بسم‌الله الرحمن الرحیم

طرح توسعه و استانداردسازی نرم‌افزاری، زیرساخت سخت‌افزاری، شبکه و امنیت

سازمان منابع طبیعی و آبخیزداری کشور

تهیه و تنظیم: بهار ۱۴۰۲

فهرست مطالب

فهرست شکل‌ها

1 مقدمه

نظام اداری هر کشور به‌مانند یک سازمان یکپارچه، تنظیم‌کننده کلیه فعالیت‌ها و ارائه‌دهنده خدمات عمومی و تخصصی در جهت نیل به هدف‌های تعیین‌شده است. هماهنگی بیشتر بین بخش‌های مختلف نظام اداری، بستری مناسب برای حل مشکلات مردم و حسن اجرای امور فراهم می‌آورد. یکی از مشکلات موجود در روند اداری کشور، رویکرد سنتی و سطح پایین فناوری مورداستفاده است. دگرگونی در نحوه برقراری ارتباط دستگاه‌های دولتی با یکدیگر[1] و همچنین بهبود بخشیدن به روابط و فرایندهای داخلی سازمان‌ها در افزایش سودمندی و بهره‌وری دولت حائز اهمیت است.

ضرورت و درک استفاده از سامانه‌های اطلاعاتی به دلیل ویژگی‌هایی چون سرعت، دقت، سهولت دسترسی و گستردگی، به‌صورت روزافزونی با استقبال سازمان‌ها مواجه گردیده است. ویژگی‌های نظیر استانداردسازی، وحدت رویه در انجام فرایندها، دسترسی‌پذیری آسان و در لحظه، حذف بایگانی‌های فیزیکی و سهولت تحلیل خروجی‌های فرایندها موجب گردیده استفاده از سامانه‌ها و به‌تبع آن رشد فناوری‌های مرتبط با این حوزه در سایر بخش‌ها نظیر زیرساخت سخت‌افزاری، شبکه و امنیت اطلاعات رشد قابل‌توجهی داشته باشد.

مطابق قانون حفاظت و بهره‌برداری از جنگل‌ها و مراتع، مسئولیت بسیار مهمی برعهده سازمان جنگل‌ها، مراتع و آبخیزداری کشور گذاشته شده است. این سازمان به نمایندگی از دولت جمهوری اسلامی ایران مالکیت حدود ۸۳ درصد از کل اراضی کشور را عهده‌دار بوده که در خصوص این اراضی علاوه بر حفظ انفال، مسئول احیا، توسعه و بهره‌برداری اصولی از جنگل‌ها، مراتع و حمایت از آب و خاک کشور نیز می‌باشد. گستردگی و تنوع وظایف و خدماتی که این سازمان ارائه می‌دهد و همچنین وجود حجم زیادی از اطلاعات و داده‌های حساس کشور مانند اطلاعات و اسناد زمین‌های ملی و دولتی، اطلاعات حدنگاری، واگذاری‌ها،

---

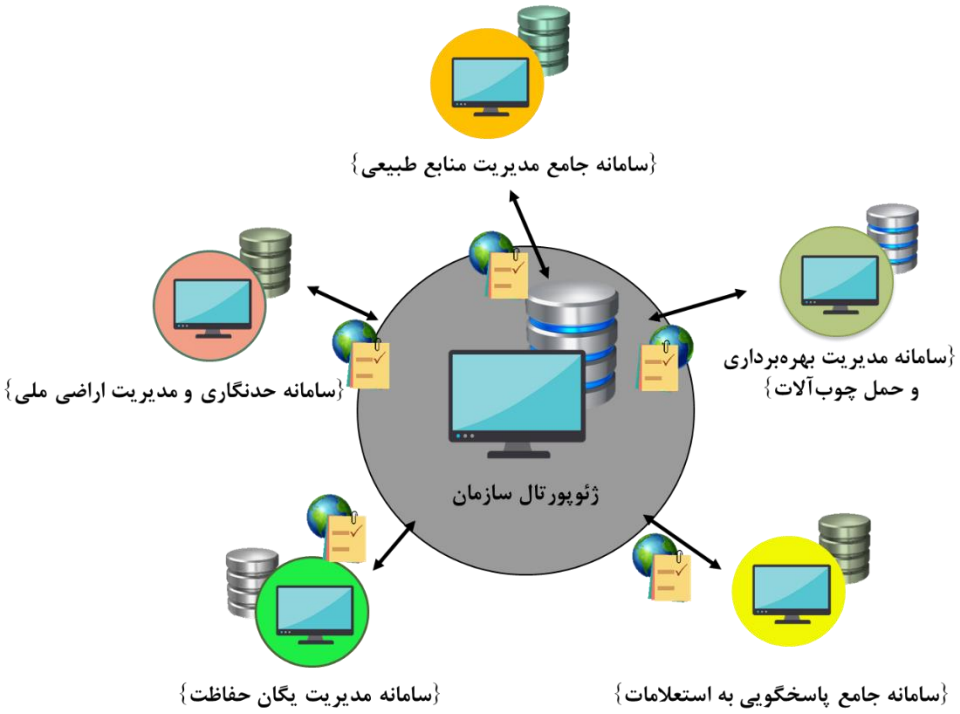
[1] Government to government

مجوزهای بهره‌برداری از منابع طبیعی، در کنار مشکلات مربوط به عدم تمرکز و یکپارچگی ذخیره‌سازی و بهره‌برداری از داده‌های موجود در سیستم‌های نرم‌افزاری مختلف و همچنین وجود تهدیداتی مانند مفقودی یا تخریب فیزیکی اسناد، تهدیدات امنیتی و جنگ سایبری، این سازمان را بر این داشت تا در حوزه وظایف خود، اقدام به اجرا و پیاده‌سازی برنامه جامعی جهت تحقق و توسعه دولت الکترونیک نماید. در راستای پیاده‌سازی سامانه‌های نرم‌افزاری با هدف تامین نیازمندی‌های مذکور ضرورت داشت تا پیش از راه‌اندازی سامانه‌ها نسبت به ایجاد زیرساخت ارتباطی پایدار و مطمئن بین واحدهای سازمان، تامین تجهیزات سخت‌افزاری و امنیت زیرساخت شبکه مرکزی سازمان و ایجاد مرکز داده جدید (مرکز داده سیار که با توجه به اهداف کلان سازمان بتوان از آن به عنوان مرکز داده پشتیبان نیز استفاده نمود) اقدام شود.

