به نام خدا

امنيت شبكه در سازمان‌هاي متوسط

مقدمه

از آن‌جا كه تمامي ارتباطات و اطلاعات سازمان‌ها اعم از كوچک، متوسط و بزرگ به صورت كامپيوتري درآمده است، لذا انتقال و دسترسي به آن‌ها نيز ملزم به ايجاد و نگهداري شبكه‌هايي است كه اين امكان را فراهم مي‌سازند. در سازمان‌هاي با ابعاد متوسط هرچند تعداد سيستم‌ها و منابع شبكه محدود مي‌باشند اما امنيت اطلاعات و ارتباطات كامپيوتري از اهميت بالايي برخوردار است. در مستند حاضر به بررسي و ذكر مواردي پرداخته شده است كه جهت ايجاد حداقل ميزان امنيت در شبكه‌هاي كامپيوتري براي سازمان‌هاي متوسط مورد نياز است. براي اين منظور كل مبحث امنيت شبكه در سازمان‌هاي متوسط به چند بخش مجزا تقسيم شده و سپس به ارائه نكات لازم به اجرا در هر كدام پرداخته شده است.

در اين مستند حداقل نيازمندي‌ها براي امن‌سازي شبكه داخلي يک سازمان متوسط ارائه شده است. اين موارد حداقل بوده و حداقل امنيت را به وجود مي‌آورد. لازم به ذكر است كه مستند تنها از ديدگاه نظارتي تهيه شده و موارد مورد نياز براي مطالبه از پيمانكار بيان شده و وارد جزئيات فني نگرديده است. در اجراي اين پروژه استفاده از مشاور و يا ناظر اجباري نمي‌باشد.

امنيت در سازمان متوسط

منظور از سازمان متوسط؛ سازماني با حدود ۲۰ تا ۵۰ كامپيوتر است. ساختار شبكه سازمان‌هاي متوسط پيچيده نيست و از يک شبكه محلي (شامل چندين سوئيچ و حداكثر يک فايروال و روتر) تشكيل شده است كه اتصال به اينترنت و شبكه دولت نيز دارد. هزينه‌ي انجام اين شرح خدمات حدود سيصد ميليون ريال (۳۰۰/۰۰۰/۰۰۰) مي‌باشد.

براي ايجاد امنيت در شبكه‌هاي كامپيوتري سازمان‌هاي با ابعاد متوسط، تمامي اقدامات لازم به نُه بخش جداگانه قابل تقسيم است:

امنيت فيزيكي

امنيت ايستگاه‌هاي كاري
امن‌سازي سرورها
امنيت ارتباطات بي‌سيم
امنيت ساختار شبكه سازمان
دستورالعمل‌ها و روال‌هاي امنيتي
نظارت امنيتي
تست نفوذ
آموزش و فرهنگ‌سازي
امنيت فيزيكي

امنيت فيزيكي به صورت ايده‌آل موارد متعددي را دربرمي‌گيرد به همين دليل در اين ابعاد پرداختن به آن ضروري نيست. پيمانكار در اين مورد مگر براي امنيت ارتباطات بي‌سيم وظيفه اجرايي به عهده ندارد و فقط بايد موارد زير را بررسي و موارد نقض آن را به اطلاع كارفرما برساند:

امنيت فيزيكي ارتباطات

امنيت فيزيكي ايستگاه‌هاي كاري
امنيت فيزيكي سرورها، سوئيچ‌ها، روترها و فايروال‌ها
امنيت فيزيكي ارتباطات بي‌سيم
امنيت فيزيكي ارتباطات

جهت ايجاد امنيت ارتباطات در بخش امنيت فيزيكي رعايت موارد زير الزامي است:

كابل‌كشي شبكه كامپيوتري طبق استاندارد TIA/EIA-568-B
عدم وجود گره‌هاي شبكه در محل‌هايي كه امكان كنترل آن‌ها وجود ندارد و يا عدم عبور كابل از محل‌هاي نزديک به گرما و برق فشار قوي و محل‌هايي كه احتمال قطعي‌هاي ناخواسته دارد.

