مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۲ ، تابستان ۱۳۹۵، ص ۶۸-۶۰

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۲ / تابستان ۱۳۹۵ / ص ۶۸-۶۰

کنترل دسترسی بر پایه ی AAA

محمود جزایری[۱]، افشین رضاخانی[۲]، لیلا ریخته چی [۳]

[۱] دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی واحد بروجرد
[۲] عضو هیئت علمی ، دانشگاه آیت الله بروجردی
[۳] عضو هیئت علمی، دانشگاه آزاد اسلامی واحد بروجرد

نام و نشانی ایمیل نویسنده مسئول:
محمود جزایری
mah_jazayeri@yahoo.com

چکیده

آنچه در بحث سیاستگذاری در یک سازمان بعنوان یک اصل و پایه باید در نظر گرفته شود بیانیه تعهد مدیریت است این به معنی اعلام رضایت و توافق مدیریت با پیاده سازی سیاست های امنیتی در سازمان می باشد. سیاست های امنیتی باید در حوزه های بسیاری از سازمان از جمله حوزه سیاست های دسترسی که سطح و میزان دسترسی افراد را مشخص می کند، حوزه سیاست های تشخیص هویت که نحوهٔ شناسایی افراد و بسته‌های مختلفی که متقاضی ورود به شبکه و استفاده از منابع هستند را مشخص می‌کند، حوزه سیاست حسابداری که چگونگی نگهداری اتفاقاتی که در شبکه می‌افتند را مشخص می‌کند و حوزه های دیگری چون حوزه سیاست گزارش تخلفات، سیاست حریم خصوصی افراد، سیاست نگهداری شبکه، سیاست در دسترس بودن، سیاست های آگاهی رسانی، تعیین گردد. در حقیقت فرآیند دسترسی و استفاده از منابع در یک سازمان یک فرآیند سه مرحله ای است که برای یک سازمان در جهت برقراری امنیت و اعمال سیاستگذاری ها پیشروی طبق این مراحل لازم و ضروری است این تکنولوژی AAA نام دارد که سه عمل احراز هویت، احراز مجوز و حسابرسی را به عنوان مراحل پایه جهت برقراری امنیت در یک سازمان در نظر گرفته است.

واژگان کلیدی: کنترل دسترسی، احرزا هویت، امنیت، AAA، سیاست های امنیتی

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۲ ، تابستان ۱۳۹۵، ص ۶۸-۶۰

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

با پیشرفت تمدن و شکل‌گیری جوامع، محدوده امنیت ابعاد بسیار گسترده‌تری یافت و با تفکیک حوزه اموال و حقوق شخصی افراد از یکدیگر و اموال عمومی و همچنین تعریف قلمروهای ملی و بین‌المللی، به تدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی، امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. آنچه در بحث سیاستگذاری در یک سازمان بعنوان یک اصل و پایه باید در نظر گرفته شود بیانیه تعهد مدیریت است این به معنی اعلام رضایت و توافق مدیریت با پیاده سازی سیاست های امنیتی در سازمان می باشد و به همین منظور می توان این طور اظهار کرد که بیانیه تعهد مدیریت را می توان مهمترین بخش از سیاست امنیت اطلاعات دانست. در حقیقت دشوارترین بخش در یک سیاست گذاری ارائه آن به شکلی است که مورد پذیرش کارکنان قرار گیرد. بدون این بیانیه هرگونه تلاش از سوی پرسنل امنیت اطلاعات فایده چندانی نخواهد داشت و بخش های مختلف سازمان این فعالیت ها را با جدیت دنبال نخواهند کرد. این بیانیه نشانگر موافقت و تمایل مدیریت در مورد امنیت اطلاعات و سیاستگذاری آن است البته باید توجه داشت که تعهد مدیریت موفقیت سیاست امنیتی را تضمین نمی کند، اما نبود آن احتمال شکست را افزایش خواهد داد در نتیجه تأییدیه سیاست امنیت اطلاعات را می توان مدرکی دانست، که بر این سیاست گذاری صحه گذاشته و امکان اعمال آن در کل سازمان را فراهم می آورد. سیاست های امنیتی باید در حوزه های بسیاری از سازمان از جمله حوزه سیاست های دسترسی که سطح و میزان دسترسی افراد را مشخص می کند، حوزه سیاست های تشخیص هویت که نحوهٔ شناسایی افراد و بسته‌های مختلفی که متقاضی ورود به شبکه و استفاده از منابع هستند را مشخص می‌کند، حوزه سیاست حسابداری که چگونگی نگهداری اتفاقاتی که در شبکه می‌افتند را مشخص می‌کند و حوزه های دیگری چون حوزه سیاست گزارش تخلفات، سیاست حریم خصوصی افراد، سیاست نگهداری شبکه، سیاست در دسترس بودن، سیاست های آگاهی رسانی، تعیین گردد.

