وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز مدیریت، توسعه و اعتباربخشی
نظام ملی مدیریت امنیت اطلاعات

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۱۴ : پیوستگی عملیات

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	تیر ۹۰
نگارش سند	۱
تعداد صفحات	۷
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات ایران
کد سند	R90040414

هدف:

هدف از تدوین این توصیه نامه بیان لزوم وجود طرح پیوستگی عملیات برای مقابله با شرایط اضطراری است که ممکن است ادامه ارائه خدمات رایانه ای سازمان را تهدید کنند.

ضرورت:

اگر ارائه خدمات در سازمان های بزرگ متوقف شود احتمالاً پیامدهای وخیمی به دنبال خواهند داشت. ساده ترین این پیامدها می تواند زیان مالی و در شرایط بدتر تهدید جان یا آبروی افراد باشد. ممکن است این پیامد ها منجر به تهدید امنیت ملی یا اغتشاشات اجتماعی گردد.

ارائه خدمات سازمان ها به صورت روزافزون به تجهیزات رایانه ای (سخت افزار و نرم افزار) و خطوط مخابراتی وابسته شده است. تعداد و شدت حمله های رایانه ای در حال افزایش است و با توجه به گسترش سریع فناوری های اطلاعاتی از یک طرف و رقابت های سیاسی یا منطقه ای از طرف دیگر، انتظار می رود این روند با شدت بیشتری افزایش یابد. همچنین ممکن است حوادث طبیعی موجب ایجاد شرایط اضطراری شوند.

بنابراین لازم است طرح های لازم برای پیشگیری از توقف ارائه خدمات در سازمان ها یا مقابله با رخدادهای رایانه ای و احیای سیستم پس از در یافت ضربه، تعریف و اجرایی شود.

الزامات:

- لازم است هر سازمان طرح ساختارمندی برای مقابله با شرایط اضطراری و تضمین پیوستگی عملیات تدوین نماید. این طرح حداقل باید حاوی مواد زیر باشد:

۱ - شناخت ماموریت و عملکرد سازمان با توجه به اهداف استراتژیک آن.

۲ - شناخت منابعی که برای اجرای فعالیت های حیاتی باید در دسترس باشند.

۳ - پیش بینی شرایط اضطراری و حوادثی که ممکن است منجر به فاجعه شوند. این پیش بینی باید بر اساس نتایج حاصل از ارزیابی ریسک انجام پذیرد.

۴ - انتخاب روش (استراتژی) مناسب برای مقابله با شرایط و حوادث منجر به فاجعه

۵ - تامین ابزار و منابع لازم برای پیاده سازی استراتژی های مربوط به مقابله با شرایط اضطراری

۶ - آزمایش و درصورت لزوم تغییر در ساختار طرح

- لازم است کلیه منابع لازم برای تداوم عملکرد سازمان اعم از پردازشی و غیر پردازشی شناسایی شده و میزان نیاز به هر یک در جهت حفظ حداقل توان عملیاتی سازمان ارزیابی شود. تجزیه و تحلیل منابع باید به وسیله افراد آگاه از نیازهای عملیاتی سازمان انجام شده و طی آن به روابط درونی بخش ها با یکدیگر و تاثیر وجود هر یک از منابع بر منابع دیگر توجه شود.

- پیش بینی منابع انسانی جایگزین برای انجام برخی از فعالیت ها که نیاز به تخصص خاصی دارند ضروری است. همچنین لازم است آموزش های لازم برای تسلط سریع بر اوضاع، پیش بینی شده و به افراد مستعدی که به نظر می رسد توانایی تطبیق سریع با شرایط را دارند ارائه شود.

- به طور کلی لازم است در طرح های اضطراری بر حفظ قدرت پردازش، تمرکز و تاکید شود.

- از آنجا که ممکن است در شرایط اضطراری از سکوهای سخت افزاری جدید یا متفاوت استفاده شود لازم است سازگاری نرم افزارهای کاربردی، سیستم عامل، پیکربندی نرم افزار و سخت افزار و عوامل فنی دیگر، در نظر گرفته شوند. با توجه به پیچیدگی و تعدد عوامل لازم است برنامه ای دوره ای برای بررسی و تایید سازگاری سیستم ها (نرم افزاری و سخت افزاری) تدوین شود.

