برگه درخواست ارائه پیشنهاد (RFP)

معاونت پژوهش و توسعه ارتباطات علمی

عنوان پروژه	طراحی معماری سامانه مدیریت امن ترافیک بین شبکه های ارتباطی
پژوهشکده	امنیت ارتباطات و فناوری اطلاعات
گروه	فناوری امنیت شبکه
تاریخ	۱۴۰۱/۰۸/۱۰

مقدمه (شامل انگیزه تعریف پروژه و سوابق آن):

پژوهشگاه ارتباطات و فناوری اطلاعات با هدف ایجاد توانمندی در جهت رصد و پایش حملات و تهدیدات در شبکه‌های ارتباطی متناسب با نوع حملات، در صدد است تا طرح بهبود امنیت را در زیرساخت شبکه های ارتباطی کشور، به صورت طراحی معماری امن ترافیک عبوری انجام دهد تا زمان انتقال ترافیک شبکه، محافظت از سرویس و شبکه در مقابل حملات، به صورت متمرکز انجام پذیرد. امن‌سازی انتقال ترافیک، باعث تضمین امنیت زیرساخت‌های اطلاعاتی و ارتباطی می‌شود. در این پروژه، طراحی ارتقا امنیت در سطح شبکه مدنظر است. در نهایت، طرح معماری، به عنوان دستاورد این پروژه در طی مدت چهار ماه تکمیل و عرضه خواهد شد. در این راستا، موارد زیر مورد انتظار است:

- مشخص شدن ارتباطات و اتصالات در شبکه هسته و تجمیع مخابراتی ایران
- چگونگی ارتباطات و تعاملات بین نهادها و زیرساختهای حیاتی، حساس و مهم به جهت مشخص‌شدن نیازمندیهای ارتقا امنیتی این اتصالات
- مشخص شدن وضعیت موجود با رویکرد رفع چالشها در کارایی ارتباطات شبکه زیرساخت در بعد امنیتی و کاهش تهدیدات و حملات رایج شبکه و جلوگیری از سد سرویس زیرساختهای حیاتی
- بررسی نیازمندیها و شرح وظایف متولیان امنیت در سطح شبکه زیرساخت ارتباطی

در این راستا از همکاری شرکتهای معتبر دارای تجربه کاری در زیرساخت ارتباطی و اطلاعاتی کشور که محصولات و خدمات امنیتی با ارزش افزوده ارایه می‌کنند و می‌توانند وضعیت موجود و چالشهای شبکه ارتباطی را با ارایه راه بردها، محصولات، طرح و برنامه و یا ارایه معماری و پیشنهاد اقدامات اولویت‌بندی شده، به وضعیت بهینه از دید امنیتی، نزدیک نمایند، استقبال می‌شود و در نهایت در قالب یک طرح معماری امنیتی شبکه زیرساخت ارتباطی این مهم انجام پذیرد.

۱. هدف پروژه:

به دلیل اهمیت تامین امنیت در شبکه‌های ارتباطی و محافظت از انتقال ترافیک و کاهش حملات و اجرای سیاستهای امن‌سازی ترافیک عبوری، نیازمند طراحی معماری جهت پیاده‌سازی gatewayهایی هستیم تا از طریق انتقال ترافیک از یک شبکه به شبکه دیگر، امن‌سازی ترافیک انجام پذیرد. این سامانه‌ها، وظیفه انتقال و تعامل بین بخش‌های شبکه را برعهده دارند. برای ایجاد اعتماد بین زیرساخت‌های ارتباطی و اطلاعاتی، نیاز مبرم به امن‌سازی ترافیک عبوری بین آنها وجود دارد. هدف از این اقدامات، برقراری ارتباطات امن و پایدار میان دستگاه‌ها، پایداری و بازدارنگی و رسیدن به یک شبکه حفاظت شده است. سابقه پیاده سازی خدمات امن سازی ترافیک عبوری بین شبکه ها، به صورت یکپارچه و متمرکز وجود ندارد و در این پروژه سعی برآن است تا این سازوکارها با توجه به نیازمندی‌ها، نحوه ارتباط آنها و نوع و حجم ترافیکی که مدیریت می‌کنند و معماری و ماژولهای اصلی نهایی شود و همچنین معماری پیشنهادی با توجه به کارکردها و نیازمندی‌های شبکه‌های محافظت شده، مشخص گردد. لازم است تا طرح معماری پیشنهادی شامل دو سطح باشد:

- طرح معماری سامانه برای امن‌سازی ترافیک داخل به خارج کشور با توجه به سیاست‌ها
- طرح معماری سامانه‌ها برای امن‌سازی ترافیک بین سازمان‌ها و قلمروهای مختلف

۲. تعاریف و اصطلاحات:

شبکه هسته: شبکه فوق سریع و پرظرفیتی است که امکان ارتباط میان شبکه‌های تجمیع و شبکه‌های خارجی (از جمله اینترنت) را فراهم می‌کند. این شبکه امکان تعامل مدیریت شده با سایر شبکه‌ها از جمله اینترنت را فراهم می‌آورد. ارتباطات میان زیرشبکه‌ها از طریق یک شبکه هسته صورت می‌پذیرد. قلمرو شرکت زیرساخت، شبکه هسته درنظر گرفته شده است.

شبکه تجمیع: درحال حاضر شبکه داخل استانی و داخل شهری شرکت مخابرات ایران، شبکه تجمیع کشور را تشکیل داده است و تحت نظارت سازمان تنظیم مقررات، نیازمندی دسترسی به خدمات را ارایه می‌دهد.

شبکه اختصاصی: شبکه‌های مستقل یا اختصاصی، زیرساخت‌های دارای شبکه ارتباطی مستقل است. این شبکه‌ها می‌توانند دارای سیاست‌ها، خدمات و مکانیزم‌های اختصاصی باشند. این شبکه‌ها دارای استقلال حداکثری از شبکه‌های عمومی کشور است. ارتباطات پایدار دستگاه‌ها و مراکز حیاتی، از طریق منابع غیراشتراکی، اختصاصی و با بالاترین اولویت تخصیص منابع و با ملاحظه تامین چندگانگی، افزونگی و منابع ذخیره لازم در شبکه اختصاصی با امکان اتصال و انفصال ارتباطات در شرایط ضروری انجام می‌گیرد.

شبکه دولت: شبکه دولت یک محیط امن و قابل اعتماد را برای تبادل داده‌ها بین سازمان‌های دولتی فراهم می‌کند. شبکه دولتی متشکل از نهادهای دولتی است. مزیت اصلی این شبکه‌ها برای سازمان‌های دولتی هزینه‌های کمتر خدمات اینترنتی و انتقال سریعتر داده‌ها برای ارتباطات بین سازمانی است.

شبکه عمومی: به منظور ارایه خدمات به عموم کاربران و کسب و کارها در کشور است.

مرکز ICT-ISAC: مراکز اشتراک‌گذاری اطلاعات متناسب با قلمروهای وظیفه اشتراک اطلاعات مربوط به حملات و تهدیدهای هر حوزه را بر عهده دارد و در مدیریت یکپارچه امنیت، موثر است.

۳. **قلمرو پروژه** (شامل مشتری پروژه، قلمرو منطقی، قلمرو فیزیکی، فناوری مورداستفاده و سایر الزامات نظیر مشخصات فنی):

طراحی سامانه مورد نظر به منظور ایجاد یک نقطه ارتباطی بین دو شبکه اما به صورت امن و با توجه به سیاستها و اولویتها است. قلمرو در دو بخش تعریف می شود: ترافیک داخل به/از خارج و ترافیک بین شبکه های داخلی

قلمر منطقی شامل شبکه های ارتباطی انتقال داده و ارایه سرویس هستند و سامانه باید با استفاده از فناوریهای امنیتی نظیر دیوار آتش، امن‌سازی و مدیریت ترافیک عبوری بین دو شبکه ارتباطی را انجام دهد.