2 ایجاد و توسعه سامانه‌های نرم‌افزاری

امروزه با گسترش دولت الکترونیک و لزوم ارائه خدمات فناورانه لزوم استفاده از ابزارهای الکترونیکی بیش از پیش احساس می‌شود. همین نیاز سبب شده بود تا پیش از اجرای این برنامه در حوزه نرم‌افزاری، تعداد زیادی از سامانه‌ها و نرم‌افزارهای مختلف توسط ادارات تابعه این سازمان به صورت جزیره‌ای و بدون رعایت اصول و استانداردهای طراحی، پیاده‌سازی و امنیت در بستر اینترنت راه‌اندازی و بهره‌برداری شود. علاوه‌بر این، مرکز داده پردازشی و ذخیره‌سازی اطلاعات این سامانه‌ها اغلب در خارج از سازمان و توسط شرکت‌های ارائه دهنده نرم‌افزار فراهم شده بود که دارای هیچکدام از الزامات این حوزه نبودند. این وضعیت سبب شده بود که هر لحظه امکان از کار افتادن سامانه، هک و حمله به پایگاه داده سامانه‌ها به دلیل به روز نبودن آنتی‌ویروس‌ها و فایروال‌ها وجود داشته باشد. از دیگر مشکلات این وضع می‌توان به عدم ارتباط بین پایگاه‌های داده مرتبط در سامانه‌ها نیز اشاره نمود. همچنین استانداردهای لازم جهت اتصال سامانه به گذرگاه خدمات دولت (GSB) در اغلب سامانه‌ها رعایت نگردیده بود. در این شرایط با توجه به لزوم بازطراحی فرآیندها و یکپارچه‌سازی بانک‌های اطلاعاتی و سامانه‌های سازمان با رویکرد استانداردسازی موارد مربوط به طراحی، پیاده‌سازی، امنیت و ... آن‌ها سازمان نسبت به ارائه طرح یکپارچه‌سازی سامانه‌های الکترونیکی و متمرکز نمودن پایگاه‌های داده در ستاد سازمان با رعایت ملاحظات زیرساخت، شبکه و امنیت نمود.

سامانه‌های الکترونیکی مورد نظر به ۲ دسته عمومی و تخصصی تقسیم می‌شوند. از یک سو مدیریت گردش اطلاعات عمومی نظیر مکاتبات بین واحدهای درون و برون سازمانی، اطلاعات مالی، بودجه‌ای و ... که از محرمانگی برخوردار بوده مد نظر می‌باشد و از سوی دیگر سامانه‌های تخصصی که مربوط به فرآیندها و خدمات مرتبط با وظایف سازمان در حوزه حفاظت از انفال و اراضی ملی که جزو بیت‌المال بوده برای سازمان دارای اهمیت می‌باشد. با توجه به عمومی بودن سامانه‌هایی نظیر اتوماسیون مکاتبات اداری، مال، حقوق و دستمزد و ... از بیان توضیحات مربوط به آن‌ها صرفنظر می‌شود. در حوزه سامانه‌های تخصصی همان‌گونه که در شکل۱ مشاهده می‌شود، ۵ سامانه یکپارچه تمام فرآیندهای تخصصی مربوط به سازمان را در سطح کشور و به صورت متمرکز مدیریت می‌نماید.



شکل ۱: طرح یکپارچه‌سازی سامانه‌های الکترونیکی سازمان جنگل‌ها، مراتع و آبخیزداری کشور

۱-۲- سامانه مدیریت بهره‌برداری و حمل چوب‌آلات

با توجه به اهمیت موضوع مقابله سیستمی با قاچاق چوب و ساماندهی بهره‌برداری چوب‌آلات، سامانه‌ای جهت مدیریت این زنجیره از قطع تا حمل چوب‌آلات و همچنین صدور الکترونیکی مجوزها در سازمان جنگل‌ها، مراتع و آبخیزداری کشور طراحی و پیاده‌سازی گردید. صدور الکترونیکی مجوزها و ایجاد پایگاه متمرکز جهت جلوگیری از جعل و دسترسی آسان به مجوزهای صادر شده، اختصاص شناسه به چوب‌آلات جهت رهگیری آن‌ها، امکان دریافت گزارش‌های لحظه‌ای و قابلیت ارتباط با سایر سامانه‌های تجاری کشور از نتایج راه‌اندازی این سامانه است.

ضرورت یا هدف

- نظارت بر زنجیره تولید، حمل و توزیع چوب‌آلات در کشور
- مبارزه سیستمی با قاچاق چوب‌آلات در کشور
- حذف روش کاغذی و سنتی به منظور جلوگیری از جعل مجوزها

۲-۲- سامانه جامع پاسخگویی به استعلامات

سازمان جنگل‌ها، مراتع و آبخیزداری کشور با توجه به قوانین مربوط به نمایندگی از دولت جمهوری اسلامی ایران، مالکیت اراضی ملی و دولتی خارج از محدوده و حریم شهر و روستا را عهده دار می‌باشد و لذا تشخیص و تفکیک حریم قانونی اراضی ملی از مستثنیات اشخاص حقیقی و حقوقی و پاسخگویی به استعلامات دستگاه‌های مرجع مستعلم از وظایف اصلی سازمان است.

سامانه استعلامات علاوه بر ایجاد وحدت رویه در فرآیند پاسخگویی به استعلامات انجام شده از سازمان، ادارات کل و شهرستانی تابعه، به صورت مکان محور، امکان پایش به هنگام پاسخ انواع استعلامات مالکیتی و به روزرسانی آنی وضعیت اراضی در سامانه حدنگاری و مدیریت اراضی ملی را نیز مهیا می‌کند.

ضرورت یا هدف:

- پاسخ به کلیه استعلامات دستگاه‌های اجرایی کشور به‌صورت الکترونیکی (موضوع بند (ث) ماده ۶۷ قانون پنجساله ششم توسعه) و از طریق مرکز ملی تبادل اطلاعات
- بهبود بخشیدن و ایجاد وحدت رویه در فرایندهای پاسخ به استعلامات
- تسهیل مدیریت و نظارت بر نحوه اجرای فرایند و تهیه آمار و گزارش‌های یکپارچه در بازهای زمانی مشخص

۲-۳- سامانه حدنگاری و مدیریت اراضی ملی

حدود ۸۰ درصد عرصه کشور را منابع طبیعی (اراضی ملی و دولتی) تشکیل می‌دهند. متولی مالکیت و حدنگاری این اراضی سازمان جنگل‌ها، مراتع و آبخیزداری کشور است. حدنگاری اراضی منابع طبیعی به منظور تشخیص و تفکیک حریم قانونی اراضی ملی و تثبیت حاکمیت دولت بر منابع ملی کشور امری ضروری است. اجرای این امر در بستر سامانه‌ای مکان‌محور موجب می‌گردد زمینه بروز بسیاری از تخلفات زمین‌خواری مسدود گردد. در کنار حدنگاری منابع طبیعی به منظور تفکیک اراضی ملی از مستثنیات اشخاص، مدیریت اقداماتی که روی اراضی ملی صورت می‌گیرد نظیر واگذاری زمین جهت اجرای

طرح‌های معدنی، طرح‌های عمومی و عمرانی دولت و طرح‌های بهره‌برداری از منابع طبیعی نیز از اهمیت بالایی برخوردار است که می‌تواند به تکمیل اطلاعات مکانی و توصیفی مربوط به حدنگاری اراضی کمک شایانی نماید.

