب پذیری های کشف شده در محیط شما تنظیم گردد. چنین نگهداری معمولاً میزان بالایی از منابع اجرایی را مصرف می کند.

سطح خودکار بودن در **IPS** ها می تواند به میزان زیادی در میان محصولات، متفاوت باشد. بسیاری از آنها باید با دقت پیکربندی و مدیریت شوند تا مشخصات الگوهای ترافیک شبکه ای را که در آن نصب شده اند منعکس کنند. تأثیرات جانبی احتمالی در سیستم هایی که بهینه نشده اند، مسدود کردن تقاضای کاربران قانونی و قفل کردن منابع شبکه معتبر را شامل می شود.

بسیاری، اما نه همه روش های امنیتی کاربران انتهایی، نیاز به نصب یک عامل در هر نقطه انتهایی دارد. این عمل می تواند مقدار قابل توجهی بار کاری اجرایی به نصب و نگهداری اضافه کند.

تکنولوژی های کنترل دسترسی ممکن است محدودیت های فنی داشته باشند. برای مثال، بعضی ممکن است با تمام ابزار موجود در شبکه شما کار نکنند، بنابراین ممکن است به چند سیستم برای ایجاد پوشش نیاز داشته باشید. همچنین، چندین فروشنده سیستم های کنترل دسترسی را به بازار عرضه می کنند، و عملکرد می تواند بین محصولات مختلف متفاوت باشد. پیاده سازی یک سیستم یکپارچه در یک شبکه ممکن است دشوار باشد. چنین عمل وصله-پینه ای یعنی رویکرد چند محصولی ممکن است در واقع آسیب پذیری های بیشتری را در شبکه شما به وجود آورد.

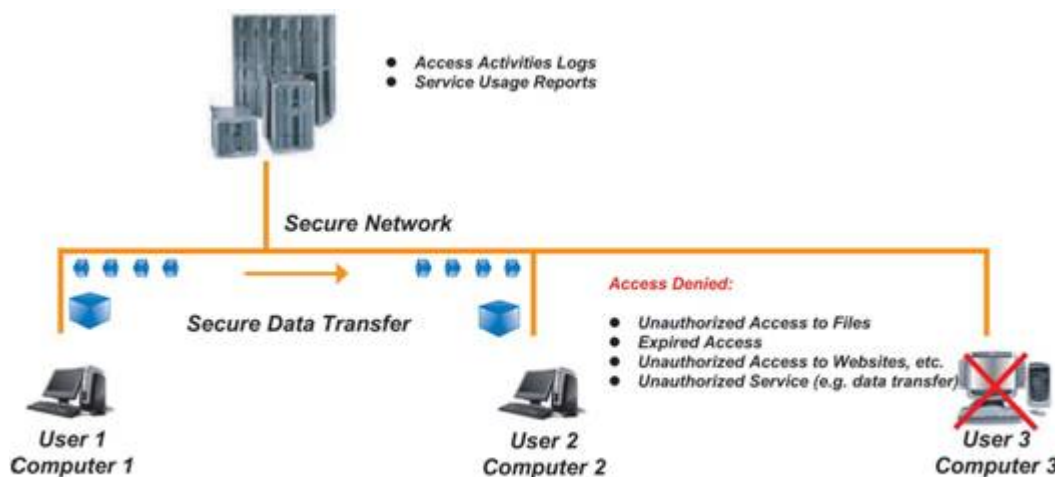
ملاحظات:

موفقیت ابزارهای امنیت سطح شبکه به نحوی به سرعت اتصالات داخلی شبکه شما وابسته است. زیرا ابزارهای IDS/IPS، مدیریت آسیب پذیری و امنیت کاربر انتهایی ممکن است منابعی از شبکه ای را که از آن محافظت می کنند، مصرف کنند. سرعت های اتصال بالاتر تأثیری را که این ابزارها بر کارایی شبکه دارند به حداقل خواهد رساند. در پیاده سازی این تکنولوژی ها شما باید به مصالحه بین امنیت بهبود یافته و سهولت استفاده توجه کنید، زیرا بسیاری از این محصولات برای کارکرد مؤثر باید به طور پیوسته مدیریت شوند و این ممکن است استفاده از آن محصولات را در کل شبکه با زحمت مواجه سازد.