- علاوه بر حفظ توان پردازشی، حفظ توان ارتباطی نیز ضروری می باشد. بنابراین لازم است کانال های مخابراتی مستقل از یکدیگر به کارگرفته شود. تنوع و تعدد این کانال ها با توجه به نیاز سازمان به تبادل داده‌ها تعیین می شود.

- لازم است در طرح های پیوستگی عملیات سازمان های حساس و حیاتی، چگونگی تامین محیط امن کاری، فضای اداری، سیستم گرمایش، سیستم سرمایش، سیستم تهویه، آب، برق، فاضلاب و مجموعه ای از وسایل دیگر از قبیل میز و صندلی، تلفن، فاکس، کامپیوترهای شخصی و فایل ها مورد توجه قرار گیرد.

- لازم است در تدوین طرح پیوستگی عملیات حداقل به سه مرحله زیر توجه نموده و در مورد زمانبندی اجراء و تامین منابع هر یک تصمیم گیری شود:

- صدور پاسخ اضطراری: شامل اقدامات اولیه ای است که به جهت حفظ بقا، محدود سازی حوزه اثر فاجعه و کاهش خسارت صورت می گیرد.

- احیاء و بازیابی سیستم: شامل اقداماتی جهت بازیابی ترتیبیِ ظرفیت از پیش تعریف شده ارائه خدمات در زمان معین. (به عنوان مثال بازگشت به ۶۰٪ ظرفیت پردازش قبل از فاجعه در زمان حداکثر چهار ساعت پس از وقوع یا کشف فاجعه).

- ارائه مجدد سرویس: شامل زمانبندی و ترتیب بازگشت به وضعیت عادی ارائه خدمات (تامین ظرفیت ۱۰۰٪ در زمانی قابل قبول).

- اگر پس از برنامه‌ریزی‌ها معلوم شود منابع مالی یا انسانی در دسترس سازمان برای مقابله با شرایط اضطراری کافی نیست باید مراتب به اطلاع مدیریت ارشد سازمان و از طریق سلسله مراتب به اطلاع مراجع بالادستی رسانده شود. انتقال از عملیات دستی به عملیات رایانه ای (و به طریق اولی از عملیات غیر شبکه به شبکه ای) در شرایطی که تامین طرح پیوستگی عملیات ناممکن است ممنوع است مگر آن که گزارش رسمی ارزیابی ریسک آن به اطلاع مدیریت ارشد سازمان رسیده و مدیریت ارشد موافقت خود را با انتقال کتباً اعلام نموده باشد.

- لازم است طرح های پشتیبان گیری و بازیابی نسخه پشتیبان با توجه به نیازهای طرح پیوستگی عملیات و احیای سیستم تدوین شوند.

- مسئولیت هریک از افراد در اجرای هر بخش از طرح پیوستگی عملیات باید از پیش تعیین شده و به اطلاع افراد رسیده باشد.

- مکانیزم آغاز طرح پیوستگی عملیات و احیای سیستم باید از پیش تعریف شده باشد به نحوی که افراد برای ایفای نقش خود منتظر احکام اداری نمانند. البته لازم است ریسک های اجرای بی مورد طرح نیز بررسی و مکانیزم های لازم برای کنترل آن پیش بینی شود.

- صحت و کفایت اجزای طرح باید طی مانور و شرایط تمرینی به آزمایش گذاشته شود.

- اگر فقط بخش هایی از شبکه سازمان دارای اهمیت حیاتی باشد، تدوین طرح پیوستگی برای آن بخش(ها) کفایت می کند. انتخاب بخش های پر اهمیت بر عهده مدیر ارشد سازمان است.

فرآیند:

برای تدوین طرح پیوستگی عملیات (مقابله با حوادث عمده رایانه ای) باید از منظری جامع و فرانگر به ماهیت سازمان، حوزه و نحوه ارائه خدمات آن و میزان وابستگی ذینفعان یا بهره برداران به خدمات ارائه شده، توجه نمود. هر چه سازمان بزرگتر و یا حوزه و تنوع ارائه خدمات آن گسترده تر باشد می توان انتظار داشت طرح از پیچیدگی بیشتری برخوردار باشد.