سامانه حدنگاری و مدیریت اراضی ملی، امکان ورود، جمع‌آوری و گزارش‌گیری اطلاعات توصیفی و مکانی مرتبط با اراضی ملی را در سازمان فراهم می‌کند به گونه‌ای که با تعیین یک محدوده جغرافیایی، آخرین مالکیت محدوده، منشأ حقوقی مالکیت اراضی ملی یا مستثنیاتی که پیش از این جزء اراضی ملی بوده و وضعیت فعلی عرصه را مشخص می‌نماید .

ضرورت یا هدف:

- ساماندهی و نظارت بر طرح حدنگار اراضی ملی منابع طبیعی
- حفظ و حراست از انفال و اراضی ملی
- حذف بایگانی فیزیکی و کاهش هزینه نگهداری اسناد و اوراق کاغذی

۴-۲- سامانه جامع مدیریت منابع طبیعی

بنا بر ماده ۲ قانون حفاظت و بهره‌برداری از جنگل‌ها و مراتع، حفظ و احیاء و اصلاح و توسعه و بهره‌برداری از جنگل‌ها و مراتع و بیشه‌های طبیعی و اراضی جنگلی بر عهده سازمان جنگل‌ها، مراتع و آبخیزداری می‌باشد. در همین راستا سازمان به‌منظور حفاظت از منابع ملی اقدام به اجرای پروژه‌های متعدد آبخیزداری و آبخوانداری می‌نماید. به‌علاوه مدیریت بهره‌برداری از مراتع، توسط مرتعداران و یا متقاضیان اجرای طرح‌های مرتبط با منابع طبیعی، به‌منظور حفظ و احیا مراتع یک امر ضروری است.

به همین منظور سامانه جامع مدیریت منابع طبیعی در دو بخش طراحی شده است. بخش اول مدیریت و ساماندهی امور مربوط به ارائه خدمات به متقاضیان اعم از صدور و تمدید پروانه مرتعداری، مدیریت بهره‌برداری، حمل و صادرات گیاهان دارویی و ... و بخش دوم مدیریت طرح‌ها و پروژه‌های حفاظتی اعم از پروژه‌های کنترل سیلاب، حفاظت خاک و ... است. طراحی این سامانه به‌گونه‌ای است که قابلیت مدیریت تجمیعی و یکپارچه لایه‌های مکانی مختلف را داشته باشد به‌نحوی‌که اولاً کاربران در بخش‌های مختلف متناظر سطوح دسترسی تعیین شده بتوانند اقداماتی نظیر ورود اطلاعات، ویرایش، پردازش و بهره‌برداری از لایه‌های مکانی و اطلاعات توصیفی را داشته باشند، ثانیاً ارتباط و دسترسی به سایر لایه‌های مکانی موردنیاز بهره‌برداران نظیر لایه‌های پوشش

گیاهی، کاداستر اراضی ملی و ... را بر اساس تقسیم‌بندی‌های حوزه آبخیز برای کاربران سامانه فراهم آورد. در کنار ورود و تکمیل اطلاعات در سامانه، بخش مهم دیگر گزارش‌گیری از سامانه متناسب نیازمندی‌های مدیران سازمان است که این موضوع نیز به‌صورت کاملاً انعطاف‌پذیر در سامانه دیده شده و به‌محض ورود اطلاعات در هر بخش به‌اندازه کافی، طراحی گزارش‌های مدیریتی متناسب با نظر خود مدیران در بخش‌های مختلف انجام خواهد شد.

ضرورت یا هدف:

- هماهنگی بیشتر با سایر بخش‌های مختلف نظام اداری کشور جهت ارتقا کیفیت تعاملات با دستگاه‌های اجرایی
- بهبود بخشیدن و ایجاد وحدت رویه در فرایندها
- دسترسی سریع و بروز به اطلاعات و آمار
- تسریع ارائه خدمات به متقاضیان در حوزه‌های مرتبط با منابع طبیعی
- تشکیل بانک اطلاعاتی کامل و جامع از پروژه‌ها، بهره‌برداران منابع طبیعی، نقشه‌های مراتع و ...

۵-۲- سامانه مدیریت یگان حفاظت

در راستای حسن اجرای وظایف و افزایش اثربخشی اقدامات یگان حفاظت، سازمان جنگل‌ها، مراتع و آبخیزداری کشور اقدام به راه‌اندازی سامانه مدیریت یگان حفاظت نموده است. این سامانه دارای زیرسامانه مرکز تماس جهت استفاده از ظرفیت گزارش‌های مردمی و همیاران طبیعت درخصوص حوادث و یا هرگونه بهره‌برداری غیرمجاز در عرصه‌های منابع طبیعی و ملی می‌باشد. علاوه بر مرکز تماس، عموم مردم و نیروهای حفاظتی می‌توانند با استفاده از اپلیکشن‌های تلفن همراه مخصوص خود هرگونه تخلف یا حادثه را با جزئیات بیشتر به همراه عکس و موقعیت مکانی گزارش نمایند. پس از ثبت گزارش جهت پیگیری و انجام اقدامات بعدی، گردش کار به صورت فرایند محور در سامانه ایجاد شده و با توجه به اهمیت موضوع، در کارتابل فرماندهان یگان و مسئولین استانی و شهرستانی ارجاع خواهد شد. در ادامه نتایج اقدامات صورت پذیرفته در زیرسامانه مدیریت تخلفات و حوادث ثبت و با توجه به نوع آن گردش کار متناسب ایجاد خواهد گردید. اقدام به‌هنگام در جهت جلوگیری از گسترش خسارات به منابع طبیعی،

برخورد قانونی با متخلفین، امکان نظارت بر اجرای احکام و تهیه گزارش‌های مدیریتی به صورت برخط از دیگر نتایج راه‌اندازی این سامانه است.

ضرورت یا هدف:

- دریافت گزارش‌های مردمی مربوط به تخلفات حوزه منابع طبیعی به صورت ۲۴ ساعته و متمرکز در سطح کشور
- ثبت الکترونیکی کلیه پرونده‌های تخلف و نظارت متمرکز بر روند رسیدگی به تخلفات در واحدهای تابعه تا اجرای احکام

با توجه به رشد فناوری اطلاعات و پیاده‌سازی سامانه‌های نرم‌افزاری جدید و توسعه آن‌ها، سازمان جنگل‌ها ناگزیر است متناظر این توسعه، سایر بخش‌های مرتبط با گسترش نرم‌افزارها نظیر به روزرسانی مرکز داده و ارتقا تجهیزات سخت‌افزاری، استانداردسازی ساختمان مرکز داده، امن‌سازی شبکه ارتباطی بهره‌برداران سامانه‌ها و استانداردسازی امنیت نرم‌افزاری و سخت‌افزاری را مطابق با استانداردهای روز فناوری اطلاعات ارتقا دهد. در این راستا، با توجه راه‌اندازی سامانه‌های جدید، ضرورت آسیب‌شناسی وضع سازمان در بخش‌های مذکور و متناظر آن استانداردسازی و بهبود آن‌ها بیش از پیش احساس می‌شود. در بخش بعدی به الزامات این حوزه‌ها و طرح سازمان در این خصوص پرداخته می‌شود.

