فرم تعریف اولویت تحقیقاتی

۱- محور پروژه

☐ تولید ☐ عمومی ☒ توزیع ☐ مطالعات کلان انرژی، اقتصادی و مدیریتی ☐ انرژی‌های نو و تجدید پذیر

۲ - عنوان دقیق پروژه:

ارزیابی امنیتی و آزمون نفوذپذیری زیرساخت‌های فناوری اطلاعات (IT) و اتوماسیون صنعتی (OT) با طراحی و نصب ids/ips در شرکت توزیع نیروی برق استان خراسان جنوبی به همراه ارائه راهکارهای مقابله

۳ - تعریف مسئله / دلایل اولویت داشتن تحقیق: (سابقه موضوعی، اقدامات انجام‌شده و نتایج به‌دست‌آمده، سابقه استفاده کاربردی در کشورهای پیشرفته بیان شود- انجام پروژه چه مشکلی از صنعت برق را حل خواهد نمود، صرفه‌جویی ناشی از انجام پروژه اعلام گردد- زیان‌های ناشی از عدم انجام پروژه روی سایر تجهیزات ذکر شود- تعداد موردنیاز اعلام گردد و ...)

با پیشرفت فناوری و افزایش سطح دیجیتال‌سازی در شبکه‌های توزیع برق، زیرساخت‌های حیاتی این صنعت به‌ویژه سیستم‌های نظارت و کنترل (SCADA)، سیستم‌های اتوماسیون توزیع (DAS)، شبکه‌های داخلی و سرورهای مرکزی، در معرض تهدیدات سایبری متعددی قرار گرفته‌اند. این تهدیدات شامل حملات Ransomware، فیشینگ، حملات DDoS، نفوذ به شبکه داخلی، سوءاستفاده از آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری، و حملات داخلی می‌شوند.

در سال‌های اخیر، حملات سایبری علیه شبکه‌های برق در داخل و خارج از کشور (مانند حمله به شبکه برق اوکراین در سال ۲۰۱۵ و حملات متعدد به زیرساخت‌های انرژی ایران) نشان داده است که شبکه‌های توزیع برق به‌عنوان یک زیرساخت حیاتی ملی، همواره در اولویت اهداف حمله سایبری قرار دارند. این حملات می‌توانند منجر به قطعی گسترده، آسیب به تجهیزات حساس، نشت اطلاعات مشترکان، اختلال در خدمات و حتی تهدید امنیت ملی شوند.

در حال حاضر، ارزیابی امنیتی در شرکت توزیع خراسان جنوبی عمدتاً به‌صورت دوره‌ای، غیرسیستماتیک و بدون استفاده از روش‌های استاندارد بین‌المللی انجام می‌شود. عدم انجام آزمون نفوذپذیری (Penetration Testing) منظم و حرفه‌ای، عدم شناسایی آسیب‌پذیری‌های پنهان و عدم اولویت‌بندی صحیح نقاط بحرانی، از جمله ضعف‌های اصلی است. همچنین، بسیاری از سیستم‌های OT (مانند PLCها و RTUها) که برای کنترل شبکه استفاده می‌شوند، با توجه به قدیمی بودن و عدم به‌روزرسانی، دارای آسیب‌پذیری‌های جدی هستند که بدون تست عملیاتی قابل شناسایی نیستند.

اجرای این پروژه می‌تواند به شناسایی واقعی آسیب‌پذیری‌ها، ارزیابی دقیق سطح امنیتی فعلی، ارائه نقشه راه امن‌سازی و کاهش ریسک وقوع حوادث سایبری کمک کند. صرفه‌جویی‌های انتظاری شامل کاهش ۵۰-۷۰٪ در خطر وقوع حادثه، کاهش هزینه‌های بازیابی پس از حمله، جلوگیری از جریمه‌های نظارتی و افزایش اعتماد عمومی به خدمات برق است.

