جمهوری اسلامی ایران

اداره کل ارتباطات و فناوری اطلاعات

استان چهارمحال و بختیاری

موضوع:

ملاحظات پدافند غیر عامل

در حوزه‌ی

ارتباطات و فناوری اطلاعات

(ویرایش دوم)

تهیه کننده:

مهندس بهروز بنی طالبی

با همکاری مهندس حمید رئیسیان

ناظر مهندس علیرضا کاظمیان

مهرماه ۹۳


بسم الله الرحمن الرحیم

تقدیم به

به تمام آزاد مردانی که نیک می اندیشند

و عقل و منطق را پیشه ی خود نموده

و جز رضای الهی و پیشرفت و سعادت جامعه، هدفی ندارند.

تشکر و قدردانی:

سپاس بی‌کران پروردگار یکتا را که هستی‌مان بخشید و به طریق علم و دانش رهنمونمان گشت و به هم‌نشینی رهروان علم و دانش مفتخرمان نمود و خوشه‌چینی از علم و معرفت را روزیمان ساخت.

چکیده:

در عصری که به نام ارتباطات نامگذاری شده، بی شک کشورها به اهمیت گسترش فناوری اطلاعات و ارتباطات به‌عنوان ابزاری برای توسعه و افزایش بهره‌وری در تمام حوزه‌ها پی برده‌اند. رشد سریع و در عین حال نامتوازن ساختار ICT، این بستر را به یکی از نقاط بالقوه آسیب پذیر و ناامن در جهان تبدیل کرده است. بنابراین به منظور مصون‌سازی این بستر از تهدیدات موجود و هم‌چنین حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی، توجه و پرداختن به موضوع پدافند غیرعامل در حوزه‌ی ارتباطات و فناوری اطلاعات امری اجتناب ناپذیر است.

پدافند غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت می‌گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد؛ ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند.

کلمات کلیدی: پدافند غیرعامل، ارتباطات و فناوری اطلاعات، اینترنت و فضای سایبری.

فهرست مطالب صفحه

فصل اول: آشنایی با پدافند غیرعامل

فصل دوم: اینترنت و فضای سایبر

فصل سوم: اصول امنیت برنامه‌های وب

فصل چهارم: سامانه مدیریت یکپارچه تهدیدUTM

فصل پنجم: پدافند غیرعامل در مراکز داده

فصل ششم: استانداردهای امنیت اطلاعات

فصل هفتم: پدافند غیرعامل در شبکه ارتباطات ثابت و سیار

فصل هشتم: پدافند غیرعامل در توسعه فیبر نوری

فصل نهم: ملاحظات پدافند غیرعامل در اینترنت ADSL

فصل دهم: پدافند غیرعامل در امنیت فیزیکی و کنترل دسترسی

فهرست شکل‌ها

صفحه

فصل اول

آشنایی با پدافند غیرعامل

۱-۱-مقدمه

پدافند غیرعامل با مفهوم کلی دفاع در برابر تهاجم، بدون استفاده از سلاح و درگیرشدن مستقیم، سابقه‌ای طولانی در تاریخ بشری به قدمت خلقت انسان دارد. انجام اقدامات دفاع غیرعامل در ابعاد گوناگون در حال حاضر در جهت مقابله با تهاجمات دشمن(نظامی و غیرنظامی)، بلاهای طبیعی و غیرطبیعی و تقلیل خسارات ناشی از حملات نظامی دشمن از قبیل: حملات هوایی، زمینی، دریایی و غیرنظامی از جمله حملات سایبری، جنگ نرم و همچنین بلاهای طبیعی نظیر: طوفان، سیل، زلزله و... غیرطبیعی : سرقت و... موضوعی بنیادی است. که وسعت و گستره آن، تمامی زیر ساخت‌های کلیدی، مراکز حیاتی، حساس و مهم نظامی و غیرنظامی کشور از جمله پالایشگاه‌ها، نیروگاه‌ها، بنادر، فرودگاه‌ها، مجتمع‌های بزرگ صنعتی، مراکز بهداشتی و درمانی، قرارگاه‌ها و مراکز عمده فرماندهی نظامی ؛ هدایت و تصمیم گیری‌های سیاسی، مراکز اصلی مخابراتی و ارتباطی، پل‌های استراتژیک، صنایع نظامی، پایگاه‌های هوایی، سایت‌های موشکی، مراکز و ایستگاه‌های رادیویی، تلویزیون، انبارهای عمده مواد غذایی و دارویی، مراکز جمعیتی و قرارگاه‌های تاکتیکی، مقرهای عمده آماری ؛ پشتیبانی و .... را در بر می‌گیرد.

تجارب حاصله از جنگ‌های گذشته از قبیل جنگ ۱۱ هفته‌ای سال ۱۹۹۹ ناتو علیه یوگسلاوی، جنگ سال ۲۰۰۳ آمریکا و انگلیس علیه عراق، جنگ ۳۳ روزه سال ۲۰۰۶ اسرائیل علیه لبنان و دیگر جنگ‌های نظامی و غیرنظامی موید این نظر است که کشور مهاجم جهت درهم شکستن اراده ملت و توان سیاسی، اقتصادی، نظامی و مدیریتی کشور مورد تهاجم با اتخاذ استراتژی انهدام مرکز ثقل، توجه خود را صرف بمباران و انهدام مراکز حیاتی، حساس و مهم می‌نماید. همچنین تجارب حاصله از بلاهای طبیعی به وجود آمده چون زلزله بم در سال۱۳۸۲، سیل گلستان در سال۱۳۸۰و ... در کشور عزیزمان ایران، موید این نظر است. کشورهایی که مورد تهاجم بلاهای طبیعی قرار گرفته‌اند به علت عدم رعایت اصول پدافند غیرعامل دچار خسارت زیاد مالی و جانی شده‌اند.

امروزه کشورهایی که طعم خرابی و خسارات ناشی از جنگ، بلاهای طبیعی و... را چشیده‌اند، جهت حفظ سرمایه‌های ملی و منابع حیاتی خود توجه خاص و ویژه‌ای به دفاع غیرعامل نموده و در راهبرد دفاع خود جایگاه والایی برای آن قائل شده‌اند. غیر از حوادث و بلایای طبیعی، موضوع تهدیدهای درونی و برونی توسط دشمن، یکی از دغدغه‌های پدافند غیر عامل است و در این مبحث وزارت بهداشت ؛ درمان و دانشگاه علوم پزشکی و خدمات بهداشتی درمانی وظیفه خطیری بر عهده دارند. با توجه به حساسیت این موضوع برماست که با استفاده از رهنمودهای رهبر عزیزمان، ولی امر مسلمین و با شناخت ژرف و کامل از ابعاد مختلف پدافند غیرعامل و اتخاذ تمهیداتی برای آن، خود را به مرز آمادگی کامل برسانیم.

۱-۲- تعریف پدافند و انواع آن

پدافند در مفهوم کلی، دفع، خنثی کردن و یا کاهش تاثیرات اقدامات آفندی دشمن و ممانعت از دستیابی به اهداف مورد نظر است. پدافند به دو بخش تقسیم می‌شود:

۱. پدافند عامل[1]

پدافند عامل عبارت از رویارویی و مقابله مستقیم با دشمن و به کارگیری جنگ افزارهای مناسب و موجود به منظور دفع حمله و خنثی کردن اقدامات آفندی دشمن .

۲. پدافند غیرعامل[2]

به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به کارگیری جنگ افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

مجمع تشخیص مصلحت نظام پدافند غیرعامل را این گونه تعریف می‌کند:
مجموعه اقدامات غیر مسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی دشمن می‌شود.

۱-۳. آشنایی با پدافند غیر عامل

۱-۳-۱- تاریخچه پدافند غیر عامل

شکل‌گیری تمدن‌های اولیه در جهان همواره با وقوع جنگ همراه بوده است، در طول تاریخ انسان‌ها از طریق پناه گرفتن در غارها، ساخت جوشن و سپر، ایجاد برج و بارو و قلاع محکم و مرتفع، حفر خندق برای حفظ جان و تامین امنیت گروهی با هدف پیشگیری از حملات غافلگیرانه دشمن اقدام نموده‌اند، دیوارهای دفاعی و خاکریزهای متعلق به آغاز سکونت انسان در ایران هنوز برجاست و شکل آن‌ها به موازات پیشرفت سلاح‌های تهاجمی و تدافعی در هر دوره تاریخی تکامل یافته است.

تفکر ساخت و احداث دیوارها و خطوط و دژهای دفاعی از قدیم الایام به عنوان یک اقدام دفاعی با هدف سد کردن و ایجاد مانع در مسیر تهاجم دشمن و ممانعت از مواجه شدن با حملات

[1] **Active Defense**
[2] **Passive Defense**

غافلگیرانه مورد توجه دولت‌های مختلف بوده و علیرغم تغییر و تکامل سلاح‌ها و روش‌های تهاجمی، کماکان با تغییر شکل و کاربری آن‌ها متناسب با نوع تهدیدات به شکل‌های دیگری همانند تونل‌ها، پناهگاه‌های چندمنظوره، سازه‌های امن زیرزمینی، دیوارها و موانع دفاعی الکترونیکی در ملاحظات دفاعی کشورها مورد توجه خاص قرار دارند[۱].

از جمله مشهورترین دیوارها و دژهای دفاعی احداث شده در طول تاریخ بشری می‌توان دیوار چین(دیوار چین به طول ۲۴۱۵ کیلومتر در سال ۳۶۴ قبل از میلاد احداث گردیده است)، سد ذوالقرنین، دیوار گرگان (دیوار دفاعی گرگان بزرگ ترین دیوار دفاعی جهان، بعد از دیوار چین می‌باشد و همزمان با دیوار چین بنا شده است)، دیوار آتلانتیک (دیوار آتلانتیک، استحکامات ساحلی بود که توسط رایش سوم برای جلوگیری از تهاجم نیروهای متفقین درجنگ جهانی دوم احداث گردید)، دیوار آنتونین، دیوار اورلئان، دیوار صلح بلفاست، دیوار برلین، دیوار لیما، دیوار ماژینو (دیوار ماژینو در مرز فرانسه و آلمان در سال ۱۹۳۰ الی ۱۹۳۵ به طول ۴۰۰ مایل جهت جلوگیری از تهاجم آلمان به سرزمین فرانسه احداث گردید)، دیوار زیگفرید، دیوار مراکش، دیوار ویتنام، دیوار لندن، دیوار کرملین، دیوار بارلو، دیوار اورشلیم و ... را نام برد.

سرزمین گسترده ایران باستان که ایران کنونی بخشی از آن است، به علت موقعیت جغرافیایی که میان دو جلگه آباد بین النهرین و پنجاب سند قرار گرفته بود مانند پلی بود که طوایف مهاجم به طرف شرق یا غرب مجبور می‌شدند از آن عبور کنند زندگی در چنین وضعیت جغرافیایی و محیط ناامن، ایرانیان را وادار نمود تا همواره به منظور در امان ماندن از تجاوز متجاوزین، خانه‌های مسکونی خود را به شکل دژ کوچکی بسازند بنابراین به هر جای این سرزمین نگاه کنید، قلعه، برج، بارو، ارگ، کهندژ، دربند، خندق و دروازه و نظایر آن‌ها از ناامنی محیط زندگی و توجه و تدبیر آگاهانه ایرانیان به ملاحظات دفاعی حکایت دارد. ساخت بناهای گروهی حصاردار در ایران با طرح‌ها و نقشه‌های گوناگون از سه هزار سال پیش شناخته شده است، حصار سیلک در کاشان، قلعه حسنلو در ارومیه، تورنگ در گرگان، تپه حصار در دامغان، نوشیجان تپه بین همدان و ملایر، قلعه بلورآباد در شهرستان خوی و ... از نمونه‌های آن می‌باشد.

ساخت اسب چوبی تروا توسط اودیسیوس یکی از افراد زیرک و هوشمند یونانی در سال ۲۱۲ قبل از میلاد، پس از نومیدی سربازان از تسخیر (سیراکیوز) نیز یکی از اقدامات تاریخی دفاع غیرعامل می‌باشد به گونه‌ای که امروزه از اسب چوبی تروا به عنوان سمبل و نماد فریب یاد می‌شود. اعراب بادیه نشین مانند سایر اقوام چادرنشین با حصار و بناهای دایمی میانه‌ای نداشتند، وجود مبارک پیامبر اسلام (ص) به مدیریت نظامی مفهومی واقعی بخشید و از انواع روش‌ها و تاکتیک‌های جنگی و بهره‌گیری موثر از زمان، مکان و موقعیت مناسب در غزوات برای رویارویی با دشمن و شکست آن‌ها استفاده می‌کرد از جمله روش‌های مورد استفاده در جنگ‌های تهاجمی و تدافعی صدر اسلام بهره گیری از شیوه‌های دفاعی غیرعامل بود که به شکل‌های مختلف در غزوات مورد توجه قرار می‌گرفت [۱].

بهره‌برداری از استتار و اختفاء جهت مخفی و پنهان‌سازی گرچه به قدمت طول تاریخ بشری می‌باشد ولی اهمیت آن در طول جنگ جهانی اول به علت ورود هواپیماهای شناسایی و عکس برداری هوایی و افزایش تدریجی دقت تسلیحات آفندی، مورد توجه جدی قرار گرفت. تا سال (۱۹۰۰) اکثر ارتش‌های دنیا از یونیفورم و لباس‌های نظامی رنگی استفاده می‌نمودند، برای مثال ارتش فرانسه در شروع جنگ جهانی اول از لباس‌های رنگی (کت آبی و شلوار قرمز) استفاده می‌نمود که پس از پی بردن به اهمیت استتار و نقش ارزنده آن در کاهش آسیب پذیری‌ها و تلفات، لباس‌های نظامی به رنگ استتار خاکی و یا سبز، قهوه‌ای و یا ترکیبی از آن‌ها درآمد و این موضوع به تدریج در سایر کشورهای دنیا رایج گردید.

واژه انگلیسی استتار[1] از لغت فرانسوی (Camoufler) به معنی آرایش نمودن اقتباس گردیده و در سال (۱۹۱۷) وارد زبان انگلیسی گردید. ارتش شوروی سابق برای هماهنگ نمودن برنامه‌های فریب و نیرنگ و اقدامات پدافند غیرعامل در برابر تهدیدات آمریکا، در سر فرماندهی کل ارتش شوروی واحد ویژه ای را برای مدیریت و اجرای برنامه‌های دفاع غیرعامل به نام (ماسکیروفکا) تاسیس نمود و در طول سال‌های ۱۹۶۰ الی ۱۹۸۳ اقدامات عمده ای از قبیل آسیب ناپذیر نمودن منابع و مراکز حیاتی و حساس خود در برابر تهاجمات احتمالی، احداث پناهگاه‌های عمیق زیرزمینی برای مردم و هیات حاکمه سیاسی، نگهداری قطعات یدکی و بحرانی در پناهگاه‌های مستحکم زیرزمینی و ساخت ماکت‌های فریب تجهیزات و تسلیحات سازمانی، ایجاد مراکز فرماندهی و کنترل متحرک و طراحی ریل‌های متحرک جهت موشک‌های قاره پیمای (SS-X-24)، ارسال اطلاعات دروغین، عایق‌سازی و استفاده از رنگ‌ها و اقلام جاذب حرارتی ؛ راداری و ... نمود.

اگر اقدامات پدافندغیرعامل را در سیر تاریخ مورد مطالعه قرار دهیم، اقدامات پیشگیرانه ملل مختلف با هدف حفظ جان، ادامه حیات و حفظ سرزمین، هنوز هم در آستانه قرن بیست و یکم که جهان آکنده از منازعات ژئوپلتیک بوده و نشانه‌ای از خاتمه‌ی قریب الوقوع درگیری‌های مسلحانه دیده نمی‌شود، انجام اقدامات پدافند غیرعامل توسط کشورهای مختلف استمرار داشته و جایگاه ویژه‌ای خود را در سیاست‌های دفاعی کشورها و ملل مختلف به عنوان یک نیاز حیاتی حفظ نموده است و با روش‌های مختلف ادامه یافته است.[۱]

۱-۳-۲- اصول پدافند غیر عامل

اصول دفاع غیرعامل، مجموعه اقدامات بنیادی و زیربنایی است که در صورت به کارگیری می‌توان به اهداف پدافند غیرعامل از قبیل، تقلیل خسارات و صدمات، کاهش قابلیت و توانایی سامانه‌های شناسایی و آشکارساز دشمن، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن و تحمیل هزینه بیشتر به وی نایل گردید. این اصول عبارتند از [۲]:

[1] **Camouflage**

- مکان‌یابی[1]

مکان‌یابی، انتخاب بهترین و مطلوبترین نقطه و محل استقرار است به طوری که پنهان و مخفی نمودن نیروی انسانی، وسایل و تجهیزات و فعالیت‌ها را به بهترین وجه امکان‌پذیر سازد. بنابراین اگر مکان‌یابی به خوبی انجام شود، به کارگیری و استفاده از وسایل و ابزار مصنوعی جهت استتار و اختفا ضرورتی پیدا نمی‌کند و یا این ضرورت به حداقل ممکن تقلیل خواهد یافت. تجربه نشان داده است که مکان‌یابی صحیح و مطلوب می‌تواند مقدار بسیار زیادی از معضلات و مشکلات استتار و اختفا را حل و فصل نموده ضمن آن‌که تهدیدات و آسیب‌پذیری‌های احتمالی را نیز کاهش و تقلیل دهد.

- استتار و اختفا[2]

فن و هنری است که با استفاده از وسایل طبیعی یا مصنوعی امکان کشف و شناسایی نیروها، تجهیزات و تأسیسات را از دیده بانی، تجسس و عکس برداری دشمن کاهش داده، مخفی نموده و حفاظت نماید. استتار، همرنگ سازی با محیط و اختفا، استفاده صحیح از عوارض طبیعی و مصنوعی زمین می‌باشد به طوری که تشخیص هدف توسط دشمن به سختی انجام گرفته و یا با تأخیر انجام پذیرد.

- پوشش [3]

پوشش، پنهان سازی و حفاظت تأسیسات، تجهیزات و نیروی انسانی در برابر دید و تیر دشمن می‌باشد.

- فریب [4]

کلیه اقدامات طراحی شده حیله‌گرانه‌ای است که موجب گمراهی و غفلت دشمن در نیل به اطلاعات و محاسبه و براورد صحیح از توان کمی و کیفی طرف مقابل گردد.

- فریب نظامی[5]

[1] Site Selection
[2] Camouflage and Concealment
[3] Cover
[4] Deception
[5] Military Deception

اقداماتی که به منظور گمراه ساختن فرماندهان تصمیم‌گیرنده دشمن انجام می‌شود تا دشمن از توانایی‌ها، اهداف و عملیات نیروهای خودی آگاه نشود، در نتیجه به اقدام (یا عدم اقدام) خاصی مبادرت ورزد که به انجام مأموریت نیروهای خودی کمک خواهد نمود.

- فریب نظامی استراتژیک[1]

فریب نظامی که توسط فرماندهان عالی نظامی و یا در حمایت و پشتیبانی از آنان طراحی و اجرا می‌گردد، این فریب به منظور تأثیرگذاردن بر عملیات، سیاست و خط مشی‌های نظامی دشمن صورت می‌گیرد. چنانچه اهداف فریبنده در یک طرح فریب بسیار گسترده _که هدف آن سردرگمی دشمن در خصوص استراتژی اصلی و یا اهداف استراتژیک باشد_فریب استراتژیک به کار برده می‌شود.

- پراکندگی[2]

گسترش، باز و پخش نمودن و تمرکز زدایی نیروها، تجهیزات، تأسیسات یا فعالیت‌های خودی، به منظور تقلیل آسیب پذیری آن‌ها در مقابل تهدیدات، به طوری که مجموعه ای از آن‌ها هدف واحدی را تشکیل ندهند.

- تفرقه و جابه‌جایی[3]

جداسازی و جابه‌جایی تجهیزات حساس و ارزشمند قابل حمل از یک نقطه به نقطه دیگر جهت کاهش شناسایی و آسیب‌پذیری این اهداف می‌باشد.

- استحکامات[4]

ایجاد هرگونه حفاظ که در مقابل اصابت مستقیم بمب، راکت، موشک، گلوله، توپخانه، خمپاره و یا ترکش آن‌ها مقاومت نموده، مانع صدمه رسیدن به نفرات و یا تجهیزات گردد.

- اعلام خبر [5]

[1] Strategic Military Deception
[2] Dispersion
[3] Separation
[4] Fortification
[5] Early Warning

آگاهی و هشدار به نیروهای خودی مبنی بر این که عملیات تعرضی دشمن نزدیک می‌باشد، این هشدار که برای آماده شدن است ؛ممکن است چند دقیقه، چند ساعت، چند روز و یا زمانی طولانی‌تر از آغاز مخاصمات اعلام گردد. تجهیزات و وسائل اعلام خبر شامل رادار، دیده‌بانی بصری، آژیر، پیام‌ها و آگهی‌های هشدار دهنده از طریق وسایل مختلف از جمله رسانه‌های گروهی می‌باشد.

۱-۳-۳- اهداف پدافند غیر عامل

۱. کاهش قابلیت و توانایی سامانه‌های شناسایی، هدف‌یابی و دقت هدف گیری تسلیحات آفندی دشمن.
۲. تقلیل آسیب‌پذیری و کاهش خسارات و صدمات تأسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم نظامی و غیرنظامی کشور در برابر تهدیدات و حملات دشمن و بلاهای غیر طبیعی.
۳. حفظ سرمایه‌های کلان ملی کشور.
۴. حفظ توان خودی جهت ادامه فعالیت‌ها و تداوم عملیات تولید و خدمات رسانی.
۵. سلب آزادی و ابتکار عمل از دشمن و ایجاد شرایط سخت و دشوار برای وی در صحنه عملیات.
۶. صرفه جویی در هزینه‌های تسلیحاتی و نیروی انسانی.
۷. افزایش آستانه مقاومت مردمی و قوای خودی در برابر تهاجمات دشمن و بلاهای غیر طبیعی.
۸. تحمیل هزینه بیشتر به دشمن از طریق وادار نمودن وی به تلف نمودن منابع محدود خود بر روی اهداف کاذب و فریبنده و سلب اصل صرفه جویی قوا از وی.
۹. بالا بردن توان دفاعی کشور.
۱۰. توزیع ثروت، جمعیت و سرمایه‌های ملی در کل فضای سرزمینی کشور از طریق اعمال سیاست تمرکززدایی، آمایش سرزمینی و پراکندگی زیرساخت‌های کلیدی و مراکز حیاتی، حساس و مهم تولیدی محصولات کلیدی (نیروگاهی، پالایشگاهی، صنعتی، نظامی، غذایی، آبرسانی،بهداشتی)
۱۱. ایجاد آمادگی‌های لازم برای مقابله با دشمن در شرایط تهدیدات نامتقارن.
۱۲. حفظ تمامیت ارضی، امنیت ملی و استقلال کشور.

۱-۴- اهمیت پدافند غیر عامل

۱. موجب زنده ماندن و حفظ بقای نیروی انسانی می‌گردد که با ارزش‌ترین سرمایه و موجودیت ملی کشور می‌باشد.
۲. موجب صرفه جویی کلان اقتصادی و ارزی در حفظ تجهیزات و تسلیحات بسیارگران قیمت نظامی و.. می‌گردد.
۳. اقدامات پدافند غیرعامل، مراکز حیاتی و حساس اقتصادی، سیاسی، نظامی، ارتباطی و مراکز عمده علمی و فرهنگی و... را در برابر حملات دشمن حفظ و ادامه فعالیت در شرایط بحران و جنگ را ممکن می‌کند.
۴. اقدامات دفاع غیرعامل موجب تحمیل هزینه قابل توجه به دشمن می‌گردد.
۵. اقدامات دفاع غیرعامل سبب به وجود آمدن تاثیرات روحی و روانی مثبت در شهروندان و رزمندگان می‌گردد.
۶. اقدامات دفاع غیرعامل موجب حفظ نیروها برای ضربه زدن در زمان و مکان مناسب و گرفتن آزادی و ابتکار عمل از دشمن می‌گردد.
۷. در مقام مقایسه (تهاجم، دفاع عامل و غیرعامل) دفاع غیرعامل مخارج و هزینه‌های کمتری دارد و از نظر اخلاقی و بشر دوستی و سیاسی مفهوم صلح دوستانه و تنش زا دارد.
۸. اجتناب ناپذیر بودن بروز جنگ‌های آینده و لزوم آمادگی دفاعی.
۹. نیل به دفاع غیرعامل در مقایسه با دفاع عامل، ساده‌تر و سهل الوصول‌تر و با سیاست خودکفایی و عدم وابستگی کشور هم جهت است.
۱۰. پیشگیری بهتر از درمان است. تصفیه آب در سرچشمه آسان تر از تصفیه در دریاست. متخصصین زلزله شناسی ژاپنی عقیده دارند: این زلزله نیست که موجب کشته شدن انسان‌های بی‌گناه و بروز خسارت می‌گردد بلکه سازه‌های ناامن می‌باشند که موجب بروز مرگ و خسارت می‌گردند.
۱۱. نظریه‌های استراتژیک و دکترین‌های نظامی، دال بر اهمیت و لزوم توجه به دفاع غیرعامل می باشند.
۱۲. اقدامات پدافند غیرعامل موجب کاهش آسیب پذیری و حفظ سرمایه‌های کلان موجود در یک کشور در شرایط وقوع جنگ یا بلاهای غیرطبیعی می‌گردد.

۱-۵- حوزه‌های عملیاتی در پدافند غیر عامل

پدافند غیرعامل حوزه وسیعی از نهادها، ارگان‌ها، سازمان‌ها و... را در بر می‌گیرد که به اختصار اشاره می‌کنیم:

۱. نظامی
۲. بهداشت و سلامت عمومی
۳. رسانه و صدا و سیما
۴. مدیریت بحران
۵. فناوری اطلاعات
۶. ارتباطات و مخابرات
۷. آب و برق
۸. حمل و نقل و ....

۱-۶- حوزه‌های علمی‌در پدافند غیر عامل

اقدامات دفاع غیرعامل حوزه وسیعی از علوم مختلف را در بر می‌گیرد به طوری که ساماندهی جامع آن نیازمند استفاده و بهره‌برداری مناسب از علوم گوناگون و متنوعی به شرح زیر بوده و باید در ایجاد ساختارهای سازمانی، طرح‌ریزی و اجرای پروژه‌های تحقیقاتی، بسط و توسعه آموزش‌های تخصصی و اقدامات اجرایی مورد توجه خاص قرار گیرد[۲].

۱. مهندسی جغرافیا و رشته‌های مربوط به آن
۲. هواشناسی، تأثیرات عوامل جوی در دید بصری و شناسایی سامانه‌های کشف هدف
۳. مهندسی شیمی، مواد، متالوژی، پلیمر، رنگ، پایروتکنیک‌ها و ...
۴. دشمن و بلاهای طبیعی شناسی و شناخت تهدیدات آن‌ها
۵. مهندسی کامپیوتر (سخت افزار، نرم افزار، شبکه و ...)
۶. مهندسی ساختمان (عمران و زیرگروه آن)
۷. مدیریت برنامه‌ریزی استراتژیک
۸. مهندسی مخابرات و ارتباطات و....

۱-۷- اولویت بندی مراکز در پدافند غیر عامل

اولویت اول پدافند غیرعامل، ایجاد امنیت و حفظ منابع انسانی است و مراکز ثقل کشور نیز بر حسب عمق آسیب و سطح تاثیرگذاری به سه دسته تقسیم می‌گردند:

۱. مراکز حیاتی[1]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری سراسری در کشور گردد.

۲. مراکز حساس[2]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری منطقه‌ای در کشور گردد.

۳. مراکز مهم[3]

مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، موجب بروز آسیب و صدمات محدود در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری محلی در کشور گردد.

[1] Vital Centers
[2] Critical Centers
[3] Important Centers

فصل دوم

اینترنت و فضای سایبر

۲-۱- ابداع اینترنت

اینترنت را می‌توان یکی از بزرگترین دست‌آوردهای علمی بشر نامید که تغییرات بسیاری را در شئون مختلف زندگی بشر ایجاد کرده است. دلایل ایجاد اینترنت نیز در جای خود جالب و قابل بررسی است به صورتی که در یک جمله می‌توان گفت اینترنت زاییده جنگ سرد است. افتتاح پروژه اسپوتنیک[۱] توسط اتحاد جماهیر شوروی زنگ خطر را برای ایالات متحده به صدا درآورد تا با تأسیس دارپا[۲] یا موسسه پروژه‌های تحقیقاتی دفاعی پیشرفته در سال ۱۹۵۸ میلادی پیش‌روی در زمینه فناوری را بازیابد. آرپا اداره فناوری پردازش اطلاعات[۳] را تاسیس نمود تا پروژه SAGE راکه برای اولین بار سامانه‌های رادار سراسر کشور را با هم شبکه کرده بود پیشتر برد. هدف اداره فناوری پردازش اطلاعات، دست یافتن به راه‌هایی برای پاسخ به نگرانی ارتش آمریکا درباره‌ی قابلیت مقاومت شبکه‌های ارتباطی‌شان بود و به عنوان اولین اقدام، رایانه‌هایشان را در پنتاگون، کوه چاین و دفتر مرکزی فرماندهی راهبردی هوایی[۴] را به یکدیگر متصل سازد.

اداره فناوری پردازش اطلاعات، مطالعه جامعی را برای نیروی هوایی ایالات متحده آمریکا منتشر کرده بود و در آن پیشنهاد داده بود که برای دستیابی به استحکام و مقاومت در برابر حوادث، از[۵]Packet switching استفاده شود. پس از کار فراوان، سرانجام در ۲۹ اکتبر ۱۹۶۹ اتصال بین مرکز سنجش شبکه کلینراک در دانشکده مهندسی و علوم کاربردی UCLA و سامانه NLS داگلاس انگلبرت در موسسه تحقیقاتیSRI International در پارک منلو در کالیفرنیا برقرار شد و آرپانت به وجود آمد. سومین مکان در آرپانت مرکز ریاضیات تعاملی Culler-Fried در دانشگاه کالیفرنیا، سانتا باربارا و چهارمی، دپارتمان گرافیک دانشگاه یوتا بود. تا پایان سال ۱۹۷۹ میلادی، پانزده مکان مختلف به آرپانت جوان پیوسته بودند که پیام‌آور رشدی سریع بود. آرپانت تنها یکی از اجداد اینترنت امروزی می‌باشد[۳].

---

[۱] اسپوتنیک (Sputnik) نخستین ماهواره فضایی جهان بود که در تاریخ ۱۲ مهر ۱۳۳۶ (۴ اکتبر ۱۹۵۷) توسط اتحاد جماهیر شوروی از پایگاه فضایی بایکونور به مدار زمین پرتاب شد. پرتاب اسپوتنیک-۱ به مدار زمین آغازگر عصر فضا و مسابقه فضایی بود.

[۲] دارپا یا سازمان پروژه‌های تحقیقاتی دفاعی پیشرفته (به انگلیسی: Defense Advanced Research Projects Agency) تاسیس ۱۹۵۸، نام یک سازمان تحقیقات و فناوری زیر نظر وزارت دفاع ایالات متحده آمریکا است.

[3] IPTO

[4] SAC

[۵] Packet switching یا راه گزینی بسته کوچک: دراین تکنولوژی بسته‌های مخصوصی [از اطلاعات] که مورد نیاز است بدون اینکه مسیر خاصی برای [انتقال] آن‌ها در نظر گرفته شود فرستاده می‌شوند. این کار بر عهده هر بسته است که راه مخصوص به خود را برای رسیدن به مقصد پیدا می‌کند.

اینترنت تا دهه ۱۹۹۰ هنوز چهره‌ای همگانی نداشت. در ششم آگوست ۱۹۹۱، سِرن[۱] پروژه وب جهان‌گستر[۲] را به اطلاع عموم رساند. وب توسط دانشمندی انگلیسی به نام «سر تیم برنرز لی»[۳] در سال ۱۹۸۹ اختراع شد. در سال ۱۹۹۳ مرکز ملی کاربردهای ابررایانش امریکا[۴] در دانشگاه ایلینوی، اولین نسخه از موزاییک[۵] را منتشر کرد و تا اواخر سال ۱۹۹۴ علاقه عمومی به اینترنتی که پیش از این آموزشی و تخصصی بود، گسترش فراوانی یافته بود. در سال ۱۹۹۶ استفاده از واژه اینترنت معمول شد و به صورت مجازی برای اشاره به وب هم استفاده شد.

۲-۲- میزان کاربران اینترنت در ایران

در حال حاضر یکی از شاخصه‌های توسعه‌یافتگی، ضریب نفوذ و تعداد کاربران اینترنت است. نکته‌ای که در اینجا باید قبل‌از ارائه آمار مورد بررسی قرار گیرد این سوال است که تعریف کاربر اینترنت چیست و چه کسی را می‌توان یک کاربر اینترنت نامید؟

در حالت کلی کاربر اینترنت به فردی گفته می‌شود که به شبکه‌ی جهانی اینترنت برای اموری مانند جستجو، مطالعه، آموزش، سرگرمی و هر منظور دیگر متصل شود اما استانداردهای بین المللی متفاوتی برای تعریف کاربران اینترنت وجود دارد که از دو منظر "اتصال به اینترنت" و "زمان استفاده" از آن قابل بررسی است. براین اساس از نگاه اتحادیه جهانی ارتباطات که یکی از معتبرترین سازمان‌های جهانی در زمینه اینترنت و فناوری اطلاعات و ارتباطات است کاربر اینترنت به شخصی اطلاق می‌شود که حداقل ۲ سال سن داشته باشد و در طول ۳۰ روز گذشته حداقل یک بار به اینترنت متصل شده باشد. اما کاربر اینترنت از نگاه وزارت بازرگانی آمریکا به فردی گفته می‌شود که حداقل دارای ۳ سال سن بوده و در حال حاضر از اینترنت استفاده می‌کند. در همین حال کاربر اینترنت از نگاه مرکز اطلاعات شبکه اینترنت چین به فردی گفته می‌شود که ۶ سال یا بیشتر داشته و حداقل ۱ ساعت در هفته از اینترنت استفاده کند. کاربر اینترنت از نگاه آژانس ملی توسعه اینترنت کره نیز اشخاص بیشتر از ۳ سالی هستند که از اینترنت جهانی یا بی‌سیم حداقل یک بار در یک ماه گذشته استفاده کرده باشند. با این وجود پایگاه مرکز آمار اینترنت معتقد است که تعریف کاربر اینترنت باید تا حد ممکن ساده و کلی باشد تا بتوان آماری که از مراکز مختلف ارائه می‌شوند را راحت‌تر با یکدیگر مقایسه کرد بر این اساس، پایگاه مذکور، کاربر اینترنت را فردی می‌داند که در حال حاضر توانایی اتصال به اینترنت را دارا است یعنی باید یک نقطه دسترسی به

---

[۱] سرن (CERN) یا سازمان اروپایی پژوهش‌های هسته‌ای (Organisation Européenne pour la Recherche Nucléaire)

[2] World Wide Web
[3] Sir Tim Berners-Lee
[4] National Center for Supercomputing Applications

[۵] یک نرم‌افزار اولیه کامپیوتری جهت دیدن داده‌های اینترنتی.

اینترنت داشته باشد و دانش اولیه در مورد چگونگی استفاده از تکنولوژی وب را دارا باشد. این سازمان اعتقاد دارد به همین سادگی می‌توان تعداد کاربران اینترنت در هر کشور را تعیین کرد و نیازی نیست که برای مسئله‌ای به این سادگی به دنبال راهکارهای پیچیده باشیم؛ اما موسسه نیلسون آنلاین تعریف سخت گیرانه‌ای از یک کاربر فعال اینترنت دارد و آن را فردی می‌داند که در یک ماه گذشته ۴۹ بار در اینترنت حضور یابد، ۱۳۵۰صفحه را بازدید کند، ۴۵ ساعت در ماه در اینترنت حضور داشته باشد، به ۷۶ دامنه مراجعه کرده باشد و در هربار حضور در اینترنت به طور متوسط ۳۲ دقیقه زمان اختصاص دهد. با وجود این تعاریف می‌توان یک تعریف کلی برای کاربر اینترنت ارائه داد و آن این است که کاربر اینترنت به کسی گفته می‌شود که در یک سال گذشته به هر نحو و روش و با هر مدتی به اینترنت وصل شده و از خدمات آن استفاده کرده باشد. در نتیجه، کاربر اینترنت فردی است که طی ۱۲ ماه گذشته با اتصال به شبکه اینترنت از یکی از خدمات اینترنتی استفاده کرده باشد.

