ریاست جمهوری
مرکز مدیریت راهبردی افتا
خلیج همیشه فارس

مرور سریع

طرح امن سازی زیرساخت های حیاتی در قبال حملات سایبری

مروری بر

طرح امن‌سازی زیرساخت‌های حیاتی

در قبال حملات سایبری

به منظور هدایت فعالیت‌ها و اقدامات دستگاه‌ها جهت تقویت امنیت و استحکام زیرساخت‌های حیاتی کشور، مرکز مدیریت راهبردی افتای ریاست جمهوری نسبت به تدوین نسخه دوم «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» اقدام نموده است.

در این نوشتار مهمترین بخش‌های این طرح در قالب عناوین ذیل مرور می‌شود:

- ضرورت و ابعاد اجرای طرح امن‌سازی
- اهداف و مأموریت‌های طرح
- اصول طرح امن‌سازی
- نقشه راه اجرای طرح امن‌سازی
- الزامات طرح امن‌سازی
- مدل بلوغ طرح امن‌سازی
- ممیزی برنامه عملیاتی

مروری بر

طرح امن‌سازی زیرساخت‌های حیاتی

در قبال حملات سایبری

فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد.
Cyberspace is as important as Islamic Revolution

ضرورت و ابعاد اجرای طرح امن‌سازی

زیرساخت‌های حیاتی نیازمند سازوکاری برای حفظ محرمانگی، یکپارچگی و دسترس‌پذیری دارایی‌های خود می‌باشند.

امروزه اکثر فعالیت‌های سازمان‌ها و آحاد مردم در فضای تولید و تبادل اطلاعات انجام می‌شود.

تهدیدات و آسیب‌پذیری‌های این فضا مواردی همچون امنیت، اقتصاد، ایمنی و سلامت عمومی را در معرض خطر قرار می‌دهد.

مخاطبان طرح

کلیه زیرساخت‌ها و دستگاه‌های دارای طبقه‌بندی کشور

به فراخور نیاز، سایر دستگاه‌ها می‌توانند از آن استفاده کنند.

فرآیند بازنگری طرح

شامل توسعه و به‌روزرسانی تمام اسناد لازم برای اجرای طرح

در دوره‌های منظم ۳ ساله انجام خواهد شد.

اسناد بالادستی طرح

سیاست‌های کلی نظام در حوزه افتا

ماده ۱۰۹ قانون برنامه ۵ ساله ششم توسعه کشور

نظام ملی پیشگیری و مقابله با حوادث فضای مجازی

اهداف و مأموریت‌های طرح

هدف

ارتقاء و تأمین امنیت فضای تولید و تبادل اطلاعات سازمان و جلوگیری از بروز اختلال در ارائه سرویس‌های حیاتی

مأموریت‌ها

- ارتقاء آمادگی زیرساخت‌ها در برابر حوادث
- اتخاذ تصمیمات آگاهانه با اشتراک و تحلیل اطلاعات
- هدایت اقدامات زیرساخت‌ها
- ارتقاء دانش امنیتی متولیان زیرساخت‌ها
- ایجاد سطح قابل‌قبول امنیت سایبری
- کمینه‌سازی پیامدهای نامطلوب حوادث سایبری
- بهره‌گیری از تدابیر صحیح در مقابله با مخاطرات
- امکان ارزیابی وضعیت امنیتی زیرساخت‌ها
- بسیج ظرفیت بخش خصوصی
- حمایت و تقویت صنعت بومی افتای کشور

اصول طرح امن‌سازی

الزامات طرح، کلی و عمومی هستند و در تمام سازمان‌ها علی‌رغم نوع، اندازه و ماهیتی که دارند، کاربرد دارد.

اگر سازمانی دارای یک سیستم مدیریت امنیت اطلاعات است، بهتر است الزمات طرح را در قالب آن برآورده نماید.

سازمان نیازمند ساختاری برای تأمین منابع انسانی و مالی برای اجرای طرح است.

