INSO
11210-4
1st. Edition
2012

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۱۲۱۰-۴
چاپ اول
۱۳۹۱

فن‌آوری اطلاعات - فنون امنیتی- امنیت شبکه فن‌آوری اطلاعات –
قسمت ۴: ایمنی دسترسی از راه دور

Information technology – Security techniques – IT network security – Part 4: Securing remot access

ICS:35.040

به‌نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود . پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب ، به عنوان استاندارد ملی ایران چاپ و منتشر می شود . بدین ترتیب ، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5]در کشور فعالیت می کند . در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت‌های علمی ، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون ، برای حمایت از مصرف کنندگان ، حفظ سلامت و ایمنی فردی و عمومی ، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی ، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/ یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور ، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید . همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره ، آموزش ، بازرسی ، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی ، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم ، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند . ترویج دستگاه بین المللی یکاها ، کالیبراسیون (واسنجی) وسایل سنجش ، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
" فن‌آوری اطلاعات – فنون امنیت – امنیت شبکه فن‌آوری اطلاعات – قسمت ۴: ایمنی دسترسی از راه دور "

رئیس:	**سمت و/یا نمایندگی**
فرهاد، نعمتی (فوق‌لیسانس مهندسی کامپیوتر)	دانشگاه آزاد اسلامی تبریز

دبیر:

خوشقدم، سهیلا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکا پژوه

اعضاء: (اسامی به ترتیب حروف الفبا)

اصل‌زاد، محمدعلی (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه
الهی، بهمن (لیسانس مکانیک)	شهرداری تبریز
بدلی افشرد، بابک (لیسانس مهندسی کامپیوتر)	اداره کل استاندارد آذربایجان‌شرقی
بدلی افشرد، محمدرضا (فوق لیسانس مهندسی برق)	نیروگاه حرارتی تبریز
جباری خامنه، حسین (دکترای آمار)	دانشگاه سراسری تبریز
خاک‌پور، علی (لیسانس مهندسی کامپیوتر)	شرکت ایران دیتا
عظیمی حسینی، سارا (لیسانس مهندسی کامپیوتر)	شرکت ریزفناوران آرکاپژوه

مسدد، شیدا
(لیسانس مهندسی کامپیوتر)
شرکت ایرانسل

فهرست مندرجات

ادامه فهرست مندرجات

پیش‌گفتار

استاندارد " فن‌آوری اطلاعات – فنون امنیت – امنیت شبکه فن‌آوری اطلاعات – قسمت ۴: ایمنی دسترسی از راه دور" که پیش‌نویس آن در کمیسیون‌های مربوط توسط شرکت ریزفناوران آرکا پژوه تهیه و تدوین شده و در یکصد و شصت و دومین اجلاسیه کمیته ملی استاندارد رایانه مورخ ۹۱/۰۲/۱۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوّب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحوّلات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در موقع لزوم تجدید نظر خواهد شد و هرگونه پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرارخواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مأخذی که برای تهیهٔ این استاندارد مورد استفاده قرارگرفته به شرح زیر است :

ISO/IEC 18028-4, 2005: Information technology – Security techniques – IT network security- Part 4: Securing remot access.

فن‌آوری اطلاعات – فنون امنیت- امنیت شبکه فن‌آوری اطلاعات – قسمت ۴: ایمنی دسترسی از راه دور

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، فراهم نمودن رهنمودهایی برای استفاده ایمن دسترسی از راه دور است. روشی که از راه دور یک رایانه را با رایانه دیگر متصل می‌کند یا با استفاده از شبکه‌های عمومی و الزامات آن برای امنیت فن‌آوری اطلاعات رایانه را به یک شبکه دیگر متصل می‌کند. در این راستا به انواع مختلفی از دسترسی از راه دور از جمله پروتکل‌های مورد استفاده، بحث و بررسی مسایل تصدیق[1] مربوط به دسترسی از راه دور می‌پردازد و پشتیبانی دسترسی از راه دوری که به‌صورت امن برقرار شده را فراهم می‌نماید. دسترسی از راه دور کاندیدی است برای کمک به مدیران شبکه و متخصصان فنی که برنامه را با استفاده از این نوع ارتباط می‌سازند. تا بتوانند از این نوع ارتباط استفاده کنند یا کسانی که تا به حال از آن استفاده می‌کنند و نیازمند افزاره[2]ای در مورد چگونگی راه‌اندازی و به‌کار انداختن امن هستند.

۲ اصطلاحات و تعاریف و کوته‌نوشت‌ها

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۱-۲

نقطه دسترسی[3]

سامانه[4] دسترسی از یک شبکه بی‌سیم را به شبکه جهانی فراهم می‌نماید.

۲-۲

استاندارد رمزگذاری پیشرفته[5]

یک مکانیسم رمزگذاری متقارن با طول کلید متغیر که یک پیاده‌سازی کارآمد مشخص شده به‌عنوان استاندارد پردازش اطلاعات فدرال استاندارد ۱۹۷ [6] را فراهم می‌نماید.

۳-۲

تصدیق

حصول اطمینان از شناسه مورد ادعا از یک هستار[7] . در این مورد کاربران تصدیق به وسیله اطلاعاتی (به‌عنوان مثال رمز عبور) و نیز با در اختیار داشتن مجوزی (به‌عنوان مثال یک نشانه) و یا خصوصیات

1- Authentication
2- Device
3- Access Point (AP)
4- Sastem
5- Advanced Encryption Standard (AES)
6- Federal Information Processing Standard (FIPS
7- Entity

شخصی (خصوصیات بیومتریک[1]) شناسایی می‌شوند. تصدیق قوی بر پایه و اساس مکانیسم قوی (به عنوان مثال بیومتریک) یا استفاده حداقل دو مورد از این عوامل است (به اصطلاح تصدیق چند فاکتور نامیده می‌شود).

۴-۲

تماس معکوس[2]

مکانیسمی برای قراردادن یک تماس به یک مکان (و آدرس) از پیش تعریف شده یا پیشنهادی پس از دریافت پارامترهای شناسه معتبر می‌باشد.

۵-۲

پروتکل تصدیق رقابت- دست‌دادن[3]

یک پروتکل تصدیق سه روشه که در RFC[4] در سال ۱۹۹۴ میلادی معرفی شده است.

۶-۲

استاندارد رمزگذاری داده [5]

یک مکانیسم رمزگذاری متقارن معروف که با استفاده از یک کلید ۵۶ بیتی است. با توجه به طول کوتاه کلید، DES به وسیله استاندارد رمزگذاری پیشرفته[6] جایگزین شده است. اما هنوز هم در حالت‌های رمزگذاری متعدد به‌عنوان مثال در 3DES یا DES سه گانه (FIPS 46-3) استفاده می‌شود.

۷-۲

منطقه نظامی[7]

یک منطقه مجزا از یک شبکه محلی و یا شبکه‌ای می‌باشد و دسترسی به آن از طریق روش ویژه‌ای و با استفاده از فایروال[8] کنترل می‌شود. یک DMZ، بخشی از شبکه داخلی نیست و امنیت کمتری برای آن درنظر درنظر گرفته شده است.

۸-۲

عدم پذیرش یک خدمت[9]

حمله به سامانه برای جلوگیری از دسترس پذیری آن است.

1- Biometric
2- Call back
3- Challenge-Handshake Authentication Protocol (CHAP)
4- Request For Comment
5- Data Encryption Standard (DES)
6- Advanced Encryption Standard (AES)
7- De-militarised zone (DMZ)
8-Firewall
9-Denial Of Service (DOS)

۹-۲

خط اشتراک دیجیتال [۱]

یک فن‌آوری که امکان دسترسی سریع به شبکه‌ها را بر روی حلقه‌های ارتباط از راه دور محلی فراهم می‌نماید.

۱۰-۲

پروتکل کنترل هاست پویا [۲]

یک پروتکل اینترنت که به‌صورت پویا آدرس‌های پروتکل اینترنت[۳] را در آغاز کار فراهم می‌نماید. (RFC 2131)

۱۱-۲

کپسوله‌سازی بار مفید امنیتی [۴]

یک پروتکل مبتنی بر IP که خدمات محرمانه‌ای را برای داده فراهم می‌نماید. به‌طور خاص، ESP یک خدمت امنیتی را برای حفاظت از محتوای داده‌های بسته IP فراهم می‌کند. ESP یک استاندارد اینترنت است (RFC 2406).

۱۲-۲

پروتکل تصدیق توسعه‌پذیر [۵]

یک پروتکل تصدیق که توسط پروتکل خدمت کاربر شماره‌گیری دسترسی از راه دور [۶] پشتیبانی شده و توسط گروه موظف مهندسی اینترنت [۷] در RFC 2284 استانداردسازی شده است.

۱۳-۲

پروتکل انتقال فایل (FTP)[۸]

یک استاندارد اینترنت (RFC 959) برای انتقال فایل‌ها میان یک سرویس‌گیرنده و سرویس‌دهنده می‌باشد.

۱۴-۲

گروه موظف مهندسی اینترنت (IETF)

گروه مسئول برای پیشنهاد و توسعه استانداردهای فنی اینترنت است.

1- Digital ubscriber Line (DSL)
2- Dynamic Host Control Protocol (DHCP)
3- Internet Protocol (IP)
4- Encapsulating Security Payload (ESP)
5- Extensible Authentication Protocol (EAP)
۶- پروتکل RADIUS برگرفته شده از Remote Authentication Dial-In User Service، استانداردی برای طراحی و پیاده‌سازی سرویس‌دهندگانی است که مسئولیت تائید و مدیریت کاربران را برعهده خواهند گرفت.
7- Internet Engineering Task Force (IETF)
8- File Transfer Protocol (FTP)

۱۵-۲

پروتکل دسترسی پیام اینترنت نسخه ۴ [۱]

یک پروتکل پست الکترونیکی است که دسترسی و مدیریت پست‌های الکترونیکی و صندوق‌های پستی واقع در یک سرویس‌دهنده پست الکترونیکی از راه دور را فراهم می‌کند (در RFC 2060 تعریف شده است).

۱۶-۲

شبکه محلی [۲]

یک شبکه محلی که معمولاً درون یک ساختمان است.

۱۷-۲

مودم[۳]

سخت‌افزار یا نرم‌افزاری است که به‌منظور استفاده از پروتکل‌های تلفن به‌عنوان پروتکل رایانه، سیگنال‌های دیجیتالی را (برای کشف رمز) به آنالوگ و یا برعکس تبدیل می‌کند.

۱۸-۲

گسترش پست الکترونیکی اینترنت چند منظوره [۴]

روشی که انتقال داده چندرسانه‌ای و دودویی را از طریق پست الکترونیکی اجازه می‌دهد، این روش در RFC 2045 تا RFC 2049 تعیین شده است.

۱۹-۲

سرویس‌دهنده دسترسی شبکه [۵]

یک سامانه، به‌طور معمول رایانه‌ای است که دسترسی به زیرساخت‌ها را برای سرویس‌گیرندگان از راه دور، میسر می‌سازد.

۲۰-۲

رمز عبور یک‌بار مصرف [۶]

رمز عبوری که فقط یک بار در نتیجه مقابله با حملات پخش، استفاده می‌شود.

۲۱-۲

حالت غیرفعال [۷]

حالت برقراری ارتباط به FTP است.

1- Internet Message Access Protocol v4 (IMAP4)
2- Local Area Network (LAN)
3- Modem
4- Multipurpose Internet Mail Extensions (MIME)
5- Network Access Server (NAS)
6- One-Time Password (OTP)
7- PASsiVe (PASV)

۲۲-۲

پروتکل تصدیق کلمه عبور [1]

یک پروتکل تصدیق که برای پروتکل نقطه به نقطه فراهم شده است (RFC 1334).

۲۳-۲

دستیار دیجیتال شخصی [2]

به‌طور معمول یک رایانه جیبی است (رایانه palmtop).

۲۴-۲

پروتکل نقطه به نقطه [3]

یک روش استاندارد برای کپسوله اطلاعات مربوط به پروتکل لایه شبکه بر روی پیوندهای نقطه به نقطه است.

۲۵-۲

پروتکل اداره پست نسخه ۳ [4]

یک پروتکل پست الکترونیکی که در RFC 1939 تعریف شده است و اجازه می‌دهد تا سرویس گیرنده پست الکترونیکی، پست الکترونیکی ذخیره شده بر روی سرویس‌دهنده پست الکترونیکی را بازیابی نماید.

۲۶-۲

حفظ حریم شخصی کاربران[5]

یک برنامه نرم‌افزاری رمزنگاری در دسترس عمومی است که براساس رمزنگاری کلید عمومی می‌باشد. قالب پیام‌ها در RFC ۱۹۹۱ و RFC ۲۴۴۰ مشخص شده‌اند.

۲۷-۲

تبادل انشعاب خصوصی [6]

به طور معمول یک رایانه مبتنی بر سوئیچ تلفن که برای یک کار مهم سوئیچ می‌شود.

۲۸-۲

خدمت کاربر شماره‌گیری دسترسی از راه دور

یک پروتکل امنیت اینترنتی (RFC 2138 و RFC 2139) برای تصدیق کاربران از راه دور می‌باشد.

1- Password Authentication Protocol (PAP)
2- Personal Digital Assistant (PDA)
3- Point-to-Point Protocol (PPP)
4- Post Office Protocol v3 (POP3)
5- Pretty Good Privacy (PGP)
6- Private Branch Exchange (PBX)

۲۹-۲

خدمت دسترسی از راه دور[1]

به طور معمول نرم‌افزار و سخت‌افزار برای فراهم کردن دسترسی از راه دور است.

۳۰-۲

دسترسی از راه دور

منظور دسترسی مجاز به سامانه‌ای خارج از حوزه امنیتی می‌باشد.

۳۱-۲

درخواست برای توضیح

عنوانی برای استانداردهای اینترنت پیشنهاد شده توسط IETF می‌باشد.

۳۲-۲

عامل محافظ امن [2]

یک پروتکل در استفاده از شبکه‌های ناامن که ورود امن از راه دور را فراهم می‌کند. SSH اختصاصی است، اما به استاندارد IETF در آینده‌ای نزدیک تبدیل خواهد شد. SSH در اصل توسط ارتباطات SSH به‌صورت امن توسعه یافته است.

۳۳-۲

لایه‌های سوکت ایمن [3]

پروتکلی است که میان شبکه و لایه کاربرد واقع شده و تصدیق مشتریان و سرویس‌دهندگان و خدمات محرمانه‌بودن و یکپارچگی را فراهم می‌کند.

لایه‌های سوکت ایمن به‌وسیله نت اسکیپ[4] توسعه یافته و بر پایه پروتکل امنیت لایه انتقال ساخته شده است.

۳۴-۲

پیوست‌های پست الکترونیکی اینترنت چند منظوره امن [5]

پروتکلی است که تبادل امن پست الکترونیکی چند منظوره را فراهم می‌نماید. نسخه ۳، نسخه فعلی آن می‌باشد که شامل پنج بخش است. بخش‌های RFC 3369 و RFC 3370 نحو پیام را تعریف می‌کند، RFC 2631 تا RFC 2633 خصوصیات پیام، گواهی رسیدگی و روش توافق کلید را تعریف می‌کند.

1- Remote Access Service (RAS)

2- Secure Shell (SSH)

3- Secure Sockets Layer (SSL)

۴- مرورگر اینترنتی است و در دهه ۹۰ یکی از محبوب‌ترین مرورگرهای اینترنتی محسوب می‌شد.

5- Security/Multipurpose Internet Mail Extensions (S/MIME)

۳۵-۲

پروتکل اینترنت خط سریال [۱]

یک پروتکل قاب[۲] کردن بسته که در RFC 1055 تعیین شده و برای انتقال داده‌ها با استفاده از خطوط تلفن به‌کار می‌رود. (خطوط سریال)

۳۶-۲

شناسه مجموعه خدمت‌ها[۳]

شناسه‌ای برای نقاط دسترسی بی‌سیم، که معمولاً در شکل یک نام می‌باشد.

۳۷-۲

پروتکل انتقال پست الکترونیکی ساده [۴]

پروتکل اینترنت (RFC 821 و پیوست‌ها) برای ارسال پست الکترونیکی به سرویس‌ده‌ندگان پست الکترونیکی (خروجی) است.

۳۸-۲

پروتکل امنیت لایه انتقال [۵]

جانشین SSL که یک پروتکل رسمی اینترنت است (RFC 2246).

۳۹-۲

مکان‌یاب منبع یکنواخت [۶]

طرح آدرس برای خدمت‌های وب می‌باشد.

۴۰-۲

تامین برق اضطراری [۷]

معمولاً سامانه‌ای مبتنی بر باتری است که برای محافظت از افزاره‌ها در برابر قطع برق، خم‌شدگی و موج به‌کار می‌رود.

۴۱-۲

پروتکل داده‌های کاربر [۸]

پروتکل شبکه اینترنت برای ارتباطات بدون اتصال می‌باشد.

1- Security/Multipurpose Internet Mail Extensions (SLIP)
2- frame
3- Service Set Identifier (SSID)
4- Simple Mail Transfer Protocol (SMTP)
5- Transport Layer Security Protocol (TLS)
6- Uniform Resource Locator (URL)
7-Uninterruptible Power Supply (UPS)
8- User Datagram Protocol (UDP)

۴۲-۲

شبکه خصوصی مجازی [1]

یک شبکه خصوصی که از شبکه‌های به اشتراک گذاشته شده، استفاده می‌نماید. به‌عنوان مثال: یک شبکه مبتنی بر پروتکل تونل‌زنی رمزنگاری که بر روی زیرساخت‌های دیگر عمل می‌نماید.

۴۳-۲

دسترسی حفاظت شده WiFi [2]

خصوصیاتی برای افزایش امنیت که محرمانه بودن و یکپارچگی را برای ارتباطات بی‌سیم فراهم می‌کند. شامل پروتکل پیاده‌سازی کلید موقتی می‌باشد (TKIP). WPA جانشین WEP است.

۴۴-۲

حریم خصوصی معادل سیمی [3]

پروتکل محرمانه رمزنگاری cipher با طول کلید ۱۲۸ بیت را پیشنهاد می‌کند و در بخش مشخصات شبکه محلی بی‌سیم استاندارد IEEE تعریف شده است.

۴۵-۲

(WiFi) [4]

علامت تجاری ارائه شده توسط WiFi در ترویج استفاده از تجهیزات شبکه محلی بی‌سیم است.

۴۶-۲

شبکه محلی بی‌سیم [5]

یک شبکه با استفاده از فرکانس‌های رادیویی است. استانداردهای متداول و مورد استفاده، IEEE 802.11b و 802.11g به‌ترتیب با حداکثر نرخ انتقال ۱۱ مگابیت در ثانیه و ۵۴ مگابیت در ثانیه که از فرکانس با پهنای باند ۲/۴ گیگاهرتز استفاده می‌کند.

۳ هدف

این استاندارد برای راهنمای مدیران شبکه و متصدیان فن‌آوری اطلاعات در مواجهه با مشکلات تامین امنیت دسترسی از راه دور در نظر گرفته شده است. این برنامه اطلاعاتی در مورد انواع مختلف فنون برای دسترسی از راه دور فراهم می‌کند و کمک می‌کند تا مخاطب مورد نظر، اقدامات کافی برای محافظت از دسترسی از راه دور در برابر تهدیدات شناسایی شده را بشناسد.

همچنین ممکن است به کاربرانی کمک کند که قصد دسترسی از راه دور به دفتر خود یا به وقت مسافرت دارند.

1- Virtual Private Network (VPN)
2-WiFi Protected Access (WPA)
3- Wired Equivalent Privacy (WEP)
4- Wireless Fidelity
5- Wireless Fidelity Wireless LAN (WLAN)

۴ خلاصه

دسترسی از راه دور، کاربر را برای ورود از طریق یک رایانه محلی به رایانه از راه دور و یا شبکه رایانه‌ای قادر می‌سازد. امکان استفاده از منابع خود را فراهم می‌آورد گویی یک پیوند مستقیم شبکه محلی وجود دارد. خدمات مورد استفاده در اینجا به‌عنوان خدمت دسترسی از راه دور شناخته می‌شود (RAS). RAS تضمین می‌نماید که کاربران از راه دور می‌توانند به منابع شبکه دسترسی داشته باشند.

به‌طور کلی RAS در موارد زیر مورد استفاده قرار می‌گیرد:

الف- ارتباط به ایستگاه‌های کاری فرد ثابت (به‌عنوان مثال: به‌طوری که کارکنان فرد می‌توانند با رایانه‌ای از راه دور، در خانه کار کنند.)؛

ب- برای ارتباط به رایانه‌های همراه (به‌عنوان مثال: برای پشتیبانی از کارکنان مشغول به کار در این زمینه و یا در سفرهای تجارتی)؛

پ- ارتباط به تمام شبکه‌های محلی (به‌عنوان مثال: برای ارتباط به شبکه‌های محلی از مکان‌های از راه دور یا دفاتر شعبه به شرکت‌های بزرگ ستاد شبکه محلی)؛

ت- فراهم کردن مدیریت دسترسی به رایانه‌های از راه دور (به‌عنوان مثال: برای نگهداری از راه دور)

سناریوهایی RAS یک راه ساده برای ارتباط کاربران از راه دور ارائه می‌دهد از جمله: کاربر از راه دور یک اتصال با شبکه اصلی برقرار می‌کند به‌عنوان مثال: با استفاده از شبکه تلفن یا یک مودم. این ارتباط مستقیم ممکن است تا زمانی که لازم است، وجود داشته باشد و می‌تواند به‌عنوان یک خط استیجاری، که فقط در زمان نیاز، فعال است، مشاهده شود. همچنین ممکن است این اتصال زمانی که DSL یا سایر فن‌آوری‌های مناسب استفاده می‌شود دائمی باشد.