یکی از وظایفی که امنیت بر عهده دارد کنترل دسترسی به منابع است. کنترل دسترسی در حقیقت در مورد رابطه بین اشیاء و موضوع ها صحبت می کند. اصطلاح کنترل دسترسی در واقع به کنترل بیشتر بر روی دسترسی به منابع سیستم اشاره دارد. در حقیقت فرآیند دسترسی و استفاده از منابع در یک سازمان یک فرآیند سه مرحله ای است که برای یک سازمان در جهت برقراری امنیت و اعمال سیاستگذاری ها پیشروی طبق این مراحل لازم و ضروری است این تکنولوژی AAA نام دارد که سه عمل احراز هویت، احراز مجوز و حسابرسی را به عنوان مراحل پایه جهت برقراری امنیت در یک سازمان در نظر گرفته است. تکنولوژی احراز هویت، احراز مجوز و حسابرسی، یکی از مهمترین ابزار برای کنترل دسترسی کاربران در یک محیط شبکه است که به صورت گسترده در محیط شبکه ای استفاده می شود. در حقیقت مساله کنترل دسترسی و استفاده از مدل های کنترل دسترسی برای پیاده سازی سیاست ها و اعمال آن در سازمان، در مرحله احراز مجوز صورت می گیرد یعنی زمانیکه کاربری بتواند به این مرحله برسد و مرحله قبلی را با موفقیت پشت سر گذارد، یک کاربر مجاز شناخته شده است و در اینجاست که با توجه به نوع ورود خود سیاست های مربوطه برای او اعمال و اجرا می شود و حق دسترسی او به منابع تعیین می گردد. جهت بوجود آمدن یک روند منظم در سیاستگذاری ها و پیشروی طبق یک اصول خاص، مدل های کنترل دسترسی بوجود آمدند و مورد استفاده قرار می گیرند زیرا سیاستگذاری در یک سازمان باید بر اساس یک خط مشی باشد تا نوع و میزان دسترسی افراد به منابع از حالت سلیقه ای و دلبخواهی خارج گردد و حالت رسمی و منطقی به خود بگیرد بنابراین استفاده از مدل های کنترل دسترسی بهترین راه حل خواهد بود.

۱- مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به اهداف و ارائه راهکار های لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را برعهده داشته و در نهایت باید تلاش کند تا سیستم را همیشه به روز نگه دارد. هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی و نیروی انسانی سازمان در مقابل هرگونه تهدید اعم از دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سیستم و خطرات ایجاد شده از سوی کاربران است. یکی از وظایف مدیریت امنیت بررسی و ایجاد یک سیستم امنیت اطلاعات است که متناسب با اهداف سازمان باشد. برای طراحی این سیستم باید عوامل مختلفی را در نظر گرفت. محاسبه ارزش اطلاعات از نظر اقتصادی، بررسی خطرات و محاسبه خسارت‌های احتمالی و تخمین هزینه، سودمندی استفاده از سیستم امنیت اطلاعات، بررسی تهدیدات احتمالی و بررسی راه‌کارهای مختلف و انتخاب سودمندترین روش برای طراحی سیستم‌های امنیت اطلاعات ضروری به نظر می‌رسد[۲،۱].

ISSN: 2745-3673
http://www.Rcsj.ir

وجود یک حفره و یا مشکل امنیتی ، یک سازمان را به روش های متفاوتی تحت تاثیر قرار خواهد داد. آشنائی با عواقب خطرناک یک حفره امنیتی در یک سازمان و شناسائی مهمترین تهدیدات امنیتی که می تواند حیات یک سازمان را با مشکل مواجه نماید، از جمله موارد ضروری به منظور طراحی و پیاده سازی یک مدل امنیتی در یک سازمان می باشد. در بحث امنیت اطلاعات شما بایستی اهمیت موضوع را به خوبی درک کنید تا بتوانید از بوجود آمدن مشکلات آینده جلوگیری کنید. با وجود کنترل های امنیت اطلاعات شما از سرقت اطلاعات سازمانی خود در امان خواهید بود، اطلاعات سازمانی شما در حوزه امنیت اطلاعات دارایی های شما به حساب می آیند که برای سازمان دارای ارزش می باشند.