امنيت فيزيكي ايستگاه‌هاي كاري

ايجاد امنيت فيزيكي در ايستگاه‌هاي كاري يک سازمان ملزم به رعايت نكات زير است:

عدم استقرار سيستم‌ها در محل‌هاي با دسترسي بسيار سخت
استقرار سيستم‌ها به دور از محل‌هاي عبور لوله‌هاي آب و گاز يا كابل‌هاي برق بدون حفاظ
استقرار سيستم‌ها در محل‌هاي با ثبات بالا و محل‌هايي كه كمتر در مسير راه افراد قرار دارند
عدم اتصال laptopهايي كه محدوديت‌هاي امنيتي روي آن اعمال نشده به شبكه سازمان

امنيت فيزيكي سرورها، سوئيچ‌ها و روترها

در راستاي امن‌سازي فيزيكي سرورها، سوئيچ‌ها و روترهاي شبكه يک سازمان رعايت موارد زير الزامي است:

١. استقرار آن‌ها در محلي امن و دور از دسترسي همگان

٢. دسترسي آسان براي مدير يا مديران شبكه سازمان

٣. استقرار آن‌ها در جعبه‌هاي محافظ (Rack)

٤. عدم وجود پايانه‌هاي آب و گاز يا كابل‌هاي بدون حفاظ برق در محل نگهداري آن‌ها

٥. استفاده از UPSهاي با ظرفيت مورد نياز سازمان

٦. وجود كپسول آتش‌نشاني در نزديكي محل استقرار سرور

امن‌سازي سرورها

در سازمان‌هاي متوسط توصيه مي‌شود حداقل ٤ عدد سرور زير نصب گردد:

١. سرور كنترلي با نصب سرويس‌هاي زير:

- (Controller, Active Directory, Windows Service Update Server (WSUS Domain

Server, log server Antivirus-

٢. DNS ,FTP Server, Web Server, File Server به عنوان پشتيبان سرور كنترلي

٣. سرور(هاي) برنامه‌هاي كاربردي (مانند اتوماسيون اداري)

٤. سرور اتصال به اينترنت (دروازه اينترنتي) و شبكه‌هاي خارجي ديگر مانند شبكه دولت (با نصب مثلا Server ISA)

سرورهاي يک، دو و سه بايد از لحاظ سخت‌افزاري كاملا قابل اطمينان (با مشخصات: دو عدد كارت شبكه G١ , دو عدد CPU 2.3G 2M cache و دو عدد Hard SATA 300G , و دو عدد Power و با قيمتي حدود بيست ميليون ريال) باشند ولي چهارمين سرور حتي مي‌تواند يک عدد رايانه شخصي مناسب هم باشد.

بر روي اين سرورها جهت اجرا و كنترل برنامه‌هاي داخلي سازمان رعايت نكات عمومي زير (جهت ايجاد و نگهداري امنيت براي اين سيستم) ضروري مي‌باشد:

داشتن دستورالعمل پيكربندي امن سرور و نصب حداقل سرويس‌هاي لازم روي آن (با جزييات بسيار بيشتر از تنظيمات ويندوز در امنيت ايستگاه‌هاي كاري (قسمت بعد))
نصب ابزارهايي براي ارسال log به log server
تنظيمات مناسب و امن براي به‌روزشدن آنتي‌ويروس و بسته‌هاي امنيتي سيستم عامل
داشتن تنظيمات خودكار براي پشتيبان‌گيري
داشتن رويكرد و ابزار امن براي پيكربندي سرور از راه دور

FTP Servers

۱. غير فعال كردن دسترسي Anonymous

۲. فعال‌سازي تنظيمات پيچيدگي انتخاب كلمات عبور

۳. تنظيم Logon Eventها

٤. فعال‌سازي سرويس Logging مربوط به FTP

٥. در صورت عدم نياز به بارگذاري اطلاعات از سايت FTP، سايت را به صورت يک طرفه تنظيم نماييد (فقط امكان ارسال يا نوشتن اطلاعات در سرور)