عدم انجام این پروژه می‌تواند منجر به قطعی‌های طولانی‌مدت، خسارت به تجهیزات حساس (مانند ترانسفورماتورها و سوئیچ‌ها)، نشت اطلاعات مشترکان، اختلال در سیستم‌های کنترل و کاهش قابلیت اطمینان شبکه شود. همچنین، عدم تطابق با الزامات ملی (سازمان تنظیم مقررات، مرکز ملی فضای مجازی) و بین‌المللی (ISO/IEC ۲۷۰۰۱, IEC ٦٢٤٤٣) می‌تواند مانع از دریافت گواهی‌های امنیتی و همکاری‌های فنی شود.

در کشورهای پیشرفته مانند آمریکا، آلمان و استرالیا، آزمون نفوذپذیری منظم (PenTest) و ارزیابی امنیتی سیستمیک برای زیرساخت‌های حیاتی اجرا می‌شود و نتایج آن به‌عنوان بخشی از سیاست‌های امنیت سایبری مورد استفاده قرار می‌گیرد. استفاده از چارچوب‌هایی مانند NIST CSF، MITRE ATT&CK و IEC ٦٢٤٤٣، به این سازمان‌ها کمک کرده تا به‌صورت پیشگیرانه و حرفه‌ای با تهدیدات روبرو شوند.

۴ - وجوه تمایز و اشتراک اولویت پیشنهادی نسبت به کارهای انجام شده قبلی یا جاری مشابه چیست؟

وجه تمایز اصلی این پروژه، اجرای یک آزمون نفوذپذیری حرفه‌ای، سیستماتیک و چندلایه (IT و OT) بر اساس استانداردهای بین‌المللی است. برخلاف اقدامات قبلی که عمدتاً به‌صورت بازرسی بصری، بررسی کلی و بدون استفاده از روش‌های استاندارد انجام شده‌اند، این پروژه از روش‌های پیشرفته تست نفوذ (Penetration Testing) مانند تست شبکه، تست برنامه‌های تحت وب، تست بی‌سیم و تست سیستم‌های صنعتی (ICS/SCADA) استفاده می‌کند.

همچنین، این پروژه تمرکز ویژه‌ای بر سیستم‌های OT (اتوماسیون صنعتی) دارد که در بسیاری از ارزیابی‌های قبلی نادیده گرفته شده‌اند. این سیستم‌ها حساسیت بالایی دارند و تست آن‌ها نیازمند تخصص خاص، ابزارهای تخصصی و دقت بالا است تا از ایجاد اختلال در عملیات جلوگیری شود.

تمایز دیگر، یکپارچه‌سازی نتایج آزمون با یک سامانه مدیریت آسیب‌پذیری (Vulnerability Management System) است که به صورت تحت وب توسعه می‌یابد. این سامانه امکان ثبت، رهگیری، اولویت‌بندی و گزارش‌دهی آسیب‌پذیری‌ها را فراهم می‌کند و از یک گزارش کاغذی و غیرعملیاتی فراتر می‌رود.

در نهایت، این پروژه نه تنها شناسایی آسیب‌پذیری، بلکه ارائه راهکارهای عملی، فنی و اداری برای مقابله با هر یک از آسیب‌پذیری‌ها را شامل می‌شود. این راهکارها بر اساس معیارهای هزینه، زمان اجرا، تأثیر و اولویت ریسک اولویت‌بندی می‌شوند و به یک برنامه عملیاتی امن‌سازی تبدیل می‌شوند.

۵ - اهداف مورد انتظار و مراحل کلی انجام تحقیق :

اهداف کلی:

انجام آزمون نفوذپذیری حرفه‌ای و استاندارد از زیرساخت‌های IT و OT شرکت.

شناسایی آسیب‌پذیری‌های فنی، اداری و عملیاتی در شبکه‌های داخلی، سرورها، سیستم‌های SCADA و DAS.

ارزیابی دقیق سطح امنیتی فعلی و تعیین نقاط بحرانی.