۲- اهداف و اهمیت سیاست های امنیتی

سیاست های امنیتی از این نظر حائز اهمیت است که به عنوان یک رکن اصلی در تصمیم گیری های موفق در مورد واگذاری اختیارات، چه برای منابع فیزیکی و چه منابع منطقی، پشتیبانی امنیتی و کنترل دسترسی به اطلاعات محسوب می شود. سیاست امنیتی باید به گونه ای تعریف شود که احتمال خطرات و میزان خسارت را به حداقل برساند زیرا در هر لحظه خطرات مختلفی از بیرون و درون سازمان، منافع سازمان را تهدید می کند در نتیجه سیاست ها قوانینی هستند که مشخص می کند چگونه برای استفاده از منابع و تخصیص صفات، تصمیمات کنترل دسترسی اتخاذ شود. هدف سیاست های امنیتی تعریف روال ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می نماید. با اجرای دقیق سیاست های امنیتی، سازمان ها می توانند تهدیدات را کاهش دهند. سیاست امنیت اطلاعات، تعیین کننده جهت امنیت اطلاعات در سازمان است و می بایست به صورت یک سند مکتوب تهیه گردد. در حقیقت به سیاست امنیتی به عنوان یک سند زنده نگریسته می شود، بدین معنا که فرایند تکمیل و اصلاح آن هیچ گاه متوقف نشده و متناسب با تغییر فناوری و نیازهای کاربران به روز می شود. این سند بایستی مکمل اهداف تجاری سازمان باشد و مشارکت مدیریت را در برقراری امنیت اطلاعات و پشتیبانی از آن، نظیر نقشی که امنیت اطلاعات در تعریف دیدگاه و مأموریت سازمان ایفا می کند، تعریف کند. همچنین، سیاست امنیت اطلاعات باید نیاز به امنیت اطلاعات و مفاهیم آن را برای تمامی کاربران منابع اطلاعاتی سازمان شرح دهد و کارمندان را در مورد مسئولیت های خود و نحوه استفاده از منابع سازمان مطلع سازد و شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست های امنیتی و راه کار به روز رسانی آنها را نیز مطرح کند لازم است که در این سند استفاده های مجاز شرح داده شوند و فعالیت های غیرمجاز به صورت لیستی ارائه گردند، به عبارت دیگر این سند بیان می کند که یک سازمان چگونه قصد دارد از سرمایه های فیزیکی و اطلاعاتی خود محافظت کند. هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است و سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر، از نظر عملی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت باشد و سطح حفاظتی قابل قبولی را ارائه نماید و می بایست سطح کنترل را با سطح بهره وری بالانس نماید . در صورتی که یک سیاست امنیتی محدودیت های زیادی را برای کاربران درپی داشته باشد، کاربران روش های نادیده گرفتن آن را بررسی و برای آن راه حل های خاص خود را پیدا خواهند کرد. در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

- چه و چرا باید محافظت شود
- چه کسی باید مسئولیت حفاظت را به عهده بگیرد
- زمینه را چگونه باید بوجود آورد که هرگونه تضاد احتمالی را حل و فصل کند

اهداف اصلی یک سیاست امنیت اطلاعات را میتوان به سه بخش محرمانگی یعنی اطمینان از اینکه اطلاعات تنها در دستان افراد مجاز قرار می گیرند، درستی یعنی حفاظت از اطلاعات در مقابل تغییر، تحریف و نابودی و دسترس پذیری یعنی اطمینان از اینکه اطلاعات و سیستم های اطلاعاتی در زمان مورد نیاز در دسترس و قابل استفاده هستند تقسیم کرد. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند و از سوی دیگر، مدیران سیستم و سازمان را در تصمیم گیری برای پیکربندی و استفاده از سیستم ها یاری رساند[۳].

۲-۱- موارد مهم در تعریف سیاست های امنیتی

در زمان تعریف سیاست های امنیتی می بایست به موارد زیر توجه گردد:

- یک سیاست امنیتی مناسب می بایست قادر به برقراری ارتباط مناسب با کاربران بوده و با ارائه یک ساختار اساسی آنان را در زمان بروز یک رویداد و یا مشکل امنیتی کمک نماید .