در صورت حذف هریک از الزامات

مخاطره ناشی از عدم اجرای آن باید مورد پذیرش قرار گیرد.

توجیه حذف الزام باید در قالب مدارک و شواهد لازم ارائه گردد.

مدیر ارشد سازمان باید اطمینان حاصل کند که ...

خط مشی امنیت اطلاعات ایجاد شده است.

خط مشی امنیت اطلاعات در سازمان مستقر گردیده است.

الزامات طرح در فرآیندهای سازمان جریان پیدا کرده است.

پشتیبانی از افراد به منظور مشارکت در اثربخشی طرح صورت می‌پذیرد.

دستاوردهای مورد انتظار طرح به دست می‌آید.

اختیارات اعضای کمیته اجرای طرح ابلاغ شده است.

اختیارات نظارت و گزارش‌دهی تعیین شده است.

اهمیت امنیت اطلاعات در سازمان ابلاغ شده است.

منابع مورد نیاز طرح در دسترس است.

نقشه راه اجرای طرح امن‌سازی

زیرساخت‌های حیاتی لازم است براساس گام‌های نقشه راه نسبت به اجرای طرح امن‌سازی اقدام نمایند. این فرآیند تکراری بوده و زمان شروع و مدت زمان لازم برای اجرای یک چرخه کامل از فرآیند فوق، با توجه به نیازمندی‌های سازمان و تعامل با مرکز افتا تعیین می‌گردد.

نقشه راه اجرای طرح امن‌سازی (ادامه...)

تشکیل کمیته اجرای طرح امن‌سازی

هر سازمان در اولین جلسه کمیته اجرای طرح امن‌سازی باید شیوه‌نامه آن را که دربرگیرنده نقش‌ها و نحوه برگزاری جلسات و شیوه هماهنگی و اجرای امور است، به تصویب برساند.

مسئولیت هدایت کمیته بر عهده ریاست سازمان یا معاونت فنی می‌باشد.

دبیر کمیته مسئولیت برگزاری جلسات و همکاری با ممیزان مرکز افتا را بر عهده دارد.

اعضای کمیته اجرای طرح امن‌سازی

- مدیر ارشد سازمان
- مدیر ارشد فناوری اطلاعات
- مدیر ارشد امنیت
- نماینده حراست
- مدیر ارشد امور اداری
- مدیر ارشد حوزه صنعتی
- حداقل ۲ کارشناس ارشد حوزه امنیت

وظایف کمیته

- تعیین محدوده اجرای طرح امن‌سازی
- تعیین فرآیندهای شروع و پیشبرد
- تأمین نیروی انسانی
- تعیین نقش‌ها و وظایف
- اتخاذ تصمیمات راهبردی
- ارائه گزارش‌های دوره‌ای اجرای طرح به مرکز افتا
- نظارت بر اجرای طرح

تعیین سطح بلوغ موجود

تعیین وضعیت جاری سازمان شامل سیاست‌ها، دارایی‌ها، حوزه کسب‌وکار و ...
و تعیین سطح بلوغ امنیتی موجود بر اساس آن

تعیین سطح بلوغ مطلوب

پس از شناخت وضعیت کنونی باید سطح بلوغ امنیتی مطلوب (براساس سطح قابل پذیرش مخاطرات) در چارچوب الزامات طرح تعیین شود.

تعیین سطح بلوغ امنیتی مطلوب با ...

نوع مأموریت ● سیاست‌های داخلی ● بودجه تخصیص یافته ● نیروی انسانی متخصص

نقشه راه اجرای طرح امن‌سازی (ادامه...)