3 ارتقا و استانداردسازی زیرساخت سخت‌افزاری، شبکه و امنیت

همان‌طور که در بخش قبل اشاره گردید متناظر یکپارچه‌سازی و توسعه سامانه‌های نرم‌افزاری ضرورت دارد تا سازمان نسبت به ارتقا و استانداردسازی سایر بخش‌های مرتبط نیز اقدام نماید. در این خصوص بررسی و شناخت کامل وضعیت زیرساخت سخت‌افزاری، شبکه و امنیت سازمان و متناظر آن آسیب‌شناسی وضع موجود به منظور طراحی وضع مطلوب امری ضروری می‌باشد. در این راستا با بررسی‌های به عمل آمده مواردی احصا شد که سازمان تصمیم گرفت با قید فوریت و در اسرع وقت نسبت به انجام اقدامات لازم در این خصوص، تمام اهتمام خود را به کار گیرد.

در حال حاضر اتاق سرور این سازمان دارای ۷ سرور فیزیکی می‌باشد که بر روی هر سرور چندین سرور مجازی (همانند سامانه اتوماسیون اداری، ارزیابی عملکرد، بانک زمین و استعلامات، همیاران طبیعت، میز خدمت، داشبورد مدیران، بایگانی، هواشناسی، چوب، صندوق توسعه، آنتی ویروس، ایمیل، حضور و غیاب، پرسنلی، حسابداری و ...) وجود دارد. همچنین تعداد ۲ عدد سخت افزار امنیت شبکه (فایروال، فاقد لایسنس)، ۱۰ عدد سوئیچ حیاتی و ارتباطی، ۲ خط اینترنت، ۲ خط MPLS (برای اتصال به شبکه ملی اطلاعات و ادارات منابع طبیعی استانها)، شبکه دولت، دستگاه پشتیبان گیری اطلاعات و دستگاه ذخیره سازی اطلاعات کلیه سرورهای سازمان، در حال سرویس دهی می‌باشند که از سالیان گذشته از لحاظ امنیت، تجهیزات و زیرساخت دارای نواقص و کمبودهای جدی می‌باشند که می‌توان به موارد ذیل اشاره نمود.

۱) عدم امکان دریافت گواهی‌های امنیتی شامل تست نفوذ شبکه ماهر و افتا و همچنین استانداردهای امنیتی به علت مناسب نبودن و ضعف تجهیزات سخت افزاری اتاق سرور که منجر به نواقص امنیتی در شبکه ستاد سازمان شده است.
۲) پایین بودن ضریب امنیت شبکه در مواقع حملات سایبری (DDoS و باج افزارها) و نبود تاب آوری سایبری و عدم امکان پاسخدهی سریع در برابر خطرات.
۳) نبود مرکز عملیات شبکه (NOC) و همچنین مرکز عملیات امنیت (SOC) در ستاد سازمان.
۴) عدم وجود قرارداد سالیانه و نبود اعتبار در راه اندازی مانیتورینگ جامع توسط شرکتهای متخصص.

۵) عدم تجهیز زیرساخت برق اتاق سرور به کابل و تابلوی برق اختصاصی و UPS و ژنراتور که می‌تواند خسارات جبران ناپذیری را به همراه داشته باشد. (از مصادیق بارز آن، قطع شدن طولانی برق سازمان و خاموش شدن کلیه تجهیزات اتاق سرور به تعداد پنج بار از ماه گذشته تا کنون می‌باشد.)

۶) عدم پیکربندی اصولی تجهیزات اکتیو که تهدیدی مهم در خصوص عملکرد صحیح در زمان حملات سایبری به حساب می‌آید.

۷) عدم بازبینی دوره ای چاه ارت و استاندارد نبودن آن.

۸) عدم استاندارد سازی اتاق سرور (شامل سقف کاذب، کف کاذب، سیستم اطفاء حریق، سیستم هشدار دما و رطوبت، سیستم خنک کننده cooling، درب ضد سرقت و سیستم کنترل تردد)

۹) نامناسب بودن محل قرارگیری اتاق سرور و عدم استقامت بنای ساختمانی اتاق سرور در برابر حوادث غیر مترقبه نظیر سیل، زلزله، آتش سوزی، اغتشاشات و ... (شامل حذف پنجره‌ها، دربهای شیشه‌ای و ...)

۱۰) مغایر بودن انجام تغییرات ساختمانی با اصول زیرساخت شبکه سازمان و جزیره‌ای عمل کردن واحدها و نبود مدیریت یکپارچه.

۱۱) نبود زیرساخت ارتباطی پایدار و مطمئن (فیبر) بین واحدهای ساختمانی با اتاق سرور و نبود لینکهای پشتیبان.

۱۲) نبود افزونگی تجهیزات (شامل سرور، سوئیچهای حیاتی و ارتباطی، فایروال، دستگاه ذخیره سازی اطلاعات و ...)

۱۳) عدم وجود سایت دوم شبکه ستاد سازمان به همراه اطلاعات کلیه سرورها در محلی غیر از مکان فعلی.

۱۴) عدم برگزاری دوره‌های تخصصی شبکه و امنیت فناوری اطلاعات توسط شرکتهای معتبر در این زمینه.

۱۵) کمبود نیروی متخصص شبکه و امنیت اطلاعات و نبود امکان جذب نیرو.

۱۶) با توجه به موارد فوق‌الذکر، مطالعات و بررسی‌هایی به منظور رفع مشکلات اساسی سازمان صورت پذیرفت که منجر به ارائه طرحی در چهار حوزه تجهیزات اکتیو (به همراه پیکربندی تجهیزات)، پسیو (کانتینر ، برق ، ژنراتور)، ارتباطات شبکه‌ای (شبکه داخلی Lanو شبکه ارتباطی بین واحدهای ستادی و صف Apn) و امنیت (گواهینامه‌های امنیتی نرم‌افزارها و تست‌های دوره‌ای، راه‌اندازی SOC، استقرار و راهبری SIEM) گردید. در ادامه به توضیح هر یک از این موارد پرداخته خواهد شد.

