	RFP **طرح پژوهشی** **" امکانسنجی راه اندازی آزمایشگاه امنیت سایبری پست بانک ایران "**	**کد طرح : ۱۴۰۲۰۱** **تاریخ تنظیم : ۱۴۰۲/۰۴/۱۵**

۱- مشخصات درخواست کننده طرح :

واحد تهیه‌کننده :	**اداره کل امنیت و زیرساخت**	**تلفن تماس کارشناس تحقیقات :** **آقای افشارزاده –۸۱۵۶۳۰۴۱**
واحد بهره بردار:	**اداره کل امنیت و زیرساخت**	

۲- ماهیت طرح :

الف) مسئله محور ☐ **ب) توسعه محور** ☐ **ج) استقرار فناوری جدید** ■

۳-واژگان کلیدی :

امنیت سایبری (Cyber Security)، تست نفوذ (Penetration test)، محیط آزمایشگاهی (VirtualBox Lab)، تهدیدات فضای سایبری (Cyber Space Threats)، اکسپلویت (Exploit)، تست وصله (Patch Test)

۴- ضرورت انجام طرح :

با افزایش حجم و پیچیدگی حملات سایبری، سازمان‌ها باید اقدامات لازم برای محافظت از اطلاعات حساس را انجام دهند. پیاده سازی امنیت سایبری به صورت موثر و درست از چالش‌های دنیای امروز است، چون هم تعداد سامانه‌ها و نرم‌افزارها بیشتر شده‌اند و هم هکرها خلاق‌تر شده‌اند به عنوان مثال استفاده از مولفه‌های قدیمی و آسیب‌پذیر در برنامه‌نویسی، بسیاری از solutionهای امنیتی سامانه‌های مورد استفاده کاربران را سست کرده، به‌نحوی که تبدیل به پنجره‌ای برای نفوذ هکرها و بروز حملات سایبری شده است. لذا به منظور بهبود وضعیت عملکرد امنیتی سازمان و ارتقا قدرت شناسایی رویدادها و حوادث امنیتی، پیاده‌سازی آزمایشگاه امنیت سایبری با ماموریت "شناسایی و ارزیابی مستمر، منظم و موردی آسیب‌پذیری‌های امنیتی و حصول اطمینان از رفع/کاهش آسیب‌پذیری‌های شناسایی شده" مورد نیاز بانک می‌باشد.

۵- تاریخچه و سوابق طرح :

این طرح تاریخچه و سابقه‌ای در بانک ندارد.

۶- اهداف طرح :

- ✓ ارتقا قابلیت مدیریت آسیب‌پذیری‌های امنیتی
- ✓ به اشتراک‌گذاری اطلاعات آسیب‌پذیری‌ها و روش‌های مقابله با آن‌ها در سطح نظام بانکی کشور، از طریق برقراری ارتباطات مورد نیاز فی‌مابین آزمایشگاه تخصصی بانک مرکزی و آزمایشگاه ایجاد شده در بانک
- ✓ کاهش مخاطرات ناشی از افشای اطلاعات مرتبط با آسیب‌پذیری‌های امنیتی پیمانکاران

۷- مشخصات فنی و استانداردهای مورد نیاز :

۱. **محدوده عملیاتی آزمایشگاه امنیت سایبری**

انتظار می‌رود محدوده عملیاتی آزمایشگاه امنیت سایبری حداقل شامل محصولات نرم‌افزاری، سرویس‌های زیرساختی و شبکه‌های رایانه‌ای متعلق به بانک و همچنین شرکت‌های تابعه بانک باشد. به عبارت دیگر آزمایشگاه مورد اشاره باید حداقل از امکانات لازم برای شناسایی و ارزیابی آسیب‌پذیری‌های امنیتی در محدوده ذیل برخوردار باشد:

۲. **محصولات نرم‌افزاری مبتنی بر وب نظیر پیشخوان‌های مجازی، تارنماهای اطلاع‌رسانی و بانکداری دیجیتالی و اینترنتی**
۳. **برنامک‌های همراه اعم از همراه‌بانک، برنامک‌های پرداخت و برنامک‌های پیام‌رسان**
۴. **واسط‌های برنامه‌سازی کاربردی (API) و ویجت‌های (Widget) ارائه شده توسط بانک**
۵. **سرویس‌های زیرساختی مانند سرویس‌های مجازی‌سازی، نام دامنه (DNS)، پست الکترونیکی سازمانی و شبکه‌های ارتباطی نظیر ارتباطات رادیویی بی‌سیم، ابری، تجهیزات شبکه و امنیتی**
۶. **برنامه‌های کاربردی رومیزی (Desktop Application)، پشتیبانی کننده از کسب و کار بانک**
۷. **بهره مندی ازتعاریف ، متدهاو یافته های روز مرتبط با طرح**
۸. **رعایت اصول گزارش دهی**
۹. **رعایت اصل امانت دهی و اخلاق حرفه ای**
۱۰. **رعایت سایر ضوابط و دستورالعمل ها حسب اعلام بانک**

