ارزیابی امنیتی سامانه‌های کنترل از طریق شبکه

پایان‌نامه کارشناسی ارشد

مهندسی برق مخابرات

استاد راهنما: دکتر سید محمدتقی المدرسی

استاد مشاور : دکتر فضل اله ادیب نیا

نویسنده: سید علی مصباحی فرد

مهرماه ۱۳۹۲

تقدیم به

پدر

مادر

برادر

بسمه تعالی

سپاس خداوند یکتا را سزاست که به حکمت کامل جهان خلقت را آفرید و با علم تامّه آن را پرورید. آسمان را وسعتی بیکران داد و با ستارگان و اقمار گوناگونِ هزاران رنگ تزیین کرد و به قدرت مطلق منظم نمود. هریک را جایگاهی معین بخشید و هر کدام را حرکتی مخصوص داد. و از کرامت بیکران دست رحمت بی‌حد بر سر زمین کشید و گوهر حیات در دل سیاره خاک مستتر ساخت. نگین فیروزه عرش وخاک پر از نقش فرش. آسمان مسخر پرندگان زمین جایگاه چرندگان و آب خانه ماهیان. هر یک به رنگی آراسته و به دیگری وابسته.

و این همه طرح و نقش و رنگ و لعاب و این همه راز و رمز و نظم تا آن وجود یگانه در آفرینش متجلی گردد و کلمه حق بر زبان بندگان جاری شود

لا اله الا الله الذی له العزت و الجلال و له الحمد و الثناء

چکیده

سامانه‌های کنترل تحت شبکه یا به اختصار NCS شامل آن دسته از سیستم‌های کنترلی هستند که در آن‌ها ارتباط میان کنترل‌کننده و دستگاهاز طرق یک شبکه مخابراتی برقرار است. اثرات ناشی از این شبکه مخابراتی بر کارایی سیستم‌های کنترل تحت شبکه درهنگام بررسی و طراحی این سامانه‌ها باید مورد ارزیابی قرار گیرد. از جمله مسائل مربوط به سامانه‌های کنترل تحت شبکه مسائل امنیتی است زیرا که امکان دسترسی افراد مختلف به این شبکه مخابراتی (خصوصاً اینترنت) که سامانه بر روی آن در حال کار است خود زمینه خرابکاری‌ها و حملات خطرناکی را به این سامانه‌ها که بسیاری از آن‌ها زیرساخت‌های مهم صنعتی را کنترل می‌کنند فراهم می‌آورد. از این رو نه تنها بررسی اثرات حملات اهمیت دارد بلکه ارائه روش‌های جدید و امنیتی متناسب با نیازها و خصوصیات سامانه‌های کنترل تحت شبکه نیز حائز اهمیت است.

آنچه در این پایان‌نامه ارائه می‌شود یک الگوریتم رمزنگاری متقارن متناسب با حجم کم داده در سامانه‌های کنترل بر علیه حملات تقلب است که با تغییر دائمی کلید و مقادیر عناصر ماتریس جایگشت ضمن برآورده کردن یکپارچگی داده و داشتن سرعت زیاد، امنیت قابل قبولی را نیز دارد و می‌تواند در مقابل حملات تقلب کارایی سامانه را به حد سامانه ایده آل تحت حمله (یعنی جایی که اثر سیستم امنیتی برای مهاجم بسیار زیاد و برای خود سامانه تقریباً ناچیز باشد) نزدیک نماید.

فهرست

فهرست اشکال

فهرست جداول

فصل اول:

مقدمه

مهندسی کنترل شاخه‌ای از مهندسی است که هدف از آن تحلیل خروجی یک سامانه بر اساس تمام پارامترهای تأثیرگذار، یا طراحی یک سامانه به هدف دست‌یابی به خروجی‌های قابل پیش‌بینی و قابل‌کنترل بر اساس ورودی‌های معین به بهترین نحو است. برای این کار مهندسان کنترل به بررسی و تحلیل نمونه‌های ریاضی حاکم بر سامانه که تمام پارامترهای اثرگذار در ورودی و خروجی را شامل می‌شود می‌پردازند چنین تحلیل‌هایی هم در حوضه فرکانس و هم در زمان انجام می‌شود تا الگوهایی از رفتارهای سامانه به دست آید. مسئله مهم در مورد این مدل‌های ریاضی آن است که معمولاً از جزئیات و نحوه ساخت مستقل‌اند. به بیان دیگر یک سامانه صرفاً مکانیکی و یا یک سامانه صرفاً الکتریکی و یا شیمیایی یا بیولوژیکی ممکن است دارای یک مدل ریاضی حاکم مشابه باشند و این فرصتی را برای ساخت یک سیستم کنترل به شکل مستقل یا به صورت ترکیبی از ابزارآلات مکانیکی، الکتریکی، شیمیایی و بیولوژیکی فراهم می‌کند.