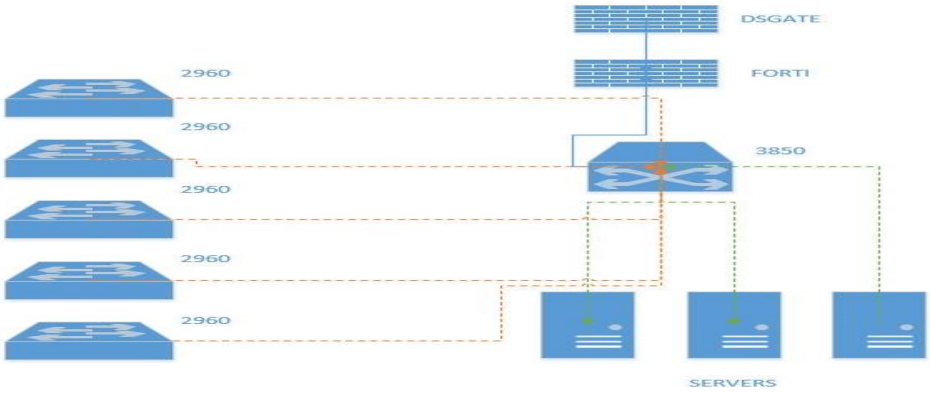
۱-۳- تجهیزات اکتیو

3-1-1- بررسی وضع موجود تجهیزات اکتیو

طی بررسی به عمل آمده در خصوص تجهیزات اکتیو شناخت شرایط موجود به شرح ذیل حاصل گردید.
با توجه به نوع کار سامانه‌ها و سیاست های مرکز داده کلیه سرویس های مرکز داده سازمان جنگلها در سه گروه به شرح زیر تقسیم می‌شوند :

- سرویس Data Base
- سرویس Application
- UI (User Interface)

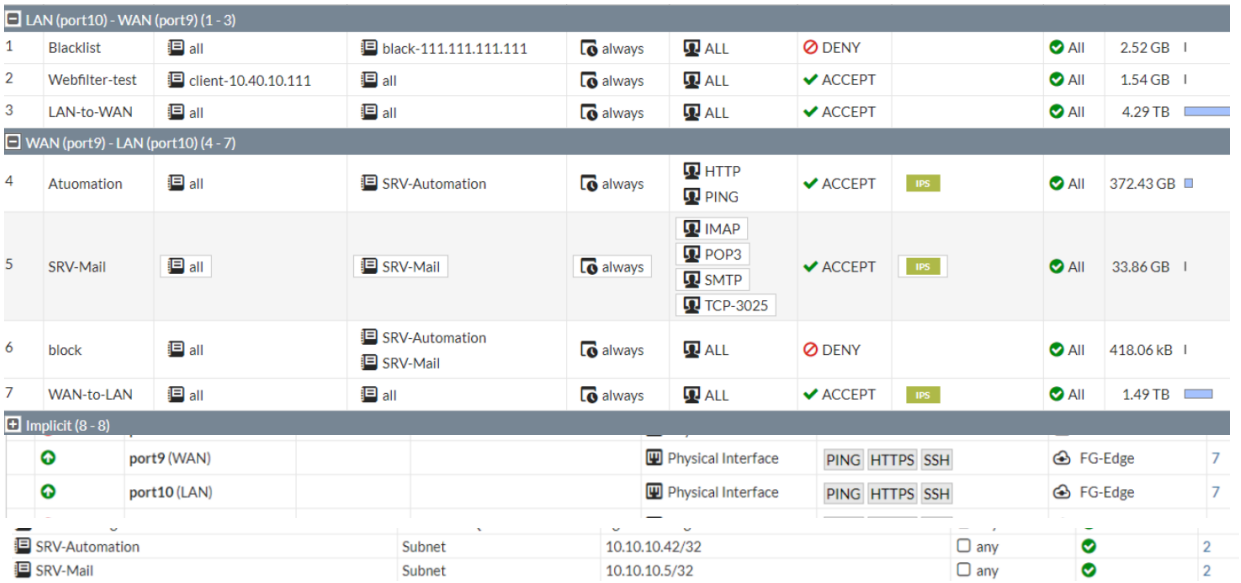
- در طراحی حال حاضر برای ارتباطات فیزیکی از یک Core Switch به عنوان مرکز ارتباطات استفاده گردیده که از نوع سوییچهای سیسکو Cisco-3850-CAT3K میباشد و از سوئیچ های Cisco-2960 به عنوان لایه Access استفاده شده است.
- با ساختار Vlan محدوده ی Broadcast Domain ساختمان‌ها مشخص شده است.
- در سوییچ Core 3850 به ازای هر Vlan یک SVI (Switch Virtual Interfaces) تعریف شده است که با استفاده از آنها Intervlan Routing بین access switchها صورت میگیرد.
- سرورها ، سوییچ های لایه ی Access و فایروال Forti با یک کابل به Switch Core متصل شده اند.
- نقطه ی Edge سازمان یک فایروال DSGATE می‌باشد که سیاست های امنیتی در لبه ی شبکه را مشخص نموده است و ارسال و دریافت ترافیک را کنترل می‌کند.
- یک فایروال Forti قبل از فایروال DSGATE قرار گرفته است که فقط سیاست دسترسی به اتوماسیون داخلی از بیرون را انجام می‌دهد.



شکل ۲: وضعیت موجود طراحی ارتباطات فیزیکی

جهت ارتباط با شبکه دولت نیز یک روتر از طرف سازمان مذکور در داخل سایت قرار گرفته که به یک سرور DL580G7 متصل گردیده و برخی کاربران دبیر خانه با یک کارت شبکه مجزا به سرویس ان متصل می‌گردند.

در بحث ارتباط فیزیکی یک Fortigate-600D صرفاً جهت انتقال ترافیک LAN to WAN و بالعکس مابین سوییچ Core و Fortigate در نظر گرفته شده که یک VDOM به نام FG-EDGE در آن ایجاد گردیده مطابق شکل زیر



شکل ۳: مانیتورینگ فایروال

- ترافیک از سمت اینترنت به سمت داخل شبکه مطابق شکل 3 فقط به ازای دسترسی به سرور Mail و اتوماسیون روی پورتهای مربوطه بسته شده است.

- لازم به ذکر است هیچ کدام از سوییچهای سایت stack نبوده و تمام انها به صورت Stand-alone زیر بار می‌باشند.
- نبود ساختار HA در سوییچ های Core

۲-۳- تجهیزات پسیو

3-2-1- بررسی وضع موجود تجهیزات پسیو

وضعیت تجهیزات پسیو به شرح ذیل می‌باشد:

- رک ۴۸ یونیت ۲ عدد
- Ups فاراتل 20KW ، ۲ عدد

- اتاق سرور (شامل سقف کاذب، کف کاذب، سیستم اطفاء حریق، سیستم هشدار دما و رطوبت، سیستم خنک کننده cooling، درب ضد سرقت و سیستم کنترل تردد) نمی‌باشد.
- بنای ساختمانی اتاق سرور هیچ گونه استقامتی در برابر حوادث غیر مترقبه نظیر سیل، زلزله، آتش سوزی، اغتشاشات و ... ندارد.