سازمان های کوچک نیز می توانند طرح های پیوستگی عملیات خود را داشته باشند. در این حالت تداوم ارائه خدمات به واحدهای داخلی مورد توجه قرار می گیرد و ممکن است طرح پیوستگی عملیات منحصر به دستورالعمل های مکتوب باشد بدون آنکه نیازی به تامین تجهیزات یا هماهنگی های برون سازمانی باشد.

طرح پیوستگی عملیات با این هدف تهیه می شود که در صورت بروز شرایط غیرعادی، سردرگمی در انجام وظایف ایجاد نشود و هر یک از افراد (دخیل در طرح) بدانند که باید چگونه عمل نمایند.

در شرایطی که افراد دخیل در طرح از بیش از یک سازمان مستقل انتخاب شده باشند هماهنگی عملیات اهمیت بسیار زیادی پیدا می کند. بهتر است در این شرایط از قرادادهای پشتیبانی متقابل استفاده شود. طی این گونه قرادادها طرفین تعهد می کنند که در صورت وقوع شرایط اضطراری، منابع انسانی یا توان پردازشی یا توان ارتباطی خود را در اختیار یکدیگر قرار دهند. کارآیی این نوع قراردادها بیشتر از امریه های دولتی است.

طرح های پیوستگی عملیات نباید در فضای تجریدی تدوین شوند و باید قابلیت اجرای آنها تضمین و تمرین شده باشد. به علاوه لازم است این طرح ها در امتداد و رابطه با فعالیت گروه های CERT باشند.

البته باید به تفاوت عملکرد طرح های CERT و پیوستگی عملیات توجه داشت.

طرح CERT برای مقابله با هر نوع رخداد تدوین می شود و افراد دخیل در آن عموماً کارشناسان رایانه ای درون سازمان هستند. این افراد وظیفه یاری رسانی روزمره به سایر افراد را (در صورت بروز وضعیت اضطراری) بر عهده دارند.

طرح پیوستگی عملیات برای مقابله با حوادث عمده ای تدوین می شود که ادامه ارائه خدمات را با مشکل مواجه نماید. در این حالت ممکن است عامل ایجاد مشکل چیزی فراتر از حوادث رایانه ای (مثلاً جنگ یا زلزله) باشد.

در سازمان هایی که وابستگی زیادی به ارائه خدمات رایانه ای دارند ممکن است نهاد مستقلی تاسیس شود و وظایف CERT و پیوستگی عملیات به آن سپرده شود. در این حالت فعالیت های مقابله با رخدادها تمرکز پیدا می کند. باید توجه داشت که این تمرکز نباید خود تبدیل به گلوگاهی امنیتی شود.

توضیحات

- فاجعه عبارت است از شرایطی که جان انسان ها یا موجودیت سازمان را تهدید نماید و یا احتمال صدمه شدید بدنی یا توقف ارائه قسمت قابل توجهی از خدمات سازمان را به دنبال داشته باشد. این شرایط ممکن است ناشی از عملکرد عوامل طبیعی یا غیرطبیعی باشد. ممکن است از واژه ترکیبی حوادث عمده نیز برای اشاره به این شرایط استفاده شود.

- طرح های مقابله با حوادث بزرگ تحت نام های مختلفی شناخته می شوند. طرح اضطراری، طرح مقابله با حوادث، طرح پیوستگی عملیات و طرح احیای سیستم یا سامانه از این جمله نام ها هستند. هرچند ممکن است بنا به تعریف، تفاوت های مفهومی برای نام های گفته شده لحاظ شود، اما در این توصیه نامه تمام عملیات ناظر بر مقابله با حوادث عمده رایانه ای، از مرحله کشف رخداد تا بازگشت به ظرفیت قبل از رخداد، مورد نظر است. بدیهی است با توجه به حوزه ارائه خدمات و اهمیت سازمان باید اثرات حوادث طبیعی بر ارائه خدمات نیز مورد توجه قرار گیرد.