گام های نقشه راه

۱- تشکیل کمیته اجرایی طرح امن سازی در سازمان

کمیته در سال ۹۹ با عنوان کمیته راهبردی مدیریت و مقابله با تهدیدات سایبری تشکیل و شامل اعضای زیر میباشد :

۱. جناب آقای مهندس نظری منش مدیرکل آمار و فناوری اطلاعات به عنوان عضو و دبیر
۲. جناب آقای صیفوری مدیرکل حراست به عنوان عضو
۳. جناب آقای عزیزی سرپرست دفتر بازرسی مدیریت عملکرد و حقوق شهروندی به عنوان عضو
۴. جناب آقای مهندس امیریان مدیریت بحران و پدافند غیر عامل به عنوان عضو
۵. سرکار خانم عرب احمدی مدیر کل امور مالی و ذیحسابی به عنوان عضو
۶. جناب آقای سند گل نظامی مدیر کل منابع انسانی ، پشتیبانی و رفاه به عنوان عضو
۷. جناب آقای مهندس پولادی عضو هیت مدیره و معاون توسعه و مدیریت و منابع به عنوان عضو و رییس کمیته راهبردی مدیریت و مقابله با تهدیدات سایبری

۲- ایجاد پروفایل و تعیین سطح بلوغ امنیتی موجود سازمان

با توجه به سیاست های شرکت که در زمینه توسعه زیربناهای حمل و نقل در چارچوب برنامه های مصوب و اهداف قوانین برنامه های توسعه ملی کشور است تمرکز امنیت بر روی سرویس های حساس سازمان می باشد.

با تهیه لیستی از این سرویس ها ، هدف گذاری در راستای لزوم شناخت و اشراف بر فناوری های نوین و بهره گیری از آنها در جهت اتخاذ تدابیر صحیح و فنی ، برای پیشگیری از مخاطرات امنیتی ، تشخیص به موقع و مقابله صحیح با مخاطرات انجام می پذیرد.

۳- تعیین سطح بلوغ امنیتی مطلوب سازمان

هدف از این بخش ، تامین فضای تولید و تبادل اطلاعات سازمان و جلوگیری از بروز اختلال در ارائه سرویس های حیاتی آن است. همچنین سازمان نیازمند ساختاری برای تامین منابع مالی بمنظور اجرای اهداف است. با عنایت به مصوبات اولین جلسه کمیته مدیریت امنیت و مقابله با تهدیدات سایبری مورخ ۱۳۹۹/۰۶/۰۳ ، به منظور مدیریت و تامین امنیت زیرساخت های فناوری اطلاعات موارد زیر بررسی و ارائه شد.

۱. سیستم پشتیبان گیری و disaster room

با توجه به تهدیدات و تحریم های سایبری و لزوم ارتقا آمادگی و مقابله کارامد بر اساس بخشنامه های شورای عالی انفورماتیک ، مرکز افتای ریاست جمحوری و سازمان پدافند غیر عامل، به منظور تجمیع و نگهداری صحیح داده ها و حفظ امنیت اطلاعات و دسترسی سریع نرم افزارها به داده ها و پایگاههای اطلاعاتی مورد استفاده در شرکت نیاز به راه اندازی سامانه ذخیره سازی انبوه می باشد. از طریق این سامانه که فضای انبوه ذخیره سازی و دسترسی سریع به داده ها توسط سامانه های متعدد فراهم می گردد. از طرفی سرعت رشد داده های از نظر حجم افزایش یافته و می بایست متناسب با این رشد سخت افزار مناسب نیز تهیه گردد.

جهت تهیه نسخه های پشتیبان از برنامه ها و پایگاههای داده مورد استفاده شرکت نیازمند تدوین استراتژی مناسب برای تهیه فایل های پشتیبان به صورت اتوماتیک و دوره ای می باشد. از طرفی قابلیت بازیابی اطلاعات در کمترین زمان همواره مد نظر بوده است. با توجه به تعدد سرور ها(حدود ۷۰ دستگاه سرور)، پایگاههای داده و نرم افزارها تهیه پشتیبان دستی عملا غیر ممکن و ناکارآمد می باشد. با تهیه این سامانه کلیه عملیات مربوط به ذخیره و بازیابی اطلاعات پشتیبان به صورت سیستماتیک و مکانیزه صورت می پذیرد و امنیت اطلاعات شرکت کاملا تامین می گردد.

