بنام خدا

چک لیست امنیت شبکه

و

دستور العمل های امنیتی شبکه

ویژه دانشجویان و مسئولین سایت ها و شبکه

تدوین : علی ثاقب موفق

چک لیست امنیتی شبکه و سایت

نام و نام خانوادگی ناظر شبکه :

ردیف	موارد حفاظتی	
۱	سیستم دیواره آتش Fire Wall	
	۱-۱	سخت افزاری بودن فایروال
	۱-۲	فعال بودن ماجول های آن (IDS,VPN ، تشخیص هویت ترافیک ، مدیریت پهنای باند، تصویه محتوی وب و .....)
	۱-۳	نوع فایر وال (Packet filtering / circuit relay/ application level Gate way)
	۱-٤	مدل ایرانی یا خارجی (به لحاظ امنیت OS)
	۱-۵	مکانیزم failover و قابلیت اطمینان بالا در صورت قطع برق و خرابی سخت افزار
	۱-۶	تعداد و نوع واسطهای بکاررفته و توان پردازشی
	۱-۷	بکارگیری سیستم تبدیل آدرس NAT
	۱-۸	محل استقرار (نقطه ورودی شبکه و آخرین فرایند برای کنترل ترافیک خروجی)
۲	آنتی ویروس	
	۲-۱	نوع ضد ویروس
	۲-۲	Update شدن مستمر آن
	۲-۳	هوشمند و huristic بودن آن
	۲-٤	License دار بودن
۳	سیستم تشخیص و پیشگیری تهاجم یا IPS , IDS	
	۳-۱	مدیریت log ها و نرم افزار log analyzer
	۳-۲	میزان کاربرد گزارشات Log
	۳-۳	سخت افزاری یا نرم افزاری بودن
	۳-۳	UpDate بودن آن
٤	مدیریت نرم افزارهای سیستمی موجود سایت (Updating&Security Patch)	
۵	بکارگیری مناسب ادوات شبکه امن و خصوصی مجازی PTMP,VLan , VPN و . . .	
	۵-۱	فعال بودن درصورت نیاز
	۵-۲	اثربخشی
۶	عدم دسترسی کاربران عادی به تجهیزات active & passive شبکه	
	۶-۱	محل فیزیکی و استقرار سوئیچ و روترها ، hub ، مودم و سخت افزارهای ارتباطی و امنیت آن
	۶-۲	محل عبوری کابل ها از رک ، سقف و کف کاذب و امنیت آن
	۶-۳	امنیت تجهیزات passive (جنس ، استحکام و محل نصب)
۷	سیستم گذرگاه امنیتی Security Gateway (ISA)	
	7-۱	تنظیمات امن پارامترهای آن
	7-۲	استفاده از گزارشات مدیریتی و کنترلی

	۳-7	بروز بودن
۸	سیستم Air conditioning سایت (کنترل دما، رطوبت، گرد و غبار و .....)	
۹	سیستم ثبت و مدیریت وقایع (logs& Event & traffic control) سایت	
	۱-۹	تهیه گزارشات دوره ای
	۲-۹	تحلیل log های سرورها و ارائه به مسئولین مربوطه
۱۰	سیستم مدیریت backup اطلاعات سروری(San – Das - Nas) در محل امن	
	۱-۱۰	امنیت محل نگهداری back up و انجام مرتب آن
	۲-۱۰	تست recovery و restore و پشتیبانی اطلاعات
۱۱	امنیت الکتریکی سایت (Earth – ups- power panel - cabling)	
	۱-۱۱	Ups و بکارگیری مؤثر و کیفیت آن
	۲-۱۱	چاه ارت
	۳-۱۱	کابل کشی و پانل برق و مسیر کابل ها
۱۲	رمز کننده های اطلاعات با درجه بندی محرمانه به بالا (Encryption)	
۱۳	آنتی اسپم و هرزنامه های مختلف (Anti spam)	
۱٤	سیستم پالایش اطلاعات تحویل به کاربر (content & image & text filtering)	
۱۵	کنترل تردد سایت	
	۱-۱۵	دوربین مداربسته
	۲-۱۵	کارت هوشمند
	۳-۱۵	پسورد ، کلید و قفل
۱۶	پویشگر آسیب پذیری شبکه وسیستم ها (vuLnerability Scanning)	
۱۷	مدیریت سخت افزارهای موجود(پردازشی و ارتباطی)	
	۱-۱۷	Upgrade مستمر
	۲-۱۷	عدم استفاده از سخت افزارهای ممنوعه و ارتباط راه دور (Remote)
۱۸	اطلاع رسانی مؤثر در سایت شبکه (نحوه حضور پرسنل)	
۱۹	بکارگیری Honypot	
	۱-۱۹	مدل و نسخه
	۲-۱۹	گزارشات مستمر و بکارگیری مؤثر آن
۲۰	مدیریت کلمات عبور و پسوردها (Athentication & Authorization)	
	۱-۲۰	تغییرات دوره ای پسورد
	۲-۲۰	رعایت مسائل پسورد دهی (ترکیب و حروف، اعداد و علائم خاص)
	۳-۲۰	استفاده از OTP برای شرکت های خصوصی

