



تاریخ: ۹۰/۷/۴  
شماره: ۷۹/۲۳۶-۸۷  
پست:  
بسم الله الرحمن الرحيم  
سازمان سما

بخشنامه به کلیه واحدهای دانشگاهی و آموزشدهنده های فنی حرفه ای سما

با عنایت به به لزوم تامین امنیت اطلاعات در ساختار شبکه واحدها و مراکز آموزشی دانشگاه، محیطهای کاری رایانه ای، پایگاههای اینترنتی، سامانههای خدماتی همچون آموزش و شهریه و رعایت موارد ذیل میبایست در نظر گرفته شود:

الف) مسایل مهم امنیتی مرتبط با شبکه و امنیت فناوری اطلاعات، در سه سطح فیزیکی (Physical)، عملیاتی (Operational) و مدیریتی (Management) (۱) حوزه فیزیکی (Physical)

هدف از امنیت اطلاعات در سطح فیزیکی، حفاظت اطلاعات در مقابل دسترسی افراد غیر مجاز به تجهیزات فیزیکی (تجهیزات مدیریتی اطلاعات و جلوگیری از سرقت و دستبرد ویا تخریب آن است. که شامل امنیت رایانهها، تجهیزات فعال و غیرفعال شبکه، اتاق سرور و نیز به کارگیری تجهیزات امنیتی مانند سنسورهای هشدار دهنده، سیستمهای برودتی، اطفای حریق و... می باشد. (۲) حوزه عملیاتی (Operational)

این حوزه شامل اقداماتی از قبیل نصب نرم افزارهای مورد نیاز و رعایت تنظیمات خاص، تعیین سطوح دسترسی، تأیید هویت جهت ورود به شبکه، تعیین نحوه دسترسی به چه منابعی و تا چه حد، برنامههای پشتیبان گیری و بازیابی و امنیت توبولوژی مانند ساخت DMZ و... می باشد. از جمله اقدامات لازم برای تامین امنیت شبکه در حوزه عملیاتی (Operational) عبارتند از:

- ۱-۲) نصب و پیکر بندی کامل نرم افزارهای مورد نیاز.
- ۲-۲) نصب و پیکر بندی نرم افزارهای توزیع کننده امکانات و تعیین کننده سطوح دسترسی.
- ۳-۲) نصب و پیکر بندی نرم افزارهای مانیتورینگ و ثبت کننده دقیق رویدادها.
- ۴-۲) نصب و پیکر بندی نرم افزارهای پروکسی، فایروال، فیلترینگ، آنتی ویروس ها و بروزرسانی مرتب آنها و دیگر برنامههای کنترل نظارت و پیشگیری.
- ۵-۲) استفاده از ماژولهای امنیتی خاص سخت افزاری.
- ۶-۲) توزیع متناسب خدمات بر اساس کلاس بندی و اعتباردهیهای متفاوت بر اساس سطح بندی کاربران.
- ۷-۲) استفاده از Directory Service و به حداقل رساندن دسترسی کاربران به منابع.
- ۹-۲) نظارت مستمر، بازیابی و بررسی رویدادها و نظارت و توجه خاص نسبت به افراد مشکل آفرین. و اعمال کنترل و هشدارهای لازم در موارد مقتضی. و در صورت لزوم معرفی به مسؤلان مربوطه.
- ۱۰-۲) نصب و پیکر بندی نرم افزارهای پشتیبان گیر و بازیابی اطلاعات و تهیه نسخه های پشتیبان منظم و نگهداری آن در جایی غیر از سرور مربوطه.
- ۱۱-۲) تهیه گزارش ها، مقایسه و تطبیق وقایع و گزارش ها.
- ۱۲-۲) تهیه نقشه جامع شبکه و تهیه فهرست کامل از سیستم های عامل و نرم افزارهای نصب شده با ذکر مشخصات آن ها.
- ۱۳-۲) الزام استفاده همگانی از دامین و محدود کردن کاربران شبکه در حد دامین.
- ۱۴-۲) ممنوعیت نصب و اجرای فیلتر شکن و استفاده از VPN ها در محیط کاری شبکه.