وقتی که این تکنولوژی ها را در اختیار دارید، بهبود پیوسته شبکه را در خاطر داشته باشید. در شبکه هایی با پویایی و سرعت گسترش بالا، تطبیق با شرایط و ابزار جدید ممکن است مسأله ساز گردد.

سطح ۳- امنیت میزبان :

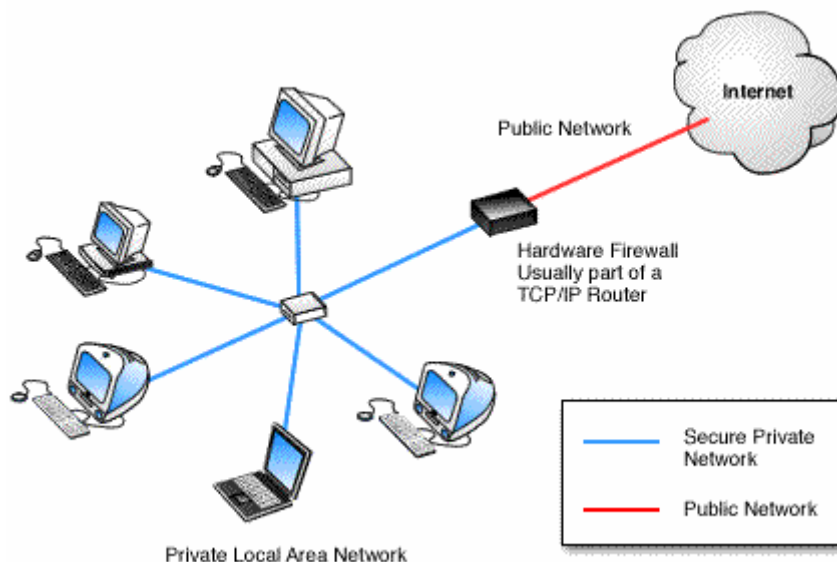
سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، Switch ها، Routerها و غیره در شبکه است. هر ابزار تعدادی پارامتر قابل تنظیم دارد و هنگامی که به نادرستی تنظیم شوند، می توانند سوراخ های امنیتی نفوذپذیری ایجاد کنند. این پارامترها شامل تنظیمات Registry، سرویس ها، توابع عملیاتی روی خود ابزار یا وصله های سیستم های عامل یا نرم افزارهای مهم می شود.



تکنولوژی های زیر امنیت را در سطح میزبان فراهم می کنند:

☑ IDS در سطح میزبان: IDS های سطح میزبان عملیاتی مشابه IDS های شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDS های سطح میزبان برای مشخصات عملیاتی بخصوصی از ابزار میزبان تنظیم می گردند و بنابراین اگر به درستی مدیریت شوند، درجه بالایی از مراقبت را فراهم می کنند.

- VA (تخمین آسیب پذیری) سطح میزبان:** ابزارهای VA سطح میزبان یک ابزار شبکه مجزا را برای آسیب پذیری های امنیتی پوشش می کنند. دقت آنها نسبتا بالاست و کمترین نیاز را به منابع میزبان دارند. از آنجایی که VA ها بطور مشخص برای ابزار میزبان پیکربندی می شوند، در صورت مدیریت مناسب، سطح بسیار بالایی از پوشش را فراهم می کنند.
- تابعیت امنیتی کاربر انتهایی:** روش های تابعیت امنیتی کاربر انتهایی وظیفه دوچندانی ایفا می کنند و هم شبکه (همانگونه در بخش قبلی مطرح شد) و هم میزبان های جداگانه را محافظت می کنند. این روش ها بطور پیوسته میزبان را برای عملیات زیان رسان و آلودگی ها بررسی می کنند و همچنین به نصب و به روز بودن فایروال ها و آنتی ویروس ها رسیدگی می کنند.
- آنتی ویروس :** هنگامی که آنتی ویروس های مشخص شده برای ابزار در کنار آنتی ویروس های شبکه استفاده می شوند ، لایه اضافه ای برای محافظت فراهم می کنند.
- کنترل دسترسی / تصدیق هویت:** ابزار کنترل دسترسی در سطح ابزار یک روش مناسب است که تضمین می کند دسترسی به ابزار تنها توسط کاربران مجاز صورت پذیرد. در اینجا نیز، احتمال سطح بالایی از تراکنش بین ابزار کنترل دسترسی شبکه و کنترل دسترسی میزبان وجود دارد.