چک لیست امنیتی سرورها (Servers)

نام و نام خانوادگی کاربر/ کاربران(Admin):

ردیف	موارد حفاظتی	
۱	قرارگیری در منطقه امن شبکه	
	۱-۱	بعد از firewall
	۱-۲	دارا بودن Server room , Server farm و استقرار سرور در آن
	۱-۳	امنیت الکتریکی آن (برق – ارت)
	۱-٤	میزان تردد به محل سرور
	۱-۵	امنیت فضا، طبقه و اتاق
۲	ضد ویروس یا آنتی ویروس License دار مناسب سرور	
	۲-۱	نوع و مدل آنتی ویروس
	۲-۲	Update دوره ای مستمر
	۲-۳	پشتیبانی و نگهداری مؤثر
۳	سیستم ثبت و مدیریت وقایع سرور (event viewer & Log Analyzer)	
	۳-۱	تحلیل Log ها و گزارشات دسترسی های غیرمجاز
	۳-۲	مسئول مربوطه و گروه تحلیل Log
٤	بروز رسانی مؤثر نرم افزارهای سیستمی	
	٤-۱	استفاده از Security Patchs
	٤-۲	درایورها
	٤-۳	ارتقاء سیستم عامل و امنیت
۵	بروز رسانی مؤثر نرم افزارهای کاربردی	
۶	بروز رسانی سخت افزاری سرور	
	۶-۱	ارتقاء CPU و هماهنگی آن و سرعت مطلوب
	۶-۲	ارتقاء RAM
	۶-۳	ارتقاء hard و متناسب با نیاز
۷	مدیریت کلمه عبور و پسورد سرور	
	۷-۱	تغییر دوره ای
	۷-۲	پسورد مناسب
	۷-۳	پسورد OTP برای مراجعین بخش خصوصی
۸	سیستم مدیریت backup اطلاعات سروری	
	۸-۱	نوع back up
	۸-۲	محل back up
	۸-۳	تست Recovery
	۸-٤	مسئول مربوطه
۹	امنیت فیزیکی و الکتریکی سرور	

	۹-۱	استفاده از UPS
	۹-۲	استفاده از ارت
	۹-۳	محل استقرار rack mount و امنیت فیزیکی
۱۰	عدم فعالسازی نرم افزارهایSharing , RAS (بجز در مواقع نصب و پشتیبانی سیستم)	
	۱۰-۱	عدم وجود نرم افزار peer to peer
	۱۰-۲	عدم وجود نرم افزارهای Sharing
	۱۰-۳	عدم امکان ارتباط telnet , ftp و Ras , ...
۱۱	کنترل دسترسی حافظه های قابل حمل (portable)	
	۱۱-۱	کنترل دسترسی CD & DVD
	۱۱-۲	کنترل دسترسی USB
	۱۱-۳	کنترل دسترسی Floppy ها
	۱۱-٤	کنترل دسترسی hard
	۱۱-۵	کنترل سخت افزاری یا نرم افزاری حافظه های جانبی متفرقه ثابت و متصل
۱۲	مدیریت و کنترل دسترسی کاربران	
	۱۲-۱	کنترل سطوح دسترسی و مجوزهای دسترسی کاربران و گروه های کاری
	۱۲-۲	کنترل دسترسی فیزیکی و سخت افزاری
	۱۲-۳	فرهنگ سازی و آموزش مباحث امنیتی
۱۳	سیستم عامل سرور (NOS)	
	۱۲-۱	License دار بودن سیستم عامل سروری
	۱۲-۲	وجود آخرین نسخه (Version) سیستم عامل و Patch های امنیتی آن
	۱۲-۳	تنظیمات امن سروری