البته در کشورهای جهان سوم و کشورهای در حال توسعه، مسئله اندکی متفاوت است، چرا که در بسیاری از این کشورها، یک خط ارتباطی اینترنت ممکن است بین تعدادی کاربر به اشتراک گذاشته شود که این مسئله موجب می‌شود از طریق شمارش تعداد خطوط ارتباطی اینترنت و یا شمارش تعداد خطوط تلفن موجود نتوان آمار صحیحی از کاربران اینترنت به دست آورد. بر این اساس با توجه به اینکه در کشور ما نیز در بسیاری از موارد مشاهده می‌شود که یک خط ارتباطی اینترنت بین چندین کاربر به اشتراک گذاشته می‌شود، تخمین نسبتا دقیق کاربران اینترنت کاری بسیار دشوار خواهد بود. با توجه به تعریف کاربر اینترنت، آمار کاربران اینترنت را می‌توان از دو منبع داخلی و خارجی مورد بررسی قرار داد. آمارهای ارائه شده از سوی «متما»[1] نشان می‌دهد که تا پایان سال ۹۱، ضریب نفوذ اینترنت در کشور برابر ۶۱,۰۶ درصد می‌باشد.

با وجودی که چند سالی است علاوه بر اینترنت دایال‌آپ[2]، اینترنت ADSL[3] در کشور راه‌اندازی شده و نیز هم‌اکنون اینترنت بر بستر وایمکس به صورت بی‌سیم نیز قابل ارائه است، بر اساس گزارش متما، بیشترین کاربران اینترنت در کشور، مشترکین[4] GPRS هستند که از طریق موبایل به اینترنت وصل می‌شوند و تعداد آن‌ها ۲۲ میلیون و ۶۲۹ هزار و ۸۰۹ نفر اعلام شده که بیش از ۳۰ درصد کاربران اینترنت را تشکیل می‌دهند. این در حالی است که طبق این آمار ۶ میلیون و ۹۳۴ هزار و ۷۶۰ نفر در کشور از طریق تلفن و با کارت اینترنتی (دایال‌آپ) از اینترنت استفاده می‌کنند که ۹/۲ درصد کاربران را تشکیل می‌دهند. در همین حال تعداد کاربران اینترنت

---

[1] مرکز مدیریت توسعه ملی اینترنت.

[2] Dial up

[3] خط رقمی مشترک نامتقارن (Asymmetric Digital Subscriber Line) که می‌توان آن را خط اشتراک دیجیتال نامید، روشی برای اتصال به اینترنت با سرعت بالا و هزینه کمتر است.

[4] جی‌پی‌آر‌اس (General Packet Radio Service) این یک سرویس ارزش افزوده جدید در نسل دوم تلفن همراه است که امکان ارسال و دریافت اطلاعات یا داده را روی شبکه تلفن همراه فراهم می‌سازد.

پرسرعت با سیم (ADSL) نیز ۸ میلیون و ۱۸۶ هزار و پانصد نفر(معادل ۱۱ درصد)، کاربران اینترنت وایمکس،[۱] ۲ میلیون و ۲۷ هزار و ۷۵ نفر (۲/۷ درصد)و میزان اتصال از طریق فیبر نوری نیز ۶ میلیون و ۱۰۶ هزار اتصال اعلام شده است.

۲-۳- مفهوم فضای سایبر

در سال‌های اخیر، واژه «سایبر»[۲] بسیار شنیده می‌شود که در خود مفاهیم گسترده و وسیعی را در بر گرفته است. فضای سایبر[۳] عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. به نظر می‌رسد به کارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفا فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه‌های متنوعی از جمله خصلت‌های روانشناختی قابل توجه نیز دارد.[۴]

واژه سایبر از لغت یونانی «کایبرنتس»[۵] به معنی سکاندار یا راهنما مشتق شده است. نخستین بار اصطلاح «سایبرنتیک»[۶] توسط ریاضیدانی به نام «نوربرت وینر»[۷] در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی و کامپیوترها است. سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه‌های ترکیبی بسیاری از این کلمه سایبر بوجود آمده مانند: فضای سایبر[۸]، شهروند سایبر[۹]، پول سایبر[۱۰]، فرهنگ سایبر[۱۱]، راهنمایی فضای سایبر[۱۲]، تجارت سایبر[۱۳]، کانال سایبر[۱۴] و... [۴].

واژه «فضای سایبر» را نخستین بار «ویلیام گیبسون»[۱۵] نویسنده داستان علمی تخیلی در کتاب «نورومنسر»[۱۶] در سال ۱۹۸۴ به کار برده است. در ایران نیز واژه سایبر در برخی از

---

[۱] wimaxیا هم‌کُنش‌پذیری جهانی برای دسترسی ریزموج (WorldWide Interoperability for Microwave Access)، پروتکل ارتباطی برای دسترسی پهن باند بی‌سیم بر پایه استاندارد IEEE 802.16 است. وای‌مکس امکان دسترسی به اینترنت را به هردو صورت ثابت و کاملا سیار در یک ناحیه گسترده فراهم می‌آورد.

[2] Cyber
[3] cyberspace
[4] www.en.wikipedia.org/wiki/Cyberspace
[5] Kybernetes
[6] Cybernetic
[7] Norbert Wiener
[8] Cyber Space
[9] Cyber Citizen
[10] Cyber Cash
[11] Cyber Culture
[12] Cyber Coach
[13] Cyber Bussiness
[14] Cyber Channel
[15] William Gibson
[16] Neuromancer

دستگاه‌های امنیتی و انتظامی وارد شده و رسمیت یافته است. مانند «پلیس سایبری» که در نیروی انتظامی جمهوری اسلامی ایران به منظور مقابله با تهدیدات و جرایم مربوط با فضای مجازی تأسیس شده است که البته عبارت «پلیس فتا» برای آن انتخاب گریده است. منظور از فتا در اینجا خلاصه‌ی عبارت «فضای تبادل و تولید اطلاعات» می‌باشد. در نتیجه به نظر می‌رسد نزدیک‌ترین عبارت در زبان فارسی در رابطه با مفهوم سایبر همین عبارت «فضای تبادل و تولید اطلاعات» می‌باشد.

۲-۳-۱- ویژگی‌های فضای سایبر

بر اساس تعریفی که از مفهوم فضای سایبر یا همان فضای تبادل و تولید اطلاعات داشتیم، لازم است به ویژگی‌های این فضا نیز اشاره‌ای داشته باشیم[۵].

- جهانی و فرامرزی بودن

از ویژگی‌های منحصر به فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد.
مرزهای جغرافیایی تا کنون نتوانسته از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار می‌نماید.

- دستیابی آسان به آخرین اطلاعات

چنانچه بخواهید به آخرین مقاله، کتاب و یا خبری که در زمینه تخصصی، در سطح جهان منتشر شده، دست یابید، ساده ترین و سریع ترین راه، استفاده از فضای سایبر است.

- جذابیت و تنوع

رسانه‌ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش استفاده می‌کنند و این ابزار در فضای سایبر قابل دستیابی است؛ به ویژه آن گاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوع و جذابیت فضای سایبر تأثیر بسزایی دارد، مشتری محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می‌تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظر سنجی و ارزیابی در این فضا بسیار آسان تر است و این

توانایی را به داده پردازان، فروشندگان و عرضه کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته‌های مشتریان و مخاطبان خود مطلع گردند.

- آزادی اطلاعات و ارتباطات

معنای واقعی آزادی اطلاعات، در فضای سایبر محقق شده است. از این رو، شما هر نوع اطلاعاتی را که بخواهید - اعم از فرهنگی، سیاسی و اقتصادی - بدون محدویت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.[1]

- مدیریت و کنترل فضای سایبر

امروزه اهمیت فضای سایبر بر کسی پوشیده نیست. فضایی که حجم عظیمی از اطلاعات در آن جابه‌جا می‌شود، اطلاعاتی که به دست آوردن آن تا چند سال پیش برای سرویس‌های امنیتی و نهادهای مختلف سیاسی و دیپلماتیک شاید کاری سخت، پرهزینه و گاهی غیرممکن بود.

۲-۴- جنگ سایبری پنجمین عرصه جنگ

در فضای سایبر ممکن است حوادث مختلفی رخ دهد از حوادث جزئ گرفته تا حوادث کلی و بزرگ؛ و لذا هر حادثه‌ای که اتفاق می‌افتد را نمی‌توان یک جنگ سایبری قلمداد کرد، در واقع حوادثی که در این فضا صورت می‌گیرد را می‌توان به لایه‌های مختلف از نظر اهمیت تقسیم کرد از یک هکر فردی که در لایه پایین قرار دارد تا سطح عالی آن که یک تجربه عملیات مشترک سایبری فیزیکی می‌باشد، لذا در بررسی حوادث سایبری می‌توان گفت که موضوع از یک نفوذ ساده شروع می‌شود و با جابجایی اطلاعات و تخریب دستگاه مورد نظر وارد بحث دفاع از منظر امنیت ملی خواهد شد، برای مثال حادثه گازی که یک نمونه از حملات سایبری انفجار در خطوط انتقال گاز روسیه به سیبری که بر اثر تأخیر و انسداد عملکرد سنسورها در تنظیم فشار لوله اتفاق افتاد منجر به یک انفجار بزرگ شد و باعث بزرگ‌ترین انفجار غیر هسته‌ای در جهان شد. به طور کلی در جنگ‌ها عرصه‌های مختلفی وجود دارد که فضای سایبری بعد از عرصه زمین، هوا، دریا و فضا، پنجمین آن‌ها می‌باشد که به عرصه‌ها دیگر نیز نفوذ دارد به همین دلیل موضوع جنگ سایبری بسیار جدی است.

[1] www.rasekhoon.net/article/show-41605.aspx

۲-۴-۱- لایه‌های جنگ سایبری

اولین چارچوب در حوزه‌ی سایبر، شناخت تهدید است که از لایه پایین که نفوذ یک هکر ساده است شروع شده و به لایه بالایی که می‌تواند به یک جنگ سایبری که یک اقدام پیشدستانه از یک جنگ کامل باشد منتهی شود. امروزه هر نوع سناریو تهدید که بر علیه یک کشور صورت می‌گیرد حتما بخشی از آن حمله سایبری می‌باشد. به طور مثال در یک جنگ نظامی کشور حمله کننده مطمئنا در صدد بهم ریختن نظامات اداری، خدماتی و در یک جمله بهم زدن تعادل کشور مورد حمله از طریق فضای سایبر خواهد بود.

۲-۴-۲- هدف از جنگ سایبری

در تهدیدات سایبری اگر حمله کننده یک هکر یا گروهی از هکرها باشد منشأ تهدید یک فرد یا یک گروه هکری است و حوزه خطر آن حوزه‌ای محدود است یعنی امنیت حوزه فردی در خطر قرار می‌گیرد این حوزه را حوزه ایمنی می‌گوییم. چنانچه منشا تهدید یک گروه یا تیم هکری متشکل از دو نفر یا چند صد نفر باشد و افراد هر کدام یا هر تیم در حوزه تخصصی سایبری خود کار کنند این گروه‌ها را گروه تروریستی هکری گویند. سطح خطر ایجاد شده این گروه‌ها در سطح امنیت عمومی می‌باشد این لایه را حوزه امنیت سایبری گویند. سطح دیگر از تهدید آن است که به جای یک فرد یا یک گروه یک کشور یا دولت تهدید را انجام دهد یعنی منشأ حمله یک کشور یا چند کشور می‌باشند و حوزه آن یک حوزه پراهمیت و پر خطر است مانند حمله به نیروگاه هسته‌ای توسط یک کشور یا نظام پولی و بانکی، سطح خطر ایجاد شده در این بخش، سطح خطر امنیت ملی است و لذا این حوزه را جنگ سایبری گویند.

۲-۴-۳- مصداق جنگ سایبری

مهم‌ترین لایه، لایه جنگ سایبری است که باید عملیات پدافند سایبری در آن صورت گیرد گرچه لایه دوم نیز که در سطح امنیت عمومی سایبری است مورد حمایت نظام پدافندی سایبری قرار می‌گیرد ولی در آن به صورت مستقیم دخالت نمی‌کند در لایه دوم بخش‌هایی مثل وزارت ارتباطات، پلیس فتا، دستگاه قضایی و دیگر دستگاه‌های ذی‌ربط متولی می‌باشند اما در لایه سوم به دلیل قرار گرفتن در سطح امنیت ملی، عملیات پدافندی سایبری توسط دستگاه‌های اجرایی و قرارگاه پدافند سایبری انجام می‌پذیرد و برای پیگیری حقوق قانونی (دفاع حقوقی و قانونی سایبری) این نوع حملات بایستی به دادگاه بین‌المللی مراجعه کرد این مسئله خود یک چالش

پیشرو است .البته سطح چهارمی نیز در این لایه‌ها وجود دارد که توسط چند کشور به چند کشور حمله سایبری انجام می‌گیرد، این دو لایه آخر مربوط به پدافند سایبری می‌شود و در حوزه بین‌المللی است. نکته مهم در لایه‌های سوم و چهارم آن است که حتما باید در حوزه پر اهمیت و پر خطر باشد تا بتوان به آن مصداق جنگ سایبری داد.

۲-۴-۴- ویژگی‌های سلاح سایبری

سلاح سایبری پنج ویژگی دارد. ویژگی اول، این ویروس یا سلاح سایبری متشکل از چند لایه می‌باشد. ویژگی دوم آن رمزدار بودن این لایه‌هاست. سومین ویژگی هوشمند بودن به صورتی که قابلیت تشخیص محیط مورد نظر را دارا می‌باشد. ویژگی بعدی آن است که از راه دور فرمان پذیر است یعنی اطلاعات را گرفته و ارسال می‌کند سپس دستور تخریب را دریافت و انجام می‌دهد و آخرین ویژگی قدرت پنهان شوندگی این ویروس‌ها یا سلاح سایبری می‌باشد. یعنی امکان دارد چندین ماه از کار افتاده و قابل دسترسی توسط آنتی ویروس‌های مختلف نباشد که با ویروس‌های معمولی کاملا متفاوت است و البته توسط آزمایشگاه‌های تخصصی ویروس‌شناسی قابل تشخیص می‌باشد.

۲-۴-۵- زیرساخت سایبری

اولین دسته زیرساخت‌ها، لایه‌های حیاتی کشور می‌باشد که توسط نرم افزارهای خاصی مدیریت می‌شوند و از کار افتادن آن‌ها موجب خطر در سطح امنیت ملی و کشور می‌شود به طور مثال نرم افزارهای مدیریتی نظام پولی و بانکی کشور. دسته دوم، زیرساخت‌های حساس می‌باشد که در آن از نرم افزارهایی استفاده می‌شود که در صورت نفوذ به آن قابلیت مدیریت جامعه مختل می‌شود. این دسته از زیرساخت‌ها بیشتر باعث بی نظمی اجتماعی در سطح کشور می‌شوند نه خسارت و تخریب. زیرساخت بعدی زیرساخت‌های مهم نام دارد که شبیه اتوماسیون اداری می‌باشد. البته اتوماسیون اداری که در بخش‌هایی کم اهمیت یا سطح امنیت پایین نسبت به بقیه زیرساخت‌های کشور باشد،چهارمین زیرساخت، و زیرساخت در سطح دستگاه‌های اطلاع رسانی است که نسبت به بقیه زیرساخت‌های سایبری از اهمیت کمتری برخور دار می‌باشد، به طور مثال در این بخش می‌توان به سایت‌های اطلاع رسانی اشاره کرد[۶][۷].

۲-۴-۶- اهداف پدافند سایبری

اولین هدف ،کاهش آسیب‌پذیری و ایمنی زیرساخت‌های فضای سایبر می‌باشد. هدف بعدی افزایش بازدارندگی و تولید قدرت در فضای سایبری است، سومین هدف، تداوم فعالیت‌های ضروری سایبری کشور است. هدف بعدی ارتقای پایداری زیرساخت‌های سایبری در برابر تهدیدات است و از دیگر اهداف اساسی؛ بومی سازی نرم افزارها، تسهیل مدیریت بحران در فضای سایبری و الگو سازی مدل دفاع به صورت کامل می‌باشد که از جمله اهداف دفاع سایبری است. که در مورد هر کدام باید تحقیق، بحث، تبادل نظر و کارهای عملیاتی انجام پذیرد.

فصل سوم

اصول امنیت برنامه‌های وب

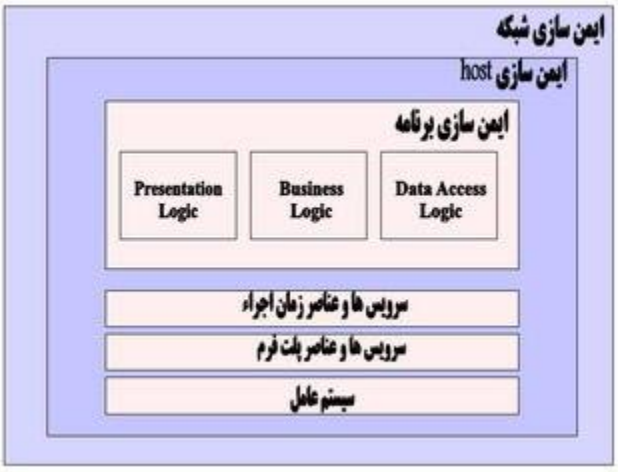
۳-۱- مقدمه

زمانی که در رابطه با امنیت برنامه‌های وب سخن به میان می‌آید تهاجم علیه یک سایت، سرقت کارت‌های اعتباری، بمباران وب سایت‌ها در جهت مستاصل کردن آنان به منظور ارائه خدمات و سرویس‌های تعریف شده، ویروس‌ها، تروجان‌ها، کرم‌ها و... در ذهن تداعی می‌گردد. صرفنظر از نوع برداشت ما در رابطه با موارد فوق، می‌بایست بپذیریم که تهدیدات امنیتی متعددی متوجه برنامه‌های وب با توجه به ماهیت آنان می‌باشد. سازمان‌ها و یا موسساتی که از اینگونه برنامه‌ها استفاده می‌نمایند و یا در صدد طراحی و پیاده‌سازی آنان می‌باشند، می‌بایست به این نکته مهم توجه نمایند که ایمن‌سازی یک برنامه وب، محدود به بکارگیری یک فن‌آوری خاص نبوده و فرآیندی است مستمر که عوامل انسانی و غیرانسانی متعددی می‌توانند بر روی آن تاثیرگذار باشند. تا زمانی که شناخت مناسبی نسبت به تهدیدات وجود نداشته باشد، امکان ایجاد یک برنامه وب ایمن وجود نخواهد داشت. بنابراین قبل از هر چیز لازم است که با مدل تهدیدات موجود آشنا شویم. هدف مدل فوق، آنالیز معماری و نحوه طراحی برنامه به منظور شناسائی نقاط آسیب پذیری است که ممکن است به صورت تصادفی توسط یک کاربر ناآگاه و یا مهاجمان با اهداف مخرب مورد سوء استفاده قرار گرفته تا با استناد به آنان بتوانند موجودیت و امنیت سیستم را با خطر مواجه نمایند.

پس از آشنایی با تهدیدات، می‌بایست با بکارگیری مجموعه‌ای از اصول امنیتی اقدام به طراحی سیستم نمود. در ادامه، پیاده‌کنندگان می‌بایست از روش‌های ایمن به منظور نوشتن کدهای مطمئن، مستحکم و قابل اعتماد استفاده نمایند. پس از طراحی و پیاده‌سازی برنامه، می‌بایست از یک شبکه ایمن، یک host مطمئن و یک پیکربندی مناسب بر روی سرویس دهنده، استفاده گردد. ایجاد یک برنامه وب ایمن، مستلزم اقدامات امنیتی چند جانبه‌ای است که موفقیت در تمامی آنان، ایمن بودن برنامه‌های وب را تضمین خواهد کرد. ایمن سازی شبکه، host و برنامه، رئوس مثلث امنیتی ایجاد برنامه‌های وب ایمن را تشکیل می‌دهند.

۳-۲- ایمن سازی شبکه، host و برنامه

به منظور ایجاد برنامه‌های وب ایمن، تبعیت از یک رویکرد جامع امری الزامی است. بنابراین، می‌بایست امنیت برنامه‌های وب را در سه لایه متفاوت بررسی و اقدامات لازم را در هر لایه با توجه به جایگاه آن انجام داد. شکل زیر سه لایه مهم به منظور ایجاد برنامه‌های وب ایمن را نشان می‌دهد.



شکل ۳-۱. ایمن سازی شبکه [۸]

شبکه، نقطه‌ی ورود به یک برنامه وب است و اولین لایه حفاظتی به منظور کنترل دستیابی به سرویس دهندگان متعدد موجود در محیط عملیاتی را فراهم می‌نماید. با این که سرویس دهندگان توسط سیستم عامل‌های نصب شده بر روی خود حفاظت می‌گردند ولی نمی‌بایست به این موضوع صرفا اکتفاء نمود و لازم است که تدابیر لازم به منظور حفاظت آن‌ها در مقابل سایر تهدیدات (نظیر ارسال سیلابی از بسته‌های اطلاعاتی از طریق لایه شبکه) نیز اندیشیده گردد.

ایمن سازی شبکه، شامل حفاظت از دستگاه‌های شبکه‌ای و داده مبادله شده بر روی آن‌ها می‌باشد. روتر، فایروال و سوئیچ عناصر اولیه زیرساخت یک شبکه را تشکیل می‌دهند. شکل زیر نحوه استفاده از عناصر فوق را در یک شبکه نشان می‌دهد.

شکل ۳-۲. عناصر شبکه: روتر، فایروال و سوئیچ[۸]

یک برنامه وب بر روی یک زیرساخت شبکه‌ای ایمن فعالیت می‌کند و به کاربران خود سرویس‌های لازم را ارائه می‌نماید. برای ایمن‌سازی شبکه، علاوه بر این که شبکه می‌بایست در مقابل حملات مبتنی بر TCP/IP از خود محافظت نماید، بلکه لازم است اقدامات متعدد دیگری نیز در این رابطه انجام شود. ایجاد اینترفیس‌های مدیریتی ایمن، استفاده از رمزهای عبور قدرتمند، حصول اطمینان از صحت ترافیک ارسالی از جمله اقدامات دیگر در خصوص ایجاد یک شبکه ایمن

می‌باشد. بدین منظور لازم است که پورت‌ها و پروتکل‌های استفاده شده در هر لایه به دقت بررسی و در صورتی که وجود آن‌ها غیرضروری تشخیص داده شود و یا استفاده از آن‌ها زمینه بروز تهدیداتی را فراهم می‌نماید، می‌بایست در همان لایه با آنان برخورد و از یک راهکار مناسب امنیتی استفاده گردد. وجود ضعف امنیتی در یک شبکه زمینه بروز تهدیدات متعددی را فراهم می‌نماید. بدون شناسائی اینگونه تهدیدات، امکان مقابله منطقی با آنان وجود نخواهد داشت[۹].

۳-۳- تهدیدات

یک مهاجم به منظور برنامه‌ریزی حملات خود به دنبال دستگاه‌های شبکه‌ای است که بر روی آن‌ها پیکربندی ضعیفی اعمال شده است. تنظیمات ضعیف پیش فرض، دستیابی بدون ضابطه به منابع موجود بر روی شبکه، وجود دستگاه‌هائی که به درستی patch و یا بهنگام نشده‌اند، حفره‌های امنیتی متعددی را در یک شبکه ایجاد می‌نماید. وجود حفره‌های امنتیی فوق و عدم برخورد مناسب با آن‌ها، احتمال موفقیت مهاجمان را افزایش می‌دهد. مهمترین تهدیدات در یک شبکه عبارتند از[۱۰]:

- جمع آوری اطلاعات
- sniffing
- spoofing
- session hijacking
- DoS (برگرفته از Denial of Service)

با آگاهی از ماهیت هر یک از تهدیدات فوق و نحوه تاثیر آن‌ها بر روی عملکرد شبکه، می‌توان امکانات حفاظتی و تدافعی مناسبی را در یک شبکه پیش بینی و پیاده سازی نمود. در ادامه به بررسی مختصر هر یک از تهدیدات فوق خواهیم پرداخت.

۳-۳-۱- جمع آوری اطلاعات

مهاجمان در اولین مرحله، اقدام به جمع آوری اطلاعات در رابطه با اهداف خود می‌نمایند. جمع‌آوری اطلاعات می‌تواند باعث افشای اطلاعات توپولوژی شبکه، پیکربندی سیستم و دستگاه‌های شبکه‌ای گردد. یک مهاجم می‌تواند در ادامه با استفاده از اطلاعات جمع آوری شده بر روی نقاط آسیب پذیر متمرکز و از حفره‌های امنیتی موجود در جهت تامین خواسته‌های مخرب خود استفاده نماید. متداولترین نقاط آسیب پذیری که شبکه را مستعد این نوع از حملات می‌نماید عبارتند از[۱۰]:

- ماهیت غیرایمن ذاتی پروتکل TCP/IP
- پیکربندی ضعیف دستگاه‌های شبکه‌ای

- استفاده غیرایمن از سرویس‌هایی که به وجود آن‌ها در یک شبکه نیاز نمی‌باشد.

همچنین حملات مبتنی بر جمع آوری اطلاعات عبارتند از:

- استفاده از Tracert به منظور تشخیص توپولوژی شبکه
- استفاده از Telnet به منظور باز نمودن پورت‌ها و جمع آوری اطلاعات اولیه
- استفاده از پویشگرهای پورت به منظور تشخیص وضعیت پورت‌ها
- استفاده از درخواست‌های broadcast برای شمارش تعداد host موجود بر روی یک subnet

به منظور پیشگیری و مقابله با این نوع حملات می‌توان از روش‌های زیر استفاده نمود:

۱. استفاده از امکاناتی که اطلاعات اضافه‌ای را در خصوص پیکربندی نظیر نام و شماره نسخه نرم افزار ارائه نمی‌نماید.
۲. استفاده از فایروال‌ها به منظور پوشش سرویس‌هایی که نمی‌بایست در معرض دید و استفاده عموم قرار داده شوند.

۳-۳-۲- استراق سمع

استراق سمع[1]، مانیتورینگ ترافیک شبکه برای داده‌هایی نظیر رمزهای عبور و یا اطلاعات پیکربندی است. با استفاده از یک برنامه packet sniffer، می‌توان به سادگی تمامی ترافیک plain text (رمز نشده) را مشاهده نمود. نقاط آسیب پذیری که شبکه را مستعد این نوع از حملات می‌نماید عبارتند از[۱۰]:

- ضعف امنیت فیزیکی
- ضعف رمزنگاری در زمان ارسال داده‌ی حساس و مهم
- وجود سرویس‌هایی که با یکدیگر به صورت متن معمولی (رمز نشده) ارتباط برقرار می‌نمایند.
- استفاده از الگوریتم‌های ضعیف رمزنگاری

مهاجمان با قرار دادن یک packet sniffer بر روی شبکه می‌توانند تمامی ترافیک را capture و آنالیز نمایند. به منظور پیشگیری و مقابله با این نوع حملات می‌توان از روش‌های زیر استفاده نمود:

- استفاده از یک سیستم امنیت فیزیکی مناسب به منظور پیشگیری از نصب دستگاه‌های مخرب بر روی شبکه
- رمزنگاری اطلاعات حساس و ترافیک برنامه بر روی شبکه

[1] sniffing

۳-۳-۳- هویت مبهم [1]

به کتمان هویت واقعی بر روی شبکه اطلاق می‌گردد و از یک آدرس مبدا جعلی که بیانگر آدرس اولیه صادرکننده پیام نمی‌باشد، استفاده می‌گردد. در بسیاری موارد از هویت مبهم، به منظور مخفی کردن منبع بروز یک تهاجم استفاده می‌شود. در برخی موارد که دستیابی به منابع موجود بر روی شبکه بر اساس آدرس متقاضیان انجام می‌شود، مهاجمان با تغییر آدرس مبداء سعی می‌نمایند به اینگونه از منابع دستیابی پیدا نمایند. متداولترین نقاط آسیب پذیری که شبکه را مستعد این نوع از حملات می‌نماید عبارتند از:

- ماهیت غیرایمن ذاتی پروتکل TCP/IP
- ضعف در فیلترینگ بسته‌های اطلاعاتی ورودی و خروجی: ترافیک ورودی و خروجی شبکه به درستی کنترل و فیلتر نمی‌گردد.

Session Hijacking -۴-۳-۳

با استفاده از این نوع حملات که به آن‌ها man in middle نیز گفته می‌شود، مهاجمان می‌توانند از یک برنامه برای تغییر شکل ظاهری خود به عنوان یک سرویس گیرنده و یا سرویس دهنده موجه استفاده نمایند. بدین ترتیب، یک سرویس دهنده و یا سرویس گیرنده واقعی فریب خورده و فکر می‌کنند که با یکhost معتبر و مجاز ارتباط برقرار نموده‌اند. در واقع، این نوع کامپیوترهای میزبان متعلق به مهاجمان بوده که سعی می‌نمایند با دستکاری شبکه خود را به عنوان مقصد مورد نظر وانمود نمایند. از این نوع حملات به منظور آگاهی از اطلاعات logon و دستیابی به سیستم و سایر اطلاعات محرمانه استفاده می‌گردد. مواردی که شبکه را مستعد این نوع از حملات می‌نماید عبارتند از:

- ضعف در امنیت فیزیکی
- ماهیت غیرایمن ذاتی پروتکل TCP/IP
- مبادله اطلاعات به صورت رمزنشده

یک مهاجم می‌تواند از ابزارهای متعددی به منظور انجام عملیات spoofing، تغییر روتینگ و دستکاری بسته‌های اطلاعاتی استفاده نماید. به منظور پیشگیری و مقابله با این نوع حملات می‌توان از روش‌های زیر استفاده نمود:

- رمزنگاری Session
- استفاده از روش Stateful inspection در سطح فایروال

[1] Spoofing

DoS -۵-۳-۳

در این نوع از حملات، امکان دستیابی کاربران مجاز به یک سرویس دهنده و یا سرویس خاص سلب می‌گردد. در حملات DoS لایه شبکه، معمولا مهاجمان با ارسال سیلابی از بسته‌های اطلاعاتی امکان استفاده از یک سرویس توسط سایر کاربران را سلب می‌نمایند. علاوه بر مشکل فوق، در چنین مواردی از پهنای باند و منابع موجود بر روی شبکه استفاده بهینه نخواهد شد. متداولترین نقاط آسیب پذیری که شبکه را مستعد این نوع از حملات می‌نماید عبارتند از:

- ماهیت غیرایمن ذاتی پروتکل TCP/IP
- ضعف در پیکربندی روتر و سوئیچ
- باگ در سرویسهای نرم افزاری

رایج‌ترین حملات DoS عبارتند از:

- ارسال سیلابی از بسته‌های اطلاعاتی نظیر حملات cascading broadcast
- بسته‌های اطلاعاتی SYN flood
- سوء استفاده از برخی سرویس‌ها

به منظور پیشگیری و مقابله با این نوع حملات می‌توان از روش‌های زیر استفاده نمود:

- فیلترینگ درخواست‌های broadcast
- فیلترینگ درخواست‌های ICMP[1]
- بهنگام‌سازی و نصب patches سرویس‌های نرم افزاری

همان‌گونه که اشاره شد در زیرساخت شبکه از روتر، فایروال و سوئیچ استفاده می‌گردد که می‌بایست ضمن آشنایی با جایگاه آن‌ها در یک شبکه با نحوه عملکرد و ایمن‌سازی آن‌ها از منظر برنامه‌های وب نیز آشنا شویم.

۳-۴- عناصر موجود در زیرساخت شبکه

زیر ساخت شبکه را می‌توان به سه لایه متفاوت دستیابی، توزیع و هسته تقسیم نمود. این لایه‌ها شامل تمامی سخت افزارهای مورد نیاز به منظور کنترل دستیابی به منابع داخلی و خارجی است. روتر، سوئیچ و فایروال مهمترین عناصر موجود در زیر ساخت یک شبکه می‌باشند. روتر، حلقه ارتباطی شبکه به دنیای خارج است و کانال مابین بسته‌های اطلاعاتی به پورت‌ها و پروتکل‌های مورد نیاز در برنامه‌های وب را ایجاد می‌نماید. مسئولیت روتر ارسال بسته‌های اطلاعاتی IP به شبکه‌هایی است که به آن‌ها متصل شده است. بسته‌های اطلاعاتی ممکن است

[1] Internet Control Message Protocol

درخواست‌های ارسالی سرویس گیرندگان به سرویس دهنده وب، پاسخ به درخواست‌های ارسالی و یا درخواست‌های صادره توسط سرویس گیرندگان داخلی شبکه باشد. پیکربندی روتر می‌بایست بگونه‌ای انجام شود تا ترافیک غیرضروری و غیر مجاز را بین شبکه‌ها فیلتر نماید. همچنین، روتر می‌بایست در مقابل پیکربندی مجدد غیرمطمئن حفاظت شود و از اینترفیس‌های مدیریتی ایمن به منظور پیکربندی مطمئن آن استفاده نماید. با توجه به نقش کلیدی نرم افزار IOS در روتر، می‌بایست همواره آخرین patch و نسخه‌های بهنگام شده بر روی آن‌ها نصب گردد.

فایروال، مسئولیت بلاک کردن تمامی پورت‌های غیرضروری را برعهده داشته و این امکان را فراهم می‌نماید که ترافیک صرفا از طریق پورت‌های شناخته شده انجام پذیرد. فایروال‌ها به منظور پیشگیری از حملات شناخته شده، می‌بایست دارای امکانات مناسبی به منظور مانیتورینگ درخواست‌های ورودی باشند. فایروال‌ها با همکاری نرم افزارهایی که از آن‌ها به منظور تشخیص مزاحمین استفاده می‌گردد، قادر به ایجاد یک محیط ایمن عملیاتی می‌باشند. همانند روتر، فایروال‌ها بر روی محیطی اجراء می‌گردند که مسئولیت مدیریت آن بر عهده یک سیستم عامل گذاشته شده است. بنابراین لازم است که در فواصل زمانی خاص نرم افزارهای تکمیلی و بهنگام شده بر روی آن‌ها نصب گردد. همچنین، مدیریت فایروال می‌بایست از طریق اینترفیس‌های ایمن انجام و پورت‌هایی که به وجود آن‌ها نیاز نمی‌باشد را غیرفعال نمود. از سوئیچ به منظور تقسیم شبکه به چندین سگمنت استفاده می‌گردد. سوئیچ دارای کمترین نقش در خصوص ایمن سازی یک شبکه می‌باشد. یکی از علل طراحی سوئیچ، بهبود کارآیی و تسهیل در امر مدیریت شبکه است.

۳-۴-۱- روتر و ملاحظات امنیتی آن

اولین خط دفاعی در یک شبکه را روتر تشکیل می‌دهد. روتر علاوه بر قابلیت روتینگ بسته‌های اطلاعاتی می‌تواند بگونه‌ای پیکربندی گردد تا بسته‌های اطلاعاتی را بر اساس نوع آن‌ها شناسایی و آندسته از بسته‌های اطلاعاتی را که ممکن است زمینه بروز حملات و تهدیدات در یک شبکه را ایجاد نمایند، بلاک کند. نظیر ICMP[1] و یا SNMP[2]. برای پیکربندی روتر با رعایت ملاحظات امنیتی، اقدامات متعددی را می‌بایست در هر یک از گروه‌های زیر انجام داد[۱۱]:

- نصب آخرین نسخه‌های بهنگام شده و patch ارائه شده

[1] Internet Control Message Protocol
[2] Simple Network Management Protocol

با عضویت در خبرنامه شرکت‌هایی که از محصولات نرم افزاری و یا سخت افزاری آن‌ها در زیرساخت فن‌آوری اطلاعات استفاده شده است، می‌توان به سرعت از توصیه‌های امنیتی آن‌ها آگاهی یافت. شرکت‌های معتبر در صورت بروز مشکل در یک محصول سخت افزاری و یا نرم افزاری در اولین فرصت اقدام به ارائه patch مربوطه می‌نمایند و این موضوع را از طریق پست الکترونیکی به اطلاع مشترکان خود می‌رسانند. توجه داشته باشید که همواره قبل از بکارگیری نسخه‌های بهنگام شده در یک محیط عملیاتی، آن‌ها را تست و پس از حصول اطمینان از صحت عملکرد اقدام به نصب نهایی آن‌ها در محیط واقعی نمود.