با روی کار آمدن سیستم‌های الکترونیکی و خصوصاً سیستم‌های رقمی نه تنها در عرصه ساخت سیستم‌های کنترل تحول ایجاد شد و سامانه‌های خودکار مبتنی بر ساختارهای الکتریکی قابل برنامه‌ریزی و بی‌نیاز از نظارت دقیق و لحظه‌ای انسانی به وجودآمد بلکه مهندسی کنترل نیز وارد عرصه‌ی کنترل رقمی شد که در آن مدل‌های ریاضی خاصی به منظور بیان روابط میان ورودی‌ها و خروجی‌های گسسته ایجاد شدند. به علاوه نسل‌های جدیدی از کنترل‌کننده‌های هوشمند مانند سیستم‌های فازی و عصبی نیز عملاً پا عرصه وجود نهادند.

در عرصه ساخت اهمیت موضوع، طراحی دقیق و ساخت دقیق سیستمی است که خروجی آن تا حد امکان با آنچه که در نقشه سیستم کنترل طراحی شده است یکسان باشد. در واقع آنچه

از جزئیات که ممکن است در هنگام بیان و تحلیل مدل ریاضی نادیده گرفته‌شده در اینجا باید لحاظ گردد. حدود نهایی ممکن برای ورودی و خروجی، توانایی‌های فناورانه موجود و تفاوت عملکرد و سرعت پاسخ ابزارآلات موجود با مقادیر مدل از جمله این موارد هستند.

اگرچه کنترل رقمی و مبتنی بر رایانه یک گام مهم در کنترل دستگاه‌ها و سیستم‌ها به شمار می‌رفت اما ایجاد فناوری شبکه‌های مخابراتی و بهبود وضعیت ارتباطات از راه دور توانست امکان کنترل از راه دور را در اختیار بگذارد که خود در کنار سیستم‌های رایانه‌ای رقمی عرصه جدیدی در سیستم‌های کنترل به شمار می‌رود. چنین سامانه‌های مبتنی بر شبکه مزیت‌هایی مانند کاهش هزینه، کنترل همزمان چند بخش از طریق یک مکان و بالا رفتن دقت را به همراه داشته است.

شکل ۱-۱: نمایی از یک سیستم کنترل تحت شبکه ایده آل. جایی که تمام ابزارهای قابل کنترل از طرق شبکه در دسترس و قابل‌کنترل هستند **[1]**

از جمله کاربردهای این‌گونه سامانه‌های کنترلی که به سامانه‌های کنترلی از طریق شبکه مشهورند و از ترکیب ابزارهای هوشمندی که قابلیت پویش محیط و یا اثرگذاری در آن را دارند و از طریق شبکه مخابراتی به منظور دستیابی به یک هدف جمعی با یکدیگر در ارتباطاند، شبکه‌های حسگرها و عامل‌های بی‌سیم به منظور پایش زیست‌محیطی، شبکه وسایل نقلیه، شبکه دوربین‌ها

به منظور اقدامات حفاظتی و مراقبتی، شبکه دوربین‌های فیلم‌برداری هماهنگ، و شبکه‌های هوشمند توزیع نیرو را می‌توان نام برد (به تصوری ۱-۱ توجه کنید)[2] .