چک لیست امنیتی رایانه

نام و نام خانوادگی کاربر(User):

ردیف	موارد حفاظتی	
۱	سیستم دیوار ه آتش	
	۱-۱	فعال بودن (on)
	۱-۲	آگاهی کاربر از firewall
۲	ضد ویروس یا آنتی ویروس	
	۲-۱	License دار بودن
	۲-۲	نوع و نسخه آن
	۲-۳	بروزرسانی مستمر از سرور و یا سایت مربوطه
	۲-٤	پشتیبانی ونگهداری
۳	نرم افزارهای Sharing	
	۳-۱	عدم وجود برنامه های Share و Peer To Peer
	۳-۲	عدم وجود برنامه های IM ,Chat
	۳-۳	عدم امکان رویت فولدرها و درایوهای کاربر
	۳-٤	عدم Share منابع و تجهیزات جانبی رایانه
٤	نرم افزارهای Game	
	٤-۱	عدم وجود بازیهای ویندوزی یا مطمئن
	٤-۲	عدم وجود بازیهای متفرقه ناامن
۵	سیستم backup اطلاعات	
	۵-۱	نوع backup و پشتیبان گیری از اطلاعات مهم رایانه
	۵-۲	محل نگهداری پشتیبان و امنیت آن
	۵-۳	تست recovery
۶	ایمنی الکتریکی	
	۶-۱	ارت
	۶-۲	استفاده از اسپلایزر و محافظ برق
	۶-۳	UPS
۷	شناسه و رمز مناسب برای Bios سیستم و application ها	
	۷-۱	پسورد مناسب
	۷-۲	تغییر دوره ای پسورد
۸	سخت افزار غیر ضروری منصوبه بر سیستم	
	۸-۱	عدم استفاده از مودم
	۸-۲	سخت افزارهای غیرضرور (میکروفن – بلندگو – دوربین و. . .)
۹	دارای امکان Join To Domain	
۱۰	عدم وجود نرم افزارهای غیر ضرور، غیر تخصصی و نامتناسب با شغل	

چک لیست امنیتی نیروی انسانی

نام و نام خانوادگی کاربر(User):

ردیف	موارد حفاظتی	
۱	میزان آگاهی کاربران از مسائل امنیتی شبکه و رایانه	
	۱-۱	درجه اهمیت موضوع برای کاربر
	۱-۲	میزان اعمال آن در کار
	۱-۳	میزان آشنایی با مسائل امنیتی در مواقع کار با اینترنت
	۱-٤	آشنایی با استفاده امن از رسانه های دیجیتالی
۲	استفاده از نشریه، مقالات و سایت امنیت شبکه و حفاظت IT شرکت زیرساخت	
	۲-۱	استفاده از نشریه زیرساخت و مقالات امنیت شبکه ای
	۲-۲	استفاده از سایر نشریات امنیت شبکه ای و سایت های اینترنتی
۳	انتقال دانش فنی تجهیزات و سیستمهای امنیتی خریداری شده به پرسنل مربوطه	
	۳-۱	مطالعه user manual مربوط به سخت افزارهای موجود و امنیت آن
	۳-۲	شرکت در دوره آموزشی مربوطه
	۳-۳	دعوت از شرکت مربوطه جهت آموزش فنی و تخصصی
	۳-٤	آموزش کاربری
	۳-۵	عدم وابستگی به شرکت طرف قرارداد
	۳-۶	انتقال دانش فنی تجهیزات خریداری شده
٤	آموزش دوره های مقدماتی و پیشرفته امنیت و حفاظت شبکه در سطح کاربران و مدیران شبکه	
	٤-۱	تعداد سمینارها، کنفرانس ها و مجمع های امنیت شبکه
	٤-۲	تعداد دوره های گذرانده شده امنیت شبکه
۵	تعریف سطوح دسترسی کاربران به اطلاعات و نرم افزارهای مربوطه	
	۵-۱	تعریف کاربران متنوع به لحاظ تخصص، کارشناسی – قراردادی – رسمی و . . .
	۵-۲	اعمال مجوزها و سطوح دسترسی کاربران و گروه های کاری
۶	رعایت و بکارگیری دستورالعمل های حفاظت IT در کار	