تدوین برنامه عملیاتی	این برنامه باید گام‌های عملیاتی سازمان برای ارتقاء سطح امنیت را مشخص کند.	تأیید برنامه عملیاتی: برنامه عملیاتی پس از تهیه توسط کمیته باید به تأیید مرکز افتا برسد.
پیاده‌سازی برنامه عملیاتی	پس از تأیید برنامه، سازمان باید نسبت به اجرای فازهای عملیاتی آن اقدام نماید.	در صورت نیاز، فرآیند برون‌سپاری از طریق شرکت‌ها و محصولات دارای مجوز افتا انجام خواهد شد.
ممیزی برنامه عملیاتی	پس از پیاده‌سازی برنامه، سازمان باید روال‌های اجرای ممیزی داخلی را تدوین و اجرا نماید.	ممیزی‌های خارجی توسط مرکز افتا یا بخش خصوصی مورد تأیید مرکز انجام می‌شود.

الزامات طرح امن‌سازی

مرکز افتا با درنظرگرفتن اولویت و محدودیت منابع در اختیار هر زیرساخت، با آن‌ها تعامل خواهد کرد.

سطح بلوغ امنیتی مطلوب در هر الزام براساس سطح قابل پذیرش مخاطرات تعیین خواهد شد.

مروری بر

طرح امن‌سازی زیرساخت‌های حیاتی

در قبال حملات سایبری

الزامات طرح امن‌سازی

مدیریت مخاطرات

مدیریت مخاطرات (راهبرد اصلی طرح امن‌سازی) فرآیندی مستمر است که در آن تهدیدات و آسیب‌پذیری‌های موجود شناسایی، ارزیابی و مدیریت می‌شوند.

برای مدیریت مخاطرات باید ...

- بافتار سازمان شناسایی شود.
- ارزشیابی مخاطرات صورت پذیرد.
- طرح مقابله با مخاطرات تهیه و اجرایی شود.
- مخاطرات به طور منظم مورد بازبینی قرار گیرد.

پایش و کنترل سایبری

با هدف پایش و کنترل سایبری باید ...

- مرکز عملیات امنیت متناسب با مأموریت‌های سازمان ایجاد شود.
- مرکز عملیات امنیت سازمان به صورت امن به مرکز عملیات امنیت ملی افتا متصل شود.

مدیریت حوادث سایبری

با هدف مدیریت حوادث سایبری در سازمان باید ...

- واحد امداد سایبری متناسب با مأموریت‌های سازمان ایجاد شود.
- سازوکاری برای اعلام حوادث سایبری به مراجع بالادستی اندیشیده شود.

مدیریت تداوم کسب‌وکار

رویکردهای سنتی تمرکز خود را فقط بر بازیابی و ترمیم قرار می‌دادند، در حالیکه در رویکرد نوین به هر دو جنبه پیشگیری و مقابله توجه می‌شود.

گام‌های فرآیند مدیریت تداوم کسب‌وکار

- شناخت منابع و سرویس‌های حیاتی سازمان
- تحلیل اثرات کسب‌وکار
- تدوین طرح‌های مدیریت تداوم کسب‌وکار
- تمرین، نگهداری و بازنگری

مدیریت هویت و دسترسی

به منظور مدیریت مؤثر هویت و دسترسی‌ها در سازمان باید ...

- هویت‌های دیجیتال تعریف شوند.
- ایجاد و مُجازشماری دسترسی به منابع و دارایی‌ها در سازمان انجام شود.
- در مواقع لزوم هویت و دسترسی‌های غیرمورد نیاز حذف گردد.
- اقدامات لازم در حوزه حفاظت فیزیکی انجام گیرد.

الزامات طرح امن‌سازی (ادامه...)

زیرساخت محرمانگی

به منظور جلوگیری از افشای اطلاعات محرمانه باید زیرساخت محرمانگی و استنادپذیری در سازمان استقرار یابد.

تمامی کاربردهای زیرساخت محرمانگی و استنادپذیری در بستر زیرساخت کلید عمومی قابل تحقق است.

مدیریت تهدیدات بدافزاری

با هدف پیشگیری از تهدیدات بدافزاری باید ...