٦. فعال‌سازي سرويس Disk Quota

۷. اعمال محدوديت‌هاي زماني براي شناسه‌هاي كاربري

۸. فعال‌سازي سرويس‌هاي Account Lockout و Account Lockout Threshold

۹. افزايش ميزان پيچيدگي و دشواري ACLها

Web Servers

۱. استفاده از سرورهاي مجزا براي برنامه‌هاي داخل شبكه و خارج از شبكه محلي

۲. امكان مميزي عملكردهاي وب سايت و نگهداري Logها در يک محل امن

۳. استفاده از پويشگر برنامه (Scanner Application)

امن سازي [DC]۱

به منظور ايجاد امنيت در Domain Controller شبكه سازمان رعايت اصول زير الزامي است:

۱. امنيت فيزيكي DC

۲. بستن دسترسي كاربر Anonymous

۳. ساخت يک شناسه كاربري با دسترسي محدود و استفاده مدير شبكه از آن و استفاده از حساب كاربري Administrator فقط در مواقع ضروري

٤. نصب فايروال و آنتي‌ويروس قابل مديريت

٥. دور نگه داشتن DC از حملات راه دور مانند عدم دسترسي به اينترنت يا مودم

٦. ايجاد امنيت بيشتر روي حساب‌هاي كاربري داخل DC

۷. جا به جا كردن محل ذخيره بانک‌هاي اطلاعاتي Active Directory

امن‌سازي [DNS]۲

پيروي از دستورات زير جهت امن‌سازي سرويس‌دهنده‌هاي DNS الزامي است:

۱. استفاده از DNS Forwarderها

۲. استفاده از سرويس‌دهنده‌هاي DNS Cache-Only

۳. استفاده از Advertiser DNSها

٤. استفاده از DNS Resolverها

٥. حفاظت و کنترل Pollution Cache

٦. فعال کردن DDNS

۷. غيرفعال کردن Zone Transfer

۸. نصب و پيکربندي فايروال روي سيستم سرويس‌دهنده DNS

۹. تنظيم کنترل دسترسي روي اطلاعات و ورودي‌هاي DNS در رجيستري

۱۰. تنظيم کنترل دسترسي روي اطلاعات و ورودي‌هاي DNS در فايل سيستم

۱۱. استفاده از DNS Root و Namespace داخلي براي شبکه سازمان

امنيت ايستگاه‌هاي کاري

پيمانکار موظف است به منظور امن‌سازي ايستگاه‌هاي کاري در شبکه، موارد زير را براي تمام دستگاه‌هاي شبکه اجرا نمايد:

تنظيمات ويندوز

داشتن دستورالعمل پيکربندي امن ويندوز شامل:

۱. استفاده از فايل سيستم NTFS براي کليه پارتيشن‌ها

۲. غيرفعال کردن Sharing Simple File

۳. استفاده از کلمه عبور براي کليه حساب‌هاي کاربري (مخصوصا administrator که به صورت پيش‌فرض بدون پسورد ايجاد مي‌شود)

٤. غيرفعال کردن حساب کاربري Guest و بقيه حساب‌هاي کاربري بلااستفاده

٥. تنظيم محافظ صفحه با کلمه عبور

٦. غيرفعال کردن Remote Desktop براي کليه سيستم‌ها

۷. فعال و تنظيم کردن Audit و Logها براي کليه سيستم‌ها

۸. غيرفعال کردن قابليت راه‌اندازي سيستم عامل توسط Floppy يا CD ROM

۹. غيرفعال کردن auto play براي CD flash , drive

۱۰. تنظيمات مناسب و يا نصب ابزارهايي براي ارسال log به log server

۱۱. تنظيمات مناسب و امن براي به‌روزشدن بسته‌هاي امنيتي سيستم عامل

۱۲. داشتن رويکرد و ابزار امن براي پيکربندي ايستگاه کاري از راه دور

تنظيمات آنتي‌ويروس

پس از پيکربندي سيستم عامل مطابق با شرايط فوق نصب و پيکربندي يک آنتي‌ويروس مناسب براي