- پروتکل‌ها

برخی از حملات نظیر DoS به دلیل وجود ضعف امنیتی در پروتکل‌ها اتفاق می‌افتد. به عنوان نمونه، مهاجمان می‌توانند با ارسال سیلابی از بسته‌های اطلاعاتی سرویس و یا سرویس‌های ارائه شده توسط یک سرویس دهنده را غیرفعال نمایند. به منظور پیشگیری و پاسخ به موقع به این نوع از حملات می‌بایست اقدامات زیر را انجام داد:

- استفاده از فیلترینگ ورودی و خروجی

بسته‌های اطلاعاتی مشکوک می‌تواند بیانگر کنکاش در شبکه، تهاجم و یا یک کسب آگاهی لازم از وضعیت شبکه موجود توسط یک مهاجم باشد. بسته‌های اطلاعاتی دریافتی شامل یک آدرس داخلی می‌تواند نشاندهنده تلاش جهت نفوذ به شبکه و آنالیز آن باشد. با این نوع بسته‌های اطلاعاتی می‌بایست در اولین محل ممکن برخورد نمود. همچنین، می‌بایست پیکربندی روتر بگونه‌ای انجام شود که صرفا اجازه خروج بسته‌های اطلاعاتی با آدرس‌های IP داخلی معتبر را بدهد. بررسی بسته‌های اطلاعاتی خروجی، یک شبکه را در مقابل حملات از نوع DoS محافظت نخواهد کرد ولی این تضمین را ایجاد خواهد کرد که حمله‌ای با محوریت یکی از سرویس گیرندگان شبکه داخلی شکل نخواهد گرفت.

- مشاهده ترافیک ICMP از شبکه داخلی:

ICMP یک پروتکل stateless است که اجازه بررسی اطلاعات در دسترس هاست را از یک هاست به هاست دیگر فراهم می‌نماید. از پیام‌های مبتنی بر ICMP در موارد متداول زیر استفاده می‌گردد:

۱. Echo request : مشخص می‌نماید که یک گره (IP یک هاست و یا روتر) بر روی شبکه در دسترس است.

۲. Echo reply : پاسخ به یک درخواست ICMP echo
۳. Destination unreachable: به هاست اعلام می‌شود که دیتاگرام نمی‌تواند توزیع گردد.
۴. Source quench: به هاست اعلام می‌شود که دیتاگرام ارسالی را با نرخ پایین‌تری ارسال نماید (به دلیل شلوغی)
۵. Redirect: به هاست یک مسیر روت بهتر اعلام می‌شود.
۶. Time Exceeded: نشاندهنده این موضوع است که عمر مفید یک دیتاگرام به اتمام رسیده است.

بلاک کردن ترافیک ICMP برروی روتر perimeter باعث حفاظت شبکه در مقابل حملاتی نظیر Cascading ping floods می‌گردد. برای بلاک کردن این پروتکل دلایل قانع کننده متعددی وجود دارد. علیرغم دید انتقادی امنیتی نسبت به این پروتکل، از آن در موارد متعددی نظیر اشکال زدایی شبکه استفاده می‌گردد. بنابراین لازم است که استفاده از پروتکلICMP کاملا کنترل شده باشد.

- پیشگیری از پیام‌های TTL[1] که اعتبار آن‌ها به اتمام رسیده است با مقادیر صفر و یک: برای شمارش تعداد hopبین یک سرویس گیرنده و یک سرویس دهنده، trace routing از مقادیر TTL صفر و یا یک استفاده می‌نماید. trace routing، به مفهوم جمع آوری اطلاعات توپولوژی شبکه است. با بلاک کردن اینچنین بسته‌های اطلاعاتی، از ارایه اطلاعات تکمیلی که بیانگر جزئیات شبکه موجود است پیشگیری می‌گردد.

- عدم دریافت و یا فوروارد ترافیک directed broadcast:

ترافیک‌هایی اینچنین قادر به شمارش تعداد هاست موجود بر روی یک شبکه می‌باشند و از آن به عنوان ابزاری جهت آماده‌سازی و تدارک حملات DoS استفاده می‌گردد. بسته‌های اطلاعاتی که حاوی آدرس‌های مبداء زیر می‌باشند را می‌بایست بلاک نمود:

[1] Time To Live

جدول ۱-۳ بسته‌های اطلاعاتی که می‌بایست بلاک شوند[۱۱].

شرح	آدرس مبداء
Historical broadcast	0.0.0.0/8
RFC 1918 Private network	10.0.0.0/8
Loopback	127.0.0.0/8
Link local networks	169.254.0.0/16
RFC 1918 private network	172.16.0.0/12
TEST-NET	192.0.20.0/24
RFC 1918 private network	192.168.0.0/16
Class D multicast	224.0.0.0/4
Class E reserved	240.0.0.0/5
Unallocated	248.0.0.0/5
Broadcast	255.255.255.255/32

- دستیابی مدیریت

پیکربندی روتر از چه مکانی و به چه صورت انجام می‌شود؟ کدام پورت‌ها و اینترفیس‌ها فعال است و مدیران شبکه از چه شبکه و یا هاستی برای پیکربندی روتر استفاده می‌نمایند؟ دستیابی به مکان پیکربندی روتر می‌بایست محدود و هرگز از اینترفیس‌های مدیریتی تحت وب بدون رمزنگاری و رعایت مسائل امنیتی نمی‌بایست استفاده گردد. علاوه بر این رعایت موارد زیر نیز توصیه می‌گردد:

۱. غیرفعال کردن اینترفیس‌هایی که از آنان استفاده نمی‌گردد.
۲. ایجاد رمزهای قوی:

از رمزهای عبور مناسب و قدرتمند به منظور استفاده در هر mode روتر می‌بایست استفاده گردد. استفاده ترکیبی از حروف الفبایی، اعداد و حروف ویژه به منظور تعریف یک رمز عبور مناسب توصیه می‌گردد.

۳. استفاده از روتینگ استاتیک:

روتینگ ایستا از تغییر اطلاعات موجود در جدول روتینگ پیشگیری می‌نماید. یک مهاجم ممکن است بتواند با تغییر مسیرها حملات از نوع DoS را برنامه ریزی و یا درخواست‌ها را به یک سرویس دهنده مخرب هدایت نماید.

۴. بازبینی اینترفیس‌های مدیریتی وب

حتی المقدور سعی گردد که اینترفیس‌های مدیریتی خارجی غیرفعال و از روش‌های دستیابی داخلی به همراه لیست‌های دستیابی استفاده گردد. سرویس‌ها بر روی یک روتر پیکربندی شده و هر پورت فعال با یک سرویس خاص مرتبط می‌گردد. به منظور کاهش میدان عملیاتی مهاجمان، سرویس‌های پیش فرض که به وجود آنان نیاز نمی‌باشد را می‌بایست غیرفعال نمود. به عنوان نمونه سرویس‌های bootps و finger که از آنان بندرت استفاده می‌گردد را می‌توان غیرفعال نمود. همچنین لازم است پورت‌های‌فعال بر روی روتر بررسی و پورت‌هایی را که به وجود آن‌ها نیاز نمی‌باشد را غیرفعال نمود.

۵. بازبینی و لاگینگ

به صورت پیش فرض، روتر تمامی عملیات deny را لاگ می‌نماید. وضعیت فوق نمی‌بایست تغییر داده شود. همچنین لازم است که فایل‌های لاگ شده به صورت اداواری بررسی تا از وقوع حملات احتمالی پیشگیری بعمل آید. برخی از روترهای مدرن دارای مجموعه ای از امکانات جدید به منظور انجام عملیات مختلف و آماری بر روی داده لاگ شده می‌باشند.

۶. تشخیص مزاحمین

به منظور پیشگیری از حملات مبتنی بر TCP/IP، روتر می‌بایست قادر به شناسایی زمان بروز یک تهاجم و اعلام آن به مدیر سیستم باشد. مهاجمان در ابتدا سعی می‌نمایند که با اولویت‌های امنیتی یک شبکه آشنا شده و در ادامه با تمرکز بر روی آن‌ها حملات خود را برنامه ریزی می‌کنند. با استفاده از سیستم‌های تشخیص دهنده مزاحمین IDS[1]، می‌توان زمان و ماهیت وقوع یک تهاجم را بررسی نمود.

[1] Intrusion Detection Systems

فصل چهارم

سامانه مدیریت یکپارچه تهدید

۴-۱- سامانه مدیریت یکپارچه تهدیدUTM[1]

UTM عبارتست از سیستم مدیریت یکپارچه تهدیدات، شامل مجموعه‌ای کامل و جامع از تمامی راهکارهای امنیتی از قبیل[۱۲]:

- برقراری دیوار آتش[2]
- ایجاد شبکه خصوصی مجازی[3]
- ضدویروس[4]
- ضدهرزنامه[5]
- شناسایی و جلوگیری از نفوذگران[6]
- فیلترینگ محتوی[7]
- مدیریت پهنای باند[8]
- ضد جاسوس افزار، ضد برنامه‌های کلاهبرداری[9]

مزایای امنیت یکپارچه در این نهفته شده است که در حقیقت به‌جای اجرای سیستم‌های متعدد که بصورت جداگانه هر کدام سرویس‌های مختلفی را ارائه دهند(آنتی ویروس، فیلترینگ محتوا، جلوگیری از نفوذ و توابع فیلتر کردن هرزنامه) یک دستگاه تمامی این سرویسها را بصورت یکپارچه ارائه دهد. سازمان‌ها با استفاده از دستگاه‌های UTM دارای انعطاف پذیری بیشتری هستند. از مزیت‌های اصلی UTM می‌توان به سادگی، نصب و استفاده کارآمد و توانایی به روز رسانی تمامی توابع امنیتی اشاره کرد.

۴-۲- تاریخچه‌ای پیرامون UTM

اولین ویرایش‌های سیستم مدیریت یکپارچه تهدیدات با نام UTM، از اوایل سال ۲۰۰۳ ایجاد شده است. با توجه به بررسی‌های انجام گرفته اولین محصول UTM توسط شرکت ServGate به بازار ارائه شده است. از آن زمان تاکنون شرکت‌های بسیاری وارد این عرصه شده‌اند که محصول خود را بصورت نرم افزاری و یا همراه با سخت افزار ارائه می‌نمایند. راهکار استفاده از UTM در مواجهه با حملات روز افزون علیه سیستم‌های اطلاعاتی سازمان‌ها از طریق هک،

[1] **Unified Threat Management**
[2] Identity Based Firewall
[3] Virtual Private Network)VPN
[4] Anti-Virus
[5] Anti-Spam
[6] Intrusion Detection and Prevention
[7] Content Filtering
[8] Bandwidth management
[9] Anti-Spyware/ Phishing

ویروس‌ها، کرم امنیتی(ترکیبی از حملات و تهدیدهای خارجی و داخلی) ضروری به نظر می‌رسد. به علاوه تکنیک‌هایی که کاربران سازمان‌ها را به عنوان لینک‌های ارتباطی ضعیف مورد هدف قرار می‌دهند، عواقبی فراتر از حد تصور در پی دارند. در حال حاضر امنیت داده‌ها و دسترسی غیر مجاز کارمندان به عمده‌ترین نگرانی شرکت‌ها تبدیل شده‌است. به این دلیل هدف‌های مخرب و از دست رفتن اطلاعات منجر به ضررهای زیاد مالی برای شرکت‌ها شده‌است. اصولا این دستگاه‌های از فناوری ASIC سخت افزاری استفاده می‌کنند تا بالاترین عملکرد را داشته باشند.

۴-۳- سرویس‌های امنیتی تشکیل دهنده UTM

از آن‌جایی که یک محصول UTM تعداد زیادی سرویس امنیتی را در درون خود بکارگیری می‌کند، لذا حجم زیادی از توان پردازنده و حافظه را به خود اختصاص می‌دهد، و شرکت‌های معتبر تولید کننده UTM، از سخت‌افزارهای قوی و بکارگیری تکنیک‌های مختلف سخت‌افزاری و نرم‌افزاری در جهت افزایش عملکرد سیستم‌های خود استفاده می‌کنند. به این منظور معمولا فعالیت بخش‌هایی از سیستم که نیاز به حجم پردازنده بالایی دارد را به سخت‌افزار واگذار می‌کنند؛ بطور مثال بجای استفاده از VPN و یا IPS نرم‌افزاری از نمونه‌های معادل آن که بصورت سخت‌افزاری تولید شده‌اند، استفاده می‌شود. به این ترتیب هر سرویس امنیتی بصورت یک کارت سخت‌افزاری طراحی و در سامانه UTM مورد استفاده قرار گرفته و کارایی را فوق‌العاده افزایش می‌دهد. مهمترین سرویس‌های امنیتی تشکیل دهنده سیستم UTM عبارتند از[۱۲]:

۴-۳-۱- فایروال

فایروال وسیله‌ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف می‌کند. علاوه بر آن از آنجایی که معمولا یک فایروال بر سر راه ورودی یک شبکه می‌نشیند لذا برای ترجمه آدرس شبکه نیز بکار گرفته می‌شود. مشخصه‌های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از[۱۳]:

۱- توانایی ثبت و اخطار:

ثبت وقایع یکی از مشخصه‌های بسیار مهم یک فایروال به شمار می‌رود و به مدیران شبکه این امکان را می‌دهد که انجام حملات را کنترل کنند. همچنین مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می‌تواند براحتی به بخش‌های مهم از اطلاعات ثبت شده دسترسی

پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

۲- بازدید حجم بالایی از بسته‌های اطلاعات:

یکی از تستهای یک فایروال، توانایی آن در بازدید حجم بالایی از بسته‌های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده‌ای که یک فایروال می‌تواند کنترل کند برای شبکه‌های مختلف متفاوت است اما یک فایروال قطعا نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیتها از طرف سرعت پردازنده و بهینه سازی کد نرم‌افزار بر کارایی فایروال تحمیل می‌شوند. عامل محدودکننده دیگر می‌تواند کارت‌های واسطی باشد که بر روی فایروال نصب می‌شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

۳- سادگی پیکربندی:

سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه‌ها می‌شود به پیکربندی غلط فایروال بر می‌گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می‌کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزرای که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

۴- امنیت و افزونگی فایروال:

امنیت فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعا اجازه ورود هکرها و مهاجمان را به سایر بخشهای شبکه نیز خواهد داد. امنیت در دو بخش از فایروال، تامین کننده امنیت فایروال و شبکه است:

الف- امنیت سیستم عامل فایروال : اگر نرم افزار فایروال بر روی سیستم عامل جداگانه‌ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل، می‌توانند نقاط ضعف فایروال نیز به حساب بیایند. بنابراین امنیت و استحکام سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

ب- دسترسی امن به فایروال جهت مقاصد مدیریتی : یک فایروال باید مکانیزم‌های امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روش‌ها می‌توانند رمزنگاری

را همراه با روش‌های مناسب تعیین هویت بکار گیرند تا بتوانند در مقابل نفوذگران تاب بیاورند.

یک سیستم تشخیص نفوذ عبارتست از ابزاری که منحصرا برای پایش دروازه‌های اطلاعاتی، فعالیتهای خصمانه و نفوذهای شناخته شده پیکربندی شده‌است. یک IDS یک ابزار تخصصی است که بخوبی قادر است تا ترافیک شبکه و یا فعالیتهای میزبان‌های آن را تجزیه و تحلیل کند. داده‌های تحلیل شده می‌توانند از آنالیز بسته‌های شبکه گرفته تا محتوای فایلهای Log متعلق به فایروالها، روترها و سرویس‌دهنده‌ها و نیز فایلهای Log سیستم‌های محلی و داده‌های جریان شبکه را شامل شوند. بعلاوه، یک IDS معمولا دارای یک پایگاه داده از الگوها و مشخصه‌های حملات شناخته شده است که می‌تواند این الگوها و مشخصه‌ها را با داده‌های ترافیک شبکه و رفتار شبکه برای یافتن موارد انطباق مقایسه کند. در مواجهه با موارد یافته شده ترافیک خطرناک، سیستم تشخیص نفوذ می‌تواند هشدارهایی را اعلام کرده و یا اقدامات خودکار مختلفی را همچون قطع جلسه ارتباطی یا لینک اینترنتی مبدأ حمله، مسدود کردن وی با به‌روز کردن قواعد فایروال و یا انجام دادن فعالیتهای بیشتر در جهت شناخت دقیقتر نفوذکننده و جمع‌آوری شواهد بیشتری در مورد فعالیتهای شرورانه انجام دهد. درصورتی که یک سیستم IDS توان پیشگیری از نفوذ را نیز داشته باشند به عنوان IPS معرفی می‌شوند؛ که در این حالت معمولا سیستم تشخیص نفوذ یا با فایروال در ارتباط بوده و بسته‌ها را از آن دریافت می‌کند و یا اینکه خود در لایه‌های پایینی هم سطح فایروال قرار داشته و فعالیت جلوگیری از نفوذ را نیز انجام می‌دهد[۱۴].

۴-۳-۲- شبکه اختصاصی مجازی[1] (VPN)

VPN دو کامپیوتر یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می‌گیرد به هم متصل می‌کند. برای نمونه می‌توان به دو کامپیوتر یکی در تهران و دیگری در مشهد که در فضای اینترنت به یک شبکه وصل شده‌اند اشاره کرد. VPN از نگاه کاربر کاملا مانند یک شبکه محلی به نظر می‌رسد. برای پیاده‌سازی چنین چیزی، VPN به هر کاربر یک ارتباط IP مجازی می‌دهد. داده‌هایی که روی این ارتباط آمد و شد دارند را سرویس گیرنده نخست به رمز در آورده و در قالب بسته‌ها بسته‌بندی کرده و به سوی سرویس دهنده VPN می‌فرستد. اگر بستر این انتقال اینترنت باشد بسته‌ها همان بسته‌های IP خواهند بود. سرویس گیرنده VPN بسته‌ها را پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می‌دهد.

[1] Virtual Private Network

۴-۳-۳- آنتی ویروس

ویروس‌ها برنامه‌هایی هستند که به شکل پنهانی، موقع اجرا شدن برنامه آلوده خود را به برنامه‌های اجرایی نظیر فایل‌های COM و EXE می‌چسبانند و معمولا بدون اینکه تاثیری در کار اصلی برنامه آلوده بگذارند، منتظر زمان فعالیت نهایی یا برقراری شرط خاصی می‌شوند. حال این فعالیت می‌تواند بزرگتر کردن فایلهای مختلف DATA باشد، یا آلوده کردن فایلهای اجرایی و یا از بین بردن اطلاعات PARTITION TABLE، معدوم کردن اطلاعات با ارزش یا از کار انداختن فایل‌های اجرایی و ... باشد. ولی در هر حال یک چیز در اکثر ویروس‌ها مشترک می‌باشد و آن انتقال ویروس از فایل‌های آلوده به فایل‌های سالم است. نرم‌افزارهای آنتی‌ویروس تمام فایل‌ها را بطور خودکار بررسی کرده و فایل‌هایی که دارای گونه‌های شناخته شده ویروس‌ها هستند را شناسایی و عکس‌العمل مناسب انجام می‌دهند.

۴-۳-۵- آنتی اسپم

اسپم در کامپیوتر به ایمیل‌هایی گفته می‌شود که به طور ناخواسته برای ما فرستاده می‌شوند و جنبه تبلیغاتی دارند. راه‌های مختلفی برای مقابله با اسپم‌ها در جاهای مختلف آمده و حتی یاهو هم یک آنتی اسپم را برای کاربرانش پیشنهاد کرده است.

۴-۳-۶- فیلترینگ

فیلتر ابزاری است که به منظور تصفیه اتصالات وب استفاده می‌شود. در کشورهای مختلف دنیا فیلترینگ به دو روش انجام می‌شود: فیلتر کردن نشانی‌های اینترنتی براساس یک لیست سیاه(در یک پایگاه داده)، و فیلتر کردن براساس محتوای هر صفحه اینترنتی. روش دوم در دنیا به فیلتر محتوا[1] معروف است که برای پهنای باند خیلی بالا قابل انجام نیست.

[1] content filter

فصل پنجم:

مرکز داده تهدیدات و ملاحظات پدافند غیرعامل

۵-۱- مقدمه

توسعه فناوری اطلاعات و ارتباطات و تحقق جامعه اطلاعاتی که (رکن اصلی آن اطلاعات است و نه فناوری) بر پایه دو زیرساخت مهم مراکز داده‌ای[۱] و زیر ساختار ارتباطی[۲] شکل می‌گیرد. با توجه به اینکه مراکز داده محل نگهداری و پردازش انواع اطلاعات ارزشمند و بعضا حساس و حیاتی هستند، باید از آن‌ها در برابر انواع تهدیدها و بلایا محافظت کرد. چرا که در صورت بروز یک حادثه جزئی ممکن است خسارات جبران ناپذیری، به ویژه به داده‌ها و اطلاعات ارزشمند موجود در این مراکز وارد آید. بنابراین در طراحی ساختار مراکز داده باید همواره سه اصل اساسی پدافند غیرعامل یعنی امنیت، ایمنی و پایداری مورد توجه قرار گیرد. به کارگیری تمهیدات و ملاحظات پدافند غیرعامل در متن طراحی‌ها، توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می‌سازد. در این بخش سعی شده است با استفاده از بررسی منابع قابل دسترسی، مراکز مهم داده ای موجود در جهان، فضاهای مورد نیاز و اعمال ملاحظات پدافندغیرعامل در طراحی معماری مراکز داده نیز می‌باشد.

مراکز داده به عنوان قلب تپنده زیرساخت‌های فناوری اطلاعات یک کشور نقش مهمی در تامین امنیت کشور دارند و با به خطر افتادن امنیت مراکز داده امنیت سرویس‌های مبتنی بر آن نیز به مخاطره می‌افتد. با توجه به روند رو به رشد و سرعت گسترش فناوری اطلاعات در ایران، ایجاد مراکز داده و توسعه ی آن‌ها اهمیت بسیاری یافته است. از سوی دیگر لحاظ نمودن اصول پدافند غیرعامل و رعایت اصول امنیتی نیز در طراحی و پیاده سازی مراکز داده اهمیت بسیاری دارد. هر مرکز داده شامل اجزایی است که هر یک متناسب با وظایفشان از ساختار خاصی برخوردار می‌باشند. برای ارائه خدمات به هریک از این اجزاء لازم است یک زیرساخت ارتباطی ایجاد شود تا از این طریق، رابطه بین اجزاء برقرار شود. تعیین ساختار مراکز داده به شدت به نوع برنامه‌های کاربردی و بار ترافیک آن دارد.

با توجه به نقش، اهمیت و حساسیت مراکز داده در کشور لازم است این موضوع به صورت ریشه‌ای و اصولی و از ابعاد مختلف مورد بررسی قرار گیرد. از آنجا که تهدیدات متصور در این حوزه در حال حاضر برای کشور بسیار زیاد و دارای ابعاد مختلفی است، می‌بایست به موضوع پدافند غیرعامل در مراکز مهم نظیر مراکز داده و غیره با نگاهی ملی نگریسته شده و ابعاد مختلف تهدیدات مورد بررسی قرار گرفته و راهکارهای عملی و اجرایی متناسب ارائه شود. از این رو می‌بایست تلاش شود تا با ارایه یک مدل بومی منطبق بر تهدیدات موجود، راهکارهای متناسب با اهمیت و سطوح مختلف مراکز داده بیان گردد.

ابتدا لازم است با دو تعریف اولیه آشنا شویم:

[1] *Data Center*
[2] *Switching Network*

۱. مرکز داده: مرکز داده محلی برای نگهداری سامانه‌های کامپیوتری و تکنولوژی‌های وابسته مانند سامانه‌های ارتباطی و سامانه‌های ذخیره سازی اطلاعات است. این مراکز معمولا شامل سامانه‌های پشتیبانی تامین منبع؛ پشتیبانی شبکه‌های ارتباطی و سامانه‌های امنیتی مخصوص می‌باشد.

۲. فضای امن: فضای امن به فضایی اطلاق می‌گردد که در مقابل اثرات بارهای ناشی از انفجار کمتر در معرض خطر قرار گرفته و نسبت به سایر فضاهای ساختمان معمولی یا فضای باز از ایمنی و مقاومت بیشتری برخوردار باشد.

۵-۲- تهدیدات مربوط مراکز داده

با توجه به خصم جبهه‌ی استکبار با نظام مقدس جمهوری اسلامی و اهمیتی که مراکز داده برای کشور دارد و روز به روز وابستگی به این مراکز بیشتر می‌شود، این زیرساخت می‌تواند به عنوان یکی از اهداف دشمن در زمان حمله و حتی در زمان صلح نیز باشد و می‌توان دو نوع مختلف از تهدیدات را برای مراکز داده متصور شد، تهدیدات نوع اول که در این قسمت به آن پرداخته شده است تهدیدات ناشی از سلاح‌های متعارف دشمن می‌باشد اما دسته دوم تهدیدات این مراکز، تهدیداتی هستند که به دنبال نابود کردن یا دسترسی به اطلاعات حیاتی و حساس موجود در این مراکز است که به تهدیدات سایبری معروفند، که هم در زمان صلح و جنگ ادامه دارند. سلاح‌های متعارفی که معمولاً دشمن برای این مراکز استفاده می‌کنند عبارتند از[۱۵]:

۱. سلاح‌های EMP:

با توجه به این موضوع که بیشتر تجهیزات موجود در مراکز داده از سیستم‌های الکترونیکی هستند. دشمن برای صدمه زدن به این مراکز، با استفاده از سلاح‌های EMP و بمب‌های الکترومغناطیسی مبادرت به ایجاد پالس‌هایی با دامنه بالا در مدت کوتاه می‌نماید که موجب تخریب کامل و جبران ناپذیر در سیستم‌ها و تجهیزات الکترونیکی می‌گردد.
برای مقابله با این سلاح‌ها می‌توان از روش‌های زیر استفاده می‌کنند:

- اصل جداسازی زیرسامانه‌ها
- زمین کردن
- استفاده از فیلترهای EMI

۲. موشک‌های دقیق و نفوذ کننده:

معمولا مراکز داده حیاتی و حساس را به صورت سازه‌های ایمنی در عمق مناسبی از خاک و یا در دل کوه می‌سازند تا آسیب پذیری این مراکز را در برابر موج انفجارهای رو سطحی افزایش داده و هزینه ی دشمن را برای آسیب زدن به این مراکز افزایش دهند بنابراین دشمن برای از بین بردن این مراکز با توجه به زیرزمینی بودن آن‌ها از موشک‌های دقیق و نفوذ کننده استفاده می‌نماید. حال با توجه به موارد ذکر شده برای مقابله با این سلاح‌ها دو روش وجود دارد، در روش اول با توجه به مقدار نفوذ سلاح‌های دشمن عمق سازه زیرزمینی تعیین گردد و در روش دوم با استفاده از اصل پراکندگی می‌توان هزینه‌ی دشمن را به نحوی افزایش داد که استفاده از این نوع سلاح برای دشمن بسیار گرانتر از هدف باشند.

۵-۳- ماموریت‌های مرکز داده :

بعضی افراد فکر می‌کنند مرکز داده مکانی برای قرارگیری سرورها است در حالی که برخی افراد تصوری کاملا متفاوت‌تر از یک مرکز داده دارند. شاید در زمانی این یک تصور صحیح بود اما اکنون مراکز داده چیزی بیش از یک مکان امن برای سرویس دهنده هستند. امروزه با پیشرفت تکنولوژی و نحوه تعاملات جدید مبتنی بر اطلاعات و تجمع اطلاعات، این مفهوم تغییر کرده و به مکانی برای ذخیره‌سازی اطلاعات یک سازمان تبدیل شده است که برای عملکرد صحیح یک سازمان ضروری هستند و عدم وجود این اطلاعات حیاتی به معنای نابودی سازمان است. ماموریت مراکز داده را می‌توان به صورت زیر بیان نمود[۱۵]:

- نگهداری Data Baseها و میزبانی فضا برای نرم افزارها از دیگر کاربردها هستند.
- ارایه خدمات نرم افزاری جهت پیشبرد اهداف سازمان‌ها می‌باشد.
- نرم افزارهایی که جهت ارایه خدمات به صورت خاص برای یک سازمان (مثلا نیروها نظامی) تهیه می‌شوند و یا نرم افزارهای آماده مانند ERP، CRM

۵-۴- معرفی مراکز داده زیرزمینی :

در این بخش به معرفی مختصری از مراکز داده معروف جهان پرداخته می‌شودکه این مراکز عبارتند از[۱۶]:

۱. مرکز داده Swiss Fort Knox:

این مرکز در کشور سویس ساخته شده است که دارای ۲ قسمت مجزا است که در دل کوه ساخته شده که از هم ۱۰ کیلومتر فاصله دارند. در تجهیزات استفاده شده در این مرکز از آخرین تکنولوژی روز دنیا استفاده شده است و در برابر انواع تهدیدات طبیعی نظیر سیل، زلزله و زمین لغزش مقاوم بوده و در طراحی آن تهدیدات مصنوعی مانند حملات تروریستی، حملات نظامی در نظر گرفته شده و دربرابر سلاح‌های EMP، تشعشعات هسته ای و گازهای سمی شیمیایی نیز مقاوم است.

شکل ۵-۱- نمایی از مرکز داده Swiss Fort Knox

شکل۵-۲- بخش‌های مختلف مرکز داده Swiss Fort Knox

۲. مرکز داده Bahnhof Pionen

این مرکز به نام مرکز جیمز بوند شرور شناخته می‌شود که به عنوان انبار نظامی استفاده می‌شده که در ۳۰ متری زیر زمین در استکهلم سوئد قرار دارد. این مرکز داده دارای آبشارهای مصنوعی می‌باشد و اتاق کنفرانس آن در محوطه‌ای بالاتر از کف تونل قرار دارد. در این مرکز از

سازماندهی شعاعی استفاده شده است و فضاهای مختلف آن را می‌توانید در شکل زیر مشاهده نمایید.

شکل ۵-۳- پلان مرکز داده Bahnhof Pionen

۳. مرکز داده Smart Bunker

این مرکز یکی از مراکز بسیار امن است که در گذشته به عنوان مرکز فرماندهی ناتو در انگلستان مورد استفاده قرار می‌گرفت. کل مساحت این مرکز داده حدود ۲۸۰۰ متر مربع است که انرژی مورد نیاز آن از انرژی باد تامین می‌شود.

۴. کوهستان آهن[1]

این مرکز داده در اختیار شرکت ماریوت است. این مرکز در ۲۲۰ فوتی زیر زمین در غار آهکی در نزدیکی پیتسبورگ واقع شده است. این مرکز دارای بخش آتش‌نشانی، تصفیه‌خانه، نیروهای حفاظت فیزیکی و همچنین نیروهای تعمیر و نگهداری ۲۴ ساعته می‌باشد.

شکل۵-۴- مرکز داده کوهستان آهن

[1] *Iron Mountain*

۵. مرکز داده مونتگومری وستلند :

این مرکز داده در فاصله ۴۰ مایلی از مترو هوستون و ۱۰۰ مایلی خلیج کاست قرار گرفته است. این مرکز داده در ۳۰۰ فوتی بالای سطح دریا و در عمق ۴۰ فوتی زیر زمین واقع شده است. مساحت کل آن ۳۳۰۰۰ فوت مربع می‌باشد که در دو طبقه ساخته شده است. این تأسیسات توسط کمپانی نفتی وستلین اویل ایجاد شده است و به دلیل اهمیت محافظت از دارایی‌های آن در زمان ساخت، کلیه ملاحظات و تدابیر مقابله با آسیب‌های بمباران‌های هسته‌ای در آن پیش‌بینی شده است. این مرکز در گذشته به نام Westlin Bunker شناخته می‌شد و از امن‌ترین نقاط جهان محسوب می‌شود.

۶. مرکز داده The mountain Complex

از این مرکز داده که در ابتدا به عنوان مرکز مقابله با بحران در یک معدن متروکه دولومیت ایجاد شده بود، در حال حاضر به عنوان محل نگهداری نسخه‌های پشتیبان اطلاعات اقتصادی مربوط به هزاران شرکت تجاری استفاده می‌شود و در شهر ازارکس در نزدیکی برانسون ایالت میسوری واقع است.

۷. مرکز داده Spring Net Underground

یکی از مراکز داده زیرزمینی بزرگ که در حدود سی متری عمق زمین قرار دارد و مساحتی در حدود ۵۶۰۰۰ فوت مربع دارد که در غارهای آهکی در شهر میزوری واقع شده است. این مرکز داده محل نگهداری اطلاعات بیماران شبکه‌های اطلاعاتی بیمارستانی می‌باشد.

۸. مرکز داده StrataSpace

این مرکز داده زیرزمینی در حدود ۵۰۰۰۰۰ فوت مربع مساحت دارد که در خارج از شهر لوییزویل واقع شده است. نمایی از ورودی مرکز داده StrataSpace در شکل ۵ نشان داده شده است.

شکل۵-۵- نمایی از ورودی مرکز داده StrataSpace و اتاق کنترل این مرکز

۵-۵- طراحی معماری مراکز داده:

در این بخش سعی شده است با توجه به تهدیدات اشاره شده در بخش قبل و بیان معیارهای اساسی و فلسفه طراحی مراکز داده و با استفاده از آیین نامهTIA و بررسی انجام شده در بخش قبل در پیشینه طراحی این مراکز برای شناسایی فضاهای مورد نیاز یک مرکز داده در سطح راهبردی و عملیاتی، ملاحظاتی در طراحی آن‌ها ارائه گردد.

۵-۵-۱- معیارهای اساسی در طراحی مرکز داده :

- ایمنی
- محدودیت‌های فضا
- محدودیت‌های بودجه
- محدودیتهای زمان

۵-۵-۲- ویژگی‌های طراحی :

اساس ویژگی‌های طراحی بر موارد زیر استوار است[۱۷]:

- ساده سازی[1]
- انعطاف پذیری[2]

[1] *Simplicity*
[2] *Flexibility*

انعطاف پذیری به این معناست که به راحتی بتوان آن را توسعه داد و در صورت تغییر تکنولوژی بتوان آن مرکز را به راحتی به روز نمود.

- مقیاس پذیری[1]
- مادولار بودن [2]

طرح به گونه‌ای طراحی گردد که فازهای مختلف بعدی هم همانند فاز ۱ باشد تا توسعه‌ی بعدی آن راحتر و ارزان تر باشد.

۵-۶-۳- فضاهای مورد نیاز یک مرکز داده امن:

فضاهای عملیاتی اختصاص یافته به مرکز داده بر اساس آیین نامه ی TIA-942 باید به گونه‌ای باشد که این فضا به سادگی قابل توسعه بوده و اعمال تغییرات محیطی در آن به سادگی امکان پذیر باشد. در مرکز داده باید فضای خالی در نظر گرفت به گونه‌ای که این فضای خالی بتواند رک‌ها و کابینت‌های مورد نیاز آتی را در خود جا دهد. فضای اطراف مرکز داده نیز باید به درستی برای توسعه و الحاقات آتی طراحی شود. بخش عمده‌ی این استاندارد به مشخصات فنی مرکز داده مربوط می‌شود. این استانداردمحیط‌های عملیاتی خاصی را در راستای کمک به تعیین مکان تجهیزات بر اساس طراحی توپولوژی ستاره ای توصیه می‌کند. طراحی مرکز داده با این محیط‌های عملیاتی امکان اضافه شدن و به روز شدن برنامه‌های کاربردی و سرورها را با حداقل مدت زمان از کار افتادگی فراهم می‌کند. بر اساس این استاندارد یک مرکز داده باید شامل محیط‌های عملیاتی کلیدی زیر باشد:

- فضاهای دسترسی دهنده و سرویس دهنده

فضاهای دسترسی دهنده و سرویس دهنده عموما داخل یا بیرون اتاق کامپیوتر قرار می‌گیرند. این فضاها در داخل اتاق ورودی نیازی به پارتیشن بندی ندارند، چرا که اتاق ورودی تحت کنترل دقیق قرار دارد. فضاهای دسترسی دهنده و سرویس دهنده‌ای که داخل اتاق کامپیوتر قرار می‌گیرند نیازمند دسترسی ایمن به فضاها هستند.