چک لیست امنیتی تجهیزات ارتباطی شبکه

نام و نام خانوادگی کاربر:

ردیف	موارد حفاظتی	
۱	پیکربندی و تنظیمات امن	
۲	بروزرسانی IOS	
۳	مدیریت پسورد	
	۱-۳	پسورد مناسب با ترکیب رقم، حرف و علامت
	۲-۳	تغییر دوره ای پسورد
	۳-۳	استفاده از پسورد OTP در صورت لزوم
٤	پشتیبان گیری وbackup از config	
	۱-٤	نوع back up
	۲-٤	محل نگهداری back up
	۳-٤	تست Recovery
۵		
	۱-۵	امین واعتبار و اطمینان
	۲-۵	دانش فنی
	۳-۵	دانش امنیتی شبکه و تجهیزات ارتباطی
۶	محل استقرار سخت افزار ارتباطی	
	۱-۶	امنیت فیزیکی و الکتریکی
	۲-۶	امنیت جایگاه و ارتباطات و اتصالات آن

چک لیست امنیتی پروژه ها و برنامه های نرم افزاری

نام و نام خانوادگی مجری و مسئول:

ردیف	موارد حفاظتی	
۱	امنیت بانکهای اطلاعاتی	
	۱-۱	نوع بانک اطلاعاتی مورد استفاده و متدولوژی طراحی(به لحاظ امنیت آن)
	۱-۲	نحوه ذخیره سازی اطلاعات (encrypt / plain text) و تصاویر
	۱-۳	بروزرسانی مؤثر (update) و Config امن آن هنگام نصب
	۱-٤	مجوزها و سطوح دسترسی کاربران
۲	امنیت برنامه نرم افزاری	
	۲-۱	امنیت زبان برنامه نویسی (Programming Language)
	۲-۲	امکان دسترسی به source برنامه و مستندات
	۲-۳	امکان کار با قسمت های مختلف برنامه متناسب با مجوزهای دسترسی
	۲-٤	امکانات تغییر رمز و Authentication مؤثر کاربر و پشتیبانی امضای دیجیتالی
	۲-۵	امکانات پشتیبان Restore , Back up اطلاعات و import& exoprt
	۲-۶	پا برجایی و stability برنامه و پیام های خطای متنوع و متناسب با خطا(Error handling)
	۲-۷	عدم امکان دسترسی به اطلاعات برنامه به غیر از نرم افزار مربوطه
۳	نیروی انسانی مربوطه پشتیبان	
	۳-۱	آگاهی به مسائل امنیت نرم افزار ها
	۳-۲	اعتماد و اطمینان و امین بودن
	۳-۳	دانش فنی تخصصی تیم پشتیبان

چک لیست امنیتی فایروال (Firewall)

نام و نام خانوادگی مسئول :