3-2-2- طرح پیشنهادی پروژه طراحی، تأمین تجهیزات، نصب و راه‌اندازی زیرساخت فیزیکی مرکز داده

- زیرساخت فیزیکی مرکز داده: تجهیزات مرکز داده شامل موارد زیر می‌باشد:
- کانتینر ماژولار دیتاسنتر
- سیستم الکتریکال که شامل تابلوهای برق، یوپی‌اس، باتری، سیستم زمین (ارتینگ)، صاعقه گیر روشنایی و غیره
- سیستم خنک‌کننده شامل اینروهای گازی، کولرگازی و غیره
- سیستم اعلام و اطفاء حریق
- دوربین مداربسته
- کنترل تردد
- سیستم مدیریت و کنترل زیرساخت فیزیکی
- کابل‌های شبکه

- ابنیه شامل ایجاد سقف و شاسی برای کانتینر ، محوطه سازی و اجرا فنس و درب ها

پروژه مرکز داده ماژولار سازمان جنگل‌ها و مراتع شامل سه مرحله اصلی است :

- مرحله اول، شامل آماده‌سازی فضا جهت نصب کانتینر رک شامل آماده‌سازی ابنیه و زیرساخت‌های ارتباطی برق و فیبر است.
- مرحله دوم، ساخت و حمل کانتینر به محل پروژه
- مرحله سوم، شامل نصب و راه‌اندازی زیرسیستم‌ها و راه‌اندازی گرم مرکز داده ماژولار است. کلیه شرکت‌کنندگان باید ضمن بازدید و بررسی ابعاد و جزییات محل نسبت به ارائه پیشنهاد خود به صورت LOMگارانتی اقدام نمایند.

برق اضطراری (دیزل‌ژنراتور)

با توجه به موجود بودن دیزل‌ژنراتور در مجموعه کارفرما، برق ورودی به کانتینر به صورت Safe است؛ بنابراین تأمین دیزل‌ژنراتور در محدوده این پروژه نمی‌باشد.

۳-۳- شبکه ارتباطی داخل ستاد سازمان

3-3-1- مقدمه و شرح مختصر پروژه

پروژه شامل ۶ قسمت اصلی ذیل می‌شود:

۱) ایجاد ارتباطات Uplink برای ارتباط مرکز داده و ساختمان‌ها؛

۲) ایجاد ارتباطات دوربین‌های ساختمان‌ها و محیط‌های اطراف با مرکز داده و نصب دوربین‌ها؛

۳) تأمین برق مرکز داده از پست اختصاصی سازمان و تهیه و نصب تابلوهای برق؛

۴) ساخت اتاق برق و دیزل ژنراتور؛

۵) تأمین، نصب و راه‌اندازی دو دستگاه دیزل ژنراتور؛

۶) تغییر موقعیت و حجم مخازن سوخت؛

برای موارد فوق اقداماتی نظیر حفاری، لوله‌گذاری، نصب منهول، نصب هندهول یا حوضچه مخابراتی، کابل‌کشی، نصب دکل، بتون‌ریزی، آسفالت‌ریزی، ایجاد اتاق برق و دیزل (الزامات مربوط به کابل برق)، نصب تابلوهای برق، جابجایی دیزل ژنراتور و غیره

لازم خواهد بود که الزامات مربوط به هر کدام از موارد باید به دقت مشخص شود. برای مثال در ادامه به الزامات مربوط به دیزل ژنراتورها اشاره خواهد شد.

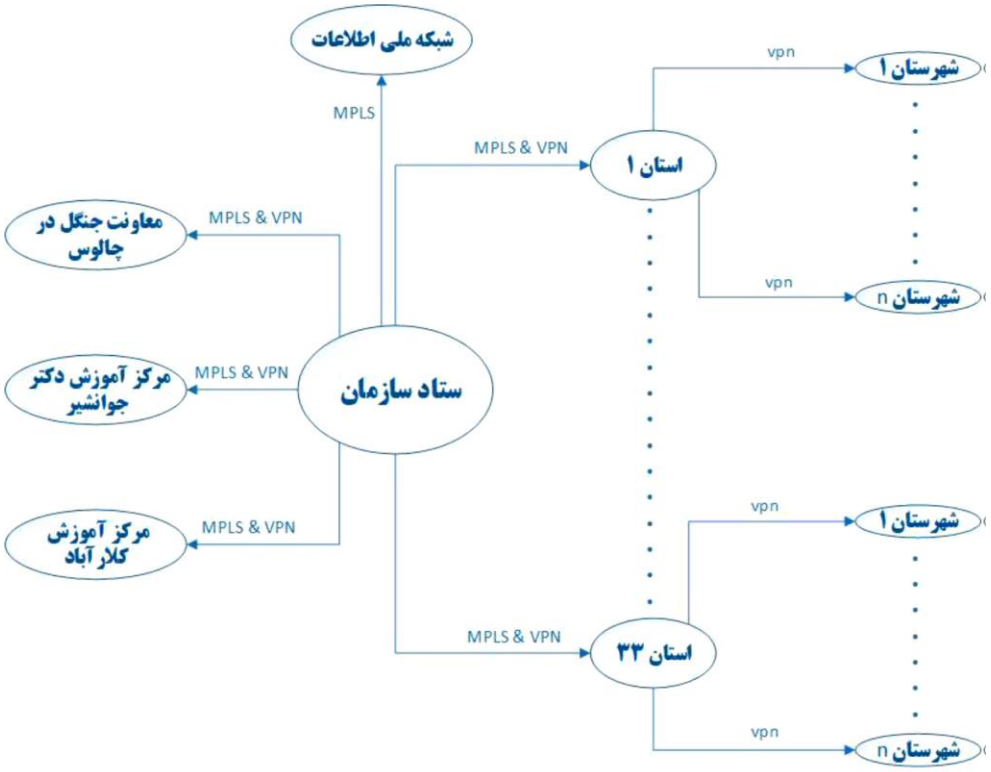
الزامات دیزل‌ژنراتورها

- دو دستگاه دیزل‌ژنراتور با توان Prime معادل 125 KVA مورد نیاز است.
- دیزل‌ژنراتورها باید قابلیت سنکرون با یکدیگر و حفاظت‌های لازم از جمله Reverse Power را داشته باشند.
- در حالت سنکرون نباید جریانی بین دیزل‌ژنراتورها شناور باشد.
- دیزل‌ژنراتور باید قابلیت سنکرون و پارالل شدن با برق نرمال شهری را با رعایت کلیه حفاظت‌ها داشته باشد.
- موتور باید Cummins ساخت کشور آمریکا-انگلیس باشد.
- ژنراتور باید Stamford (ایتالیائی یا انگلیسی) باشد.
- گاورنر باید الکترونیکی باشد.
- موتور، ژنراتور و تابلوهای برق هر کدام باید دارای یک پلاک شامل نام، مدل، مشخصات و پارامترهای فنی، شماره سریال، تاریخ ساخت و غیره باشد.
- دیزل‌ژنراتورها باید دارای کوپل اروپای غربی، آمریکا و یا انگلیس باشد.
- کلیه نیازمندی کنترلی کارفرما باید به طور کامل مرتفع گردد.
- مجهز به مخزن سوخت روزانه در زیر شاسی حداقل برای ۸ ساعت کار مداوم باشد.
- مجهز به محافظ لرزه‌گیرهای فنری مناسب و مورد تایید کارفرما باشد.
- مستندات و مدارک ورود دیزل ژنراتور بصورت پکیج به کشور ارائه شود.
- باید برگه سبز گمرکی دیزل‌ژنراتور به کارفرما تحویل داده شود.
- دارای حداقل دوسال گارانتی و ۱۰ سال خدمات پشتیبانی به همراه آموزش نصب و راه‌اندازی در محل باشد.
- باید چک لیست استاندارد برای تحویل، نصب و راه‌اندازی ارائه شده و کلیه‌ی مراحل مطابق با آن چک لیست‌ها اجرا گردد.
- کلیه دستور العمل‌های تعمیر و نگهداری از جمله دستورالعمل EM، PM و CM به همراه جزئیات و مطابق با نظر کارفرما و ناظر مربوطه ارائه شود. این دستورالعمل‌ها باید به صورتی تدوین گردد که یک اپراتور غیر متخصص نیز بتواند با توجه به آن، EM را رفع نماید.

