ریاست جمهوری
مرکز فناوری اطلاعات، ارتباطات و امنیت

پیش نویس

خط مشی ایزوله سازی شبکه‌های اداری از شبکه‌های دیگر برای سازمان های متصل به شبکه دولت

نسخه ۱,۰

مرداد ماه ۱۳۹۷

فهرست مطالب

مقدمه

امنیتِ سایبریِ مناسب، جزء بنیادین رشد و موفقیت سازمان ها در عصر دیجیتال بوده و متقابلاً برای سازمان های دولتی، عدم احتراز آن مخاطرات امنیت ملی را در پی خواهد داشت. با توجه به رویکرد الکترونیکی شدن خدمات و تعاملات اداری و تجاری در همه ی سطوح و با هدف تحقق ایران الکترونیک، لازم است اسناد الکترونیکی دولت بر بسترهای نا امن مانند اینترنت ذخیره سازی و مبادله نشوند. همچنین با توجه به عدم اشراف کامل به لایه های سخت افزاری و نرم افزاری محصولات غیر بومی (که بعضا گریزی از کاربری آنها نداریم)، شبکه ی امن (با در نظر گرفتن نسبی بودن امنیت) به شبکه ای اطلاق می شود که دسترسی های آن، کنترل حداکثری را دارا بوده و امکان نفوذ به آن بسیار مشکل باشد، لذا این شبکه باید از شبکه های دیگر جداسازی شده باشد. و این، یکی از الزامات شبکه دولت است. بر اساس بخشنامه شماره ۱۷۳۹۸۳۶ مورخ ۱۳۹۶/۱۲/۱۵ سازمان اداری استخدامی کشور، مکاتبات بین سازمانی می باید بر بستر شبکه ی دولت (که ایزوله از اینترنت و شبکه های دیگر می باشد) صورت پذیرد. به منظور اجرایی شدن بخشنامه موصوف، سازمان های دولتی موظف به اتصال سامانه های اتوماسیون اداری خود به سامانه ی رصد (سامانه ی رهگیری و پیگیری مکاتبات در دستگاه مقصد) بر بستر شبکه دولت می باشند لذا سازمان های دولتی ضمن الزام به ایجاد شبکه اداری می باید وب سرویس اتصال به سامانه رصد را فعال نمایند.

هدف از تدوین این خط مشی

هدف از تدوین این خط مشی، وضع دستورالعملی جهت ایجاد شبکه ایزوله اداری از شبکه‌های دیگر اعم از اینترنتی برای سازمان های متصل به شبکه دولت به همراه الزامات و روش های مدیریت و صیانت از شبکه های ایجاد شده در سطح کلان می باشد.

دامنه کاربرد

این خط مشی برای کلیه سازمان هایی می باشد که به شبکه دولت متصل بوده و باید از این خط مشی مطلع و به آن عمل نمایند.

تبعات نقض خط مشی

نقض بندهای این خط مشی، توسط سامانه‌ها یا مسئولین امنیتی بصورت خودکار یا شهودی ثبت شده و ممکن است منجر به اخذ دسترسی از فرد و یا دستگاه متخلف و / یا برخورد بر اساس حساسیت تخلف گردد.

تعاریف

جداسازی فیزیکی : در این نوع جداسازی که شامل جداسازی در لایه های دسترسی، توزیع ، هسته شبکه و مرکز داده (اعم از سوئیچ ها، مسیر یاب ها، پلتفرم های مجازی سازی و موارد مشابه) می باشد تمامی تجهیزات اکتیو و پسیو مستقل از یکدیگر بوده و اصطلاحاً دوشبکه فاصله ی هوایی[1] دارند.

جداسازی منطقی: در این نوع جداسازی، شبکه ها در لایه های مختلف ارتباطی با توجه به قابلیت های فنی سخت افزارها، بطور مستقل از یکدیگر جدا سازی می شوند. عموما بستر فیزیکی کابلی یا نوری، پلتفرم ها و تجهیزات زیرساختی در شبکه های جداسازی شده یکسان می باشد.