اما چالش‌های اساسی آن مانند مسئله پایداری [3]، محدودیت پهنای باند، گم شدن بسته‌های اطلاعاتی و تأخیر تصادفی شبکه مخابراتی و نیز چالش‌های امنیتی هم مهندسان کنترل و هم مهندسان مخابرات را به خود مشغول کرده است[4]. البته امروزه سخت‌افزارهای شبکه آن‌چنان پیشرفت کرده‌اند که بتوانند از لحاظ تأخیر و نرخ پایین گم شدن بسته‌ها و توانایی در انتقال حجم داده مورد نیاز برای یک سیستم کنترل تحت شبکه قابل‌اعتماد باشند. اما امنیت یک سامانه کنترل به جهت ارتباط تنگاتنگ آن با ابزارآلات و مکان‌های حیاتی و مهم مانند سیستم‌های کنترل آب و فاضلاب، سیستم‌های کنترل شبکه نیرو و گاز و یاسامانه‌های کنترل نیروگاه‌های هسته‌ای و نیز سامانه‌ای کنترل شبکه‌های ریلی نه تنها شامل مسائلی همچون محافظت در مقابل دزدی اطلاعات ویا تغیر غیرمجاز داده‌ها می‌شود بلکه فراتر از آن باید شامل ایجاد شبکه‌های پشتیبان مخابراتی و نیرو، سیستم‌های تشخیص نفوذ، سیستم‌عامل‌های مناسب، آنتی ویروس‌های مناسب و به‌روز و سایر اقدامات امنیتی نرم‌افزاری و سخت‌افزاری و همچنین بازبینی مستمر و برنامه‌ریزی‌شده سیستم‌های سخت‌افزاری و نرم‌افزاری باشد که خود مستلزم به‌کارگیری افراد مجرب و کارآمد در زمینه امنیت شبکه است. به علاوه می‌بایست قبل از مرحله اجرا تمام اثرات ناشی از خرابی شبکه مخابراتی یا حملات عمدی و غیر عمدی سایبری ممکن به سامانه کنترلی بر خروجی آن مورد بررسی قرارگرفته تا علاوه بر اتخاذ تمهیدات لازم برای جلوگیری از آن‌ها نسبت به آمادگی لازم در مقابل خروجی‌های ناخواسته و مضر اقدامات لازم انجام شود. خصوصاً آنکه بر خلاف گذشته که این سامانه‌ها بر پایه شبکه‌های اختصاصی ساخته می‌شدند، امروزه با گسترش دسترسی به شبکه‌های عمومی خصوصاً اینترنت علاقه‌مندی به اجرای سامانه‌های کنترلی بر اساس این شبکه‌های عمومی در حال گسترش است و در نتیجه مخاطرات و تهدیدات ممکن آن نیز افزایش پیدا کرده است.

باید توجه داشت که ازدست رفتن کنترل در هر سامانه کنترلی ممکن است موجب ایجاد آسیب‌های غیرقابل‌جبران انسانی مالی زیست‌محیطی یا به خطر افتادن امنیت ملی یک کشور گردد. از این رو در طول سالیان گذشته دستگاه‌های مختلف دولتی یا خصوصی استانداردها و پارامترهایی را برای امنیت سیستم‌های کنترل تعریف کرده‌اند.