ارائه راهکارهای عملی و اولویت‌بندی شده برای رفع آسیب‌پذیری‌ها.

توسعه سامانه مدیریت آسیب‌پذیری برای پیگیری و به‌روزرسانی مستمر.

افزایش آگاهی و ظرفیت سازمانی در حوزه امنیت سایبری.

مراحل کلی اجرا:

آماده‌سازی و برنامه‌ریزی (۱,۵ ماه):

تعریف محدوده (Scope)، اخذ مجوزهای لازم، تشکیل تیم متخصص.

جمع‌آوری اطلاعات (Reconnaissance) (۱ ماه):

شناسایی دامنه‌ها، IPها، سرویس‌ها، سیستم‌های OT و شبکه‌های فرعی.

شناسایی آسیب‌پذیری (Vulnerability Scanning) (۱,۵ ماه):

استفاده از ابزارهایی مانند Nessus، OpenVAS و ابزارهای تخصصی OT.

آزمون نفوذپذیری (Penetration Testing) (۳ ماه):

تست شبکه، تست برنامه‌های تحت وب، تست بی‌سیم، تست سیستم‌های صنعتی (ICS/SCADA).

تحلیل نتایج و رتبه‌بندی ریسک (۱ ماه):

استفاده از ماتریس ریسک (احتمال × پیامد) و رتبه‌بندی آسیب‌پذیری‌ها.

توسعه سامانه مدیریت آسیب‌پذیری (۲ ماه):

طراحی و پیاده‌سازی نرم‌افزار تحت وب برای ثبت و پیگیری آسیب‌پذیری‌ها.

ارائه راهکارهای مقابله و آموزش (۲ ماه):

ارائه گزارش فنی، راهکارهای امن‌سازی، آموزش کارکنان و واحد IT.

گزارش نهایی و نقشه راه (۱ ماه):

ارائه گزارش جامع، داشبورد امنیتی و برنامه عملیاتی امن‌سازی.
کل دوره پیشنهادی: ۱۳ ماه

۶ - الزامات واستانداردهای لازم جهت رعایت در انجام این پروژه چیست؟

اسناد بالادستی ملی:
سند ملی انرژی
برنامه‌های توسعه پنج‌ساله کشور
مصوبات شورای عالی انرژی
دستورالعمل‌های سازمان تنظیم مقررات و ارتباطات رادیویی (ATIC)
ضوابط مرکز ملی فضای مجازی
استانداردهای بین‌المللی:
ISO/IEC ۲۷۰۰۱ (مدیریت امنیت اطلاعات)
NIST SP ۸۰۰-۱۱۵ (راهنمای تست نفوذ)
OWASP Testing Guide (برای تست برنامه‌های تحت وب)
IEC ٦٢٤٤٣ (امنیت سیستم‌های اتوماسیون صنعتی)
PTES (Penetration Testing Execution Standard)
الزامات فنی و امنیتی:
عدم تداخل با سیستم‌های کنترل عملیاتی (OT) در حین تست
رعایت حریم خصوصی و امنیت داده‌ها
استفاده از ابزارهای تست نفوذ مجاز و ثبت تمامی فعالیت‌ها
رمزگذاری داده‌های حساس و دسترسی مبتنی بر نقش (RBAC)
انجام تست‌ها در ساعات غیر(Off-Peak) ☐ برای کاهش ریسک

۷- مشخصات محصول نهایی پروژه: ☑ گزارش ☐ نرم افزار ☐ سخت افزار ☑ دستورالعمل

در صورتی‌که خروجی به‌صورت نرم‌افزار باشد- سیستم‌عامل پیشنهادی: **تحت وب** ☐ **ویندوز** ☐ **اندروید** ☐

سایر .....