مزایا:

این تکنولوژی های در سطح میزبان حفاظت بالایی ایجاد می کنند زیرا برای برآورده کردن مشخصات عملیاتی مخصوص یک ابزار پیکربندی می گردند. دقت و پاسخ دهی آنها به محیط میزبان به مدیران اجازه می دهد که به سرعت مشخص کنند کدام تنظیمات ابزار نیاز به به روز رسانی برای تضمین عملیات امن دارند.

معایب:

بکارگیری و مدیریت سیستم های سطح میزبان می تواند بسیار زمان بر باشند. از آنجایی که این سیستم ها نیاز به نمایش و به روز رسانی مداوم دارند، اغلب ساعات زیادی برای مدیریت مناسب می طلبند. اغلب نصبشان مشکل است و تلاش قابل ملاحظه ای برای تنظیم آنها مورد نیاز است. همچنین، هرچه سیستم عامل بیشتری در شبکه داشته باشید، یک رویکرد برپایه میزبان، گران تر خواهد بود و مدیریت این ابزار مشکل تر خواهد شد. همچنین، با تعداد زیادی ابزار امنیتی سطح میزبان در یک شبکه، تعداد هشدارها و علائم اشتباه می تواند بسیار زیاد باشد.

ملاحظات:

بدلیل هزینه ها و بار اضافی مدیریت، ابزار در سطح میزبان باید بدقت بکار گرفته شوند. بعنوان یک اصل راهنما، بیشتر سازمان ها این ابزار را فقط روی سیستم های بسیار حساس شبکه نصب می کنند. استثناء این اصل یک راه حل تابعیت امنیتی کاربر انتهایی است، که اغلب برای پوشش دادن به هر ایستگاه کاری که تلاش می کند به شبکه دسترسی پیدا کند، بکار گرفته می شود.

سطح ۴ - امنیت برنامه کاربردی

در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خود کرده است. برنامه هایی که به میزان کافی محافظت نشده اند، می توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه نویسان هنگام تولید کد به امنیت توجه ندارند. این یک مشکل تاریخی در بسیاری از برنامه های با تولید انبوه است. ممکن است شما از کمبود امنیت در نرم افزارها آگاه شوید، اما قدرت تصحیح آنها را نداشته باشید.

برنامه ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل های دیگر، روی وب قرار داده می شوند. این برنامه ها، همچون بخش فروش، مدیریت ارتباط با مشتری، یا سیستم های مالی، می توانند هدف خوبی برای افرادی که نیت بد دارند، باشند. بنابراین بسیار مهم است که یک استراتژی امنیتی جامع برای هر برنامه تحت شبکه اعمال شود.

تکنولوژی های زیر امنیت را در سطح برنامه فراهم می کنند:

- پوشش محافظ برنامه: از پوشش محافظ برنامه به کرات به عنوان فایروال سطح برنامه یاد می شود و تضمین می کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای ایمیل، سرورهای پایگاه داده و ماشین های مشابه نصب می شود، برای کاربر شفاف است و با درجه بالایی با سیستم یکپارچه می شود.
- یک پوشش محافظ برنامه برای عملکرد مورد انتظار سیستم میزبان تنظیم می گردد. برای مثال، یک پوشش روی سرور ایمیل به این منظور بیکربندی می شود تا جلوی اجرای خودکار برنامه ها توسط ایمیل های وارد شونده را بگیرد، زیرا این کار برای ایمیل معمول یا لازم نیست.