ISSN: 2745-3673
http://www.Rcsj.ir

- تدوین رویه های مناسب به منظور برخورد با یک مشکل امنیتی. در این رویه ها می بایست محدوده مسئولیت ها به دقت مشخص گردد.
- تعیین دقیق نوع و مکان ذخیره سازی اطلاعات مهمی که برای یک سازمان ارزش حیاتی دارند.
- مشخص نمودن اقداماتی که می بایست پس از بروز یک مشکل امنیتی انجام شود.
- سیاست های امنیتی به عنوان اصول عملیاتی رویه های امنیتی مطرح می باشند. بنابراین، می بایست به اندازه کافی عمومی باشند تا بتوان آنان را با استفاده از فن آوری ها و پلت فرم های موجود پیاده سازی نمود.
- سیاست های امنیتی می بایست اطلاعات لازم برای کارشناسان حرفه ای فن آوری اطلاعات در خصوص نحوه پیاده سازی کنترل های امنیتی به منظور حمایت از سیاست های امنیتی را ارائه نمایند.
- محدوده سیاست های امنیتی برای یک سازمان، به اندازه و پیچیدگی های آن بستگی دارد.
- اطلاع رسانی، یک عنصر امنیتی است که اغلب به فراموشی سپرده می شود. اکثر کاربران فعالیت های روزمره خود را با نادیده گرفتن مسائل امنیتی انجام می دهند. بدون وجود آموزش های لازم، اغلب پرسنل در ابتدا سعی می نمایند کار خود را بگونه ای که راحت تر می باشند انجام دهند و در مرحله بعد به امنیت انجام کار فکر کنند. تدوین سیاست ها و رویه های امنیتی بدون این که کاربران نسبت به آنان آگاهی داشته باشند، نتایج مثبت و مشهودی را در زمینه ایجاد یک سیستم ایمن به دنبال نخواهد داشت.
- تنظیم مقررات سیاست های امنیتی یک سازمان باید با توجه به رعایت قوانین و مقررات و یا الزامات قانونی قابل اجرا در سطح یک کشور باشد که این در رابطه با موسسات مالی و شرکت هایی که خدمات عمومی ارائه می دهند باید در این ضمینه بسیار دقیق و خاص باشد زیرا آنها در جهت منافع عمومی باید عمل کنند[۳،۴].

۲-۲- نیازمندی های اولیه یک سیاست

- باید قابل اجرا و پیگیری قانونی باشد
- باید مختصر و قابل فهم باشد
- باید تعادل بین محافظت و بهره وری سیستم را برقرار کند
- باید در دسترس افرادی که مشمول آن می شوند باشد

ویژگی های زیر توصیه مؤکد می شود:

- شرح دلایلی که این سیاست امنیت را لازم می کند
- توصیف آنچه در این سیاست پوشانده می شود
- تعریف مسئولیت ها
- شرح نحوه برخورد با تخلفات از آن سیاست

۳- ماهیت کنترل دسترسی

یکی از اصلی ترین وظایف امنیت، کنترل دسترسی به منابع است. کنترل دسترسی خیلی بیشتر از این است که تعیین کنیم که یک کاربر بتواند از یک فایل یا سرویس استفاده کند یا نه. اصطلاح کنترل دسترسی در واقع به کنترل بیشتر بر روی دسترسی به منابع سیستم اشاره دارد، کنترل دسترسی به مکانیزمی گفته می شود که از طریق آن بتوان نحوه دسترسی کاربران به منابع سیستم را محدود به نیازهایشان کرد، یعنی فرض را بر این می گذاریم که هویت کاربر مورد تایید قرار گرفته است و اکنون چگونگی نحوه دسترسی کاربر به منابع باید کنترل گردد. معمولاً صدور مجوز با استفاده از کنترل‌های دسترسی پیاده‌سازی می‌شود. برای حفاظت از اطلاعات بایستی دسترسی به اطلاعات کنترل شود و افراد غیرمجاز نباید توانایی دسترسی داشته باشند. بدین منظور روش‌ها و تکنیک‌های کنترل دسترسی لازم می‌باشد. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس‌تر و با ارزش‌تر نیاز به مکانیزم کنترل دسترسی قوی‌تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله احراز هویت و تصدیق هویت است. کنترل دسترسی در حقیقت در مورد رابطه بین اشیاء و موضوع ها صحبت می کند. انتقال اطلاعات از یک شیء به یک موضوع را دسترسی می نامند. دسترسی صرفاً یک موضوع منطقی و یا فنی نیست، که براحتی می تواند باعث افشاء اطلاعات شود و یا مشکلات خاص خود را ایجاد کند. یک موضوع یک موجودیت فعال محسوب می شود، این موجودیت فعال از طریق فرآیندی به نام دسترسی به دنبال بدست آوردن داده از قسمت های منفعل یا همان اشیاء هستند. یک موضوع می تواند شامل یک کاربر، یک برنامه، یک پایگاه داده، یک پروسس، یک فایل و ... باشد. یک