كليه ايستگاه‌هاي كاري با رعايت نكات زير الزامي است:

۱. استفاده از آنتي‌ويروس داراي License معتبر

۲. نصب آنتي‌ويروس براي كليه سيستم‌هاي سازمان، بدون استثنا

۳. تنظيم ثبت مرتب و خودكار Logهاي آنتي‌ويروس

٤. تنظيم به‌روزرساني منظم و خودكار آنتي‌ويروس

۵. استفاده از آخرين نسخه آنتي‌ويروس

٦. تنظيم شناسايي و حذف خودكار ويروس‌هاي يافت شده توسط آنتي‌ويروس

امنيت ارتباطات بي‌سيم

در صورتي كه در ساختار شبكه يک سازمان از تكنولوژي ارتباطات بي‌سيم جهت انتقال اطلاعات استفاده شود، رعايت موارد زير الزامي است:

استفاده از تكنولوژي رمزنگاري WEP
تغيير تنظيمات پيش‌فرض SSID
اختصاص آدرس‌هاي IP به ايستگاه‌هاي كاري بي‌سيم به صورت دستي نه DHCP
غير فعال كردن حالت Ad-Hoc در صورت استفاده از Access Point
ايجاد ACLهاي مخصوص سازمان
ثبت MAC آدرس‌هاي تک تک ايستگاه‌هاي كاري در ACLهاي مربوط به Access Pointها
غيرفعال‌سازي سرويس File and Printer sharing در صورت عدم نياز به استفاده از آن‌ها.
چيدمان صحيح نقاط دسترسي (Access Point) به گونه‌اي كه گستره امواج راديويي تنها در دامنه تعيين شده شبكه سازمان باشد

جدا ساختن شبكه‌هاي بي‌سيم و سيم‌كشي شده توسط فايروال.

آموزش و اطلاع‌رساني كاربران در مورد اهميت امنيت ارتباطات بي‌سيم

امنيت ساختار شبكه سازمان

پيمانكار موظف است پس از بررسي ساختار فعلي شبكه و نيازهاي سازمان، طراحي امني براي شبكه سازمان ارائه و آن را اجرا كند. لازم به ذكر است كه پيش از طراحي امن ، پيمانكار بايد ارزيابي امنيتي موردي انجام دهد. در تهيه ساختار امن شبكه و پياده‌سازي آن بايد موارد بيان شده در اين فصل لحاظ گردد. پس از طراحي امن، پيمانكار موظف است RFP براي خريد تجهيزات سخت‌افزاري تهيه نمايد و پس از خريد توسط كارفرما آن تجهيزات را تست كند و تحويل بگيرد.

طراحي امن شبكه

در طرح شبكه موارد زير بايد لحاظ گردد:

۱. در صورت وجود سرورهايي كه به خارج از سازمان سرويس مي‌دهند بايد ناحيه DMZ ايجاد شود.

۲. در صورت نياز بايد سرور يا شبكه VPN ايجاد شود.

۳. سرورهاي داخلي يا خارجي بايد از هم مجزا باشند.

٤. بين شبكه اينترنت و شبكه DMZ بايد از يک مسيرياب يا فايروال استفاده كرد.

۵. بين شبكه DMZ(و در صورت عدم وجود اينترنت) و شبكه داخلي سازمان بايد از فايروال استفاده كرد.

٦. در صورتي كه نياز سازمان به چند ناحيه مجزا باشد اين نواحي بايد ايجاد و بين آن‌ها مسيرياب يا

فايروال قرار گيرد.

