| | تشریح پروژه واگذاری | |
|---|---|---|
| | TDF02-0 | |
| | RFP20-5 | |

| | |
|---|---|
| عنوان پروژه: | طراحی و پیاده‌سازی پایلوت سیستم کنترل نیروگاهی دارای بیشترین کاربرد در نیروگاه‌های کشور و اجرای تست نفوذ سایبری جهت ارزیابی امنیتی |
| عنوان طرح: | طرح ارزیابی امنیتی سامانه‌های مبتنی بر ICT در صنعت برق |
| واحد اجرایی: | مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق |

**برآورد کلی مدت زمان اجرای پروژه:** ۸ ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

زیرساخت‌های حیاتی و تاسیسات بنیادین کشورها از جمله صنعت برق همواره توسط عوامل مختلفی مورد تهدید امنیتی بوده و می‌باشند. با توجه به اینکه زیرساخت برق علاوه بر تامین برق مصرفی مشترکین عمومی، به عنوان زیرساخت کلیه صنایع نیز محسوب می‌شود، صنعت برق باید سرویس قابل اطمینانی را ارائه دهد؛ بنابراین تداوم سرویس برق‌رسانی، تامین و حفظ امنیت و پایایی آن از اهمیت ویژه‌ای برخوردار است. از طرف دیگر بکارگیری سیستم‌های خودکار و سیستم‌های حفاظت مبتنی بر میکروپروسسور با استفاده از فناوری‌های مبتنی بر ICT در صنعت برق در حال گسترش می‌باشد. همچنین با توجه به رویکرد صنعت برق در زمینه حرکت به سمت شبکه هوشمند و از آنجا که این شبکه متشکل از سیستم‌های سنتی و شبکه‌های پیشرفته مخابراتی و IT می‌باشد لذا تامین و حفظ امنیت سایبری با توجه به تهدیدات و آسیب‌پذیری‌هایی که برای تجهیزات مبتنی بر ICT در محیط‌های صنعتی وجود دارد، اهمیت ویژه‌ای خواهد یافت.

همانطور که در سند راهبردی توسعه فناوری‌های امنیت فناوری اطلاعات و ارتباطات صنعت برق اشاره شده است یکی از رده‌هایی که حفظ امنیت آن از اهمیت بالایی برخوردار می‌باشد، رده تولید است. بخش عمده‌ای از سیستم‌های صنعتی مبتنی بر ICT در نیروگاه‌ها، از PLCها و شبکه کنترلی مرتبط با آن تشکیل شده است. همچنین سابقه حمله بر روی PLCها توسط بدافزار stuxnet، اهمیت پرداختن به امنیت در این حوزه را دو چندان می‌سازد.

هدف از اجرای این پروژه طراحی و پیاده‌سازی پایلوت آزمایشگاهی سیستم کنترلی نیروگاهی (DCS شرکت زیمنس– Teleperm XP/T2000) و اجرای تست نفوذ سایبری جهت ارزیابی امنیتی آن می‌باشد. لازم است تا با شبیه‌سازی رفتار Field شامل چرخه‌های کنترلی قابل اجرا (ساده شده‌ی آن‌چه در واحد نیروگاهی سیکل ترکیبی اتفاق می‌افتد) عملکرد سیستم کنترل و همینطور تاثیر نفوذ/حملات سایبری بر عملکرد سیستم کنترل قابل نمایش باشد.

مراحل کلی پیشنهادی برای اجرای این پروژه به شرح زیر می‌باشد:

- طراحی و پیاده‌سازی امولاتور جهت شبیه‌سازی رفتار Field در یک واحد نیروگاهی
- طراحی معماری سیستم کنترلی Teleperm XP/T2000
- بررسی و انتخاب تجهیزات مورد نیاز جهت پیاده‌سازی پایلوت سیستم کنترلی نیروگاه
- خرید تجهیزات و پیاده‌سازی پایلوت سیستم کنترلی
- راه‌اندازی و تست عملکرد سیستم کنترلی در پایلوت آزمایشگاهی
- آموزش نحوه کارکرد و برنامه‌ریزی سیستم کنترلی به محققین مرکز امنیت پژوهشگاه نیرو
- انجام تست نفوذ سایبری بر روی پایلوت و ارائه گزارش تست

مشخصات محصول نهایی(خروجی مورد انتظار):

- گزارش فنی شامل جزئیات طراحی امولاتور (شبیه‌ساز رفتار Field در یک واحد نیروگاهی)
- گزارش فنی شامل جزئیات طراحی معماری شبکه کنترلی سیستم DCS زیمنس Teleperm XP/T2000، لیست تجهیزات، نقشه اتصالات
- نرم‌افزارهای مربوط به مانیتورینگ و کنترل
- برنامه سیستم‌های کنترلی
- پایلوت آزمایشگاهی سیستم کنترلی (شامل امولاتور، PLCها، ES، OT و ... ) با قابلیت اجرای چرخه‌های فرآیندی نیروگاهی به صورت شبیه‌سازی شده
- پکیج آموزشی
- گزارش آسیب‌پذیری‌های پایلوت، سناریوهای تست نفوذ شامل تمامی مراحل
- گزارش انجام تست نفوذ و نتیجه آن