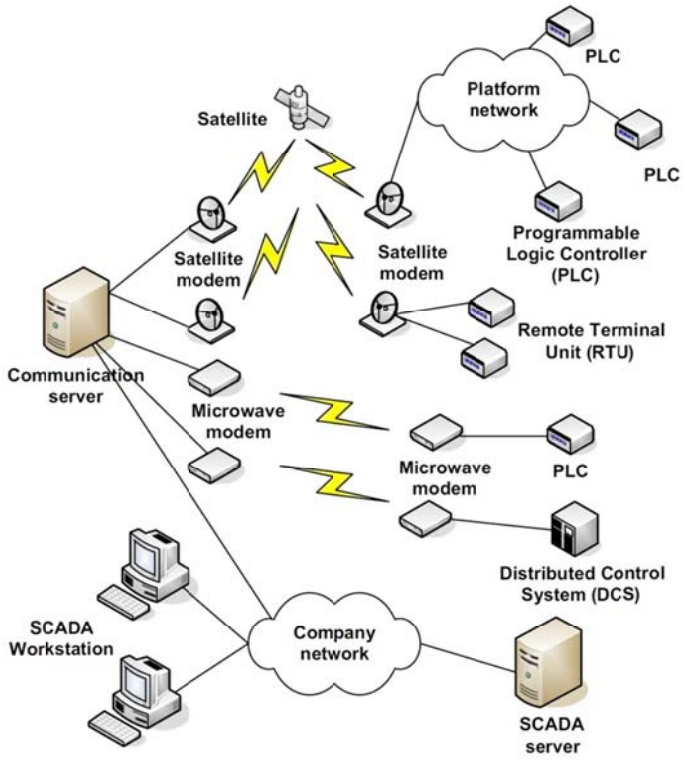
در سیستم کنترل تمام داده‌ها احتیاج به رمزنگاری ندارند اما اغلب داده‌ها به احراز هویت نیازمندند. از یک دیدگاه عملی تفاوت میان این دو آن است که هزینه رمزنگاری داده در مقایسه با هزینه احراز هویت سری بسیار قابل‌ملاحظه‌تر است، خصوصاً در ابزارهای پایین‌دستی نهایی مانند RTU[1] و PLC[2] درسیستم‌های SCADA[3] (به تصویر ۱-۲ توجه کنید). نمونه‌هایی از داده‌هایی که باید رمز شوند شامل کلمات عبور و نام‌های کاربری وامثال آن است. درحالی‌که داده در یافتی از یک حسگر معمولاً به نهاننگاری نیازمند نیست. استفاده از ابزارات BITW[4] در شبکه‌هایEthernet و ارتباطات سریال (rs232) زمینه را برای به‌روزرسانی سخت‌افزارهای موجود با رمزنگاری بدون نیاز به جایگذاری دستگاه‌ها وسخت‌افزارها فراهم می‌آورد. باید توجه داشت که به‌روزرسانی سیستم زمانی کاملاً موثر خواهد بود که تمام ابزارت بتوانند خود را با آن هماهنگ کنند[5].

با گسترش شبکه‌های عمومی و اینترنت نه تنها سامانه‌ای کنترل صنعتی گسترش پیداکرده‌اند بلکه سامانه‌های جدید کنترلی تحت شبکه که حساسیت بسیار بیشتری به تأخیر دارند مانند سیستم‌های اتاق عمل از راه دور نیز در حال ظهورند و سؤال اساسی آن است که آیا روش‌های گذشته برای مقابله با تهدیدات امنیتی در شبکه برای این سامانه‌ها نیز مناسب‌اند؟ گرچه برخی پارامترهای کلی در ایجاد امنیت را می‌توان دراینجا نیز به کاربرد اما به نظر می‌رسد برخی ازروش‌ها (مانند رمزنگاری‌های معمول) کند تر از آن هستند که بتوان در این‌گونه سامانه‌ها که محتاج سرعت پاسخ‌دهی بالا هستند استفاده کرد. به علاوه برای ایجاد امنیت اطلاعات که شامل

---

[1]Remote Terminal Unit
[2]Programmable Logic Controller
[3]Supervisory And Data Acusition
[4]Bump in the Wire

محرمانگی، یکپارچگی، تصدیق هویت و عدم انکار است، بعضاً بایدالگوریتم‌های متفاوتی مانند استفاده از کدهای درهم‌ساز و اضافه کردن برچسب زمانی استفاده کرد که خود موجب بالا رفتن تأخیر می‌شود؛ بنابراین به نظر می‌رسد که لازم است روش جدیدی برای امنیت داده ارائه گردد که ضمن داشتن سرعت مناسب به تواند نیازهای امنیت اطلاعات یک سامانه کنترل تحت شبکه خصوصاً تصدیق هویت و یکپارچگی را فراهم کند. ایده‌آل‌ترین حالت آن است که تمهیدات امنیتی برای کاربران مجاز اصلاً به چشم نیاید (بر خروجی سیستم کنترل اثرگذار نباشد) درحالی‌که برای کاربران غیرمجاز و مهاجمین حصاری غیرقابل نفوذ ایجاد کند.



شکل ۱-۲: سیمای کلی یک سیستم SCADA**[6]**

در فصل دوم به بررسی مسائل امنیتی در شبکه‌های رایانه‌ای می‌پردازیم، در فصل سوم مروری کلی بر مفاهیم رمزنگاری را خواهیم گفت و در فصل چهارم مروری بر استانداردهای موجود در مورد NCS و تحقیقات انجام‌شده توسط دیگران را ارائه خواهیم داد. و در فصل پنج و شش الگوریتم رمزنگاری‌ای را متناسب با نیازمندی به سرعت و یکپارچگی در سامانه‌های کنترل تحت شبکه خصوصا سامانه‌های کنترلی آنی بیان خواهیم کرد و نتایج آن را خواهیم دید.