ISSN: 2745-3673
http://www.Rcsj.ir

شیء می تواند یک کاربر، فایل، کامپیوتر، پایگاه داده، پرینتر، دستگاه ذخیره سازی و از این قبیل باشد. موضوع همیشه موجودیتی است که اطلاعات یا داده ها را از، یا درباره اشیاء بدست می آورد، همچنین این موجودیت اطلاعات یا داده های ذخیره شده در اشیاء را می تواند تغییر یا اصلاح کند. اشیاء همیشه موجودیت هایی هستند که اطلاعات یا داده ها را ارائه می دهند و یا میزبان اطلاعات هستند. نقش بین اشیاء و موضوع ها را می توان ارتباط بین نرم افزار و پایگاه داده و یا یک فایل و پروسس آن تصور کرد که برای انجام یک عملیات یا وظیفه در کنار هم جمع شده اند. واژه کنترل دسترسی محدوده وسیعی از کنترل ها را در بر می گیرد که می تواند از مجبور کردن یک کاربر به استفاده از نام کاربری و رمز عبور معتبر برای ورود به سیستم تا جلوگیری از دسترسی کاربران به منابع خارج از محدوده دسترسی اعمال شده برای آنان باشد[۱۱،۱۲].

۴- هدف کنترل دسترسی

کنترل دسترسی به مکانیزمی گفته می شود که از طریق آن بتوان نحوه دسترسی کاربران به منابع سیستم را محدود به نیازهایشان کرد. که هدف اصلی در کنترل دسترسی جلوگیری از دسترسی غیرمجاز به اطلاعات بوده و روشی شناخته شده برای به اجرا در آوردن اهدافی نظیر محرمانگی، یکپارچگی و تائید هویت افراد و سیستم ها می باشد. یکی از دغدغه ها و چالش هایی که ذهن بشر را به خود مشغول کرده فراهم نمودن محیطی امن و تحت کنترل در مجموعه ایی بدون ایجاد محدودیت، درجهت ارتقای بُعد فکری آنان است تا بتوانند کلیه قسمتهای مجموعه و همچنین دسترسی افراد مختلف از جمله مراجعه کنندگان را کنترل نمایند. AAA متشکل از سه روش Authentication، Authorization و Accounting می باشد و باعث افزایش امنیت نرم افزار می گردد. Authentication روشی است که امکان شناسایی هر کاربر را با استفاده از پروتکل امنیتی که برای آن تعریف شده است برای دسترسی به نرم افزار فراهم می کند. Authorization به ما اجازه می دهد که سرویس هایی که هر کاربر امکان استفاده از آنها را دارد محدود کنیم و Accounting به ما امکان مشاهده سرویس هایی که کاربران به آنها دسترسی پیدا کرده اند را می دهد. افزایش تعداد سرورهای شبکه در پی راه اندازی سرویس های مختلف، Data Base های مختلف کاربران و سیاست های متنوع، دسترسی افراد را به منابع مختلف ایجاد خواهد کرد بطوریکه پس از مدتی جهت اضافه کردن کاربر جدید به سیستم، نیاز به تعریف آن در چندین سرور وجود خواهد داشت. این پراکندگی و لزوم اعمال سیاست های متمرکز ،مدیران شبکه را ناچار به اتخاذ تدابیری مؤثرتر می کند لذا تعریف و پیاده سازی AAA Server یکی از این تدبیرهاست که بر دسترسی کاربران به منابع شبکه ، مدیریت مستقیم و متمرکز نظارت خواهد داشت. AAA Server یک برنامه نرم افزاری سرور است که امکان دسترسی کاربران را با منابع کامپیوتری شبکه برقرار می کند. این برنامه برای شبکه های Enterprise سرویس های Authentication، Authorization و Accounting را فراهم می آورد. در واقع AAA Server با دسترسی شبکه ، سرورهای Gateway ، Database ها و جدول های اطلاعاتی کاربران در تعامل است.

۵- انواع کنترل دسترسی براساس روش پیاده سازی و اجرایی و عملیاتی

کنترل های دسترسی می توانند بر اساس روش پیاده سازی طبقه بندی شوند. در این حالت به سه طبقه بندی مدیریتی ، منطقی یا فنی و فیزیکی نقسیم بندی می شوند.