ردیف	موارد حفاظتی	
۱	ویژگیها و قابلیتهای سیستم دیواره آتش Fire Wall	
	۱-۱	محل استقرار امن (نقطه ورودی شبکه و آخرین فرایند برای کنترل ترافیک خروجی)
	۱-۲	بروز بودن قوانین، policy ها و Rule ها
	۱-۳	فعال بودن ماجول ها (IDS,VPN ، IDP ، تشخیص هویت ترافیک ، مدیریت پهنای باند، تصویه محتوی وب و .....)
	۱-۴	نوع فایر وال (Packet filtering / circuit relay/ application level Gate way) (برخی فایروالها به عنوان Deep Inspection شناخته میشوند که کلیه مشخصات را دارا هستند)
	۱-۵	مدل فایروال و ایرانی یا خارجی بودن آن به لحاظ امنیت OS – در شرایط فنی یکسان، ایرانی (شرکتهای ایرانی محصولات UTM را ارائه میدهند که به لحاظ امنیتی خوب است)
	۱-۶	مکانیزم failover و قابلیت اطمینان بالا در صورت قطع برق و خرابی سخت افزار
	۱-۷	بکارگیری سیستم تبدیل آدرس NAT
	۱-۸	بکارگیری مناسب روشهای شبکه امن و خصوصی مجازیVPN , VLan و . . .
۲	ماجول آنتی ویروس فایروال	
	۲-۱	رتبه ضد ویروس نسبت به سایر آنتی ویروس ها (سایت AVComparative)
	۲-۲	بروز رسانی و Update شدن مستمر آن
	۲-۳	قابلیت های هوشمندی و huristic بودن آن
	۲-۴	دارای License و شرکت پشتیبانی کننده قوی در ایران
۳	سیستم تشخیص و پیشگیری تهاجم یا IDS , IPS (IDP)	
	۳-۱	استفاده از نرم افزار log analyzer
	۳-۲	تفکیک Log های تولید شده و ارائه گزارشات مدیریت
	۳-۳	رتبه ، مدل، سخت افزاری یا نرم افزاری بودن
	۳-۴	بروز رسانی و Upgrade بودن (بروز بودن OS دارای اهمیت بالایی است)
۴	سیستم گذرگاه امنیتی Security Gateway (درون یا برون سازمانی)	
	4-۱	تنظیمات امن پارامترهای سیستم
	4-۲	ارائه گزارشات مدیریتی و کنترلی
	4-۳	بروز بودن که بسیار مهم است.
۵	سیستم ثبت و مدیریت وقایع (logs & Event & traffic control) و نحوه هشداردهی به مسئولین (sms,email ...)	
	5-۱	تهیه گزارشات دوره ای
	5-۲	تحلیل log های سرور و ارائه به مسئولین مربوطه
۶	سیستم مدیریت backup اطلاعات سروری(San – Das - Nas) در محل امن	
	6-۱	انجام عملیات دوره ای back up و نگهداری امن آن
	۶-۲	بررسی و تائید تست recovery و restore اطلاعات (مانور)
	۶-۳	کیفیت و رتبه UPS و بکارگیری مؤثر آن
۷	استفاده از آنتی اسپم و جلوگیری از هرزنامه های مختلف (Anti spam)	
۸	سیستم پالایش اطلاعات تحویلی به کاربر (content & image & text filtering)	
۹	پویشگر آسیب پذیری شبکه وسیستم ها (vuLnerability Checking&Scanning) بر روی OS	
۱۰	پویشگر و تست آسیب پذیری های شبکه و سیستم ها (VuLnerability Checking & Scanning) بر روی Application	

چک لیست امنیتی سایت

نام و نام خانوادگی مسئول :

ردیف	موارد حفاظتی	
۱	عدم دسترسی کاربران عادی به تجهیزات active & passive شبکه	
	۱-۱	محل فیزیکی و استقرار سوئیچ و روترها ، hub ، مودم و سخت افزارهای ارتباطی و امنیت آن
	۱-۲	محل عبوری کابل ها از رک ، سقف و کف کاذب و امنیت آن
	۱-۳	امنیت تجهیزات passive (رعایت استانداردها، جنس ، استحکام و محل نصب)
۲	سیستم Air conditioning سایت (کنترل دما، رطوبت، گرد و غبار و ..... که بایستی بصورت اتوماتیک کنترل شود)	
۳	امنیت الکتریکی سایت (Earth – ups- power panel - cabling)	
	۳-۱	سیستم UPS و بکارگیری مؤثر و کیفیت آن
	۳-۲	چاه ارت که اهمیت فوق العاده ای دارد
	۳-۳	امنیت کابل کشی و پانل برق و مسیر کابل ها
۴	کنترل و نظارت بر تردد در سایت	
	۴-۱	دوربین مداربسته
	۴-۲	بکارگیری کارت هوشمند
	۴-۳	پسورد ، کلید و قفل
۵	بکارگیری Honypot (یا برای تست امنیت شبکه میتوان از روشهای Penetration Test های دوره ای، ارزیابی سطح امنیت شبکه بصورت دوره ای، عضویت در سایتهای معتبر بین المللی جهت اطلاع از اخرین حملات اینترنتی و ... نیز استفاده کرد)	
	۵-۱	مدل و نسخه ابزار مورد استفاده
	۵-۲	گزارشات مستمر و بکارگیری مؤثر آن

