معرفی سازمان

شرکت فرودگاههای کشور به موجب مصوبه شورایعالی اداری در تاریخ ۱۳۷۰/۱۲/۲۵ و به منظور نیل به اهداف و تکالیف مندرج در قانون توسعه کشور و در راستای رونق بخش حمل و نقل هوایی و تحول ساختاری در زمینه تفکیک تصدی از حاکمیت رسما آغاز به کار نمود . این شرکت همانگونه که از ماده ۱ اساسنامه و اصلاحیه آن مستفاد می گردد با هدف بازرگانی نمودن سیستم عملیات اجرایی و بخش تصدی فعالیتها و وظایف سازمان هواپیمایی کشوری شکل گرفت . دستیابی به این اهداف و اخذ مجوزهای لازم از دستگاههای ذیربط دولتی ومجلس شورای اسلامی در سالهای گذشته همواره اهداف استراتژیک این شرکت را تحت تاثیر قرار داده و برنامه ریزی برای دستیابی به فرایندهای لازم جهت برطرف نمودن این چالشها، روند فعالیتهای شرکت را همواره تحت تاثیر قرار داده است .

سازمان هواپیمایی کشوری

سازمان هواپیمایی کشوری ابزار حاکمیت دولت در بخش مهم و حساس صنعت حمل و نقل هوایی است که بر مجموعه فعالیتهای هوانوردی و فرودگاهی و حمل و نقل نظرات عالیه اعمال مینماید. هدف اساسی این سازمان تامین ایمنی و سلامتی پروازها در فضای هوائی کشور می باشد. در سطح بین المللی کشور به عضویت سازمان بین المللی هواپیمائی کشور (ایکائو) در آمده و سازمان هواپیمائی کشوری به عنوان نماینده رسمی جمهوری اسلامی ایران در سازمان ایکائو می باشد.

سازمان هواپیمائی کشوری به منظور تقویت حوزه مرکزی در جهت اعمال حاکمیت دولت در صنعت حمل و نقل هوائی و انتزاع وظایف تصدی از سازمان با ایجاد شرکت فرودگاههای کشور کلیه وظایف مربوط به اداره، نگهداری، توسعه، تجهیز و بهره برداری از فرودگاههای کشور را به آن شرکت انتقال داد. اکنون عمده وظایف آن در زمینه سیاست گذاری، برنامه ریزی و تعیین خط مشی ها میباشد.

خلاصه ای از فعالیتها:

۱. تدوین سیاستها و مقرارت ملی هوانوردی

سازمان به منظور کنترل فضای کشور و تامین ایمنی پرواز هواپیماهای داخلی و خارجی و برقراری ارتباط هوایی درون و برون مرزی و با در نظر گرفتن استاندارد ها و رویه های توصیه شده بین المللی ایکائو، مقررات و استاندارد های ملی هوانوردی در زمینه فعالیت های هوانوردی از جمله مراقبت پرواز، ارتباطات هوانوردی، ایمنی زمینی، تامین و نصب سیستم های ارتباطی، ناوبری، راداری، روشنایی باند، فعالیتهای امنیتی، ساخت فرودگاهها، تسهیلات فرودگاهی، ساخت و منتاژ و تعمیر و نگهداری و خرید و اجاره انواع هواپیماها، تنظیم شبکه پروازی داخلی و بین المللی را تدوین و یا مورد بازنگری قرار داده است.

با توجه به وظیفه سازمان ایکائو مبنی بر تصویب استانداردهای بین المللی، سازمان از طریق شرکت در اجلاس ها و کمیته های تخصصی هوانوردی آن سازمان بین المللی و ارایه نظریات مختلف در مورد پیش نویس استاندارد های بین المللی نقش بسزایی را در روند تصویب این استانداردها ایفا می نماید.

سازمان همچنین در اجلاس ها و کمیته های طرحهای هوانوردی منطقه خاورمیانه به عنوان یکی از اعضای موثر در منطقه شرکت نموده تا بتواند طرحهای هماهنگ هوانوردی منطقه در زمینه مسیرهای هوایی و تجهیزات هوانوردی و عبور و مرور هواپیماها و برقراری ارتباطات هوانوردی را به تصویب برسان د.

فعالیت تجاری پروازهای بین المللی میان دو کشور نیاز به انعقاد موافقت نامه های دو جانبه میان جمهوری اسلامی ایران و سایر کشور ها دارد که سازمان در اجرای این وظیفه پس از مذاکره با کشور های مختلف تا کنون حدود ۷۰ موافقت نامه دو جانبه حمل و نقل هوایی را منعقد نموده است.

سازمان در مورد صدور گواهینماه های لازم برای ثبت هواپیما، صلاحیت خدمه پروازی، قابلیت پرواز هواپیما ها، کارگاههای تعمیراتی هواپیما، طراحی و ساخت هواپیما اقدام نموده و

همچنین به منظور ارائه خدمات حمل و نقل هوائی ایمن جهت تامین نیازمندیهای مسافر و بار مجوز های لازم را برای ایجاد شرکت های حمل و نقل هوائی داخلی، فعالیت شرکتهای حمل و نقل هوائس خارجی در ایران، باشگاههای هوانوردی، مرکز آموزش هوانوردی، شرکتهای فرودگاهی و دفاتر خدمات مسافرت هوائی و شرکتهای خدمات کارگزاری هوائی صادر کرده است که گام موثری را در زمینه خصوصی سازی فعالیتها برداشته است.

علاوه بر این بر وضعیت جسمانی خلبانان و کنترلرها نظارت نموده و با آماده سازی دومین هواپیمای فلایت چک با برنامه های منظم دستگاههای ناوبری را کنترل کرده است.

۲. خدمات هوانوردی

جریان عبور و مرور نشست و برخاست هواپیما از جهت تامین ایمنی پرواز و حسن تدبیر امور تخت سه وظیفه مهم ارتباطات و ناوبری و نظارت طبقه بندی شده که اساس خدمات و پشتیبانی کننده واحد مدیریت عبور و مرور هوائی را تشکیل میدهند.

مدیریت عبور و مرور هوائی با ایجاد حدود ۱۵۰۰۰۰ نوتیکال مایل مسیرهای هوایی داخل و بین المللی در چهارچوب حدود ۶۷ معبر (کریدور) هوائی و از طریق ایجاد مرکز کنترل فضای کشور و ایجاد حدود ۱۶ پایانه هوایی در محدوده فضای فرودگاههای کشور و امکانات برج کنتل در حدود ۴۴ فرودگاه عبور و مرور و نشست و برخاست هواپیما ها را به منظور اجتناب از برخورد با یکدیگر یا با شایر موانع انجام می دهند.