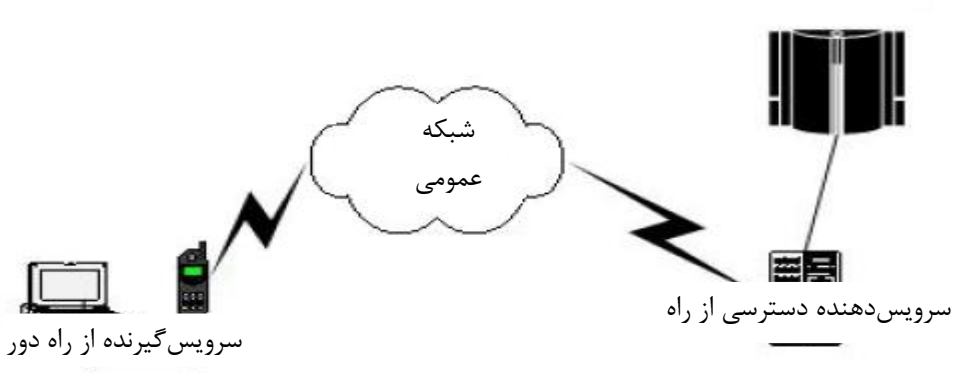
قابل توجه: دسترسی از راه دور به یک بنگاه اقتصادی باید همیشه از طریق یک سرویس‌دهنده دسترسی از راه دور هدایت شود، شماره‌گیری مستقیم به رایانه برابر با خطرات بسیاری است و در نتیجه باید حذف شود. در شرکت، مودم باید فقط در مکان‌های تعریف شده مورد استفاده قرار گیرد.

ایجاد یک ارتباط RAS به‌طور کلی نیاز به سه مؤلفه زیر دارد:

۱- مولفه‌های یک شبکه محلی در داخل شبکه شرکت‌ها، که RAS را فراهم می‌کند (به‌عنوان مثال: نرم‌افزار RAS نصب شده است) و آماده است تا ارتباطات RAS را قبول کند. این به‌عنوان سرویس‌دهنده RAS و سرویس‌دهنده دسترسی شناخته شده است.

۲- یک رایانه از راه دور که در آن نرم‌افزار RAS نصب شده است و ارتباط RAS آغاز به‌کار می‌کند. به‌عنوان سرویس‌گیرنده RAS شناخته شده است. مشتریان از راه دور ممکن است ایستگاه‌های کاری و یا رایانه‌های همراه باشند.

۳- رسانه بر روی ارتباط RAS ارتباطی برقرار می‌کند. در اکثر سناریوهای RAS، سرویس‌گیرنده برای برقراری ارتباط از یک شبکه ارتباط از راه دور استفاده می‌کند. حداقل یک خط تلفن و یک مودم برای ورود به آن مورد نیاز است بسته به نوع معماری RAS، فن‌آوری‌های متنوع ارتباط می‌توانند در سمت سرویس‌دهنده مورد استفاده قرار گیرد.



شکل ۱- دسترسی از راه دور به منابع

RAS به‌عنوان معماری سرویس‌گیرنده/سرویس‌دهنده اجرا می‌شود: یک سرویس‌گیرندهRAS ممکن است طوری پیکربندی شده باشد که به‌طور خودکار در زمان نیاز منابع شبکه شرکت‌های بزرگ، با شماره‌گیری شماره تلفن رایانه‌ای که در آن نرم‌افزار سرویس‌دهنده RAS نصب شده، اتصال RAS را برقرار کند.

به‌طور متناوب، کاربر می‌تواند اتصال RAS را به‌صورت دستی آغاز کند. برخی از سیستم عامل‌ها به RAS اجازه می‌دهند که بلافاصله اتصال به سامانه زیرین فعال شود. امکان دارد که یک سامانه سرویس‌گیرنده از هر نوع رایانه‌ای باشد. (به‌عنوان مثال، لپ تاپ، PDA، تلفن).

یک سامانه سرویس‌گیرنده پس از برقراری ارتباط، ممکن است از برنامه‌های کاربردی مختلفی استفاده کند، برخی از برنامه‌ها ممکن است پیامدهای امنیتی داشته باشد.

۵ الزامات امنیتی

از نقطه نظر امنیتی، سرویس‌دهنده و سرویس‌گیرنده RAS تحت کنترل یک خط‌مشی امنیتی داده شده، مورد نظر می‌باشد. درحالی‌که رسانه ارتباطی خارج از کنترل و احتمالاً در محیط رقیب مورد نظر است. مکانیسم‌های امنیتی بر روی خطراتی که از جانب اشخاص غیرمجاز است، تمرکز می‌کنند. (مثلاً افراد یا فرآیندها) ممکن است:

الف- دسترسی به سرویس‌گیرنده RAS را به‌دست آورند.

ب- دسترسی به سرویس‌دهنده RAS را به‌دست آورند.

پ- دسترسی بلوک به سرویس‌دهنده RAS (عدم پذیرش خدمت) باشد.

ت- استراق سمع اطلاعات مبادله شده میان سرویس‌گیرنده و سرویس‌دهنده RAS باشد.

ث- تغییر اطلاعات مبادله شده باشد.

از جمله خدمت‌های امنیتی برای مقابله با این خطرات، خدمات محرمانه بودن، خدمات تصدیق و کنترل دسترسی هستند. بنابراین، اهداف امنیتی زیر در دستیابی به RAS اعمال می‌شوند:

تصدیق: کاربر از راه دور باید به‌طور منحصربه‌فردی توسط سامانه RAS شناخته شده باشد. هویت کاربر باید از طریق یک مکانیسم تصدیق در هر برقراری ارتباط با شبکه محلی انجام شود. در زمینه دسترسی به سامانه،

مکانیسم‌های کنترل اضافی باید استفاده شوند تا اطمینان حاصل شود که دسترسی به سامانه توسط کاربران از راه دور به درستی کنترل می‌شود (به‌عنوان مثال: محدود کردن دسترسی به زمان‌های خاص و یا فقط به نقاط ارتباط از راه دور مجاز).

روش‌های مختلفی برای تصدیق کاربران و فرآیندهای متفاوت در کیفیت و فن‌آوری وجود دارد. شایع‌ترین، بلکه آسیب‌پذیرترین روش، استفاده از کلمات عبور است.

کنترل دسترسی: هنگامی که کاربر از راه دور تصدیق شده است، سرویس‌دهنده دسترسی از راه دور باید قادر به محدود کردن تعامل کاربر با شبکه باشد. این مستلزم مجوزها و محدودیت‌هایی است که برای منابع شبکه محلی توسط مدیران مجاز تعیین شده است، همچنین اجرای این روش‌ها برای کاربران از راه دور به‌علاوه هر گونه محدودیت‌های خاص برای کاربران از راه دور وجود دارد. (به‌عنوان مثال: دوره خاصی در طول روز، یک ارتباط برای هر کاربر).

امنیت ارتباطات: جایی‌که منابع محلی از راه دور در دسترس قرار می‌گیرند، بر روی ارتباط برقرار شده RAS، داده‌های کاربر نیز منتقل می‌شود. به‌طورکلی الزامات امنیتی، که در شبکه محلی با توجه به حفاظت از ارتباطات اعمال می‌شوند (محرمانه بودن، جامعیت، اعتبار) نیز باید برای انتقال داده‌ها از روی ارتباطات RAS قابل پیاده‌سازی باشند.

با این حال، حفاظت از ارتباطات RAS به‌ویژه ارتباطات بحرانی را می‌توان با استفاده از تعدادی از رسانه‌ها و پروتکل‌های ارتباطی منتقل کرد، که به‌طور کلی نمی‌توان تحت کنترل اپراتور شبکه محلی تصور کرد.

دسترس‌پذیری: دسترسی از راه دور برای جریان اصلی فعالیت‌های تجارت استفاده می‌شود، فراهم بودن دسترسی به RAS بسیار مهم است. ممکن است جریان روان از فرآیندهای تجارت در صورت شکست، کل دسترسی به RAS یا در صورتی‌که ارتباطات دارای پهنای باند ناکافی باشند، مختل شود. این خطر می‌تواند تا حدودی در زمینه خاصی از طریق استفاده از ارتباطات RAS جایگزین یا اضافی کاهش یابد. این امر به‌خصوص در مکانی اتفاق می‌افتد که در آن از اینترنت به‌عنوان ابزار ارتباطی استفاده می‌شود. در اینجا به‌طور کلی برای هر ارتباط یا پهنای باند هیچ ضمانتی وجود ندارد.

معماری سرویس‌گیرنده/سرویس‌دهنده سامانه‌های RAS به این معنی است که هر دو سرویس‌گیرنده و سرویس‌دهنده RAS با توجه به نوع محیط عملیاتی و نحوه استفاده، در معرض خطرات خاصی هستند.

مشتریان RAS مجبور نیستند که ثابت باشند (به‌عنوان مثال: رایانه خانگی)، اما همچنین ممکن است افزاره‌های همراه باشند (به‌عنوان مثال: لپ‌تاپ). با این حال، محل مشتری به‌طور معمول تحت کنترل هیچ اپراتور شبکه نمی‌باشد، خصوصاً در جایی‌که مشتری متحرک باشد، باید فرض کرد که محیط ناامن و به‌ویژه در معرض تهدید است. به‌طور خاص تهدیداتی که باید اینجا در نظر گرفته شوند، عبارتند از: تهدیدات فیزیکی از قبیل دزدی و آسیب.

سرویس‌دهندگان RAS به‌طورکلی بخشی از شبکه محلی هستند که کاربران از راه دور مایل به ورود به آن هستند. آن‌ها تحت کنترل اپراتور شبکه هستند و بنابراین می‌توانند با مقررات امنیتی، مطابق با درخواست محلی پوشیده شوند. وظیفه اصلی سرویس‌دهنده RAS حصول اطمینان از این موضوع است که تنها کاربران

مجاز متصل به شبکه می‌توانند به آن دسترسی داشته باشند، تهدید به سرویس‌دهنده RAS شامل افتادن آن در داخل منطقه‌ای از حملات است که در آن هدف، دسترسی‌های غیرمجاز به شبکه محلی است.

۶ انواع ارتباطات دسترسی از راه دور

راه‌های مختلفی برای ایجاد ارتباط میان مشتری و رایانه در شبکه محلی از راه دور وجود دارد:

الف- شماره‌گیری مستقیم برای دسترسی به سرویس‌ده.

ب- شماره‌گیری برای دسترسی به فراهم کننده سرویس‌ده خدمات اینترنتی و دسترسی به یک شبکه محلی از راه دور بر روی اینترنت.

پ- دسترسی بدون شماره‌گیری به‌وسیله ارتباطات دائمی خود به شبکه دیگر.

شکل ۲ این نوع ارتباطات از راه دور را نشان می‌دهد، کاربر متحرک ۲ از طریق ISP و اینترنت و توسط یک فایروال که کنترل دسترسی را میان اینترنت و شبکه محلی فیلتر شده را دارد، به شبکه دسترسی دارد. کاربر متحرک ۱ نیز می‌تواند یک کاربر WLAN باشد و پس از آن RAS، نقطه دسترسی (AP) نامیده می‌شود. این دسترسی به سرویس‌دهنده نیز توسط فایروال کنترل (خط نقطه‌دار) کنترل می‌شود.

یادآوری- کاربران متحرک ممکن است از شماره‌گیری، خط استیجاری، پهنای باند و یا ارتباط بی‌سیم استفاده کنند.

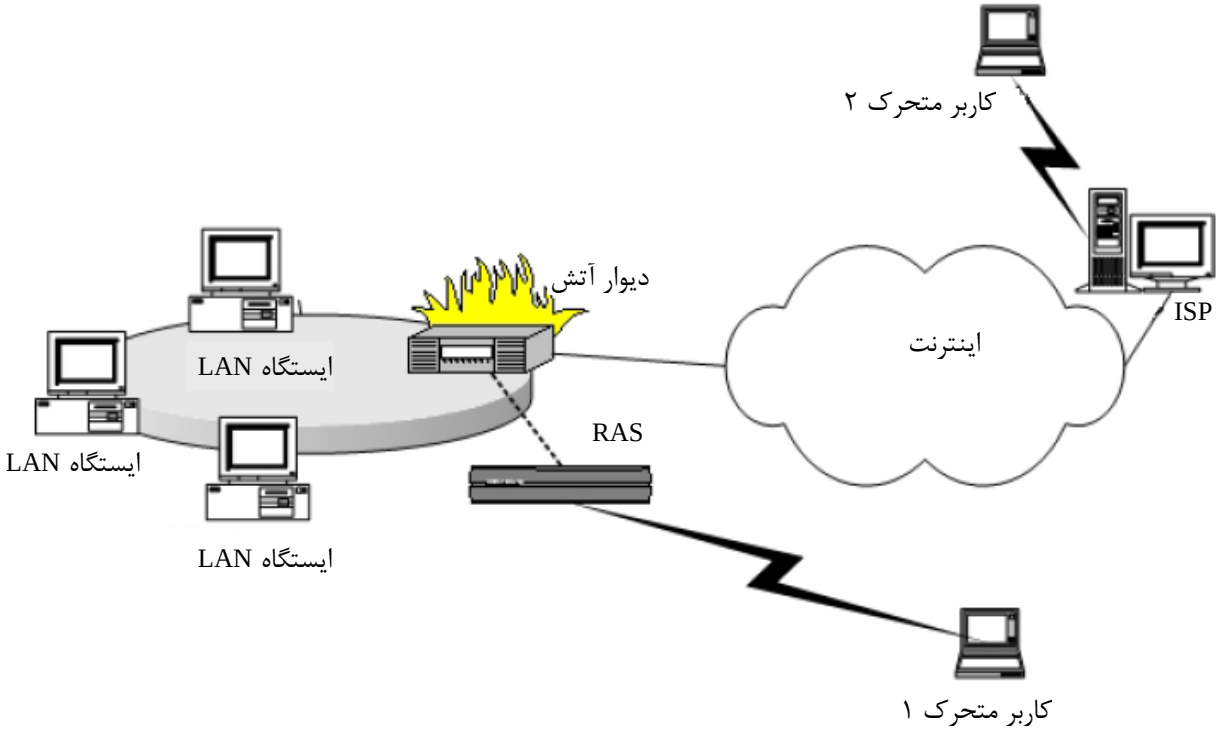
وضعیت با اصطلاح "نقاط حساس[1] WLAN " از طریق دستیابی کاربر متحرک ۲ به نقطه دسترسی WLAN به‌جای استفاده از یک مودم محلی توصیف می‌شود. این بدان معنی است که دسترسی به اینترنت به‌طور کلی از طریق WLAN AP و یک فراهم‌کننده سرویس‌ده اینترنت فراهم می‌شود.

روش‌های متنوعی برای استفاده مشتری به‌منظور ارتباط به ISP وجود دارد. ممکن است مشتری از فن‌آوری‌های سیمی و/ یا بی‌سیم استفاده نماید. بسته به نوع روش مورد استفاده، خطرات اضافی ممکن است رخ دهد، به‌عنوان مثال: WLAN نیاز دارد به‌منظور حفظ محرمانه بودن، اقدامات امنیتی خاصی اعمال کند.

این روش‌ها شامل جوانب مثبت و منفی خاصی هستند که باید به حساب آیند. به‌عنوان مثال: شماره‌گیری مستقیم مد نظر باشد تا اطمینان حاصل شود که تنها کاربران مجاز، شماره دسترسی به شبکه از راه دور را می‌دانند. با این حال، ابزار اسکن برای اعداد شماره قابل دسترسی (وار دایلینگ[2]) به هکرها برای شناسایی مودم‌های موجود فعال در انتظار برای تماس‌های دریافتی کمک می‌کنند. اینترنتی که از شماره گیری استفاده می‌کند در هر مکالمه یک مزیت برای کاربر از راه دور فراهم می‌کند.کاربر ممکن است برای ارتباط با شبکه محلی از راه دور به شرکت‌های محلی مربوطه دسترسی داشته باشد. با این حال این روش ارتباط ممکن است نیاز به سرویس‌دهنده پیچیده و گرانی برای تنظیم و پیکربندی داشته باشد.

1- Hot spots

2- War dialers



شکل ۲- انواع دسترسی از راه دور

۷ فنون ارتباط دسترسی از راه دور

۷-۱ کلیات

دسترسی از راه دور تنها باید تحت نیاز دانستن اصول ارائه شود. بنابراین، یک بنگاه اقتصادی مجبور است تعیین کند، که سامانه‌ها و برنامه‌های کاربردی خارج از محیط باید توسط کدام کاربر در دسترس باشند. نوع دسترسی از راه دور باید توسط خدمت از راه دوری که استفاده می‌شود، تعریف شود.

۷-۲ دسترسی به خدمت‌های ارتباطی

۷-۲-۱ محافظت از ارتباطات کلی

رایج‌ترین دسترسی، دسترسی به خدمات ارتباطات درون سازمانی است، یعنی دسترسی به یک حساب پست الکترونیکی کاربر، به یک سرویس‌ده FTP و یا یک سرویس‌ده وب. پیوست ت فهرست بررسی بر روی پیاده-سازی و بهره‌برداری از یک سرویس‌ده پست الکترونیکی امن فراهم می‌کند و پیوست ث در راه‌اندازی و اداره یک سرویس‌ده وب به‌صورت امن کمک می‌کند.

راه‌های مختلفی برای محافظت از ارتباطات میان سرویس‌دهنده و سرویس‌گیرنده وجود دارد، بنابراین اصالت، محرمانه بودن و جامعیت خدمت‌ها ارائه شود. مانند:

الف- لایه سوکت ایمن روشی برای تصدیق طرفین ارتباط (تصدیق سرویس‌دهنده و سرویس‌گیرنده) و تبادل اطلاعات میان آن‌ها را رمزنگاری می‌نماید. لایه سوکت ایمن به‌وسیله هر مرورگر وب و تقریباً توسط تمام سیستم عامل‌ها پشتیبانی می‌شود. گروه موظف مهندسی اینترنت (IETF) به‌وسیله پروتکل امنیت لایه

انتقال (TLS) توسعه یافته است که براساس SSL به‌عنوان استاندارد اینترنت (RFC 2246) برای حفاظت از ارتباطات سرویس گیرنده/سرویس دهنده است.

ب- امنیت پروتکل اینترنت (IPsec) راه‌های تصدیق طرفین ارتباط و همچنین حفاظت از اطلاعات منتقل شده را فراهم می‌نماید. همچنین IPsec توابعی برای مقابله با مسائل مربوط به مدیریت کلید ارائه می‌دهد (به RFC 2401 معماری امنیتی برای پروتکل اینترنت مراجعه کنید).

پ- پوسته امن (SSH) یک پروتکل برای ورود امن از راه دور و سایر خدمات شبکه امن بر روی شبکه‌های نا امن است. پوسته امن یک پیوند ارتباطی امن را پس از تصدیق موفق کاربر از راه دور برقرار می‌کند و مجموعه‌ای از دستورات و خدمت‌ها را فراهم می‌کند. (به‌عنوان مثال: انتقال امن فایل).

این روش‌ها، تصدیق امن و خدمت‌های محرمانه بودن و جامعیت را فراهم می‌نماید و به‌علاوه باید در نرم‌افزار ارتباطات استفاده شوند. با توجه به این واقعیت که SSL بخش مشترک موجود در مرورگرهای اینترنت است دسترسی به رایانامه مبتنی بر وب ممکن است به‌راحتی با ایجاد یک ارتباط SSL قبل از دسترسی به حساب رایانامه کاربر به‌صورت کاملاً محافظت شده، انجام شود.

تفاوت عمده میان روش‌ها در این واقعیت نهفته است که SSL/TLS و IPsec معمولاً به‌عنوان ویژگی‌های ارتباطات زیربنایی آماده هستند بنابراین امنیت شبکه خدمت و SSH در گرو امنیت برنامه کاربردی است.

این فنون نیز برای ارتباط یک سرویس‌گیرنده FTP به سرویس‌دهنده FTP قابل اجرا است در نتیجه دسترسی به داده‌های ذخیره شده در آن سرویس‌دهنده را اجازه می‌دهد.

یادآوری- بسیاری از پروتکل‌های اینترنتی، به‌عنوان مثال: شبکه راه دور که قابلیت‌های دسترسی به پایانه را فراهم می‌کند و یا FTP انتقال فایل، تنها انجام پیاده‌سازی مکانیسم‌های تصدیق‌های ضعیف، و به‌طور معمول ارسال اطلاعات رمز عبور در متن واضح را اجازه می‌دهد. تونل‌زنی از جمله پروتکل‌ها از طریق پروتکل‌های امن مانند SSH، SSL/TLS و یا IPsec نه تنها محرمانه بودن بلکه بهبود قابل توجه برای فرایند تصدیق را فراهم می‌کند.

توجه داشته باشید که بسیاری از سرویس‌دهنده‌های وب که از SSL/TLS استفاده می‌کنند تنها تصدیق سرویس‌دهنده برای کاربر را فراهم می‌کند اما بالعکس آن را انجام نمی‌دهند بلکه نیاز است تا کاربر گواهینامه سرویس‌دهنده را بررسی نماید.

۷-۲-۲ محافظت از پست الکترونیکی

اگرچه پست الکترونیکی، خدمتی است که به‌طور کلی پیام رسانی قابل اطمینان را فراهم نمی‌کند ولی مطابق با پیش‌نیازهای خاص و به اجبار دسترسی به سرویس‌دهنده‌های پست الکترونیکی را از خارج اجازه می‌دهد. راه مشترک برای فراهم کردن دسترسی به یک سرویس‌دهنده پست الکترونیکی، فراهم کردن یک رابط وب به حساب‌های پست الکترونیکی است، که به کاربران در جاده‌ها دسترسی به پست الکترونیکی خود را اجازه می‌دهد. این روش تنها نیاز به یک رایانه به همراه یک مرورگر دارد، یعنی ممکن است بر روی هر رایانه موجود استفاده شود. از سوی دیگر، در این روش به کاربران اجازه دانلود پست الکترونیکی خود و پاسخ به آن در زمان آفلاین در نظر گرفته نشده است.