- کنترل دسترسی/تصدیق هویت: مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می توانند به برنامه دسترسی داشته باشند.
- تعیین صحت ورودی: ابزارهای تعیین صحت ورودی بررسی می کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورد استفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربر می تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود مگر اینکه خلافش ثابت شود!
- به عنوان مثال، یک فرم وبی با یک بخش **zip code** را در نظر بگیرید. تنها ورودی قابل پذیرش در این قسمت فقط پنج کاراکتر عددی است. تمام ورودی های دیگر باید مردود شوند و یک پیام خطا تولید شود. تعیین صحت ورودی باید در چندین سطح صورت گیرد. در این مثال، یک اسکریپت جاوا می تواند تعیین صحت را در سطح مرورگر در سیستم سرویس گیرنده انجام دهد، در حالیکه کنترل های بیشتر می تواند در سرور وب قرار گیرد. اصول بیشتر شامل موارد زیر می شوند:
 - کلید واژه ها را فیلتر کنید. بیشتر عبارات مربوط به فرمانها مانند «insert»، باید بررسی و در صورت نیاز مسدود شوند.
 - فقط دیتایی را بپذیرید که برای فلید معین انتظار می رود. برای مثال، یک اسم کوچک ۷۵ حرفی یک ورودی استاندارد نیست.

مزایا

ابزارهای امنیت سطح برنامه موقعیت امنیتی کلی را تقویت می کنند و به شما اجازه کنترل بهتری روی برنامه هایتان را می دهند. همچنین سطح بالاتری از جوابگویی را فراهم می کنند چرا که بسیاری از فعالیت های نمایش داده شده توسط این ابزارها، ثبت شده و قابل ردیابی هستند.

معایب:

پیاده سازی جامع امنیت سطح برنامه می تواند هزینه بر باشد، چرا که هر برنامه و میزبان آن باید بصورت مجزا ارزیابی، پیکربندی و مدیریت شود. بعلاوه، بالابردن امنیت یک شبکه با امنیت سطح برنامه می تواند عملی ترسناک! و غیرعملی باشد. هرچه زودتر بتوانید سیاست هایی برای استفاده از این ابزارها پیاده کنید، روند مذکور موثرتر و ارزان تر خواهد بود.

ملاحظات

ملاحظات کلیدی برنامه ها و طرح های شما را برای بلندمدت اولویت بندی می کنند. امنیت را روی برنامه ها کاربردی خود در جایی پیاده کنید که بیشترین منفعت مالی را برای شما دارد. طرح ریزی بلندمدت به شما اجازه می دهد که ابزارهای امنیتی را با روشی تحت کنترل در طی رشد شبکه تان پیاده سازی کنید و از هزینه های اضافی جلوگیری می کند.

سطح ۵ - امنیت دیتا

امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را در بر می‌گیرد. رمزنگاری دیتا، هنگامی که ذخیره می‌شود و یا در شبکه شما حرکت می‌کند، به عنوان روشی بسیار مناسب توصیه می‌گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می‌کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می‌گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می‌توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می‌دهد که سیاست های دسترسی و ابزار امنیتی مناسبی را که باید بکار گرفته شوند، مشخص کنید.

تکنولوژی های زیر امنیت در سطح دیتا را فراهم می‌کنند:

- رمزنگاری: طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می‌شوند. تقریباً تمام طرح ها شامل کلیدهای رمزنگاری/رمزگشایی هستند که تمام افرادی که به دیتا دسترسی دارند، باید داشته باشند. استراتژی های رمزنگاری معمول شامل RSA و PGP هستند.
- کنترل دسترسی / تصدیق هویت: مانند تصدیق هویت سطوح شبکه، میزبان و برنامه، تنها کاربران مجاز دسترسی به دیتا خواهند داشت.



مزایا

رمزنگاری روش اثبات شده ای برای محافظت از دیتای شما فراهم می‌کند. چنانچه نفوذگران تمام ابزارهای امنیتی دیگر در شبکه شما را خنثی کنند، رمزنگاری یک مانع نهایی و موثر برای محافظت از اطلاعات خصوصی و دارایی دیجیتال شما فراهم می‌کند.

معایب

بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می‌تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می‌تواند تبدیل به یک بار اجرایی در سازمان‌های بزرگ یا در حال رشد گردد.

ملاحظات

رمزنگاری تا عمق مشخص باید به دقت مدیریت شود. کلیدهای رمزنگاری باید برای تمام ابزارها و برنامه‌های تحت تأثیر تنظیم و هماهنگ شوند. به همین دلیل، یک بار مدیریتی برای یک برنامه رمزنگاری موثر مورد نیاز است.