چک لیست امنیتی سرورها (Servers)

نام و نام خانوادگی مسئول :

ردیف		موارد حفاظتی
۱		قرارگیری سرور در منطقه امن شبکه (پشت فایروال و تجهیزات امنیتی لازم)
	۱-۱	قرار گیری در منطقه امن منطقی
	۱-۲	رعایت موارد امنیتی در دسترسی راه دور به سرور
۲		ضد ویروس یا آنتی ویروس License دار مورد استفاده در سرور
	۲-۱	رتبه، نوع و مدل آنتی ویروس
	۲-۲	بروز رسانی و Update مستمر
	۲-۳	استفاده از log های آنتی ویروس
۳		سیستم ثبت و مدیریت وقایع سرور (event viewer & Log Analyzer)
	۳-۱	تجزیه و تحلیل Log ها
	۳-۲	ارائه گزارشات تحلیلی Log و دسترسی های سرور
۴		بروز رسانی مؤثر نرم افزارهای سیستمی مثل سیستم عامل سرور
	۴-۱	استفاده از Security Patchs ها به طور مداوم
	۴-۲	ارتقاء سیستم عامل متناسب با تکنولوژی و مسائل امنیتی
۵		بروزرسانی مؤثر نرم افزارهای کاربردی و Application های موجود در سرور و استفاده از نرم افزارهای امنیتی و چک برنامه ها
۶		مدیریت کلمه عبور و پسورد برای سرور
	۶-۱	تغییر دوره ای پسورد سرور
	۶-۲	انتخاب پسورد مناسب برای Administrator
	۶-۳	پسورد OTP برای دسترسی شخص ثالث به سرور
۷		سیستم مدیریت backup اطلاعات سرور
	۷-۱	نحوه back up و پشتیبان گیری (استاندارد، روزانه، هفتگی، ماهیانه و ...)
	۷-۲	محل نگهداری اطلاعات back up
	۷-۳	تست و بررسی Recovery و آزمایش آن (مانور)
	۷-۴	تعیین صلاحیت فنی/امنیتی مسئول پشتیبان گیری
۸		امنیت فیزیکی و الکتریکی و برق سرور
	۸-۱	استقرار در رک (Rackmount)
	۸-۲	امنیت فضا، طبقه و اتاق و محل سرور به لحاظ فیزیکی - قرار گیری در Server room
	۸-۳	استفاده از UPS و سنسور دما و سیستم آلارم دهی (Sound , SMS)
۹		عدم فعالسازی نرم افزارهایSharing , RAS بر روی سرور
	۹-۱	عدم وجود نرم افزار peer to peer
	۹-۲	عدم Sharing فایل ها و برنامه ها بصورت بی مراقب
	۹-۳	ارتباط telnet , ftp و Ras , ...
۱۰		مدیریت و کنترل دسترسی کاربران به برنامه های سرور (کنترل دسترسی و مجوزهای دسترسی کاربران و گروه های کاری)
۱۱		تعیین صلاحیت فنی/امنیتی Administrator سرور
۱۲		سیستم عامل سرور (NOS)
	۱۱-۱	امن بودن و License دار بودن سیستم عامل سروری و open source بودن آن
	۱۱-۲	وجود آخرین نسخه (Version) سیستم عامل و Patch های امنیتی آن
	۱۱-۳	تنظیمات امن سروری Secure Config (عدم استفاده از پیش فرض)

چک لیست امنیتی تجهیزات ارتباطی شبکه (Router & Switch & Modem)

نام و نام خانوادگی مسئول :