فصل دوم:

مفاهیم امنیت شبکه

از دیدگاه امنیت اگر رخداد ناخوشایند و خطرناکی به یکی از رده‌های "دسترسی غیرمجاز به داده‌ها "، "نشت اطلاعات محرمانه "، " از دسترسخارج شدن خدمات یک سرویس‌دهنده "، "تغیر مخفیانه داده‌ها "، " سرقت داده‌ها "، "نابود شدن داده‌ها "، " جعل داده‌ها"، "اختلال در عملکرد صحیح ماشین کاربر" و هر نوع "تعرض به حریم خصوصی داده‌ای یک کاربر" تعلق بگیرد آنگاه امنیت داده عبارت است از مجموعه تمهیدات و اقداماتی که شامل یکی از بندهای زیر باشد:

۱ تمهیداتی که اطمینان می‌دهند رخداد ناخوشایندی هرگز اتفاق نمی‌افتد.

۲ تمهیداتی که امکان وقوع رخداد خطرناک را کاهش می‌دهند.

۳ تمهیداتی که نقاط حساس به خرابی و حمله را در سطح شبکه توزیع کند.

۴ تمهیداتی که اجازه می‌دهند شرایط بعد یک رخداد خطرناک در اسرع وقت و با کمترین هزینه و با حداقل اثرات نامطلوب به حالت عادی بازگردد.

با توجه به تعاریف بالا حمله تلاشی است خطرناک یا غیر خطرناک تا یک منبع قابل‌دسترسی از طریق شبکه، به گونه‌ای مورد تغییر یا استفاده قرار گیرد که مورد نظر نبوده است.

حملات شبکه را به سه دسته عمومی تقسیم می‌توان تقسیم کنیم:

۱ دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه

۲ یا دست‌کاری غیرمجاز اطلاعات بر روی یک شبکه

۳ حملاتی که منجر به اختلال در ارائه سرویس می‌شوند و اصطلاحاً Denial of Service[1] نام دارند.

[1] Dos Attacks

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 می‌توان 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 رایانه‌های 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 در مسیریاب‌ها[1] است. منابع شبکه را نیز می‌توان تجهیزات انتهایی مانند مسیریاب و دیوار آتش یا سازوکارهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبکه، حفاظت از شبکه در مقابل حملات فوق است [4].

امنیت شبکه[2] پردازه‌ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می‌شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تأییدشده‌اند:

۴ شناسایی بخشی که باید تحت محافظت قرار گیرد.

۵ تصمیم‌گیری درباره مواردی که باید در مقابل آن‌ها از بخش مورد نظر محافظت کرد.

۶ تصمیم‌گیری درباره چگونگی تهدیدات

۷ پیاده‌سازی امکاناتی که بتوانند از دارایی‌های شما به شیوه‌ای محافظت کنند که از نظر هزینه به صرفه باشد.

۸ مرور مجدد و مداوم پردازه و تقویت آن در صورت یافتن نقطه ضعف.

به علاوه چالش‌هایی نیز در مورد اجرای یک سیستم امنیتی دریک سامانه کنترلی تحت شبکه وجود دارد از جمله آنکه بسته‌های نرم‌افزاری امنیتی به منظور به‌روزرسانی نرم‌افزاری و سخت‌افزاری امنیتی یک سیستم کنترل شبکه معمولاً با آن ناهم‌خوان هستند یا مستلزم اقدامات اولیه‌ای می‌باشند؛ مثلاً لازم است برنامه‌ریزی‌هایی برای جدا کردن یک سیستم از شبکه انجام شود

[1] Router
[2] Network Security

یا حتی از لحاظ اقتصادی عملیات به‌روزرسانی مورد بررسی قرار گیرد. عملکرد برخی از ابزارها ونرم‌افزارهای امنیتی ممکن است بر کارایی سیستم کنترل اثر نامطلوب گذارد.