[1] *Scalability*
[2] *Modularity*

- منطقه توزیع اصلی

فصل مشترک اتاق ورودی با اتاق کامپیوتر منطقه ی توزیع اصلی است. اتاق ورودی می‌تواند در کنار منطقه توزیع اصلی قرار بگیرد یا با آن ترکیب شود. منطقه توزیع اصلی شامل اتصالات متقاطع اصلی است که نقطه‌ی مرکزی توزیع سیستم کابل کشی ساختار یافته مراکز داده بوده و در مواقعی که منطقه توزیع تجهیزات مستقیما از منطقه توزیع اصلی استفاده می‌کند، می‌تواند شامل اتصالات متقاطع افقی باشد. این فضا داخل اتاق کامپیوتر قرار دارد و می‌تواند به منظور تامین امنیت بیشتر، در یک اتاق مخصوص چند عملکردی در داخل مرکز داده واقع شود. هر مرکز داده می‌بایست حداقل یک منطقه‌ی توزیع اصلی داشته باشد. از آنجا که این فضا مرکز فعالیت ساختار کابل کشی مرکز داده است، روترهای هسته اتاق کامپیوتر، سوئیچ‌های LAN هسته، سوئیچ‌هایSAN هسته و PBXها اغلب درون منطقه توزیع اصلی قرار می‌گیرند. تجهیزات مورد نیاز دسترسی دهنده نیز اغلب در منطقه توزیع اصلی قرار می‌گیرد تا در اتاق ورودی نیازی به مدار نبوده و محدودیت‌های حداکثر طول مجاز مدار رعایت شود. زمانی که اتصالات متقاطع افقی در منطقه توزیع اصلی قرار نگرفته باشد، می‌توان از منطقه توزیع افقی به عنوان منطقه توزیع تجهیزات نیز استفاده نمود. در این صورت منطقه توزیع افقی می‌تواند شامل اتصالات متقاطع افقی (به عنوان نقطه توزیع کابل کشی به منطقه توزیع تجهیزات) باشد. منطقه توزیع افقی داخل اتاق کامپیوتر قرار گرفته، لیکن می‌تواند به منظور امنیت بیشتر در یک اتاق مخصوص در اتاق کامپیوتر قرار گیرد. منطقه توزیع اصلی، نقطه‌ی مرکزی است که سیستم کابل‌کشی مرکز داده در آن قرار گرفته است. همان‌گونه که بیان شد هر مرکز داده می‌بایست حداقل یک منطقه‌ی توزیع اصلی داشته باشد. در مراکز داده‌ای که کاربران متعددی دارند، نظیر مراکز داده اینترنتی و تجهیزات چند منظوره منطقه‌ی توزیع اصلی می‌بایست فضای امنی باشد. منطقه توزیع اصلی می‌بایست در مرکز فضاها قرار بگیرد تا از استانداردهای حداکثر فاصله مجاز برای پشتیبانی، شامل حداکثر طول کابل‌های که دسترسی دهنده برای اتاق ورودی مورد استفاده قرار می‌دهد عدول ننماید. ملاحظات معماری، مکانیکی و الکتریکی منطقه توزیع مرکزی نظیر اتاق کامپیوتر است.

- منطقه توزیع افقی

منطقه توزیع افقی فضایی است که امکان سیم کشی به منطقه توزیع تجهیزات را فراهم می‌نماید. سوئیچ‌های LAN، سوئیچ‌های SAN و میز فرمان پشتیبانی کننده تجهیزات نهایی اغلب در منطقه توزیع افقی قرار می‌گیرند. منطقه توزیع افقی معمولا شامل سوئیچ‌های LAN، سوئیچ‌های SAN، و سوئیچ‌های کیبورد، ویدئو و ماوس برای تجهیزات نهایی مستقر در منطقه توزیع تجهیزات است. مراکز داده می‌توانند شامل فضاهای چند طبقه برای اتاق‌های کامپیوتر باشند که هر طبقه توسط اتصالات متقاطع افقی مخصوص به خود تغذیه می‌شود. در مراکز داده کوچک،

از آنجا که امکان پشتیبانی کل اتاق کامپیوتر توسط منطقه توزیع مرکزی وجود دارد، ممکن است نیازی به منطقه توزیع افقی نباشد. با این وجود اغلب مراکز داده معمولی دارای چندین منطقه‌ی توزیع افقی می‌باشند.

منطقه توزیع اصلی می‌تواند به عنوان منطقه توزیع افقی برای تجهیزات نزدیک یا حتی برای کل اتاق کامپیوتر (اگر اتاق کامپیوتر کوچک باشد) به کار برده شود. برای هر طبقه می‌بایست حداقل یک منطقه توزیع افقی وجود داشته باشد. ممکن است مناطق توزیع افقی اضافی برای پشتیبانی از تجهیزات در برابر محدودیت‌های طول افقی کابل‌ها نیاز باشد. حداکثر تعداد اتصالات به ازای هر منطقه ی توزیع افقی می‌بایست مطابق ظرفیت سینی کابل‌ها بوده، امکان توسعه ی آتی را نیز فراهم آورد. در مراکز داده ای که دارای کاربران متعددی می‌باشند، نظیر مراکز داده ی اینترنتی و تجهیزات چندمنظوره، منطقه ی توزیع افقی می‌بایست فضای امنی باشد. الزامات معماری، الکتریکی و مکانیکی منطقه توزیع افقی نیز نظیر اتاق کامپیوتر است.

- منطقه توزیع تجهیزات

منطقه توزیع تجهیزات فضایی است که به تجهیزات نهایی نظیر سیستم‌های کامپیوتری و تجهیزات ارتباطی اختصاص داده شده است. این فضا می‌تواند به عنوان اتاق ورودی، منطقه توزیع اصلی و منطقه توزیع افقی مورد استفاده قرار بگیرد. در صورت تمایل می‌توان یک نقطه اتصال داخلی بین کابل کشی افقی ایجاد نمود، به این نقطه اتصال در اصطلاح منطقه توزیع ناحیه ای اطلاق می‌شود، که مابین منطقه توزیع افقی و منطقه توزیع تجهیزات واقع می‌شود تا موجب افزایش انعطاف پذیری فضا گذشته، چیدمآن‌های متنوعی را امکان پذیر سازد. منطقه توزیع تجهیزات اتاق‌های ارتباطی، اتاق ورودی، منطقه توزیع اصلی و منطقه ی توزیع افقی را در بر نمی‌گیرد. تجهیزات نهایی اغلب یا روی کف و یا روی کابینت‌ها و قفسه‌ها قرار می‌گیرند. کابل‌های افقی در منطقه توزیع تجهیزات پایان یافته و به سخت افزارهای قرار گرفته روی کابینت‌ها و قفسه‌ها متصل می‌شوند. می‌بایست برای هر قفسه یا کابینت انرژی کافی و سخت افزار موردنیاز تعبیه شوند تا طول سیم‌های رابط و خطوط انرژی کاهش یابد.

- منطقه پشتیبانی مراکز داده

منطقه پشتیبانی مرکز داده فضایی بیرون از اتاق کامپیوتر است که به پشتیبانی از تجهیزات اتاق کامپیوتر اختصاص داده شده است. این فضا می‌تواند شامل مرکز عملیات، پشتیبانی دفاتر پرسنل، اتاق ایمن، اتاق‌های الکتریکی، اتاق‌های مکانیکی، انبارها، اتاق‌های باز کردن تجهیزات و باراندازها باشد. مرکز عملیات ممکن است نیازمند سیم کشی برای تجهیزات نصب شده روی دیوارها و سقف (نظیر مانیتورها و تلویزیون‌ها) باشد. هریک از اتاق‌های الکتریکی، مکانیکی، انبارها،

اتاق‌های باز کردن تجهیزات و باراندازها می‌بایست دارای حداقل یک تلفن دیواری باشند. اتاق‌های الکتریکی و مکانیکی می‌بایست حداقل یک اتصال اطلاعاتی برای دسترسی به سیستم مدیریت تجهیزات داشته باشند.

۵-۶-۴- ملاحظات معماری فضاهای عملیاتی کلیدی مرکز داده :

موارد زیر در معماری فضاهای عملیاتی کلیدی مد نظر قرار می‌گیرد[۱۸]:

- سیستم‌های زیر ساخت یکپارچه
- سیستم تغذیه جریان برق

به منظور حفظ ایمنی و افزایش ضریب امنیت تجهیزات موجود باید دو منبع برای تسهیلاتی مانند برق، آب ایجاد نمود. برق مورد نیاز باید از دو بخش مجزا تامین شود.

- سیستم تهویه و خنک کننده‌ها

تجهیزات الکتریکی و تجهیزات پردازش اطلاعات از نظر گرما و رطوبت به شرایط ویژه‌ای برای کار نیاز دارند. بنابراین سامانه تهویه باید به گونه‌ای طراحی شود که بتوان عواملی نظیر گرما، رطوبت، میزان هوای لازم و ... را کنترل نمود. سامانه‌های خنک‌کننده مرکز داده باید به گونه‌ایی عمل کنند که دمای مرکز داده را بین ۲۱ تا ۲۳ درجه سانتیگراد نگه دارند و رطوبت نسبی آن بین ۴۵ تا ۵۰ درصد باشد. همچنین یک خنک کننده اضافی برای مواقع ضروری باید در نظر گرفته شود. سیستم تهویه در این مراکز به این گونه است که در کف به فاصله یکی در میان بین کابینت‌ها و خروجی کانال‌های هوای سرد قرار دارد و در فاصله‌های دیگر در سقف، کانال‌هایی برای جمع آوری هوا گرم قرار گرفته‌اند که هوای خنک از بین دستگاه‌ها گذشته و از طریق کانال‌های موجود در سقف آن طرف دستگاه‌ها جمع می‌گردد.

- کف‌های کاذب :

با توجه به سیستم تهویه و دسته بندی کابل‌هایی که از کف این فضاها می‌گذرد، کف این فضاها را به صورت کاذب اجرا می‌کنند.

- سیستم امنیت فیزیکی:

سیستم‌های امنیتی فیزیکی به کار رفته در مراکز داده عبارت است از:

۱. سیستم اعلام حریق(سنسور دود و گرما)
۲. سیستم اطفای حریق

۳. سیستم خاموش کردن سیستم‌ها در شرایط خاص
۴. سنسورهای حساس به حرکت
۵. سنسورهای حساس به آب
۶. سنسورهای مشخص کننده میزان رطوبت

۵-۷- ملاحظات پدافند غیر عامل در طراحی معماری این مراکز

۱. با توجه به وابستگی شدید این مراکز به تجهیزات الکترونیکی و این موضوع که سلاح‌های EMP یکی از تهدیدات محتمل این مراکز می‌باشند باید تمام سیستم‌ها الکترونیکی به صورت مناسبی به زمین متصل گردند یا از فیلترهای EMI در این تجهیزات استفاده گردد.
۲. باید در تمام مراحل طراحی تا ساخت مراکز داده اصول استتار، اختفا و فریب صورت گیرد.
۳. می‌توان با استفاده از اصل پراکندگی، به جای یک مرکز داده بزرگ چندین مرکز کوچکتر و با فاصله مناسب ایجاد نمود تا حمله به این مراکز برای دشمن صرفه اقتصادی نداشته باشد.
۴. در طراحی سیستم‌های تهویه باید برای جلوگیری از ورود امواج به مرکز حتماً حداقل یک خم و حداکثر دو خم نود درجه تعبیه گردد.
۵. با توجه به امکان حملات شیمیایی و میکروبی باید فیلترهایی برای سیستم تهویه تعبیه شود.
۶. تمام ورودی‌ها و خروجی‌ها باید موج گیر و سیستم هوابند داشته باشند.
۷. با انتخاب عمق مناسب برای اجرای این مراکز می‌توان از آسیب پذیری آن‌ها در برابر موشک‌های دقیق و نفوذ کننده کاست.
۸. این مراکز وابستگی شدیدی به انرژی برق دارند و همانگونه که قبلا اشاره شد علاوه بر استفاده از برق شهری باید ژنراتورهایی در نظر بگیرند تا در هنگام قطع برق وارد مدار شوند و از زمان قطع برق تا بکار افتادن ژنراتورها باید باطری‌های شارژ شده ای در نظر گرفته شوند که برق لازم را برای سیستم‌ها مهیا سازند.

فصل ششم

استانداردهای امنیت اطلاعات

۶-۱- مقدمه

زیرساخت‌هایی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیرساخت‌های امنیت فضای تبادل اطلاعات در کشور، تاثیر بسزائی در ایمن‌سازی فضای تبادل اطلاعات خواهند داشت. لذا به‌منظور رفع نابسامانی موجود در وضعیت امنیت فضای تبادل اطلاعات همزمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور، توجه به مقوله ایمن‌سازی فضای تبادل اطلاعات، ضروری به نظر می‌رسد. این امر علاوه بر کاهش صدمات و زیان‌های ناشی از وضعیت فعلی، نقش موثری در فرآیند تدوین سند راهبردی امنیت فضای تبادل اطلاعات کشور خواهد داشت.

۶-۲- سیستم مدیریت امنیت اطلاعات [1]

با ارایه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمان‌ها، دفعتا مقدور نمی‌باشد و لازم است این امر بصورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام گیرد. برای این منظور لازم است هر سازمان بر اساس یک متدولوژی مشخص، اقدامات زیر را انجام دهد[۱۹]:

۱. تهیه طرح‌ها و برنامه‌های امنیتی مورد نیاز سازمان
۲. ایجاد تشکیلات مورد نیاز جهت ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان
۳. اجرای طرح‌ها و برنامه‌های امنیتی سازمان

در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها ارائه شده‌اند که استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد و گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد از برجسته‌ترین استانداردها و راهنماهای فنی در این زمینه محسوب می‌گردند.

در این استانداردها، نکات زیر مورد توجه قرار گرفته شده است:

۱. تعیین مراحل ایمن‌سازی و نحوه شکل‌گیری چرخه امنیت اطلاعات و ارتباطات سازمان
۲. جزئیات مراحل ایمن‌سازی و تکنیکهای فنی مورد استفاده در هر مرحله
۳. لیست و محتوای طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان

[1] ISMS : Information security management system

۴. ضرورت و جزئیات ایجاد تشکیلات سیاستگذاری، اجرائی و فنی تامین امنیت اطلاعات و ارتباطات سازمان
۵. کنترل‌های امنیتی موردنیاز برای هر یک از سیستم‌های اطلاعاتی و ارتباطی سازمان

۶-۳- مروری بر استانداردهای مدیریت امنیت اطلاعات

استانداردهای مدیریتی ارائه شده در خصوص امنیت اطلاعات و ارتباطات سازمان‌ها، عبارتند از[۲۰]:

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد

در این بخش، به بررسی مختصر استانداردهای فوق خواهیم پرداخت.

۶-۳-۱- استاندارد BS7799 موسسه استاندارد انگلیس

استاندراد BS7799 اولین استاندارد مدیریت امنیت اطلاعات است که نسخه اول آن (BS7799:1) در سال ۱۹۹۵ منتشر شد. نسخه دوم این استاندارد (BS7799:2) که در سال ۱۹۹۹ ارائه شد، علاوه بر تغییر نسبت به نسخه اول، در دو بخش ارائه گردید. آخرین نسخه این استاندارد، (BS7799:2005) نیز در سال ۲۰۰۵ و در سه بخش منتشر گردید.

- بخش اول

در این بخش از استاندارد، مجموعه کنترل‌های امنیتی موردنیاز سیستم‌های اطلاعاتی و ارتباطی هر سازمان، در قالب ده دسته‌بندی کلی شامل موارد زیر، ارائه شده است[۲۱]:

۱- تدوین سیاست امنیتی سازمان

در این قسمت، به ضرورت تدوین و انتشار سیاست‌های امنیتی اطلاعات و ارتباطات سازمان، بنحوی که کلیه مخاطبین سیاست‌ها در جریان جزئیات آن قرار گیرند، تاکید شده است. همچنین جزئیات و نحوه نگارش سیاست‌های امنیتی اطلاعات و ارتباطات سازمان، ارائه شده است.

۲- ایجاد تشکیلات تامین امنیت سازمان

در این قسمت، ضمن تشریح ضرورت ایجاد تشکیلات امنیت اطلاعات و ارتباطات سازمان، جزئیات این تشکیلات در سطوح سیاستگذاری، اجرائی و فنی به همراه مسئولیت‌های هر یک از سطوح، ارائه شده است.

۳- دسته‌بندی سرمایه‌ها و تعیین کنترل‌های لازم

در این قسمت، ضمن تشریح ضرورت دسته‌بندی اطلاعات سازمان، به جزئیات تدوین راهنمای دسته‌بندی اطلاعات سازمان پرداخته و محورهای دسته‌بندی اطلاعات را ارائه نموده است.

۴- امنیت پرسنلی

در این قسمت، ضمن اشاره به ضرورت رعایت ملاحظات امنیتی در بکارگیری پرسنل، ضرورت آموزش پرسنل در زمینه امنیت اطلاعات و ارتباطات، مطرح شده و لیستی از مسئولیت‌های پرسنل در پروسه تامین امنیت اطلاعات و ارتباطات سازمان، ارائه شده است.

۵- امنیت فیزیکی و پیرامونی

در این قسمت، اهمیت و ابعاد امنیت فیزیکی، جزئیات محافظت از تجهیزات و کنترلهای موردنیاز برای این منظور، ارائه شده است.

۶- مدیریت ارتباطات

در این قسمت، ضرورت و جزئیات روالهای اجرائی موردنیاز، بمنظور تعیین مسئولیت هر یک از پرسنل، روال‌های مربوط به سفارش، خرید، تست و آموزش سیستم‌ها، محافظت در مقابل نرم‌افزارهای مخرب، اقدامات موردنیاز در خصوص ثبت وقایع و پشتیبان‌گیری از اطلاعات، مدیریت شبکه، محافظت از رسانه‌ها و روال‌ها و مسئولیت‌های مربوط به درخواست، تحویل، تست و سایر موارد تغییر نرم‌افزارها ارائه شده است.

۷- کنترل دسترسی

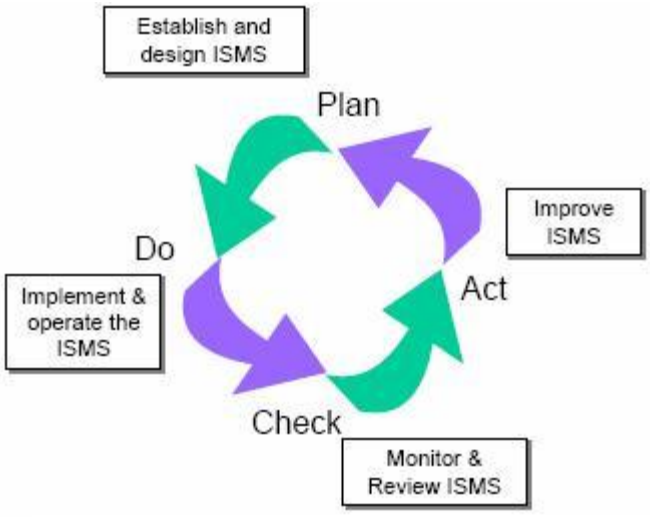
در این قسمت، نیازمندی‌های کنترل دسترسی، نحوه مدیریت دسترسی پرسنل، مسئولیت‌های کاربران، ابزارها و مکانیزم‌های کنترل دسترسی در شبکه، کنترل دسترسی در سیستم‌عامل‌ها و نرم‌افزارهای کاربردی، استفاده از سیستم‌های مانیتورینگ و کنترل دسترسی در ارتباط از راه دور به شبکه ارائه شده است.

۸- نگهداری و توسعه سیستم‌ها

در این قسمت، ضرورت تعیین نیازمندی‌های امنیتی سیستم‌ها، امنیت در سیستم‌های کاربردی، کنترل‌های رمزنگاری، محافظت از فایل‌های سیستم و ملاحظات امنیتی موردنیاز در توسعه و پشتیبانی سیستم‌ها، ارائه شده است.

- بخش دوم

در این بخش از استاندارد برای تامین امنیت اطلاعات و ارتباطات سازمان، مطابق شکل (۱) یک چرخهٔ ایمن سازی شامل ۴ مرحلهٔ طراحی، پیاده سازی، تست و اصلاح ارائه شده و جزئیات هر یک از مراحل به همراه لیست و محتوای مستندات موردنیاز جهت ایجاد سیستم مدیریت امنیت اطلاعات سازمان، ارائه شده است.



شکل ۶-۱- مراحل ایمن سازی بر اساس استاندارد BS7799[۲۰]

- بخش سوم

در این بخش ضمن در نظر گرفتن مسایل امنیتی به مدیریت ریسک مخصوصا در کارهای تجاری پرداخته شده است.

۶-۳-۲- استاندارد ISO/IEC 17799 موسسه بین‌المللی استاندارد

در سال ۲۰۰۰، بخش اول استاندارد BS7799:2 بدون هیچگونه تغییری توسط موسسهٔ بین المللی استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر شد[۲۰].

۶-۳-۳- راهنمای فنی ISO/IEC TR13335 موسسه بین‌المللی استاندارد

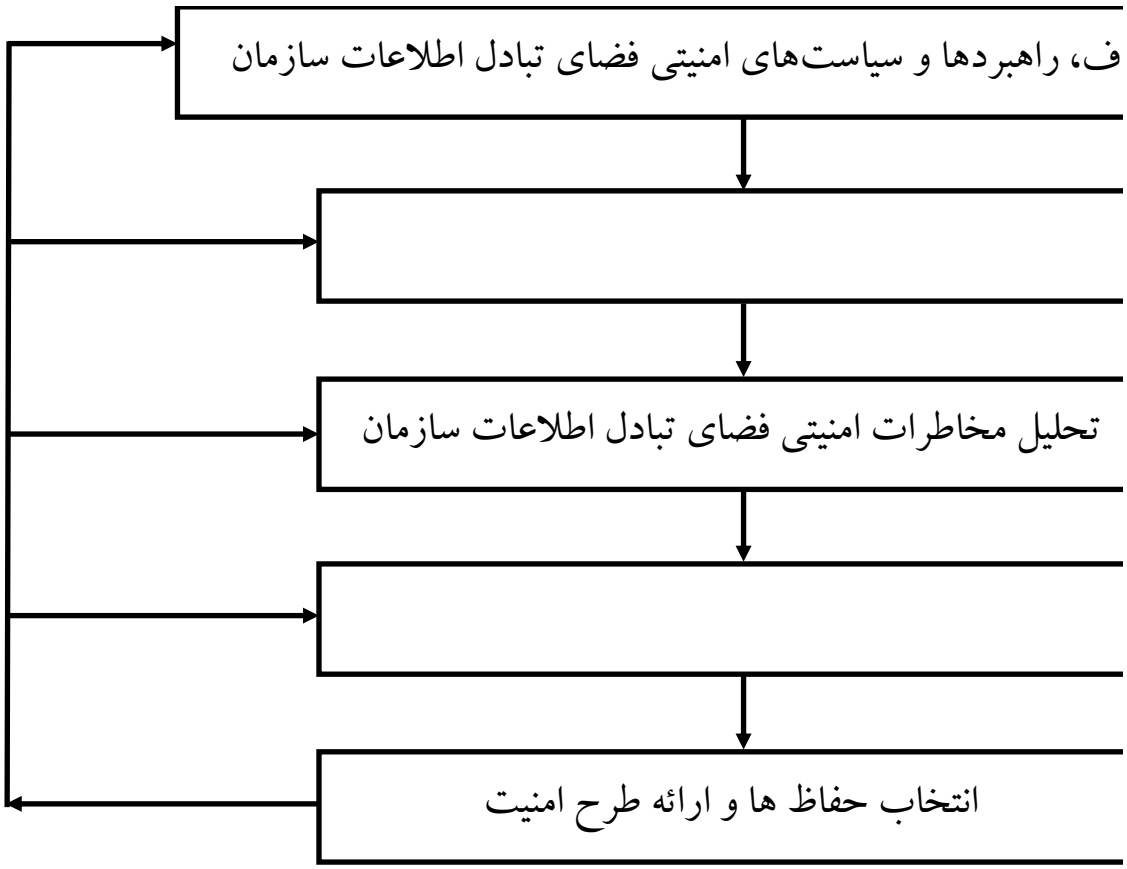
این گزارش فنی در قالب ۵ بخش مستقل در فواصل سالهای ۱۹۹۶ تا ۲۰۰۱ توسط موسسهٔ بین المللی استاندارد منتشر شده است. اگر چه این گزارش فنی به عنوان استاندارد ISO منتشر نشد و عنوان Technical Report بر آن نهاده شد، لیکن تنها مستندات فنی معتبری است که جزئیات و تکنیکهای مورد نیاز مراحل ایمن سازی اطلاعات و ارتباطات را تشریح نموده و در واقع مکمل استانداردهای مدیریتی BS7799 و ISO/IEC 17799 می‌باشد.

- بخش اول

در این بخش که در سال ۱۹۹۶منتشر شد، مفاهیم کلی امنیت اطلاعات از قبیل سرمایه، تهدید، آسیب پذیری، ریسک، ضربه و ... روابط بین این مفاهیم و مدل مدیریت مخاطرات امنیتی، ارائه شده است.

- بخش دوم

این بخش که در سال ۱۹۹۷منتشر شد، مراحل ایمن سازی و ساختار تشکیلات تامین امنیت اطلاعات سازمان ارائه شده است. بر اساس این گزارش فنی، چرخه‌ی ایمن سازی مطابق شکل ۶-۲ به ۵ مرحله شامل تدوین سیاست امنیتی سازمان، تحلیل مخاطرات امنیتی، تعیین حفاظها و ارائه طرح امنیت، پیاده سازی طرح امنیت و پشتیبانی امنیت اطلاعات، تفکیک شده است.



شکل۶-۲- مراحل ایمن سازی بر اساس گزارش فنی ISO/IEC 13335[۲۲]

- بخش سوم

در این بخش که در سال ۱۹۹۸منتشر شد، تکنیکهای طراحی، پیاده سازی و پشتیبانی امنیت اطلاعات از جمله محورها و جزئیات سیاستهای امنیتی سازمان، تکنیک‌های تحلیل مخاطرات امنیتی، محتوای طرح امنیتی، جزئیات پیاده سازی طرح امنیتی و پشتیبانی امنیت اطلاعات، ارایه شده است.

- بخش چهارم

در این بخش که در سال ۲۰۰۰ منتشر شد، ضمن تشریح حفاظهای فیزیکی، سازمانی و حفاظهای خاص سیستم‌های اطلاعاتی، نحوهٔ انتخاب حفاظهای مورد نیاز برای تامین هریک از مولفه‌های امنیت اطلاعات، ارائه شده است.

- بخش پنجم

در این بخش که در سال ۲۰۰۱ منتشر شد، ضمن افزودن مقولهٔ ارتباطات و مروری بر بخشهای دوم تا چهارم این گزارش فنی، تکنیکهای تامین امنیت ارتباطات از قبیل شبکه‌های خصوصی مجازی، امنیت در گذرگاه‌ها، تشخیص تهاجم و کدهای مخرب، ارائه شده است.

۶-۴- مستندات ISMS

بر اساس استانداردهای مدیریت امنیت اطلاعات و ارتباطات، هر سازمان باید مجموعه مستندات مدیریت امنیت اطلاعات و ارتباطات را به شرح زیر، برای خود تدوین نماید[۲۰]:

- اهداف، راهبردها و سیاستهای امنیتی فضای تبادل اطلاعات دستگاه
- طرح تحلیل مخاطرات امنیتی فضای تبادل اطلاعات دستگاه
- طرح امنیت فضای تبادل اطلاعات دستگاه
- طرح مقابله با حوادث امنیتی و ترمیم خرابیهای فضای تبادل اطلاعات دستگاه
- برنامه آگاهی رسانی امنیتی به پرسنل دستگاه
- برنامه آموزش امنیتی پرسنل تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه

در این بخش، به بررسی مستندات فوق خواهیم پرداخت.

۱. اهداف، راهبردها و سیاست‌های امنیتی

اولین بخش از مستندات ISMS سازمان، شامل اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه می‌باشد.

۲. اهداف امنیت فضای تبادل اطلاعات دستگاه

در این بخش از مستندات، ابتدا سرمایه‌های فضای تبادل اطلاعات دستگاه، در قالب سخت‌افزارها، نرم‌افزارها، اطلاعات، ارتباطات، سرویسها و کاربران تفکیک و دسته‌بندی شده و سپس اهداف کوتاه‌مدت و میان‌مدت تامین امنیت هر یک از سرمایه‌ها، تعیین خواهد شد. نمونه‌ای از این اهداف، عبارتند از:

نمونه‌هایی از اهداف کوتاه مدت امنیت:

- جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه سرمایه‌های فضای تبادل اطلاعات دستگاه
- مهار خسارت‌های ناشی از ناامنی موجود در فضای تبادل اطلاعات دستگاه
- کاهش رخنه‌پذیری‌های سرمایه‌های فضای تبادل اطلاعات دستگاه

نمونه‌هایی از اهداف میان مدت امنیت:

- تامین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها، متناسب با حساسیت آن‌ها.
- تامین صحت عملکرد و قابلیت دسترسی برای نرم‌افزارها، متناسب با حساسیت آن‌ها.
- تامین محرمانگی، صحت و قابلیت دسترسی برای اطلاعات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی.
- تامین محرمانگی، صحت و قابلیت دسترسی برای ارتباطات، متناسب با طبقه‌بندی اطلاعات از حیث محرمانگی و حساسیت ارتباطات.
- تامین قابلیت تشخیص هویت، حدود اختیارات و پاسخگوئی، حریم خصوصی و آگاهی‌رسانی امنیتی برای کاربران شبکه، متناسب با طبقه‌بندی اطلاعات قابل دسترس و نوع کاربران.

۳. راهبردهای امنیت فضای تبادل اطلاعات دستگاه

راهبردهای امنیت فضای تبادل اطلاعات دستگاه، بیانگر اقداماتی است که به منظور تامین اهداف امنیت دستگاه، باید انجام گیرد. نمونه‌ای از راهبردهای کوتاه‌مدت و میان‌مدت امنیت فضای تبادل اطلاعات دستگاه، عبارتند از:

نمونه‌هایی از راهبردهای کوتاه مدت امنیت:

- شناسائی و رفع ضعفهای امنیتی فضای تبادل اطلاعات دستگاه
- آگاهی‌رسانی به کاربران فضای تبادل اطلاعات دستگاه
- کنترل و اعمال محدودیت در ارتباطات شبکه داخلی دستگاه

نمونه‌هایی از راهبردهای میان مدت امنیت:

- رعایت استانداردهای مدیریت امنیت اطلاعات

- تهیه طرح‌ها و برنامه‌های امنیتی فضای تبادل اطلاعات دستگاه، بر اساس استانداردهای فوق
- ایجاد و آماده‌سازی تشکیلات تامین امنیت فضای تبادل اطلاعات دستگاه
- اجرای طرح‌ها و برنامه‌های امنیتی فضای تبادل اطلاعات دستگاه

۴. سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه

سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه، متناسب با دسته‌بندی انجام شده روی سرمایه‌های فضای تبادل اطلاعات دستگاه، عبارتند از:

- سیاست‌های امنیتی سرویس‌های فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی سخت‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی نرم‌افزارهای فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی اطلاعات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی ارتباطات فضای تبادل اطلاعات دستگاه
- سیاست‌های امنیتی کاربران فضای تبادل اطلاعات دستگاه

۵. طرح تحلیل مخاطرات امنیتی

پس از تدوین اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه و قبل از طراحی امنیت فضای تبادل اطلاعات، لازم است شناخت دقیقی از مجموعه فضای تبادل اطلاعات موجود دستگاه بدست آورد. در این مرحله، ضمن کسب شناخت نسبت به اطلاعات، ارتباطات، تجهیزات، سرویس‌ها و ساختار شبکه ارتباطی دستگاه، ضعفهای امنیتی موجود در بخشهای مختلف، شناسائی خواهند شد تا در مراحل بعدی، راهکارهای لازم به منظور رفع این ضعفها و مقابله با تهدیدها، ارائه شوند. روش تحلیل مخاطرات امنیتی، باید در مجموعه راهبردهای امنیتی فضای تبادل اطلاعات دستگاه، مشخص شده باشد.

در تحلیل مخاطرات امنیتی، به مواردی پرداخته می‌شود که بصورت بالقوه، امکان دسترسی غیرمجاز، نفوذ و حمله کاربران مجاز یا غیرمجاز فضای تبادل اطلاعات دستگاه، به منابع (سرمایه‌های) فضای تبادل اطلاعات دستگاه و منابع کاربران این فضا را فراهم می‌نمایند. در این مستند، لازم است مخاطرات امنیتی فضای تبادل اطلاعات، حداقل در محورهای معماری شبکه، تجهیزات شبکه، سرویس‌دهنده‌های شبکه، مدیریت و نگهداری شبکه و تشکیلات و روشهای مدیریت امنیت شبکه، بررسی شوند.