شبکه اداری : به این شبکه، اینترانت امن سازمانی نیز اطلاق می شود، میزبان خدمات Back-Office سازمان (از جمله اتوماسیون اداری، ERP و موارد مشابه) می باشد که بدلیل حساسیت امنیتی اطلاعات مبادله شده در آنها، می باید از اینترنت و شبکه های دیگر جدا باشد. مکاتبات سازمانی صرفا بر بستر این شبکه انجام می گردد.

شبکه اینترنت : در این شبکه دسترسی به منابع اینترنتی فراهم شده وگردش فرایندهای مرتبط با امور اداری و سازمانی بر این بستر ممنوع می باشد.

مفروضات

- جداسازی شبکه ای به دو صورت جداسازی فیزیکی و منطقی در سطوح مختلف شبکه صورت می پذیرد.
- اتصالات شبکه های داخلی، سازمانی یا اداری الزاماً کابلی بوده هرگونه اتصالات بی سیم در لایه دسترسی ممنوع می باشد.
- کاربران در شبکه های اداری و یا اینترنتی می توانند از میزکارمجازی در جایگزینی از کاربری مستقیم رایانه های شخصی استفاده کنند، به این معنی که از طریق رایانه به میزکار مجازی در مرکز داده متصل شده، کی برد، موس، مانیتور، و غیره بر روی رایانه ی مجازی فعال می باشند.
- جداسازی توسط ایزولاتور (دیسک سخت و کارت شبکه جداگانه به ازاء هر شبکه) بدلیل محدودیت ها و مشکلات، قابل قبول نمی باشد.

انواع روش های جداسازی شبکه ای و ایجاد شبکه های اداری و اینترنتی

بر مبنای مفروضات و تعاریف فوق الذکر، انواع روش های جداسازی شبکه ای برای بهره برداری از خدمات شبکه های اداری و اینترنتی به شرح جدول ۱ می باشند :

جدول ۱ : انواع روش های جداسازی شبکه ای

ردیف	نوع جداسازی	توضیحات
۱	**فیزیکی**	در این ساختار، جداسازی فیزیکی زیرساخت شبکه و مرکز داده در تمامی لایه ها برای دسترسی جداگانه به منابع اینترنتی و اداری سازمان صورت می پذیرد.

[1] Air Gap

۲	**منطقی/ مجازی**	در این ساختار، جداسازی ارتباطات شبکه و مرکز داده در لایه های مختلف زیرساختی برای دسترسی جداگانه به منابع اینترنتی و اداری صورت می پذیرد.

تمهیدات لازم جهت صیانت از ایزوله‌سازی شبکه های اداری

با عنایت به طبقه بندی و محرمانگی اطلاعات و اسناد تولید شده در شبکه اداری سازمان ها، صیانت و حفاظت از این سرمایه ها در مقابل آسیب پذیری هایی که محرمانگی، تمامیت و دسترسی را تهدید می کنند امری حیاتی است و انتقال آنان به خارج از شبکه، باید تابع قواعد مشخصی باشد، لذا موارد زیر در همین خصوص ارائه می گردند.

- صدور بخشنامه ممنوعیت انجام امور اداری بر بستر اینترنت :

لازم است کاربران دستگاه های اجرایی نسبت به انجام امور محوله سازمانی که ارتباطی با اینترنت ندارند (شامل و نه محدود به: مکاتبات، گردش فرایندها، اتوماسیون اداری، تهیه صورتجلسات، گزارشات و غیره) در شبکه اداری سازمان اقدام نمایند. در صورتی که بر اساس شرح وظایف کاربر، سرویس اینترنت مبنای انجام وظیفه باشد تهیه محتواها و گزارشات تجمیع شده حاصل از جستجو در اینترنت یا جمع بندی گزارشات، در شبکه اینترنتی ممنوع بوده و برای اینکار می بایستی از شبکه اداری استفاده نمود (انتقال امن محتواهای جستجو شده یا گزارشات به شبکه اداری و انجام تحلیل و تهیه گزاشات تجمیعی).