۱۱ **.کارکردهای اصلی آزمایشگاه امنیت سایبری**

۱۲. مطالعه و بررسی وضعیت فعلی بانک، احصاء نقاط قوت وضعف و ارائه گزارش شناخت
۱۳. شناسایی و رصد پایگاه‌های معرفی آسیب‌پذیری‌های امنیتی
۱۴.دریافت، تریاژ و پردازش گزارشات آسیب‌پذیری
۱۵. کشف آسیب‌پذیری‌ها در حین پاسخگویی به رخدادهای امنیت اطلاعات
۱۶.پویش، شناسایی و ارزیابی بهنگام آسیب‌پذیری‌های امنیتی
۱۷. ارزیابی امنیتی پیکربندی‌ها
۱۸. تنظیم و ارائه طرح‌های کاهش اثر/رفع آسیب‌پذیری‌های امنیتی شناسایی شده
۱۹.پی‌جویی و سنجش اثربخشی اقدامات انجام شده در راستای کاهش اثر/رفع آسیب‌پذیری‌های امنیتی شناسایی شده
۲۰.سنجش عملکرد فرآیند مدیریت واصله‌های امنیتی
۲۱.پویش برنامه‌های کاربردی، سرویس‌ها و دارایی‌های فعال در شبکه‌های رایانه‌ای با هدف شناسایی موارد مشکوک و غیرمجاز
۲۲. تحلیل علل ریشه‌ای آسیب‌پذیری‌های شناسایی شده
۲۳. ایجاد هماهنگی میان واحدهای ذی‌ربط در فرآیند رسیدگی به آسیب‌پذیری‌های شناسایی شده
۲۴. اطلاع‌رسانی آسیب‌پذیری‌های شناسایی شده به واحدهای مرتبط

۲۵. توسعه محتوای آموزشی و ارائه مشاوره‌های مورد نیاز در زمینه رسیدگی به آسیب‌پذیری‌های امنیتی
۲۶. مدیریت سوابق ارزیابی‌های انجام شده، آسیب‌پذیری‌های شناسایی شده و اقدامات انجام شده به منظور کاهش اثر/رفع آن‌ها
مری نگهداری و به‌روزرسانی ابزارهای پویش و ارزیابی آسیب‌پذیری‌های امنیتی
۲۸. اعلان آسیب‌پذیری‌های امنیتی فراگیر (آسیب‌پذیری‌های امنیتی مرتبط با محصولات یا سرویس‌های زیرساختی مورد استفاده توسط اعضای شبکه بانکی کشور) به آزمایشگاه تخصصی بانک مرکزی
۲۹. تعامل منظم و مستمر با آزمایشگاه تخصصی بانک مرکزی، به منظور تسهیم دانش در حوزه مدیریت آسیب‌پذیری‌های امنیتی

۸- نتایج مورد انتظار (خروجی مورد انتظارطرح) :

۱- مطالعه و بررسی وضعیت فعلی بانک، احصاء نقاط قوت وضعف و ارائه گزارش شناخت
۲- انجام پژوهش‌های مرتبط و بررسی تجارب سایر بانک‌ها درخصوص چگونگی پیاده‌سازی آزمایشگاه امنیت سایبری
۳- بررسی وضعیت موجود بانک از نظر تجهیزات سخت‌افزاری و نرم‌افزاری مرتبط
۴- تدوین طرح و طراحی مدل آزمایشگاه امنیت سایبری
۵- پیاده‌سازی مدل (آزمایشگاه) باتوجه به الزامات ابلاغی بالادستی از سوی بانک مرکزی ج.ا.ا به شرح ذیل:

امنیت و ارتقاء قدرت شناسایی رویدادها و حوادث امنیتی نیاز است که آزمایشگاه‌هایی با قابلیت زیر وجود داشته باشد:

- تحلیل رفتارهای ترافیکی
- توسعه و تست قوانین شناسایی و همبسته‌های جدید
- تست اکسپلویت‌ها
- تست وصله پیش از اعمال آنها