ردیف	موارد حفاظتی	
۱	پیکربندی و تنظیمات امن روتر یا سوئیچ (… ACL,port security, Encryption)	
۲	بروزرسانی IOS روتر	
۳	مدیریت پسورد Password	
	۱-۳	ترکیب رقم، حرف و علامت و رعایت استانداردهای یک پسورد مناسب
	۲-۳	تغییر دوره ای پسورد
۴	پشتیبان گیری وbackup از config و IOS دستگاه	
	۱-۴	نحوه back up (استاندارد، روزانه، هفتگی، ماهانه و …)
	۲-۴	امنیت محل نگهداری back up
	۳-۴	تست Recovery و فراخوانی اطلاعات (مانور)
۵		
	۱-۵	امین، اعتبار و اطمینان
	۲-۵	دانش و تخصص فنی لازم و کافی
	۳-۵	بینش امنیتی و حفاظتی شبکه و تجهیزات ارتباطی و شناخت اهمیت آن
۶	محل استقرار سخت افزار ارتباطی	
	۱-۶	امنیت فیزیکی و الکتریکی (برق، UPS، ارت و شرایط گرما و رطوبت دستگاه)
	۲-۶	سیستم آلارم دهی (… , Sound , sms) داخل رک

دستورالعمل های امنیتی سیستم عامل

الف – سیستم عامل Windows

۱- از مدل OTP (One Time Password) جهت اختصاص دسترسی به شرکت های طرف قرارداد بمنظور دسترسی به سیستم عاملهای شبکه و ایستگاههای کاری حساس استفاده گردد.

۲- استفاده از مکانیزم Sharing درسیستم عامل های خانواده Windows به صورت پیش فرض منع گردد ، خصوصا در مواقعیکه اطلاعات با طبقه بندی حفاظتی بر روی حافظه Local آنها وجود دارد.

موارد خاص این زمینه، باید به صورت تقاضای مکتوب به این اداره کل ارائه شود.

۳- حق دسترسی به کامپیوتر از طریق شبکه (Access This Computer Over Network) از روی سرور وب به طور کامل تحت کنترل قرار گیرد.

٤- ورود به Bios سرور می بایستی با کلمه عبور بوده و مراحل بوت شدن رایانه سرور به ترتیب از هارد ، سپس فلاپی و یا CD- ROM انجام می شود.

۵- سرور دسترسی از راه دور (Remote Access Server) در صورت عدم نیاز غیرفعال گردد.

٦- گزینه RUN بر روی منو فایل برای ایستگاههای کاری مخصوص کاربران غیرفعال شود.

۷- دسترسی به REGEDIT32.EXE فقط از طریق دسترسی های مجاز انجام گردیده و ترجیحا از روی ایستگاههای کاری حذف شود تا سیستم های عامل ایستگاههای کاری از آسیب مصون بمانند.

۸- از آنجایی که Internet Information Service 5.0 (IIS5) بصورت پیش فرض بر روی همه سرورهای Win2k وجود دارد ، ضروری است از روی سرورهای غیر وب از حالت نصب خارج (Uninstall) گردد.

ب – سیستم عامل Unix Based

۱- اطمینان حاصل شود کلمه عبور کاربر Superuser به طور منظم تغییر داده شود.

۲- مجوزهای دایرکتوری سیستم root/ و dev/ و tmp/ و usr/ و bin / و etc/ و sbin به طور منظم بررسی شوند.

۳- اطمینان حاصل شود برای رمزنگاری کلمه عبورهای کاربری از روشMD5 استفاده می شود.

٤- با کمک دستور Cron برای انجام کارها بازمانبندی منظم، فایل های وقایع نگاری امنیتی(Security log files) به یک مکان جداگانه برای انجام بررسیهای لازم کپی شود.

٥- اطمینان حاصل شود همه کلمه های عبور Shadow فعال شده اند تا کلمه های عبور hash خارج از /etc/passwd ذخیره شوند.

٦- از Property های موجود برای بهبود امنیت در نسخه Unix علاوه بر تنظیمات و اعمال پایه ای ایجاد امنیت در سیستم عامل ها استفاده شود.

٧- امکانات امنیتی اضافی که در نسخه Unix مورد استفاده وجود دارد برای تأمین امنیت بیشتر تنظیم شود(بعنوان مثال ارزشهای متفاوت Secure Level در BSD)

دستور العمل های امنیتی سرویس های شبکه

۱- غیرفعال کردن سرویس های غیرضروری و مخاطره آفرین چون Autoloading , Tftp , Bootp , Telnet و استفاده از سرویس های SSH و FTP به عنوان جایگزین

۲- محدودسازی زمان اتصال : Time Out برای کنسول و خط VTY

۳- در صورت امکان غیرفعال سازی گزینه های زیر :