سایر روش‌ها به کاربران استفاده از سرویس‌گیرنده‌های پست الکترونیکی استاندارد خود را اجازه می‌دهد اما هنوز هم به اندازه کافی محرمانه بودن و حفظ حریم خصوصی با توجه به مفهوم پروتکل‌های پست الکترونیکی فراهم نیست. به‌طور کلی، سرویس‌گیرنده پست الکترونیکی به یک دفتر پست (به‌عنوان مثال اداره برنامه رایج تمام حساب‌های پست‌های الکترونیکی دریافتی) با تصدیق خود و کاربر بعد از متن واضح دسترسی پیدا می‌کند. دو پروتکل اصلی دسترسی پست الکترونیکی استفاده می‌شوند (POP3 و IMAP4) در درجه اول این پروتکل‌ها در روش متفاوتی با پست‌های الکترونیکی دریافتی برخورد می‌کنند.

۱- پروتکل POP3 تمام پست‌های الکترونیکی در دسترس را دانلود کرده و کاربر می‌تواند به‌صورت محلی با آن کار کند.

۲- پروتکل IMAP4 اجازه می‌دهد تا کاربر فقط هدر[1] رایانامه‌های خود را دانلود کند و پس از آن به دانلود رایانامه به دستگاه‌های محلی را تصمیم بگیرد.

باید به این واقعیت توجه کرد که این پروتکل‌ها به‌تنهایی مکانیسم‌های امنیتی کافی، تصدیق قوی و قابل اطمینان بودن انتقال را که باید به‌صورت اضافی ارائه شود، فراهم نمی‌کند.

یادآوری- شما نیز ممکن است از محتویات پست الکترونیکی محافظت کنید (این محافظت شامل آدرس فرستنده، آدرس گیرنده و خط موضوع نمی‌شود). این دو مشخصه اصلی عبارتند از: PGP (حفظ حریم خصوصی بسیار خوب) و S/MIME (تبادل اطلاعات چندمنظوره امن) که خدمات قابل اطمینان بودن، جامعیت، اصالت و عدم انکار از مبدا را فراهم می‌نماید هر دو اینها می‌توانند به‌صورت مناسبی در بسیاری از برنامه‌های سرویس‌دهنده پست الکترونیکی، یکپارچه شوند. اما هیچ‌یک به دلیل اینکه فرستنده و گیرنده آدرس در متن واضح منتقل می‌شوند، در برابر تحلیل ترافیک محافظت نمی‌کنند.

یک سرویس‌دهنده پست الکترونیکی در دسترس کاربران راه دور باید در منطقه نظامی(DMZ) یک شبکه واقع شده باشد. وظیفه DMZ است تا شبکه خارجی را با شبکه داخلی با ایزوله کردن رایانه‌هایی که به‌صورت مستقیم توسط هر شبکه‌ای دسترسی دارند، جدا کند. قرار دادن سرویس‌دهنده پست الکترونیکی داخل یک DMZ به این معنی است که این دستگاه قابل دسترس در شبکه‌های خارجی و شبکه داخلی است. برای اجتناب از این کار که باعث ایجاد خطر برای شبکه‌های داخلی است، باید اقدامات خاصی در نظر گرفته شود. به‌طور کلی باید از ارتباط آنلاین میان یک رایانه از شبکه‌های خارجی با رایانه دیگر در شبکه داخلی که از طریق DMZ می‌تواند ایجاد شود، اجتناب کرد. این عمل را می‌توان یا با استفاده از پیکربندی دروازه‌های مربوطه و رایانه میانی مطابق با آن و یا با استفاده از گروهی از رایانه‌ها به‌دست آورد که این نوع جداسازی را فراهم می‌کند.

پیکربندی مناسب نیازمند مراقبت از مسائل زیر است:

الف- سرویس‌دهنده پست الکترونیکی باید فقط میزبان یک نرم‌افزار خاص یا یک سیستم عامل کمینه باشد تا از سوءاستفاده ماشین میانی برای حمله جلوگیری کند.

ب- دسترسی خارج از شبکه به برنامه‌های کاربردی دقیقاً تعریف شده، باید محدود شود (به‌وسیله آدرس IP و شماره پورت شناسایی شود).

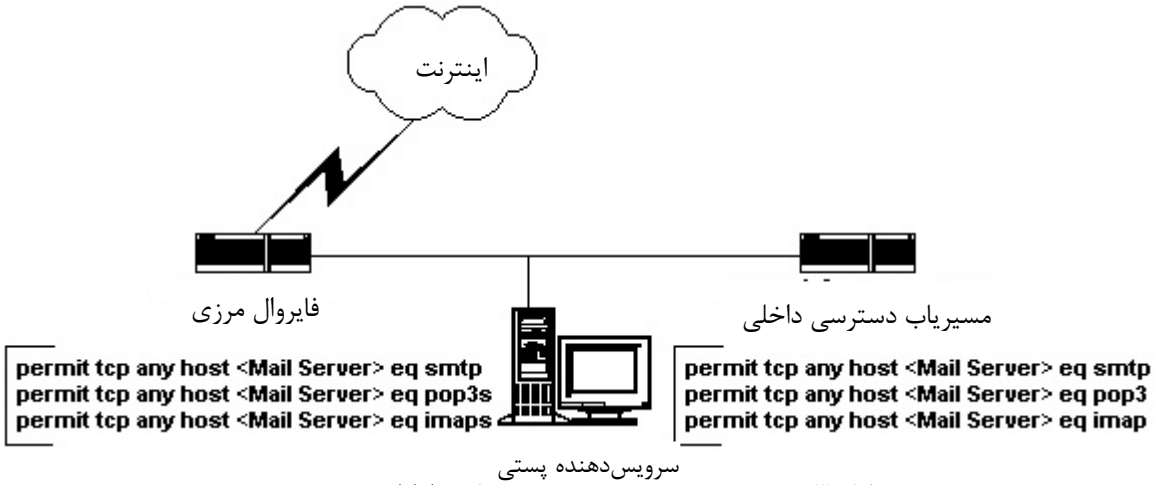
1- Header

پ- دسترسی از شبکه‌های داخلی نیز باید از طریق آدرس‌های تعریف‌شده و پورت برای آدرس‌های منابع (آن دسته از رایانه‌ها که برای دسترسی در شبکه داخلی اجازه دارند) و همچنین برای آدرس مقصد و نیز برای جریان اطلاعات محدود شود. این محدود کردن را می‌توان توسط فایروال یا مسیریاب به‌دست آورد.
خدمت‌های ارتباطی دیگری مانند سرویس‌دهنده وب ممکن است درون یک DMZ قرار داشته باشد و بر این اساس از آن محافظت شود. جدول ۱شماره پورت و پروتکل‌هایی را فراهم می‌کند که ممکن است هنگام قرار دادن یک سرویس‌دهنده پست الکترونیکی در DMZ در نظر گرفته شود.

جدول ۱ – شماره پورت‌های مربوطه و پست الکترونیکی

شماره	نام	توضیحات
۲۲	ssh	ورود از طریق پوسته امن
۲۵	smtp	پروتکل smtp متعارف با قابلیت TLS/SSL
۴۶۵	smtps	Smtp بر روی TLS/SSL
۱۴۳	imap	پورت imap متعارف
۹۹۳	imaps	پورت imap بر روی TLS/SSL
۱۱۰	pop3	پورت pop3 متعارف
۹۹۵	pop3s	پورت pop3 بر روی TLS/SSL

شکل ۳ پیکربندی‌های مختلف مورد نیاز را بر روی مسیریابی که در اینترنت و شبکه داخلی قرار دارد نشان می‌دهد. در این صورت، دسترسی از خارج به سرویس‌دهنده پست الکترونیکی تنها از طریق IMAP بر روی SSL/ TLS و POP بر روی SSL/TLS اجازه داده می‌شود در هنگام ارسال پست الکترونیکی ممکن است با استفاده از SMTP طبیعی انجام شود. از داخل شبکه، دسترسی با استفاده از IMAP یا POP بدون پشتیبانی‌های اضافی توسط TLS/SSL اجازه داده می‌شود. این دستورات یک شبه زبان توصیف فهرست دستورات دسترسی مورد نیاز برای فایروال مرزی و مسیریاب داخلی است.
به‌وسیله تعریف، هر پورت دیگر برای اجتناب از نقاط ضعف مربوط به پورت‌ها و پروتکل‌های دیگر منع شده است.
امکان دارد تدابیر حفاظتی دیگری برای جلوگیری از سوءاستفاده از سرویس‌دهنده رایانامه SMTP اعمال شود (به‌عنوان مثال محدود کردن ارتباطات SMTP برای جلوگیری از پست‌های الکترونیکی ناخواسته)



شکل ۳- دسترسی به سرویس‌دهنده یک رایانامه درون DMZ

۳-۲-۷ محافظت از یک ارتباط [1]

پروتکل انتقال فایل خدمت دیگری است که امکان دارد در داخل DMZ قرار گرفته باشد. FTP در دو حالت عملیاتی مشخص شده است:

الف- حالت PORT (همچنین به‌عنوان حالت طبیعی یا فعال شناخته شده است)

ب- حالت PASV (همچنین به‌عنوان حالت غیرفعال شناخته شده است)

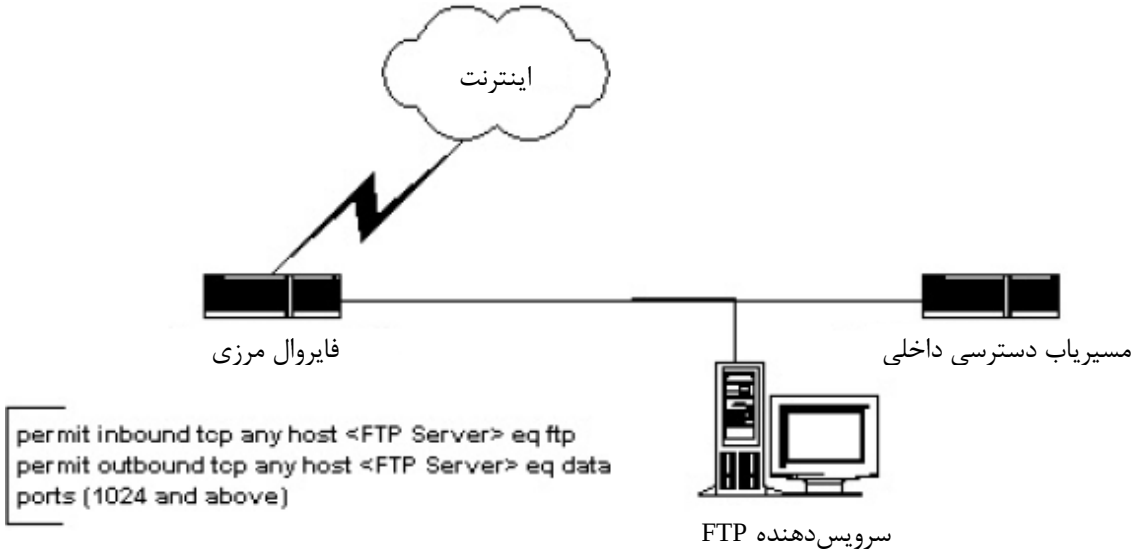
این حالت‌ها در ایجاد کانال داده‌ها متفاوت هستند: در حالت PASV کانال فرمان و کانال داده توسط سرویس گیرنده FTP با دسترسی به سرویس‌دهنده FTP برقرار می‌شوند و در حالت PORT، سرویس‌گیرنده FTP یک کانال فرمان باز می‌کند و بعد از آن سرویس‌دهنده FTP هنگامی‌که درخواست مشتری را پذیرش می‌کند کانال داده‌ها را باز می‌کند. FTP با استفاده از پورت ۲۱ برای ساخت کانال فرمان مشخص شده است، برای پورت کانال داده به‌صورت پویا به‌طور معمول از محدوده پورت ۱۰۲۴ تا پورت ۵۰۰۰ اختصاص داده شده است.

اصولاً حالت PORT راه‌اندازی امن‌تری از یک فایروال فیلترینگ بسته در زمان ارائه قابلیت‌های FTP به مشتریان از راه دور را اجازه می‌دهد. فقط پورت TCP 21 نیار دارد تا برای راه‌اندازی کانال فرمان مشتری تازه وارد شده به‌صورت محدود باز شود. سپس استقرار زیرین کانال داده برای باند بیرونی باز است. شکل ۴ فیلتر کردن کافی برای DMZی که حاوی یک سرویس‌دهنده FTP است، نشان می‌دهد.

در مقابل پیاده‌سازی یک سرویس‌دهنده FTP با استفاده از ارتباطات حالت PASV به فایروال ساده برای باز کردن از محدوده پورت گسترده شروع شده از پورت ۱۰۲۴ برای ارتباط با ارتباطات دریافتی نیاز دارد. چنین راه‌اندازی موجب خطرهای خود فایروال می‌شود.

متاسفانه، حالت PORT نمی‌تواند در ترکیب با تبدیل آدرس شبکه در فایروال به‌دلیل ایجاد کانال داده‌ها مجزا استفاده شود. حالت PASV بر این محدودیت‌ها غلبه می‌کند، چرا که همه کانال توسط سامانه سرویس‌دهنده آغاز به‌کار کرده است.

1- File Transfer Protocol (FTP)



شکل ۴- دسترسی به یک سرویس‌دهنده یک FTP درون یک DMZ

خطرات ضمنی در باز کردن این طیف گسترده از پورت‌ها می‌تواند با اجرای فنون پیچیده‌تر فایروال حل شود: فایروال‌ها با فراهم کردن کامل فنون بازرسی، مجوز تقاضای پورت‌های ورودی به‌طور موقت، مجوز ارائه خدمات FTP حالت PASV بدون نیاز به طیف گسترده‌ای از پورت‌های باز ورودی را فراهم می‌کنند. نتیجه یکسان می‌تواند با استفاده از اختصاص یک جزء پروکسی FTP در فایروال فراهم شود.

زمانی‌که با توجه به فراهم کردن قابلیت‌های FTP به سرویس‌گیرندگان از راه دور مهم است که به یاد داشته باشید که پروتکل FTP خود تنها، فراهم‌کننده اقدامات بسیار اساسی امنیت است. محرمانگی پشتیبانی نمی‌شود و خدمت‌های تصدیق در سطح بسیار ابتدایی فراهم می‌شوند. به‌عنوان مثال: کلمات عبور در متن واضح منتقل می‌شوند که حملات Reply را اجازه می‌دهد.

بنابراین، خدمت‌های FTP باید در هر زمانی که ممکن باشد در ترکیب با پروتکل‌های تونل‌زنی لایه امنیت زیرین اجرا شود (به‌عنوان مثال: TLS/SLS)، و یا برنامه‌های کاربردی انتقال فایل مانند FTP امن یا SCP (کپی امن) هر دو را بر اساس پروتکل SSH بهبود دهد. هر دو گونه‌های مختلف اجرای قوی تصدیق و همچنین ارائه خدمات محرمانه را اجازه می‌دهد.

۳-۷ دسترسی به منابع LAN

این دسترسی نیاز به راه‌اندازی ماشین آلات و پیکربندی سامانه خاص دارد. با توجه به این واقعیت است که یک کاربر از راه دور با دسترسی به منابع در داخل یک شبکه، خطری بالا را به این شبکه تحمیل می‌کند، دسترسی از راه دور مجبور است تا الزامات زیر را برطرف کند:

تصدیق: یک مکانیسم قوی تصدیق و یا دو عامل تصدیق برای اطمینان از شناسایی یک کاربر از راه دور تصدیق شده است.

مجوز: بعد از تصدیق موفق، یک کاربر از راه دور می‌تواند به آن دسته از حقوق مسلم که او را به‌انجام کار تعریف شده خود اجازه می‌دهد، دست یابد. به این ترتیب، کاربر نقش کاربر از راه دور خاص را بازی می‌کند.

کنترل دسترسی: قبل از دسترسی به منابع یا داده‌ها، دسترسی یک کاربر از راه دور در برابر حقوق اعطا شده خود، بررسی شده است.

محرمانه بودن، صحت و یکپارچگی: با توجه به منابع و داده‌هایی که استفاده می‌شوند، ایمنی ارتباطات باید با ارائه خدمات محرمانه بودن، صحت و یکپارچگی برقرار شود.

این الزامات توسط پروتکل تونل‌زنی امن برآورده خواهد شد که در استفاده برای شبکه‌های خصوصی مجازی از جمله مکانیسم‌های تصدیق مناسب است. برای جزییات بیشتر ب استاندارد ISO/IEC 18028-5 رجوع کنید (شبکه‌های خصوصی مجازی).

مکانیسم‌های تصدیق مناسب برای کاربران از راه دور به‌عنوان مثال: کلمه عبور تک زمانی(OTP) نشانه‌ای است که یک کلمه عبور منحصر به‌فرد در هر زمان را فراهم می‌دهد که قابل دسترسی توسط کاربری است که شماره شناسایی شخصی خود را (PIN) وارد می‌کند. نشانه‌هایی مانند این دو عامل، تصدیق را فراهم می‌کنند که در آن یک کاربر هم باید یک نشانه داشته باشد و هم اینکه PIN مناسب را بداند.

اصالت ممکن است توسط نقش‌های خاصی که امکان دارد به گروهی از کاربران از راه دور اختصاص داده شود، نصب شود. یک گروه باید آن دسته از حقوق مسلم که ملزم به انجام وظایف آن‌ها در حالت از راه دور هستند را دریافت کنند. به این ترتیب دسترسی محدود برای کاربران از راه دور به‌راحتی می‌تواند اجرا شود.

کنترل دسترسی ممکن است با یک خط‌مشی پشتیبانی شده توسط مکانیسم‌های فراهم شده از سیستم عامل‌های مربوطه مورد استفاده، اجرا شود. به‌عنوان مثال، خط‌مشی حساب کاربری ممکن است حقوق و محدودیت‌های مورد نیاز را ایجاد کند. همچنین امکان دارد سیستم عامل خط مشی‌های گروهی را فراهم کند به‌طور خاص آن‌ها را برای کاربران از راه دور توسعه دهد.

رایج‌ترین مجموعه از پروتکل‌هایی که استفاده می‌شود با RADIUS، فراهم می‌شود. این پروتکل‌ها، در اصل تنها برای شماره‌گیری دسترسی از راه دور توسعه یافته‌اند، که تصدیق، مجوز و حسابداری متمرکز را برای دسترسی به شبکه قادر می‌سازند و توسط VPN و مکانیسم‌های تصدیق قوی پشتیبانی می‌شوند. پروتکل‌ها به‌صورت زیر کار می‌کنند:

یک سرویس‌گیرنده RADIUS (معمولاً سرویس‌دهنده دسترسی از قبیل سرویس‌دهنده شماره‌گیری، سرویس‌دهنده VPN، و یا نقطه دسترسی بی‌سیم) اعتبار کاربر و اطلاعات پارامتر ارتباط را در شکل یک پیام RADIUS به یک سرویس‌دهنده RADIUS می‌فرستد. سرویس‌دهنده ADIUS اعتبار می‌بخشد و مجوز درخواست سرویس گیرنده RADIUS را می‌دهد، و پیام RADIUS را در پاسخ می‌فرستد. مشتری RADIUS همچنین پیام حسابداری RADIUS را به سرویس‌دهنده‌های RADIUS ارسال می‌کند. علاوه‌براین، استانداردهای RADIUS استفاده از پروکسی RADIUS را پشتیبانی می‌کند. یک پروکسی RADIUS یک رایانه است که احتمالاً پیام‌های میان سرویس‌گیرندگان و سرویس‌دهندگان RADIUS را از طریق پروکسی RADIUS دیگر ارسال می‌کند. پیام‌های RADIUS میان سرویس‌گیرنده و سرویس‌دهنده دسترسی هرگز ارسال نشده است.

پیام‌های RADIUS به‌عنوان پیام‌های پروتکل داده کاربر (UDP) فرستاده می‌شوند. پورت UDP1812 برای پیام‌های تصدیق RADIUS استفاده می‌شود و پورت UDP1813 برای پیام‌های حسابداری RADIUS مورد

استفاده قرار می‌گیرد. فقط یک پیام RADIUS در اجناس مقرون به‌صرفه برای انتقال UDP یک بسته RADIUS گنجانده شده است.

در RFC 2865 انواع پیام‌های RADIUS زیر تعریف می‌شود:

درخواست دسترسی: توسط مشتری RADIUS برای درخواست تصدیق و مجوز به یک شبکه برای دسترسی به ارتباط فرستاده می‌شود.

قبول دسترسی: در پاسخ به پیام درخواست دسترسی توسط سرویس‌دهنده RADIUS ارسال می‌شود. این پیام به اطلاع مشتری RADIUS که اقدام به ارتباط معتبر و مجاز کرده‌است، می‌رسد.

رد دسترسی: در پاسخ به پیام درخواست دسترسی توسط سرویس‌دهنده RADIUS ارسال می‌شود. این پیام به اطلاع مشتری RADIUS که اقدام به رد ارتباط کرده است می‌رسد. سرویس‌دهنده RADIUS این پیام را که اعتبارنامه به‌صورت معتبر نیست و یا اقدامات ارتباط به‌صورت مجاز نیست، را ارسال می‌کند.

رقابت دسترسی: در پاسخ به پیام دسترسی توسط سرویس‌دهنده RADIUS ارسال می‌شود. این پیام یک رقابت به سرویس‌گیرنده RADIUS است که نیاز به پاسخ دارد.

پیوست ب پشتیبانی از پیاده‌سازی و استقرار RADIUS در درون محیط ویندوز مایکروسافت۲۰۰۰ را فراهم می‌کند.

۴-۷ دسترسی برای نگهداری

این نوع دسترسی از راه دور برای ارتباط مدیران سامانه در زمانی که به اداره سامانه‌های از راه دور نیاز است، فراهم شده است. با توجه به این واقعیت، این گروه از کاربران معمولاً بالاترین حقوق دسترسی در سامانه را دارند، دسترسی باید در امن‌ترین راه برقرار شود. همچنین، هر نوع فعالیت انجام‌شده از راه دور باید وارد سامانه شود و پس از آن رسیدگی شود، به‌ویژه هنگامی که مدیریت سامانه به یک فراهم‌کننده خدمات برون سپاری می‌شود.