۶. معماری شبکه ارتباطی

در این بخش، لازم است معماری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- ساختار شبکه ارتباطی
- ساختار آدرس‌دهی و مسیریابی
- ساختار دسترسی به شبکه ارتباطی

۷. تجهیزات شبکه ارتباطی

در این بخش، لازم است تجهیزات شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- محافظت فیزیکی
- نسخه و آسیب‌پذیریهای نرم‌افزار
- مدیریت محلی و از راه دور
- تصدیق هویت، تعیین اختیارات و ثبت عملکرد سیستم، بویژه در دسترسی‌های مدیریتی
- ثبت وقایع
- نگهداری و به‌روزنمودن پیکربندی
- مقابله با حملات علیه خود سیستم، بویژه حملات ممانعت از سرویس

۸. مدیریت و نگهداری شبکه ارتباطی

در این بخش، لازم است مدیریت و نگهداری شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- تشکیلات و روشهای مدیریت و نگهداری شبکه ارتباطی
- ابزارها و مکانیزم‌های مدیریت و نگهداری شبکه ارتباطی

۹. سرویس‌های شبکه ارتباطی

در این بخش، لازم است سرویس‌های شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- سیستم عامل سرویس‌دهنده
- سخت‌افزار سرویس‌دهنده، بویژه رعایت افزونگی در سطح ماژول و سیستم
- نرم‌افزار سرویس
- استفاده از ابزارها و مکانیزم‌های امنیتی روی سرویس‌دهنده‌ها

۱۰. تشکیلات و روشهای تامین امنیت شبکه ارتباطی

در این بخش، لازم است تشکیلات و روشهای امنیت شبکه ارتباطی دستگاه، حداقل در محورهای زیر مورد تجزیه و تحلیل قرار گیرد:

- طرح‌ها، برنامه‌ها و سایر مستندات امنیتی
- تشکیلات امنیت، روالهای اجرائی و شرح وظایف پرسنل امنیت

۶-۵- طرح امنیت

پس از تحلیل مخاطرات امنیتی شبکه ارتباطی دستگاه و دسته‌بندی مخاطرات امنیتی این شبکه، در طرح امنیت، ابزارها و مکانیزم‌های موردنیاز به منظور رفع این ضعف‌ها و مقابله با تهدیدها، ارایه می‌شوند. در طرح امنیت، لازم است کلیه ابزارها و مکانیزم‌های امنیتی موجود، بکار گرفته شوند. نمونه‌ای از این ابزارها عبارتند از[۲۲]:

۱. سیستم‌های کنترل جریان اطلاعات و تشکیل نواحی امنیتی
   - فایروال‌ها
   - سایر سیستم‌های تامین امنیت گذرگاه‌ها
۲. سیستم‌های تشخیص و مقابله یا تشخیص و پیشگیری از حملات، شامل:
   - سیستم‌های مبتنی بر ایستگاه
   - سیستم‌های مبتنی بر شبکه
۳. سیستم فیلترینگ محتوا (بویژه برای سرویس E-Mail)
۴. نرم‌افزارهای تشخیص و مقابله با ویروس
۵. سیستم‌های تشخیص هویت، تعیین حدود اختیارات و ثبت عملکرد کاربران
۶. سیستم‌های ثبت و تحلیل رویدادنامه‌ها
۷. سیستم‌های رمزنگاری اطلاعات
۸. نرم‌افزارهای نظارت بر ترافیک شبکه

۹. نرم‌افزارهای پویشگر امنیتی
۱۰. نرم‌افزارهای مدیریت امنیت شبکه

ویژگیهای اصلی سیستم امنیتی شبکه ارتباطی دستگاه، عبارتند از:

- چندلایه بودن سیستم امنیتی
- توزیع‌شده بودن سیستم امنیتی
- تشکیل نواحی امنیتی جهت کنترل دقیق دسترسی به سرویس‌های شبکه
- یکپارچگی مکانیزم‌های امنیتی، بویژه در گذرگاه‌های ارتباطی شبکه
- تفکیک زیرساختار مدیریت امنیت شبکه (حداقل بخش اصلی سیستم امنیتی شبکه)
- انتخاب اجزاء سیستم امنیتی شبکه، از Brandهای مختلف، بنحوی که ضعفهای امنیتی یکدیگر را پوشش داده و مخاطره باقیمانده را کاهش دهند
- انتخاب محصولاتی که دارای تائیدیه‌های معتبر، از موسسات ارزیابی بین‌المللی می‌باشند

۶-۵-۱- شرح وظایف کمیته راهبری امنیت:

- بررسی، تغییر و تصویب سیاستهای امنیتی شبکه
- پیگیری اجرای سیاستهای امنیتی از مدیر امنیت شبکه
- تائید طرح‌های و برنامه‌های امنیت شبکه دستگاه شامل:
  - طرح تحلیل مخاطرات امنیتی
  - طرح امنیت شبکه
  - طرح مقابله با حوادث و ترمیم خرابیها
  - برنامه آگاهی‌رسانی امنیتی کاربران
  - برنامه آموزش واحد پشتیبانی امنیت شبکه
- بررسی ضرورت تغییر سیاستهای امنیتی شبکه
- بررسی، تغییر و تصویب تغییرات سیاستهای امنیتی شبکه

۶-۵-۲- شرح وظایف مدیر امنیت :

- تهیه پیش نویس سیاستهای امنیتی شبکه و ارائه به کمیته راهبری امنیت شبکه

- نظارت بر اجرای کامل سیاستهای امنیتی شبکه توسط واحد پشتیبانی امنیت شبکه، کاربران شبکه، مدیران و کارشناسان ادارات و طراحان امنیت شبکه دستگاه
- تهیه طرح‌ها و برنامه‌های امنیت شبکه دستگاه با کمک واحد مشاوره و طراحی و ارائه آن‌ها به کمیته راهبری
- مدیریت واحد پشتیبانی امنیت شبکه دستگاه و نظارت بر عملکرد اجزاء این واحد
- تشخیص ضرورت و پیشنهاد بازنگری و اصلاح سیاستهای امنیتی شبکه
- تهیه پیش نویس تغییرات سیاستهای امنیتی شبکهگ

۶-۵-۳- شرح وظایف واحد پشتیبانی امنیت :

شرح وظایف پشتیبانی حوادث امنیتی شبکه[۲۲]:

۱. تشخیص و مقابله با تهاجم.
۲. آگاهی‌رسانی به کاربران شبکه در خصوص روشهای جدید نفوذ به سیستم‌ها و روشهای مقابله با آن.
۳. آسیب‌پذیریهای جدید ارائه شده برای سیستم‌های مختلف و روشهای بر طرف نمودن آن‌ها.
۴. تشخیص و مقابله با ویروس.
۵. آگاهی‌رسانی به کاربران شبکه در خصوص ویروسهای جدید و روشهای مقابله با آن‌ها.

فصل هفتم:

ملاحضات پدافند غیر عامل در شبکه تلفن ثابت و همراه

۷-۱- آشنایی مقدماتی با نحوه کار شبکه تلفن ثابت(PSTN)

شروع کار با تلفن ثابت از لحظه برداشتن گوشی و شنیدن صدای بوق اغاز می‌شود. این صدا به این معنی است که فرد مجاز به شماره گیری و استفاده از شبکه تلفن ثابت است. ارتباط با مرکز تلفن محلی[۱] خود به‌وسیله دو رشته سیم مسی که از درب منزل یا محل کار به نزدیکترین پست[۲] رفته است و از پست به کافو[۳] و از کافوها به چاله حوضچه که در زیر زمین توسط مخابرات حفر شده می‌رود و از آنجا به مرکز تلفن وارد و در آن‌جا از طریق دو رشته سیم مسی به سالن MDF[۴]متصل می‌شود. در تلفن ثابت هویت مشترک مشخص است (این کار را مخابرات از طریق کشیدن دو رشته سیم مسی تا در منزل یا محل کار و دادن بوق این کار برای مشترک فراهم کرده است.) پس مرحله اول در شبکه مخابرات هویت یا شناسایی معتبر بودن مشترک است.

مکان مشترک نیز دقیقا مشخص است یعنی سوییچ هنگامی‌که کسی با این مشترک کار دارد راحت آن را پیدا کرده و به آن زنگ می‌زند. بخش بعدی محل ثبت charging است یعنی هر مشترک هر چقدر با تلفن خود به دیگران زنگ بزند هزینه آن در سوییچ متصل شده به آن ثبت می‌شود. و نهایتا ارائه سرویس‌های جانبی مثل نمایشگر شماره تلفن و انتقال مکالمه و... است که این هم در سوییچی که تلفن به آن متصل شده است انجام می‌گیرد. پس به طور خلاصه شبکه تلفن ثابت مشخصات زیر را دارا می‌باشد [۲۳]:

۱. هویت یا شناسایی مشترک
۲. مکان مشخص جهت تماس گرفته شدن با آن
۳. محل ثبت charging
۴. ارائه سرویسهای جانبی

وقتی فرد شروع به شماره‌گیری می‌کند، سوییچ مخابراتی (دستگاهی است که کار مسیر یابی و مسیر دهی را انجام می‌دهد و در ضمن وظیفه ثبت charging که همان مدت زمان مکالمه است را برعهده دارد و ضمنا ارائه سرویسهای مختلف اعم از انتظار مکالمه -انتقال مکالمه - نمایشگر شماره تلفن و غیره به عهده سوییچ می‌باشد.) شماره‌های گرفته شده را تجزیه و تحلیل می‌کند و مسیر آن را تشخیص می‌دهد.

---

[1] LOCAL

[۲] جعبه‌های کوچک سربی رنگ که در روی دیوار معابر نصب شده و به مقداری کابل وارد و خارج شده است

[۳] کافوها کمدهای سبز رنگی است که در کنار خیابان‌ها نصب شده است

[۴] سالن MDFسالنی است که در آن کانکتورهای زیادی بر روی شلفهای ایستا نصب شده است از یک طرف به ازای هر پورت یا شماره تلفن دورشته سیم مس از سمت سوییچ به آن وارد شده است و از سمت دیر دورشته سیم مسی که از سمت مشترک(منزل یا محل کار شما) آمده به آنجا می‌رسد و با ارتباط این دو شما می‌توانید به سوییچ وصل شده و یا اصطلاحا بوق داشته باشید.

به عنوان مثال این‌که این شماره داخل شهری است یا بین شهری و یا بین الملل توسط سوییچ مشخص شده و مسیر را به مرکز بعدی که هرکدام وظیفه خاصی به عهده دارند را می‌رساند. به عنوان نمونه می‌توان به این مثال اشاره کرد که وقتی فردی از تهران یک شماره در کرمانشاه را می‌گیرد(مثل ۰۸۳۱۳۲۷۲۲۲۲) سوییچ محلی با دیدن ۰ می‌فهمد که باید کل شماره را به سوییچ بین شهری بدهد. بنابراین ابتدا به سوییچ بین شهری[1] تهران داده و سوییچ بین شهری با دیدن رقم دوم یعنی عدد ۸ می‌فهمد که باید کل شماره را به سوییچ بین شهری (STD) منطقه ۸ کشور که در همدان می‌باشد بدهد. سوییچ STD همدان با دیدن رقم سوم که ۳ می‌باشد شماره را به PCکرمانشاه می‌دهد (PCیک نوع سوییچ بین شهری است ولی از لحاظ levelپایین تر از STDمی‌باشد) PCکرمانشاه با دیدن رقم چهارم که ۱ می‌باشد تشخیص می‌دهد که شماره مربوط به شهر کرمانشاه می‌باشد و با توجه به پیش شماره ۳۲۷ به مرکز مربوطه تحویل داده می‌شود و مشترک شماره ۲۲۲۲ در مرکز ۳۲۷ زنگ می‌خورد.

این مسیری بود که طی زمانی خیلی کم برای تماس بین تهران و کرمانشاه باید طی شود. برای شماره‌های بین الملل مسئله کمی‌فرق می‌کند بدین ترتیب که مرکز محلی بادیدن ۰۰ در ابتدای شماره تلفن کل شماره را به STDداده و STDها هم شماره را به سوییچ بین الملل که ISC نامیده می‌شود می‌دهند و سپس مراحل بین شهری و شهری را مانند مثال قبل طی می‌کند. سوییچ‌های تلفن ثابت به دو نوع آنالوگ و دیجیتال تقسیم می‌شود که سرویس‌هایی که ذکر شد صرفا در سوییچ‌های دیجیتال قابل ارائه می‌باشد.

۷-۲- ساختار شبکه‌های تلفن همراه

تلفن‌های همراه دستگاهای رادیویی هستند که توسط ارسال و دریافت صدا بر روی امواج اقدام به برقراری ارتباط در یک منطقه می‌کنند. امروزه میلیون‌ها نفر در سراسر جهان از تلفن‌های سلولی (همراه) استفاده می‌کنند. در واقع تلفن‌های همراه نوع پیشرفته رادیو تلفن‌های دهه ۱۸۸۰هستند که در آن زمان روی خودروها نصب و استفاده می‌شد. این سامانه دارای یک یا چند دکل آنتن مرکزی برای هر شهر بود و هر دکل می‌توانست تا ۲۵ کانال ارتباطی را تا شعاع۴۰ الی۵۰ مایل پوشش دهد. اما به علت محدودیت کانال‌های ارتباطی امکان مشترک شدن برای همه وجود نداشت. تلفن همراه دیگر به عنوان یک تلفن سیار محسوب نمی‌شود؛ با حضور نسل‌های جدید و فراهم آوردن امکان برقراری ارتباط بین گوشی تلفن‌های همراه با وسیله‌های دیگر از طریق فناوری بلوتوث، گوشی‌های تلفن همراه به مرور جایگزین بسیاری از وسایل کنونی خواهد شد. کنترل وسایل مختلف خانه و حتی بهره گیری از گوشی تلفن همراه برای پرداخت پول به جای کارت بانکی امکان پذیر شده است. اینک با گوشی‌های تلفن همراه می‌توان با چند نفر بازی کرد،

[1] STD

تلویزیون تماشا کرد، موسیقی گوش کرد، به اینترنت متصل شد و از امکانات شبکه اینترنت پرسرعت بهره مند شد. ارسال پیام‌های متنی کوتاه، پیام صوتی و عکس توسط تلفن‌های همراه خیلی زود به کارهایی پیش پا افتاده بدل شد و در حال حاضر سازندگان این گوشی‌ها در پی فناوری پیشرفته تری برای نسل تازه گوشی‌ها هستند. لذا می‌توان نسل‌های مختلف شبکه‌های تلفن همراه را مورد بررسی قرار داد.

آنتن‌های مخابراتی دارای چندین اسکلت مثلثی بر روی بالای خود هستند. این تعدد مربوط به اپراتورهای مختلفی می‌شود که به صورت همزمان از یک دکل مخابراتی استفاده می‌کنند. اسکلت‌های مثلثی پوشش ۳۶۰ درجه ای خود را به سه قسمت ۱۲۰ درجه ای تقسیم می‌کنند، که این ۳ بخش نیز می‌توانند به ۳ قسمت ۴۰ درجه ای دیگر تقسیم شوند. سلول منطقه ایست حول یک آنتن مخابراتی که از لحاظ تئوری یک ۶ ضلعی است که تحت پوشش امواج همان آنتن مخابراتی می‌باشد. هر کدام از ایستگاه‌های مرکزی با انتشار امواج با قدرت کم از نفوذ موج به خارج محدوده سلول خودشان جلوگیری می‌کنند. این ویژگی باعث می‌شود تا سلولهایی که وجه اشتراکی با هم ندارند از فرکانس‌های مشابهی در سطح شهر استفاده کنند.

تلفن همراه سامانه‌ای سلولی است زیرا مناطق تحت پوشش آن به سلول‌های تقریبا ۶ گوش تقسیم‌بندی می‌شود. بدین ترتیب کل فضای مورد نظر تحت پوشش سلول‌های مختلف قرار می‌گیرند. در مرکز هر سلول یک دکل آنتن به نام(BTS) نصب می‌شود و برحسب ظرفیت هر سلول تعداد مشترکان تغییر می‌کند. در سیستم آنالوگ تلفن‌های همراه، هر سلول، یک هفتم از کانالهای ۲ طرفه صوتی را مورد استفاده قرار می‌دهد، از این جهت در یک دسته هفت تایی از سلولها تداخل فرکانسی وجود ندارد، زیرا هر کدام از آن‌ها از یک دسته از فرکانس‌های یکتا استفاده می‌کنند. شبکه‌های دیجیتالی از سه بخش اصلی گوشی موبایل، تجهیزات شبکه[1] و تجهیزات سوئیچ[2] تشکیل شده‌اند که تجهیزات شبکه BSS خود شامل ۴ قسمت BTS، BSC، TRCو OMC می‌باشند[۲۴].

۷-۲-۱- ایستگاه پایه (BTS):

در شبکه موبایل اولین بخشی که به طور مستقیم با گوشی موبایل در ارتباط است به لفظ عوام آنتن موبایل و به تعبیر تخصصی (Base Transceiver Station) می‌باشد. ترکیب پنل‌های آنتن‌ها متفاوت است، این تفاوت در تعداد هر کدام از این پنل‌ها در یک جهت می‌باشد. این تفاوت صرفا به خاطر نوع سیستم (دستگاه) استفاده شده است و هیچ ربطی به ظرفیت آنتن ندارد. این پنل‌ها توسط کابلهای ضخیم سیاه رنگی که به آن فیدر[3] می‌گویند به دستگاه BTS متصل است.

[1] BSS
[2] NSS
[3] FEEDER

فیدرها نوعی کابل درون تهی هستند و در آن سیم لوله مسی قرار گرفته و موج بر می‌باشد. از آن‌جایی که در فرکانس‌های بالا الکترون‌ها از پوسته عبور می‌کنند به همین منظور برای انتقال از موج بر استفاده می‌شود نه سیم. در نهایت توسط خطوط انتقال این دستگاه به دستگاه دیگری به نام BSCکه وظیفه مدیریت بین چند BTS را دارد متصل می‌شود[۲۵].

۷-۲-۲- کنترل کننده ایستگاه پایه (BSC[1]):

دومین مرحله بعد از آنتن موبایل (BTS) در شبکه دستگاهی به نام BSC است. وظیفه کنترل چند BTS به عهده یک BSCاست و کار آن بسیار با اهمیت می‌باشد، چون تنظیم یکسری از پارامترهای مهم شبکه که راجع به کیفیت مکالمه و تماس مطلوب است در این دستگاه تعریف می‌شود. مثلا وقتی فرد در حال صحبت با گوشی موبایل خود است و در یک اتومبیل در حال حرکت نشسته (و در حال صحبت خیابآن‌های متعددی را پشت سر می‌گذارد) ولی همچنان به مکالمه خود ادامه می‌دهد. در این حالت فرد از چندین آنتن موبایل گذشته و هر آنتن موبایل تماس را به آنتن دیگر دست به دست کرده است و کانال ترافیکی تماس را با خود پاک کرده و به یک آنتن دیگر تحویل داده است. این مدیریت مکالمه که در حال حرکت اتفاق می‌افتد به HAND OVER معروف است و وظیفه BSC مرتبط با آن BTS می‌باشد. و دیگر اینکه قدرت تشعشع (برد آنتن موبایل) نیز در این دستگاه تعریف می‌شود، بدین صورت که از طریق BSCبر روی خروجی یک آنتن مورد نظر تضعیف گذاشته می‌شود که فرکانس آن با آنتن‌های دیگر تداخل نکند.

BTSها صرفا حکم یک واسطه رادیویی را بین BSC و گوشی موبایل دارند که قدرت خروجی آن هم حتی با BSC معین می‌شود. هر BTS با هر ساختاری که دارد در BSC مرتبط با خود دارای یک دیتا بیس می‌باشد، این دیتا بیس شامل فرکانس‌هایی که BTS باید با آن کار کند، شماره تایم اسلات‌هایی که بر روی خطوط انتقال باید از آن استفاده کند - تعداد کانالهای ترافیکی و سیگنالینگی و... - و شماره‌های LAC و CIمی‌باشد.

شبکه موبایل طبق آنچه بیان شد به صورت سلول‌های ۶ ضلعی تقسیم و در نظر گرفته می‌شود و سایت BTSکه غالبا سه جهت (سکتور) دارد بین سه سلول قرار می‌گیرد وهر جهت یک سلول را پوشش می‌دهد.در شبکه برای پیدا کردن موقعیت یک مشترک می‌بایست هر سلول دارای کدی باشد که به این کدCI[2] گفته می‌شود که این کد در ایران ۵ رقمی‌می‌باشد. حال یک شهر را به چند منطقه بزرگ که خود این مناطق شامل چندین CIمی‌باشد تقسیم می‌کنند و به آن LAC

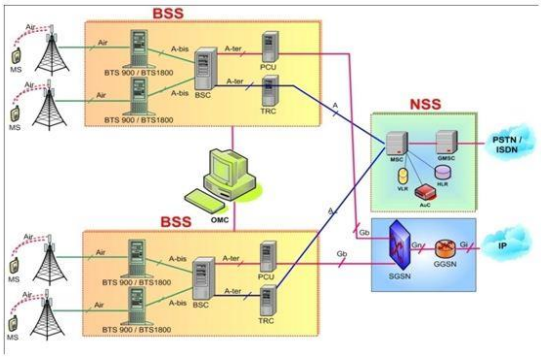
[1] Base Station Controller

[2] Cell ID

می‌گویند. شهری مانند تهران غالبا به چند LAC و شهرهای کوچکتر به یک LAC تقسیم می‌شوند. کد LAC معمولا ۴ رقمی‌است. به طور مثال در میدان ولیعصر تهران یک BTS نصب شده که دارای سه جهت (سکتور) می‌باشد. به این سلولها مثلا در LAC به شماره ۱۲۱۱ و در CIهای ۱۲۱۱۵ و ۲۲۱۱۵ و ۳۲۱۱۵ تعریف می‌شود و اگر فرد تحت پوشش سکتور سوم این سایت باشد در VLRاین آدرس ثبت می‌شود LAC=1211و CI=32115 و این آدرس این شخص در سوییچ می‌باشد. البته لازم به ذکر است که سوییچ موبایل برای پیدا کردن این فرد هنگام تماس با موبایلش مجبور است در کل LAC عمل پیجینگ را انجام دهد.

۷-۲-۳- مرکز راهبری شبکه (OMC):

مدیریت امنیت شبکه، مدیریت پایگاه داده شبکه، مدیریت عملکرد شبکه، مدیریت کارایی شبکه، مدیریت تعمیر و نگهداری شبکه، مدیریت کاربری (ویژه). علاوه بر این در ساختار نسل ۲,۵ علاوه بر سوئیچ مداری(Circuit Switch)، سوئیچ بسته بندی(Packet Switch) نیز بکار برده شده است و اطلاعات بصورت بسته بندی ارسال می‌گردند.



شکل ۷-۱شبکه‌های نسل ۲,۵ [۲۶]

۷-۳- شبکه موبایل چگونه کار می‌کند؟

درشبکه موبایل به دلیل وجود موبایل که یک وسیله بدون سیم است و از لحاظ فیزیکی به جایی متصل نیست ممکن است در هر لحظه مکان آن تغییرکند و یا در یک روز در نقاط مختلف کشور (و حتی جهان) حرکت کند. اما برقراری ۴ مشخصه تلفن ثابت برای موبایل‌ها با این روش پیاده سازی می‌شود که قبل از هر چیزی ذکر این مورد ضروری است که گوشی موبایل با روش بدون سیم (wireless) از طریق امواج الکترو مغناطیس با آنتی که به آن BTS گفته می‌شود ارتباط دارد و از طریق آن به شبکه موبایل وصل می‌شود(به جای دو رشته سیم مسی).

۷-۳-۱ تعیین هویت:

در موبایل به علت تغییر مکان مشترک (مستقل از مکان بودن) نیاز به مرکزی وجود دارد که اطلاعات تمام مشترکین یک کشور و یا یک شرکت ارائه دهنده سرویس موبایل در آن ثبت شود تا هر وقت شبکه نیاز داشت در اختیارشبکه قرار گیرد (این کار در تلفن ثابت در همان مرکز سرویس دهنده انجام می‌گیرد). به این مرکز HLR[1] گفته می‌شود، این مرکزها به صورت متمرکز در یک یا بعضا در نقاط محدودی در یک کشور ایجاد می‌شود و برای اینکه یک مشترک امکان استفاده از شبکه را داشته باشد به مشترک کارتی به نام SIM[2]داده می‌شود که این کارت وسیله شناسایی مشترک در شبکه است. پس اگر SIMکارت در گوشی موبایل قرار گیرد و تعاریف مخصوص آن در HLR ثبت گردد مشترک می‌تواند در هر مکانی از کشور امکان تماس گرفتن یا گرفته شدن را داشته باشد.

۷-۳-۲- مکان مشترک در شبکه موبایل

هنگامی‌که یک مشترک در شبکه حرکت می‌کند آخرین مکان آن در HLR ثبت می‌شود بنابراین هرکس بخواهد به یک موبایل زنگ بزند آخرین مکان آن از HLR پرسیده می‌شود و بعد به موبایل زنگ می‌خورد.

۷-۳-۳- ثبت charging

ثبت مقدار هزینه مکالمه موبایل در آخرین سوییچی که به موبایل سرویس می‌دهد انجام می‌گیرد. مثلا مشترکی از تهران به سمت مازندران رفته و از آن‌جا به مشهد می‌رود و در طی مسیر چندین بار به نقاط مختلف تماس گرفته است. هنگامی‌که در محدوده تهران بوده در سوییچ‌های تهران ثبت شده و در مازندران در سوییچ مازندران و در مشهد در سوییچ مشهد ثبت می‌شود. در آخر کلیه هزینه مکالمات از سراسر کشور به مرکزی در تهران که مرکز صورتحساب است، ارسال می‌شود و بعد از جمع بندی و محاسبه برای مشترک صورتحساب ارسال می‌شود (در تلفن ثابت تمام هزینه‌های مکالمه در مرکز سرویس دهنده ثبت می‌شود) [۲۵].

[1] Home Location Registration

[2] Subscriber Identity Module

۷-۳-۴- ارائه سرویس‌های جانبی

این سرویس‌ها توسط آخرین سوییچ سرویس دهنده به موبایل از طریق HLR سوال می‌شود که چه سرویسهایی باید در اختیار مشترک گذاشته شود. مثل انتقال مکالمه (اتظار مکالمه) نمایشگر شماره و... و سپس آن سرویس‌ها توسط آخرین سوییچ سرویس دهنده در اختیار مشترک قرار می‌گیرد. (در تلفن ثابت همان سوییچ محلی که تلفن به آن وصل است این کار را انجام می‌دهد.) اکنون می‌توان نحوه کار کردن در این شبکه (شبکه موبایل) را تشریح کرد. با توجه به مجموعه نکات بالا می‌توان گفت که در ابتدا تلفن همراه نزدیک ترین آنتن مخابراتی تلفن همراه را شناسایی می‌کند. زمانی که فرد اقدام به برقراری تماس تلفنی و یا روشن نمودن تلفن همراه خود می‌کند، تلفن همراه یک پیام به همان آنتن ارسال می‌کند. در این مرحله تماس از طریق کابل و یا فیبر نوری به نقطه دسترسی بیسیم، واقع در پایین دکل که به یک سویچ چند پورت متصل است، حرکت می‌کند. این تماس (به همراهی بقیه تماس‌ها) ۲ راه برای انتقال به شبکه اصلی را دارد. راه اول که روش معمول انتقال داده‌هاست، از طریق خطوط T1و یا T3 بر روی بستر کابلی واقع در زیر زمین انجام می‌پذیرد. در روش دوم داده‌ها از طریق یک آنتن بیسیم پرقدرت که در دید مستقیم یکی دیگر از سایتهای دارای اتصال کابلی قرار دارد، توسط امواج ریزموج منتقل می‌گردند. این روش یا به صورت پشتیبان در زمان ضعف اتصال زمینی استفاده می‌شود و یا زمانی که از لحاظ فیزیکی خطوط T1و یا T3به کلی وجود ندارند.

تماس ورودی از شبکه اصلی به سمت سوییچ باز می‌گردد و پس از آن به بالا، به سمت آنتن هدایت می‌شود تا به سمت دستگاه تلفن همراه برود (در صورتی این اتفاق رخ می‌دهد که دستگاه تلفن در پوشش همان آنتن باشد). اگر فرد جابجا شود سیگنالی مبتنی بر تغییر سلول از طرف سلول تحت پوشش آنتن جدید به سمت تلفن همراه ارسال می‌گردد، که از آن زمان به بعد آن سلول مسئول برقراری ارتباط تلفن با شبکه اصلی می‌باشد.

۷-۴- ملاحضات پدافند غیر عامل در شبکه‌های ارتباط ثابت

۷-۴-۱- اصل اختفا

- تغییر مکان منطقی اجزا با کارکرد مشخص
- شبکه‌های خصوصی مجازی
- اختفای اماکن از طریق تلفیق اماکن با کارکردهای گوناگون در یک مکان جغرافیایی
- اختفای تماس‌ها از طریق تغییر مشخصات قراردادی

- استفاده مناسب از تنوع کاربری و ایجاد تماس‌ها در کلاف‌هایی از تماس‌های عمومی‌که توسط مهاجم به سهولت قابل شناسایی نباشد
- حذف نقاط با ارزش که به دلیل خاصی می‌بایست در رسانه‌ها منتشر شوند
- اختفای توصیفات اجزای با ارزش و دارایی‌های موجود در شبکه

۷-۴-۲- اصل استتار

- استتار درون شبکه‌ای

عبارت است از اینکه تجهیزات با ارزش درون شبکه‌ای تا حد امکان مشابه سایر اجزا جلوه داده شوند. هدف اصلی در این روش آن است که نقش اجزای مختلف شبکه به خوبی قابل شناسایی و حدس زدن نباشد. به عنوان مثال یک مشترک نباید به راحتی تشخیص دهد که مرکز مخابراتی وی یک مرکز محلی، منطقه‌ای یا ملی است.

- استتار برون شبکه‌ای

عبارت است از اینکه دارایی‌های با ارزش از دید خارج از شبکه قابل تمیز از دارایی‌های عادی نباشند. از دید خارج از شبکه مجموعه‌ای از پارامترها از قبیل مشخصات مربوط به ترافیک ارتباطات، تدابیر امنیتی که ذینفعان شبکه جهت استفاده از آن اتخاذ می‌کنند و دامنه و کیفیت مخاطبین و مراجعات انسانی به یک عنصر، توصیف گر سطح اهمیت آن در شبکه است. یکی از مهم‌ترین کارهایی که جهت حصول این مهم انجام می‌شود تحلیل‌های آماری ترافیک است. به همین دلیل ضروری است تدابیری اتخاذ شود که یا امکان تحلیل آماری از دشمن گرفته شود یا با تحت تاثیر قرار دادن داده‌ها سعی در گمراه نمودن دشمن در تحلیل داده‌ها شود. از این رو یکی از روش‌های ارایه‌ی داده‌ی غلط به دشمن اینست که داده‌های ترافیک به گونهای تنظیم شود که تحلیل‌های آماری روی تماس‌های مهم، حساس و حیاتی مشابه سایر تماس‌ها باشد. هم‌چنین با توجه به این استدلال که معمولا میزان اهمیت یک دارایی نسبت منطقی با میزان تدابیر امنیتی مربوط دارد؛ لذا یک رویکرد صحیح این است که تدابیر امنیتی که برای حفاظت از دارایی‌های مهم، حساس و حیاتی اتخاذ می‌شود مشابه تدابیر امنیتی عمومی‌به نظر برسد.

۷-۴-۳- اصل استحکامات و موانع

در شبکه‌ی تلفن ثابت از گونه‌های مختلف استحکامات و موانع می‌توان بهره برد. از استحکامات فیزیکی گرفته تا روش‌های نرم افزاری کنترل دسترسی که در ادامه به برخی از آن‌ها اشاره می‌گردد.[۲۷]

۱. استفاده از انواع ساز و کارهای دفاعی از جمله:
   - دیواره‌های آتش
   - سامانه‌های کنترل دسترسی
   - کشف و توقیف سامانه‌های نا متعارف
   - سامانه‌های تشخیص حمله و نفوذ

۲. استفاده از فاصله

این روش به انواع تدابیری اشاره دارد که فاصله ابزارهای موجود در دست دشمن را از ابزارهایی که می‌توانند امنیت شبکه را تهدید کنند؛ زیاد می‌کند. به عنوان مثال بومی‌سازی قراردادهای شبکه‌ای باعث ایجاد فاصله شبکه با معیارهای استاندارد و به همین تناسب دشواری شناخت شبکه توسط دشمن می‌شود.

۳. استفاده از زیستگاه‌ها

در این روش از تجمع مفید دارایی‌های معمولی جهت محافظت از دارایی‌های مهم، حساس و حیاتی بهره‌گیری می‌شود. به عنوان مثال ارتباطات مهم، حساس و حیاتی با خارج از کشور، می‌تواند از طریق شماره‌هایی صورت پذیرد که مهاجرین بیشتری در خارج از کشور دارد.

۷-۴-۴- اصل پراکندگی

به‌طور کلی ایجاد پراکندگی در دارایی‌های مهم، حساس و حیاتی از لحاظ فیزیکی و منطقه‌ای به عنوان یک اصل دفاعی ضرورت دارد. به عنوان مثال لازم است:

۱. حتی المقدور تاسیسات مهم، حساس و حیاتی از جمله مراکز منطقه‌ای و ملی به صورت پراکنده در جغرافیای کشور قرار داده شود.
۲. ارتباطات با ارزش دارای پراکندگی زمانی یا مکانی باشند.

۷-۴-۵- اصل توزیع شدگی

توزیع شدگی در شبکه‌ی تلفن ثابت به معنی ایجاد شرایطی برای توزیع ارزش دارایی‌ها، و نیز حمایت عملکردی اجزای شبکه از یکدیگر در شرایط بحران است.

توزیع شدگی مصادیق متعددی دارد از جمله:

۱. توزیع تماس‌ها از طریق استفاده از خطوط تماس متعدد.
۲. توزیع داده تماس‌هایی مثل نمابر روی تماس‌های توزیع شده.
۳. توزیع تجهیزات و اجزا به‌منظور ایجاد افزونگی پشتیبان.
۴. ایجاد افزونه برای انباره‌های داده‌ای.
۵. نیروهای انسانی متعدد برای مدیریت و نگهداری اماکن و تجهیزات خاص.

۷-۴-۶- اصل فریب

این اصل شامل قرار دادن ساز و کارهایی در جهت شناسایی هدف‌های اشتباه و اتلاف انرژی مهاجمین می‌شود. از جمله مکانیزم‌های این روش می‌توان به موارد زیر اشاره کرد:

۱. ایجاد مکانیزم‌های ظرف عسل[1]

در این روش سیستم یا قسمتی از آن برای فریب دادن کاربر غیر مجاز به‌صورت عمدی مورد استفاده قرار می‌گیرد.

۲. تنظیم اطلاعات اشتباه در پیغام‌های امضای تجهیزات
۳. مهم جلوه دادن اطلاعات بی ارزش.

۷-۵- راه‌کارهای پدافند غیرعامل در شبکه‌های ارتباطات سیار

در این بخش به بیان راه‌کارهای پدافند غیر عامل به منظور تامین امنیت، ایمنی و پایداری شبکه‌های ارتباطات سیار پرداخته می‌شود. هدف از این راه‌کارهای امنیتی بالا بردن مقاومت شبکه، کاهش میزان خسارات و تسهیل بازسازی شبکه در حملات و شرایط بحران و مخاصمات بین الملل است. در یک دسته بندی راه‌کارهای امن، ایمن و پایدارسازی شبکه ارتباطات سیار را می‌توان به دو بخش تقسیم نمود:

الف) راهکارهای مربوط به امنیت شبکه: راهکارهایی که کلان‌تر و غالبا از جنس معماری و طراحی بوده و لازمه‌ی برخی از آن‌ها تغییرات گسترده و زیربنایی در شبکه‌های ارتباط سیار می‌باشد.

[1] Honey Pot

ب) راهکارهای مربوط به پیاده‌سازی: راه‌کارهایی که اجرایی‌تر و جزئی‌تر هستند و پارامترهای عملی در آن‌ها لحاظ شده است.

۷-۵-۱- راهکارهای طراحی شبکه

همانطور که بیان شد راهکارهای طراحی عموما کلان‌تر و از جنس معماری و طراحی می‌باشند. این راهکارها بر اساس اصول راهبردی و مبتنی بر محورهای دفاعی بیان شده است. اصول کلی حاکم بر راهکارهای این بخش پیشگیری از حمله و نفوذ، جلوگیری از انتشار و تشدید، شناسایی و بازسازی در حد ممکن است. این راهکارها شامل موارد زیر می‌شوند[۲۸]:

۱. محرمانه و مخفی نگه داشتن اطلاعات ساختار، طراحی و پیاده‌سازی شبکه و نیز اطلاعات مربوط به اطلاعات مهم، حساس و حیاتی شبکه که تاثیر به‌سزایی در امنیت شبکه و جلوگیری از نفوذ دشمن دارد. بعنوان مثال طبقه‌بندی محرمانه‌ی اطلاعات جداول مسیریابی شبکه از این نمونه می‌باشند.
۲. مستقل‌سازی حداکثری بخش‌های مختلف شبکه ارتباطات سیار از دیگر شبکه‌های مخابراتی و رایانه‌ای.
۳. اجرای اصول و راه‌کارهای امنیتی در طراحی و پیکربندی زیرشبکه‌ها جهت جلوگیری از حمله و نفوذ به شبکه.
۴. رعایت اصول طراحی منطقه‌ای در شبکه‌ی ارتباطات سیار به‌گونه‌ای که حملات به یک مرکز یا منطقه صرفا منجر به اختلال یا دسترسی غیر مجاز به همان مرکز (منطقه) شود و یا کمترین میزان مشترکین را تحت تاثیر قرار دهد. یکی از اصول مهم در این راهکار، طراحی شبکه به زیرشبکه‌های نسبتا مستقل است.
۵. رعایت اصول طراحی لایه‌ای در شبکه‌ی ارتباطات سیار به گونه‌ای که نفوذ و صدمه به یک لایه وسیله‌ای برای گسترش نفوذ به لایه‌های دیگر نشود.
۶. طراحی شبکه به صورتی که تا حد ممکن اختلال یا دسترسی به یک سرویس به سایر خدمات صدمه‌ای وارد نکند.
۷. معماری و طراحی شبکه به گونه‌ای که در صورت گسترش خسارات به مراکز، در لایه‌ها و کاربردهای دیگر خسارت تضعیف گردد نه تشدید.
۸. طراحی و معماری به گونه‌ای که در حوادث و حملات به سرعت، مکان، نوع، عامل و سطح تاثیر شناسایی شود.
۹. طراحی دفاع در شبکه‌های ارتباطات سیار به گونه‌ای که دشمن برای حمله، به دانش سطح بالا و متنوع، هزینه‌ی زیاد، ابزار و تجهیزات متعدد، پیشرفته و پیچیده نیاز داشته باشد.

استفاده از راهکارهای بومی و نوآورانه‌ی امن، ایمن و پایدارسازی شبکه و عدم استفاده از پیشنهادات، روش‌ها و الگوریتم‌های امنیتی شناخته شده می‌تواند منجر به چنین نتایجی شود.