۷. نواحي مختلف شبكه داخلي، DMZ و ورود شبكه اينترنت به سازمان بايد در لايه فيزيكي از هم مجزا شوند (يا به صورت فيزيكي و يا VLAN)

۸. در صورت وجود ارتباط بي‌سيم بايد در ناحيه جدا قرار گرفته و از مسيرياب و VPN استفاده شود.

۹. ساختار IP و Subnet Mask و Routing IP طراحي و اجرا شود.

امنيت VPN

تكنولوژي VPN اين امكان را فراهم مي‌آورد تا بتوانيم از شبكه‌هاي عمومي مانند اينترنت به صورت امن به جاي شبكه‌هاي خصوصي استفاده كنيم. در موارد زير استفاده از VPN ضروري است:

۱. لازم باشد مدير يا كارمندي از راه دور مثلاً منزل يا محل مسافرت به منابع شبكه داخلي سازمان دسترسي داشته باشد

۲. سازمان داراي نماينده يا نمايندگاني در مكان‌هاي دور از سازمان يا شهرها و كشورهاي ديگر باشد

۳. پشتيباني توسط كارشناسان يا مديران شبكه خارج سازمان

٤. وجود ارتباط بي‌سيم

در صورت نياز به استفاده از VPN مي‌توان از سرويس دهنده ISA استفاده نمود كه رعايت موارد زير در اين مورد الزامي است:

۱. تنظيم پيچيدگي انتخاب كلمات عبور

۲. استفاده از پروتكل‌هاي MS-CHAP v2 و EAP به جاي پروتكل‌هاي PAP، SPAP و CHAP

۳. غيرفعال كردن پروتكل‌هاي PAP، SPAP و CHAP

٤. استفاده از پروتكل L2TP به جاي IP در ارتباطاتي كه از IPSec استفاده مي‌كنند

٥. انتقال كليه كاربران داراي سطح دسترسي از راه دور به يک گروه كاربري جهت مديريت متمركز

٦. تعيين سطح دسترسي‌هاي مورد نياز كاربر يا گروه‌هاي كاربران به فايل‌ها، برنامه‌ها و منابع شبكه داخلي با توجه به نياز آن‌ها

۷. فعال‌سازي و تنظيم دقيق Log Event جهت كنترل دقيق ارتباطات VPN

فايروال

در صورت نياز به فايروال مي‌توان از فايروال‌هاي سخت‌افزاري يا نرم‌افزاري متناسب همانند ISA يا لينوكس استفاده كرد. در صورت استفاده از سرويس‌دهنده ISA جهت مديريت امنيت شبكه سازمان، رعايت موارد زير كاملاً ضروري است:

تنظيمات لازم مربوط به سيستم عامل

۱. عدم نصب ISA Server روي Controller Domain

۲. عدم نصب سرويس يا برنامه‌هاي كاربردي روي سيستم سرويس‌دهنده ISA

۳. افزايش ميزان دشواري كلمات عبور كاربران سيستم سرويس‌دهنده ISA

٤. حذف كليه سرويس‌هايي كه مورد استفاده سيستم عامل و ISA قرار نمي‌گيرند

٥. به‌روزرساني و نصب بسته‌هاي امنيتي سيستم‌عامل و ISA به طور مرتب

٦. غيرفعال كردن سرويس Printer Sharing File and روي كارت شبكه خارجي[٣]

٧. غيرفعال كردن سرويس Microsoft Networks Client for روي كارت شبكه خارجي

٨. غيرفعال كردن NetBIOS مربوط به TCP/IP روي كارت شبكه خارجي

تنظيمات لازم مربوط به ISA Server

١. فعال كردن Packet Filtering

٢. فعال كردن Filtering Fragment

٣. فعال كردن options Filtering of IP

٤. فعال كردن Detection Intrusion

٥. حذف كليه دسترسي‌ها از قسمت Site and Content Rule يا تنظيم دسترسي‌هاي اين قسمت براي كاربر يا گروهي از كاربران