بنابراین، دسترسی تنها باید با یک رایانه خاص که از راه دور اداره می‌شود فراهم شود. اقدامات زیر لازم است:

۱- دسترسی باید فقط از طریق یک حساب خاصی که بر روی دستگاه تعریف شده فراهم شود.

۲- ارتباط میان کاربر از راه دور و دستگاهی که اداره می‌شود باید با استفاده از ابزاری مانند SSH محافظت شود.

۳- کاربر باید با استفاده از مکانیسم‌های تأیید تصدیق شود.

۴- هر کاربر مجاز برای اداره یک سامانه از راه دور، باید در روش‌ها ومکانیسم‌های مناسب آموزش ببینند.

۵- هر گونه اقدام باید به سامانه وارد شود.

۶- ورودی‌ها باید بلافاصله پس از یک مدیریت از راه دوری که هدایت شده، یا در اولین فرصت در مورد فعالیت‌های نگهداری خارج از ساعت رسیدگی شوند.

مکانیسم بازگشتی (نیاز به حفاظ‌های اضافی، همچنین بند ۲-۸) یک گزینه است. به‌دنبال این الزامات خطرات ضمنی با این نوع دسترسی از راه دور محدود می‌شوند.

۸ راهنمای عملکرد برای انتخاب و پیکربندی

۸-۱ کلیات

بند زیر در مورد اقدامات لازم برای مقابله با تهدیدهای شناسایی‌شده، بحث می‌کند. هر اقدام پیشنهادی، جزئیات و جوانب مثبت و منفی را معرفی خواهد کرد. ساختار طوری است که مناطق سرویس‌گیرنده و سرویس‌دهنده و ارتباطات RAS به‌طور جداگانه معرفی خواهد شد. اقدامات مشترک در پایان، بحث خواهند شد.

در این مرحله، ما به ملاحظه تهدیدات به سرویس‌گیرنده و سرویس‌دهنده به‌طور کامل و به‌صورت جداگانه می‌پردازیم، به‌عنوان مثال، اگر یک سرویس گیرنده RAS به‌خطر بیافتد، سرویس‌دهنده RAS به‌صورت خودکار در معرض خطر قرار می‌گیرد.

علاوه‌برآن باید به خاطر سپرد که به‌عنوان مثال در محیط ویندوز، هر سرویس‌گیرنده RAS همچنین می‌تواند به‌عنوان یک سرویس‌دهنده RAS عمل کند، به‌طوری که تهدیدهایی که به سرویس‌دهنده RAS اعمال می‌شود به همان اندازه ممکن است به سرویس‌گیرنده نیز RAS اعمال شود.

۸-۲ محافظت از سرویس‌گیرنده RAS

۸-۲-۱ سرویس‌گیرنده RAS ثابت

ممکن است یک سرویس گیرنده ثابت برای اولین بار از لحاظ فیزیکی محافظت شود، یعنی امکان دارد در اتاقی نگهداشته شود که تنها افراد مجاز می‌توانند به آنجا دسترسی داشته باشند. ممکن است این یک رویکرد مناسب برای دور کار[1] که از یک دفتر خانه استفاده می‌کنند، باشد.

یک سرویس گیرنده RAS ثابت ممکن است با استفاده از یک مودم تلفنی، مودم‌های کابلی و یا ارتباط DSL به سرویس‌دهنده RAS متصل شود. نوع دوم و سوم از ارتباط نیاز به اقدامات اضافی برای پهنای باند برای یک ارتباط دائمی به اینترنت دارند. یک روش ساده نصب و راه‌اندازی درست، به‌اصطلاح "فایروال شخصی" است که دسترسی از خارج به رایانه متصل را محدود می‌کند.

۸-۲-۲ تمام سرویس‌گیرندگان RAS

برای تمام سرویس‌گیرندگان RAS سطوح مختلفی از امنیت قابل اجرا برای جلوگیری از سوء استفاده از رایانه و ایمن‌سازی ارتباط از راه دور وجود دارد.

اولین مانعی که به‌وجود می‌آید سخت افزار خود رایانه است. یک روش آسان برای محافظت از رایانه و جلوگیری از سوءاستفاده، نصب یک رمز عبور بوت است، که شناسایی کاربر را قبل از بوت شدن سامانه اجرا می‌کند. این سد اولین مانع برای حملات بالقوه است، اما این کار ایمنی کافی را فراهم نمی‌کند. مانع دوم، سیستم عامل است. برای رایانه‌های قابل حمل و ایستگاه‌های کاری، باید سیستم عاملی مورد استفاده قرارگیرد که شناسایی و تصدیق کاربر را فراهم نماید. اکثر سیستم عامل‌ها این ویژگی را فراهم می‌کنند. حساب مورد استفاده باید یک حساب کاربری عادی باشد، نه یک حساب مدیر، زیرا این حساب امتیازات بیشتری فراهم می‌نماید و بنابراین تنها باید برای مدیریت یک رایانه مورد استفاده باشد. همچنین به یاد داشته باشید که به کیفیت کافی رمز عبور باید تاکید شود.

1- Telecommuter

اگر اطلاعات ذخیره شده بر روی یارانه با ارزش باشد پس باید تمهیدات بیشتری در محل انجام شود.
سیستم عامل باید اقدامات امنیتی بیشتری را نسبت به پیش‌فرض انجام دهد. لذا بهتر است تمام اجزای غیرضروری از سیستم عامل حذف شده و فقط آن دسته از برنامه‌هایی که مورد نیاز هستند، نصب شود. همچنین، ویژگی‌هایی مانند تنظیمات شبکه طوری محدود شود که فقط آن دسته از خدمات مورد نیاز برای آن سامانه خاص، مجاز است.
تصدیق قوی می‌تواند با استفاده از کارت‌های هوشمند، کارت‌های نشانه یا مکانیسم بیومتریک به‌دست آیند. تصدیق قوی همچنین به‌عنوان دو یا چند عامل تصدیق شناخته می‌شود که برای تحقق حداقل دو روش شناسایی، نیاز دارد.
محافظت رمزگذاری دیسک سخت در مقابل افشای اطلاعات ذخیره شده را فراهم می‌کند. این خدمات محرمانه باید از الگوریتم‌های قوی استفاده کنند. (همچنین به استاندارد ISO/IEC 18033-3، مراجعه کنید).
یکی‌دیگر از مسائل مهم پیکربندی، تنظیمات مودم است. مودم سرویس‌گیرنده باید به گونه‌ای تنظیم شود که به‌طور کلی تماس‌های دریافتی را قبول نمی‌کند. به این ترتیب باید یک ارتباط توسط کاربر سرویس‌گیرنده آغاز شود.
در بسیاری از شرایط یک فایروال شخصی ممکن است در صورتی امنیت را بهبود می‌بخشد که به‌درستی پیکربندی شده باشد.
در نهایت، برای جلوگیری و محدود کردن خسارات ناشی از کدهای مخرب، باید برنامه ضدویروس نصب شده و به‌طور مرتب بروز شود.

۸-۳ حفاظت از سرویس‌دهنده RAS

۸-۳-۱ تنظیم فیزیکی و منطقی

امنیت فیزیکی سرویس‌دهنده RAS، یک ضرورت است. معمولاً، سرویس‌دهنده RAS بخشی از زیرساخت‌های سرویس‌دهنده یک سازمان است و باید امنیت فیزیکی همان سرویس‌دهنده‌های دیگر را داشته باشد. مانند هر خدمت دیگر به خارج، یک سرویس‌دهنده RAS باید درون یک DMZ واقع شده باشد. این کار شامل حفاظت در برابر دسترسی فیزیکی غیرمجاز به‌وسیله نگه‌داشتن آن به‌صورت قفل‌شده در یک اتاق سرویس‌دهنده و حفاظت در برابر قطع برق با استفاده از UPS است. دیگر اقدامات لازم، تنظیم کردن امن و پیکربندی سرویس‌دهنده RAS، مدیریت امن و تهیه پشتیبان و روش‌های بازیابی است.
اگرچه شایع‌ترین نوع از سرویس‌دهنده RAS، هنوز یک سرویس‌دهنده دسترسی را از طریق مودم یا با استفاده از خط تلفن و یا ISDN فراهم می‌نماید، اما در عین حال در حال حاضر راه‌حل‌هایی وجود دارد که در آن شماره‌گیری در خدمات محلی فراهم کننده RAS در خارج از کنترل سازمان اتفاق می‌افتد. دسترسی بیشتر سپس توسط اینترنت فراهم شده است و کنترل و محدود شده توسط پیرامون آن، سامانه فایروال است.
مزیت این روش این است که هزینه‌ها پایین نگه‌داشته می‌شوند (معمولاً شماره‌گیری در تلفن محلی)، ضرر این است که مشتری باید دو بار شناسایی شود: اولین بار توسط ISP و سپس دوباره در مکان از راه دور.

۸-۳-۲ سرویس‌دهنده و مودم RAS

برای یک سرویس‌دهنده RAS فراهم کردن اقدامات دسترسی چندگانه به مودم باید در مکانی باشد که اطمینان حاصل شود که ارائه مودم خطرات اضافی را به زیرساخت مطرح نمی‌کند.

رایانه باید پیکربندی شود تا وظیفه ارائه خدمات RAS را به‌انجام برساند و همه خدمات دیگر باید حذف شوند. این بدان معنی است که سیستم عامل سخت شده است و همه ارتقاها و تعمیرات مربوطه اعمال شده‌اند. فقط برای مدیران و کارکنان نگهداری، اجازه دسترسی به سرویس‌دهنده فیزیکی وجود دارد. حساب‌های کاربر عادی نباید نصب شده باشد.

درصورتی‌که سرویس‌دهنده RAS نیز سایر خدمات را فراهم کند پس باید آزمون شده و تصدیق شود که ترکیبی از خدمات، خطرات جدید را معرفی نمی‌کند. پشتیبانی از پیکربندی صریح برای RAS ممکن است توسط فروشنده این نرم‌افزار فراهم شود.

دیگر مسائل مهم در حساب کاربری باید در تهیه پشتیبان از داده‌ها در نظر گرفته شود، از جمله اطلاعات فایل‌های ورود به سامانه جمع‌آوری شود، انتقال فایل‌های ورود به سامانه مربوط به ایستگاه مدیریت (از جمله ارزیابی روزانه خود) و توسعه طرح‌های فوق العاده.

پیش از فعالیت فراهم‌کردن خدمات دسترسی از راه دور، سرویس‌دهنده باید در برابر آسیب‌پذیری‌های شناخته‌شده مورد آزمون قرار گیرد. آزمون‌ها باید شامل پیکربندی‌های محلی و آزمون نفوذ شبکه باشد.

مودم باید پیکربندی شود تا به‌صورت انفعالی در یک جهت کار کند، در این مورد، به تماس‌های ورودی اجازه داده می‌شود. در صورت امکان، پیکربندی باید تصدیق در مودم را اجازه دهد و پس از آن تماس دوباره را شروع کند (همچنین به‌عنوان شماره‌گیری دوباره شناخته می‌شود) تا به تعداد از پیش ذخیره شود. این تماس دوباره فقط با مشتریان ثابت و یا لپ‌تاپ‌هایی که از طریق تلفن‌های همراه متصل می‌شوند، کار می‌کنند. این امر تضمین می‌کند که تنها آدرس‌های شناخته شده (شماره تلفن) متصل شده‌اند و محدود کردن هزینه برای هستار فراخوانی را اجازه می‌دهد.

تجهیزات مدرن تلفن (به‌عنوان مثال: PBX) ویژگی‌هایی مانند مسیریابی مجدد از تماس‌هایی که ممکن است تماس را به تعدادی دیگر از انتخاب‌ها هدایت کند را فراهم می‌کند. بنابراین، مکانیسم‌های تماس دوباره نیاز دارد تا حمایت‌های اضافی را تامین کند.

به‌عنوان پیشنهاد برای تنظیم سرویس‌گیرنده، باید یک برنامه ضد ویروس نصب و به‌صورت منظم بروز شود.

۸-۳-۳ سرویس‌دهنده دسترسی

اگر دسترسی از راه دور راه‌اندازی شده است به‌طوری که شماره‌گیری در یک فراهم‌کننده خدمات محلی اینترنت (ISP) جهت دسترسی به شبکه صورت گیرد، باید توسط یک سرویس‌دهنده دسترسی شبکه (NAS) کنترل شود. سپس دسترسی به ISP خارج از کنترل مستقیم شرکت خواهد شد و نتیجه هرگونه تصدیق که وجود دارد به این شرکت شناخته نمی‌شود.

NAS به‌مانند هر دستگاه شبکه‌ای دیگر باید محافظت شود، یعنی باید به‌طور پیوسته به صورت قفل شده نگه داشته شود تا فقط مدیران مجاز به آن دسترسی فیزیکی داشته باشند. مدیریت دستگاه باید با خط‌مشی

محلی فراهم شود، اگر یک سامانه مدیریت شبکه، بر فعالیت خود پایش کند پس از آن ترافیک میان مدیریت سامانه وNAS است که باید چه در شبکه محلی چه در تونل برای مخفی کردن نوع اطلاعات خود نگه داشته شود.

NAS نوعی دروازه میان شبکه سازمانی محلی و جهان خارج است، بنابراین مکانیسم‌های پیشنهادی در استاندارد ISO/ IEC 18028-3 باید استفاده شوند.

۸-۳-۴ نقطه دسترسی بی‌سیم

اگرچه نقاط دسترسی برای شبکه محلی بی‌سیم نوعی سناریو دسترسی از راه دور نیستند اما ممکن است در فراهم کردن دسترسی به یک شبکه مورد استفاده قرار گیرند. بنابراین از جمله AP، به‌عنوان نقاط دسترسی برای سایر فنون بی‌سیم، باید در DMZ قرار گیرد و به این ترتیب از آن محافظت شود. اطلاعات اضافی در مورد امنیت بی سیم در بند ۵-۸ ارائه شده است.

۸-۴ حفاظت از ارتباط

۸-۴-۱ کلیات

ارتباط میان سرویس‌گیرنده و سرویس‌دهنده RAS از طریق تعدادی مراحلی حرکت می‌کند. در ابتدا ارتباط برقرار می‌شود، سپس وارد عمل خواهد شد و بعد استفاده از آن فسخ خواهد شد. همه مراحل برقراری ارتباط نیاز به حفاظت دارد.

بند زیر به مراحل مختلف ارتباط امن به‌ترتیب ارتباط میان سرویس‌گیرنده و سرویس‌دهنده RAS متمرکز می‌شود.

۸-۴-۲ برقراری ارتباط

ایجاد ارتباط امن نیاز به تصدیق کاربر از راه دور دارد. این مورد هنگامی‌که پروتکل مورد استفاده برای دسترسی از راه دور راه‌اندازی شده، اتفاق می‌افتد.

راه‌های مختلفی برای تصدیق کاربر، که از لحاظ امنیتی نیز متفاوت هستند، وجود دارد. دو پروتکل اول در میان یک سرویس‌گیرنده(peer) و سرویس‌دهنده (دهنده اعتبار) استفاده می‌شوند پروتکل سوم توسط سرویس‌دهنده تصدیق استفاده می‌شود، که وارد شدن طرح‌های تصدیق اضافی را اجازه می‌دهد.

شایع‌ترین طرح تصدیق از پروتکل تصدیق رمز عبور(PAP) استفاده می‌کند. PAP پروتکل دست دادن دو طرفه است که در آن یک دهنده تصدیق (سرویس‌دهنده) دریافت اعتبار از peer (سرویس‌گیرنده) است و براساس این مدارک اجازه دسترسی را داده یا منع می‌کند. اعتبارنامه‌ها را در متن واضح فرستاده و معمولاً شامل شناسه کاربری و رمز عبور است. بنابراین این پروتکل حفاظت در برابر حملات، Reply را فراهم نمی‌کند.

طرح تصدیق بهتر، توسط پروتکل دست‌دادن-رقابت پیشنهاد شده است. CHAP یک پروتکل دست دادن سه راهه است، که در آن تصدیق یک چالش به جفت خود ارسال می‌کند. این چالش منحصربه‌فرد است و باید هر زمان که یک چالش فرستاده شد، تغییر داده شود. جفت با یک مقدار hash محاسبه‌شده بر روی پارامترهای شناسه خود (به‌اصطلاح "رمز") به "چالش" پاسخ می‌دهد. تصدیق کننده نتیجه را با محاسبات

خود مقایسه می‌کند و به‌دسترسی اجازه می‌دهد یا منع می‌کند. اعتبارنامه‌های منتقل شده با استفاده از الگوریتم hash رمزگذاری شده‌اند (اغلب MD5 مورد استفاده قرار می‌گیرند). CHAP در برابر حملات پاسخ برای چالش‌های غیرقابل پیش‌بینی محافظت می‌نماید.

رویکرد کلی‌تر با خدمات کاربر شماره‌گیری تصدیق (RADIUS)[1] مانند آنچه که در بند ۷-۳ معرفی شده، فراهم گردیده است.

سرویس‌دهنده RADIUS معمولاً پارامترهای کاربران را به‌صورت متمرکز ذخیره می‌کند. به‌عنوان مثال اسرار مشترک برای کاربران از راه دور را نگه می‌دارد. در صورتی که کاربری بخواهد به یک سامانه در شبکه دسترسی داشته باشد، یک درخواست دسترسی به سرویس‌دهنده RADIUS شناسه کاربر، رمز عبور، شناسه سامانه و پورت سامانه کاربر در دسترسی می‌فرستد. هنگامی‌که یک رمز عبور وجود داشته باشد با استفاده از ابزار رمزنگاری پوشانده می‌شود. سرویس‌دهنده RADIUS ممکن است یا به درخواست پاسخ دهد یا آن را به سرویس‌دهنده RADIUS دیگر ارسال کند. اگر سرویس‌دهنده به درخواست پاسخ دهد، به‌دلیل اینکه انتقال داده‌ها معتبر هستند برای اولین بار بررسی می‌شود. شناسایی معتبر حداقل باید شامل شناسه کاربری و رمزعبور باشد اما ممکن است شامل آدرس سامانه و پورت ارائه شده نیز باشد. اگر یک درخواست به سرویس‌دهنده RADIUS دیگر فرستاده شود در اصل بعد از آن محل سرویس‌دهنده RADIUS به‌عنوان یک سرویس‌گیرنده عمل می‌کند. به این ترتیب تصدیق اضافی ممکن است به اجرا گذاشته شود. مثال‌ها: تصدیق سیستم‌عامل UNIX، ویندوز ۲۰۰۰ یا تصدیق NOVELL هستند. همچنین سرویس‌دهنده RADIUS ممکن است در طرح تصدیق PAP و CHAP استفاده شود.

تصدیق قوی دیگری که مورد استفاده قرار می‌گیرد ممکن است تصدیق با استفاده از گواهینامه‌های دیجیتال و یا با استفاده از نشانه صورت پذیرد. این روش تصدیق تنها متکی بر دانش کاربر نیست، بلکه دارای یک نشانه و یا گواهی است. بنابراین این‌ها دو فاکتور تصدیق نامیده می‌شوند. امکان دارد تصدیق بیومتریک نیز شامل شود.

یادآوری- شبکه قدیمی‌تر سامانه کنترل دسترسی کنترل‌کننده دسترسی ترمینال (TACACS) و مشتقات آن XTACACS و TACACS هنوز هم وجود دارند اما به اندازه RADIUS نقش مهمی را ایفا نمی‌کنند.

۸-۴-۳ رمزنگاری ارتباطات

تهدید استراق سمع تنها می‌تواند با استفاده از رمزنگاری مقابله شود. رمزگذاری پیوند ارتباطات را به آن دسته از امکاناتی که در آن تجهیزات رمزنگاری مناسب فراهم شده است، محدود می‌کند. رمزگذاری محتوا انعطاف‌پذیری بیشتری را فراهم کرده و همچنین ارتباط به سرویس‌دهنده‌ها را اجازه می‌دهد، که رمزنگاری را ارائه نمی‌کند. همچنین این محرمانه بودن را فقط میان رمزگذاری نقاط انتهایی مربوطه فراهم می‌نماید.

به‌عنوان مثال استفاده از نرم‌افزار مانند حفظ اسرار خیلی خوب (PGP)، یک بسته نرم‌افزار برای رمزگذاری محتوا است که رمزنگاری مبتنی بر رمزنگاری کلید عمومی را فراهم می‌کند در نتیجه خدماتی مانند عدم انکار و اعتبار را اجازه می‌دهد.

1- Authentication Dial-in User Service

مهم : در هنگام استفاده از یک برنامه رمزنگاری، اطمینان حاصل کنید که طول کلید مورد استفاده کافی است. همچنین، روش‌های تعریف به‌منظور بررسی صحت و اعتبار گواهی‌های کلید عمومی را قبل از وارد کردن و استفاده از آن‌ها از طریق پست الکترونیکی دریافت کنید.

برای دسترسی از راه دور، راه‌های کافی برای محافظت از محتویات یک ارتباط با استفاده از شبکه‌های خصوصی مجازی فراهم‌شده (VPN) وجود دارد. تعدادی از محصولات موجود هستند که این نوع حفاظت را فراهم می‌کنند. اطمینان حاصل کنید که که فقط پروتکل‌های استاندارد برای VPN استفاده شود. راهنمایی در مورد این موضوع در آینده یک استاندارد بین المللی ارائه می‌دهد (استاندارد ISO/IEC 18028-5).

۸-۵ امنیت بی‌سیم

پروتکل‌های بی‌سیم ممکن است در سناریوهای مختلف در منطقه دسترسی از راه دور استفاده شوند:

الف- پروتکلی مانند بلوتوث به‌این دلیل استفاده می‌شود تا به‌صورت محلی تلفن‌های همراه، مودم و یا مؤلفه‌های دسترسی به اینترنت پرسرعت مورد نظر را جهت دسترسی سرویس‌گیرنده از راه دور یک سامانه ارتباط دهند.

ب- پروتکل‌های LAN بی‌سیم از جمله پروتکل‌های تعریف‌شده در IEEE 802.11 مجموعه‌ای از استانداردهایی هستند که ممکن است در ارتباط سامانه‌های دسترسی از راه دور مشتری به شبکه‌های عمومی یا خصوصی مورد استفاده قرار گیرد.