۲.۱ منابع شبکه

در یک شبکه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه‌ای از منابع شبکه را معرفی می‌کند که باید در مقابل انواع حمله‌ها مورد حفاظت قرار گیرند.

۱ تجهیزات شبکه مانند مسیریاب‌ها، سوئیچ‌ها و دیوارهای آتش.

۲ اطلاعات عملیات شبکه مانند جداول مسیریابی و پیکربندی لیست دسترسی که بر روی روتر ذخیره‌شده‌اند.

۳ منابع نامحسوس شبکه مانند عرض باند و سرعت.

۴ اطلاعات و منابع اطلاعاتی متصل به شبکه مانند پایگاه‌های داده و سرورهای اطلاعاتی.

۵ پایانه‌هایی[1] که برای استفاده از منابع مختلف به شبکه متصل می‌شوند.

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

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

مجموعه فوق به عنوان دارایی‌های یک شبکه قلمداد می‌شود.

۲.۲ تحلیل خطر

پس از تعیین دارایی‌های شبکه و عوامل تهدیدکننده آن‌ها، باید خطرات مختلف را ارزیابی کرد. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطای ممکن محافظت کرد، اما امنیت ارزان به دست نمی‌آید؛ 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 عامل اصلی در تحلیل خطر عبارت‌اند از:

[1] Terminal

۱ احتمال انجام حمله

۲ خسارت وارده به شبکه در صورت انجام حمله موفق

۲.۳ سیاست امنیتی

در دنیایی که وجه مشخصه آن فناوری سطح بالا و ارتباطات گسترده می‌باشد، هر سازمانی نیاز به سیاست‌های امنیتی که مدبرانه تدوین‌شده باشند دارد. در هر لحظه خطرات مختلفی از بیرون و درون سازمان توسط رخنه‌گرها[1]، رقبا و یا کشورهای خارجی منافع سازمان را تهدید می‌کند. هدف سیاست‌های امنیتی تعریف روال‌ها، راهنماها و تمریناتی است که امنیت را در محیط سازمان برقرار و مدیریت می‌نماید. با اجرای دقیق سیاست‌های امنیتی، سازمان‌ها می‌توانند تهدیدات را کاهش دهند.

سیاست امنیتی یک سازمان سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فناوری ارتباطات را بیان می‌نماید. سیاست امنیتی باید عمومی و در حوزه دید کلی باشد و به جزئیات نپردازد. جزئیات می‌توانند طی مدت کوتاهی تغییر پیدا کنند اما اصول کلی امنیت یک شبکه که سیاست‌های آن را تشکیل می‌دهند ثابت باقی می‌مانند. به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، بدین معنا که فرایند تکمیل و اصلاح آن هیچ‌گاه متوقف نشده، متناسب با تغییر فناوری و نیازهای کاربران به‌روز می‌شود.

چنین سندی شامل 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 سیاست‌های امنیتی و راه‌کار به‌روزرسانی آن‌ها می‌باشد. بهترین روش برای دستیابی به امنیت اطلاعات، فرموله نموده سیاست امنیتی است. مشخص نمودن سرمایه‌های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر اینکه چه افرادی به چه سرمایه‌هایی دسترسی دارند) در اولین گام باید انجام شود.

---

[1] هکر

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 تصمیم‌گیری برای پیکربندی و استفاده از سیستم‌ها یاری رساند.

شکل ۲-۱: شمای کلی سیاست‌های امنیتی**[5]**

در 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 زمینه‌ای را به وجود آورد که هرگونه تضاد احتمالی را حل و فصل کند.

برای تدوین سیاست امنیتی پس از تحلیل ریسک‌های سازمان، می‌توان به روش‌هایی که دیگران برگزیده‌اند متوسل شد. معمولاً تجارب مفیدی که قبلاً در صنایع مشابه انجام‌شده و نتایج خوبی از آن‌ها نتیجه شده است به صورت عمومی گزارش‌شده و در قالب مقالات تخصصی ارائه می‌گردند. استانداردهای شناخته‌شده‌ای نیز برای این کار وجود دارد که می‌توان از آن‌ها هم بهره گرفت. بهترین سیاست امنیتی در شرایطی تدوین می‌گردد که مدیریت سازمان سیاست کلی را ارائه نموده و یا دستور پیاده‌سازی اصول امنیتی را در سازمان صادر کند. تدوین‌کنندگان سیاست سازمان باید فعالیت خود را بر پایه اصول و استانداردهای صنعتی مانند ISO17799 و یا HIPAA

انجام دهند. رویه‌ها، راهنماها و تجربیات، پایه‌ای برای ایجاد و توسعه فناوری امنیتی در سازمان‌های مختلف هستند [5].