- مسدودسازی رسانه های انتقال اطلاعات در شبکه اداری :

به منظور صیانت از امنیت اطلاعات تولید شده در شبکه اداری، لازم است رسانه های انتقال اطلاعات (مانند درگاه USB، CD/DVD Writer ، حافظه خوان و موارد مشابه) مسدود گردیده و از راهکار انتقال امن فایل و طی فرایندی مشخص برای انتقال اطلاعات به/ از شبکه اداری استفاده نمود.

- بررسی، ارتقاء و تست نفوذ دوره ای سرمایه های نرم/سخت افزاری شبکه :

به منظور اطمینان نسبی از امنیت شبکه اداری ایجاد شده لازم است بصورت دوره ای نسبت به تست نفوذ و بررسی و ارتقاء سامانه ها، تجهیزات ارتباطی- امنیتی، رایانه ها و میز کارهای مجازی، پیکره بندی ها و سایر موارد مرتبط اقدام نمود.

- بهره گیری از مکانیزم های مقاوم سازی و ایجاد امنیت و سلامت برای گره های شبکه :

با هدف کاهش و کنترل حملات ، اعمال و تحمیل سیاست های امنیتی مبتنی بر کاربران احراز هویت شده در شبکه، احراز هویت و تخصیص اجازه های دسترسی مشخص برای ارتباطات شبکه، رمزنگاری ارتباطات شبکه و غیره لازم است از مکانیزم های ایجاد امنیت و سلامت برای گره های شبکه استفاده نمود. این مکانیزم‌ها شامل تمامی دستورالعمل‌های ابلاغی

توسط مرکز مدیریت راهبردی افتا و بقیه نهادهای ذی‌ربط در این حوزه، جهت امن‌سازی سازمان‌ها می‌باشد. برخی از ارکان این مکانیزم ها عبارتند از:

- ایجاد شبکه های مجازی محلی[2] در شبکه اصلی به منظور جداسازی ترافیک های مختلف درون یک شبکه
- ایجاد شبکه ای از رایانه ها مبتنی بر مدیریت متمرکز به منظور مدیریت بهینه منابع شبکه و اتصال تمامی رایانه ها به دامین دستگاه و ارائه نام کاربری محدود به کاربران
- نصب آنتی ویروس دارای مجوز و فعال سازی دیواره آتش و مورد تایید مراجع امنیتی روی رایانه های شبکه اداری و بروز رسانی مداوم آنها
- تعریف لیست مجاز برنامه ها به منظور جلوگیری از نصب و اجرای برنامه های ناخواسته
- استفاده از سیستم های عامل دارای پشتیبانی امنیتی (وصله های امنیتی) از طرف شرکت تولید کننده و ارائه راهکارهای بروز رسانی مستمر آنها
- پیاده سازی پروتکل های امنیت پورت[3] به منظور جلوگیری از اتصال گره های نا امن به شبکه و یا جابجایی گره های در شبکه
- بهره گیری از مکانیزم های آزمایش سلامت[4] و غیر فعال سازی امکانات، سرویس ها و برنامه های غیر ضروری در سیستم های عامل و تجهیزات شبکه
- بهره گیری از مکانیزم های جلوگیری از نشت و فقدان داده ها[5] در شبکه
- اعمال سیاست های امنیتی مربوط به نام کاربری و کلمه عبور و استفاده از عامل دوم برای احراز هویت

- بکارگیری چرخه امنیتی انتشار سامانه های نرم افزاری در شبکه اداری سازمان :

به منظور ارزیابی معماری امنیتی ، بررسی سابقه آسیب پذیری های پیشین و اجزاء تشکیل دهنده، کشف آسیب پذیری های جدید و رفع آن در سامانه های شبکه اداری سازمان ها، وجود چرخه امنیتی (ارزیابی مداوم) تولید و انتشار سامانه ، امری ضروری می باشد.

- استفاده از نرم افزار های دارای گواهینامه امنیتی:

نظر به اهمیت سامانه های مورد استفاده در شبکه های حیاتی، بررسی آنان توسط مراجع ذیصلاح امنیتی الزامی بوده و تنها نرم افزار هایی مجاز به استفاده در اینگونه شبکه ها هستند که موفق به کسب گواهینامه امنیتی شده اند.