٦. حذف كليه Web Proxy listenerها در صورت عدم نياز به استفاده از Web Publishing Rules

٧. ايجاد Protocol Ruleهاي لازم جهت دسترسي‌هاي برون سازماني

٨. محدودسازي دسترسي كاربران به پروتكل‌ها و تنظيم امكان دسترسي افرادي كه به آن‌ها نياز دارند

٩. تنظيم ارسال هشدارهاي امنيتي ISA Server به E-Mail مدير شبكه

١٠. بازبيني مرتب و منظم Log Eventها

١١. ذخيره دقيق و منظم Logها روي يک حافظه جداگانه و كپي‌برداري روزانه از آن‌ها

١٢. فعال كردن فيلترهاي DNS، POP و SNMP

١٣. غير فعال كردن فيلتر SOCKS

١٤. فقط قراردادن آدرس‌هاي شبكه داخلي در LAT

١٥. فقط قرار دادن دامنه‌هاي[٤] شبكه داخلي در LDT

١٦. استفاده از سياست‌هاي[٥] RRAS در كنترل دسترسي‌ها و مديريت VPN

١٧. استفاده از كلمات عبور پيچيده، به خصوص اگر از PPTP استفاده مي‌شود

١٨. اقدام به استفاده از L2TP/IPSec در اولين زمان ممكن

مستندسازي و تدوين دستورالعمل‌ها و روال‌هاي امنيتي

مهمتر از ايجاد امنيت در شبكه سازمان حفظ و تداوم امنيت مي‌باشد، به همين منظور معمولا تشكيلاتي در سازمان براي اين هدف تشكيل مي‌گردد. اما در سازمان‌هايي با اين ابعاد مستندسازي و تهيه و اجراي دستور العمل‌ها و روال‌هايي براي امنيت كفايت مي‌كند.

پيمانكار موظف است مستندات زير را در صورت عدم وجود تهيه و در صورت وجود به‌روزرساني و سازگار كند:

۱. نقشه شبكه سازمان

۲. مستندات مربوط به محل قرار گيري سخت‌افزارها و شماره‌هاي آن‌ها (اموال سازمان)

۳. مستندات مربوط به كابل‌كشي‌ها و محل قرار گيري سرورها، سوئيچ‌ها و روترها

پس از مستندسازي شبكه سازمان بايد دستورالعمل‌هايي وجود داشته باشد كه با پيروي از آن‌ها اين امنيت ايجاد شده پايدار بماند.

اين دستورالعمل‌ها توسط پيمانكار تهيه و بعدا توسط پرسنل كارفرما اجرا خواهند شد. هر كدام از آن‌ها حداقل يكبار توسط پيمانكار نيز بايد اجرا شوند. حداقل دستورالعمل‌هاي مورد نياز در زير آمده‌اند.

روال پشتيبان‌گيري

در تعيين روندها و دستورالعمل‌هاي پشتيبان‌گيري از اطلاعات سيستم‌هاي يک سازمان لازم است تا آيين‌نامه‌اي مدون طراحي شود. در اين آيين‌نامه حداقل به نحوه، ابزار، نوع، زمان و محل ذخيره پشتيبان‌گيري بايد پرداخته شود.

در زير به ذكر مواردي پرداخته‌ايم كه بايد در تهيه آيين‌نامه روندهاي پشتيبان‌گيري يک سازمان حتماً مورد توجه قرار بگيرد. اين پشتيبان‌ها از اطلاعات سرورها و اطلاعات رايانه‌هاي كاربران بايد باشد.