- کلیه دستورالعمل‌ها باید پیش از تحویل دیزل‌ژنراتورها ارائه شود؛ در صورت ناقص بودن مستندات، تحویل گرفتن دیزل‌ژنراتورها به تعویق خواهد افتاد و کلیه خسارت‌های وارده بر عهده پیمانکار خواهد بود.
- کاتالوگ، User manual، دیتاشیت و Technical Data دیزل‌ژنراتور باید به صورت کامل ارائه شود و به تایید ناظر برسد.
- پارت لیست کلیه قطعات موتور و ژنراتور باید با ارائه همه‌ی جزئیات ارائه شود.
- هر دیزل‌ژنراتور باید یک گرم‌کن رادیاتور و یک گرم‌کن باتری داشته باشد.
- کلیه‌ی کابل‌ها، کلیدها و غیره در سمت تابلو و دیزل‌ژنراتور باید دارای لیبل‌گذاری مناسب باشد.
- هزینه و مسئولیت تحویل، بارگیری، حمل، تخلیه، نصب و راه‌اندازی دیزل‌ژنراتور، کلیه لوازم جانبی و غیره تماماً بر عهده برنده مناقصه است.
- پس از تأیید نماینده کارفرما مبنی بر شروع عملیات نصب و راه‌اندازی، باید نفر متخصص که از قبل به تأیید نماینده کارفرما رسیده باشد عملیات نصب، تست و روشن نمودن دیزل‌ژنراتورها را با نظارت نماینده کارفرما یا مهندس ناظر و مطابق توصیه سازنده دیزل (دفترچه راهنما) انجام دهد.
- پیمانکار متعهد است کلیه‌ی مراحل کار از جمله ایجاد ارتباط بین قطعات و المان‌های مختلف سیستم برق اضطراری را به درستی و مطابق با بروزترین استانداردهای موجود اجرا نموده و از صحت عملکرد سیستم به طور کامل اطمینان حاصل نماید. بدیهی است در صورت مشاهده و وقوع هرگونه اختلال در هر مقطع از قرارداد، کارفرما مخیر است برخورد مقتضی را انجام دهد.

۳-۴- شبکه ارتباطی ستاد سازمان با واحدهای صف

سازمان جنگل‌ها، مراتع و آبخیزداری کشور در جهت دستیابی به اهداف و انجام تکالیف قانونی در اسناد بالادستی اقدام به ایجاد شبکه امن داخلی سازمان در سطح ستاد، ۳۳ اداره کل و بیش از ۴۰۰ اداره شهرستان با همکاری شرکت مبین نت، با هدف دسترسی به سامانه‌های سازمان در بستری امن و پرسرعت نموده است. نمای کلی شبکه سازمان در شکل ذیل نشان داده شده است.



شکل ۴: شبکه ارتباطی ستاد سازمان با واحدهای صف

ایجاد این شبکه داخلی موجب گردیده است امنیت داده‌های سازمان در سطح قابل قبولی برقرار شود اما جهت پوشش کامل در بخش‌های مرزی کشور نیاز به موارد توسعه‌ای در این بخش نیزمی‌باشد.

۵-۳- امنیت

در حوزه امنیت نرم‌افزاری و سخت‌افزاری، علاوه بر مواردی که در بخش‌های گذشته در خصوص امنیت تجهیزات اکتیو، پسیو و شبکه سازمان به صورت اختصاصی اشاره گردید، ضرورت دارد تا در سایر مواردی نظیر جداسازی شبکه اینترنت از شبکه‌های داخلی، انجام تست‌های دوره‌ای (تست نفوذ) و اخذ گواهینامه‌های امنیتی، راه‌اندازی مرکز عملیات امنیت (SOC) و استقرار و پشتیبانی SIEM نیز اقدامات لازم جهت پیاده‌سازی استانداردها و ضوابط ابلاغی، صورت پذیرد. در ادامه توضیحاتی در خصوص هر یک از موارد مذکور ارائه خواهد گردید.

3-5-1- جداسازی شبکه

در راستای قوانین و مقررات بالادستی و تکالیف قانونی، این سازمان در نظر دارد نسبت به جداسازی اینترنت از سایر شبکه های داخلی نظیر شبکه دولت، شبکه ملی اطلاعات و شبکه امن اختصاصی سازمان اقدام نماید. یکی از راه کارهای این حوزه جداسازی با استفاده از اپلیکیشن های مجازی می‌باشد که جهت اجرای این راه کار نیاز به تجهیزات سخت افزاری به شرح ذیل می‌باشد:

منابع مورد نیاز برای ۷۰۰ نفر (ستاد سازمان، چالوس، کلاک، کلارآباد):

- هر ماشین مجازی: برای ۱۶ نفر
- برای ۷۰۰ نفر: ۴۴ ماشین مجازی
- Ram: 36 GB * 44 = 1584 GB → 4 * 512 GB
- CPU: 16 Core * 44 = 704 Core → 4 * Intel Xeon Platinum 8280
- HDD (SSD): 200 GB * 44 = 9 TB → 5 * 3.2 TB (with Raid)
- Server: 2 * HP Proliant DL380 G10
- San Switch: 2 * EMC DS-6510R-B 48P

۳-۵-۲- اخذ گواهینامه امنیتی سامانه‌ها ، تست نفوذ و ...

با توجه به راه اندازی و توسعه سامانه های تخصصی و از سوی دیگر ارتقا روزافزون استانداردهای امنیتی مربوط به این حوزه، ضرورت دارد تا متناظر تهدیدات امنیتی به وجود آمده در حوزه های نرم‌افزاری، به صورت دوره‌ای نسبت به انجام تست‌های دوره‌ای بر روی سامانه‌ها اقدام گردد. در این سازمان نیز با توجه به توسعه سامانه‌های نرم‌افزاری یکپارچه و متمرکز، انجام این تست‌ها بر روی سرورهای سازمان از اهمیت بسیار بالایی برخوردار است که این امر مستلزم اخذ گواهینامه‌های امنیتی افتا برای سامانه‌های نرم‌افزاری و همچنین انجام تست‌های نفوذ، بار، عملکردی و ... بر روی سرورها می‌باشد.

۳-۵-۳- راه اندازی مرکز عملیات امنیت (SOC)

ایجاد مرکز عملیات امنیت (SOC) بمنظور تحلیل و پایش مستمر تهدیدات و مقابله با حملات سایبری در کنار مرکز عملیات شبکه (NOC) و نیز تیم واکنش اضطراری رخدادهای کامپیوتری (CERT) جهت پاسخگویی بلادرنگ به حملات و رخدادهای امنیتی می‌تواند متضمن ادامه سرویسهای کسب و کار و افزایش سطح امنیت و در دسترس پذیری سامانه های حیاتی هر سازمانی شود.