به منظور کنترل هوا پیما ها در فضای کشور تجهیزات و سیستم های ارتباطی و ناوبری و نظارتی مختلفی تدارک و در ایستگاههای هوانوردی نصب گردیده که عبارت از ۵ رادار و بیش از ۱۸ سیستم کنترل از راه دور زمین به هوا، بیش از ۱۰ سیستم فرود با دستگاه و بیش از ۳۰ دستگاه ارائه دهنده سمت و زاویه و بیش از ۴۰ دستگاه راهنمای جهت یابی و بیش از ۳۰ دستگاه فاصله یاب می باشند.خرید تجهیزات جهت ایجاد مرکز کنترل جدید به منظور ارائه خدمات هوانوردی در منطقه اطلاعات پرواز و سیستم های رادار ثانویه جهت نصب در

ایستگاههای هوانوردیو برقراری سیستم نظارت اتوماتیک وابسته / ارتباطات حلقه ای داده ها میان خلبانان و کنترلر و جایگزینی سیستم های ارتباطی ماهواره ای انجام شده و در آینده نزدیک به طور کامل در مدار قرار گرفت.

تهیه طرحهای تقریب ورودی و خروجی، بر روی مناطق خطر، محدوده و احتیاطی و مبادله حدود ۱۰ میلیون فقره پیامهای هواپیمائی از جمله فعالیتهای دیگر برای ارائه خدمات هوانوردی است.

در هر سال به حدود بیش از ۴۰۰ هزار پرواز تجاری داخلی و خارجی و غیره تجاری و عبوری بر فراز فضای هوائی کشور خدمات هوانوردی ارائه می شود که با افزایش تجهیزات و بهبود آموزش نیروی انسانی متخصص می توان ظرفیت ارائه خدمات را در مقیاس وسیعی با ایمنی بیشتر افزایش داد.

۳. خدمات فرودگاهی

با اتمام احداث فرودگاههای در حال ساخت، تعداد ۷۸ فرودگاه تجاری مورد بهره برداری قرار خواهد گرفت و در حال حاضر بهره برداری از ۶۴ فرودگاه به عهده شرکت فرودگاههای کشور و تعداد ۱۵ فرودگاه تحت مدیریت سایر ارگانها میباشد.

فرودگاهها در حال بهره برداری جهت ارائه خدمات مورد نیاز استفاده کنندگان از آنها دارای اکانات متعدد در بخش هوائی و زمینی و راهای دسترسی و تسهیلات فرودگاهی می باشند که نگهداری و توسعه آنها به عهده مدیریت فرودگاه است و همچنین هماهنگی میان نهاد های مستقر در فرودگاه از جمله وظایف عمده می باشد.

به لحاظ پذیرش نوع هواپیما ۱۱ فرودگاه در حال بهره برداری قابل پذیرش هواپیمای پهن پیکر و ۳۰ فرودگاه قابل پذیرش هواپیمای بدنه متوسط و ۵۸ فرودگاه قابل پذیرش هواپیمای بدنه باریک می باشند. از فرودگاههای موجود تعداد ۵ فرودگاه به صورت بین المللی هستند که امکان جابجایی مسافر و بار به نقاط خارج از کشور در آنها وجود دارد. در هر سال حدود ۲۰

میلیون مسافر داخلی و بین المللی و ۱۰۰ هزار تن از طریق پایانه های فرودگاهی برای انجام سفر هوائی استفاده می نمایید که فرودگاه امکانات لازم را فراهم می آورد.

از سرمایه گذاری بخش خصوصی در فرودگاههای کشور استقبال گردیده و تا کنون طرحهای متعددی از جمله پارکینگ و توسعه ترمینال مسافری به اجرا در آمده که مهمترین آنها راه اندازی هتل ترانزیت فرودگاه مهر آباد به منظور بهره گیری توریست ها و شخصیت های تجاری میباشد. البته در نظر است تا بتوانیم اداره و بهره برداری برخی از فرودگاهها را نیز به بخش خصوصی واگذار نماییم تا بخشی از وظایف تصدی را به بخش غیر دولتی انتقال داده باشیم.

امروزه برای ورود هواپیماهای باری به فرودگاه های تهران، مشهد، تبریز، اصفهان بدون تشریفات و در فاصله ۶ ساعت قبل از پرواز مجوز ترافیکی صادر می گردد و تلاش گردیده تا تسهیلات لازم برای تخلیه و بارگیری آنها فراهم شود.

۴. خدمات حمل و نقل هوائی

تعداد ناوگان تجاری هوائی کشور اعم از تملیکی و اجاره ای تحت پوشش شرکتهای حمل و نقل هوائی دولتی و غیر دولتی نزدیک به ۱۰۰ فروند هواپیما با ظرفیت بیش از ۱۴۰۰۰ صندلی و بیش از ۱۰ فروند هواپیما با ظرفیت حدود ۹۰۰ تن بار می باشد. در نتیجه تنگناهای اقتصادی و دشواری های تامین قطعات و عدم نوسازی، ناوگان به تدریج به لحاظ زمانی و کارکرد هواپیماها دارای عمر متوسط بیش از ۲۲ سال میباشد در دو سال گذشته با ارائه تسهیلات بانکی به شرکتهای حمل و نقل هوای نسبت به افزایش هواپیماهای تملیکی و نو سازی ناوگان متناسب با شبکه پروازی کشور اقداماتی صورت پذیرفته است.

در فرودگاههای کشور تمامی خدمات زمینی هواپیما، کترینگ و خدمات بار به وسیله شرکتهای حمل و نقل هوائی داخلی انجام می پذیرد که اخیراً با واگذاری این نوع خدمات به شرکتهای مستقل بخش خصوصی موافقت گردیده و از حالت انحصاری خارج شده است.

در سال حدود ۱۰ میلیون مسافر با ناوگان هوائی در داخل و خارج از کشور جابجا می گردد که نزدیک به ۲۰٪ آنها به وسیله شرکتهای حمل و نقل هوائی خصوصی انجام می شود.

۵. تعمیرات هواپیما

سطح تعمیر و نگهداری هواپیما در بعضی از شرکتهای هواپیمائی کشور رده های C،B،A را میپوشاند و در مورد هواپیماهای بدنه متوسط و باریک حتی به رده D می رسد در مورد تعمیر و نگهداری هواپیماهای توپولف ۱۵۴ نیز دو مرکز تعمیراتی در مشهد و کیش تاسیس گردیده که در سال جاری ۴۷ مورد چکهای فنی در دوره های ۳۰۰، ۶۰۰، ۱۲۰۰ ساعت در آنجا انجام پذیرفت و موجبات صرفه جویی ارزی را فراهم آورده است.

و با اعلام رسمی به شرکتهای هواپیمایی مبنی بر استفاده الزامی از کروی پروازی ایرانی بجای خلبانان روسی اجاره هواپیماهای بدون خلبان روسی در دیتور کار قرار گرفته که تا پایان سال رقم استفاده از خلبانان روسی به صفر خواهد رسید که این تصمیم در نوع خود سهم بسزایی در کاهش ارزبری خواهد داشت.