در بسیاری از این سناریوها، سازمان قابلیت‌های دسترسی از راه دور را یا فقط به‌صورت نفوذ بسیار محدود در پیکربندی و یا راه‌اندازی پروتکل‌های ارتباطات بی‌سیم درگیر فراهم می‌کند.

به‌عنوان مثال: یک کاربر تلفن همراه ممکن است با استفاده از تسهیلات دسترسی شبکه‌های بی‌سیم عمومی (به اصطلاح نقطه حساس) فراهم‌شده در فرودگاه، از راه دور به سامانه سرویس‌گیرنده دسترسی ارتباط یابد. زیرساخت‌های دسترسی بی‌سیم در این مثال به‌طور معمول به‌وسیله ISPها و کاربران یا سازمان خود، به‌کار افتاده‌اند که هیچ تاثیری روی مسائل پیکربندی ندارد.

اگرچه پروتکل‌های بی‌سیم برخی از خدمت‌های امنیتی را فراهم می‌کنند، اما این نمی‌تواند در محتوای سناریو در منطقه دسترسی از راه دور قابل اعتماد باشد.

بنابراین درصورتی‌که پروتکل‌های بی‌سیم مجاز به پیاده‌سازی قابلیت‌های دسترسی از راه دور در ارتباط باشند، تمام خدمت‌های امنیتی موردنیاز مانند تصدیق یا محرمانه بودن باید با استفاده از قابلیت‌های پروتکل‌های سطح بالاتر که در زیربند ۸-۳ معرفی شده‌اند، اجرا شوند. یک رویکرد مشترک با استفاده از پروتکل تونل مانند IPSEC یا SSL/TLS، تصدیق قوی و محرمانه بودن را فراهم می‌کند.

در چنین وضعیتی است که در آن یک سازمان می‌تواند اقدامات فنی اضافی زیرساخت‌های دسترسی بی‌سیم مورد نیاز را برای تضمین نقطه دسترسی پیکربندی کند. در حال حاضر سه روش اساسی برای ایمنی دسترسی به یک AP که در داخل پروتکل‌های IEEE 802.11 ساخته شده است، وجود دارد.

الف- شناسه مجموعه خدمات (SSID)؛

ب- کنترل دسترسی رسانه (MAC) فیلتر کردن آدرس؛

پ- حریم خصوصی معادل سیمی (WEP) و یا دسترسی حفاظت‌شده WiFi (WPA)؛
حتی امکان دارد همه این سه روش امنیت کافی را برای سازمان فراهم نکنند.
SSID مکانیسمی را فراهم می‌کند تا شبکه‌های بی‌سیم به چند شبکه تقسیم‌بندی شده که توسط یک یا چند AP ارائه خدمات می‌دهند. هر نقطه دسترسی همراه با SSID پیش فرض تولید کننده، تولید کننده آن AP و اطلاعات بالقوه دیگر AP مربوطه را شامل می‌شود. بنابراین، SSID باید به سطح درونی تغییر نماید تا به‌راحتی SSID قابل حدس نباشد و اطلاعاتی در مورد عملکرد سازمان نه برای AP و نه بر روی تجهیزات خود فراهم نکند. حداقل امنیت مورد نیاز برای یک AP، منع پخش SSID آن است، در غیر این‌صورت هر افزاره شنوایی می‌تواند SSID را ضبط کند و برای ارتباط به AP در تماس صحیح SSID سعی کند. بنابراین، به‌شدت توصیه می‌شود که APها با حالت پخش غیرفعال پیکربندی شوند، اگرچه هنوز هم راهی برای ضبط SSID وجود دارد که پخش نمی‌شود.
یک آدرس MAC، رابط شبکه‌ای یک رایانه را شناسایی می‌کند در حالی‌که SSID یک AP را مشخص می‌کند، هر کارت رابط شبکه دارای آدرس MAC منحصربه‌فرد است. برای افزایش امنیت WLAN، در صورت امکان، AP باید رایانه‌های سرویس‌گیرنده معتبر توسط آدرس MACشان شناسایی نماید. اگرچه کلاه‌برداری از آدرس‌های MAC امکان‌پذیر است، اما این برخی از حفاظت‌ها به دسترسی به WLAN، را اضافه می‌کند.
WEP به داشتن آسیب‌پذیری‌های اساسی که بر محرمانه بودن، صداقت و اصالت تاثیر می‌گذارد، شناخته شده‌است.
با این حال، با استفاده از یک کلید مشترک که هر کدام ۴۰ یا ۱۰۴ بیت هستند، رمزگذاری را برای ارتباطات فراهم می‌کند. این کلید با یک بردار با مقداردهی اولیه ۲۴ بیت الحاق شده است، در نتیجه با طول کلید ۶۴ و یا ۱۲۸ بیت است. با توجه به شناخت نقاط ضعف پروتکل‌ها، کلیدهای WEP باید به‌صورت مکرر تغییر کنند، در نتیجه امنیت افزایش می‌یابد. WPA جانشین WEP درصورتی‌که به‌درستی با ارائه کلیدهای مشترک آتی پیکربندی شده باشد، بر این ضعف غلبه می‌کند.
علاوه‌براین، استفاده از پروتکل پیکربندی میزبان پویا (DHCP) توسط AP ویژگی رزرو سرویس‌گیرنده را فراهم می‌کند (آدرس MAC رایانه به آدرس IP تعریف شده محدود می‌شود) و یا آدرس ایستا توصیه می‌شود.
در صورت استفاده از آدرس‌های IP غیرقابل دستیابی، آدرس زیر شبکه IP داخلی (معمولاً 192.168.0.0) به آدرس دیگری از زیر شبکه تغییر می‌کند. همچنین، منع دسترسی بی‌سیم اجرایی به WAP و مسیریاب بی‌سیم منجر به اجتناب از اصلاحات توسط مهاجمان می‌شود.
در نهایت، وضعیت WLAN بر پایه نظم و قاعده ارزیابی می‌شود.
فهرست بررسی‌ها با جزئیاتی در مورد امنیت WLAN در پیوست ج فراهم شده است.

۸-۶ اقدامات سازمانی

اقدامات سازمانی باید شامل خط‌مشی‌های دسترسی از راه دور باشد، که نقش‌های مختلف کاربران، مدیران و کارکنان امنیتی را تعریف می‌کند. همچنین، مسئولیت‌های افراد درگیر، تعریف شده است. اطلاعات بیشتر در

مورد یک خط‌مشی شبکه مناسب (از جمله دسترسی از راه دور) در استاندارد ISO/IEC 18028-1 آمده است. مثال‌هایی برای خط‌مشی‌های دسترسی از راه دور در پیوست الف آمده است.

برای برخی از افزاره‌های تلفن همراه (به‌عنوان مثال، PDA ، تلفن هوشمند) پیاده‌سازی محافظت فنی کافی، امکان‌پذیر نیست. بنابراین ممکن است نیاز به اقدامات سازمانی بیشتری برای مقابله با خطرات موجود باشد.

مباحث دیگر تحت پوشش اقدامات سازمانی طرح‌های احتمالی، پشتیبان‌گیری، بازیابی، آموزش کارکنان، آگاهی کاربر و آموزش کاربر هستند.

اطلاعات بیشتر در مورد این موضوعات در استانداردهای ISO/IEC 13335 و ISO/IEC 17799 یافت می‌شود.

۸-۷ ملاحظات حقوقی

پیاده‌سازی فن‌آوری دسترسی از راه دور باید با در نظر گرفتن هر قوه مقننه قابل اجرا و یا محدودیت‌های پایشی یا الزامات بر عهده گرفته شود.

مجریان باید به قراردادی کافی و سایر جنبه‌های قانونی استقرارهای دسترسی از راه دور که در جای خود هستند اطمینان داشته باشند. تا از مراجعه در صورت وقایع پیش بینی نشده مطمئن شوند.

۹ نتیجه‌گیری

دسترسی از راه دور به یک رویکرد طرح‌ریزی شده خوب و آغاز با یک خط‌مشی امنیتی مناسب نیاز دارد و ابزار فنی و همچنین ابزار سازمانی و قانونی را پوشش می‌دهد.

پیوست الف

(اطلاعاتی)

نمونه خط‌مشی امنیتی دسترسی از راه دور

الف-۱ هدف

هدف از این خط‌مشی تعریف استاندارد برای ارتباط با شبکه (نام شرکت) از هر میزبانی است. این استانداردها برای به حداقل رساندن مواجهه بالقوه (نام شرکت) از خسارت ممکن ناشی از استفاده غیرمجاز از منابع (نام شرکت) طراحی شده است. خسارات شامل از دست دادن حساسیت و یا اطلاعات محرمانه شرکت، مالکیت معنوی، صدمه به تصویر عمومی، صدمه به سامانه‌های داخلی بحرانی (نام شرکت) و غیره است.

الف-۲ هدف و دامنه کاربرد

این خط‌مشی برای همه کارمندان (نام شرکت)، پیمانکاران، فروشندگان و عوامل (نام شرکت) متعلق و یا رایانه متعلق به شخص و یا ایستگاه کاری مورد استفاده برای ارتباط به (نام شرکت) شبکه است. این خط‌مشی شامل ارتباطات دسترسی از راه دور مورد استفاده برای انجام کار در حق (نام شرکت)، از جمله خواندن و یا ارسال پست الکترونیکی و مشاهده منابع صفحات وب اینترانت کاربرد دارد.

پیاده‌سازی دسترسی از راه دور که تحت پوشش خط‌مشی‌های مشمول است اما محدود به مودم شماره‌گیری، تقویت قاب، ISDN، DSL، VPN، SSH و کابل مودم و غیره نمی‌شود.

الف- ۳ خط‌مشی

الف-۳-۱ کلیات

۱- این مسئولیت کارکنان (نام شرکت)، پیمانکاران، فروشندگان و عوامل با مزایای دسترسی از راه دور به شبکه شرکت‌ها (نام شرکت) است برای اطمینان از اینکه ارتباط دسترسی از راه دور آن‌ها به اندازه همان کاربر در محل ارتباط (نام شرکت) مورد توجه واقع شده است؛

۲- دسترسی عمومی به اینترنت برای استفاده‌های ضروری تفریحی توسط اعضای خانواده از طریق شبکه (نام شرکت) بر روی رایانه‌های شخصی است که به کارمندان خدماتی با سهم یکسان اجازه داده می‌شود. کارمند (نام شرکت) برای اطمینان از اینکه اعضای خانواده هیچ خط‌مشی را (نام شرکت) نقض نمی‌کند، فعالیت‌های غیرقانونی انجام نمی‌شود، و از دسترسی برای منافع تجارت در خارج استفاده نمی‌شود، مسئول است. کارمند (نام شرکت) باید مسئولیت عواقب سوءاستفاده از دسترسی را داشته باشد؛

۳- لطفاً خط‌مشی‌های زیر را برای جزئیات بیشتر حفاظت از اطلاعات زمانی‌که دسترسی به شبکه شرکت‌های بزرگ از طریق روش‌های دسترسی از راه دور، و استفاده قابل‌قبول از شبکه امکان‌پذیر است، بررسی کنید. (نام شرکت):

الف- خط‌مشی رمزگذاری قابل‌قبول؛

ب- خط‌مشی شبکه خصوصی مجازی(VPN)[1]؛

ج- خط‌مشی ارتباطات بی‌سیم؛

د- خط‌مشی مورد استفاده قابل‌قبول

1- Virtual Private Network

۴- برای کسب اطلاعات بیشتر در مورد (نام شرکت) گزینه‌های دسترسی از راه دور، از جمله نحوه سفارش و یا خدمات قطع ارتباط، مقایسه هزینه‌ها، عیب‌یابی و غیره، رفتن به وب‌سایت، خدمات دسترسی از راه دور وجود دارد.

الف-۳-۲ الزامات

۱- دسترسی از راه دور امن باید به شدت کنترل شود. کنترل از طریق تصدیق کلمه رمز یک‌بار مصرف یا کلید عمومی/خصوصی با عبارات عبور قوی اجرا خواهد شد. برای کسب اطلاعات در مورد ایجاد عبارت عبور قوی خط‌مشی رمز عبور را ببینید.

۲- در هیچ زمانی نباید هر کارمند (نام شرکت) نام کاربری و یا رمز رایانامه خود را در اختیار هر کسی، حتی اعضای خانواده قرار دهد.

۳- (نام شرکت) کارکنان و پیمانکاران با مزایای دسترسی از راه دور باید اطمینان حاصل کنند که (نام شرکت) تعلقاتشان و یا رایانه شخصی و یا ایستگاه کاری، که از راه دور به (نام شرکت) شبکه شرکت‌ها متصل هستند، در همان زمان، به‌استثنای شبکه‌های شخصی که تحت کنترل کامل کاربر هستند به شبکه دیگری متصل نیستند.

۴- (نام شرکت) کارکنان و پیمانکاران با مزیت‌های دسترسی از راه دور به (نام شرکت) شبکه شرکت نباید از هیچ حساب رایانامه (نام شرکت) (به‌عنوان مثال: هاتمیل، یاهو، AOL) ، و یا دیگر منابع خارجی برای انجام تجارت (نام شرکت) استفاده کنند بدین وسیله اطمینان حاصل می‌شود که تجارت رسمی هرگز با تجارت شخصی اشتباه نمی‌شود.

۵- مسیریاب اختصاص داده شده برای خطوط ISDN که برای دسترسی به شبکه پیکربندی می‌شود (نام شرکت) باید حداقل الزامات تصدیق CHAP را برآورده سازد.

۶- پیکربندی دوباره تجهیزات یک کاربر خانگی برای اهداف تونل‌زنی شکافته شده یا متعلق به دو شبکه متفاوت در هر زمان ممکن است.

۷- تقویت قاب باید حداقل شرایط تصدیق استانداردهای DLCI را فراهم کند.

۸- پیکربندی سخت‌افزار غیراستاندارد باید توسط خدمات دسترسی از راه دور به تصویب برسد، و InfoSec باید تنظیمات امنیتی را برای دسترسی به سخت‌افزار تایید کند.

۹- همه میزبان‌ها از طریق فن‌آوری‌های دسترسی از راه دور، (نام شرکت) به شبکه داخلی متصل هستند که باید از بروزترین نرم‌افزار ضدویروس استفاده شود (URL را در سایت نرم‌افزار شرکت‌های بزرگ اینجا قرار دهید)، این شامل رایانه‌های شخصی است. ارتباطات قسمت سوم باید با الزاماتی که در بخش سوم توافقنامه بیان شده مطابقت کند.

۱۰- تجهیزات شخصی که برای ارتباط به شبکه‌ها (نام شرکت) مورد استفاده هستند باید الزامات (نام شرکت) متعلق به تجهیزات برای دسترسی از راه دور را برآورده نمایند.

۱۱- سازمان‌ها و یا افرادی که مایل به پیاده‌سازی راه حل‌های دسترسی از راه دور غیراستاندارد برای (نام شرکت) محافظت شبکه هستند باید قبل از دسترسی از راه دور و InfoSec تائید را به‌دست آورند.

الف- ۴ اجرا

هر کارمند که از این خط‌مشی سرپیچی نماید ممکن است در ارتباط با اقدام انضباطی نهایت فسخ اشتغال باشد.

الف-۵ اصطلاحات و تعاریف

مودم کابلی: شرکت‌های کابلی مانند پهنای باند AT&T دسترسی به اینترنت را در طول کابل ارائه می‌دهند.

کابل کواکسیال تلویزیون: یک مودم کابلی این کابل کواکسیال را قبول می‌کند و می‌تواند داده‌ها را از اینترنت با پهنای باند بیش از ۱/۵مگابیت در ثانیه دریافت کند. در حال حاضر این کابل تنها در جوامع خاصی در دسترس است.

CHAP: پروتکل تصدیق دست دادن چالش یک روش تصدیق است که از تابع hash یک‌طرفه استفاده می‌کند.

DLCI: شناسه ارتباط پیوند داده (DLCI) یک شماره منحصربه‌فرد اختصاص یافته به یک مدار مجازی دائم (PVC) نقطه پایان در یک شبکه تقویت قاب است. DLCI یک نقطه پایانی PVC خاص را در داخل کانال دسترسی یک کاربر در یک شبکه تقویت قاب شناسایی می‌کند و اهمیت محلی فقط به آن کانال بستگی دارد.

شماره‌گیری در مودم: دستگاه جانبی که رایانه‌ها را برای ارسال ارتباطات از طریق خطوط تلفن به یکدیگر متصل می‌کند. مودم، داده‌های دیجیتال رایانه‌ای را برای ارسال از طریق خطوط تلفن به سیگنال‌های آنالوگ تبدیل می‌کند، و سپس به سیگنال‌های دیجیتال برمی‌گرداند تا توسط رایانه در انتهای دیگر خوانده شود، به این ترتیب نام "مودم" برای مدولاتور/ دمدولاتور نهاده‌اند.

داشتن ارتباط همزمان به بیش از یک شبکه از طریق یک رایانه و یا افزار شبکه. مثال‌ها عبارتند از: وارد شدن به شبکه شرکت‌ها از طریق ارتباط اترنت محلی، و شماره‌گیری به AOL و یا دیگر فراهم‌کنندگان خدمات اینترنتی (ISP). (نام شرکت) دسترسی از راه دور به شبکه خانه، و ارتباط خود به شبکه دیگری، مانند دسترسی از راه دور زوج را فراهم می‌کند. پیکربندی مسیریاب ISDN به شماره‌گیری داخل (نام شرکت) و یک ISP به مقصد بستگی دارد.

DSL: خط مشترک دیجیتال شکلی از دسترسی به اینترنت با سرعت بالا در رقابت با مودم‌های کابلی است. DSL از طریق خطوط تلفن استاندارد کار می‌کند و از سرعت داده‌ها بیش از ۲ مگابیت در ثانیه در پایین‌دست (کاربر) و آهسته‌تر سرعت بالادست (به اینترنت) پشتیبانی می‌کند.

تقویت قاب: روشی از ارتباطات که می‌تواند به تدریج از سرعت ISDN به سرعت یک خط T1 برود. تقویت قاب به جای استفاده در هر زمان هزینه صدور صورت حساب با سهمیه یکسان دارد. تقویت قاب متصل از طریق شبکه شرکت تلفن است.

ISDN: دو نوع از شبکه دیجیتالی خدمات مجتمع و یا ISDN وجود دارد: BRI و PRI. BRI برای دسترسی اداره یا از راه دور خانگی مورد استفاده قرار می‌گیرد. BRI دو کانال "حامل" با ۶۴ کیلوبیت (در مجموع ۱۲۸ کیلوبیت) و کانال D1 برای اطلاعات سیگنالینگ دارد.

دسترسی از راه دور: هرگونه دسترسی به شبکه شرکت‌ها (نام شرکت) از طریق غیر (نام شرکت) شبکه کنترل شده، افزاره یا رسانه است.

تونل‌زنی شکافته‌شده: همزمان با دسترسی مستقیم به یک غیرشبکه (نام شرکت) (مانند اینترنت، و یا یک شبکه خانگی) از یک افزاره از راه دور (رایانه شخصی، PDA، تلفن WAP، و غیره) در زمانی‌که با (نام شرکت) شبکه شرکت‌ها از طریق یک تونل VPN[1] اتصال است. شبکه خصوصی مجازی VPN یک روش برای دسترسی به یک شبکه از راه دور از طریق "تونل‌زنی" از میان اینترنت است.

1- Virtual Private Network

پیوست ب

(اطلاعاتی)

پیاده‌سازی RADIUS و گسترش بهترین روش‌ها

ب-۱ کلیات

این پیوست راهنمایی در مورد استفاده از RADIUS را برای محیط مایکروسافت ویندوز ۲۰۰۰ و سیستم عامل فراهم می‌کند.

برای پرداختن به مسائل امنیتی RADIUS، باید موارد زیر و بکارگیری بهترین روش‌ها رعایت شود.

ب-۲ پیاده‌سازی بهترین شیوه‌ها

برای پرداختن به مسائل امنیتی RADIUS در هنگام اجرای سرویس‌دهنده، سرویس‌گیرنده و یا پروکسی RADIUS از بهترین شیوه‌های زیر استفاده شود.

۱- برای فراهم کردن اطلاعات محرمانه برای کل پیام RADIUS، IPsec با استفاده از ESP و یک الگوریتم رمزنگاری مانند DES3 پیاده‌سازی می‌شود.

این مورد در RFC 3162 شرح داده شده است. توسط رمزنگاری کل پیام RADIUS با IPsec، زمینه‌های RADIUS حساس (مانند زمینه تصدیق کننده درخواست در پیام درخواست دسترسی) و صفات (مانند رمز عبور کاربری، رمز عبور تونل، و صفات MPPE کلید) از مشاهده دیگران محافظت شده‌اند. مهاجم ابتدا باید پیام RADIUS محافظت ESP را قبل از اینکه آنها بتوانند محتوای پیام RADIUS را تحلیل کنند، رمزگشایی کند. پشتیبانی از گواهی IPsec مبتنی بر تصدیق برای جلوگیری مهاجم از حملات آنلاین در برابر سرویس‌دهنده RADIUS توصیه شده است.

به‌طور متناوب یا در رابطه با استفاده از IPsec، باید کارهای زیر انجام شود:

۱- اجازه پیکربندی و استفاده از اسرار به‌اشتراک گذاشته شده حداقل به طول ۳۲ رقم هگزا دسیمال و یا حداقل به طول ۲۲ کاراکتر صفحه کلید.

۲- پیاده‌سازی استفاده از ویژگی تصدیق کننده پیام برای همه پیام‌های درخواست دسترسی

برای یک سرویس‌گیرنده RADIUS، پیاده‌سازی استفاده از ویژگی تصدیق‌کننده پیام برای همه پیام‌های درخواست دسترسی و اجازه پیکربندی آن را می‌دهند. برای سرویس‌دهنده RADIUS و یا پروکسی، پیاده‌سازی استفاده از ویژگی پیام تصدیق کننده مورد نیاز برای همه پیام‌های درخواست دسترسی و اجازه پیکربندی آن را می‌دهند.