واحد مقابله با بدافزار متناسب با مأموریت‌های سازمان ایجاد گردد.

سامانه‌های حفاظتی در تمامی درگاه‌های ورود اطلاعات به سازمان استقرار یابد.

مدیریت زنجیره تأمین

مهمترین اقدام برای شناسایی به موقع موارد نفوذ و اختلال در زیرساخت‌های حیاتی کشور، مدیریت همه جانبه فنی و حفاظتی زنجیره تأمین در فرآیند طراحی، پیاده‌سازی، بهره‌برداری و نگهداری می‌باشد.

برای مدیریت مؤثر زنجیره تأمین در سازمان باید ...

نقش‌ها و مسئولیت‌های متولیان تعیین شود.

آموزش‌های امنیتی مورد نیاز واحدهای مختلف ارائه شود.

سازوکار لازم برای ارزیابی امنیتی محصولات ایجاد شود.

سازمان ملزم به برون‌سپاری برخی از خدمات و رعایت ملاحظات امنیتی مطابق با اسناد بالادستی گردد.

ملاحظات امنیتی تأمین محصولات تخصصی حوزه کسب‌وکار سازمان رعایت شود.

آموزش و فرهنگ‌سازی

بی‌شک کارکنان دارای دانش و آگاهی سایبری یکی از مهمترین خطوط دفاعی در تأمین امنیت سازمان هستند.

به منظور فرهنگ‌سازی سایبری در سازمان باید ...

بر اساس برنامه تدوین‌شده، دوره‌های آموزشی مورد نیاز تشکیل گردد.

سالانه حداقل یک همایش عمومی به منظور ارتقاء فرهنگ امنیت سایبری برگزار شود.

مدل بلوغ طرح امن‌سازی

به منظور سنجش توانایی‌های سازمان، ۱۰ دامنه منطبق با الزامات طرح در نظر گرفته شده که هر یک شامل یک سری اهداف و اقدامات است.

با هدف ایجاد قابلیت سنجش پیشرفت سازمان، هر دامنه به سطوحی که به آن سطح شاخص بلوغ گفته می‌شود، تقسیم شده است.

سطوح بلوغ امنیتی طرح عبارتند از...

سطح بلوغ ۱ ﴿ تعریف شده﴾
وضعیت موجود شناسایی و برخی اقدامات اولیه انجام شده است.

سطح بلوغ ۲ ﴿ مدیریت شده﴾
برنامه لازم برای دستیابی به هدف، تدوین و قدمی در جهت بهبود امنیت برداشته شده است.

سطح بلوغ ۳ ﴿ امن ﴾
اقدامات لازم در قالب فرآیندهای مربوطه به صورت منظم و دوره‌ای انجام می‌شود.

سطح بلوغ ۴ ﴿ بهینه شده﴾
فعالیت‌های لازم در قالب فرآیندهای بهبودیافته و به صورت یک فرهنگ سازمانی صورت می‌پذیرد.

نمای کلی از دامنه‌ها و اهداف مدل بلوغ امنیت سایبری در صفحه بعد ارائه شده است.

ممیزی برنامه عملیاتی

به منظور اطمینان از اثربخشی اجرای برنامه عملیاتی امن‌سازی، مرکز افتا موظف است کلیه ممیزی‌ها را بر اساس ابزار ارزیابی سطح بلوغ ارائه شده، مدیریت و سازمان را از نتیجه آن مطلع نماید.

سازمان برای انجام ممیزی (داخلی یا خارجی) باید اقدامات ذیل را به انجام رساند

- هماهنگی برای برگزاری ممیزی با ذینفعان
- نظارت داخلی بر کیفیت انجام ممیزی‌ها
- پیگیری نتایج ممیزی‌های انجام شده
- پیگیری انجام اقدامات اصلاحی

فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد.
Cyberspace is as important as Islamic Revolution

نمای کلی از دامنه‌ها و اهداف مدل بلوغ امنیت سایبری