۶. آموزش و مطالعات

دانشکده صنعت هواپیمائی کشوری به عنوان مرکز آموزش های تخصصی صنعت هوانوردی در کشور به شمار می رود که از فضای آموزشی مناسب، آزمایشگاههای مجهز و شبیه سازهای ارتباطی، راداری برخوردار است. سطوح آموزش های کارشناسی مراقبت پرواز، الکترونیک، مخابرات، تعمیر و نگهداری هواپیما در دانشکده وجود دارد و تلاش بر آن است تا تمامی دوره ها بصورت کاربردی انجام شود. علاوه بر این دوره های کوتاه مدت اطلاعات پرواز، خدمات فروش بلیط هواپیما، زبان انگلیسی فنی و عمومی، کامپیوتر اصول پرواز، از جمله فعالیتهای آنجاست. اخیراً نسبت به راه اندازی دوره های مشترک بین المللی در زمینه مدیریت فرودگاهی و ارتباطات، ناوبری و نظارت / مدیریت عبور و مرور هوائی با همکاری موسسات یاتا و نیوزیلند اقدام

شده است. دانشکده به عضویت دایمی پروژه جهانی Trainer در آمده و در زمینه تهیه طرح دروس استاندارد شده مربوط به شیوه های مدرن ارزیابی و امتحانات، هدایت هواپیما از طریق دیتا فعال بوده و می تواند از سایر موارد تهیه شده در کشور های دیگر استفاده نماید.

مرکز آموزش فنون هوایی عهده دار ارایه خدمات آموزشی و تفریحی در زمینه عملیات کایت، بالن، گلایدر، چتر بازی، خلبانی می باشد. این مرکز علاوه بر تهران در شهر های مشهد، شیراز، اهواز، همدان، اصفهان، تبریز و کرمانشاه دارای شعبه است. برگزاری نمایش های هوائی در مجموعه پروازی آسمان ری و جزیره کیش از جمله فعالیتهای آنهاست. با همکاری آموزش و پرورش نیز نسبت به تاسیس دبیرستان هوانوردی در نظام آموزشی متوسطه کشور اقدام گردیده است. با واگذاری بخشی از این فعالیتها به بخش غیر دولتی گستره انجام آنها برای جوانان فراهم آمده است.

مرکز مطالعات نیز مطالعه و بررسی طرح جامعه شبکه فرودگاهی و طرح جامع کنترل فضای کشور و چگونگی به کارگیری تجهیزات و سیستم های جدید هوانوردی و طرح جامع اتوماسیون اداری سازمان در راستای نظام جامع آمارهای ثبتی و طرحی سیستم ۱۲۸ کاناله AFIN و AIS را در دست انجام دارد. علاوه بر آن در تهیه طرح جامع حمل و نقل کشور همکاری مستمر دارد.

شبکه و انواع آن

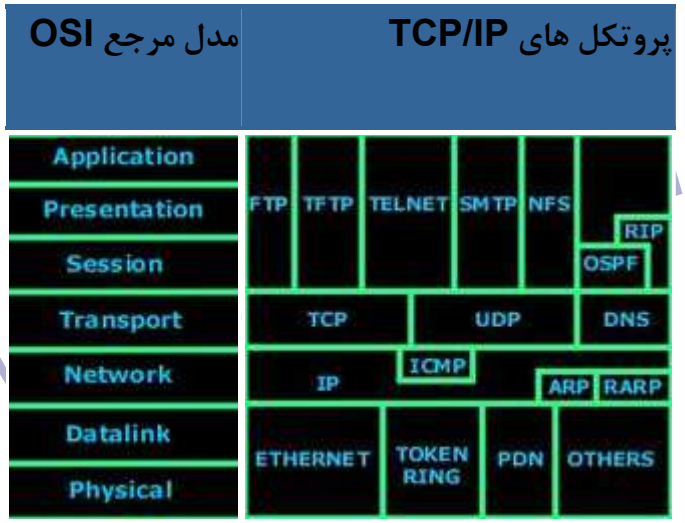
یک شبکه کامپیوتری از اتصال دو و یا چندین کامپیوتر تشکیل می گردد . شبکه های کامپیوتری در ابعاد متفاوت و با اهداف گوناگون طراحی و پیاده سازی می گردند . شبکه های(Local-Area Networks : LAN) و (WAN:Wide Area ´ Networks) دو نمونه متداول در این زمینه می باشند. در شبکه های LAN ، کامپیوترهای موجود در یک ناحیه محدود جغرافیائی نظیر منزل و یا محیط کار به یکدیگر متصل می گردند . در شبکه های WAN ، با استفاده از خطوط تلفن و یا مخابراتی ، امواج رادیوئی و سایر گزینه های موجود ، دستگاه های مورد نظر در یک شبکه به یکدیگر متصل می گردند .

شبکه های کامپیوتری چگونه تقسیم بندی می گردند ؟

شبکه ها ی کامپیوتری را می توان بر اساس سه ویژگی متفاوت تقسیم نمود : توپولوژی ، پروتکل و معماری

- **توپولوژی** ، نحوه استقرار(آرایش) هندسی یک شبکه را مشخص می نماید . bus , ring و star ، سه نمونه متداول در این زمینه می باشند .
- **پروتکل** ، مجموعه قوانین لازم به منظور مبادله اطلاعات بین کامپیوترهای موجود در یک شبکه را مشخص می نماید . اکثر شبکه ها از "اترنت" استفاده می نمایند. در برخی از شبکه ها ممکن است از پروتکل Ring Token شرکت IBM استفاده گردد . پروتکل ، در حقیت بمنزله یک اعلامیه رسمی است که در آن قوانین و رویه های مورد نیاز به منظور ارسال و یا دریافت داده ، تعریف می گردد . در صورتی که دارای دو و یا چندین دستگاه (نظیر کامپیوتر) باشیم و بخواهیم آنان را به یکدیگر مرتبط نمائیم ، قطعا" به وجود یک پروتکل در شبکه نیاز خواهد بود .تاکنون صدها پروتکل با اهداف متفاوت طراحی و پیاده سازی شده است . TCP/IP یکی از متداولترین پروتکل ها در زمینه شبکه بوده که خود از مجموعه پروتکل هائی دیگر ، تشکیل شده است . جدول زیر متداولترین پروتکل های TCP/IP را نشان می دهد . در کنار جدول فوق ، مدل مرجع OSI نیز ارائه شده است تا مشخص گردد که هر یک از پروتکل های فوق در چه لایه ای از مدل OSI کار می کنند . به موازات حرکت از پائین ترین لایه (لایه فیزیکی) به بالاترین لایه (لایه

Application) ، هر یک از دستگاههای مرتبط با پروتکل های موجود در هر لایه به منظور انجام پردازش های مورد نیاز ، زمانی را صرف خواهند کرد .