۳- پیاده‌سازی یک تولید کننده رمزنگاری با کیفیت تصادفی برای تصدیق کننده درخواست.

برای فراهم‌کردن حفاظت اضافی برای دسترسی تصدیق سرویس‌گیرنده در اجرای RADIUS ، از بهترین شیوه های زیراستفاده شود:

۱- اجرای انواع EAP و EAP که از روش‌های تصدیق قوی استفاده می‌کنند.

یـک مثـال خـوب از یـک روش قـوی از EAP، روش EAP-TLS اسـت، کـه نیـاز بـه تبـادل دسترسـی سرویس‌گیرنده و گواهینامه‌های سرویس‌دهنده RADIUS دارد. همه پیام‌های EAP نیاز به ویژگـی تصـدیق کننده پیام دارند، که محافظت از پیام درخواست دسترسی را فراهم می‌کند و با IPsec محافظت نمی‌شود.

۲- پیاده‌سازی روش‌های تصدیق از تصدیق متقابل استفاده می‌کنند.

با تصدیق متقابل، هر دو طرف اعتبار ارتباط نظیر خود را تمام می‌کنند. اگر هر تصدیق با مشکل مواجه شـد، اقدام به ارتباط پذیرش نمی‌شود. به‌عنوان مثال: TLS-EAP و MS-CHAP V2 روش‌هـای تصـدیق متقابـل هستند. با استفاده از EAP-TLS، سرویس‌دهنده RADIUS گواهینامه دسترسی سرویس‌گیرنده کـاربر را تایید می‌کند و مشتری دسترسی گواهی رایانه سرویس‌دهنده RADIUS را تائید می‌کند. بـا MS-CHAP V2، هر دو سرویس‌گیرنده دسترسی و سرویس‌دهنده دسترسی مدرک آگاهی از رمز عبور حسـاب کـاربر را فراهم می‌کنند.

۳- اگر شما تصدیق PAP را پیاده‌سازی کنید، به‌طور پیش فرض استفاده از آن را غیرفعال کنید.

به عنوان مثال، کارت OTP/Token از PAP برای ارسال اطلاعات تصدیق استفاده مـی‌کنـد. در صـورتی کـه باید PAP را اجرا کنید، استفاده از آن را به‌طور پیش فرض غیرفعال کنید و اسرار مشترک طولانی و تصـدیق کننده درخواست رمزنگاری کیفیت را پیـاده‌سـازی کنیـد. ایـن صـحیح اسـت کـه IEEE 802.1X از PAP پشتیبانی نمی‌کند، ولی این موضوع فقط شامل ارتباطات PPP است.

۴- اگر شما تصدیق CHAP را پیاده‌سازی کنید، از چالش CHAP قوی استفاده کنید.

مانند تصدیق‌کننده‌ها درخواست RADIUS، چالش CHAP باید به‌صورت تصادفی و دارای کیفیت رمزنگاری باشد.

۵- اگر شما تصدیق MS - CHAP را پیاده‌سازی کنید، مدیر شبکه محلی از رمزگـذاری پاسـخ‌هـای چـالش MS-CHAP و یا تغییر رمز عبور پشتیبانی نمی‌کند.

ب-۳ استقرار بهترین شیوه

برای پرداختن به مسائل امنیتی RADIUS در هنگام استقرار یک راه‌حل RADIUS، از استقرار زیر بهتـرین روش‌ها استفاده کنید:

الف- برای فـراهم کـردن اطلاعـات محرمانـه بـرای کـل پیـام RADIUS، سـرویس‌گیرنـدگان RADIUS و سرویس‌دهندگان را به استفاده از IPsec با ESP با DES3 برای تمام ترافیک RADIUS پیکربندی کنید.

پیکربندی IPsec ESP با DES3 برای ترافیک RADIUS به پیاده‌سازی IPsec بستگی دارد. به‌عنـوان مثـال: اگر شما از مسیریابی و خدمات دسترسی از راه دور ویندوز ۲۰۰۰ به‌عنوان یک سـرویس‌دهنـده دسترسـی و ویندوز ۲۰۰۰ IAS به‌عنوان سرویس‌دهنده RADIUS در یک مسیر فعـال محـیط دامنـه خـدمات اسـتفاده می‌کنید، شما می‌توانید خط‌مشی‌های IPSec فعال برای محتوی سامانه مناسب با قـانونی کـه از رمزگـذاری ESP و DES3 برای همه ترافیک و از پورت 1812 UDP و 1813 استفاده می‌کند را پیکربندی نمائید. بـرای اطلاعات بیشتر، به راهنمای ویندوز سرور ۲۰۰۰ مراجعه کنید.

به‌طور متناوب یا در رابطه با استفاده از IPsec، شما باید کارهای زیر را انجام دهید:

۱- از اسرار مشترک قوی متشکل از توالی تصادفی ارقام هگزادسیمال حداقل به‌طول ۳۲ رقم و یا یک توالی تصادفی از حروف بالا و با حروف کوچک، اعداد و علائم نقطه‌گذاری که حداقل به‌طول ۲۲ کاراکتر باشد، استفاده کنید. در حالت ایده‌آل، اسرار مشترک باید توسط رایانه تولید شود.

۲- از رموز مشترک مختلف برای هر دو سرویس‌دهنده و سرویس‌گیرنده RADIUS استفاده نمایید.

۳- نیاز به استفاده از ویژگی تصدیق‌کننده پیام برای همه پیام‌های درخواست دسترسی است.

طوری پیکربندی کنید که هر سرویس‌گیرنده RADIUS ویژگی پیام تصدیق‌کننده را به همه پیام‌های درخواست دسترسی ارسال کند.

۴- از سرویس‌گیرندگان، سرویس‌دهندگان و پروکسی که احراز هویت‌کنندگان قوی رمزنگاری را به‌کار می‌برند استفاده نمایید.

به‌منظور فراهم کردن حمایت‌های اضافی برای دسترسی تصدیق سرویس‌گیرنده برای استقرار RADIUS خود، از بهترین شیوه‌های زیر استفاده کنید:

۱- در صورتی‌که PAP مورد نیاز نباشد، استفاده از آن را در سرویس‌دهنده دسترسی و RADIU غیرفعال کنید.

تنها استفاده قابل‌قبول از PAP برای ارتباط امن، OTP و تصدیق کارت رمز است، که در آن رمز عبور آنتروپی بالا دارد و با هر بار استفاده تغییر می‌کند. با این حال، فراهم‌کردنPAP پیکربندی اشتباه سرویس-گیرندگان دسترسی به مذاکره PAP با سرویس‌دهندگان، دسترسی آن‌ها را اجازه می‌دهد و کلمه عبور حساب کاربر حفاظت‌نشده را ارسال می‌کند. راه‌حل بهتر استفاده از EAP و انواع EAP برای OTP و تصدیق کارت رمز است.

۲- اگر MS-CHAP مورد نیاز است، استفاده از رمزنگاری مدیر شبکه محلی را غیرفعال کنید.

درصورتی‌که شما از ویندوز ۲۰۰۰ IAS استفاده می‌کنید مقدار کلید ریجستری را روی سرویس‌دهنده IAS تنظیم کنید :

HKEY-LOCAL_MACHINE\System\CurrentControlSet\Services\RemoteAccess\Policy LM Authentication to 0

۳- استفاده از EPA و یک نوع EAP با یک روش تصدیق قوی.

تصدیق IEEE 802.1x برای نقاط دسترسی بی‌سیم به استفاده از EAP نیاز دارد، از ویژگی‌های احرازهویت کننده، حفاظت از هر پیام درخواست دسترسی و عدم پشتیبانی از تصدیق PAP است.

۴- از یک روش اعتبارسنجی متقابل مانند TLS-EAP و یا V2 CHAP-MS

پیوست پ

(اطلاعاتی)

دو حالت از FTP

دو حالت از FTP وجود دارد:

۱- حالت PORT

۲- حالت PASV

حالت PORT از FTP

۱- سرویس‌گیرنده FTP : این پورت‌ها پاسخ تصادفی را در محدوده اعداد بالا باز می‌کند. (به‌منظور این مثال: پورت‌های ۶۰۰۰ TCP و TCP 6001 را در نظر می‌گیریم.)

۲- سرویس‌گیرنده FTP: این مورد به‌منزله ارسال درخواست برای باز کردن یک کانال فرمان از پورت به پورت FTP TCP21 سرویس‌دهنده است.

۳- سرویس‌دهنده FTP: کلمه OK را از پورت TCP21 به پورت TCP 6000 سرویس‌گیرنده FTP ارسال می‌کند.

۴- سرویس‌گیرنده FTP: این مورد به‌منزله درخواست داده (دستور پورت) به سرویس‌دهنده FTP است. سرویس‌گیرنده FTP شامل دستور PORT شماره پورت داده است که برای دریافت اطلاعات باز می‌شود. در این مثال: سرویس‌گیرنده FTP پورت ۶۰۰۱ مربوط به TCP را برای دریافت داده باز کرده است.

۵- سرویس‌دهنده FTP: سرویس‌دهنده FTP یک ارتباط جدید وارد شونده به سرویس‌گیرنده FTP بر روی پورت نشان داده شده باز می‌کند. پورت منبع سرویس‌دهنده FTP، پورت TCP20 است. در این مثال سرویس‌دهنده FTP، داده‌ها را از پورت TCP20 خود به پورت TCP 6001 سرویس‌گیرنده ارسال می‌کند.

در این گفتگو، دو ارتباط برقرار شده‌اند: ارتباط به خروجی که توسط سرویس‌گیرنده FTP آغاز و ارتباط ورودی توسط سرویس‌دهنده FTP ایجاد شده است. توجه داشته باشید که اطلاعات موجود در دستور PORT (که در طول کانال فرمان فرستاده شده) در بخش داده مربوط به بسته ذخیره شده است.

پ-۲ حالت PASV

پیاده‌سازی محبوب‌ترین FTP حالت منفعل یا حالت PASV است. ارتباطات حالت PASV مربوط به FTP به‌طور پیش‌فرض بر روی مرورگرهای محبوب هستند. یکی از مزایای عمده‌ای از حالت PASV این است که سرویس‌دهنده نیاز به ایجاد یک ارتباط ورودی جدید به سرویس‌گیرنده FTP ندارد. همان‌طور که بعداً خواهید دید، این باعث می‌شود FTP حالت PASV کمی بیشتر موافق فایروال باشد.

توالی رویدادهای حالت PASV مربوط به FTP شبیه به این می‌مانند:

۱- سرویس‌گیرنده FTP : پورت‌های پاسخ تصادفی را در محدوده اعداد بالا باز می‌کند. (برای اهداف این مثال پورت‌های TCP 6000 و TCP 6001 را فرض خواهیم کرد).

۲- سرویس‌گیرنده FTP: این مسئله به‌منزله ارسال درخواست برای باز کردن یک کانال فرمان از TCP پورت ۶۰۰۰ به FTP سرویس‌دهنده TCP پورت ۲۱ است.
۳- سرویس‌دهنده FTP: کلمه OK را از پورت TCP 21 به پورت TCP 6000 سرویس‌گیرنده FTP ارسال می‌کند (پیوند کانال فرمان). کانال فرمان در این مرحله ایجاد شده است.
۴- سرویس‌گیرنده FTP: یک درخواست دستور PASV می‌فرستد و سرویس‌دهنده FTP یک شماره پورت باز می‌کند تا سرویس‌گیرنده FTP بتواند اقدام به ایجاد ارتباط کانال داده‌ها کند.
۵- سرویس‌دهنده FTP: در طول کانال فرمان شماره پورت TCP را می‌فرستد که سرویس‌گیرنده FTP بتواند ارتباط برای ایجاد کانال داده‌ها را آغاز کند. در این مثال، سرویس‌دهنده FTP پورت ۷۰۰۰ را باز می‌کند.
۶- سرویس‌گیرنده FTP: این یک ارتباط جدید از پورت TCP 6001 پاسخ خود را به کانال داده ۷۰۰۰ سرویس‌دهنده FTP باز می‌کند. انتقال داده‌ها از طریق این کانال اتفاق می‌افتد.
توجه داشته باشید که سرویس‌گیرنده FTP حالت PASV همه ارتباطات را آغاز می‌کند. سرویس‌دهنده FTP هرگز نیازی برای ایجاد یک ارتباط تازه برگشتی به سرویس‌گیرنده FTP ندارد.

پیوست ت

(اطلاعاتی)

فهرست‌های بررسی برای خدمت پستی امن

فهرست‌های بررسی زیر به طرح‌ریزی، پیکربندی و راه‌اندازی یک سرویس‌دهنده پستی کمک می‌کند، آن‌ها موضوعاتی مانند سیستم‌عامل، امنیت پستی، کنترل فیلتر کردن محتویات را تحت پوشش قرار می‌دهد.

ت-۱ فهرست بررسی سرویس‌دهنده پست الکترونیکی سیستم عامل

تکمیل	اقدام
	طرح پیکربندی و پیاده‌سازی از سرویس دهنده پست الکترونیکی
O	شناسایی توابع از سرویس دهنده پست الکترونیکی.
O	شناسایی گروه‌های اطلاعاتی که در سراسر سرویس‌دهنده پست الکترونیکی ذخیره، پردازش و انتقال داده می‌شوند.
O	شناسایی الزامات امنیتی از اطلاعات.
O	شناسایی میزبان اختصاص داده‌شده برای اجرای سرویس‌دهنده پست الکترونیکی.
O	شناسایی خدمات شبکه که توسط سرویس‌دهنده پست الکترونیکی فراهم یا پشتیبانی می‌شود.
O	شناسایی کاربران و گروهی از کاربران از سرویس‌دهنده پست الکترونیکی و تعیین امتیاز برای هر رده از کاربر.
O	شناسایی کاربران مجاز برای سرویس دهنده پست الکترونیکی
	انتخاب سیستم عامل مناسب برای سرویس‌دهنده پست الکترونیکی
O	قرار گرفتن در معرض حداقل آسیب پذیری‌ها.
O	اعمال محدودیت اجرایی یا فعالیت‌های سطح ریشه برای کاربران مجاز.
O	اعمال رد دسترسی به اطلاعات در سرویس‌دهنده دیگری که برای دسترسی مورد نظر است.
O	اعمال غیرفعال کردن خدمات شبکه غیرضروری که امکان دارد درون سیستم‌عامل یا نرم‌افزار سرویس‌دهنده ایجاد شود.
O	هزینه‌های قابل‌قبول برای بیمه و تعهد (برخی از شرکت‌های بیمه بیش از سیستم عامل معین تعهد دارند).
O	گماشتن کارکنان باتجربه در دسترس برای نصب، پیکربندی، امنیت و نگهداری سیستم عامل .
	الحاق و ارتقاء سیستم عامل
O	شناسایی و نصب تمام الحاق‌های ضروری و ارتقاء برای سیستم عامل.
O	شناسایی و نصب تمام الحاق‌های ضروری و ارتقاء برای برنامه‌های کاربردی و خدمات همراه با سیستم عامل.
	حذف یا غیرفعال کردن خدمات غیرضروری و برنامه‌های کاربردی
O	غیرفعال کردن یا حذف خدمات غیرضروری و برنامه‌های کاربردی.

ادامه جدول ت-۱

	پیکربندی سیستم عامل تصدیق کاربر
O	حذف یا غیرفعال کردن حساب‌ها و گروه‌های پیش‌فرض غیرضروری
O	ایجاد حسابهای کاربری برای رایانه‌های خاص.
O	غیر فعال کردن حساب‌های غیر تعاملی.
O	ایجاد گروه‌های کاربری برای رایانه‌های خاص.
O	ایجاد حساب‌های کاربری برای رایانه‌های خاص.
O	بررسی خط‌مشی کلمه عبور سازمان و تنظیم کلمات عبور حساب‌ها به‌طور مناسب (مثال: طول و پیچیدگی).
O	پیکربندی رایانه برای رد کردن ورود به سامانه بعد از تعداد محدودی از شکست تلاش‌ها.
O	نصب و پیکربندی مکانیسم‌های امنیتی دیگر برای تقویت احراز هویت.
	آزمون امنیت سیستم عامل
O	آزمون سیستم عامل بعد از نصب اولیه برای تعین آسیب‌پذیری‌ها.
O	آزمون دوره‌ای سیستم عامل (به‌عنوان مثال هر سه ماه یکبار) برای تعین آسیب‌پذیری‌های جدید.

ت-۲ سرویس‌دهنده پست الکترونیکی و محتوای فهرست امنیتی

تکمیل	اقدام
	ارتقا امنیت در برنامه کاربردی سرویس‌دهنده پست الکترونیکی
O	نصب نرم‌افزار سرویس‌دهنده بر روی میزبان اختصاص داده‌شده
O	نصب حداقل خدمات اینترنتی مورد نیاز.
O	اعمال هر الحاق یا ارتقاء برای تصحیح آسیب‌پذیری‌های شناخته‌شده.
O	حذف یا غیرفعال کردن تمام خدمات نصب‌شده توسط برنامه کاربردی سرویس‌دهنده پست الکترونیکی اما ضروری نیست (به‌عنوان مثال پست الکترونیکی مبتنی بر وب، FTP، مدیریت از راه دور).
O	حذف تمام مستندات فروشنده از روی سرویس‌دهنده.
O	اعمال الگوی امنیتی مناسب یا ارتقا متن به سرویس‌دهنده.
O	پیکربندی مجدد SMTP، POP، بنرخدمات IMAP (در صورت لزوم غیره) نه به گزارش سرویس‌دهنده پست الکترونیکی و نوع و نسخه سیستم عامل.
O	غیرفعال‌کردن دستورات پست الکترونیکی غیرضروری و خطرناک (به‌عنوان مثال: VRFY، EXPN)
	پیکربندی سیستم عامل و کنترل دسترسی به سرویس‌دهنده پست الکترونیکی
O	محدود کردن دسترسی به برنامه‌های کاربردی سرویس‌دهنده پست الکترونیکی به زیرمجموعه‌ای از منابع محاسباتی.

ادامه جدول ت-۲

O	محدودکردن دسترسی کاربران از طریق کنترل‌های دسترسی اضافی اجراشده توسط سرویس‌دهنده پست الکترونیکی که در آن بیشتر کنترل دسترسی از سطح به‌صورت جزئی موردنیاز است.
O	پیکربندی برنامه‌های کاربردی سرویس‌دهنده پست الکترونیکی برای اجرا فقط تحت یک کاربر انفرادی منحصر بفرد و شناسایی گروه با کنترل دسترسی محدود کننده.
O	اطمینان از سرویس‌دهنده پست الکترونیکی به‌عنوان ریشه یا مدیر یا سامانه که در حال اجرا نیست.
O	پیکربندی سیستم عامل میزبان به‌طوریکه سرویس‌دهنده پست الکترونیکی می‌تواند فایل‌های ثبت را بنویسد اما نمی‌تواند بخواند.
O	پیکربندی سیستم عامل میزبان به‌طوریکه فایل‌های موقت ایجاد شده توسط برنامه‌های کاربردی سرویس‌دهنده پست الکترونیکی به مسیرهای فرعی محافظت شده مناسب و مشخص شده محدود شده‌اند.
O	پیکربندی سیستم عامل میزبان به‌طوریکه دسترسی به هر فایل موقت ایجاد شده توسط برنامه کاربردی سرویس‌دهنده پست الکترونیکی به فرآیند سرویس‌دهنده پست الکترونیکی که این فایل‌ها را ایجاد کرده‌اند، محدود شده‌اند.
O	اطمینان از سرویس‌دهنده پست الکترونیکی که نمی‌تواند فایل‌های خارج از ساختار فایل‌های مشخص‌شده اختصاصی سرویس‌دهنده پست الکترونیکی را ذخیره کند.
O	پیکربندی سرویس‌دهنده پست الکترونیکی برای اجرا در chroot jail [a] در میزبان لینوکس و یونیکس
O	نصب صندوق‌های پست الکترونیکی کاربران بر درایوهای مختلف دیسک سخت یا بخش‌های منطقی مختلف از سیستم عامل و برنامه‌های کاربردی سرویس‌دهنده پست الکترونیکی.
O	محدود کردن اندازه فایل‌های پیوست که مجاز هستند.
O	اطمینان از فایل‌های ثبت ذخیره‌شده در محلی به اندازه مناسب.
	راهکارهای تعامل با فایل پیوست و محتوی آسیب رسان
O	پیاده‌سازی اسکنر ویروس متمرکز (در دروازه پست الکترونیکی، فایروال و یا سرویس‌دهنده پست الکترونیکی)
O	نصب اسکنرهای ویروس بر روی میزبان‌های مشتری.
O	بروز رسانی همه بانک‌های اطلاعاتی ویروس بر تمام اسکنرها به‌صورت هفتگی یا زمانی که حادثه خاص بدی وجود دارد.
O	آموزش کاربران در مورد خطرات و ویروس‌ها و چگونگی به حداقل رساندن این خطرات.
O	آگاه‌سازی کاربران در هنگام وقوع حادثه
O	پیکربندی محتوای فیلترکردن برای جلوگیری از پیام‌های مشکوک.
O	پیکربندی محتوای فیلترکردن برای جلوگیری از پیام‌هایUCE (پست الکترونیکی‌های ناخواسته تجاری).
O	پیکربندی تحلیل‌های لغوی در صورت لزوم.

a- در سیستم‌عامل یونیکس، chroot عملی است که دایرکتوری ریشه آشکار را برای فرآیند و فرزندان در حال اجرای جاری تغییر می‌دهد. برنامه‌ای که در چنین محیط اصلاح‌شده‌ای اجرا می‌شود نمی‌تواند فایل‌های خارج از درخت دایرکتوری نام‌گذاری شود (درنتیجه نمی‌تواند دسترسی شود) محیط اصلاح شده زندان chroot نامیده‌می‌شود

ادامه جدول ت-۲

O	ایجاد محتوی خط‌مشی فیلتر کردن.
O	اضافه کردن سلب مسؤلیت قانونی از پست‌های الکترونیکی در صورت لزوم.
O	پیکربندی سرویس‌دهنده پست الکترونیکی برای جلوگیری از پست الکترونیکی از فهرست‌های ممنوع بازپخش.
O	پیکربندی سرویس‌دهنده پست الکترونیکی برای جلوگیری از پست الکترونیکی از دامنه خاص در صورت نیاز.
O	پیکربندی تصدیق بازپخش پست الکترونیکی بر روی سرویس‌دهنده.
O	پیکربندی سرویس‌دهنده پست الکترونیکی برای استفاده از تصدیق رمز نگاری شده.
O	پیکربندی سرویس‌دهنده پست الکترونیکی برای پشتیبانی دسترسی به وب فقط از طریق SSL/TLS و فقط در صورتی که چنین دسترسی به آن ضروری باشد.