همچنین مرکز عملیات امنیت باید بتواند از نتایج آزمایشگاه‌های تحلیل بدافزار و تحلیل شواهد نیز بهره‌مند گردد. " حداکثر ظرف مدت ۶ ماه از تاریخ ابلاغ این نامه، نسبت به راه‌اندازی و بهره‌برداری از آزمایشگاه امنیت سایبری با ماموریت "شناسایی و ارزیابی مستمر، منظم و موردی آسیب‌پذیری‌های امنیتی و حصول اطمینان از رفع/ کاهش آسیب‌پذیری‌های شناسایی شده" در آن بانک/موسسه اعتباری اقدامات لازم صورت پذیرفته و یا ایجاد این قابلیت و خدمات امنیتی مربوطه به صورت برون سپاری از طریق شرکت‌های دارای مجوز مرکز راهبردی افتای ریاست جمهوری برنامه‌ریزی و در دستور کار قرار گیرد. همچنین انتظار می‌رود فرآیندهای لازم جهت ارتباط موثر با آزمایشگاه تخصصی اداره امنیت اطلاعات بانک مرکزی پیش‌بینی؛ و نتیجه اقدامات نیز به آن اداره ارسال گردد.

-۶

اهداف کلان آزمایشگاه امنیت سایبری

راه‌اندازی آزمایشگاه امنیت سایبری در بانک‌ها و مؤسسات اعتباری غیر بانکی در راستای اهداف ذیل انجام خواهد شد:

- ارتقاء قابلیت مدیریت آسیب‌پذیری‌های امنیتی در بانک‌ها و مؤسسات اعتباری غیر بانکی
- به اشتراک‌گذاری اطلاعات آسیب‌پذیری‌ها و روش‌های مقابله با آن‌ها در سطح نظام بانکی کشور، از طریق برقراری ارتباطات موردنیاز فی‌مابین آزمایشگاه تخصصی بانک مرکزی و آزمایشگاه‌های ایجادشده در بانک‌ها و مؤسسات اعتباری غیر بانکی
- کاهش مخاطرات ناشی از افشای اطلاعات مرتبط با آسیب‌پذیری‌های امنیتی پیمانکاران

محدوده عملیاتی آزمایشگاه امنیت سایبری

انتظار می‌رود محدوده عملیاتی آزمایشگاه امنیت سایبری حداقل شامل محصولات نرم‌افزاری، سرویس‌های زیرساختی و شبکه‌های رایانه‌ای متعلق به بانک/موسسه اعتباری غیر بانکی و همچنین شرکت‌های تابعه آن بانک/موسسه باشد. به‌عبارت‌دیگر آزمایشگاه مورداشاره باید حداقل از امکانات لازم برای شناسایی و ارزیابی آسیب‌پذیری‌های امنیتی در محدوده ذیل برخوردار باشد:

- محصولات نرم‌افزاری مبتنی بر وب نظیر پیشخوان‌های مجازی، نارنماهای اطلاع‌رسانی و بانکداری دیجیتالی و اینترنتی
- برنامک‌های همراه اعم از همراه بانک، برنامک‌های پرداخت و برنامک‌های پیام‌رسان
- واسط‌های برنامه‌سازی کاربردی (API) و ویجت های (Widget) ارائه‌شده توسط آن بانک یا موسسه اعتباری غیر بانکی
- سرویس‌های زیرساختی مانند سرویس‌های مجازی سازی، نامه دامنه (DNS)، پست الکترونیکی سازمانی و شبکه‌های ارتباطی نظیر ارتباطات رادیویی/بی سیم، ابری، تجهیزات شبکه و امنیتی
- برنامه‌های کاربردی رومیزی (Desktop Application)، پشتیبانی‌کننده از کسب‌وکار بانک یا موسسه اعتباری غیر بانکی

کارکردهای اصلی آزمایشگاه امنیت سایبری

حداقل کارکردهای اصلی آزمایشگاه امنیت سایبری عبارت‌اند از:

- شناسایی و رصد پایگاه‌های معرفی آسیب‌پذیری‌های امنیتی؛
- دریافت، تریاژ و پردازش گزارشات آسیب‌پذیری؛
- کشف آسیب‌پذیری‌ها در حین پاسخگویی به رخدادهای امنیت اطلاعات؛
- پویش، شناسایی و ارزیابی بهنگام آسیب‌پذیری‌های امنیتی؛
- ارزیابی امنیتی پیکربندی‌ها؛

۹- مدت زمان اجرای طرح :

۱ سال

۱۰- محل تأمین اعتبار طرح :

٪۱ هزینه های غیر عملیاتی بانک در سال ۱۴۰۲

۱۱- مستندات مرتبط با طرح :

۱- الزامات ابلاغی بانک مرکزی ج.ا.ا

۲- رعایت کلیه استانداردها وضوابط درون/ برون سازمانی مرتبط با طرح حسب اعلام بانک

۱۲- واحدهای مرتبط با اجرای طرح :

ر	نام واحد	نقش
۱		
۲		
۳		
۴		