OSI از کلمات Open Systems Interconnect اقتباس و یک مدل مرجع در خصوص نحوه ارسال پیام بین دو نقطه در یک شبکه مخابراتی و ارتباطی است . هدف عمده مدل OSI ، ارائه راهنمائی های لازم به تولید کنندگان محصولات شبکه ای به منظور تولید محصولات سازگار با یکدیگر است .

مدل OSI توسط کمیته IEEE ایجاد تا محصولات تولید شده توسط تولید کنندگان متعدد قادر به کار و یا سازگاری با یکدیگر باشند . مشکل عدم سازگاری بین محصولات تولیدشده توسط شرکت های بزرگ تجهیزات سخت افزاری زمانی آغاز گردید که شرکت HP تصمیم به ایجاد محصولات شبکه ای نمود و محصولات تولید شده توسط HP با محصولات مشابه تولید شده توسط شرکت های دیگر نظیر IBM ، سازگار نبود . مثلا" زمانی که شما چهل کارت شبکه را برای شرکت خود تهیه می نمودید ، می بایست سایر تجهیزات مورد نیاز شبکه نیز از همان تولید کننده خریداری می گردید(اطمینان از وجود سازگاری بین آنان) . مشکل فوق پس از معرفی مدل مرجع OSI ، برطرف گردید .

مدل OSI دارای هفت لایه متفاوت است که هر یک از آنان به منظور انجام عملیاتی خاصی طراحی شده اند . بالاترین لایه ، لایه هفت (Application) و پائین ترین لایه ، لایه یک (Physiacal) می باشد . در صورتی که قصد ارسال داده برای یک کاربر دیگر را داشته باشید ، داده ها حرکت خود را از لایه هفتم شروع نموده و پس از تبدیل به سگمنت ، datagram ، بسته اطلاعاتی (Packet) و فریم، در نهایت در طول کابل (عموما" کابل های twisted pair) ارسال تا به کامپیوتر مقصد برسد .

- **معماری** ، به دو گروه عمده معماری که عمدتا" در شبکه های کامپیوتری استفاده می گردد ، اشاره می نماید : Peer-To-Peer و Server - Client . در شبکه های Peer-To-Peer سرویس دهنده اختصاصی وجود نداشته و کامپیوترها از طریق workgroup

به منظور اشتراک فایل ها ، چاپگرها و دستیابی به اینترنت ، به یکدیگر متصل می گردند .

در شبکه های Client - Server ، سرویس دهنده و یا سرویس دهندگانی اختصاصی وجود داشته (نظیر یک کنترل کننده Domain در ویندوز) که تمامی سرویس گیرندگان به منظور استفاده از سرویس ها و خدمات ارائه شده ، به آن log on می نمایند . در اکثر سازمان و موسسات از معماری Client - Server به منظور پیکربندی شبکه های کامپیوتری ، استفاده می گردد.

مفاهیم امنیت شبکه

امنیت شبکه یا Network Security پردازه ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند:

۱-شناسایی بخشی که باید تحت محافظت قرار گیرد.

۲-تصمیم گیری درباره مواردی که باید در مقابل آنها از بخش مورد نظر محافظت کرد.

۳-تصمیم گیری درباره چگونگی تهدیدات

۴-پیاده سازی امکاناتی که بتوانند از دارایی های شما به شیوه ای محافظت کنند که از نظر هزینه به صرفه باشد.

۵-مرور مجدد و مداوم پردازه و تقویت آن درصورت یاقتن نقطه ضعف

برای درک بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبکه می پردازیم.

۱- منابع شبکه

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبکه را معرفی می کند که باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

۱ -تجهیزات شبکه مانند روترها، سوئیچ ها و فایروالها

۲-اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره شده اند.

۳-منابع نامحسوس شبکه مانند عرض باند و سرعت

۴-طلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه های داده و سرورهای اطلاعاتی

۵-ترمینالهایی که برای استفاد هاز منابع مختلف به شبکه متصل می شوند.

۶-اطلاعات در حال تبادل بر روی شبکه در هر لحظه از زمان

۷-خصوصی نگهداشتن عملیات کاربرن و استفاده آنها از منابع شبکه جهت جلوگیری از شناسایی کاربران.

مجموعه فوق به عنوان دارایی های یک شبکه قلمداد می شود.

۲- حمله

حال به تعریف حمله می پردازیم تا بدانیم که از شبکه در مقابل چه چیزی باید محافظت کنیم. حمله تلاشی خطرناک یا غیر خطرناک است تا یک منبع قابل دسترسی از طریق شبکه ، به گونه ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.برای فهم بهتر بد نیست حملات شبکه را به سه دسته عمومی تقسیم کنیم:

۱-دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲-دستکاری غیرمجاز اطلاعات بر روی یک شبکه

۳-حملاتی که منجر به اختلال در ارائه سرویس می شوند و اصطلاحا Denial of Service نام دارند.

کلمه کلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یک عمل مجاز یا غیرمجاز به عهده سیاست امنیتی شبکه است، اما به عبارت کلی می توان دسترسی غیرمجاز را تلاش یک کاربر جهت دیدن یا تغییر اطلاعاتی که برای وی در نظر گرفته نشده است، تعریف نمود اطلاعات روی یک شبکه نیز شامل اطلاعات موجود بر روی رایانه های متصل به شبکه مانند سرورهای پایگاه داده و وب ، اطلاعات در حال تبادل بر روی شبکه و اطلاعات مختص اجزاء شبکه جهت انجام کارها مانند جداول مسیریابی روتر است. منابع شبکه را نیز می توان تجهیزات انتهایی مانند روتر و فایروال یا مکانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه ، حفاظت از شبکه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه کرد:

۱-ثابت کردن محرمانگی داده

۲-نگهداری جامعیت داده

۳-نگهداری در دسترس بودن داده

۳ _تحلیل خطر

پس از تعیین دارایی های شبکه و عوامل تهدیدکننده آنها ، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاکتور اصلی در تحلیل خطر عبارتند از :

۱-احتمال انجام حمله

۲-خسارت وارده به شبکه درصورت انجام حمله موفق

۴- سیاست امنیتی

پس از تحلیل خطر باید سیاست امنیتی شبکه را به گونه ای تعریف کرد که احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات

نپردازد. جزئیات می توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست های آن را تشکیل می دهند ثابت باقی می مانندر واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

۱-چه و چرا باید محافظت شود.

۲-چه کسی باید مسئولیت حفاظت را به عهده بگیرد.

۳-زمینه ای را بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

سیاستهای امنیتی را می توان به طور کلی به دو دسته تقسیم کرد:

۱-مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.