ت-۳ فهرست بررسی زیرساخت‌های شبکه

تکمیل	اقدام
O	**موقعیت شبکه**
O	سرویس‌دهنده پست الکترونیکی بر روی شبکه داخلی قرار دارد و توسط دروازه پست الکترونیکی و یا فایروال حفاظت شده و یا سرویس‌دهنده پست الکترونیکی در DMZ قرار داده شده است.
	پیکربندی فایروال
O	سرویس‌دهنده پست الکترونیکی توسط یک فایروال محافظت می‌شود.
O	سرویس‌دهنده پست الکترونیکی در صورتی‌که با تهدید بالاتری مواجه شود یا آسیب‌پذیرتر باشد توسط یک لایه کاربردی فایروال حفاظت می‌شود.
O	فایروال تمام ترافیک‌های میان اینترنت و سرویس‌دهنده پست الکترونیکی را کنترل می‌کند.
O	فایروال تمام ترافیک ورودی به سرویس‌دهنده پست الکترونیکی به‌غیر از پورت ۲۵ TCP(SMTP)، پورت ۱۱۰ TCP (POP3)، پورت ۱۴۳ TCP (IMAP)، پورت ۳۹۸ TCP (LDAP)، پورت ۶۳۶ TCP (LDAP امن) را در صورت لزوم بلوکه می‌کند.
O	فایروال آدرس IP و یا زیرشبکه‌هایی که گزارش‌های IDS در حال حمله به شبکه‌های سازمانی است را بلوکه می‌کند.
O	فایروال مدیر شبکه و یا مدیر سرویس‌دهنده پست الکترونیکی را از فعالیت‌های مشکوک از طریق وسیله مناسب آگاه می‌سازد.
O	فایروال محتوی فیلتر کردن را فراهم می‌کند (برنامه کاربردی لایه فایروال).
O	فایروال برای حفاظت در برابر حملات DOS پیکربندی شده است.
O	فایروال رویدادهای بحرانی را ثبت می‌نماید.
O	فایروال و سیستم عامل فایروال به آخرین و بیشترین سطح امنیت وصل شده است.

ادامه جدول ت-۳

	سامانه کشف نفوذ
O	IDS برای پایش بر ترافیک شبکه قبل از هرگونه فایروال یا مسیریاب پیکربندی شده است (مبتنی بر شبکه).
O	IDS برای پایش بر ترافیک شبکه به و از سرویس‌دهنده پست الکترونیکی پس از فایروال پیکربندی شده است.
O	IDS برای پایش تغییرات فایل‌های حیاتی بر روی سرویس‌دهنده پست الکترونیکی (مبنی بر میزبان یا فایل بررسی‌کننده یکپارچه شبکه) پیکربندی شده است .
O	IDS آدرس‌های IP یا زیر شبکه‌هایی که به شبکه‌های سازمانی حمله می‌کنند (در ارتباط با فایروال) بلوکه می‌کند.
O	IDS شبکه یا مدیر سرویس‌دهنده پست الکترونیکی را ازحملات از طریق ابزارهای مناسب آگاه می‌سازد.
O	IDS برای تشخیص پورت اسکن کاوش‌ها پیکربندی می‌شود.
O	IDS برای تشخیص حملات DOS پیکربندی می‌شود.
O	IDS برای ثبت وقایع پیکربندی می‌شود.
O	IDS بارها با امضای حمله جدید (بر مبنای هفتگی) بروز رسانی می‌شود.
O	IDS برای پایش بر منابع سامانه‌های موجود در میزبان سرویس‌دهنده پست الکترونیکی پیکربندی می‌شود (مبنی بر میزبان).
	سوئیچ‌های شبکه
O	سوئیچ‌های شبکه در بخش شبکه سرویس‌دهنده پست الکترونیکی برای حفاظت در برابر استراق سمع شبکه استفاده می‌شود.
O	سوئیچ‌های شبکه در بالاترین حالت امنیتی برای شکست حقه بازی ARP و حملات مسموم ARP پیکربندی می‌شود.
O	سوئیچ‌های شبکه برای ارسال تمام ترافیک روی بخش شبکه به میزبان IDS پیکربندی می‌شود (مبنی بر شبکه).

ت-۴ فهرست بررسی امنیت سرویس‌گیرنده پست الکترونیکی

تکمیل	اقدام
	الحاق و بروز رسانی سرویس گیرنده پست الکترونیکی
O	بروز رسانی سرویس‌گیرنده پست الکترونیکی به امن‌ترین نسخه
O	اعمال هر گونه الحاق ضروری به سرویس‌گیرنده پست الکترونیکی
O	اعمال هر گونه الحاق ضروری به مرورگر (برای سرویس‌گیرنده پست الکترونیکی که با مرورگر یکپارچه شده‌اند (به‌عنوان مثال outlook و Netscap)
	امنیت سرویس گیرنده پست الکترونیکی
O	اطمینان از سیستم عامل بروز شده به امن‌ترین سطح الحاق.

ادامه جدول ت-۴

O	پیکربندی سیستم عامل برای اجازه دسترسی تنها برای کاربران مناسب به پیام‌های ذخیره‌شده محلی و فایل‌های پیکربندی سرویس‌گیرنده پست الکترونیکی.
O	تامین یا حذف اسکریپت ویندوزهای میزبان (فقط ویندوزهای میزبان).
O	تغییر عمل پیش‌فرض به فایل‌های مرتبط با اسکریپت ویندوز میزبان از اجرا تا ویرایش (فقط ویندوزهای میزبان).
O	اطمینان از این‌که سیستم عامل برای نمایش تمام پسوندهای فایل پیکربندی شده است (فقط ویندوزهای میزبان).
O	اطمینان از سیستم عاملی که حداقل امتیاز مفهوم را اجرا می‌کند برای این‌که کدهای مخرب در زمینه امنیتی که بر روی آن آغاز شده است اجرا می‌شوند (به‌عنوان مثال سطح دسترسی کاربر).
O	اطمینان مولفه‌های حیاتی از سیستم عامل از کدهای مخرب محافظت می‌شوند.
O	استفاده از فایل رمزگذاری سامانه برای محافظت از پست الکترونیکی ذخیره‌شده محلی بر روی درایو دیسک سخت کاربر (مخصوصاً برای رایانه‌های لپ تاپ مهم است).
O	پیکربندی سیستم عامل سرویس‌گیرنده برای قفل خودکار بعد از یک دوره ثابت عدم‌فعالیت.

ت-۵ مدیریت ایمن و سرویس‌دهنده پست الکترونیکی

تکمیل	اقدام
	ورود به سیستم
O	ثبت خطاهای تنظیم پشته IP.
O	ثبت برطرف‌کننده مشکلات پیکربندی (به‌عنوان مثال: DNS، NIS، WINS).
O	ثبت خطاهای پیکربندی سرویس‌دهنده پست الکترونیکی (به‌عنوان مثال، عدم تطابق با DNS، خطاهای پیکربندی محلی، پایگاه داده مستعاراز مد افتاده).
O	ثبت فایل معیوب و مجوز مسیرها، میانبرهای نا امن، و پیوندهای قوی.
O	ثبت پایگاه داده مستعار از مد افتاده.
O	ثبت کمبود منابع سیستم (به‌عنوان مثال فضای دیسک، حافظه، پردازشگر).
O	ثبت پایگاه داده مستعار بازسازی شده.
O	ثبت ورود به سامانه‌ها (موفق و شکست خورده).
O	ثبت مشکلات امنیتی (به‌عنوان مثال هرزنامه).
O	ثبت ارتباطات از دست رفته (مشکلات شبکه).
O	ثبت شکست‌های پروتکل.
O	ثبت وقفه‌های ارتباط.
O	ثبت عدم پذیرش ارتباط.

ادامه جدول ت-۵

O	ثبت استفاده از دستورات VRFY و EXPN.
O	ثبت ارسال به نیابت از طرف.
O	ثبت ارسال به‌عنوان.
O	ثبت دانلود.
O	ثبت آدرس‌های ناهنجار.
O	ثبت آمار جمع‌آوری پیام.
O	ثبت ایجاد پیام‌های خطا.
O	ثبت شکست‌های تحویل (خطاهای دائمی).
O	ثبت پیام‌های معوقه (خطاهای ناپایدار).
O	ذخیره ورود به سامانه میزبان به‌طور جداگانه (Syslog).
O	بایگانی ورود ثبت‌ها مطابق با الزامات سازمانی.
O	بررسی ثبت‌های روزانه.
O	بررسی ثبت‌های هفتگی (برای اکثر روندهای بلند مدت).
O	استفاده از ابزارهای تحلیل خودکار فایل ثبت.
	پشتیبان‌گیری از سرویس‌دهنده پست الکترونیکی
O	ایجاد یک **خط‌مشی** پشتیبان‌گیری از سرویس‌دهنده پست الکترونیکی.
O	پشتیبان‌گیری تدریجی از سرویس‌دهنده پست الکترونیکی روزانه به‌طور هفتگی.
O	پشتیبان‌گیری کامل از سرویس‌دهنده پست الکترونیکی هفتگی به‌طور ماهانه.
	بایگانی پشتیبان‌گیری‌های بازیافتی از یک توافق به‌طور دوره‌ای.
O	مراجعه با **خط‌مشی**‌های امنیتی سازمان (بهتر است این اقدام بر توصیه‌های ارائه‌شده در اینجا مقدم باشد).
O	قطع ارتباط با سامانه‌های به خطر افتاده از شبکه و یا مراحلی که شامل حمله است چنانچه می‌توان شواهد اضافی را جمع‌آوری کرد.
O	رسیدگی به میزبان‌های مشابه برای تعیین در صورتی‌که مهاجم سامانه‌های دیگر را به خطر بیندازد.
O	مشورت با مدیریت، مشاور حقوقی و اجرای قوانین مناسب (ارتباط با اجرای قوانین فوری در صورتیکه پیگرد قانونی مد نظر باشد).
O	تحلیل نفوذ.

ادامه جدول ت-۵

O	بازگرداندن سامانه.
O	ارتباط مجدد سامانه به شبکه.
O	بررسی سامانه جهت اطمینان از امنیت.
O	پایش سامانه و شبکه بر نشانه‌هایی از تلاش دسترسی دوباره مهاجم به شبکه یا سامانه.
O	مستندات دروس آموخته شده.

پیوست ث

(اطلاعاتی)

فهرست‌های بررسی برای خدمات صفحات وب امن

فهرست زیر برای پشتیبانی از طرح‌ریزی، نصب و راه‌اندازی سرویس‌دهنده وب ایمن مورد نظر است.

ث-۱ فهرست سیستم‌عامل سرویس‌دهنده وب

تکمیل	اقدام
	طرح‌ریزی وپیکربندی و آرایش سرویس‌دهنده وب
O	شناسایی توابعی از سرویس‌دهنده وب
O	شناسایی رده‌هایی از اطلاعات که از طریق سرویس‌دهنده وب ذخیره، پردازش و انتقال داده خواهند شد.
O	شناسایی الزامات امنیتی از اطلاعات.
O	شناسایی چگونگی اطلاعات منتشر شده به سرویس‌دهنده وب.
O	شناسایی میزبان اختصاصی برای اجرای سرویس‌دهنده وب.
O	شناسایی خدمات شبکه که ارائه داده خواهد شد و یا توسط سرویس دهنده وب پشتیبانی خواهد شد.
O	شناسایی کاربران و رده‌هایی از کاربران سرویس‌دهنده وب و تعیین امتیاز برای هر رده از کاربر.
O	شناسایی روش‌های کاربران مجاز برای سرویس‌دهنده وب.
	انتخاب سیستم عامل مناسب برای سرویس‌دهنده وب
	قرار گرفتن در معرض حداقل آسیب‌پذیری‌ها
O	اعمال محدودیت اجرایی یا فعالیت‌های سطح ریشه فقط برای کاربران مجاز.
O	اعمال رد دسترسی به اطلاعات در سرویس‌دهنده دیگری که برای دسترسی در نظر گرفته شده است.
O	اعمال غیرفعال‌کردن خدمات شبکه غیرضروری که ممکن است درون سیستم عامل یا نرم‌افزار سرویس‌دهنده ایجاد شود.
O	هزینه‌های قابل‌قبول برای بیمه و تعهد (بعضی از شرکت‌های بیمه بیش از سیستم عامل معین تعهد دارند).
O	گماشتن کارکنان باتجربه در دسترس برای نصب، پیکربندی، امنیت و نگهداری سیستم عامل.
	الحاق و ارتقاء سیستم عامل
O	شناسایی و نصب تمام الحاق‌های ضروری و ارتقاء برای سیستم عامل.
O	شناسایی و نصب تمام الحاق‌های ضروری و ارتقاء برای برنامه‌های کاربردی و خدمات شامل سیستم عامل.
O	حذف یا غیرفعال کردن خدمات غیرضروری و برنامه‌های کاربردی

ادامه جدول ث-۱

O	غیرفعال کردن یا حذف خدمات غیرضروری و برنامه‌های کاربردی.
O	پیکربندی سیستم عامل تصدیق کاربر
O	حذف یا غیرفعال کردن حساب‌ها یا گروه‌های پیش‌فرض موردنیاز.
O	غیرفعال کردن حساب‌های غیرتعاملی.
O	ایجاد گروه‌های کاربری برای رایانه‌های خاص.
O	ایجاد حساب‌های کاربری برای رایانه‌های خاص.
O	بررسی خط‌مشی کلمه عبور سازمان و تنظیم کلمات عبور حساب‌ها به‌طور مناسب (به‌عنوان مثال: طول و پیچیدگی).
O	پیکربندی رایانه برای رد کردن ورود به سامانه پس از تعداد محدودی از شکست تلاش‌ها.
O	نصب و پیکربندی مکانیسم‌های امنیتی دیگر برای تقویت تصدیق .
	آزمون امنیت سیستم عامل
O	آزمون سیستم عامل بعد از نصب اولیه برای تعیین آسیب‌پذیری‌ها.
O	آزمون دوره‌ای سیستم عامل (به‌عنوان مثال هر سه ماه یکبار) برای تعین آسیب‌پذیری‌های جدید.

ث-۲ فهرست پیکربندی و نصب مطمئن سرویس‌دهنده وب

تکمیل	اقدام
	نصب مطمئن سرویس‌دهنده وب
O	نصب نرم‌افزار سرویس‌دهنده بر روی سرویس‌دهنده وب.
O	نصب حداقل خدمات اینترنتی موردنیاز.
O	اعمال هر الحاق یا ارتقاء برای تصحیح آسیب‌پذیری‌های شناخته شده.
O	ایجاد دیسک فیزیکی یا بخش منطقی اختصاصی (جدا از سیستم عامل و برنامه‌های کاربردی سرویس‌دهنده) برای محتوی وب سایت.
O	حذف یا غیرفعال‌کردن تمام خدمات نصب‌شده توسط برنامه کاربردی سرویس‌دهنده وب اما ضروری نیست (به‌عنوان مثال گروهبندی کننده، پروتکل انتقال فایل (FTP)، مدیریت از راه دور).
O	حذف تمام اسناد نمونه، اسکریپت‌ها و کدهای اجرایی.
O	حذف تمام اسناد فروشنده از روی سرویس‌دهنده.
O	اعمال قالب امنیتی مناسب یا سخت‌شدن اسکریپت به سرویس‌دهنده.
O	پیکربندی مجدد بنر خدمات HTTP (و غیره درصورت لزوم) نه با گزارش سرویس‌دهنده وب و نوع و نسخه سیستم عامل.

ادامه جدول ث-۲

	پیکربندی کنترل‌های دسترسی سیستم عامل میزبان سرویس‌دهنده وب
O	طوری پیکربندی شده است که محتوی فایل‌های وب توسط فرآیندهای خدمات وب می‌توانند خوانده شوند اما نوشته نمی‌شوند.
O	طوری پیکربندی شده است که فرآیندهای خدمات وب در مسیرهایی که در آن محتوی وب عمومی ذخیره شده نمی‌توانند نوشته شوند.
O	طوری پیکربندی شده است که فقط فرآیندهای مجاز برای اداره سرویس‌دهنده وب می‌توانند فایل‌های محتوی وب را بنویسند.
O	طوری پیکربندی شده است که برنامه‌های کاربردی وب می‌توانند ثبت فایل‌های سرویس دهنده وب را بنویسند.
O	طوری پیکربندی شده است که فایل‌های ایجاد شده موقتی توسط برنامه‌های کاربردی سرویس‌دهنده وب به مسیر های فرعی محافظت‌شده مناسب و مشخص‌شده، محدود شده‌اند.
O	طوری پیکربندی شده است که فایل‌های موقتی ایجاد شده در دسترس توسط برنامه‌کاربردی سرویس‌دهنده وب به فرآیند خدمات وب که این فایل‌هارا ایجاد کرده محدود شده‌اند اما ثبت فایل‌ها نمی‌توانند توسط برنامه‌های کاربردی سرویس‌دهنده وب خوانده شوند.
O	با محتوی وب بر روی درایو سخت یا بخش منطقی از سیستم عامل و برنامه کاربردی وب نصب شده است
O	طوری پیکربندی شده است که اگر ارسال فایل به سرویس‌دهنده وب اجازه داده شود اندازه‌ای برای آن قرار داده می‌شود که مقداری از فضای دیسک سخت برای این منظور اختصاص داده شود.
O	طوری پیکربندی شده‌است که ثبت فایل‌ها در محلی که اندازه آن مناسب است، ذخیره شود.
	پیکربندی مسیر محتوی وب امن
O	درایو دیسک سخت یا بخش منطقی برای محتوی وب ایجاد شده، اختصاص یافته است زیرا مسیرهای مرتبط منحصراً برای فایل‌های محتوی سرویس‌دهنده وب از جمله گرافیک به استثنای اسکریپت‌ها و برنامه‌های دیگر است.
O	تعریف مسیر واحد منحصراً برای تمام اسکریپت‌های خارجی یا برنامه‌های اجرا شده به‌عنوان بخشی از محتوی سرویس‌دهنده وب (به‌عنوان مثال CGI و ASP) می‌باشد.
O	غیرفعال‌کردن اجرای اسکریپت‌ها که منحصراً تحت کنترل حساب‌هاب اداری نیستند این عمل با ایجاد و کنترل دسترسی به مسیر جداگانه مورد نظر شامل اسکریپت‌های مجاز انجام می‌شود.
O	ایجاد گروه‌های کاربری برای رایانه.
O	غیرفعال‌کردن استفاده از پیوندهای سخت یا نمادین (با نام مستعار، کلیدهای میانبر برای ویندوز).
O	تعریف ماتریس دسترسی کامل به محتوی وب، شناسایی پوشه‌ها و بر هم‌زدن درون سند سرویس‌دهنده وب که محدود شده و در دسترس هستند (و توسط چه کسی).
O	بررسی خط‌مشی کلمه عبور سازمان، و تنظیم کلمه عبور مناسب حساب (به‌عنوان مثال: طول، پیچیدگی).
O	استفاده از فایل robots.txt در صورت لزوم.

ادامه جدول ث-۵

	استفاده از شبکه یکپارچه
O	نصب فایل بررسی یکپارچگی برای حفاظت از فایل‌های پیکربندی سرویس‌دهنده وب، فایل‌های کلمه عبور محتوی وب.
O	بروزرسانی فایل مجموعه بررسی یکپارچه هر زمان که ارتقاء یا تغییری در محتوی رخ دهد.
O	ذخیره مجموعه بررسی بر روی رسانه حفاظت شده یکبار نوشته شده.
O	مقایسه منظم مجموعه بررسی.

ث-۳ فهرست بررسی محتوای وب

تکمیل	اقدام
	اطمینان از انواع اطلاعات زیر از طریق یک سرویس‌دهنده وب عمومی در دسترس نیست.
O	سوابق نفوذپذیر یا طبقه‌بندی شده.
O	قوانین و شیوه‌های کارکنان داخلی.
O	اطلاعات محرمانه یا اختصاصی.
O	سوابق تحقیقاتی.
O	سوابق مالی (فراتر از این‌که قبلاً در دسترس عمومی بوده‌اند).
O	فیزیک سازمان‌ها و روش‌های امنیت اطلاعات.
O	اطلاعاتی در مورد شبکه سازمان و اطلاعات زیرساخت‌های سامانه.
O	مواد چاپ‌شده بدون اجازه کتبی از مالک.
O	خط‌مشی‌های امنیتی و خصوصی که نشان‌دهنده نوع اقدامات امنیتی در محل است.
	ایجاد خط‌مشی رسمی مستند گسترده سازمانی و فرآیندی برای تصویب محتوی وب عمومی آن
O	شناسایی اطلاعات که بهتر است بر روی وب منتشر شود.
O	شناسایی مخاطبان هدف.
O	شناسایی انشعابات احتمالی منفی از انتشار اطلاعات.
O	شناسایی اینکه بهتر است چه کسی مسؤل ایجاد و انتشار این اطلاعات باشد.
O	فراهم کردن راهنماهایی در سبک‌ها وقالب‌های مناسب برای انتشار وب.
O	فراهم کردن بررسی مناسب اطلاعات برای حساسیت و کنترل‌های توزیع انتشار (حساسیت‌ها شامل اطلاعات مجموعه است).
O	تعیین دسترسی مناسب و کنترل‌های امنیتی.