جهت تداوم سرویس دهی در زمان بروز حادثه طبیعی و غیر طبیعی ملزم به ایجاد یک سایت disaster در خارج از ساختمان و استقرار تجهیزات و کپی یک نسخه از اطلاعات و ایجاد امنیت در نگهداری اطلاعات میباشیم .

۲. فایروال بومی

با توجه به تحریم های سایبری و به روز نشدن فایروال های خارجی و امکان نفوذ و بک دور در این سخت افزار ها و بر اساس بخشنامه های مکرر سازمان پدافند غیر عامل نیاز به تهیه دو دستگاه فایروال بومی در لبه شیکه جهت جلوگیری از حملات و نفوذ احتمالی می باشد .

۳. SOC (مرکز عملیات امنیت)

با توجه به حملات و تهدیدات استفاده از soc راهکار اجتناب ناپذیر در شرکت است. مرکز عملیات امنیت (SOC) واحدی است که یک تیم امنیت اطلاعات را برای نظارت و تجزیه و تحلیل وضعیت امنیتی سازمان به طور مستمر در خود جای داده است. هدف تیم SOC کشف، تحلیل و پاسخ به حوادث امنیت سایبری است .طی بررسی انجام شد برای ۲۰۵ نقطه مورد نیاز EPS (تعداد رویدادهایی که در واحد ثانیه توسط تجهیزات و برنامه های کاربردی تولید می شود) برای هر دستگاه برابر با ۵۱۸,۶۲۵ می باشد . با این توضیح میزان حجم رویداد برای هر روز در شرکت حدود ۳۶,۹۳ گیگابایت می باشد .

۴. ISMS (سیستم مدیریت امنیت اطلاعات)

سیستم مدیریت امنیت اطلاعات ابزاری برای شناسایی، مدیریت و به حداقل رساندن احتمال وقوع تهدیداتی است که بواسطه از دست دادن اطلاعات با آنها مواجه خواهیم شد . این موارد مشتمل بر تهدیدات داخلی شرکت ، تهدیدات خارجی شرکت ، تهدیدات اتفاقی و تهدیدات ناشی از خطاهای عمدی و غیر عمدی است. هدف اصلی این سیستم برقراری مکانیسمی برای حفاظت از این موقعیت ها می باشد.طبق بخشنامه شماره ۸۶-۱۳۷۱۱/م/۳۸۵۰۵ مورخ ۱۳۸۶/۰۸/۱۰ معاون اول محترم رئیس جمهور، کلیه دستگاههای دولتی و غیردولتی موظف به تهیه طرح سیستم مدیریت امنیت اطلاعات (ISMS) شدند و همچنین با توجه به اهمیت این سیستم مدیریتی در کشور طبق مصوبه هیات وزیران کلیه دستگاه‌های اجرایی مشمول ماده پنج قانون خدمات کشوری، ملزم شدند نسبت به پیاده‌سازی سامانه مدیریت امنیت اطلاعات ISMS اقدام نمایند.

۴- تدوین برنامه عملیاتی امن سازی

موارد مطروحه در فاز سوم نقشه راه در جلسه کمیته مدیریت امنیت و مقابله با تهدیدات سایبری مورخ ۱۳۹۹/۰۶/۰۳ مصوب گردیده است فلذا با توجه به الزام دریافت مشاوره از شرکت های دارای پروانه خدمت "مشاوره و استقرار استانداردهای مدیریت امنیت اطلاعات" از مرکز افتا، مذاکراتی با برخی از این شرکت ها صورت گرفته است که نیازمند بررسی ، تائید و تامین منابع مالی از طرف اعضا کمیته اجرایی طرح امن سازی در سازمان می باشد. لازم به ذکر است که اجرای فازهای بعدی نقشه راه مستلزم انجام کامل این فاز می باشد .

۵- تایید برنامه عملیاتی امن سازی توسط مرکز افتا

۶- پیاده سازی برنامه عملیاتی امن سازی

۷- ممیزی اجرای برنامه عملیاتی

محمودرضا نظری منش

مدیر کل دفتر آمار و فناوری اطلاعات