۲-محدود کننده (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودکننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشکلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد. المانهای دخیل در سیاست امنیتی در RFC 2196 لیست و ارائه شده اند.

۵- طرح امنیت شبکه

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یک طرح امنیت شبکه می رسیم. المانهای تشکیل دهنده یک طرح امنیت شبکه عبارتند از :

۱-ویژگیهای امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا بکارگیری SSH

۲-فایروالها

۳-مجتمع کننده های VPN برای دسترسی از دور

۴-تشخیص نفوذ

۵-سرورهای امنیتی AAA (Authentication، Authorization and Accounting) و سایر خدمات AAA برای شبکه

۶-مکانیزمهای کنترل دسترسی و محدودکننده دسترسی برای دستگاههای مختلف شبکه

۶- نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می کند. در واقع یکی از بهترین شیوه های دفاع در مقابل حملات شبکه ، طراحی امنیت شبکه به صورت منطقه ای و مبتنی بر توپولوژی است و یکی از مهمترین ایده های مورد استفاده در شبکه های امن مدرن ، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می شود.

نواحی امنیتی بنابر استراتژی های اصلی ذیل تعریف می شوند.

۱-تجهیزات و دستگاههایی که بیشترین نیاز امنیتی را دارند (شبکه خصوصی) در امن ترین منطقه قرار می گیرند. معمولا اجازه دسترسی عمومی یا از شبکه های دیگر به این منطقه داده نمی شود. دسترسی با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از

دور امن (SRA) کنترل می شود. کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه به شدت انجام می شود.

۲-سرورهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه ای امن ، خصوصی و مجزا قرار می گیرند. کنترل دسترسی به این تجهیزات با کمک فایروال انجام می شود و دسترسی ها کاملا نظارت و ثبت می شوند.

۳-سرورهایی که باید از شبکه عمومی مورد دسترسی قرار گیرند در منطقه ای جدا و بدون امکان دسترسی به مناطق امن تر شبکه قرار می گیرند. درصورت امکان بهتر است هر یک از این سرورها را در منطقه ای مجزا قرار داد تا درصورت مورد حمله قرار گرفتن یکی ، سایرین مورد تهدید قرار نگیرند. به این مناطق DMZ یا Demilitarized Zone می گویند.

۴-استفاده از فایروالها به شکل لایه ای و به کارگیری فایروالهای مختلف سبب می شود تا درصورت وجود یک اشکال امنیتی در یک فایروال ، کل شبکه به مخاطره نیفتد و امکان استفاده از Backdoor نیز کم شود.

رویکردی عملی به امنیت شبکه لایه بندی شده

امروزه امنیت شبکه یک مسأله مهم برای ادارات و شرکتهای دولتی و سازمان های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست های فضای سایبر، کارمندان ناراضی و هکرها رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.

در این قسمت 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 زیرساختار 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

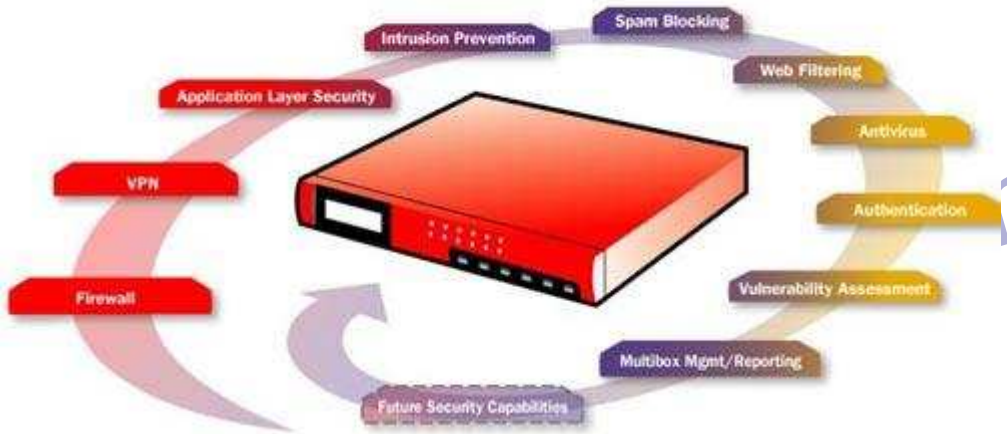
۳- میزبان

۴- برنامه کاربردی

۵- دیتا

در این سلسله مقالات 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 اخلال 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 چیزیست که شما می خواهید.

تکنولوژی های بحث شده در اینجا مجموعاً 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	فایروال آنتی ویروس در سطح شبکه رمزنگاری شبکه خصوصی مجازی
۲	شبکه	سیستم تشخیص/جلوگیری از نفوذ (IDS/IPS) سیستم مدیریت آسیب پذیری تبعیت امنیتی کاربر انتهایی کنترل دسترسی/ تایید هویت کاربر
۳	میزبان	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان تبعیت امنیتی کاربر انتهایی آنتی ویروس کنترل دسترسی/ تایید هویت کاربر
۴	برنامه کاربردی	سیستم تشخیص نفوذ میزبان سیستم ارزیابی آسیب پذیری میزبان کنترل دسترسی/ تایید هویت کاربر تعیین صحت ورودی
۵	داده	رمزنگاری کنترل دسترسی

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. DMZ معمولاً وب سرورها، مدخل ایمیل

ها، آنتی ویروس شبکه و سرورهای DNS را دربرمی 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 سرورها 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.

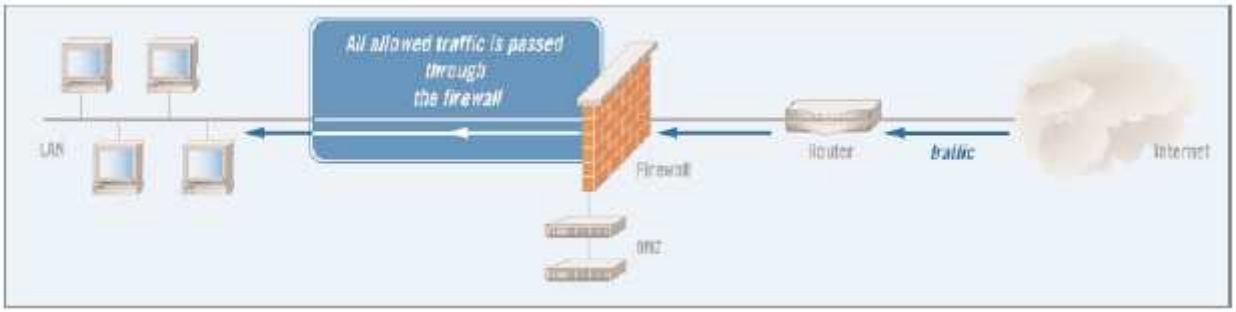
تکنولوژیهای زیر امنیت را در پیرامون شبکه ایجاد می کنند:

- **فایروال ـ** معمولاً یک فایروال روی سروری نصب می گردد که به بیرون و درون پیرامون شبکه متصل است. فایروال سه عمل اصلی انجام می دهد ۱- کنترل ترافیک ۲- تبدیل آدرس و ۳- نقطه پایانی VPN. فایروال کنترل ترافیک را با سنجیدن مبداء و مقصد تمام ترافیک واردشونده و خارج شونده انجام می دهد و تضمین می کند که تنها تقاضاهای مجاز اجازه عبور دارند. بعلاوه، فایروال ها به شبکه امن در تبدیل آدرس های IP داخلی به آدرس های قابل رویت در اینترنت کمک می کنند. این کار از افشای اطلاعات مهم درباره ساختار شبکه تحت پوشش فایروال جلوگیری می کند. یک فایروال همچنین می تواند به عنوان نقطه پایانی تونل های VPN (که بعداً بیشتر توضیح داده خواهد شد) عمل کند. این سه قابلیت فایروال را تبدیل به بخشی واجب برای امنیت شبکه شما می کند.

- **آنتی ویروس شبکه ـ** این نرم افزار در DMZ نصب می شود و محتوای ایمیل های واردشونده و خارج شونده را با پایگاه داده ای از مشخصات ویروس های شناخته شده مقایسه می کند. این آنتی ویروس ها آمد و شد ایمیل های آلوده را مسدود می کنند و آنها را قرنطینه می کنند و سپس به دریافت کنندگان و مدیران شبکه اطلاع می دهند. این عمل از ورود و انتشار یک ایمیل آلوده به ویروس در شبکه جلوگیری می کند و جلوی گسترش ویروس توسط شبکه شما را می گیرد. آنتی ویروس شبکه، مکملی برای حفاظت ضدویروسی است که در سرور ایمیل شما و کامپیوترهای مجزا صورت می گیرد. بمنظور کارکرد مؤثر، دیتابیس ویروس های شناخته شده باید به روز نگه داشته شود.

- **VPN ـ** یک شبکه اختصاصی مجازی (VPN) از رمزنگاری سطح بالا برای ایجاد ارتباط امن بین ابزار دور از یکدیگر، مانند لپ تاپ ها و شبکه مقصد استفاده می کند. VPN اساساً یک تونل رمزشده تقریباً با امنیت و محرمانگی یک شبکه اختصاصی اما از میان اینترنت ایجاد می کند. این تونل VPN می تواند در یک مسیریاب برپایه VPN، فایروال یا یک سرور در ناحیه DMZ پایان پذیرد. برقراری ارتباطات VPN برای تمام بخش های دور و بی سیم شبکه یک عمل مهم است که نسبتاً آسان و ارزان پیاده سازی می شود.

!Error



مزایا

تکنولوژی های ایجاد شده سطح پیرامون سال هاست که در دسترس هستند، و بیشتر خبرگان IT با تواناییها و نیازهای عملیاتی آنها به خوبی آشنایی دارند. بنابراین، از نظر پیاده سازی آسان و توأم با توجیه اقتصادی هستند. بعضیاز 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 مدت هاست 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 دیتابیس خود داشته باشد و این ویروس داخل یک فایل رمزشده قرار نداشته باشد. اگرچه VPN رمزنگاری مؤثری ارائه می کند، اما کار اجرایی بیشتری را برروی کارمندان IT تحمیل می کنند، 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 هرکدام از تکنولوژی های مذکور اجازه می دهد که به تنهایی پوشش مؤثری برای شبکه ایجاد کنند.

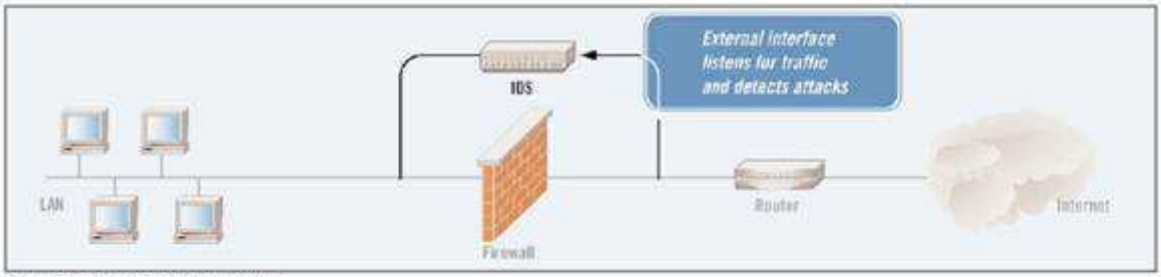
انواع ابزاری که در DMZ شما قرار دارد نیز یک فاکتور مهم است. این ابزارها چه میزان اهمیت برای کسب و کار شما دارند؟ هرچه اهمیت بیشتر باشد، معیارها و سیاست های امنیتی سفت و سخت تری باید این ابزارها را مدیریت کنند.

سطح ۲- امنیت شبکه

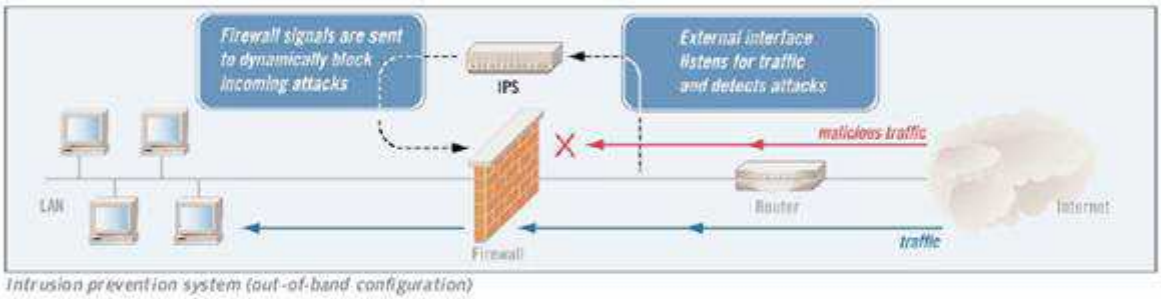
سطح شبکه در مدل امنیت لایه بندی شده به WAN و LAN داخلی شما اشاره دارد. شبکه داخلی شما ممکن است شامل چند کامپیوتر و سرور و یا شاید پیچیده تر یعنی شامل اتصالات نقطه به نقطه به دفترهای کار دور باشد. بیشتر شبکه های امروزی در ورای پیرامون، باز هستند؛ یعنی هنگامی که داخل شبکه قرار دارید، می توانید به راحتی 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:

- **IDSها (سیستم های تشخیص نفوذ) و IPSها (سیستم های جلوگیری از نفوذ) ـ**

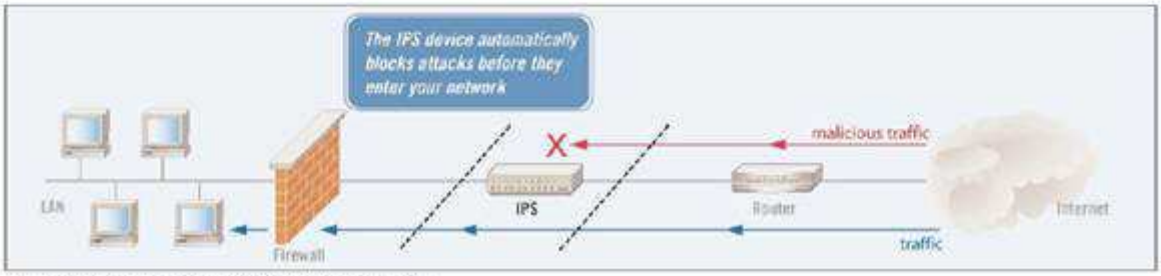
تکنولوژیهای IDS و IPS ترافیک گذرنده در شبکه شما را با جزئیات بیشتر نسبت به فایروال تحلیل می کنند. مشابه سیستم های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده ای از مشخصات حملات شناخته شده مقایسه می کنند. هنگامی که حملات تشخیص داده می شوند، این ابزار وارد عمل می شوند. ابزارهای IDS مسؤولین IT را از وقوع یک حمله مطلع می سازند؛ ابزارهای IPS یک گام جلوتر می روند و بصورت خودکار ترافیک آسیب رسان را مسدود می کنند. IDSها و IPSها مشخصات مشترک زیادی دارند. در حقیقت، بیشتر IPSها در هسته خود یک IDS دارند. تفاوت کلیدی بین این تکنولوژی ها از نام آنها استنباط می شود. محصولات IDS تنها ترافیک آسیب رسان را تشخیص می دهند، در حالیکه محصولات IPS از ورود چنین ترافیکی به شبکه شما جلوگیری می کنند. پیکربندی های IDS و IPS استاندارد در شکل نشان داده شده اند:



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 می دهند: (۱) شبکه را برای آسیب پذیری ها پیمایش می کنند و (۲)روند مرمت آسیب پذیری یافته شده را مدیریت می کنند. در گذشته، این تکنولوژی VA (تخمین آسیب پذیری) نامیده می شد. اما این تکنولوژی اصلاح شده است، تا جاییکه بیشتر سیستم های موجود، عملی بیش از تخمین آسیب پذیری ابزار شبکه را انجام می دهند.

سیستم های مدیریت آسیب پذیری ابزار موجود در شبکه را برای یافتن رخنه ها و آسیب پذیری هایی که می توانند توسط هکرها و ترافیک آسیب رسان مورد بهره برداری قرار گیرند، پیمایش می کنند. آنها معمولاً پایگاه داده ای از قوانینی را نگهداری می کنند که آسیب پذیری های شناخته

شده برای گستره ای از ابزارها و برنامه های شبکه را مشخص می کنند. در طول یک پیمایش، سیستم هر ابزار یا برنامه ای را با بکارگیری قوانین مناسب می آزماید.

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

- **تابعیت امنیتی کاربر انتهایی** – روش های تابعیت امنیتی کاربر انتهایی به این طریق از شبکه محافظت می کنند که تضمین می کنند 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 سیستم های ناامن کارمندان و ابزارهای VPN و RAS می گیرد.

روش های امنیت نقاط انتهایی براساس آزمایش هایی که روی سیستم هایی که قصد اتصال دارند، انجام می دهند، اجازه دسترسی می دهند. 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 تأییدهویت در سطوح شبکه، میزبان، نرم افزار و دیتا در چارچوب امنیتی لایه بندی شده می پردازیم. میان طرح های کنترل دسترسی بین لایه های مختلف همپوشانی قابل توجهی وجود دارد. معمولاً تراکنش های تأیید هویت در مقابل دید کاربر اتفاق می افتد. 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 می دهند. در حالیکه فایروال به ترافیک، برپایه مقصد نهایی آن اجازه عبور می دهد، ابزار IPS و IDS تجزیه و تحلیل عمیق تری را برعهده دارند، و بنابراین سطح بالاتری از محافظت را ارائه می کنند. با این تکنولوژی های پیشرفته، حملاتی که داخل ترافیک قانونی شبکه وجود دارند و می توانند 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 غیرعملی خواهد بود. بعلاوه، شبکه ساختار پویایی دارد. ابزار جدید، ارتقاءدادن 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، همچانکه پدیده های اخیر چون Mydoom، Sobig، و Sasser گواهی بر این مدعا هستند. برنامه های امنیتی کاربران انتهایی این درهای پشتی خطرناک به شبکه را می بندند.

معایب

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 دیتای کم ارزش مدفون شود. مدیران IDS ممکن است به سرعت حساسیت خود را نسبت به اطلاعات تولید شده توسط سیستم از دست بدهند. برای تأثیرگذاری 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 IPSها 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 سیستمهایی 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 اتصالی 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 بهبودیافته 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.