حوزه مدیریتی (Management)

این حوزه شامل اقداماتی از قبیل مدیریت و سیاست گذاری شبکه، تدوین و آماده سازی ضوابط، شیوه نامه ها و هدایت امور به منظور آماده سازی محیطی امن برای شبکه می باشد. از جمله محورهای مهمی که میبایست در سیاست های شبکه مد نظر قرار گیرد عبارتند از:

نشانی: تهران - پاسداران نیسان نم - تلفن: ۷۲-۲۵۸۸۱۶۷ و ۲۲۵۸۲۷۸۰؛ فاکس: ۲۲۵۴۹۶۰۶ منطقه پستی ۱۹ - صندوق پستی ۴۶۶/۱۹۵۸۵



پایگاه

تاریخ:  
شماره:  
پوست:

- ۱-۳ سیاست توزیع متناسب خدمات بر اساس کلاس بندی و اعتباردهی های متفاوت.
- ۲-۳ سیاست مشخص جهت پشتیبان گیری منظم و نگهداری و استفاده از آن.
- ۳-۳ سیاست مشخص جهت تهیه گزارش ها، مقایسه و تطبیق وقایع و گزارش ها.
- ۴-۳ سیاست و طرح مشخص جهت توسعه های کمی و کیفی مورد نیاز و فزاینده مطابق با تحولات آینده و انعطاف پذیری در برابر تهدیدات و تحولات.
- ۵-۳ سیاست مشخص جهت نظارت مستمر، بازبینی و بررسی رویدادها.
- ۶-۳ نظارت و مانیتورینگ و بازرسی لاگها.

ب) ملاحظات امنیتی در شبکه های بی سیم:

در خصوص شبکه های بی سیم نیز می بایست به مسایل و موضوعات دیگری خاص آن حوزه توجه داشت. اصول امنیتی شبکه های مبتنی بر بی سیم را می توان به شرح زیر تبیین کرد:

- ۱) Hide SSID Broadcast
- ۲) Use Encryption Protocol و استفاده از بالاترین سطح رمزنگاری در شبکه.
- ۳) MAC Address Filtering
- ۴) Site-Survey و استفاده از AP های با آنتن و شعاع ارسال سیگنال متناسب با نیاز و اجتناب از افزایش بی جهت قدرت ارسال سیگنال

ج) مسایل مهم امنیتی مرتبط با پایگاه اینترنتی:

- ۱) دانستن طرح و برنامه منحصر امنیتی جهت فعالیت موثر و هدف مند اطلاع رسانی در فضای سایبر.
- ۲) ثبت مستقیم دامین توسط دانشگاه و عدم واگذاری ثبت دامین به افراد و شرکت هایی خارج از سازمان. (در صورت مالکیت دامین ها توسط شرکت های خصوصی مراتب در اسرع وقت به واحد دانشگاهی مربوطه انتقال یابد).
- ۳) تأمین فضای مورد نیاز سایت های اطلاع رسانی از داخل کشور و انتخاب میزبان مناسب برای سایت. (در صورت وجود هاست خارجی موضوع انتقال آن به داخل کشور در اسرع وقت در دستور کار قرار گیرد).
- ۴) انتخاب میزبان مناسب جهت تهیه فضای سایت و تضمین های کافی جهت پشتیبانی های لازم.
- ۵) استفاده از نرم افزارهای ایمن.
- ۶) دقت لازم در انتخاب نوع CMS از نظر متن بار یا متن بسته و نیز امکان پشتیبانی و توسعه نرم افزار و هم خوانی آن با زیرساخت های موجود.
- ۷) دقت در رعایت قوانین و موازین نظام مقدس اسلامی در طراحی و محتوای پایگاه اینترنتی.
- ۸) توجه به جهت امنیتی در استفاده از امکانات نرم افزارها به ویژه دقت و احتیاط در استفاده از امکانات تعاملی و ارتباطی با کاربر در نرم افزارهای مدیریت محتوا و درگاهها.
- ۹) رعایت نکات امنیتی در استفاده از نامهای کاربری و گذرواژه های مربوط به کنترل پنل، انتقال فایل و ایمیل ها، و احتیاط در تنظیم گزینه های کنترل پنل.
- ۱۰) استفاده از آخرین به روز رسانی ها، وصله های امنیتی و سرویس یک ها.
- ۱۱) استفاده از نرم افزارهای امنیتی و ضد ویروس.
- ۱۲) پشتیبان گیری سایت و نگهداری نسخه های آن در مکان هایی دیگر اضافه بر مکان جاری سایت.
- ۱۳) سرکشی مداوم به سایت، بازبینی و بررسی رویدادها و دسته بندی آن ها برای ملاحظات بعدی.
- ۱۴) امکان استفاده از رمزنگاری در موارد خاص به عنوان مهمترین ابزار برقراری امنیت در فضای تبادل داده.

دکتر فریدون رهنمای رودپشتی

معاون پژوهشی دانشکده آزاد اسلامی