سیاست‌های امنیتی را می‌توان به طور کلی به دو دسته تقسیم کرد:

۱ مجاز (Permissive): هر آنچه به طور مشخص ممنوع نشده است، مجاز است.

۲ محدودکننده (Restrictive): هر آنچه به طور مشخص مجاز نشده است، ممنوع است.

معمولاً ایده استفاده از سیاست‌های امنیتی محدودکننده بهتر و مناسب‌تر است چون سیاست‌های مجاز دارای مشکلات امنیتی هستند و نمی‌توان تمامی موارد غیرمجاز را برشمرد.

۲.۴ ساختار سیاست های امنیتی

ساختار سیاست امنیتی مرکب از اجزاء زیر است:

۱ عبارتی در رابطه با موضوع سیاست

۲ چگونگی اجرای سیاست در محیط سازمان

۳ نقش و مسئولیت افراد مختلف تأثیرگذار در سیاست

۴ سیاست به چه میزان انعطاف‌پذیر است؟

۵ اعمال، فعالیت‌ها و فرایندهای مجاز و غیرمجاز

۶ موارد سخت‌گیری و عدم انعطاف سیاست

۲.۵ طرح امنیت شبکه

با تعریف سیاست امنیتی به پیاده‌سازی آن در قالب یک طرح امنیت شبکه می‌رسیم. المان‌های تشکیل‌دهنده یک طرح امنیت شبکه عبارت‌اند از:

۹ ویژگی‌های امنیتی هر دستگاه مانند کلمه عبور مدیریتی و یا به‌کارگیریSSH

۱۰ فایروال‌ها

۱۱ مجتمع کننده‌هایVPN برای دسترسی از دور

۱۲ تشخیص نفوذ

۱۳ سرورهای امنیتیAAA[1] و سایر خدمات AAA برای شبکه

۱۴ سازوکارهای کنترل دسترسی و محدودکننده دسترسی برای دستگاه‌های مختلف شبکه

۲.۶ نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یک شبکه امن ایفا می‌کند. در واقع یکی از بهترین شیوه‌های دفاع در مقابل حملات شبکه، طراحی امنیت شبکه به صورت منطقه‌ای و مبتنی بر توپولوژی است و یکی از مهم‌ترین ایده‌های مورد استفاده در شبکه‌های امن مدرن، تعریف نواحی و تفکیک مناطق مختلف شبکه از یکدیگر است. تجهیزاتی که در هر ناحیه قرار می‌گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن، تأمین می‌کند. همچنین منطقه بندی یک شبکه باعث ایجاد ثبات بیشتر در آن شبکه نیز می‌شود. نواحی امنیتی بنا بر راهبُردهای اصلی ذیل تعریف می‌شوند.

تجهیزات و دستگاه‌هایی که بیش‌ترین نیاز امنیتی را دارند (شبکه خصوصی) در امن‌ترین منطقه قرار می‌گیرند. معمولاً اجازه دسترسی عمومی یا از شبکه‌های دیگر به این منطقه داده نمی‌شود. دسترسی با کمک یک دیواره آتش و یا سایر امکانات امنیتی مانند دسترسی از دور امن[2] کنترل می‌شود. کنترل شناسایی و احراز هویت و مجاز یا غیرمجاز بودن در این منطقه به شدت انجام می‌شود.

سرورهایی که فقط باید از سوی کاربران داخلی در دسترس باشند در منطقه‌ای امن، خصوصی و مجزا قرار می‌گیرند. کنترل دسترسی به این تجهیزات با کمک دیواره آتش انجام می‌شود و دسترسی‌ها کاملاً نظارت و ثبت می‌شوند.

[1] Authentication, Authorization, Accounting
[2] SRA: Secure Remoat Acsess