انتخاب زمان تهيه نسخه پشتيبان

- روزانه
- هفتگي
- ماهانه
- سالانه

انتخاب يكي از انواع نسخه پشتيبان

- Full
- Incremental
- Deferential
- Copy

انتخاب محل ذخيره و نگهداري نسخه پشتيبان

۱. حافظه خارجي[٦]

۲. Floppy، CD يا DVD

۳. سرور يا يک سيستم جداگانه براي اين منظور

٤. محل ذخيره On-Line

در تعيين موارد فوق رعايت اصول ارائه شده در جدول زير الزامي است

زمان	نوع	محل ذخيره
روزانه	Incremental, Deferential	4،3
هفتگي	Incremental, Deferential	4،3 ،2
ماهانه	Full	2،1
سالانه	Full	2،1

توصيه مي‌شود حتما حداقل يک مدل پشتيبان‌گيري برروي حافظه خارجي، CD و ... در نظر گرفته شود که ماهانه يا هفتگي باشد و اين اطلاعات پشتيبان در محلي امن غير از اتاق سرور نگهداري شود.

دستورالعمل‌هاي نگهداري شبکه

در اين ابعاد سازماني حفظ پايداري شبکه (Availability) و مديريت استفاده از آن بزرگترين دستاوردي است که از امنيت توقع مي‌رود. به همين منظور تهيه و اجراي آيين‌نامه‌ها و روال‌هاي نگهداري شبکه که در اين راستا مي‌باشد ضروري است:

دستورالعمل نگهداري سيستم‌عامل‌ها

روال نامگذاري سيستم‌ها
روال نگهداري و به‌روزرساني آنتي‌ويروس‌ها
فرآيندها و فرم‌هاي بازبيني‌هاي دوره‌اي سيستم‌ها
روال انتقال تا بازگشت سيستم‌ها جهت تعمير
روال نگهداري و به‌روزرساني مستندات شبکه
روال بررسي دوره‌اي logها
آيين‌نامه انتخاب و تغيير کلمات عبور کاربران
آيين‌نامه روند تهيه نسخه پشتيبان
آيين‌نامه روند جابجايي، تعويض يا خريد قطعات
آيين‌نامه سطوح دسترسي هريک از کاربران به منابع ديگر سيستم‌ها و منابع شبکه سازمان
روال نگهداري و به‌روزرساني مستندات شبکه مانند گرفتن backup از سيستم عامل ِ همه تجهيزات مانند سوئيچ و روتر و سرور براي به حداقل رساندن زمان در دسترس نبودن سيستم و روال نگهداري از نسخه‌هاي پشتيبان در سازمان

نظارت امنيتي

کنترل و نظارت امنيتي بر شبکه از موارد بسيار با اهميت در امر نگهداري امنيت شبکه‌هاي کامپيوتري مي‌باشد. پيمانکار موظف است که ابزار لازم جهت استفاده‌ي مدير شبکه سازمان جهت اسکن و کنترل شبکه را به منظورهاي زير فراهم آورد:

کنترل شبکه از لحاظ عدم اتصال سيستم‌هاي غير مجاز به شبکه سازمان
شناسايي سرويس‌هاي تهديد آميز
تعيين ميزان انحراف از سرويس‌هاي مجاز تعريف شده براساس سياست‌هاي امنيتي سازمان
بررسي و تحليل logها
بهتر است تعداد ابزارها تا حد امکان کم و يا از طريق واسط متمرکز اداره شوند.

تست نفوذ

اجراي تست نفوذ از مهمترين روش‌ها براي اطمينان از وجود يک امنيت نسبي است. در سازمان‌هاي متوسط لازم است تا به صورت دوره‌اي تست نفوذ جهت اطمينان از وجود امنيت اجرا شود و پيمانکار موظف است که در انتهاي پروژه يک بار تست نفوذ را انجام دهد و سپس حدود سه ماه پس از پايان پروژه نيز يکبار ديگر تست نفوذ انجام شود. پيمانکار بايد ضمن ارائه‌ي گزارش اين تست به کارفرما ، آسيب‌هاي قابل رفع شناسايي شده را رفع کند. حداقل موارد زير در اين تست بايد مورد نظر قرار گيرند:

۱. سوراخ‌هاي امنيتي هسته سيستم عامل[۷] براي تمام ايستگاه‌ها به خصوص سرورها و تجهيزات شبکه