۵-۱ کنترل های دسترسی مدیریتی

کنترل مدیریتی عبارتند از سیاست ها، رویه ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول تایید شده است. کنترل های دسترسی مدیریتی خط مشی ها و دستورالعمل هایی هستند که توسط خط مشی امنیتی سازمان برای اجبار به پیاده سازی سراسری کنترل های دسترسی تعریف شده اند. کنترل‌های مدیریتی چارچوب روند امن کسب و کار و مدیریت افراد را تشکیل می دهد و بیشتر بر روی دو موضوع کارکنان و فعالیت های تجاری (مردم و خط مشی ها) تمرکز می کنند. این کنترل‌ها به افراد نحوه امن و مطمئن انجام کسب و کار را می گویند و نیز اینکه چگونه روال روزانه عملیات‌ها هدایت شود. برای مثال خط مشی ها، دستورالعمل ها، بررسی کردن عدم سوء پیشینه، طبقه بندی داده ها، آموزش های امنیتی، نظارت بر انجام کارها، کنترل کردن کارکنان و انجام تست های مختلف از انواع کنترل های دسترسی مدیریتی می باشند. نمونه‌های دیگر از کنترل‌های مدیریتی عبارتند از سیاست امنیتی شرکت‌های بزرگ، سیاست مدیریت رمز عبور، سیاست استخدام و سیاست‌های انضباطی. کنترل‌های مدیریتی، پایه ای برای انتخاب و پیاده سازی کنترل‌های منطقی و فیزیکی است. کنترل‌های منطقی و فیزیکی، پیاده سازی و ابزاری برای اعمال کنترل‌های مدیریتی هستند.

ISSN: 2745-3673
http://www.Rcsj.ir

۵-۲ کنترل های دسترسی منطقی یا فنی

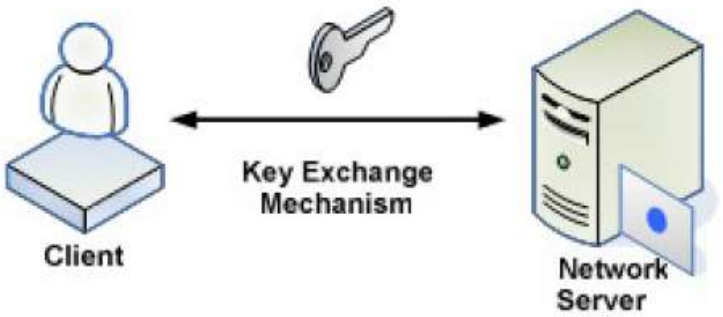
کنترل های دسترسی منطقی و کنترل های دسترسی فنی مکانیزم های سخت افزاری و نرم افزاری هستند که بوسیله محافظت از منابع و سیستم ها دسترسی به آنها را کنترل و مدیریت می کنند. برای مثال رمزنگاری، کارت های هوشمند ، رمزهای عبور، سیستم های تشخیص هویت Biometric ، لیست کنترل های دسترسی و پروتکل ها، فایروال ها، مسیریاب ها و سیستم های تشخیص نفوذ برخی از انواع کنترل های دسترسی منطقی یا فنی هستند، در این موضوع کنترل دسترسی فنی و منطقی را می توان در کنار هم استفاده کرد.

۵-۳ کنترل های دسترسی فیزیکی

کنترل های دسترسی فیزیکی حصارها و موانع فیزیکی هستند که از دسترسی مستقیم و غیر مجاز به سیستم ها و منابع جلوگیری می کنند. برای مثال گاردهای امنیتی، فنس ها، سیستم های تشخیص حرکت، درب های قفل شده، پنجره های مهر و موم شده، سیستم های روشنایی، سیستم های محافظت از کابل کشی، قفل های لپ تاپ، سگ های نگهبان، دوربین های امنیتی و سیستم های هشدار دهنده یا آلارم از انواع کنترل های دسترسی فیزیکی هستند[۶،۷].