۴. **مراحل اجرا و شرح خدمات پروژه**

مرحله اول: تعیین مولفه‌های مهم شبکه در لایه زیرساخت ارتباطی

فعالیت‌های پیش‌بینی‌شده برای این مرحله عبارت‌اند از :

۱. تعیین ارتباطات و توپولوژی شبکه هسته، شبکه تجمیع و شبکه دسترسی

۲. تعیین ارتباطات و توپولوژی مراکز CDN، زیرساختهای ابر(انواع آن)، سامانه های DNS و مراکز داده در سطح کشور

مرحله دوم: تعیین وضعیت موجود شبکه های ارتباطی و نحوه امن‌سازی ترافیک عبوری

فعالیت‌های پیش‌بینی‌شده برای این مرحله عبارت‌اند از :

۳. تعیین ارتباطات شبکه اختصاصی، ارتباطات شبکه دولت،ارتباطات شبکه عمومی

۴. تحلیل بازیگران، ذیفنعان و شرح وظایف متولیان

۵. بررسی تهدیدات، آسیب‌پذیری و مخاطرات شبکه های ارتباطی موجود

مرحله سوم: طراحی معماری سامانه امن سازی ترافیک عبوری بین شبکه های ارتباطی

فعالیت‌های پیش‌بینی‌شده برای این مرحله، عبارت‌اند از :

۱. تعیین چارچوب ارایه معماری با توجه به معماری های موجود دنیا

۲. تعیین راهبردها و سیاستهای مربوط به فرآیندهای اجرایی

۳. ارایه طرح معماری مفهومی (شناسایی توابع ماژول‌ها ، ارتباط توابع با یکدیگر)

۴. ارایه طرح معماری سیستمی (مشخص کردن اجزاء تمام ماژول‌ها، ارتباط اجزاء با یکدیگر (ماژول‌ها و ذی‌نفعان) وتدوین نقش و مسئولیتهای ذی نفعان و بازیگران

۵. ارایه طرح معماری فناورانه

۵. خروجی‌های هر مرحله از اجرای پروژه

خروجی‌های پیش‌بینی‌شده برای هر یک از مراحل اجرای پروژه، عبارت‌اند از :

خروجی‌های مرحله اول: گزارش مولفه‌های مهم شبکه در لایه زیرساخت ارتباطی

خروجی‌های مرحله دوم: گزارش وضعیت موجود شبکه‌های ارتباطی و نحوه امن‌سازی بر ترافیک عبوری

خروجی‌های مرحله سوم: طرح معماری سامانه امن سازی ترافیک عبوری بین شبکه های ارتباطی

۶. حداکثر مدت‌زمان مجاز و اعتبار برای ارائه پیشنهاد و اجرای پروژه

مدت اجرای پروژه ۴ ماه است.

- **حداکثر مدت‌زمان مجاز برای ارائه پیشنهاد:**

دریافت‌کننده RFP، می‌بایست حداکثر ۱۴ روز پس از دریافت RFP، پیشنهاد خود را بر اساس مکانیسم پیش‌بینی‌شده دربند ۸ این RFP، تحویل پژوهشگاه ارتباطات و فناوری اطلاعات نماید. پیشنهادهای ارائه‌شده پس‌ازاین تاریخ، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهند بود.

- **حداکثر مدت‌زمان مجاز برای اجرای پروژه:**

حداکثر مدت‌زمان پیش‌بینی‌شده و قابل‌پذیرش برای اجرای این پروژه، ۴ ماه می‌باشد. چنانچه پیشنهاددهنده در فرم پیشنهاد پروژه، مدت‌زمان اجرای پروژه را بیش از مدت‌زمان مجاز اعلام نماید، قابل وصول توسط پژوهشگاه ارتباطات و فناوری اطلاعات نخواهد بود.