از آنجاییکه هدف حمله کنندگان ، تحت شعاع قرار دادن یک یا چند ضلع از اضلاع مثلث امنیت شامل محرمانگی (Confidentiality)، صحت (Integrity) و در دسترس پذیری (Availability) است و با توجه به اینکه روشها و تکنولوژی های مورد استفاده در حملات سایبری به زیرساختهای داده ای، روز بروز پیچیده تر میشوند ، طراحی و پیاده سازی یک مرکز عملیات امنیت کارا می‌تواند تا حد قابل قبولی ،آسودگی خاطر را برای مدیران کسب و کار و مدیران فن آوری اطلاعات و ارتباطات، در حوزه امنیت به ارمغان آورد.

بنابراین هدف اصلی ایجاد مرکز عملیات امنیت ، محافظت از اصلی ترین دارایی های غیر فیزیکی سازمان ،یعنی اطلاعات و داده های حساس است. طراحی و پیاده سازی مرکز عملیات امنیت برای سازمان جنگل‌ها که تا کنون به صورت جامع به آن نیندیشیده است، کار را بسیار دشوار می‌نماید اما نکته قابل توجه این است که می‌توان با یک نقشه راه مناسب، جهت نیل به این هدف گامهای مؤثری را طی کرد.

هدف اصلی از نقشه راه ایجاد مرکز عملیات امنیت ،طرح ریزی و اجرای مرحله به مرحله فازهای عملیاتی، بر اساس تحلیل شکاف موجود بین وضعیت جاری و وضعیت دلخواه و نیز الویت بندی فازهای مورد نیاز جهت حصول وضعیت مطلوب با در نظر گرفتن سه بعد زمان ، هزینه و اهداف مورد نظر است

در طراحی ساختار و معماری مرکز عملیات امنیت ، توجه به طراحی و پیاده سازی سه جزء سازنده آن ،یعنی فرآیندها ،نیروی انسانی و تکنولوژی (محصولات امنیتی) و بخصوص ایجاد مکانیزمی استاندارد ،جهت ارتباط کارای این سه جزء بر اساس نیازها ،اهداف و بودجه پیش بینی شده می‌تواند نقش بسزایی در شکل گیری این مرکز حیاتی ایفا کند که این سازمان در حال حاضر در مرحله تهیه RFP مربوط به راه‌اندازی مرکز SOC می‌باشد و به محض آماده شدن طرح، اقدامات لازم در خصوص اجرای آن صورت خواهد پذیرفت.

4-5-3- استقرار، پشتیبانی و راهبری SIEM

در این طرح طی دو مرحله استقرار سامانه مربوطه در حوزه SIEM با توجه به آخرین شرایط موجود سازمان اقدام شده و در هر مرحله آموزش‌های لازم را نیز برای کارشناسان سازمان ارائه می‌شود. در این بخش کلیات مربوط به راه‌اندازی سامانه ارائه شده

و پس از انتخاب مجری، قبل از استقرار، مجری باید جزئیات طرح خود را بصورت مکتوب به سازمان ارائه نموده و تأیید وی را جهت انجام آن دریافت نماید.

استقرار اولیه بر اساس شرایط موجود سازمان و حداکثر ۴۰ روز پس از ابلاغ قرارداد باید انجام شود و در آن کلیه تجهیزات و سامانه‌های سازمان و تمامی نقاط ورودی و خروجی شبکه باید پوشش داده شود.

استقرار نهایی پس از پیاده‌سازی توپولوژی جدید شبکه و انتقال تجهیزات به مرکز داده اصلی، انجام خواهد شد.

در مرحله استقرار، مجری موظف است کلیه تجهیزات و سامانه‌های اعلام شده از سوی سازمان را با استفاده از نصب رابط‌های مورد نیاز (Agent) و یا بصورت مستقیم به سامانه متصل، لاگ آنها را دریافت و تحلیل نموده و در صورت نیاز واکنش‌های لازم را بصورت مدیریت شده اعمال نماید. ضروری است مجری طرح تعامل لازم را با توسعه‌دهندگان و راهبران سامانه‌های عملیاتی سازمان جهت تعامل این سامانه‌ها با سامانه SIEM را انجام دهد. ارائه خدمات از راه دور بصورت ۲۴*۷ (در تمامی ساعات شبانه‌روز و در کلیه روزهای سال) توسط تیم کارشناسی مستقر در مرکز MSSP، خدمات پشتیبانی مورد نیاز باید مدنظر قرار داشته باشد. بنابراین زمان پشتیبانی و ارائه خدمات شرکت، ۷ روز هفته و ۲۴ ساعت شبانه‌روز خواهد بود و مسؤلیت اعلام هشدارهای امنیتی نیز بصورت ۱۰۰٪ و در تمامی لحظات به عهده مجری می‌باشد. می‌بایست تنظیمات را به گونه‌ای کانفیگ شود که در صورت شناسایی IPهای مخرب در شبکه سازمان بلافاصله BLOCK ACTION در دستگاه UTM، IPهای مهاجم را مسدود نماید.

داشبوردهای فنی و مدیریتی مناسب جهت بررسی و پایش رخدادهای امنیتی باید مطابق درخواست سازمان تولید و در اختیار سازمان قرارگیرد. این داشبوردها در دو سطح فنی و مدیریتی خواهد بود.

مجری موظف است گزارشات فنی و مدیریتی لازم را در دو قالب زیر ارائه نماید:

الف) گزارشات مدیریتی بصورت دو هفته یک بار

ب) گزارش فنی بعد از وقوع هر رخداد، شامل جزئیات کامل از نوع رخداد، زمان و منشأ وقوع آن، نحوه شناسایی، اقدامات انجام شده جهت مدیریت تبعات رخداد و اقدامات پیشگیرانه لازم جهت جلوگیری از تکرار آن.

مجری متعهد به یکپارچه‌سازی سرویس Threat Intelligenceخود با سایر سرویس‌های امنیتی موجود در سازمان است.

1-4-5-3- شرح و توضیح فعالیت‌های مرتبط با استقرار، پشتیبانی و راهبری SIEM

A. Vulnerability Service
B. Data Enrichment
C. Data Visualization (Custom Dashboard)
D. Threat Intelligence
E. Auto Report
F. Management Report
G. Security Management Review
H. Technical Report
I. Alert Rule Tuning Count
J. Alert Tuning Time
K. Deploy Custom Use Case
L. Incident Investigation Request
M. Customer’s Alarm
N. None Standard Data Source Log Management
Analytical Security Report
O. Product Major Upgrade
P. Asset Management
Q. UEBA Application
R. UEBA Tuning Time
S. Machine Learning Job
T. ML Job Tuning
U. Forensic service
V. Malware Service
W. Compliance Reporting
X. Hunting Service