۲. سرريزي بافر[۸] براي سرورها به خصوص وب

۳. دسترسي‌هاي فايل و [Directory۹]

٤. تروجان‌ها[١٠]

٥. گذر واژه‌هاي ضعيف

آموزش و فرهنگ‌سازي

همان طور كه قبلا هم تصريح شد حفظ امنيت از خود آن مهمتر و مشكل‌تر است؛ و حفظ تداوم امنيت به عهده پرسنل سازمان است. پس اين امر محقق نمي‌شود مگر با آموزش و فرهنگ‌سازي. آموزش كاركنان و مديران شبكه هر سازماني الزامي است. اين آموزش بايد در دو سطح عمومي (كاربران) و مدير شبكه (راهبران) اجرا شود. مطالب مورد نظر براي كاربران بايد به دو صورت تئوري ٤ ساعت و عملي ٤ ساعت ارائه شود. براي مدير شبكه يا جانشين وي نيز در دو مرحله تئوري ٢٠ ساعت و عملي ١٠ ساعت آموزش‌هايي در نظر گرفته مي‌شود كه در ادامه به محتواي اين دوره‌ها مي‌پردازيم.

آموزش مديران شبكه (راهبران)

١. مفاهيم امنيت

٢. چرخه‌ي امن كردن سيستم

٣. انواع حملات و تهديدهاي شبكه

٤. روش‌هاي مقابله با حملات و تهديدات

٥. ارزيابي امنيت شبكه و مديريت امنيت شبكه

٦. پيكربندي امن تجهيزات شبكه (سوييچ ، روتر ، فايروال)، سيستم عامل‌ها، نرم‌افزارها

٧. نصب نرم‌افزارهاي امنيتي

٨. نصب وصله‌هاي امنيتي

٩. ثبت وقايع و استفاده و مديريت از Event Log (رويدادنگاري)

١٠. مواجهه با حوادث

١١. تسلط به روال‌ها و دستورالعمل‌هاي تدوين شده براي امنيت شبكه

١١-١ اهميت و مديريت كلمات عبور خود و ديگر كاربران

١١-٢ مديريت و نگهداري سرويس‌هايي مانند patchهاي امنيتي و آنتي‌ويروس‌ها

١١-٣ اهميت و مديريت سطوح دسترسي كاربران به ديگر سيستم‌ها و منابع شبكه

١١-٤ اهميت و نحوه پشتيبان‌گيري

١١-٥ آشنايي و مديريت دسترسي به اينترنت و به اشتراک‌گذاري آن

١١-٦ آشنايي و تسلط به روال‌هاي ارائه شده جهت اجرا مانند نحوه بازگرداني backupهاي سيستم عامل‌هاي تجهيزات

آموزش كاربران

١. مفاهيم امنيت

٢. چرخه‌ي امن كردن سيستم

۳. نكات خاص مانند پشتيبان‌گيري

٤. نكات فني استفاده از امكانات اعم از نرم‌افزارها، سخت‌افزارها و سيستم عامل

۵. آشنايي با پيكربندي سيستم عامل

٦. استفاده از ابزارهاي امنيتي مانند آنتي‌ويروس

۷. انتخاب گذرواژه

۸. مواجهه با حوادث

۹. اجرا، به‌روزرساني و درک پيام‌هاي آنتي‌ويروس

۱۰. توانايي تشخيص موارد بحراني و نحوه برخورد اوليه با آن

۱۱. درک اوليه حداقل امنيت ايستگاه‌هاي كاري و توانايي بررسي آن در موارد ساده (مثل فعال بودن فايروال رايانه شخصي)

۱۲. آشنايي با مشكلات امنيتي IE و MS Outlook و نحوه به اشتراک‌گذاري اطلاعات

۱۳. درک لزوم تهيه نسخه پشتيبان

۱٤. خطرات ناشي از برنامه‌هاي دانلود شده از سايت‌هاي نامعتبر