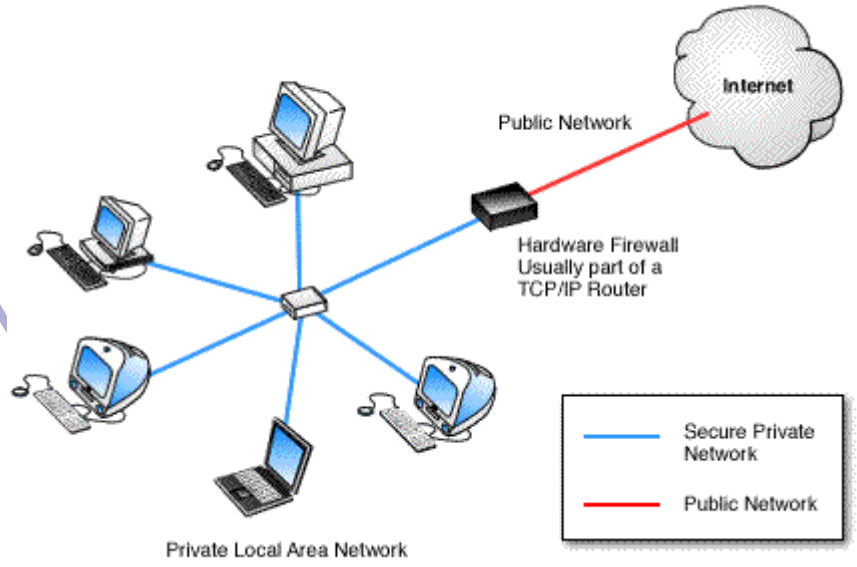
سطح ۳- امنیت میزبان

سطح میزبان در مدل امنیت لایه بندی شده، مربوط به ابزار منفرد مانند سرورها، کامپیوترهای شخصی، سوئیچ ها، روترها 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 رجیستری، 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** ـ IDSهای سطح میزبان عملیاتی مشابه IDSهای شبکه انجام می دهند؛ تفاوت اصلی در نمایش ترافیک در یک ابزار شبکه به تنهایی است. IDSهای 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 پویش 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، درصورت 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 باراضافی 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 نیات 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 پیکربندی 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 دربرمی گیرد. رمزنگاری دیتا، هنگامی که ذخیره می شود و یا در شبکه شما حرکت می کند، به عنوان روشی بسیار مناسب توصیه می گردد، زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شما را محافظت می کند. امنیت دیتا تا حد زیادی به سیاست های سازمانی شما وابسته است. سیاست سازمانی می گوید که چه کسی به دیتا دسترسی دارد، کدام کاربران مجاز می توانند آن را دستکاری کنند و چه کسی مسوول نهایی یکپارچگی و امن ماندن آن است. تعیین صاحب و متولی دیتا به شما اجازه می دهد 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 می کنند:

- **رمزنگاری** – طرح های رمزنگاری دیتا در سطوح دیتا، برنامه و سیستم عامل پیاده می شوند. 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 PKI، PGP و RSA 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 می کند. 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 می کند.

معایب

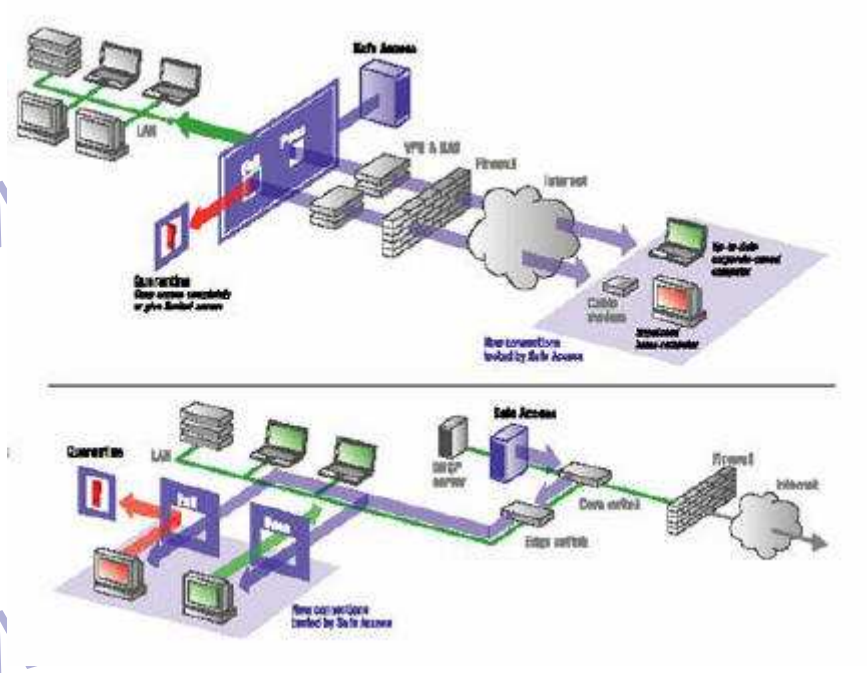
بار اضافی برای رمزنگاری و رمزگشایی دیتا وجود دارد که می تواند تأثیرات زیادی در کارایی بگذارد. به علاوه، مدیریت کلیدها می تواند تبدیل به یک بار اجرایی در سازمان های بزرگ یا در حال رشد گردد.

ملاحظات

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

دفاع در مقابل تهدیدها و حملات معمول

دیدیم که چگونه رویکرد امنیت لایه بندی شده در مقابل تهدیدها و حملات معمول از شبکه شما محافظت می کند و نشان می دهد که چگونه هر سطح با داشتن نقشی کلیدی در برقراری امنیت شبکه جامع و مؤثر، شرکت می کند.



بعضی حملات معمول شامل موارد زیر می شود:

- **حملات به وب سرور** ـ حملات به وب سرور دامنه زیادی از مشکلاتی را که تقریباً برای هر وب سرور ایجاد می شود، در برمی گیرد. از دستکاری های ساده در صفحات گرفته تا در اختیار گرفتن سیستم از راه دور و تا حملات DOS. امروزه حملات به وب سرور یکی از معمول ترین حملات هستند. Code Red و Nimda به عنوان حمله کنندگان به وب سرورها از شهرت زیادی! برخوردارند.

- **بازپخش ایمیل ها بصورت نامجاز** ـ سرورهای ایمیلی که بصورت مناسب پیکربندی نشده اند یک دلیل عمده برای ارسال هرزنامه ها بشمار می روند. بسیاری از شرکت های هرزنامه ساز در پیدا کردن این سرورها و ارسال صدها و هزاران پیام هرزنامه به این سرورها، متخصص هستند.

- **دستکاری میزبان دور در سطح سیستم** ـ تعدادی از آسیب پذیری ها، یک سیستم را از راه دور در اختیار حمله کننده قرار می دهند. بیشتر این نوع کنترل ها در سطح سیستم است و به حمله کننده اختیاراتی برابر با مدیر محلی سیستم می دهد.
- **فراهم بودن سرویس های اینترنتی غیرمجاز** ـ توانایی آسان بکارگیری یک وب سرور یا سرویس اینترنتی دیگر روی یک کامپیوتر ریسک افشای سهوی اطلاعات را بالا می برد. اغلب چنین سرویس هایی کشف نمی شوند، در حالی که در شعاع رادار دیگران قرار می گیرند!
- **تشخیص فعالیت ویروسی** ـ در حالی که برنامه ضدویروس در تشخیص ویروس ها مهارت دارد، این نرم افزار برای تشخیص فعالیت ویروسی طراحی نشده است. در این شرایط بکارگیری یک برنامه تشخیص نفوذ یا IDS شبکه برای تشخیص این نوع فعالیت بسیار مناسب است.

نتیجه گیری

هکرها و تروریست های فضای سایبر به طور فزاینده ای اقدام به حمله به شبکه ها می کنند. رویکرد سنتی به امنیت ـ یعنی یک فایروال در ترکیب با یک آنتی ویروس ـ در محافظت از شما در برابر تهدیدهای پیشرفته امروزی ناتوان است.

اما شما می توانید با برقراری امنیت شبکه با استفاده از رویکرد لایه بندی شده دفاع مستحکمی ایجاد کنید. با نصب گزینشی ابزارهای امنیتی در پنج سطح موجود در شبکه تان (پیرامون، شبکه، میزبان، برنامه و دیتا) می توانید از دارایی های دیجیتالی خود محافظت کنید و از افشای اطلاعات خود در اثر ایجاد رخنه های مصیبت بار تا حد زیادی بکاهید.