---

[2] VLAN

[3] مانند 802.1X

[4] Health Check

[5] Data Leakage Prevention

- بهره گیری از مرکز عملیات امنیت :

پیاده سازی مرکز عملیات امنیت جهت مواجهه مناسب و موثر با رویدادهای امنیتی در مقابل تهدیدهای احتمالی، ارتقاء امنیت و پایداری داده ها و خدمات از طریق حفاظت از زیرساخت های اطلاعاتی، کاهش زمان اختلال در ارایه خدمات، بهبود و تسریع در پاسخ ها و واکنش های امنیتی و کاهش هزینه های ناشی از حملات سایبری امری حیاتی می باشد. ارکان اصلی مرکز عملیات امنیت عبارتند از :

- سامانه مدیریت یکپارچه رخدادها[6]
- سامانه های تشخیص و جلوگیری از نفوذ[7]
- سامانه های رهگیری جرم[8]
- سامانه مدیریت آسیب پذیری[9]
- سامانه مدیریت حوادث (پاسخگویی به حوادث)[10]
- سامانه پایش ارتباطات[11]

بکارگیری مکانیزم های جلوگیری از نقض سیاست های اعمال شده

با توجه به اینکه نقض و تخطی از سیاست های اعلامی و اعمال شده چه بصورت سهوی و چه عمدی، می تواند خسارات غیر قابل جبرانی را برای سازمان به همراه داشته باشد لذا لازم است تمهیداتی مشخص در پایش اجرای سیاست های اعلامی و اعمال شده مد نظر قرار گیرد. به عنوان نمونه، غیر فعال کردن امکان راه اندازی[12] رایانه های شبکه با استفاده از لوح فشرده یا USB ویندوز در سامانه ورودی/خروجی پایه[13] رایانه (به منظور جلوگیری از نقض سیاست های اعمال شده در خصوص رسانه های انتقال اطلاعات) امری اجتناب ناپذیر می باشد. سازمان ها می بایستی لیستی از اقدامات لازم به منظور جلوگیری از نقض سیاست های اعمال شده تهیه، مصوب و اعمال نمایند.

سیاست های انتقال اطلاعات بین شبکه اداری و اینترنتی و درون شبکه ای

با توجه به اینکه جداسازی شبکه ای و تمهیدات مکمل باعث بروز محدودیت در انتقال اطلاعات بین شبکه ها و درون شبکه می گردد لذا سیاست های انتقال اطلاعات به شرح زیر می باشد :

- انتقال اطلاعات به شبکه اداری سازمان : این کار صرفا از طریق راهکار انتقال امن فایل بصورت یک طرفه و از طریق رایانه اینترنتی سازمان امکانپذیر می باشد.

---

[6] Security Information and Event Management
[7] IDS/IPS
[8] Forensics
[9] Vulnerability Assessment
[10] Incident Response Management System
[11] Flow Monitoring System
[12] Boot
[13] Basic Input / Output System (BIOS)

- *انتقال اطلاعات در داخل شبکه اداری* : این کار با استفاده از حافظه اختصاصی سازمانی برای هر کاربر در داخل شبکه اداری امکان پذیر می باشد. با استفاده از این راهکار، اطلاعات کاربر در هر نقطه از شبکه اداری سازمان با رعایت موارد امنیتی در دسترس می باشد.

- *انتقال اطلاعات از شبکه اداری به بیرون* : این کار از طریق جریان کاری[۱۴] زیر و از داخل سامانه تعبیه شده صورت می پذیرد :

گام اول : آپلود فایل در سامانه توسط شخص متقاضی

گام دوم : تایید مدیر شخص متقاضی در سامانه

گام سوم : بررسی موضوع توسط حراست سازمان در سامانه

گام چهارم : تحویل اطلاعات از طریق رایانه حراست، مستقر در نقاط مورد تایید به شخص متقاضی به نحو مقتضی مورد تایید حراست

---

[1] Workflow [4]