۷-۵-۲- راهکارهای پیاده‌سازی شبکه

راهکارهای پیاده‌سازی، اجرایی‌تر و جزئی‌تر بوده و برخی از آن‌ها در واقع روش‌هایی برای عملیاتی کردن راهکارهای طراحی شده هستند. این راهکارها به دو گروه قابل تقسیم هستند که در ادامه به بررسی آن‌ها می‌پردازیم. در این بخش مجموعه‌ای از راهکارهای ایمن‌سازی شبکه ارتباطات سیار که بیشتر در حوزه پیاده‌سازی است، بیان شده است[۲۸].

- اعمال اصول امنیتی در نصب تجهیزات و راه‌اندازی شبکه

راه‌اندازی مراکز و نصب تجهیزات شبکه باید در مناطقی که احتمال وقوع حمله یا حوادث غیر مرقبه کمتر و یا شرایط برای جبران خسارات احتمالی مناسب‌تر باشد صورت پذیرد.

- اجرای اصول اختفا، استتار و فریب در نصب تجهیزات و راه‌اندازی مراکز

اختفا به معنی مخفی سازی از دید دشمن، استتار به معنی مشابه سازی اهداف (تجهیزات، کابل‌ها و مراکز) و فریب به معنی به اشتباه انداختن دشمن در مورد اهداف واقعی است که این سه راهکار به عنوان سه اصل مهم پدافند غیرعامل باید در پیاده‌سازی شبکه ارتباط سیار در نظر گرفته شود.

- پراکندگی حداکثری مراکز و تجهیزات

یکی دیگر از روش‌های دفاعی در پدافند غیرعامل پراکنده‌سازی حداکثری تجهیزات مهم، حساس و حیاتی شبکه ارتباطات سیار است. البته ماهیت شبکه ارتباطات سیار پراکنده بوده که این خود یک حسن به حساب می‌آید ولی بخش متمرکز شبکه همچون نظارت و مدیریت از مراکز آسیب‌پذیر شبکه ارتباطات سیار محسوب می‌شود.

- مقاوم سازی مراکز و ارتباطات

با امن سازی شبکه ارتباطات سیار می‌توان از برخی حملات نرم پیشگیری نمود. به همین خاطر الزام اپراتور تلفن همراه به مقاوم سازی امنیتی و پیاده‌سازی استانداردها، رویه‌ها و

راهکارهای فنی امنیتی برای حفظ امنیت شبکه ارتباطات سیار تحت مدیریت خود نقش به‌سزایی در بالا بردن مقاومت شبکه تلفن همراه در هنگام حملات دشمن و حوادث غیر مترقبه خواهد داشت.

- راه‌اندازی مراکز پاسخگویی به حوادث امنیتی

در کنار ایجاد موسسات ملی امداد و نجات برای شبکه‌ها سامانه‌های رایانه‌ای CERT ملی، به‌طور خاص برای شبکه‌های ارتباط سیار نیز باید گروه‌ها و مراکز پاسخگو به حوادث امنیتی (IRT[1]) راه‌اندازی شود.

- تدارک تجهیزات و اجزای جبرانی در شبکه ارتباطات سیار

به‌منظور بازسازی سریع شبکه‌ی ارتباطات سیار، باید به میزان قابل قبولی اجرای شبکه و قطعات جانبی برای جایگزینی وجود داشته باشد.

- رعایت اصول راه‌اندازی سریع

جهت بازسازی، ترمیم و راه‌اندازی مجدد شبکه آسیب دیده باید اصولی رعایت شود تا محل و نحوه ذخیره‌سازی تجهیزات و لینک‌های جایگزین، شیوه‌های حمل و نقل آن‌ها، روش نصب و تعمیر آن‌ها سریع و آسان باشد.

- توسعه‌ی توان تولید و پشتیبانی داخلی در تجهیزات شبکه

تا حد امکان قابلیت ساخت و تعمیرات اساسی تجهیزات در داخل کشور و شرکت‌ها و نیروهای داخلی فراهم گردد. نکته دیگری که در این‌جا باید ذکر شود تلاش برای کاهش هزینه تولید، تعمیر و نصب تجهیزات شبکه به‌منظور بالا بردن صرفه و امکان مالی برای بازسازی خسارت محتمل زمان حادثه است. شاید یکی از روش‌ها نیز استفاده از توان داخلی برای تولید و پشتیبانی تجهیزات شبکه باشد.

[1] Incident Response Team

۷-۵-۳- راهکارهای امنیتی مربوط به فرایندها و روال‌ها

در این بخش راهکارهای امنیتی مربوط به پیاده‌سازی شبکه‌های ارتباط سیار بیان می‌گردد. این موارد به‌طور مستقیم قابل تست و پیاده‌سازی نیستند بلکه به منظور تدوین دستورالعمل‌ها، قوانین و رویه‌ها مورد بررسی قرار می‌گیرند[۲۹].

- بالا بردن اولویت امنیت نزد اپراتورهای همراه
- اپراتورهای تلفن همراه باید روال‌های درون و برون سازمانی را که امنیت شبکه تلفن همراه را تقویت می‌کند اجرا نماید.
- رعایت روال‌های امنیتی مربوط به مشترکان
- در روال‌های مربوط به خرید، صدور و تخصیص SIM به مشترکان باید اصول امنیتی جهت فاش نشدن اطلاعات در نظر گرفته شود.
- معتمد و آگاه بودن مدیران و مجریان شبکه
- یکی از مسایلی که تاثیر به‌سزایی در امنیت شبکه تلفن همراه دارد، معتمد بودن و آگاهی داشتن مدیران و مجریان است به گونه‌ای که ایشان با برخورد با برخی معضلات امنیتی و یا مشکلات پیش‌بینی نشده در شرایط عادی و بحرانی بتوانند به خوبی تصمیم‌گیری کنند. همچنین وضعیتی اتفاق نیوفتد که خودشان خواسته یا ناخواسته عامل یا تشدید کننده حملات دشمن شوند. طبق آمارهای بین‌المللی اکثر حملات و نفوذها به شبکه‌ها با واسطه یا بی‌واسطه از طریق کارکنان سازمان‌ها است نه هکرهای خارجی.
- از جمله مسایلی که باید رعایت شود اینست که تا حد ممکن نصب، راه اندازی و نگهداری تجهیزات مراکز مهم و به‌طور خاص، حساس و حیاتی توسط افراد مورد اعتماد و تایید شده صورت پذیرد. در صورتی که چاره‌ای جز بکار گیری نیروهای خارجی و یا ناشناخته نیست این افراد باید تحت نظارت و کنترل کامل افراد معتمد باشند.
- همچنین مدیران و متولیان آگاه شبکه ارتباطات سیار باید نظارت، بازدید و تست‌های دوره‌ای و مرتب در مراکز و لایه‌های شبکه بر روی طراحی‌ها، سخت افزار و نرم‌افزار شبکه داشته باشند.
- مراعات کنترل دسترسی و امنیت فیزیکی
- رفت و آمدها به مراکز و اماکن مهم، حساس و حیاتی شبکه ارتباطات سیار، همچنین دسترسی‌های فیزیکی و غیر فیزیکی به سخت افزارها و نرم افزارها باید طبق اصول از پیش تعریف شده و کاملا مطابق با آن باشد. همچنین کلیه دسترسی‌ها نیز به طرق مختلف باید تحت کنترل و نظارت و قابل بررسی باشد.
- ایجاد روال‌های امن در مورد اطلاعات شبکه
- اطلاعات ساختاری، طراحی و عملیاتی شبکه ارتباطات سیار، تعداد و نوع ارتباط سیستم‌ها، جدول مسیریابی، ظرفیت اجزای شبکه، نسخه نرم افزار و سخت افزار، وضعیت حال حاضر و

برنامه آینده توسعه شبکه، ایرادات و مشکلات فعلی شبکه ارتباطات سیار باید تحت طبقه‌بندی صحیح و منطبق با اصول پدافند غیرعامل قرار گیرد.

- ایجاد ساختار اطلاع رسانی عمومی

بسیاری از نفوذها به شبکه‌ها، ویروس‌های مخرب در شبکه، حملات از کار انداختن تجهیزات، مشکلات ناشی از شبکه اینترنت در GPRS، از ورودی گوشی و سیم مشترک حاصل می‌شود. با گسترش قابلیت‌های حافظه‌ای و پردازشی گوشی‌های تلفن همراه، روز به روز بر این تهدیدات افزوده می‌شود. به عنوان مثال بیشتر ویروس‌های شناخته شده‌ی موبایل که می‌تواند ترافیک و سیگنالینگ شبکه را تحت تاثیر قرار دهد از طریق بلوتوث منتقل می‌شود که ارتباطی با شبکه ارتباطات سیار ندارد. آموزش عمومی‌کاربران تلفن همراه، گسترش و بالا بردن سطح اطلاعات عمومی‌مشترکین از تهدیدات، مشکلات و عوارض امنیتی ممکن در مورد تلفن همراه، تدوین دوره‌های آموزشی از جمله راهکارهایی هستند که می‌توانند نقش موثری در کاهش این مشکلات داشته باشند.

فصل هشتم:

پدافند غیرعامل و توسعه فیبرنوری

۸-۱- مقدمه

از ویژگی‌های بشر، پویندگی و کمال گرایی است که به دنبال آن سیر تحولات بشری در طول تاریخ صورت گرفته است. عبور از عصر حجر، رسیدن به دوره کشاورزی و بعد از آن عصر صنعت، ورود به دوره رایانه‌ها و ابر رایانه‌ها، انسان ابزار ساز را به یک طراح مبتکر و سازنده هوش مصنوعی تبدیل کرده است. برقراری ارتباط از راه دور، در تمام دوران تاریخ بشری، از امیال و آرزوهای بزرگ آدمی‌بوده است. برقراری ارتباط، ازطریق ایجاد دود، توسط سرخپوستان، ارسال نامه‌ها توسط کبوترهای نامه بر و چاپار، اختراع مورس و سپس تلفن، نمونه‌هایی است که بشر، در اعصار مختلفی توانست، دامنه ارتباط خود را با پیرامونش توسعه دهد. در عصر رایانه‌ها و ماهواره‌ها، بشر می‌تواند در آن واحد، تصویر، صدا و دیگر اطلاعات مورد نیاز خود را در حداقل زمان، ارسال و یا دریافت کند. همزمان با ورود به قرن بیست و یکم و علی رغم توسعه و پیشرفت ارتباطات رادیویی و ماهواره‌ای و به دلیل انتشار روز افزون امواج الکترومغناطیسی، در فضای جو و به دنبال آن، ایجاد آلودگی صوتی در شهرهای بزرگ، توجه دست اندرکاران صنعت مخابرات و مراکز تحقیقاتی به ارتباطات با سیم و فناوری‌های روز، یعنی فیبرنوری چشمگیرتر شد، تا آنجا که، در خیلی از کشورها شبکه تلویزیونی کابلی و ISDN مجهز به سیستم پیشرفته انتقال فیبرنوری شده است.

فیبرنوری به عنوان محیط انتقال امواج نوری مورد استفاده قرار می‌گیرد و از تار شیشه‌ای ساخته می‌شود که سطح مقطع آن شامل دو ناحیه هسته و غلاف با ضریب شکست متفاوت می‌باشد. فیبر نوری از یک فیبر شیشه‌ای بمنظور ارسال اطلاعات شبکه، درقالب پالس‌های نوری استفاده می‌نماید. داده‌ها در داخل این پالس‌های نوری (با استفاده از یک دیود لیزری یا دیود نورگسیل) رمزگذاری می‌گردند. در طی ۵ سال گذشته، محیط فیبرنوری، بطور روزافزونی در سیستم‌های شبکه، مورد استفاده قرارگرفته‌اند[۳۰].

۸-۲- کارکرد فیبر نوری

تکنولوژی فیبر نوری، در مقایسه با رسانه استاندارد مسی، از پیچیدگی بیشتری برخوردار است. عامل این پیچیدگی در این حقیقت نهفته است که سیگنال‌های نوری فیبر، بجای گذارهای ولتاژ، از نوع پالسهای نوری هستند. سیگنال‌های فیبر نوری، یک‌ها و صفرهای سیگنال را از طریق

خاموش و روشن کردن منبع نوری، تولید می‌نماید. منبع نور معمولی یا یک دیود لیزری یا برخی از انواع دیودهای نورگسیل می‌باشد. نور حاصل از منبع، متناسب با الگوی داده‌هایی که می‌بایست رمزگذاری شوند، فلاش می‌زند. این پالس‌های نوری، اغلب بطور لحظه‌ای در داخل رسانای شیشه‌ای، از منبع به مقصد سفر می‌کنند. این هادی شیشه‌ای توسط یک روکش بنام cladding احاطه می‌شود. زیرا cladding دارای شاخص انعکاسی کمتری نسبت به فیبر شیشه‌ای بوده و مثل یک آینه سیگنال نوری را به داخل هسته فیبر باز می‌گرداند. هنگامی‌که پالس‌های نوری به مقصد می‌رسند یک سنسور، وجودیا عدم وجود سیگنال نوری را احساس نموده و علائم ON و OFF رابه سیگنال‌های الکتریکی نمایش داده شده با صفر و یک، تبدیل می‌کند. توجه به‌این نکته مهم است که هرچه افت و خیزهای سیگنال نوری بیشتر باشد، امکان بیشتری برای بروز افت سیگنال (تضعیف) وجودخواهد داشت. بعلاوه در مورد هر کانکتور فیبر نوری بین منبع ومقصد، امکان افت سیگنال وجود دارد. بنابراین کانکتورها می‌بایست در هر نقطه اتصال، بطور دقیق نصب گردند.

اغلب شبکه‌های WAN/LAN مبتنی بر فیبر نوری، از دو فیبر استفاده می‌کنند: یک فیبر برای ارسال ا طلاعات و فیبر دیگر برای دریافت داده‌ها مورد استفاده قرار می‌گیرد. این سیستم به‌این دلیل مورد استفاده قرار می‌گیرد که نور فقط در یک جهت در سیستم‌های فیبر نوری حرکت می‌نماید (جهت ارسال). تبدیل یک فرستنده فیبرنوری به یک فرستنده /گیرنده کاری مشکل خواهد بود.

۸-۳- تفاوت فیبرنوری و کابل مسی

از جمله مزایای استفاده از فیبرنوری در قبال کابل مسی می‌توان به موارد زیر اشاره کرد:

فیبرنوری سبکتر و ارزانتر از کابل مسی است و حجم کمتری را اشغال می‌کند. علاوه بر آن ظرفیت انتقال فیبرنوری چندین هزار برابر کابل مسی و فاقد اثرات نویز محیطی است، ضمن آنکه طول عمر بیشتر و تلفات کمتری دارد. فیبر نوری[1] رشته‌ای از تارهای بسیار باریک شیشه‌ای است که از آن برای ارسال سیگنال‌های نوری استفاده می‌شود. مزایای فیبر نوری نسبت به سایر رسانه‌های انتقال داده آنقدر زیاد است که بحق می‌توان کاربرد آن را انقلابی در این زمینه دانست. هر چند که فیبر نوری در دنیای فناوری بسیار جوان محسوب می‌شود اما در تمام کشورهای صنعتی و در حال توسعه جهان، توجیه ویژه‌ای به شبکه‌های مبتنی بر فیبر نوری می‌شود.

[1] optical fiber

۸-۴- علم اپتیک، ضرورت پیدایش و ساختار فیبرنوری

توجه فیزیکدانان و مطالعات و تحقیقات آنان در زمینه شناخت نور، تجزیه و شکست آن در منشور و عدسی‌ها، بازتاب و انعکاس آن در آینه‌ها و بدست آوردن قوانین مربوط به آن، موجب پیدایش علم اپتیک شد. اختراع میکروسکوپ، تلسکوپ، دوربین، عینک، لنز و لیزر و ... و کاربردهای وسییع آن‌ها در صنعت، نجوم، پزشکی و... از دستاوردهای دانشمندان این علم به شمار می‌رود که هم راستا با توسعه علوم الکترونیک، مخابرات و رایانه، برقراری ارتباطات مخابراتی را توسط فناوری فیبرنوری در یک گستره وسیع شاهد هستیم.

یک فیبر نوری از سه بخش مهم تشکیل شده است که عبارتند از هسته، روکش و بافر رویه. هسته همان رشته شیشه‌ای اصلی است که سیگنال‌های نوری در آن حرکت می‌کنند. دور این هسته، روکش قرار دارد که وظیفه بازگشت نور منعکس شده به هسته را دارد و این دو در روکشی پلاستیکی به نام بافر رویه قرار گرفته‌اند که وظیفه حفاظت هسته و روکش از آسیب‌های طبیعی را بر عهده دارد. هزاران رشته فیبر نوری یک کابل نوری را به وجود می‌آورند و هر کابل می‌تواند پهن باندی آنچنان وسیع را تامین کند که به تنهایی برای میلیون‌ها کاربر کفایت کند. کابل‌های نوری در روکش‌هایی به نام jacket حفاظت می‌شوند.

فیبرهای نوری معمولا در دو نوع تک حالته و چند حالته ساخته می‌شوند که نوع اول برای ارسال یک سیگنال در هر فیبر استفاده می‌شود (همانند تلفن) و نوع دیگر برای ارسال چند سیگنال در یک فیبر مورد استفاده قرار می‌گیرند (همانند شبکه‌های کامپیوتری.) فیبرهای تک حالته دارای هسته‌ای به قطر حدود ۰۱ میکرون و فیبرهای چند حالته دارای هسته‌ای به قطر تقریباً ۵۵ میکرون هستند(هر میکرون یک هزارم میلی متر).

مساله بزرگی که با حل آن، فیبرهای نوری ساختاری منحصر به فرد در انتقال امواج نوری می‌یابند، مسئله عبور نور از انحنا است. همان ور که همه می‌دانند نور فقط در مسیر مستقیم منتشر می‌شود و این مطلب می‌تواند بزرگ‌ترین مشکل در انتقال آن از طریق کابل باشد. در فیبرهای نوری این مسئله با انکسار و انعکاس مداوم حل یا به عبارتی بهتر شبیه سازی شده است. روکش محیط بر هسته فیبر، همانند آینه آب کاری شده است و به این ترتیب در هر انحنا نوری که در مسیر مستقیم سیر می‌کند با برخورد به سطح آینه‌ای روکش، مجددا به داخل هسته باز می‌گردد. بدین ترتیب هر چند که نور همچنان در خط مستقیم حرکت می‌کند اما ناچار است

شکست‌های مداوم، مسیر فیبر را بپیماید و در نهایت به مقصد برسد. نکته مهم در این میان، خلوص شیشه موجود است که اگر درصد خلوص آن پایین باشد سیگنال نوری تضعیف می‌شود. چنانچه داده‌ها نتوانند ازطریق سیگنال‌های نوری منتقل شوند، یا به بیانی دیگر امواج نوری نتوانند داده‌ها را حمل کنند، فناوری فیبر نوری دست کم در دنیای کامپیوتر، رسانه به درد خوری محسوب نمی‌شود. خوشبختانه چنین نیست و یک فرستنده نوری در مبدا سیستم رله فیبر نوری می‌تواند سیگنال‌های فیبر نوری را رمز نگاری کند. این سیگنال‌ها پس از طی مسافتی در درون فیبر نوری، در صورتی که مسافت طولانی باشد، در بازتاب نوری تقویت شده (به دفعات مورد نیاز) و سرانجام به دریافت کننده نوری می‌رسند. دریافت کننده، سیگنال‌های نوری را دریافت و رمز گشایی می‌کند. این فرآیند تقریبا همانند عملکرد تلگراف است. در فرآیند تلگراف، متن مورد نظر تحویل مسئول رمز نگاری می‌شود. او متن را تبدیل به رمزهای مورس می‌کند، این داده‌ها از طریق کابل (و به مدد تقویت کننده‌ها) به مقصد می‌رسد. مسئول بازگشایی رمز، آن‌ها را تبدیل به متن عادی می‌کند و متن به گیرنده تحویل داده می‌شود.

در سیستم رله فیبر نوری، فرستنده از اشعه لیزر برای رمز نگاری داده استفاده می‌کند. بازیاب (یا تقویت کننده) معمولا برای مسافتهایی بیش از یک کیلومتر به کار می‌رود و از تضعیف و بازتاب اشعه لیزر در فیبر نوری جلوگیری می‌کند. در مقصد، دریافت کننده نوری، برای تشخیص نور از فتوسل یا فتودیود استفاده می‌کند. در نهایت داده‌های حاصل دقیقا همان داده‌های تحویل داده به فرستنده هستند.

۸-۵- کاربردها و عناصر خط اتصال فیبر نوری

یک سیستم ارتباط موج نوری شامل یک فرستنده، یک رسانه انتقال و یک گیرنده است. فرستنده علامت الکترونی رمز گذاری شده را گرفته و آنرا به علامت نوری تبدیل می‌کند، پس از آن علامت نوری توسط رسانه انتقال (در اینجا کابل فیبر نوری) به یک تکرار کننده یا گیرنده فرستاده می‌شود. علامت نوری در گیرنده آشکار شده و به سیگنال‌های الکتریکی تبدیل می‌شود و بعد از آن با رمز گشایی به خروجی مناسب تبدیل می‌گردد. از فیبر نوری به دلیل افت اندک و پهنای باند گسترده، می‌توان به جای کابل TP یا کابل‌های کواکسیال به عنوان رسانه انتقال در یک سیستم ارتباط یک استفاده کرد. کابل‌های فیبر نوری دارای مزایای زیادی هستند که برخی از آن‌ها عبارتند از[۳۱] :

۱. افت اندک و پهنای باند زیاد
۲. اندازه کوچک و شعاع خمش کم
۳. غیر هادی، غیر تشعشعی و غیر القایی بودن
۴. وزن اندک
۵. فراهم آوردن ظرفیت رشد طبیعی.

اندازه کوچک، شعاع خمش کم (در حد چند سانتیمتر) و وزن اندک فیبرها و کابل‌های نوری در جایی اهمیت پیدا می‌کنند که فضا مثل فضای درون سفینه‌های فضایی، کشتی‌ها، و مجراهای شلوغ زیر خیابآن‌های شهر بسیار گران باشد. فیبرهای نوری موج برهایی عایق هستند و از این جهت دچار مشکلاتی مانند تداخل ناشی از تشعشع و مدارهای زمینی بسته، نمی‌شوند. همچنین هنگامی‌که در یک کابل بدون فلز نصب شوند آسیب‌ها و خرابی‌های ناشی از نور که در دیگر خطوط انتقال پیش می‌آید، گریبان آن‌ها را نمی‌گیرد و سرانجام مهندسی که از فیبرهای نوری استفاده می‌کند با انعطاف پذیری زیادی مواجه است. او می‌تواند یک کابل فیبر نوری را نصب کرده و از آن در یک سیستم با ظرفیت اندک (سرعت پایین بیت) استفاده کند. وی با افزایش نیازهای سیستم می‌تواند از مزایای ظرفیت‌های پهن باند فیبرهای نوری استفاده کرده و آنرا با تغییر الکترونیک پایانه‌ها به یک سیستم پر ظرفیت (ظرفیت با یک بیت) تبدیل کنید. چون افت خطوط انتقال فلزی با افزایش سرعت انتقال افزایش می‌یابد، کاربرد این خطوط در سرعت‌های بالاتر محدودیت پیدا می‌کند. از سوی دیگر سیستم فیبر نوری با افت ثابت در سرعت‌های متفاوت، این محدودیت را نداشته و سرعت آن برای پاس دادن به اقتضائات سیستم به طور طبیعی قابل افزایش است.

قسمت‌های کلیدی عبارتند از فرستنده که شامل منبع نوری و مدار تحریک همراه آن است، کابل که برای حفاظت مکانیکی و محیطی تارهای نوری داخل آن به کار می‌رود، و گیرنده که شامل آشکار ساز نوری به اضافه مدارات تقویت و بهبود سیگنال است و همچنین کانکتورها. تار نوری کابل شده یکی از مهمترین عناصر خط اتصال تار نوری است. کابل، علاوه بر محافظت تارهای شیشه‌ای ضمن نصب و سرویس، ممکن است حاوی سیم‌های مسی برای تغذیه تکرار کننده‌های مورد لزوم باشد که در فواصل معین برای تقویت و بازسازی متناوب سیگنال در هنگام کاربرد اتصال در فواصل دور به کار می‌روند. معمولا کابل‌ها از چندین تار شیشه‌ای استوانه‌ای به نازکی مو تشکیل می‌شوند که هر کدام از آن‌ها یک کانال مستقل ارتباطی هستند.

کابل‌های تار نوری مانند کابل‌های مسی، قابل نصب در هوا، کانال‌های زیر زمینی، زیر دریا و یا مستقیما دفن در زمین هستند. به دلیل محدودیت ساخت و یا نصب، کابل‌های تکی به طول چند صدمتر تا چندین کیلومتر برای کاربردهای فواصل دور ساخته می‌شوند. طول حقیقیی یک کابل، با ملاحظات عملی مختلف از قبیل اندازه پیچش و وزن آن تعیین می‌شود. از طول‌های کوتاهتر کابل معمولا در کانال‌های زیر زمینی استفاده می‌کنند. طول‌های بلندتر را در نصب هوایی یا به شکل دفن مستقیم در زمین، به کار می‌برند. خط کامل انتقال در فواصل دور، با پیوند کابل‌های مختلف تکی به یکدیگر شکل می‌گیرند.

یکی از مشخصه‌های اصلی تار نوری، میزان تضعیف آن به عنوان تابعی از طول موج است. در تکنولوژی اولیه، منحصرا از باند طول موج۸۰۰-۹۰۰nm استفاده می‌شد، زیرا در این ناحیه، تارهای ساخته شده آن زمان حداقل تضعیف را در منحنی تضعیف کلی نشان می‌دادند و منابع و آشکارسازهای نوری مناسب جهت کار در این طول موجها در دسترس بودند. با کاهش غلظت یونهای هیدروکسیل و ناخالصی‌های یون فلزی در ماده تار، سازندگان بلاخره موفق به ساخت موج برهایی نوری با تلفات بسیار پایین در ناحیه ۱۶۰۰- ۱۱۰۰ nm شدند. پهنای باند این طیف را معمولا ناحیه با طول موج بلند می‌گویند. به دلیل این‌که، تارهای سیلیکای خالص دارای حداقل اعوجاج سیگنال در طول موج ۱۳۰۰nm هستند، بنابراین میزان علاقه به استفاده از این طول موج افزایش یافت.

موقعی که سیگنال نوری، مسافت معینی را در تار نوری طی می‌کند، ممکن اسیت میزان تضیعیف و اعوجاج سیگنال به درجه‌ای برسد که برای تقویت و بازسازی آن در داخل خط انتقال، به تکرار کننده‌های میانی نیاز شود. تکرار کننده نوری مجموعه‌ای از یک گیرنده و یک فرستنده است که پهلو به پهلوی هم قرار گرفته‌اند و قسمت گیرنده، سیگنال نوری را آشکار و تبدیل به سیگنال الکتریکی کرده و پس از تقویت و بازسازی، به ورودی الکتریکی قسمت فرستنده ارسال می‌کند. قسمت فرستنده، سیگنال الکتریکی را مجددا تبدیل به سیگنال نوری می‌کند و سپس به موج بر تار نوری می‌فرستد. البته با توجه به‌این‌که معمولا شبکه‌های کامپیوتری خیلی طولانی نیستند در آن‌ها کمتر از تکرار کننده‌ها استفاده می‌شود. بیشتر کاربرد تکرار کننده‌ها در سیستم‌های مخابراتی است که در مسافت‌های طولانی از فیبر استفاده می‌شود.

۸-۶- نگاهی به استفاده از فیبر نوری در شبکه مخابرات ایران

در سال ۱۳۸۴ شبکه ملی فیبر نوری کشور در مراسمی به بهره برداری رسید. این شبکه توان خدمات مخابراتی کشور را افزایش داد و به عنوان یک شبکه پیشرفته زیرساخت مخابراتی امکان تعامل شبکه مخابرات کشور با کشورهای منطقه را فراهم نمود. شبکه ملی فیبر نوری ۹۰۰ شهر را با عرض باند گسترده نزدیک به ۴ برابر آنچه که تاکنون در زیرساخت‌های ارتباطی کشور ایجاد شده است به هم متصل می‌کند. ایجاد این شبکه فیبر نوری بیش از ۶۶۰۰ میلیارد ریال هزینه داشته است.

افتتاح این پروژه، زیرساخت‌های محلی و شهری ارتباطات کشور با سرعت‌های بیشتر و کیفیت برتر، به یکدیگر و به زیرساخت‌های منطقه‌ای و جهانی ا طلاعات، می‌پیوندد. با به کارگیری آخرین فناوری‌های انتقال نوری، در این شبکه، زیرساخت لازم برای تمام کاربردهای الکترونیکی از قبیل تجارت الکترونیکی، دولت الکترونیکی و بانک داری الکترونیکی در شبکه‌های مادر مخابراتی کشور فراهم و ارائه خدمات ارتباطی ارزان، پرسرعت و با کیفیت عالی به آحاد جامعه‌ایران اعم از روستایی و شهری، ممکن می‌شود.

مسیرهای اصلی این شبکه دارای طول ۳۱ هزار کیلومتر و مسیرهای فرعی آن به طول ۲۵ هزار کیلومتر است که در مجموع ۵۶ هزار کیلومتر کابل فیبر نوری را شامل می‌شود. مدیریت شبکه ملی فیبر نوری، از طریق مرکز کنترل مستقر در تهران و۳۰ استان قابل دسترسی و نظارت است که به نحو مطلوب امنیت فیزیکی شبکه و عملکرد آن تحت کنترل قرار می‌گیرد. همه فیبر نوری مورد نیاز این شبکه از تولید داخلی تامین شده است. ماشین آلات تولید فیبر نوری در بخش ساخت پیش سازه برای ظرفیت اسمی۵۰ هزار کیلومتر فیبر نوری استاندارد در سه شیفت کاری طراحی شده‌اند و عملا می‌توانند پیش سازه لازم برای ساخت ۳۰ هزار کیلومتر فیبر نوری استاندارد را تولید کنند[۳۰].

۸-۷- پدافند غیر عامل شبکه فیبر نوری

یکی از مهمترین مسایل در خصوص نگهداری وحفاظت مناسب از شبکه فیبرنوری موضوع با اهمیت پدافند غیرعامل می‌باشد که می‌بایست جهت طراحی واجراء سامانه وخطوط انتقال واتصال رعایت الگوهای حفاظتی و امنیتی مورد توجه واقع شود. این شیوه حفاظت شامل دو بخش سخت

افزاز و نرم افزار شبکه فیبر نوری می‌گردد. در این بخش به برخی از موارد با اهمیت پدافند غیرعامل شبکه فیبر نوری اشاره می‌شود[۳۰]:

۱. رعایت استانداردهای ایمنی واصول پدافند غیرعامل در شبکه ارتباط فیبر نوری مراکز تحقیقاتی، مخابراتی وفناوری اطلاعات وآی تی و ...
۲. رعایت مسایل ایمنی در شیوه رمزگذاری داده‌ها در درون پالس نوری
۳. توجه به مبانی پدافند غیرعامل دیود لیزری مورد استفاده در سیستم‌های فیبر نوری
۴. پدافند غیر عامل هادی شیشه‌ای درون فیبرنوری جهت جلوگیری از شکست نور
۵. پدافند غیرعامل سرعت مناسب ارسال سیگنالهای نوری در داخل هسته فیبر
۶. امنیت فرستنده وگیرنده‌های فیبر نوری
۷. پیشگیری از ایجاد انحناء در شبکه کابل نوری
۸. رعایت کیفیت در تولید شیشه مورد استفاده در فیبر
۹. پیشگیری از تخریب سامانه سیگنال رسانی نوری
۱۰. پدافند غیر عامل سامانه‌های رمزنگار فرستنده نوری و رمزگشا وگیرنده نوری
۱۱. ایمنی و حفاظت منابع نوری انتقال دهنده اطلاعات فیبر نوری
۱۲. حفاظت اطلاعات نقشه خطوط انتقال شبکه فیبر نوری کشور از اصول پدافند غیرعامل
۱۳. حفاظت اطلاعات مدارهای وایستگاه‌های تکرار کننده و منابع ارسال فیبر نوری
۱۴. رعایت اصول ایمنی در خطوط انتقال فیبرنوری زمینی وهوایی
۱۵. حفاظت شبکه فیبر نوری در مقابل امواج الکترومغناطیس
۱۶. افزایش تعداد نقاط تماس بین المللی شبکه فیبر نوری جهت پیشگیری از تخریب نقطه تماس واحد
۱۷. ۵۶ هزار کیلومتر شبکه فیبرنوری و ۶۶۰۰ میلیارد ریال سرمایه گذاری در پروژه فیبر نوری به عنوان زیرساخت ارتباطی کشور از اولویت‌های پدافند غیرعامل است.

فصل نهم:

ملاحظات پدافند غیر عامل در اینترنت ADSL

۹-۱- مقدمه

امروزه استفاده از اینترنت با پهنای باند بالا به عنوان یکی از معیارهای توسعه جامعه مدنی شناخته می‌شود و دولت‌ها سعی می‌کنند در راستای رسیدن به دولت الکترونیکی و استفاده از ابزارهای نوین فناوری حداکثر تلاش خود را مبذول نمایند. استفاده از سرویس‌های بی‌شماری که در سایه دولت الکترونیک به افراد جامعه داده می‌شود، همواره باعث می‌شود که متقاضیان به این گونه سرویس‌ها افزایش یابند و در سایه افزایش این سرویس‌ها عملا امکان پرداخت هزینه‌های سنگین اینترنتی برای کاربران وجود ندارد و ضمنا اتصال تلفنی به اینترنت باعث کندی بیش از حد سرویس‌دهی می‌گردد.

در این راستا شرکت‌های بزرگ ارائه خدمات اختصاصی[1] در زمینه ارتباطات که در حال حاضر تعداد آنها به یازده عدد می‌رسد، تجهیزات رایانه‌ای و ارتباطی را جهت جذب این گروه از کاربران خریداری کرده و در اکثر مراکز مخابراتی مستقر کرده‌اند. شبکه‌های یازده‌گانه تحت مدیریت شرکت‌های PAP تدارک و مدیریت ارتباط ADSL[2] در سطح کشور را به عهده دارند. بسیاری از ادارات، بانک‌ها، شرکت‌های خصوصی و منازل افراد از طریق این شبکه‌ها به یکدیگر و یا به شبکه اینترنت متصل شده‌اند. در حال حاضر بیش از یک‌صد هزار پورت با پهنای باندهای مختلف در سطح کشور فعال است و پیش بینی می‌شود این تعداد به سرعت افزایش یابد. تکنولوژی اطلاعات و ارتباطات و پیشرفت‌های چشمگیر بوجود آمده در این موضوع باعث شده تا دولت‌های پیشرفته کنونی را وادار سازد ضمن توسعه و ارتقاء این تکنولوژی، ساز و کار نظارت و امنیت این نوع ارتباطات را در رئوس کارهای خود قرار دهد. به دلیل محدودیت منابع شرکت‌های خصوصی یازده گانه در سرمایه گذاری، در حال حاضر هیچگونه تدابیر امنیتی خاصی برای محافظت از این شبکه‌ها لحاظ نشده است و در صورت اختلال در این شبکه‌ها زیان‌های شدیدی بوجود خواهد آمد. اهمیت این موضوع با توجه به ضرورت انتقال شبکه‌های بانکی از زیر ساخت‌های ارتباطی ماهواره‌ایی به زیر ساخت کابلی افزایش پیدا می‌کند. تنها جایگزین شبکه‌های ماهواره‌ایی، شبکه‌های ADSL ایجاد شده توسط شرکت‌های PAP می‌باشد. راه حل اصلی در این زمینه ایجاد مرکز کنترل امنیتی اختصاصی خطوط ADSL(با توجه به ماهیت و معماری خاص این سیستم‌ها) می‌باشد.

