



شرکت مادر تخصصی تولید نیرو
برق حرارتی

پیشنهاد پروژه واگذاری

TDF02-0

RFP20-7



عنوان پروژه:	پایده سازی پایگاه دانش آسیب پذیری های امنیتی، تهدیدات، حملات و بدافزارهای سامانه های کنترل و اتوماسیون صنعت برق
عنوان طرح:	طرح توسعه زیرساخت های امنیتی در صنعت برق
واحد اجرایی:	مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق

برآورد کلی مدت زمان اجرای پروژه: ۵ ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

امنیت سایبری سامانه های کنترل و اتوماسیون صنعتی و اسکادا به دلیل به کارگیری در زیرساخت های حساس، حیاتی و مهم در این دهه به حدی پراهمیت شده که به عنوان یک دغدغه مهم بین المللی عنوان گردیده است. سامانه های کنترل و اتوماسیون صنعتی حوزه برق (انرژی) نیز به دلیل اهمیت بسیار بالای خود از حملات و رخدادهای سایبری بی بهره نبوده اند، سروصدایی که بدافزار Industroyer در حمله به زیرساخت های برق اوکراین (۲۰۱۵ تا ۲۰۱۷) به راه انداختن موجب شد توجه نخبگان به سمت سامانه های کنترل صنعتی حوزه برق بیشتر جلب شود و این نکته بر آن ها روشن شود که این سامانه ها تا چه میزان می توانند حساس و آسیب پذیر باشند.

یکی از موارد بسیار مهم در اجرای راهبردهای امنیت سایبری، اطلاع رسانی به موقع و آگاهی بخشی امنیتی در سطوح مختلف به مدیران، متولیان، سرپرستان و کارشناسان صنایع، شرکت ها و سازمان های مرتبط است. با توجه به جایگاه برجسته اطلاع رسانی به موقع و تاثیر آن بر روی عملکرد سایر راهبردها و سازوکارهای ارتقاء امنیت سایبری، طراحی و پایده سازی پایگاه دانش آسیب پذیری های امنیتی، تهدیدات، حملات و بدافزارهای سامانه های کنترل و اتوماسیون صنعت برق بسیار حائز اهمیت است.

در این پروژه، هدف این است که بستری جهت ارائه اطلاعات مکفی در حوزه های آسیب پذیری های امنیتی، تهدیدات، حملات و بدافزارهای سامانه های کنترل و اتوماسیون صنعت برق طراحی و پایده سازی شود. این محصول باید بتواند با توجه به توصیه های سازندگان و استانداردها، راهکارهای امنیتی پیشنهاد دهد و از مولفه های اساسی که یک پایگاه اطلاع رسانی امنیت سایبری به آنها نیاز دارد برخوردار باشد.

مشخصات محصول نهایی (حداقل ویژگی های مورد انتظار):

- دسترسی کاربران (با توجه به سطح دسترسی مشخص شده) به اطلاعات آسیب پذیری های امنیتی سامانه های کنترل و اتوماسیون صنعتی
- امکان آشنایی کاربر با محصولات آسیب پذیر
- امکان آشنایی کاربر با تهدیدات امنیتی
- ارائه راهکارهایی برای رفع و یا کاهش آسیب پذیری های امنیتی سامانه های کنترل و اتوماسیون صنعتی
- دسترسی کاربر به اطلاعات بدافزارها و حملات حوزه سامانه های کنترل و اتوماسیون صنعتی جهت پیشگیری از وقوع این حملات در صنعت برق
- امکان ارائه گزارش های تحلیلی متنوع با توجه به پارامترهای مختلف آسیب پذیری ها، تهدیدات، حملات و بدافزارها
- ارائه راهکارهایی برای پیشگیری، مقابله و پاکسازی بدافزارها و حملات حوزه سامانه های کنترل و اتوماسیون صنعتی
- زیرساخت امکان دریافت گزارش موارد مشکوک از کاربران