مشخصات فنی محصول:

ثبت آسیب‌پذیری: امکان ثبت آسیب‌پذیری‌های شناسایی شده با جزئیات (نوع، سیستم، سطح خط، منبع)

پیگیری و مدیریت وضعیت: پیگیری وضعیت رفع (در حال انجام، حل شده، رد شده)

اولویت‌بندی ریسک: نمایش آسیب‌پذیری‌ها بر اساس سطح ریسک (قرمز، نارنجی، زرد)

پیشنهاد راهکار: ارائه خودکار راهکارهای رفع بر اساس نوع آسیب‌پذیری

۸- واحد بهره‌بردار نتایج تحقیق: .....

۹ - پیش‌بینی مدت‌زمان اجرای پروژه (ماه) : ۱۳ ماه	**۱۰- پیش بینی مبلغ (میلیون ریال):**
نام شخص پیشنهاددهنده پروژه :	**شماره تماس:**

امضاء

دلایل تحقیقاتی بودن

☐ پروژه‌های بهینه‌سازی سیستم‌ها و روش‌ها که با تغییر یا اصلاح در طراحی، عملکرد و بهره‌برداری و با روش‌های شناخته‌شده یا ابداعی و یا تلفیقی انجام‌پذیر می‌باشند.

☐ پروژه‌های طراحی و ساخت سیستم‌ها و دستگاه‌ها برای اولین بار در کشور (مشابه‌سازی و نمونه‌سازی) که باهدف کسب هرگونه دانش فنی طراحی، ساخت و تکمیل تجهیزات و سیستم‌ها انجام می‌شوند.

☐ پروژه‌های بررسی‌های فنی که با بهبود و تغییر روش‌ها و یا توسعه در سیستم‌ها، کاهش هزینه‌های سرمایه‌گذاری و یا بهره‌برداری را به دنبال داشته باشند.

☐ پروژه‌هایی که شامل تلفیق روش‌های موجود و انتخاب روش تلفیقی درزمینهٔ موردنظر باشند. در این پروژه‌ها، بایستی برتری روش تلفیقی بر روش‌های موجود نشان داده شود.

☐ پروژه‌هایی که متضمن کار در مرزهای دانش و فن باشند.

☐ پروژه‌هایی که برای اولین بار روش‌های شناخته‌شده روی سیستم‌ها و تجهیزات را پیاده می‌کنند. فاز اجرایی (عملیاتی) این پروژه‌ها باکار عملی توأم با آزمایش همراه است.

☐ پروژه‌هایی که برای اولین بار با انجام مطالعات موردی مشکلی از مشکلات صنعت برق را حل نمایند.

☐ پروژه‌هایی که شامل آزمایش‌های خاص و غیرمعمول روی سیستم‌ها با روش‌های شناخته‌شده باشند. این آزمایش‌ها، بایستی استاندارد بوده و یا توسط مرجع معتبری تائید شده باشند.

☐ پروژه‌هایی که شامل آزمایش‌های خاص روی سیستم‌ها با روش‌های ابداعی به‌صورت شبیه‌سازی نرم‌افزاری یا سخت‌افزاری باشند. در این پروژه‌ها روش‌های ابداعی با روش‌های استاندارد مقایسه می‌شوند.

☐ مطالعات مرتبط با مدیریت، نیروی انسانی و مسائل اجتماعی که برای اولین بار انجام‌شده و نتایج آن‌ها مورداستفاده در صنعت برق باشد.

☐ مطالعات مرتبط با مسائل مالی و اقتصادی در جهت کاهش هزینه‌های جاری و سرمایه‌گذاری در صنعت برق که برای اولین بار انجام گیرد.

☐ پروژه‌های مشابه با تفاوت اصولی درروش تحقیق، اجرا و یا کاربرد در مناطق مختلف

☐ پروژه‌های باهدف تداوم و تکمیل پروژه‌های انجام‌شده قبلی

☐ پروژه‌های مشابه با تکنولوژی بالا و یا به‌منظور تسریع یا اطمینان در حصول نتیجه و دست‌یابی به فنون مختلف