۶- احراز هویت

یکی از بزرگترین چالش ها در زمینه شبکه ها، پشتیبانی کافی و به اندازه از سرویس های امنیتی برای ارتباطات و سرویس های فراهم شده می باشد. احراز هویت یک فرآیند تشخیص دیجیتالی است که یک موجودیت را در موجودیت دیگر شناسایی می کند. این موجودیت می تواند کاربر و موجودیت دوم سرور باشد. شناسایی معمولا براساس نام کاربری و کلمه عبور و یا شماره تلفن است. ایده احراز هویت بر این اساس است که هر کاربری دارای اطلاعات منحصر به فردی است که او را از دیگر کاربران متمایز می کند. فرآیند اعتبار سنجی یک کاربر یا یک وسیله مانند یک مسیریاب، سوییچ و ... می باشد. برای اتصال هر کاربر به شبکه یک نام کاربری و کلمه عبور نیاز است تا مشخص گردد چنین کاربری وجود دارد یا خیر؟ و اگر وجود دارد با ارائه کلمه عبور از صحت آن مطمئن شویم. برای تصدیق صحت کاربر علاوه بر کلمه عبور از امضاهای دیجیتال و شماره تلفن هم استفاده می شود. رایج ترین مدل های معماری برای برای احراز هویت، مدل احراز هویت دو قسمتی می باشد. این مدل زمانی بکار برده می شود که دو گره، یک کلاینت و یک سرور بدون هیچ واسطه ای بعنوان قسمت سوم مانند دروازه یا پراکسی، با هم ارتباط دارند. کلاینت مجبور است که شناسایی شود که برای این منظور به سرور دسترسی پیدا می کند [5].

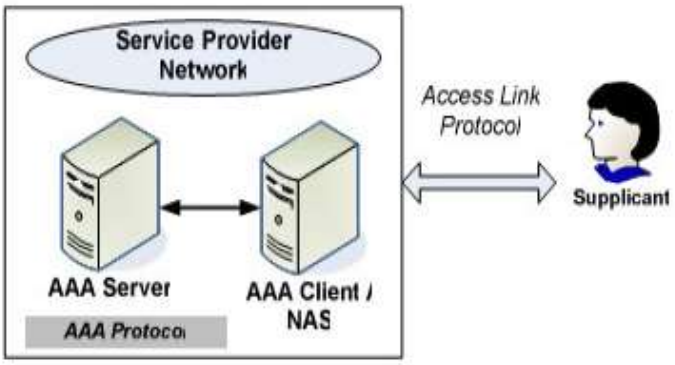


شکل ۶-۱ مدل دو بخشی احراز هویت

با توجه به تعداد زیاد کاربرانی که مایل به استفاده از شبکه می باشند و همچنین اندازه شبکه، مدل احراز هویت دو بخشی اصلاح شده و به مدل سه بخشی تبدیل شده است و این روش بدلیل احراز هویت موثرتر و رضایت بخش تر بوجود آمده است. کاربران درخواست خود را به شبکه می فرستند و سرور دسترسی به شبکه بعنوان یک کلاینت AAA عمل می کند و برای کلاینت ها درخواست اجازه دسترسی را صادر

ISSN: 2745-3673
http://www.Rcsj.ir

می کند سرور احراز هویت، مسئول و عامل واقعی در رابطه با دسترسی به کاربران است. عملیات سرور AAA براساس پایگاه داده و مشخصات کاربر از قبیل نام کاربران، کلمه عبور، حسابداری، مورد بررسی قرار می گیرد. سرور AAA مشخصات کاربر را با پایگاه داده مرکزی خود مقایسه کرده و در صورتیکه تطبیق داشته باشد دسترسی داده می شود و در غیر این صورت دسترسی رد خواهد شد [5,8] .



شکل ۶-۲ مدل سه بخشی احراز هویت

در شبکه های خصوصی یا کلی نظیر اینترنت احراز هویت با استفاده از نام کاربری و کلمه عبور صورت می گیرد. دانستن کلمه عبور در واقع دسترسی کاربر را به منابع مورد نیازش گارانتی می کند. عمل احراز هویت، در طراحی شبکه هایی با حجم کم و متوسط عموماً توسط تجهیزات مسیریابی و یا دیواره های آتش انجام می گیرد . علت استفاده از این روش، مجتمع سازی و ساده سازی پیاده سازی عمل احراز هویت است. با استفاده از امکانات موجود نیاز به استقرار یک سیستم مجزا برای صدور پذیرش هویت کاربران مرتفع می گردد. از سوی دیگر در شبکه هایی با حجم و پیچیدگی نسبتاً بالا، عموماً با توجه به پردازش بالای مختص عمل احراز هویت سیستمی بصورت مستقل و مجزا به این امر اختصاص می یابد. از نقص های این سیستم می توان به دزدیده شدن کلمه عبور، اتفاقی لو رفتن و فراموش کردن آن اشاره کرد.
فعال نمودن احراز هویت در چهار مرحله انجام می شود:

- فعال نمودن AAA بر روی سخت افزارهای مورد نظر
- ایجاد بانک اطلاعاتی از کدهای کاربری کاربران یا تجهیزات شبکه به همراه کلمه های عبور
- ایجاد فهرست روش انجام عمل احراز هویت. این فهرست ها به تعیین روش مورد نظر برای عمل احراز هویت اختصاص دارند.
- اعمال فهرست های روش ساخته شده از مرحله قبل

همان گونه ذکر شد، این بانک اطلاعاتی می تواند داخل تجهیزات مورد استفاده در شبکه های با حجم کم پیاده سازی شود. در شبکه های با حجم نسبتا بالا که در آنها نیاز به استفاده از سیستمی مختص احراز هویت احساس می شود، تجهیزات فعال شبکه به گونه ای پیکربندی می شوند که عمل احراز هویت را با استفاده از پایگاه های داده ای مستقر بر روی سیستم های مختص این فرآیند، انجام دهند. به عنوان اولین پردازش، Authentication راهی را جهت تشخیص هویت کاربران فراهم می آورد که بطور معمول اینکار با وارد کردن کلمه کاربری و کلمه عبور صحیح قبل از برقراری دسترسی خاص صورت می گیرد[۹].

۷- نتیجه گیری

در این مقاله به مفهوم امنیت در سازمان ها پرداختیم و به بررسی احراز هویت و کنترل دسترسی پرداختیم، در حقیقت احراز مجوز به دومین A در AAA اشاره دارد. احراز مجوز فرآیندی است که طی آن به کاربران و یا تجهیزات متقاضی دسترسی به منابع، امکان استفاده از منبع یا منابع مستقر بر روی شبکه داده می شود. بعد از احراز هویت تعیین می کند که کاربر اجازه دسترسی به کدام منابع و سرویس های شبکه را دارد و از کدامیک منع می شود. دسترسی کاربر به سطح احراز مجوز کاربر بستگی دارد. پیرو احراز هویت صورت گرفته شده احراز مجوز جهت انجام وظیفه های خاص پس از ورود به سیستم صورت می گیرد. به عنوان مثال کاربر تصمیم به اجرای دستوراتی روی

ISSN: 2745-3673
http://www.Rcsj.ir

سیستم دارد، پردازش احراز مجوز مشخص می کند که آیا کاربر اجازه اجرای آن دستورات خاص را دارد یا خیر. به بیان ساده تر احراز مجوز پردازشی است برای کاربر که سیاست هایی خاص را در رابطه با نوع فعالیت، کیفیت، منابع و سرویس ها برقرار می کند.

تشکر و قدردانی

با تشکر از جناب آقای دکتر افشین رضاخانی، خانم دکتر لیلا ریخته چی

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] A. Cau, H. Janicke, B. Moszkowski, “Verification and enforcement of access control policies”, Form Methods Syst Des, De Montfort University, pp. 333-327, May 2013.

[۲] مصطفی حق جو، علی‌اصغر صفائی. "بانک اطلاعات علمی- کاربردی"، جلد دوم، انتشارات دانشگاه علم و صنعت ایران، ۱۳۸۷.

[3] M. Koch, L. V. Mancini, F. P. Presicce, “Conflict Detection and Resolutionin Access Control Policy Specifications”, Freie Universit¨at Berlin, Univ. di Roma La Sapienza, George Mason University, LNCS 2303, pp. 223–238, 2002.

[4] M. Sandhu, R.S. Ferraiolo, D.F. and Kuhn, D.R. ‘‘The NIST model for rolebased access control: toward a unified standard’’, In Proceeding of 5th ACM Workshop on Role-Based Access Control, pp. 47–63, Berlin, Germany (2000).

[5] A. P. Maranda, R. Rutkowska, “Implementation of Usage Role-Based Access Control Approach for Logical Security of Information Systems”, Institute of Information Technology, Lodz University of Technology, Poland, 2014.

[6] V. F. Crescini and Y. Zhang ،“a system for dynamic access control”, international journal of advertising, Australia, pp, 145-165, November 2005.

[7] R. Gupta, M. Bhide, “A Generic XACML Based Declarative Authorization Scheme for Java”, Verlag Berlin Heidelberg, pp. 44–63, 2005.

[8] Urs Hengartner and Peter Steenkiste, "Access Control to Information in Pervasive Computing Environments", Ninth Workshop on Hot Topics in Operating Systems (HotOS IX), ACM, May 2003, pages 157-162.

[9] M. Kudo, J. Myllymaki, H. Pirahesh and N. Qi, "A Function-Based Access Control Model for XML Databases", CIKM’05 of ACM, page 115-122, November 2005.