۹-۲- بررسی تکنولوژی ADSL

به دنبال پیشرفت دانش و فناوری اطلاعات و ارتباطات وگسترش شبکه‌های اطلاع رسانی و اینترنت با پهنای باند وسیع و در نتیجه آن بروز و ظهور نیازهای ارتباطی و خدمات مخابراتی در

[1] PAP: Private Access Provider
[2] Asymmetric Digital Subscriber Line

جوامع مختلف نیاز به ارسال اخبار، گزارش، پیام، منابع اطلاعاتی و غیره هر چه بیشتر افزایش یافت. بنابراین با ظهور اینترنت و اتصال رایانه‌ها به یکدیگر به صورت یک شبکه جهانی بحث انتقال داده‌ها بین نقاط مختلف جهان در کمترین زمان ممکن مطرح گردیده است. از آنجا که عموم کاربران، خانگی و تجاری بوده و از طرفی توانایی پرداخت هزینه‌های سنگین توسط این گروه ازکاربران وجود ندارد شرکت‌های بزرگ طراح و سازنده تجهیزات رایانه‌ای و ارتباطی جهت جذب این گروه از کاربران همواره به دنبال راه حل‌های اساسی در جهت طراحی، ساخت و تأمین تجهیزات و ابزارهای مناسب و ارزان قیمت بدون استفاده از زیر ساخت‌های ارتباطی قبلی (سیم مسی) بوده و هستند. لذا این‌گونه شرکت‌ها غالباً به دنبال روش‌هایی بوده‌اند تا بتوان با استفاده از تجهیزات و امکانات موجود و قدیمی خدمات جدید ارتباطی را فراهم ساخت.

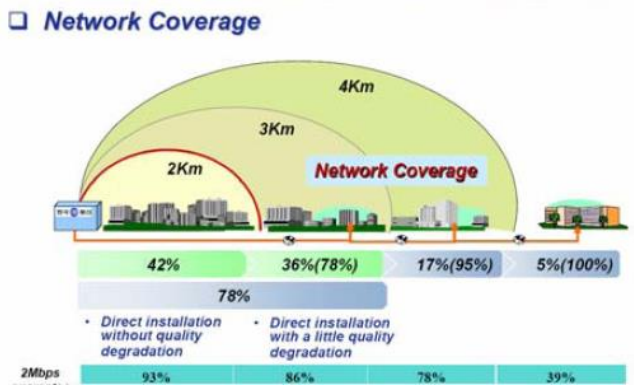
بنابراین با توجه به انجام و گسترش کابل کشی تلفن (وجود سیم مسی) از اوایل قرن بیستم تا به حال که تقریباً تمامی منازل، ادارات، سازمان‌ها و مراکز اجتماعی دارای آن هستند تحقیقات زیادی به منظور استفاده از زوج سیم کابل مسی جهت رسیدن به سرعت‌های بالاتر انتقال اطلاعات صورت گرفت که نتیجه آن تحت عنوان فناوری DSL و ADSL مطرح شد. در اغلب منازل و ادارات برخی از کشورهای دنیا، کاربران از یک DSL نامتقارن (ADSL) استفاده می‌نمایند. تکنولوژی ADSL در واقع نوعی از DSLها می‌باشد که ارتباط آن نامتقارن است، یعنی سرعت ارسال داده در ثانیه کمتر از دریافت آن می‌باشد. تکنولوژی ADSL فرکانس‌های قابل دسترس دریک خط را تقسیم تا کاربران اینترنت قادر به دریافت و ارسال اطلاعات باشند.

تکنولوژی ADSL با سایر تکنولوژی‌های مربوط به دستیابی به اینترنت نظیر مودم‌های کابلی و اینترنت ماهواره‌ای رقابت می‌نماید. بر طبق آمار اخذ شده در سال ۱۹۹۹، بیش از ۳۳۰۰۰۰ منزل در امریکا از ADSL استفاده کرده اند. تعداد کاربران استفاده از مودم‌های کابلی تا سال ۱۹۹۹ به مرز ۱۳۵۰۰۰۰ کاربر رسیده است. بر این اساس تا اواخر سال ۲۰۰۳، تعداد مشترکین مودم‌های کابلی به مرز ۸,۹۸۰,۰۰۰ و مشترکین DSL به ۹,۳۰۰,۰۰۰ رسیده اند[۳۲].

تکنولوژی ADSL پهنای باند ۱,۱ مگاهرتزی خطوط مسی را به کانال‌های ۴ کیلوهرتزی تقسیم می‌کند و آخرین کانال را جهت ارسال صدا و فاکس معمولی تخصیص می‌دهد و ۲۵۶ کانال دیگر را برای انتقال دو طرفه اطلاعات استفاده می‌کند. به این ترتیب که ۶۴ کانال را برای خط ارسال اطلاعات و ۱۲۸ کانال دیگر را جهت دریافت اطلاعات استفاده می‌کند. در بهترین حالت اگر ۱۹۲ کانال ۴ کیلو هرتزی موجود را استفاده کند، در تئوری سرعت باید به حدود ۹ مگابیت در ثانیه برسد. این خطوط از تمامی پهنای موجود در خطوط مسی دوطرفه استفاده می‌کنند تا بالاترین سرعت ممکن در ثانیه را بر خلاف خطوط معمول ارائه دهند. تکنولوژی ADSL همچنین به صورت یک ارتباط دایمی[1] است به طوری که استفاده کننده قادر می‌باشد به صورت ۲۴ساعته و ۷ روز هفته از ارتباط با شبکه (اینترنت) بهره مند شود.

[1] Always – on

ADSL از یک تکنولوژی با نام "تکنولوژی حساس به مسافت" استفاده می‌نماید. در این تکنولوژی متناسب با افزایش طول خط ارتباطی، کیفیت سیگنال افت و سرعت خط ارتباطی کاهش پیدا می‌نماید. ADSL دارای محدودیت ۱۸۰۰۰ فوت (۵۴۶۰ متر) است. کاربرانی که در مجاورت و نزدیکی شرکت ارائه دهنده سرویس DSL قرار دارند، دارای کیفیت و سرعت مناسبی بوده و متناسب با افزایش مسافت، کاربران اینترنت از نظر کیفیت و سرعت دچار افت خواهند شد. تکنولوژی ADSL قادر به ارائه بالاترین سرعت در حالت " از اینترنت به کاربر " تا ۸ مگابیت در ثانیه است. (در چنین حالتی حداکثر مسافت ۶۰۰۰ فوت و یا ۱۸۲۰ متر خواهد بود.) البته سرعت انتقال اطلاعات در محدوده ذکر شده علاوه بر عامل فاصله ارتباطی به نوع سیم استفاده شده نیز، بستگی دارد.



شکل ۹-۱- پوشش شبکه ADSL[۳۲]

۹-۳- سرویسهای قابل ارائه توسط شرکتهای PAP

فناوری ADSL با توجه به تجهیزات و توپولوژی که برای ارائه خدمات به مشترکین دارد می‌تواند علاوه بر ارائه خدمات اینترنت پر سرعت سرویس‌های دیگری از جمله سرویس سه گانه مبتنی بر همین بستر ارائه دهد. منظور از سرویس‌های سه‌گانه، ارائه اینترنت پرسرعت، تلفن و تلویزیون اینترنتی در قالب یک بسته به مشترکان است. مسلما هر یک از این سرویس‌ها، کاربردها و جذابیت‌های خود را دارد که ارائه همه آنها با هم و با قیمت مناسب، بر جذابیت‌های آنها می‌افزاید.

- **سرویس‌های ویدئو**

به ارسال و پخش برنامه‌های ویدئویی یا تلویزیونی برای مشترکان از طریق زیرساخت باند وسیع و توسط پروتکل اینترنت سرویس تلویزیون اینترنتی یا IP-TV گفته می‌شود. این سرویس

معمولا با سرویس‌های دیگری مانند ویدئو بر طبق تقاضا و تلفن اینترنتی و اینترنت پرسرعت، در قالب یک" بسته" به مشترکین ارائه می‌شود.
سرویس‌های ویوئو در قالب سرویس‌های زیر قابل ارائه است[۳۳] :

❖ ویدئو بر اساس تقاضا[1]

در سرویس ویدئو بر اساس تقاضا یا VoD، مشترکین بر اساس درخواست به تصاویر مورد نظر دسترسی خواهند داشت.

❖ انتشار ویدئو[2]

با ارائه این سرویس کاربران می‌توانند به ارسال تصاویر بر روی شبکه به صورت همگانی بدون نیاز به اشغال پهنای باند اختصاصی بپردازند. مانند پخش شبکه‌های صدا و سیما جهت مشترکین. با پشتیبانی از تکنولوژی Broadcasting، دیگر نیازی به اضافه نمودن پهنای باند برای تمامی مشترکین نیست، در این روش تجهیزات شبکه خود از داده‌ها به تعداد کاربران کپی سازی نموده و به تمامی کاربران با کیفیتی عالی بدون در نظر گرفتن تعداد آنها سرویس می‌دهد.

❖ کاربردهای سرویس ویدئو

۱. پخش دیجیتالی تلویزیون
۲. ویدئو بر طبق تقاضا
۳. آموزش از راه دور

- **سرویس تلفن اینترنتی**

با توجه به اینکه روش‌های برقراری ارتباط تلفنی در حال تغییر است، امروزه برای برقراری ارتباط تلفنی راه دور اغلب از تکنولوژیی به نام سرویس تلفن اینترنتی یا VoIP[3] استفاده می‌شود. سرویس VoIP یک روش برای تبدیل سیگنال‌های آنالوگ صوت به داده‌های دیجیتال است که از طریق اینترنت منتقل می‌شوند. سرویس VoIP می‌تواند یک ارتباط اینترنت استاندارد را به یک روش مجازاً رایگان برای برقرای ارتباطات تلفنی در هر جای دنیا تبدیل کند.

[1] Video On Demand
[2] Video Broadcasting
3 Voice Over IP

- **سرویس بازی‌های شبکه**[1]

بوسیله تجهیزات شرکت‌های PAP، سرویس دهنده با استفاده از حداقل پهنای باند ممکن می‌تواند به ارائه سرویس بازی‌های تحت شبکه بپردازد. این تجهیزات با تشخیص سیگنالهای مخصوص بازی‌ها، آنها را کپی کرده و به کاربران بازی به صورت همزمان ارسال می‌کند. بدین وسیله با حداقل پهنای باند بین مراکز برترین کیفیت سرویس بوجود می‌آید.

- **سرویس اینترنت**

امروزه اینترنت رفته رفته جزء لاینفکی از زندگی انسان‌ها در این عصر می‌شود. بدون شک هر فردی به نقش وسیع اینترنت و شبکه‌های اطلاع رسانی داده‌ها و اهمیت آن در تجارت الکترونیکی، آموزش الکترونیکی، دولت الکترونیکی، پول الکترونیکی و دیگر نیازهای روز پی خواهد برد. اما در این بین نحوه اتصال وکیفیت این نوع ارتباط اهمیت قابل ملاحظه‌ای دارد. فناوری ADSL امکان ارتباط پر سرعت کاربر را با شبکه جهانی اینترنت فراهم می‌سازد به طوری که کاربر با استفاده از خط تلفن موجود درمحل کار و یا منزل بدون این‌که خط اشتغال گردد می‌تواند ارتباطی پرسرعت و دایمی‌را با بهترین کیفیت با شبکه اینترنت و شبکه‌های اطلاع رسانی داشته باشد.

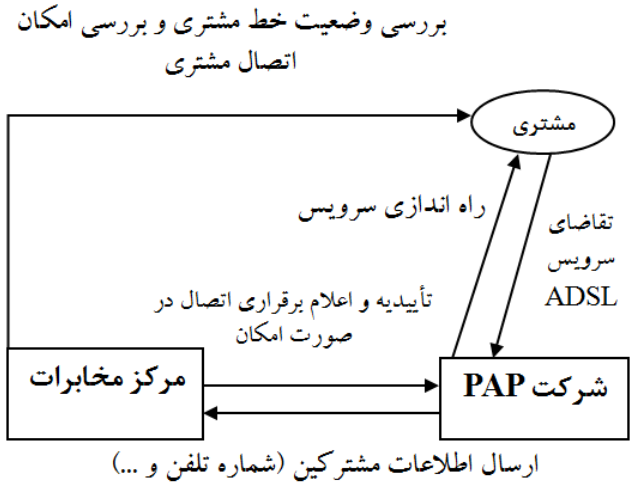
۹-۴- معماری شبکه‌های ADSL

امروزه در دنیا شرکت‌های موجود در امور مخابراتی، توسط میلیون‌ها کیلومتر کابل، فیبر و بسترهای آماده و فراهم خود از یک طرف و شرکت‌های ارائه دهنده خدمات شبکه اینترنت با اتکا به فناوری‌ها و روش‌های نوین از طرف دیگر، پا به عرصه گذاشته‌اند تا بتوانند با مشارکت یکدیگر و استفاده از تکنیک‌ها و ابزار فن آوری اطلاعات و ارتباطات، خدمات شبکه با پهنای باند بالا را برای تمامی اقشار، ادارات و جوامع فراهم آورند.

تکنولوژی ADSL فرق چندانی با سایر گزینه‌های متداول دسترسی پرسرعت همچون مودم‌های کابلی ندارد. مهم‌ترین مشخصه این شبکه‌ها، ترکیب و تجمیع ترافیک ارتباطی گروه بزرگی از مشترکان در لبه شبکه[2] و ارسال این ترافیک یکپارچه به سمت هسته اینترنت[3] از طریق لینک‌های بسیار سریع مخابراتی است. لبه شبکه علاوه بر تجمیع ترافیک‌ها، بسیاری از عملیات مدیریتی و امنیتی را نیز برعهده دارد و از این لحاظ یکی از مهم‌ترین عناصر این ساختار به‌شمار

[1] GAME NETWORK
[2] Edge Network
[3] Internet Core

می‌رود. شکل زیر نحوه ارتباط شرکت‌های PAP با مراکز مخابراتی و نحوه درخواست سرویس توسط مشتری را نشان می‌دهد.



شکل ۹-۲- نحوه ارتباط شرکت‌های PAP و مخابرات و مشتری[۳۲]

برای بهره گیری از تکنولوژی ADSL در حالت عمومی‌و نگاه کلی باید از وجود دو دستگاه خاص برای این منظور استفاده نمود. یکی از این دستگاه‌ها باید در محل مشترکین و دستگاه دیگر در محل ارائه دهنده خدمات ADSL، نصب گردد. در محل مشترکین از یک ترانسیور ADSL استفاده می‌گردد. شرکت ارائه دهنده خدمات ADSL از یک دستگاه با نام DSLAM[۱] استفاده می‌نماید. تجهیزات و تمهیداتی که برای برقراری ارتباط کاربر تا شرکت PAP مورد نیاز است عبارتند از:

الف ـ سمت کاربر:

۱. مودم‌های ADSL

۲. تضمین اینکه خط کاربر از نوع تقسیم فرکانسی نباشد.

ب ـ مراکز مخابراتی

۱. Splitter + Micro Filter[۲]

۲. DSLAM

ج ـ شرکت‌های PAP

۱. فایروال‌های سخت افزاری و نرم افزاری

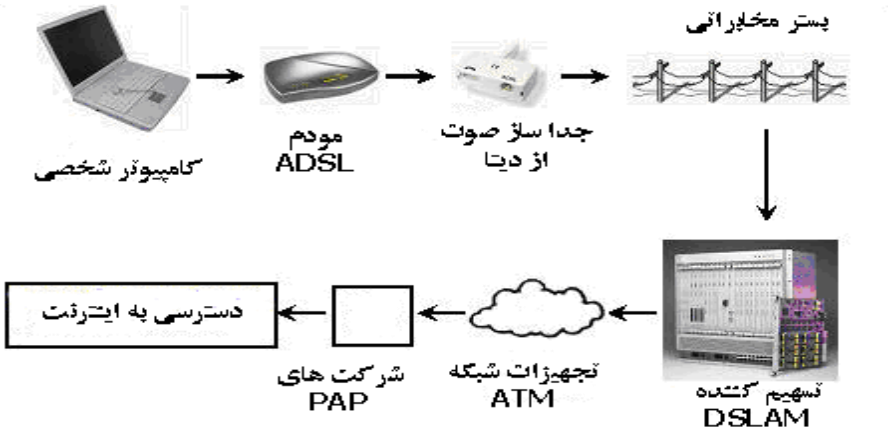
[1] Digital Subscriber Line Access Multiplexer

[۲] جداکننده

۲. مسیریاب‌های توزیع اینترنت

شبکه‌های ADSL از نقطه محل مشترک شروع و با استفاده از زوج سیم مسی مخابرات به مرکز مخابرات منتقل می‌گردد. در مرکز مخابرات سر کابل مشترک توسط یک جدا کننده به دو بخش ارایه خدمات تلفن صوتی و بخش ارایه خدمات دیتا تقسیم می‌گردد. کاربران با به کارگیری جداکننده‌های[1] نسبتاً ارزان قیمت در محل خود قادر به استفاده همزمان از سیم تلفن خود برای اتصال به گوشی تلفن و مودم خواهند بود.

بخش ارایه خدمات دیتا در نهایت توسط بستر ارتباطی و تجهیزات مستقر در مرکز مخابرات به DSLAMها و تجهیزات شرکت‌های PAP برای ارایه خدمات شبکه به کاربران متصل می‌گردد. برای بررسی موضوع و تجهیزات مورد استفاده، شکل زیر که بیانگر شیوه ارتباطی و ساختار شبکه ADSL می‌باشد، ترسیم شده است. در ادامه هر یک از اجزا این شبکه بررسی خواهند شد.



شکل ۹-۳- شیوه ارتباطی و ساختار شبکه ADSL[۳۳]

- **مودم ADSL**

مودم ADSL دستگاهی است که می‌تواند یک کامپیوتر یا یک مسیریاب را از طریق خط DSL برای بهره‌گیری از خدمات ADSL به مرکز خدمات دهنده متصل کند. مودم‌های ADSL نیز همانند تمامی مودم‌ها وظیفه اصلی دریافت و ارسال اطلاعات[2]را به عهده دارند. در واقع این مودمها امواج فرکانس بالا[3] را (در محدوده 25 KHz تا 1 MHz)[4] برای ارسال به DSLAMها مدوله[5] کرده و امواج دریافتی از DSLAMها را در محل کاربر مجددا رمزگشایی[6] و به صورت دیتا

[1] Splitter
[2] Transceiver
[3] high-frequency tones
[4] Voice bands are in 0-4 kHz range
[5] modulate
6 Demodulate

به کامپیوتر کاربر منتقل می‌کند. مودم‌های ADSL قادر هستند با در اختیار داشتن مسیریاب DSL[1]، مدیریت اتصال به شبکه و نحوه اشتراک گذاری ارتباط و منابع را نیز مدیریت کنند.

- **تسهیم کننده DSLAM**

تسهیم کننده‌های DSLAM که اغلب با نام Dee-slam شناخته می‌شوند، ابزاری هستند که چندین کانال انتقال با سرعت پایین تر را در کانالی با سرعت بالا در انتهای یک اتصال برای دسترسی پرسرعت مشترکین یک شرکت PAP ترکیب می‌کند. (تسهیم کننده دیگری در انتهای دیگر اتصال، این فرآیند را معکوس می‌سازد تا کانال‌های با سرعت پایین را مجددا تولید کند.)

تصویر تسهیم کننده Siemens DSLAM SURPASS hiX 5625 شرکت زیمنس را که در بخش Passive تجهیزات ADSL شرکت‌های PAP به کار رفته است در شکل زیر را نشان داده شده است.

شکل ۹-۴- تصویر تسهیم کننده Siemens DSLAM SURPASS hiX 5625[۳۳]

بعلاوه DSLAM می‌تواند امکاناتی همچون مسیریابی یا تخصیص آدرس دینامیکی IP را نیز برای مشترکین فراهم کند. در واقع DSLAM را می‌توان دلیل اصلی تفاوت بین سرویس‌دهی از طریق ADSL و از طریق مودم کابلی به حساب آورد. در این ارتباط‌ها DSLAM خطوط ارتباطی جهت یافته از سوی تعداد زیادی از مشترکین را دریافت نموده و آن‌ها را روی یک خط ارتباطی با ظرفیت بالا به اینترنت منتقل می‌کند. دستگاه‌های DSLAM قادر به پشتیبانی چندین نوع DSL یک مرکز تلفن واحد و تعداد گوناگونی از پروتکل‌ها و روش‌های مدوله سازی هستند. تصاویر رک و کارت‌های DSLAM در شکل‌های زیر نشان داده شده اند.

1 DSL Router

شکل ۹-۵- DSLAM rack[۳۳]

مسیر رسیدن دیتا به تسهیم کننده‌های DSLAM :

۱. محل کاربر که از طریق مودم ADSL متصل می‌گردد.
۲. مسیر کابل[1] از محل کاربر تا مرکز مخابرات که اغلب Last Mile نامیده می‌شود.
۳. تسهیم کننده DSLAM که وظیفه دریافت و ارسال اطلاعات از کاربر را به عهده دارد. این دستگاه همچنین وظیفه تلفیق اطلاعات و صدا را بر روی خط ارتباطی کاربر بر عهده دارد. در آن سوی خط وظیفه جداسازی صدا و اطلاعات و ارسال اطلاعات به شبکه‌های دیتا و ارسال صدا به سوییچ‌های مخابراتی را باید انجام دهد.
۴. مرکز MDF[2]که در واقع یک رک[3] برای اتصال خطوط مشترکین از خارج مرکز مخابرات به داخل مرکز می‌باشد. از این مرکز برای اتصال خطوط مشترکین به خطوط تجهیزات شبکه استفاده می‌شود. مراکز MDF معمولاً در مجاورت مراکز سوییچ مخابراتی بنا می‌شوند و فاصله چندانی از یکدیگر ندارند.

شکل ۹-۶- مرکز MDF شرکت مخابرات[۳۳]

[1] Local Loop
2 Main Distribution Frame
3 Rack

۹-۵- پروتکل‌های ارتباطی شبکه‌های ADSL

برای رفع چالش‌هایی که در خصوص بکارگیری سرویس‌های ADSL وجود دارد، اجرای یک پروتکل مشخص بین کاربر و فراهم‌کننده خدمات توصیه می‌شود. این پروتکل از نوع پروتکل‌های محلی است که به منظور شناسایی وظایف مشخص میان دو نقطه اجرا می‌شود و در ارتباطات خارج از آن حوزه نقش ندارند. در حال حاضر چهار گزینه در این خصوص وجود دارد که هر یک مزایا و نقاط ضعف منحصر به خود را دارند و عبارتند از [۳۴]:

- **آدرس دهی ثابت IP [1]**

اولین و در واقع ابتدایی‌ترین راه حل، تخصیص یک آدرس IP به هر کاربر است که خود به تنظیم آن روی کامپیوتر خود اقدام می‌کند. این روش اساساً یک پروتکل نیست، تنها یک راه‌حل سریع برای مشکل است که از ابعادی گسترده برخوردار است. برای مثال، مشکل استفاده همزمان چند کامپیوتر و یک کاربر از ارتباط ADSL به این ترتیب حل نمی‌شود.

- **پروتکل پیکربندی پویای میزبان (DHCP [2])**

این روش برای این منظور طراحی شده است که پیکربندی IP را روی کامپیوتر کاربران به صورت خودکار انجام دهد. این پروتکل در شبکه‌های محلی سازمانی نیز از کاربرد گسترده‌ای برخوردار است. به‌ویژه در مورد پایانه‌هایی که به طور موقت به این شبکه‌ها متصل می‌گردند (برای مثال کامپیوترهای Laptop). پروتکل DHCP در حقیقت یک جهش محسوس نسبت به روش آدرس‌دهی ثابت محسوب می‌شود.

- **پروتکل تونل‌زنی لایه۲ (L2TP [3])**

پروتکل L2TP، به عنوان یک گزینه نسبتاً جدیدتر برای شبکه‌های دسترسی باند پهن مطرح است و با ایجاد یک تونل مجازی از داخل شبکه اینترنت، کاربر را به هر نقطه مشخصی متصل می‌کند و کلیه تنظیمات لازم برای برقراری سرویس از داخل این تونل بر تجهیزات کاربر اعمال می‌گردد. پروتکل L2TP در عمل یک شبکه مجازی یا VPN [4] روی شبکه فراهم کننده

[1] Static IP Address
[2] Dynamic Host Configuration Protocol
[3] Layer 2 Tunneling Protocol
[4] Virtual Private Network

ایجاد می‌کند که از امنیت خوبی نیز برخوردار است، ولی درعوض پیچیدگی و سرباره بیشتری دارد. به‌ویژه در شبکه‌های بزرگ دسترسی با چندین هزار کاربر، مدیریت این تونل‌ها دشوار خواهد بود.

- **پروتکل نقطه به نقطه روی ATM (PPPoA[1]) و پروتکل نقطه به نقطه روی اترنت(PPPoE[2])**

این پروتکل ترکیبی است از پروتکل‌های PPTP [3] و L2F[4] که توسط شرکت سیسکو توسعه یافته است. این پروتکل ترکیبی است از بهترین خصوصیات موجود در L2F و PPTP. این پروتکل فریم‌های PPP را برای ارسال بر روی شبکه‌های IP مانند اینترنت و علاوه بر این برای شبکه‌های مبتنی بر X.25، Frame Relay و یا ATM کپسوله می‌کند. هنگامی که اینترنت به عنوان زیر ساخت تبادل اطلاعات استفاده می‌گردد، L2TP می‌تواند به عنوان پروتکل Tunneling از طریق اینترنت مورد استفاده قرار گیرد.

۹-۶- نقاط آسیب پذیر شبکه‌های ADSL

با توجه به ساختار معماری شبکه‌های ADSL نقاط آسیب پذیر می‌تواند هر یک از تجهیزات فعال و غیر فعال به کار گرفته شده در ساختار شبکه ADSL باشد. تجهیزات غیر فعال شبکه‌های ADSL شامل ساختمان‌ها و مکان‌های استقرار تجهیزات مربوطه، بستر رسانه، تجهیزات اتصال و ... می‌باشد. نقاط آسیب پذیر تجهیزات غیرفعال شبکه‌های ADSL و تدوین ملاحظات پدافند غیر عامل برای این بخش از تجهیزات در مبحث امنیت فیزیکی مورد بررسی قرار می‌گیرد. تجهیزات فعال شبکه‌های ADSL از جمله مودم‌های ADSL، تسهیم کننده‌های DSLAM، مسیریاب‌ها، پروتکل‌های ارتباطی، سرورهای AAA[5]، اگر مطابق سیاست صحیح و برنامه ریزی شده‌ای تهیه و بومی سازی نشده باشند هنگام بروز مخاصمات بین الملل یا جنگ‌های سایبری و فیزیکی به شدت در معرض آسیب پذیری هستند به علاوه در صورت عدم تنظیم صحیح در مواقع تهدیدات امنیتی نیز می‌توانند مورد هجوم و آسیب قرار گیرند.

[1] Point to Point Protocol over ATM
[2] Point to Point Protocol over Ethernet
[3] Point to Point Tunneling Protocol
[4] Layer 2 Forwarding
[5] AAA Server: Authentication Authorization Accounting server

۹-۶-۱. مودم‌های ADSL

با توجه به پروتکل‌های ارتباطی و شیوه‌های اتصال به شبکه ADSL که در بخش قبلی مورد بحث قرار گرفت، از آنجایی که برای دسترسی و اتصال به شبکه ADSL معمولاً نام کاربری و رمز عبور مورد استفاده قرار می‌گیرد، اولین خطری که در استفاده از مودم‌ها، کاربران شبکه را مورد تهدید قرار می‌دهد، دسترسی به این اطلاعات می‌باشد. از آنجا که کاربران معمولا برای انتقال نام کاربری و رمز عبور خود از مودم استفاده می‌کنند، باید اطمینان داشته باشند که مودم و برنامه‌ی سرویس دهنده‌ی آن بدرستی نصب شده‌اند، صحیح عمل می‌کنند، و دقیقا آنچه را که مورد انتظار است را انجام می‌دهند. بعضی از مودم‌ها می‌توانند حاوی کدها و دستورالعمل‌های خاص برای نفوذ به شبکه یا کامپیوتر کاربران یا حاوی دستورالعمل‌هایی برای ارسال اطلاعات به نقاط دیگر باشد. بنابراین اولین گام در امنیت شبکه‌های ADSL استفاده از مودم‌های امن که مورد بررسی و ممیزی قرار گرفته‌اند می‌باشد. گام بعدی استفاده از مودم‌هایی است که به طور داخلی به کارگیری از رمزکننده‌ها را برای ارسال اطلاعاتی نظیر نام کاربری و رمز عبور به کار می‌گیرند.

۹-۶-۲. خطوط ارتباطی مخابراتی

عمل شنود بر روی سیم‌های مسی، چه در انواع Coax و چه زوج‌های بهم تابیده، هم‌اکنون نیز از راه‌های نفوذ به شمار می‌آیند. با استفاده از شنود می‌توان اطلاعات بدست آمده از تلاش‌های دیگر برای نفوذ در سیستم‌های کامپیوتری را گسترش داد و به جمع‌بندی مناسبی برای حمله رسید. هرچند که می‌توان سیم‌ها را نیز به گونه‌ای مورد محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه‌ی فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال‌های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین‌ترین حد خود نسبت به استفاده از سیم در ارتباطات می‌شود. بنابراین یکی از نقاط آسیب پذیر در شبکه‌های ADSL مسیر کابل و نحوه انجام آن می‌باشد. باید با توجه به روش‌های عبور کابل از مسیر حفاظت شده و امن نظیر عبور از داکت‌های فولادی و مستحکم با توجه به حساسیت مراکز، نسبت به ایمن کردن تجهیزات اتصال مسیر، اقدام نمود.

۹-۶-۳. تسهیم کننده‌ها (DSLAM)

با توجه به عملکرد و وظیفه تسهیم کننده‌ها، همانند آنچه که در مورد مودم‌های ADSL در مورد کدهای مخفی برای نفوذ و ارسال اطلاعات به نقاط خارج از شبکه اشاره شد، در این مورد نیز

مورد توجه و ارزیابی قرار گیرد. اصولا باید در مورد این تجهیزات نیز ممیزی و دقت لازم در مورد به کارگیری تجهیزات مطمئن و بومی شده، صورت پذیرد.

نکته دوم در مورد این تجهیزات بررسی و اطمینان از عدم وجود دستورات کنترلی در این تجهیزات می‌باشد. توسط دستورات کنترلی می‌توان از طریق شبکه و از راه دور عملکرد این تجهیزات را تغییر داد و یا کارکرد آن‌ها را مختل نمود. از آنجایی که یکی از اهداف امنیت و ملاحظات پدافند غیر عامل، پایداری در ارائه سرویس می‌باشد باید این موضوع و تهدید را در مورد این تجهیزات به دقت مورد توجه قرار داد.

در این خصوص موارد زیر حائز اهمیت می‌باشند:

- تجهیزات passive شرکت‌های PAP در محوطه‌های باز و پیرامونی مراکز مخابراتی و درون کانکس‌هایی که دارای هیچ گونه امنیت فیزیکی نمی‌باشد، قرار گرفته است و امکان نفوذ به آنها به سادگی وجود دارد.
- تعداد بسیار زیادی از پورت‌های شرکت‌های PAP بدون استفاده (نداشتن کاربر) مانده است.
- پرسنل مراکز مخابراتی دانشی در خصوص این تجهیزات ندارند و در صورت بروز مشکل صرفا با مراجعه متخصصین شرکت‌های PAP مشکل رفع خواهد شد.
- کابل‌های رک‌ها بدون رعایت نکات امنیتی به اتاق‌های MDF مراکز مخابراتی رفته است.

۹-۷- تهدیدات و حملات علیه شبکه‌های ADSL

سیستم‌های شبکه‌های کامپیوتری از طریق راه‌های بسیار زیادی می‌توانند مورد حمله واقع شوند که موجب ایجاد خسارات بسیار زیادی می‌گردند. این حملات می‌توانند به صورت‌های زیر باشند[۳۴]:

- **ممانعت از ارائه سرویس (DOS[1]):**

هکرها از طریق قطع جریان اطلاعات به وسیله قطع کردن دستگاههای مهم و بحرانی مثل سرور، روتر و دیوار آتش و یا با ارسال بیش از حد بسته‌های اطلاعاتی به سرورها اقدام به خارج کردن آنها و عدم سرویس دهی آنها می‌نمایند. همچنین در صورت بروز مخاصمات بین الملل شرکت‌ها و کشورهای سازنده تجهیزات ممکن است برای ضربه زدن به کشور در مورد تجهیزاتی که از آنها در شبکه وجود دارد، اقدام به خارج کردن از سرویس دهی این نوع از تجهیزات از راه دور و

[1] Denial of Service

مبتنی بر شبکه اینترنت نمایند. در این نوع حمله، کاربر دیگر نمی‌تواند از منابع و اطلاعات و ارتباطات استفاده کند. این حمله از نوع فعال است و می‌تواند توسط کاربر داخلی و یا خارجی صورت گیرد.

- **سرقت اطلاعات :**

هکرها و حمله کنندگان برای دست یابی به اطلاعات اختصاصی سازمان‌ها و تخریب آن با روش‌هایی همچون استراق سمع و نفوذ به داخل سازمان و یا بهره‌گیری از برنامه‌های کامپیوتری جهت شناسایی و یافتن کلمه عبور کاربران مجاز اقدام به سرقت اطلاعات می‌نمایند.

- **تخریب داده‌ها:**

حمله کننده‌ها به داده‌های ذخیره شده بر روی دیسک‌ها در زمان انتقال بین شبکه خسارت وارد می‌نمایند. این حمله یک حمله فعال است که در آن جامعیت و صحت اطلاعات را با تغییرات غیر مجاز بهم می‌زند و باعث اختلال جدی در عملکرد صحیح شبکه می‌شود.

- **تحلیل ترافیک:**

در این نوع حمله مهاجم براساس بسته‌های اطلاعاتی ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب می‌کند. این حمله یک نوع حمله غیر فعال است و اکثرا توسط کاربران خارجی صورت می‌گیرد. با بدست آوردن این نوع تحلیل می‌توانند برای شناسایی و از کار انداختن شریان‌های اصلی کشور بهره بگیرند.

- **جعل هویت**

این نوع حمله یک نوع حمله فعال است که در آن هکر هویت یک فرد مجاز شبکه را جعل می‌کند و برای اختلال در صحت عملکرد شبکه یا برای دریافت اطلاعات از آن بهره می‌گیرد.

- **تحریم**

یکی دیگر از تهدیداتی که متوجه عملکرد صحیح شبکه و توسعه آن است، وضع تحریم‌ها و عدم ارائه تجهیزات و قطعات و خدمات فنی در رابطه با تجهیزات فنی شبکه نظیر تسهیم کننده‌های DSLAM، مسیریابها و ... می‌باشد.

- **حملات ضد امنیتی مسیریاب‌ها**

حمله به مسیریاب‌ها و سوئیچ‌های شبکه بخش مهمی از حملات منطقی را تشکیل می‌دهند. حملات ضد امنیتی منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ‌ها، را می‌توان به سه دسته‌ی اصلی تقسیم نمود :

۱- حمله برای غیرفعال سازی کامل
۲- حمله به قصد دستیابی به سطح کنترل
۳- حمله برای ایجاد نقص در سرویس‌دهی

در یک شبکه که شامل مجموعه‌ای از نقاط است وجود تأسیسات کافی و غیر قابل نفوذ امنیتی در یک نقطه و از سوی دیگر نبود امنیت کافی در نقاط دیگر شبکه شبیه به آن است که یک محافظ در جلوی میز کامپیوتر واقع شده باشد حال آنکه کامپیوتر کاملا در دسترس باشد این مسئله حاکی از آن است که چنانچه بخشی از شبکه غیر قابل نفوذ و سایر نقاط آسیب پذیر باشد در عمل گویی کل شبکه با مشکل امنیتی مواجه است.

۹-۸- ملاحظات پدافند غیر عامل

به منظور حفاظت از تجهیزات و برقراری امنیت خدمات شبکه‌های ADSL با رویکرد پدافند غیر عامل و به منظور دست یافتن به اهداف ترسیم شده در اسناد پدافند غیر عامل موارد زیر می‌تواند تا حدود زیادی مشکلات مهم را در این حوزه برطرف نماید[۳۴]:

۱. تجهیزاتی که دارای بیشترین نیاز امنیتی هستند، در امن ترین منطقه قرار گیرند و اجازه دسترسی عمومی به آن‌ها و یا از سایر شبکه‌های دیگر به این منطقه داده نشود. دسترسی‌ها باید با کمک یک فایروال و یا سایر امکانات امنیتی مانند دسترسی از راه دور[1] به طور امن کنترل شود. همچنین کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه باید با درجه امنیت بالایی انجام شود.
۲. سرورهایی که در این شبکه‌ها مورد استفاده و دسترسی هستند، در منطقه‌ای جداگانه و دارای ضریب امنیتی بالاتر نسبت به سایر بخش‌ها قرار گیرند تا در صورت مورد حمله قرار گرفتن یکی، سایرین مورد تهدید قرار نگیرند. به این مناطق، مناطق خارج از تهدیدات نظامی[2] گفته می‌شود.