– Ipsec Policy Agent برای جلوگیری از تغییر غیرمجاز در پیکربندی پروتکل Ipsec

-Spooler به منظور محدود کردن دسترسی به پرینتر از طریق وب سرور

-Licensing Logging Service

- Logical Disk Manager Admin Service

-Remote Registry Service برای جلوگیری از تغییر غیرمجاز در Registry از راه دور

-Removal Stronge

-Run a Service برای جلوگیری از اجرای برنامه ها در قالب سرویس

-Tcp/ip NetBios Helper برای جلوگیری از رویت سیستم های موجود در همسایگی شبکه

-Server Service برای جلوگیری از تغییر غیرمجاز در پیکربندی سرور

-Task Scheduler برای جلوگیری از اجرای خارج از کنترل برنامه ها با کدهای مخرب

-Telephony Service برای جلوگیری از اتصال به سرویس دهنده های Telephony غیرمجاز

-Windows Installer

-Windows Time

-WorkStation Service برای جلوگیری از امکان اجرای برنامه ها از راه دور

-Computer Browser برای جلوگیری از امکان مشاهده سایر کامپیوترهای همسایه و منابع به اشتراک گذاشته شده

-Network Monitor Agent برای جلوگیری از دستیابی به ترافیک سایر زیرشبکه های متصل

-RPC Locator برای جلوگیری از یافتن برنامه های قابل اجرای موجود در مسیرهای دیگر

-**Directory Browsing** برای جلوگیری از مرور دایرکتوریهای که در شبکه Share شده اند.

٤- محدودسازی **IP** اتصال به روتر جهت پیکربندی مدیریتی و همچنین برای DSLAM

۵- جداسازی شبکه با Vlan و Subnetting

٦- کنترل دسترسی از طریق VPN بعنوان یک اقدام پیشگیرانه قبل از FTP Login قرار گیرد.

۷- دسترسی به تمامی پورتهای TCP/ IP ثبت و بررسی شود.(سخت افزار ذخیره سازی و نرم افزار تحلیل Log مربوطه فراهم شود)

۸- اقدامات پیشگیرانه به منظور اطمینان از اینکه سرور FTP بمنظور دسترسی به سیستم فایل شبکه شرکت استفاده نمی شود.

۹- در صورت استفاده از مدل آدرس دهی ایستا ، DHCP client غیرفعال شود.

۱۰- Shut Down کردن پورت Auxiliary

دستورالعمل های مسیر یابی (تجهیزات ارتباطی دیتا)

۱- حتی الامکان در لایه های مرزی و Send دیتا از پروتکل های مسیریابی ایستا (Static) جهت مسیریابی شبکه استفاده شود.

۲- در صورت استفاده از الگوریتم های مسیریابی دینامیک داخلی یا خارجی (Dynamic Routing) باید از مکانیزم های تشخیص هویت جهت امن سازی تبادل اطلاعات مسیریابی استفاده شود.

۳- لازم است مکانیزم های Direct BroadCast , Source Routing مسیریاب ها غیرفعال گردند.

٤- در صورت استفاده از الگوریتم های مسیریابی دینامیک و در موارد ضروری از مکانیزم های Route Filtering برای جلوگیری از انتشار اطلاعات مسیریابی داخلی به شبکه های خارجی استفاده شود.

٥- لازم است امکانات اتصال مستقیم به مسیریاب یا سوئیچ های شبکه ای مثل پورت Console یا AUX تحت کنترل قرار داشته باشد تا از سوء استفاده از این امکانات برای دخالت در مسیریابی جلوگیری شود.

٦- حتی الامکان بایستی از مکانیزم تبدیل آدرس های شبکه NAT در نقاط اتصال شبکه های داخلی و خارج از سازمان و یا برای حفاظت از بخش های خاص شبکه استفاده شود.

۷- لازم است پروتکل ها و تجهیزات مسیریابی شبکه از طریق شناسایی آدرس های مبدأ و مقصد بسته های اطلاعاتی و بررسی مجاز بودن ارسال آنها تحت کنترل قرار گیرد.

۸- پیکربندی ، راه اندازی و یا نصب مجدد مسیریاب توسط افراد معتمد انجام شود.

من ا... التوفیق – علی ثاقب موفق