دانشگاه آزاد اسلامی
سازمان مرکزی

تاریخ: ۹۰/۷/۴
شماره: ۷۹/۲۳۶۰۸۷
پیوست:

باسمه‌تعالی

**بخشنامه به کلیه واحدهای دانشگاهی و آموزشکده های فنی حرفه ای سما**

با عنایت به به لزوم تامین امنیت اطلاعات در ساختار شبکه واحدها و مراکز آموزشی دانشگاه، محیط‌های کاری رایانه‌ای، 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 ثبت و مدیریت اطلاعات و جلوگیری از سرقت و دستبرد ویا تخریب آن است. که شامل امنیت رایانه‌ها، تجهیزات فعال و غیرفعال شبکه، اتاق سرور و نیز به‌کارگیری تجهیزات امنیتی مانند سنسورهای هشدار دهنده، سیستم‌های برودتی، اطفای حریق و.. می‌باشد.

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 توپولوژی مانند ساخت DMZو... می‌باشد، از جمله اقدامات لازم برای تأمین امنیت شبکه در حوزه عملیاتی (Operational) عبارتند از؛

۲-۱) 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.

۲-۳) نصب و پیکر بندی نرم افزارهای مانیتورینگ و ثبت کننده دقیق رویدادها.

۲-۴) نصب و پیکر بندی نرم افزارهای پروکسی، فایروال، فیلترینگ، آنتی ویروس ها و بروزرسانی مرتب آنها و دیگر برنامه‌های کنترل ونظارت وپیشگیری.

۲-۵) استفاده از ماژول‌های امنیتی خاص سخت‌افزاری.

۲-۶) توزیع متناسب خدمات بر اساس کلاس‌بندی و اعتباردهی‌های متفاوت بر اساس سطح بندی کاربران.

۲-۷) استفاده از Directory Service و به حداقل رساندن دسترسی کاربران به منابع.

۲-۹) نظارت مستمر، بازبینی و بررسی رویدادها و نظارت و توجه خاص نسبت به افراد مشکل آفرین. و اعمال کنترل و هشدارهای لازم در موارد مقتضی، ودر صورت لزوم معرفی به مسؤلان مربوطه.

۲-۱۰) نصب و پیکربندی نرم افزارهای پشتیبان گیر و بازیابی اطلاعات و تهیه نسخه‌های پشتیبان منظم و نگهداری آن در جایی غیر از سرور مربوطه.

۲-۱۱) تهیه گزارش ها، مقایسه و تطبیق وقایع و گزارش ها.

۲-۱۲) تهیه نقشه جامع شبکه و تهیه فهرست کامل از سیستم های عامل و نرم افزارهای نصب شده با ذکر مشخصات آن ها.

۲-۱۳) الزام استفاده همگانی از دامین و محدود کردن کاربران شبکه در حد دامین.

۳-۱۴) ممنوعیت نصب و اجرای فیلتر شکن و استفاده از VPN ها در محیط کاری شبکه.

۳) حوزه مدیریتی (Management)

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

نشانی: تهران - پاسداران نیستان نهم - تلفن: ۷۲-۲۲۵۸۸۱۶۷ و ۲۲۵۸۲۷۸۰ نمابر: ۲۲۵۴۹۶۰۶ منطقه پستی ۱۹ - صندوق پستی ۱۹۵۸۵/۴۶۶

۳-۱) سیاست توزیع متناسب خدمات بر اساس کلاس بندی و اعتباردهی های متفاوت.

۳-۲) 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.

۳-۴) 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.

۳-۵) سیاست مشخص جهت نظارت مستمر، بازبینی و بررسی رویدادها.

۳-۶) نظارت و مانیتورینگ و بازرسی لاگ‌ها.

**ب) ملاحضات امنیتی در شبکه‌های بی‌سیم:**

در خصوص شبکه های بی سیم نیز می‌بایست به مسایل و موضوعات دیگری خاص آن حوزه توجه داشت. اصول امنیتی شبکه‌های مبتنی بر بی سیم را می‌توان 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 هایی با آنتن و شعاع ارسال سیگنال متناسب با نیاز و اجتناب از افزایش بی‌جهت قدرت ارسال سیگنال.

**ج) مسایل مهم امنیتی مرتبط با پایگاه اینترنتی:**

۱) داشتن طرح وبرنامه مشخص امنیتی جهت فعالیت مؤثر 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 دامین‌ها توسط شرکت‌های 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 باز 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 جهات 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 ودرگاه‌ها.

۹) رعایت نکات ایمنی در استفاده از نام‌های کاربری و گذرواژهای مربوط به کنترل پنل، انتقال فایل و ای‌میل‌ها، و احتیاط در تنظیم گزینه‌های کنترل پنل.

۱۰) استفاده از آخرین به روز رسانی‌ها، وصله های امنیتی و سرویس پک‌ها.

۱۱) استفاده از نرم افزارهای امنیتی و ضد ویروس.

۱۲) پشتیبان گیری سایت و نگه‌داری نسخه‌های آن درمکان‌هایی دیگر اضافه بر مکان جاری سایت.

۱۳) سرکشی مداوم به سایت، بازبینی و بررسی رویدادها و دسته بندی آن‌ها 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 دانشگاه آزاد اسلامی**