- **سقف اعتبار برای اجرای پروژه:**

۷. سایر الزامات و محدودیت‌های موجود در اجرای پروژه

علاوه بر محدودیت موجود در خصوص زمان اجرای پروژه، لازم است پیشنهاددهندگان در تنظیم پیشنهاد خود، موارد ذیل را نیز رعایت فرمایند :

- پیشنهاد باید در قالب آخرین نسخه از "فرم پیشنهاد پروژه" موجود در سایت پژوهشگاه ارتباطات و فناوری اطلاعات (حوزه معاونت پژوهش و توسعه ارتباطات علمی، دفتر امور پژوهشی، فرم‌ها)، تنظیم و ارائه گردد.
- در جدول ساختار شکست پروژه پیش‌بینی‌شده در بخش ۲-۳-۷ فرم پیشنهاد پروژه، لازم است شرح فعالیت‌های هر مرحله از پروژه (مطابق شرح فعالیت‌های پیش‌بینی‌شده در RFP به همراه موارد احتمالی که پیشنهاددهنده، انجام آن‌ها را ضروری می‌داند) به همراه کلیه اطلاعات درخواست شده در فرم، به تفکیک برای هر فعالیت و مرحله، ارائه گردد. از خالی گذاشتن ستون‌های این جدول برای فعالیت‌های پروژه، خودداری گردد.
- در جدول مشخصات منابع انسانی پیش‌بینی‌شده در بخش ۳-۱ فرم پیشنهاد پروژه، لازم است نام و سایر مشخصات درخواست شده برای کلیه پرسنلی که در اجرای پروژه به‌صورت واقعی مشارکت دارند با ذکر میزان مشارکت درج گردد.
- هزینه‌های سربار، تنها برای پیشنهاددهندگان حقوقی (دانشگاه‌ها) پیش‌بینی‌شده است و شرکت‌ها می‌توانند بجای هزینه سربار، هزینه‌های اضافی متحملِ بابت این پروژه را عنوان نمایند.
- پیشنهاد سود خالص برای شرکت‌های خصوصی .

۸. تحویل پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات

- **حداقل شرایط پیشنهاد قابل تحویل:**

پیشنهادهایی قابل وصول می‌باشند که شرایط مندرج دربندهای ۶ و ۷ این RFP را کاملاً رعایت نموده باشند. در زمان ارائه پیشنهاد به پژوهشگاه ارتباطات و فناوری اطلاعات، رعایت شرایط مذکور، کنترل‌شده و در صورت عدم رعایت هر یک از موارد، از تحویل پیشنهاد، خودداری خواهد شد.

- **نحوه تحویل پیشنهاد:**

پیشنهاددهندگان می‌بایست پیشنهاد خود را به نام معاونت پژوهش و توسعه ارتباطات علمی به دبیرخانه پژوهشگاه ارتباطات و فناوری اطلاعات، تحویل داده و رسید دریافت نمایند. (درصورتی‌که مدارک به سایر واحدهای دیگر پژوهشگاه تحویل داده شود در فراخوان ثبت نخواهد شد و این پژوهشگاه در قبال آن هیچ‌گونه مسئولیتی ندارد)

۹. نحوه ارزیابی پیشنهاد

ارزیابی پیشنهادهای رسیده بر اساس پارامترهای زیر خواهد بود:

۱- میزان تسلط به ابعاد و جوانب پروژه (امتیاز این ردیف با توجه به سمینار ارائه‌شده توسط پیشنهاددهنده و نیز مطالب ارائه‌شده در فرم پیشنهاد پروژه در خصوص شرح خدمات، خروجی‌ها، اهداف و . . . تعیین می‌گردد)

۲- نحوهٔ تخصیص منابع انسانی شامل کیفیت و کمیت نیروها (رزومه و سابقه کاری لازم در ارتباط با انجام خدمات موردنیاز پروژه، تعداد و تناسب نیروها با توجه به حجم کار، نوع رابطه استخدامی نیروها بر اساس مدارک ارائه‌شده)

۳- کیفیت ساختار شکست پروژه متناسب با شرح خدمات و اهداف پروژه

۴- کیفیت ساختار سازمانی پیش‌بینی‌شده برای انجام پروژه(تیم‌های اجرایی، مدیریت پروژه و...)

۵- ساختار و روال‌های پیش‌بینی‌شده برای کنترل و مدیریت پروژه و تأیید صحت خروجی‌ها

۶- روال‌ها، متدولوژی و استانداردهای پیشنهادی برای اجرای شرح خدمات

۷- نحوه ارائه زمان‌بندی و پوشش کامل و به‌موقع شرح خدمات

۸- مبلغ پیشنهادی