به نام خدا

وزارت علوم، تحقیقات، و فناوری

پژوهشگاه علوم و فناوری اطلاعات ایران

(ایرانداک)

خلاصهٔ گزارش طرح پژوهشی سازمانی

عنوان طرح پژوهشی

ارزیابی پیکربندی امنیتی در زیرساخت شبکه پژوهشگاه علوم و فناوری اطلاعات ایران

تاریخ شروع طرح پژوهشی	۱۳۹۹/۰۵/۲۹	**تاریخ پایان طرح پژوهشی**	۱۴۰۰/۰۸/۱۷
نام و نام خانوادگی مجری طرح پژوهشی	امیر حسین صدیقی		
نام و نام خانوادگی همکاران طرح پژوهشی			

دربارهٔ طرح پژوهشی

امنیت سایبری به معنای محافظت از سیستم‌ها، شبکه‌ها، و برنامه‌ها در برابر حملات سایبری است. این حملات معمولاً با هدف دستیابی، تغییر یا از بین بردن اطلاعات حساس، اخاذی پول از کاربران، و یا وقفه در فرآیندهای سازمان انجام می‌شوند. امروزه انجام اقدامات مؤثر در زمینه امنیت سایبری چالش‌برانگیز شده است زیرا تعداد دستگاه‌ها نوعا بیش از تعداد افراد سازمان است و مهاجمان نیز هر روز به شیوه تازه‌ای اقدام به حمله می‌کنند. بنابراین ارزیابی و تشخیص آسیب‌پذیری‌های امنیتی برای سازمان‌ها از اهمیت خاصی برخوردار گشته است. یکی از آسیب‌پذیری‌های مهم، وجود نقص امنیتی در پیکربندی زیرساخت شبکه یک سازمان است.

در این پژوهش قصد داریم تا به ارزیابی پیکربندی امنیتی زیرساخت شبکه پژوهشگاه علوم و فناوری اطلاعات ایران بپردازیم. در این راستا ابتدا با کمک کارشناسان پژوهشگاه اقدام به شناسایی دارایی‌های موجود در زیرساخت شبکه پژوهشگاه کردیم. سپس با توجه به سهم بالای تجهیزات سیسکو در سیاهه دارایی‌ها، تمرکز خود را به ارزیابی امنیتی آن‌ها معطوف ساختیم. در ادامه با استفاده از مطالعات کتابخانه‌ای، ابعاد مختلف پیکربندی امنیتی این تجهیزات، به همراه دستورات مورد نیاز برای بررسی و اصلاح پیکربندی‌ها را استخراج کردیم و در قالب چک‌لیستی برای ارزیابی پیکربندی امنیتی تجهیزات شبکه ارائه دادیم. در ادامه و با همکاری کارشناسان شبکه، تجهیزات مدنظر را با استفاده از چک‌لیست طراحی شده ارزیابی کردیم. نتایج این بررسی حاکی از وضعیت مناسب

پیکربندی امنیتی در زیرساخت شبکه پژوهشگاه است.

روش پژوهش

این پژوهش از دو گام مختلف تشکیل شده است. گام اول این طرح به ارائه چک‌لیستی برای ارزیابی پیکربندی امنیتی تجهیزات شبکه می‌پردازد. در این گام با استفاده از مطالعات کتابخانه‌ای، ابتدا پیشینه پژوهش شامل استانداردها و روش‌های بهین مورد بررسی و مطالعه قرار گرفته و سپس با مطالعه راهنمای تجهیزات موجود اقدام به شناسایی ابعاد مختلفی خواهیم کرد که باید در پیکربندی امنیتی تجهیزات مدنظر قرار گیرند. در ادامه و با استفاده از این اطلاعات و راهنمایی‌ها، چک‌لیستی برای ارزیابی پیکربندی امنیتی تجهیزات مدنظر ارائه می‌شود.

گام دوم به ارزیابی پیکربندی امنیتی و ارائه راهکار برای اصلاح آن اختصاص دارد. در این گام، از رویکرد ارزیابی بهره گرفته و با کمک چک‌لیست تهیه شده در گام قبل به بررسی وضعیت پیکربندی امنیتی تجهیزات شبکه می‌پردازیم. با توجه به نتایج حاصل از این ارزیابی، وضعیت موجود پیکربندی امنیتی تجهیزات مشخص شده و برای موارد عدم تطابق، راهکار اصلاح پیکربندی ارائه می‌شود.

یافته‌های طرح پژوهشی

بر پایه یافته‌های پژوهش تجهیزات سیسکو، بیشترین سهم از تجهیزات موجود در زیرساخت شبکه پژوهشگاه را به خود اختصاص داده‌اند و لذا تمرکز این پژوهش بر ارزیابی پیکربندی امنیتی این تجهیزات معطوف شد. در ادامه و با استفاده از مطالعات کتابخانه‌ای چک‌لیستی برای ارزیابی پیکربندی امنیتی این تجهیزات پیشنهاد شد. این چک‌لیست، ارزیابی امنیتی را در سه بخش واحد مدیریتی، واحد کنترل و واحد داده انجام می‌دهد که هر یک ابعاد مختلفی را به شرح زیر در بر می‌گیرند.

- ❖ واحد مدیریتی
  - ✓ قوانین مدیریتی احراز هویت، مجوزهای دسترسی و حساب‌های کاربری (AAA)
  - ✓ قوانین دسترسی
  - ✓ قوانین اعلان
  - ✓ قوانین مربوط به کلمات عبور
  - ✓ قوانین SNMP
- ❖ واحد کنترل

- ✓ قوانین سرویس سراسری
- ✓ قوانین ثبت وقایع
- ✓ قوانین NTP
- ✓ قوانین Loopback

❖ واحد داده

- ✓ قوانین مسیردهی
- ✓ فیلتر روتر مرزی
- ✓ احراز هویت در مسیریابی

برای تعیین وضعیت پیکربندی امنیتی تجهیزات مدنظر از روش ارزیابی استفاده شد. بر طبق نتایج این ارزیابی، واحد داده با ۱۰۰ درصد تطابق با چک‌لیست پیشنهادی از وضعیت مطلوب‌تری برخوردار است. در جایگاه‌های بعدی واحد کنترل و واحد مدیریتی به ترتیب با ۹۶ درصد و ۸۹ درصد تطابق قرار دارند.

نتیجه‌گیری و پیشنهادها

بر اساس نتایج به دست آمده، وضعیت پیکربندی امنیتی کنونی تجهیزات مناسب ارزیابی می‌شود زیرا عدم تطابق‌های مشاهده شده در پیکربندی امنیتی واحد کنترل (دو مورد عدم تطابق) و واحد مدیریتی (یک مورد عدم تطابق) با توجه به شرایط و دلایل ارائه شده از سوی کارشناسان زیرساخت شبکه پژوهشگاه قابل قبول است و بدین ترتیب پیکربندی امنیتی موجود برای تجهیزات سیسکوی پژوهشگاه با توجه به چک‌لیست پیشنهادی تایید می‌گردد. با توجه به کارهای صورت گرفته در این پژوهش می‌توان موارد زیر را به عنوان پیشنهادهای آتی مطرح کرد.

- بررسی امنیتی سرورهای فیزیکی و مجازی پژوهشگاه
- بررسی معماری امنیتی شبکه و ارائه راهکارهای بهبوددهنده