[1] RAS: Remote Access Control
[2] DMZ: Demilitarized Zone

۳. از فایروال‌ها به صورت لایه‌ای استفاده شود، استفاده از فایروال‌ها به شکل لایه‌ای و به کارگیری فایروال‌های مختلف سبب می‌شود تا درصورت وجود یک اشکال امنیتی در یک فایروال، کل شبکه به مخاطره نیفتاده و امکان استفاده از کدهای جاسوسی و خرابکارانه نیز به حداقل برسد.
۴. امکان استفاده از تهدیدات مربوط به استراق سمع که طی آن دشمن می‌تواند بدون اطلاع طرفین، اطلاعات و پیام‌ها را شنود کند، به حداقل برسد. استفاده از فضاهای امن در قسمت‌های passive و active می‌تواند به این مساله کمک کند.
۵. حملات مرتبط با تحلیل ترافیک که طی آن بر اساس یک سری بسته‌های اطلاعاتی، مهاجم می‌تواند ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب کند، شناسایی شود. این حملات از نوع غیر فعال است و اکثراً توسط کاربران خارجی صورت می‌گیرد.
۶. امکان دستکاری پیام‌ها و داده‌ها که بر اساس آن مهاجم می‌تواند جامعیت و صحت اطلاعات را با تغییرات غیر مجاز برهم زند از بین برود. این نوع حملات نیز توسط کاربران خارجی صورت می‌گیرد. همچنین امکان جعل هویت که طی آن مهاجم هویت یک فرد مجاز شبکه را جعل می‌کند به حداقل میزان ممکن برسد.
۷. امنیت ارتباطات که در آن با استفاده از فایروال‌ها، سیستم‌های ضد ویروس، سرورهای کنترل دسترسی و احراز هویت، نرم افزارهای مانیتورینگ، ثبت و تحلیل رویدادها می‌توان به تشخیص هویت و کنترل کاربران پرداخت، به وجود می‌آید.
۸. امنیت سیستم‌ها که در آن با بهره گیری از پویشگرهای امنیتی، آنتی ویروسها، IDS[1] وIPS[2] به ثبت و کنترل دسترسی کاربران به منابع پرداخته می‌شود، لحاظ شود.
۹. سطوحی از امنیت کاربردها به وجود آید که طی آن با بهره گیری از سیستمهای IDS، آنتی ویروس، پویشگر امنیتی و فیلترهای محتوا بر دسترسی کاربران نظارت می‌شود.
۱۰. از مدل‌هایی از مسیریاب‌ها استفاده شود که سیاست‌های امنیتی در قبال کلاینت‌ها در آنها کاملا رعایت شده است و همچنین در مسیریابها، سعی شود که تهدیدها شناسایی شده و از دسترسی شبکه‌های ناشناس جلوگیری گردد.
۱۱. از دیواره‌های آتش[3] برای رسیدن به امنیت برای کاربران استفاده شود که این امر در بسیاری از مسیریابها تعبیه شده است.
۱۲. ایجاد مکانیزم تولید و تغییر کلید رمز کننده اطلاعات[4] داخل مسیریابها برای بالابردن ضریب ایمنی لحاظ شود و همچنین تشخیص و شناسایی حملات خطرناک از طریق پست الکترونیکی و سایر روشها مورد نظر قرار گیرد.

1 Intrusion Detection System
2 Intrusion Prevention System
3 Firewall
4 IKE: Internet Key Exchange

فصل دهم:

ملاحظات پدافند غیرعامل در برقراری امنیت فیزیکی و کنترل دسترسی

۱۰-۱- مقدمه

اینکه نیروی انسانی فارغ از مسائل و مشکلات روزمره، چگونه ساعت‌ها در یک جای ثابت، با هوشمندی کامل نسبت به مراقبت از مواضع و یا منطقه تحت حفاظت خود اقدام نماید، جای تأمل و بررسی دارد. سامانه‌های حفاظت و نظارت الکترونیکی، درصورتیکه بطور صحیح طراحی و پیاده‌سازی شوند علاوه بر آنکه خیلی از آسیب‌ها را به حداقل می‌رسانند، به حداقل سرویس‌دهی و نگهداری نیاز دارند.

۱۰-۲- تجهیزات امنیت فیزیکی و کنترل دسترسی

تجهیزات امنیت فیزیکی و کنترل دسترسی شامل سامانه‌های دوربین مدار بسته، حفاظت پیرامونی، کنترل تردد و اعلام و اطفای حریق می‌باشد.

۱۰-۲-۱- سامانه دوربین مدار بسته

این سامانه، مجموعه‌ایست که به تصویربرداری توسط دوربین‌های ویدئویی و انتقال تصاویر برای نمایش محدود می‌پردازد. تهیه تصاویر مداربسته ممکن است اهداف اصلی زیر را دنبال کند[۳۵]:

- حفاظت، حراست و ایمنی
- کنترل، مدیریت و نظارت
- آموزش و تحقیقات

امروزه از این سامانه برای حفاظت و نظارت بر اماکن مهم، پرتردد و یا پرخطر استفاده می‌شود. با بکارگیری این سامانه، امکان شناسایی و ردیابی آسان فراهم می‌گردد. سامانه دوربین مداربسته از بخش‌های ذیل تشکیل شده است[۳۵]:

- ایجاد تصویر دوربین
- بستر انتقال تصویر
- نمایش تصاویر
- کنترل و ذخیره‌سازی تصاویر

۱۰-۲-۲- سامانه حفاظت پیرامونی

روش‌های حفاظت از پیرامون به دو دسته حفاظت فیزیکی و استفاده از سامانه‌های هوشمند الکترونیکی تقسیم می‌شوند[۳۶]:

۱. حفاظت فیزیکی

جهت ایجاد حفاظت فیزیکی متناسب با استانداردهای جهانی، نیاز به موانع اولیه‌ای به شرح ذیل می‌باشد:

- مصنوعی (حصار، برج مراقبت و...)
- انسانی
- حیوانی (سگ‌های نگهبان)
- عامل (مکانیکی، الکتریکی، الکترونیکی)
- کنترل‌ها و بازدیدها (درب‌های ورود،خروج و بازدیدها)

۲. سامانه‌های هوشمند الکترونیکی

این سامانه‌ها را به جهت نوع کاربری به دو دسته زیر می‌توان تقسیم کرد:

- محیط داخل

این سامانه‌ها برای شناسایی هر گونه نفوذ به داخل ساختمان یا ناحیه مشخصی از ساختمان به کار می‌روند.

- محیط خارج

این سامانه‌ها برای تشخیص نفوذ به پیرامون یک مجموعه بکار می‌روند. غالبا در فضای آزاد مانند حصار و یا اطراف ساختمآن‌های بزرگ نصب می‌گردند.

۱۰-۲-۳- سامانه‌های کنترل، بازرسی و شناسایی

این سامانه‌ها، به منظور مدیریت دسترسی و تردد انسانی (و خودرو) در مناطق تحت حفاظت و نیز مدیریت هشدارهای متناظر با رخداد حوادث به کار گرفته می‌شوند. سامانه‌های کنترل تردد را می‌توان به دو گروه طبقه‌بندی کرد:

۱. سامانه‌های کنترل تردد نفر

این سامانه‌ها با توجه به روش دریافت و قرائت اطلاعات که منتج از میزان امنیت مورد نیاز می‌باشد به سه گروه ذیل تقسیم می‌گردد:

- روش‌های غیرزیستی: دراین روش‌ها، جهت دریافت اطلاعات و شناسایی افراد از کارت‌های کنترل تردد، فناوری RFID یا کلمه رمز و PIN استفاده می‌گردد.
- روش‌های زیستی: در این روش‌ها، جهت دریافت اطلاعات و شناسایی افراد از مشخصات فیزیولوژیکی (اثر انگشت، چهره، شبکیه چشم، قرنیه، گوش، دما نگاشت دست یا صورت، شکل دست، سیاهرگ دست) یا رفتاری (امضاء و صوت) افراد استفاده می‌گردد.
- روش‌های ترکیبی: در این روش‌ها، از ترکیب دو یا چند روش زیستی، غیرزیستی و یا تلفیقی از سامانه‌های زیستی و غیرزیستی به منظور حصول ایمنی بیشتر استفاده می‌گردد.

۲. سامانه‌های کنترل تردد خودرو

نحوه عملکرد این سامانه‌ها به این شکل است که وسیله نقلیه از مسیرهای ویژه و گیت‌های مخصوص، عبور نموده و پس از تعیین هویت خودرو بر حسب اینکه مجاز به ورود است یا خیر، اجازه ورود به آن داده می‌شود و یا از تردد آن جلوگیری می‌گردد. تکنیک‌های متفاوتی برای پیاده‌سازی سامانه کنترل تردد خودرو وجود دارد که مهمترین آن‌ها عبارتست از[۳۷]:

- سامانه‌های قرائت اطلاعات شناسایی خودرو با استفاده از امواج رادیویی
- سامانه‌های قرائت اطلاعات شناسایی خودرو با استفاده از مادون قرمز

همچنین در برخی موارد استفاده از سامانه‌های مشابه کنترل تردد نفر نیز مرسوم می‌باشد، که در این روش مشخصات خودرو روی کارت تردد آن ثبت می‌گردد.

۱۰-۲-۴- سامانه‌های اعلام و اطفاء حریق

سامانه‌های اعلام و اطفاء حریق خودکار، سرمایه و اطلاعات باارزش و جان پرسنل را از گزند صدمات آتش‌سوزی دور نگه خواهد داشت. این سامانه‌ها مبتنی بر تشخیص دود، حرارت، نشت گاز و شعله توسط آشکارسازهای متناسب با آن و اعلام خطر خودکار توسط دستگاه‌های مرکزی است.

۱۰-۳- ملاحظات پدافند غیرعامل در امنیت فیزیکی و کنترل دسترسی

امنیت فیزیکی در محیط فناوری اطلاعات و ارتباطات در سه بعد امنیت فیزیکی داده‌ها و اطلاعات، امنیت فیزیکی شبکه و ارتباطات و امنیت فیزیکی سخت‌افزارها و تجهیزات قابل بررسی است. در ادامه توضیحات مختصری از هرکدام از این ابعاد به همراه ملاحظات مربوطه بیان خواهد گردید[۳۸].

۱۰-۳-۱- امنیت فیزیکی داده‌ها و اطلاعات

ارتباط مستقیمی بین میزان امنیت فیزیکی و امنیت داده‌ها و اطلاعات وجود دارد. در حقیقت، هدف بسیاری از حملات و خرابکاری‌های فیزیکی در سامانه‌ها، کارگزارها و شبکه‌ها، نفوذ و دسترسی به اطلاعات و داده‌های حساس سازمان‌ها می‌باشد.

اهم حوزه‌های امنیت فیزیکی داده‌ها و اطلاعات به شرح ذیل می‌باشد:

- محفظه‌ها/مخازن داده

اطلاعات طبقه‌بندی شده و محرمانه و نیز سامانه‌های اطلاعاتی حساس باید در محفظه‌ها و اتاق‌هایی نگهداری شوند که دسترسی به آن‌ها محدود بوده و محیط پیرامون آن‌ها نیز دارای حفاظ‌های امنیتی مناسبی باشد. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

۱. ورود به اتاق‌های کارگزارها و مخازن داده‌ها و اطلاعات می‌بایست منوط به اخذ مجوزهای مشخص باشد.
۲. تا حد امکان نباید اطلاعات مهم در رایانه‌های شخصی نگهداری شوند.
۳. این اطلاعات حتی‌الامکان می‌بایست در رسانه‌های فقط خواندنی ذخیره گردند.
۴. محفظه‌ها/ مخازن اطلاعات می‌بایست از نزدیکی به مواد و تجهیزات پرخطر در امان باشند.
۵. لازم است اعمالی چون خوردن، نوشیدن، سیگار کشیدن و نظایر آن در مجاورت و درون محفظه‌ها و اتاق‌هایی که حاوی اطلاعات و تجهیزات اطلاعاتی هستند، ممنوع گردد.

- کلیدهای محفظه‌ها/مخازن امنیتی

در این بخش منظور از کلید انواع کلیدهای مکانیکی، شماره شناسایی خصوصی، کارت‌های دسترسی و یا ترکیبی از دو یا چند مورد فوق می‌باشد. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:
کلیدهای محفظه‌ها/ مخازن امنیتی باید با توجه به بالاترین درجه حساسیت اطلاعات و یا تجهیزاتی که توسط آن قابل دسترسی هستند، محافظت شوند. کلیدهای محفظه‌ها/ مخازن امنیتی باید زمانی که یکی از موارد زیر محقق شد، تغییرکنند:

- شواهدی از حمله و یا نفوذ رؤیت شود.
- تهدیدات و خطرات غیرقابل قبولی مشاهده شود.
- فردی که به این مکان‌ها دسترسی داشته است، تغییر کند.

۱۰-۳-۲- داده‌های در حال تبادل

شنود و یا استراق سمع الکترونیکی یکی از هوشمندانه‌ترین راه‌های سرقت داده‌های در حال تبادل محسوب می‌شود. امروزه مهاجمین با کمترین تجهیزات ممکن نیز قادر به شنود و رونوشت تمامی فعالیت‌های انجام شده روی کامپیوتر قربانی هستند؛ نظیر ثبت تمامی کلیدهایی که بر روی صفحه کلید فشار داده می‌شوند، تمامی اطلاعاتی که روی یک مانیتور نمایش داده می‌شوند و تمامی فایل‌هایی که برای چاپگر ارسال می‌شوند. انواع روش‌های شنود و محافظت در مقابل آن‌ها به شرح ذیل می‌باشد[۳۹]:

- شنود از طریق کابل‌ها و سیم‌ها

سیم‌ها و کابل‌های الکتریکی، به خاطر نوع عملکردشان، جزء اولین گزینه‌های انتخابی مهاجمین برای استراق سمع می‌باشند. مهاجم به راحتی می‌تواند مکالمه‌ای را که بین یک جفت سیم در حال انجام است با یک پیوند ساده دنبال کند. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:
به طور منظم تمامی سیم‌هایی که داده‌ها را حمل می‌کنند جهت یافتن آسیب‌های فیزیکی، بازرسی شوند.
با استفاده از کابل‌های حفاظدار، از امکان نظارت غیرمجاز سیم‌ها کاسته شود.

- شنود از طریق اترنت

از آنجایی‌که مهاجمین به طور گسترده‌ای از اترنت و سایر شبکه‌های محلی، برای استراق سمع استفاده می‌کنند، می‌بایست اطمینان حاصل شود که سامانه‌ها، زیرشبکه‌ها و شبکه‌هایی که استفاده نمی‌شوند، دارای پورت‌های کابل‌های دوسویه فعال و یا اترنت در درونشان نیستند. تمامی آدرس‌های IP که در شبکه‌ها مشخص شده‌اند به صورت دوره‌ای بررسی شوند تا اطمینان حاصل گردد میزبان غیرمجازی از طریق اینترنت در شبکه فعالیت نداشته است. از نرم‌افزارهای مانیتورینگ LAN استفاده شود، تا به محض تشخیص یک بسته که از یک آدرس ناشناخته استفاده می‌کند، هشدارهای صوتی خود را فعال کند.

- شنود از طریق پورت‌های کمکی روی ترمینال‌ها

بسیاری از ترمینال‌های کامپیوتری مجهز به یک پورت چاپگر جهت استفاده و یک پورت برای چاپگر کمکی هستند. اگر مهاجمی بتواند یک ارتباط با پورت‌های چاپگر برقرار کند، می‌تواند از این پورت‌ها برای شنود استفاده کند. اگر از پرینتر کمکی استفاده می‌شود اطمینان حاصل شود که کابل‌های دیگری به پورت چاپگر ترمینال متصل نیستند.

۱۰-۳-۳- پشتیبان داده‌ها

حفاظت فیزیکی یک پشتیبان، به اندازه حفاظت فیزیکی یک کارگزار و یا سامانه اطلاعاتی اهمیت دارد؛ زیرا در صورت خرابی، یا به سرقت رفتن پشتیبان، بخش اعظمی از اطلاعات، نابود یا به سرقت می‌رود. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

- پشتیبان‌ها در مکان‌هایی که توسط عموم قابل دسترسی هستند، قرار داده نشوند.
- پشتیبان‌ها ونسخه‌های اصلی می‌بایست در مکان‌های جداگانه نگهداری شوند.
- تمامی رسانه‌های ذخیره‌سازی می‌بایست به صورت «غیرقابل نوشتن » ذخیره شوند.
- بمنظور حفاظت از اطلاعات نسخه‌های پشتیبان، می‌بایست از قفل‌های سخت‌افزاری و نرم‌افزاری استفاده شود. قبل از دورانداختن رسانه‌های ذخیره‌سازی، اطمینان حاصل شود که داده‌های موجود بر روی آن‌ها کاملاً پاک شده‌اند. یکی از مطمئن‌ترین راه‌های امحاء رسانه‌های ذخیره‌سازی تخریب فیزیکی می‌باشد.

۱۰-۳-۴- رسانه‌های غیرالکترونیکی

رسانه‌های دیجیتالی، تنها منابع ذخیره‌سازی داده‌ها نیستند که باید قبل از دور انداختن پاکسازی کامل شوند، بلکه رسانه‌های دیگری نیز وجود دارند که ممکن است حاوی اطلاعات مهمی برای مهاجمین و قفل‌شکن‌ها باشند؛ از جمله این رسانه‌ها می‌توان به نتیجه چاپی نرم‌افزارها، یادداشت‌ها، مستندات طراحی، کدهای مقدماتی، مستندات برنامه‌ریزی، خبرنامه‌های داخلی، دفترچه‌های تلفن و یادداشت شرکت، راهنمای کاربر و نظایر آن اشاره کرد. برای نمونه اگر مستند چاپ شده طراحی و معماری شبکه در دسترس باشد یک مهاجم می‌تواند با دسترسی به آن از کارگزارها، لینک‌ها و سامانه‌های مختلف مطلع شده، نقاط ضعف توپولوژی را یافته و از آن استفاده نماید. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

- رسانه‌ها می‌بایست در مکان‌های امن نگهداری شوند.
- می‌بایست به کاربران آموزش داده شودکه اطلاعات حساس را بدون رعایت موارد امنیتی به هیچ عنوان در معرض نمایش نگذارند و یا دور نیندازند.

۱۰-۴-۵- امنیت فیزیکی شبکه و ارتباطات

شبکه، دارای منابعی فیزیکی همچون سامانه‌ها، دستگاه‌های شبکه (مسیریاب، سوئیچ، دیوارآتش، هاب و...)، اتاق کارگزار و تجهیزات آن، تجهیزات ذخیره‌سازی و نظایر آن می‌باشد. شبکه، نحوه ارتباط منابع را با یکدیگر مشخص می‌کند. به عبارت دیگر لینک‌های جریان داده را بین این عناصر مشخص می‌کند.
بنابراین امنیت فیزیکی یک شبکه در بردارنده امنیت موارد زیر است:

- منابع فیزیکی موجود در شبکه
- نحوه ارتباط‌دهی منابع فیزیکی (توپولوژی فیزیکی شبکه)
- لینک‌های موجود بین منابع فیزیکی (کابل‌کشی)
- محیط شبکه (مرز شبکه با بیرون نظیر ارتباطات اینترنت، شبکه محلی، شبکه مجازی خصوصی، برنامه‌های کاربردی و ...)
- دستگاه‌های ایمنی شبکه (مسیریاب، دیوار آتش)

مهمترین اصل در امن‌سازی منابع فیزیکی موجود در شبکه آن است که دسترسی فیزیکی به این منابع محدود و کنترل شود. بسیاری از روش‌های حفاظتی که روی یک شبکه و یا سامانه اعمال

می‌شود، توسط نرم‌افزارها فراهم می‌گردد، ولی اگر یک مهاجم (داخلی یا خارجی) موفق شود به صورت فیزیکی به یک کامپیوتر و یا شبکه دسترسی پیدا کند، امکان محدود کردن فعالیت‌ها و نفوذهای بعدی وی به شبکه داخلی و محرمانه سازمان، بسیار مشکل خواهد شد. برخی از خطراتی که از جانب مهاجمین، سازمان را تهدید می‌کنند عبارتند از[۴۰]:

- ورود و خروج غیرمجاز
- نظارت و کنترل از راه دور
- دسترسی غیرمجاز به کامپیوترها و سرورها و منابع اطلاعاتی حساس
- سرقت داده‌ها، اطلاعات و تجهیزات
- نصب سخت‌افزارها و یا نرم‌افزارهای استراق سمع
- تخریب و یا دستکاری ساختارها و کابل‌های ارتباطی
- سرقت کامپیوترها، سرورها و سایر عناصر شبکه
- نصب برنامه‌های مخرب، ویروس‌ها و کرم‌ها

پس از دسترسی به اطلاعات و منابع اطلاعاتی وضعیت به مراتب دشوارتر خواهد شد. مهاجمین قادرند اطلاعات را تغییر دهند، پاک کنند، یا اینکه اطلاعات بدست آمده را به رقبا و یا دشمنان بفروشند، آن‌ها را در اینترنت پخش کنند و سازمان‌ها را از این ناحیه متحمل خسارات فراوانی نمایند. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

- دسترسی به شبکه داخلی از نواحی پذیرش عمومی و سایر نواحی بایستی محدود شود.
- جهت ورود به اتاق کارگزار و به طور کلی مکان‌های امن می‌بایست از کارت‌های شناسایی استفاده گردد.
- اتاق کارگزار می‌بایست به تجهیزات نظارت ویدئویی و همچنین UPS مجهز گردد.
- حدالمقدور از پنجره‌ها در مراکز داده استفاده نشود.
- لازم است در اطراف سامانه‌های مهم نظیر کارگزارها، حفاظ‌های مناسب تعبیه گردد.
- کابل‌ها در زیرزمین جاسازی شده و با پوشش‌های حفاظتی مقاوم شوند.
- مانیتورها و صفحه کلیدها در فواصل دوری از پنجره‌ها و درب‌ها و دریچه‌ها قرار داده شوند.
- کابل‌های شبکه از سامانه‌های استراق سمع حفاظت شوند.
- صفحه نمایش، میزکار و حتی تابلوهای اتاق کنفرانس پس از اتمام کار پاک گردند.
- درایوهای فلاپی دیسک و CD-ROM از روی سامانه‌های مهم حذف گردند.

سطح امنیتی مطلوب برای Rack انتخاب گردد. در کمترین سطح امنیتی، Rackها صرفاً چارچوب‌هایی هستند که سرورها را نگهداری می‌کنند و هیچ نوع حفاظت دیگری برای تجهیزات ایجاد نمی‌کنند. در حالت متوسط امنیتی، Rackها ازچهار طرف دارای دیواره‌هایی هستند که محتویات درون آن را نمایش می‌دهد. ولی در سطوح امنیتی بالاتر، Rackها به طور کامل از چهار طرف توسط درها یا دیواره‌هایی حفاظت می‌شوند که هرکدام از این چهار طرف قفل مخصوص به خود دارد.

۱۰-۳-۶- امنیت فیزیکی تجهیزات/سخت‌افزار

در این بخش سعی شده است محدوده دید کوچکتر شده و امنیت سامانه‌های رایانه‌ای و سخت‌افزارهای مربوط به آن‌ها مورد توجه قرار گیرد. نکته مهم اینست که تجهیزات و سامانه‌های اطلاعاتی مهم و با ارزش (نظیر کارگزارها، تجهیزات اطلاعاتی دارای طبقه‌بندی، نمونه‌ها و مدل‌های مهندسی، اطلاعات مالی، سیاسی، نظامی و ...) باید در مکان‌های ایمن نگهداری شوند.

۱۰-۴- بمب الکترومغناطیسی

این بمب در اصل یک موج ضربه‌ای الکترومغناطیس است که یک میدان مغناطیسی بسیار قوی ایجاد می‌کند، این میدان مغناطیسی به نوبه خود، میدان الکتریکی با قدرت هزاران ولت بر متر به صورت ناپایدار در هادی‌های الکترونیک ایجاد کرده و با وارد شدن به یک دستگاه هادی جریان برق، این دستگاه را با توجه به میزان مقاومت آن بدون هیچ‌گونه سر و صدا یا بر جای ماندن نشانه‌ای منهدم کرده و یا به آن آسیب می‌رساند. شناسایی عوامل حملات الکترومغناطیس بسیار دشوار می‌باشد. از این روش می‌توان برای نابود کردن و ایجاد اختلال در تجهیزات الکتریکی و الکترونیکی بویژه رایانه‌ها، تجهیزات ارتباطی، رادیو یا گیرنده‌های رادار استفاده کرد[۳۸].

اقدامات حفاظتی در برابر موج الکترومغناطیسی بر پایه جلوگیری از ورود، انتشار و انعکاس انرژی استوار است. بر این اساس، انرژی از قطعات، تجهیزات و ادوات، دور نگه داشته می‌شود. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است:

- از پوشش و موانع فلزی کافی در اطراف ادوات و تجهیزات (شیلد الکترومغناطیسی) استفاده شود.
- جلوگیری کننده‌های سریع جریان در خطوط تغذیه، سیگنال و خطوط کنترلی نصب گردد.

- اتصال بین دیواره و جلوگیری کننده‌های سریع جریان و ارتباط این دو به زمین با امپدانس پایین ایجاد گردد و علاوه بر آن نقاط ورودی و محل اتصالات کنترل شود.
- هیچگاه برای شبکه از کابل‌های مسی بر روی زمین (به خصوص در بیرون ساختمان) استفاده نشود مگر اینکه با یک عایق پوشانده شده باشند.
- از فیلترهای الکتریکی و کف پوش‌های ضدالکتریسیته استفاده شود.

۱۰-۵- عوامل محیطی مخرب

عملکرد صحیح سامانه‌های رایانه‌ای و سخت‌افزارهای مرتبط با آن‌ها، شرایط محیطی و فیزیکی خاصی را می‌طلبد. عواملی همچون انفجار، آتش، دود، رطوبت، ضربه، پارازیت الکتریکی، سیل و زلزله می‌تواند تأثیرات مخرب فراوانی در عملکرد و صحت تجهیزات، سامانه‌ها و اطلاعات داشته باشد. برخی از ملاحظات پدافند غیرعامل در این حوزه به شرح ذیل است[۴۰]:

- می‌بایست پوشش‌های مستحکمی جهت استفاده از تجهیزات و سامانه‌های مهم در نواحی پرخطر پیش‌بینی و تهیه گردد.
- لازم است در نزدیکی سامانه‌های مهم، تجهیزات اطفاء حریق نصب و به پرسنل آموزش‌های کاربری لازم ارائه شود.
- علاوه بر رایانه‌ها، کابل‌کشی ساختمان نیز می‌بایست در برابر آتش‌سوزی ایمن باشد.
- با توجه به مضرات دود برای سامانه‌های رایانه‌ای و این موضوع که در برخی مواقع دود علامت خطر آتش‌سوزی می‌باشد، می‌بایست سامانه‌های تشخیص دود در اتاق‌های حاوی تجهیزات مهم، نصب و راه‌اندازی گردد.
- هرگز نباید در اطراف مکان‌هایی که حاوی اطلاعات و سخت‌افزارهای حساس هستند، از درب‌ها و دیوارهای شیشه‌ای استفاده شود.
- رایانه‌ها نباید در مجاورت پنجره‌ها و یا در سطوح فوقانی اتاق‌ها قرارداده شوند.
- لازم است از جاسازی تجهیزات سنگین در مجاورت سامانه‌های رایانه‌ای جلوگیری شود.
- لازم است حسگرهای تشخیص رطوبت در کف اتاق کارگزار و سایت‌های رایانه استفاده شود. این سنسورها می‌بایست طوری تنظیم شوند که هنگام وجود رطوبت آسیب‌زننده به صورت خودکار جریان برق را قطع نمایند.

لازم است برای کارگزارها و سایر سامانه‌های اطلاعاتی مدار الکتریکی جداگانه‌ای به همراه یک محافظ الکتریکی در نظر گرفته شود تا از ایجاد پارازیت جلوگیری شود.

مراجع

۱. بنایی، سجاد. (زمستان ۱۳۸۹). مفاهیم کلان امنیت محیطی در حوزه فناوری اطلاعات و ارتباطات. تهران: سازمان فناوری اطلاعات ایران.

۲. جلالی، غلامرضا. (۱۳۸۹). روش و مدل براورد تهدیدات و پدافند غیرعامل. تهران: انتشارات دانشگاه امام حسین(ع).

۳. بنایی، سجاد؛ سهامی، سهیلا؛ مختار، سمیرا. (زمستان ۱۳۸۹). انواع حملات در فضای سایبر. تهران: سازمان فناوری اطلاعات ایران .

۴. خبرگذاری فارس. (زمستان ۱۳۸۹). فضای سایبر میدان اصلی تهاجم و دفاع. تهران: سازمان فناوری اطلاعات ایران.

۵. اسکندری، حمید؛ امیرصوفی، رحمت‌اله. (۱۳۹۱). تهدیدات فضای سایبر و مدیریت امنیت اطلاعات. تهران: بوستان حمید.

6. Janczewski. (2008). Cyber warfare and cyber terrorism. Newzealnad: Lech university of Auckland.

7. National Cyber Security Aliance. (2007). Top 8 cyber practices Texas A&M Research Foundation (2006). National security threat list. Retrieved from

۸. فغانی، محمدرضا؛ سعیدی، حسین؛ گلشنی، پیمان. (زمستان ۱۳۸۹). بررسی آسیب‌پذیری‌های وب. تهران: سازمان فناوری اطلاعات ایران.

۹. مرکز پدافند غیرعامل فاوا. (زمستان ۱۳۸۹). مرکز عملیات امنیت. چهارمین کنفرانس ملی C41.

۱۰. مرکز پدافند غیرعامل فاوا. (پاییز ۱۳۸۹). مقدمه‌ای بر ضرورت و چگونگی آموزش و فرهنگ‌سازی در حوزه‌ی امنیت ICT. تهران: شرکت مخابرات ایران.

11. Kellerman, McNevin. (2008). Electronics security:Rist Mitigation in Financial Transaction.

12. The National Strategy to secure Cyberspace[U.S] http://www.dhs.gov/interweb/assetlibrar

۱۳. مرکز پدافند غیرعامل فاوا. (زمستان ۱۳۸۹).پنهان نگاری و تحلیل پنهان نگاری. تهران: سازمان فناوری اطلاعات ایران .

۱۴. مرکز پدافند غیرعامل فاوا. (زمستان ۱۳۸۹). دیواره آتش. تهران: سازمان فناوری اطلاعات ایران.

15. Sadowsky, George; X.Dempsey, James; Greenberg, Alan; j.Mack, Barbara. (2003). IT Security Handbook; infoDev, Worldbank.

16. http://frweb.tamu.edu/security/SECGUI1DT Eh/rTe amstl.htm#National%20Security

۱۷. عبداللهی، محمد. طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری. پایان‌نامه کارشناسی ارشد. دانشگاه صنعتی شریف.

۱۸. سایت مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (certcc)

۱۹. علمداری، شهرام. (۱۳۸۷). دستورالعمل براورد تهدید و تدوین سناریو. تهران: سازمان پدافند غیرعامل.

۲۰. سازمان فناوری اطلاعات ایران. (تیر ۱۳۹۰). مرکز مدیریت و توسعه و اعتبار بخشی، توصیه‌نامه‌های امنیت اطلاعات: کد سند R90040107 و کد سند:R9003105. تهران: سازمان فناوری اطلاعات ایران .

۲۱. پورمند، علی. استانداردی برای امنیت اطلاعات www.imi.ir/tadbir

۲۲. جعفری، نیما. سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح. ماهنامه‌ی تدبیر. شماره ۱۸۹.

۲۳. مرکز پدافند غیرعامل فاوا. (پاییز ۱۳۸۹). مقدمه‌ای برپدافند غیرعامل در حوزه‌ی شبکه‌ی ارتباطات ثابت. تهران: سازمان فناوری اطلاعات ایران.

24. Andrea Goldsmith. Wireless communications. Cambridge University Press. 2005. p. 1.

25. Ke-Lin Du, M. N. S. Swamy. Wireless Communication Systems: From RF Subsystems to 4G Enabling Technologies. Cambridge University Press ،2010. p. 1-2.

26. David Tse, Pramod Viswanath. Fundamentals of Wireless Communication. Cambridge University Press ،2005. pp. 1-3.

27. Joshua S. Gans, Stephen P. King and Julian Wright. Handbook of Telecommunications Economics, Volume 2: Technology Evolution and the Internet, ch. 7. North Holland ،2006. p. 243-244.

28. David Tse, Pramod Viswanath. Fundamentals of Wireless Communication. Cambridge University Press ،2005. p. 4.

29. Sasha Dekleva, J. P. Shim, Upkar Varshney, Geoffrey Knoerzer. Evolution and emerging issues in mobile wireless networks. . Communications of the ACM (ACM) Vol. 50, No. 6 (2007): 38-43.

۳۰. گرین، پاول. (۱۳۸۸). فیبر نوری، فناوری فیبر تا منازل (FTTH). مترجم جمال صوفیه. تهران: انتشارات یزدا.

31. F. S. Ferreira, Mário. Nonlinear effects in optical fibers: limitations and benefits. Department of Physics, University of Aveiro, 3810-193 Aveiro, Portugal.

۳۲. نامخواه، ناصر. (پاییز ۱۳۸۹). اینترنت و نظام سلطه. تهران: شرکت مخابرات ایران.

۳۳. سعدی، حمیدرضا. (پاییز ۱۳۸۹). نیمه پنهان. تهران: شرکت مخابرات ایران.

34. Defense Advanced Research Projects Agency. Retrieved 2007-05-21

۳۵. مشهدی، حسن. (۱۳۹۰). الگوی ارزیابی تهدیدات، آسیب‌پذیری و آنالیز ریسک زیرساخت‌های حیاتی. تهران: مجتمع پدافند غیرعامل دانشگاه مالک اشتر.

۳۶. نامخواه، ناصر. (زمستان ۱۳۸۹). امنیت سخت افزاری در رایانه‌های شخصی. تهران: سازمان فناوری اطلاعات ایران.

۳۷. عبدا...خانی، علی. (۱۳۸۶). تهدیدات امنیت ملی. تهران: انتشارات بین‌المللی ابرار معاصر تهران.

۳۸. افتخاری، اصغر. (۱۳۸۵) . کالبد شکافی تهدید. تهران: انتشارات مرکز مطالعات دفاعی و امنیت ملی دانشکده فرماندهی و ستاد.

۳۹. مرادیان، محسن. (۱۳۸۵). درامدی بر ابعاد و مظاهر تهدیدات. تهران: انتشارات مرکز آموزش و پژوهش شهید سپهبد صیاد شیرازی.

۴۰. سالیوانت، جان. (۱۳۸۹). حفاظت راهبردی از زیرساخت‌های حیاتی. مترجم محمد ابراهیم‌نژاد. تهران: انتشارات بوستان حمید.

Abstract:

In the present era which is called the age of communication and information technology, communities have realized the importance of ICT as a means to develop and increase productivity in all areas. Rapid and unbalanced growth of the ICT caused that this area has become potentially vulnerable and insecure parts of the world. Therefore, in order to protect this field from the existing threats and also protecting national security and privacy of citizens in today's international conflict considering and addressing passive defense in the field of communications and information technology is an inevitable fact.

Indeed, the passive defense refers to a set of strategies and plans which do not require the use of weapons and its implementation can prevent damages. In other words, passive defense not only increases the defense power in times of crisis but also reduce the disaster consequences and it is possible to restore damaged areas with lowest cost. In fact, passive defense plans are prepared and implemented in peacetime. So given the opportunity in time of peace to provide plans, this topic should examined.

keywords: passive defense, communication and information technology, Internet and cyberic space.

Ministry of Communication and Information Technology

ICT of Chahar Mahal va Bakhtiari

Title:

Considerations of Passive Defense

In

Communication and Information Technology

(Ver.2)

By: Behrouz Banitalebi

Oct. 2014