ادامه جدول ث-۳

O	فراهم‌کردن راهنما بر روی اطلاعات موجود در کد منبع از محتوی وب.
O	ملاحظات حریم خصوصی کاربران وب
O	خط‌مشی حریم خصوصی منتشر شده.
O	ممنوعیت جمع‌آوری داده‌های شناسایی شخصی بدون اجازه صریح کاربر.
O	ممنوعیت استفاده از کوکی‌های (cooki) ماندگار.
O	استفاده از کوکی جلسه، در صورت استفاده به وضوح در خط‌مشی حریم خصوصی منتشرشده، مشخص می‌شود.
	سمت سرویس‌گیرنده ملاحظات امنیتی محتوی را فعال می‌کند
O	فقط زمانی استفاده می‌شود که کاملاً موردنیاز باشد.
O	اقدامات صورت‌گرفته‌ای بدون مجوز صریح کاربر وجود ندارد.
O	استفاده از محتوی فعال سمت سرویس‌گیرنده پرخطر وجود ندارد.
O	هنگامی‌که گزینه‌های دیگر ممکن، فراهم می‌شود (به‌عنوان مثال: متن واضح و آشکار همراه با PDF فراهم می‌شود).
	سمت سرویس‌دهنده ملاحظات امنیتی محتوی را فعال می‌کند
O	درک آسان و ساده.
O	محدود کردن یا نخواندن یا ننوشتن از فایل‌ها.
O	محدود کردن یا تعامل نکردن با دیگر برنامه‌ها (به‌عنوان مثال ارسال پست الکترونیکی).
O	الزاماتی برای اجرا با امتیازات تنظیم شماره شناسایی کاربر (suid) وجود ندارد.
O	استفاده از نام‌های مسیر به‌طور صریح (به‌عنوان مثال بر مسیر متغیر تکیه نمی‌شود).
O	هیچ مسیر، هر دو مجوز نوشتن و اجرا را ندارند.
O	همه فایل‌های اجرایی در پوشه‌های اختصاصی قرار داده شده‌اند.
O	SSIS غیرفعال می‌شود.
O	همه ورودی کاربران دارای اعتبار است.
O	صفحه‌های پویای ایجاد شده، کاراکترهای خطرناک را ایجاد نمی‌کند.
O	بهتر است رمز گذاری مجموعه کاراکترها به‌طور واضح در هر صفحه تنظیم شوند.
O	بهتر است اطلاعات کاربران برای توالی بایت و به‌منظور کاراکترهای خاص برای طرح کدگذاری داده شده، اسکن شوند.
O	کوکی‌ها بهتر است برای هر کاراکتر خاص مورد بررسی قرار گیرد.
O	مکانیسم رمزنگاری برای رمزگذاری کلمات عبور وارد شده از طریق فرم‌های اسکریپت استفاده شده است.

ادامه جدول ث-۳

O	برای برنامه‌های کاربردی وب که توسط نام کاربری و کلمه عبور محدود شده‌اند هیچ یک از صفحات وب در این برنامه کاربردی باید بدون رفتن از طریق فرآیند ورود به سامانه مناسب در دسترس نباشند.
O	تمام نمونه‌های اسکریپت‌ها حذف می‌شوند.
O	هیچ اسکریپت شخص ثالث یا کدهای قابل‌اجرایی بدون تائید کد منبع استفاده نمی‌شوند.

ث-۴ تصدیق وب و فهرست رمزنگاری

تکمیل	اقدام
	تصدیق وب و فن‌آوری رمز نگاری
O	برای منابع وب به حداقل حفاظت نیاز است و برای هر کدام، یک پیکربندی کوچک، تعیین مخاطبان به‌طور واضح، تصدیق مبنی بر آدرس وجود دارد.
O	برای منابع وب حفاظت اضافی نیاز است اما برای هر کدام، یک پیکربندی کوچک، تعیین مخاطبان به‌طور واضح، تصدیق مبنی بر آدرس به عنوان خط دوم دفاعی وجود دارد.
O	برای منابع وب حداقل حفاظت مورد نیاز است اما برای هر کدام تعیین مخاطبان به‌طور واضح، پیکربندی اساسی یا تصدیق خلاصه وجود ندارد.
O	برای منابع وب حفاظت در برابر بمباران‌های مخرب، پیکربندی اساسی یا تصدیق خلاصه موردنیاز است.
	پیکربندی SSL/TLS
O	برای پیکربندی‌ها نیاز به حداقل تصدیق است اما نیازمند رمز نگاری، استفاده از گواهی خود امضا نیز است.
O	برای پیکربندی‌ها نیاز به تصدیق سرویس‌دهنده و رمزنگاری و استفاده از گواهی صادرشده از شخص ثالث است
O	برای پیکربندی‌ها نیاز به سطح متوسطی از تصدیق سرویس‌گیرنده است، پیکربندی سرویس‌دهنده نیازمند نام کاربری و کلمه عبور از طریق SSL/TLS است.
O	برای پیکربندی‌ها نیاز به سطح بالاتری از تصدیق سرویس‌گیرنده است، پیکربندی سرویس‌دهنده نیازمند گواهی سرویس‌گیرنده از طریق SSL/TLS است.
O	برای سازمان‌ها نیاز به سطح متوسط از رمزنگاری، استفاده از DES است.
O	برای سازمان‌ها نیاز به سطح بالایی از رمزنگاری، استفاده از RC4 (بالاتر) یا 3DES (بالاترین) است.
O	پیکربندی شبکه بررسی‌کننده یکپارچگی فایل برای پایش به گواهی سرویس‌دهنده وب.
O	در صورتی‌که SSL/TLS در سرویس‌دهنده وب مورد استفاده قرارگیرد مطمئن باشید که دسترسی از طریق پورت ۸۰ ، TCP غیرفعال است.
O	اگر بیشتر ترافیک در سرویس‌دهنده وب از طریق SSL/TLS رمزنگاری شود مطمئن باشید که مکانیسم‌های ورود به سامانه و آشکارسازی مناسب در سرویس‌دهنده وب به‌کار گرفته شده است (برای اینکه پایش شبکه در برابر جلسه SSL/TLS رمزنگاری شده بی‌اثر است).

ث-۵ فهرست بررسی زیرساخت‌های شبکه

تکمیل	اقدام
	محل شبکه
O	سرویس‌دهنده وب در یک DMZ یا برون‌سپاری به یک سازمان قرار گرفته که برای محافظت از فایروال مناسب است.
O	این DMZ بر اساس رابط سوم (یا بیشتر) در فایروال قرار نگرفته است.
	پیکر بندی فایروال
O	سرویس‌دهنده وب توسط فایروال حفاظت شده است.
O	سرویس‌دهنده وب در صورتی‌که با تهدید بزرگی مواجه شود یا آسیب‌پذیر باشد توسط یک لایه کاربردی فایروال حفاظت می‌شود.
O	فایروال همه ترافیک‌های میان اینترنت و سرویس‌دهنده وب را کنترل می‌کند.
O	فایروال همه ترافیک‌های ورودی به سرویس‌دهنده وب به‌جز پورت TCP (HTTP)80 و یا 443 (HTTPS) را بلوکه می‌کند.
O	فایروال آدرس‌های IP (در رابطه با IDS) یا زیر شبکه‌هایی که گزارش حمله به شبکه‌های سازمانی می‌کند را بلوکه می‌کند.
O	فایروال مدیران وب و شبکه را از فعالیت مشکوک از طریق وسایل مناسب آگاه می‌سازد.
O	فایروال محتوی فیلتر کردن را ارائه می‌دهد.
O	فایروال برای حفاظت در برابر حملات خدمات، پیکربندی شده است.
O	فایروال حمله درخواست‌های URL شناخته شده و ناهنجار را کشف می‌کند.
O	فایروال رویدادهای بحرانی و حیاتی را ثبت می‌کند.
O	فایروال و سیستم عامل فایروال به آخرین و امن‌ترین سطح وصل می‌شود.
	سامانه‌های تشخیص نفوذ IDS
O	IDS مبتنی بر میزبان برای سرویس‌دهنده وب است که عمل اولیه SSL/TLS را انجام دهد.
O	IDS پیکربندی‌شده برای پایش بر ترافیک شبکه، قبل از هرگونه فایروال یا مسیر یاب فیلتر می‌شود (مبتنی بر شبکه است).
O	IDS پیکربندی شده ناظرترافیک شبکه به و از سرویس‌دهنده پس از فایروال است.
O	IDS پیکربندی شده برای پایش بر تغییرات فایل‌های حیاتی بر روی سرویس‌دهنده وب است (مبتنی بر میزبان و یا جستجوگر یکپارچه فایل).
O	IDS آدرس‌های IP (در ارتباط با فایروال) یا زیرشبکه‌هایی که در حال حمله به شبکه‌های سازمانی هستند را بلوکه می‌کند.
O	IDS شبکه و مدیر وب را از حملات، از طریق وسایل مناسب را آگاه می‌سازد.
O	IDS پیکر بندی‌شده برای تشخیص کاوش‌های اسکن پورت است.
O	IDS پیکر بندی‌شده برای تشخیص DOS است.

ادامه جدول ث-۵

O	IDS پیکر بندی‌شده برای تشخیص درخواست‌های URL ناهنجار است.
O	IDS پیکر بندی‌شده برای ثبت رویدادها است.
O	IDS غالباً با امضای حمله جدید بروز رسانی شده‌است (هر هفته).
O	IDS پیکر بندی شده برای پایش بر منابع سامانه در دسترس بر روی میزبان سرویس‌دهنده وب است(مبتنی بر میزبان).
	سوئیچ‌های شبکه
O	سوئیچ‌های شبکه بر روی بخش شبکه سرویس‌دهنده وب برای حفاظت در برابر استراق سمع شبکه استفاده می‌شود.
O	سوئیچ‌های شبکه در حالت امنیتی بالا برای شکست حقه‌های ARP و حملات مسموم ARP پیکربندی می‌شود.
O	سوئیچ‌های شبکه برای ارسال همه ترافیک در بخش شبکه به میزبان IDS (مبتنی بر شبکه) پیکربندی می‌شود.

ث-۶ فهرست بررسی‌های سرویس‌دهنده وب امن

	ورود به سامانه
O	استفاده از قالب ثبت ترکیب شده برای ذخیره ثبت به انتقالات و یا پیکربندی دستی اطلاعات مشروح توسط قالب ثبت ترکیب شده، قالب استانداردی برای ورود به انتقالات می‌شود.
O	فعال‌کردن ارجاع‌دهنده ثبت یا عامل ثبت در صورتی‌که قالب ثبت ترکیب شده در دسترس نباشد.
O	ایجاد نام ثبت فایل مختلف برای وب سایت‌های مجازی مختلف که ممکن است به‌عنوان بخشی از یک سرویس‌دهنده وب فیزیکی واحد، پیاده‌سازی شود.
O	استفاده از شناسایی کاربر از راه دور که در RFC 1413 مشخص شده است.
	ذخیره ثبت‌ها بر روی میزبان‌های جداگانه (syslog).
O	بایگانی ثبت مطابق الزامات سازمان.
O	بررسی ثبت به‌طور روزانه.
O	بررسی ثبت به‌طور هفتگی (برای روند بلند مدت).
O	استفاده از ابزارهای تحلیل فایل ثبت خودکار.
	پشتیبانی از سرویس‌دهنده وب
O	ایجاد یک خط‌مشی پشتیبانی سرویس‌دهنده وب.
O	پشتیبانی تدریجی از سرویس‌دهنده وب مبنی بر روزانه تا هفتگی.
O	پشتیبانی کامل از سرویس‌دهنده وب مبنی بر هفتگی تا ماهانه.
O	پشتیبانی بایگانی به‌طور دوره‌ای.

O	نگهداری کپی معتبر از وب سایت‌ها.
	بازیابی از یک سازش
O	مشورت خط‌مشی‌های امنیتی سازمان (بهتر است این کار در اینجا مقدم بر توصیه‌های ارائه شده باشد).
O	قطع سامانه‌های به خطر افتاده از شبکه یا انجام مراحلی شامل حمله، تا اندازه‌ای که شواهد اضافی را به‌توان جمع‌آوری کرد.
O	بررسی دیگر میزبان‌های مشابه برای تعیین، در صورتی‌که مهاجم سامانه‌های دیگر را نیز به خطر بیاندازد.
O	مشورت با مدیریت، مشاور حقوقی، اجرای قانون به‌صورت مناسب (تماس با اجرای فوری در صورتی‌که پیگرد قانونی مدنظر باشد).
O	تحلیل نفوذ.
O	بازگرداندن سامانه.
O	ارتباط مجدد سامانه با شبکه.
O	آزمون سامانه برای اطمینان از امنیت.
O	پایش بر سامانه و شبکه برای اشاره به مهاجم که تلاش دوباره برای دسترسی به سامانه و شبکه دارد.
O	مستندات دروس آموخته شده.
	آزمون امنیت
O	اسکن‌های آسیب‌پذیر به‌طور دوره‌ای بر روی سرویس‌دهنده وب و شبکه، پشتیبانی از شبکه را انجام می‌دهد.
O	بروزرسانی اسکنر آسیب‌پذیر قبل از آزمون.
O	تصحیح هر کمبود شناسایی‌شده توسط اسکنر آسیب‌پذیر.
	مدیریت از راه دور و بروز رسانی محتوی
O	استفاده از مکانیسم تصدیق قوی (به‌عنوان مثال جفت کلید عمومی، خصوصی، دو عامل تائید هویت).
O	محدودکردن میزبان که برای اداره یا بروزرسانی محتوی از راه دور بر روی سرویس‌دهنده وب توسط آدرس IP و شبکه داخلی می‌تواند استفاده شود.
O	استفاده از پروتکل‌های امن (به‌عنوان مثال پوسته امن، HTTPS).
O	اجرای مفهوم حداقل امتیاز در مدیریت از راه دور و بروزرسانی محتوی (به‌عنوان مثال تلاش برای حداقل‌رساندن حقوق دسترسی برای مدیریت از راه دور/ بروز رسانی حساب‌ها).
O	تغییر در حساب‌ها به‌طور پیش فرض یا کلمه‌های عبور با کاربرد مدیریت از راه دور یا برنامه کاربردی.
O	اجازه ندادن به مدیریت از راه دور از اینترنت از طریق فایروال
O	نصب نکردن سهم هر فایل بر روی شبکه داخلی از سرویس‌دهنده وب یا برعکس.

پیوست ج

(اطلاعاتی)

فهرست‌های بررسی امنیت شبکه محلی بی‌سیم

تکمیل	اقدام
O	توسعه خط‌مشی امنیتی سازمان که استفاده از فن‌آوری بی‌سیم را نشان می‌دهد.
O	اطمینان از کاربران در شبکه که به‌طور کامل در آگاهی امنیت رایانه آموزش داده شده‌اند.
O	انجام یک ارزیابی پرخطر برای درک ارزش دارایی‌ها در سازمان که نیازمند حمایت هستند.
O	اطمینان از اینکه سرویس‌گیرنده NIC و نرم‌افزار دائمی پشتیبان IP ارتقا می‌یابد به‌طوریکه الحاق‌های امنیتی ممکن است به‌عنوان رخداد موجود، گسترش یافته باشد (قبل از خرید).
O	انجام ارزیابی‌های امنیتی جامع در فواصل منظم (شامل اعتباری که نقطه دسترسی خارج از قاعده در 802.11 WLAN وجود ندارد).
O	اطمینان از حفاظت مرز خارجی در محل در اطراف محیط یا ساختمان سازمان.
O	تکمیل نظرسنجی سایت برای سنجش و ایجاد پوشش AP برای سازمان.
O	نگاهی به موجودی کامل از تمام APها و دستگاه‌های بی‌سیم 802.11.
O	آزمون تجربی مرزهای محدوده AP برای تعیین میزان دقیق پوشش بی‌سیم.
O	اطمینان از کانال‌های AP که حداقل پنج کانال مختلف از هر گونه شبکه‌های بی‌سیم نزدیک برای جلوگیری از تداخل.
O	تعیین محل APها در داخل ساختمان در مقابل دیوارهای خارجی و پنجره‌های نزدیک.
O	تعیین محل APها درمناطق امن برای جلوگیری از دسترسی فیزیکی غیرمجاز و دستکاری کاربر.
O	ایجاد اطمینان از اینکه APها در تمام ساعاتی که استفاده نمی‌شده‌اند، تبدیل شده‌اند.
O	ایجاد اطمینان از اینکه تنظیم مجدد تابع برروی APها فقط در زمان نیاز استفاده و تنها به گروهی از افراد مجاز استناد می‌شود.
O	باز گرداندن AP به حداقل تنظیمات امنیتی زمانی که توابع تنظیم مجدد استفاده می‌شود.
O	تغییر SSID پیش فرض در AP به مقداری که به آسانی قابل حدس نباشد.
O	غیرفعال‌کردن ویژگی پخش SSID به‌طوری‌که سرویس‌گیرنده SSID باید مطابق AP باشد.
O	اعتبار سنجی رشته کاراکتر SSID که نام سازمان یا محصولات را منعکس نمی‌کند (بخش، اداره، خیابان، غیره).
O	غیرفعال کردن انتشار becon (بسته ای است که در صورت عدم تشخیص دریافت نشانه از ایستگاه تولید می‌شود) از AP
O	درک و ایجاد اطمینان از همه پارامترهای پیش‌فرض تغییر داده شده
O	غیرفعال کردن همه پروتکل‌های مدیریتی، غیر ضروری و ناامن در AP .

ادامه جدول

O	فعال‌کردن تمام ویژگی‌های امنیتی از محصولات WLAN شامل تصدیق پنهانی و ویژگی حریم خصوصی WEP/WPA.
O	اطمینان از اندازه کلیدهای رمزنگاری که حداقل ۱۲۸ بیت یا در صورت امکان بزرگتر است.
O	ایجاد اطمینان از کلیدهای مشترک پیش‌فرض که به‌طور دوره‌ای توسط بیشتر کلیدهای منحصربفرد ایمن جایگزین می‌شوند.
O	نصب فایروال پیکربندی شده درست میان زیرساخت‌های سیمی و شبکه‌های بی‌سیم (AP یا هاب به APها).
O	نصب برنامه ویروس‌کش و نرم‌افزار فایروال شخصی برروی سرویس‌گیرنده‌های بی‌سیم.
O	قرار گرفتن فهرست‌های کنترل دسترسی به آدرس فیزیکی (MAC).
O	قرار گرفتن IPSec مبنی بر فن‌آوری شبکه خصوصی مجازی برای ارتباطات بی‌سیم.
O	اطمینان از رمزنگاری مورد استفاده تا حد امکان حساسیت داده‌ها قوی شده در شبکه و سرعت پردازنده رایانه.
O	اطمینان از تمام کلمه‌های عبور اداری قوی APها و همه کلمات عبور که به‌طور مرتب تغیر یافته‌اند.
O	اطمینان از "ad hoc mod" (یک شبکه غیر متمرکز از شبکه‌های بی‌سیم) برای 802.11 غیرفعال شده است.
O	استفاده از آدرس IP روی شبکه در صورت امکان.
O	استفاده از DHCP با ویژگی رزرو سرویس‌گیرنده.
O	فعال کردن مکانیسم‌های مجاز کاربر برای رابط‌های مدیریت از AP.
O	اطمینان از مدیریت ترافیک معین برای APها که یک زیرشبکه اختصاصی سیمی هستند.

پیوست چ

(اطلاعاتی)

کتابنامه

[1] ISO/IEC TR 13335-4:2000, Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards
[2] ISO/IEC TR 13335-5:2001, Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security
[3] ISO/IEC 17799:2000, Information technology - Code of practice for information security management
[4] ISO/IEC 18033-3, IT security techniques - Encryption algorithms — Part 3: Block ciphers7)
[5] NIST Special Publication 800-44: 2002 Guidelines on Securing Public Web Servers
[6] NIST Special Publication 800-45: 2002 Guidelines on Electronic Mail Security
[7] NIST Special Publication 800-46: 2002 Security for Telecommuting and Broadband Communications
[8] NIST Special Publication 800-48: 2002 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
[9] IETF RFC 768 User Datagram Protocol (1980)
[10] IETF RFC 821 Simple Mail Transfer Protocol (1982)
[11] IETF RFC 959 File Transfer Protocol (1985)
[12] IETF RFC 1055 Nonstandard for transmission of IP datagrams over serial lines: SLIP (1988)
[13] IETF RFC 1334 PPP Authentication Protocol (1992)
[14] IETF RFC 1413 Identification Protocol (1993)
[15] IETF RFC 1939 Post Office Protocol – Version 3 (1996)
[16] IETF RFC 1991 PGP Message Exchange Formats (1996)
[17] IETF RFC 1994PPP Challenge Handshake Authentication Protocol (CHAP) (1996)
[18] IETF RFC 2045 to IETF RFC 2049 Multipurpose Internet Mail Extensions (MIME) (1996)
[19] IETF RFC 2060 Internet Message Access Protocol - Version 4rev1 (1996)
[20] IETF RFC 2131 Dynamic Host Configuration Protocol (1997)
[21] IETF RFC 2139 RADIUS Accounting (1997)
[22] IETF RFC 2246 The TLS Protocol Version 1.0 (1999)
[23] IETF RFC 2284 PPP Extensible Authentication Protocol (EAP) (1998)
[24] IETF RFC 2401 Security Architecture for the Internet Protocol (1998)
[25] IETF RFC 2406 IP Encapsulating Security Payload (ESP) (1998)
[26] IETF RFC 2440 OpenPGP Message Format (1998)
[27] IETF RFC 2631 Diffie-Hellman Key Agreement Method (1999)
[28] IETF RFC 2632 S/MIME Version 3 Certificate Handling (1999)
[29] IETF RFC 2633 S/MIME Version 3 Message Specification (1999)
[30] IETF RFC 2865 Remote Authentication Dial In User Service (RADIUS) (2000)
[31] IETF RFC 3162 RADIUS and IPv6 (2001)
[32] IETF RFC 3369 Cryptographic Message Syntax (CMS) (2002)
[33] IETF RFC 3370 Cryptographic Message Syntax (CMS) Algorithms (2002)