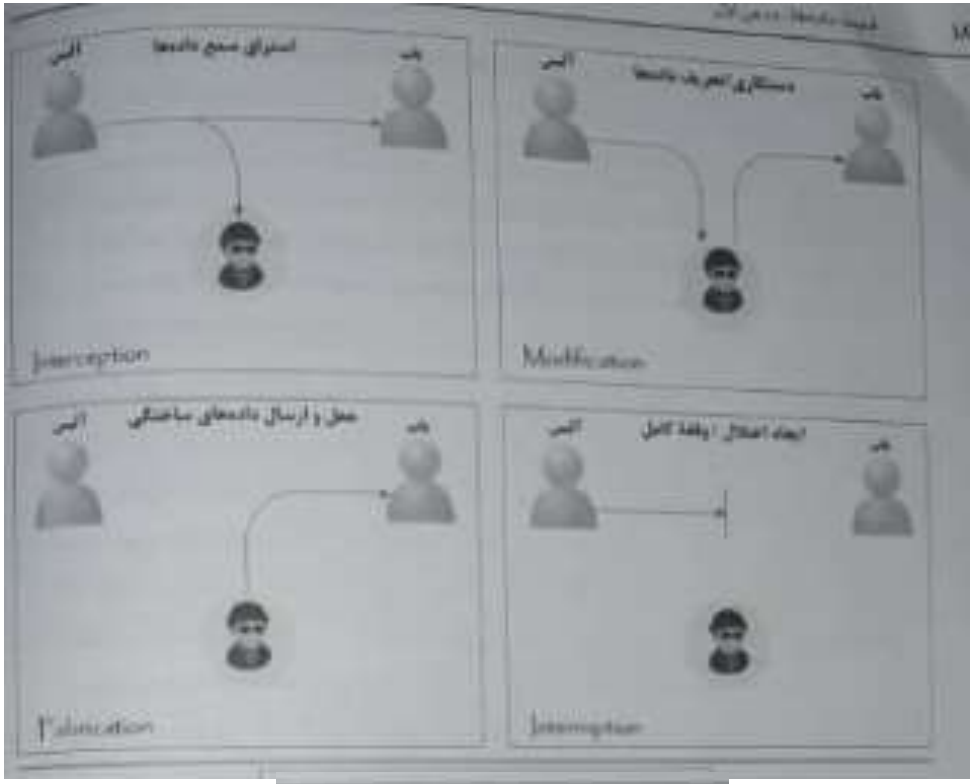


شکل1-2انواع حملات در مقابل کانال امن

هرگاه درابتدای متن منظور عام از موجودیت یاد کردیم مضمون این واژه به یکی از عوامل زیر اشاره دارد:
1)کاربران اعم از کاربران معمولی مدیران شبکه کاربران میهمان مشتریان محلی یا راه دور
2)ایستگاه ها مثل ماشین های کاربری سرویس دهنده ها و ترمینال ها
3)روازه ها شامل تجهیزاتی مثل مسیر یاب سوئیچ و پراکسی
4)سرویس دهنده های امنیتی شامل ایستگاه های مدیریت.مراکز نگهداری از کلمات عبور وکلید های رمز و نظائر ان ها

تمهیدات امنیتی در هر شبکه بایستی در سه مورد زیر مشخص شده باشند:
1)تمهیدات پیشگیری از وقوع حمله
2)تمهیدات کشف حمله(در صورت وقوع)
3)تمهیدات بازیابی و خروج از بحران پس از وقوع حمله دقت داشته باشید که تمهیدات پیشگیرانه هرگز تضمین کننده عدم وقوع حمله نیستند.

حملاتی که علیه منابع موجود یت های یک شبکه شکل می گیرند به دو رده کلی تر((حملات فعال))و ((حملات غیر فعال))تقسیم بندی می شوند.حملات فعال انهایی هستند که به محض شروع علائم اشکاری از خود بروز می دهند و کشف انها امکان پذیر است.به عنوان مثال حمله ی نوع ((وقفه))یا از کار افتادن یک سرویس در شبکه خود را نشان خواهد داد.حمله نوع ((دستکاری پیام)) یا((جعل پیام)) با توسل به مکانیزم های خاص قابل کشف است و در رده ی حملات فعال دسته بندی می شوند.میزان ((اسیب)) به منابع و موجودیت های شبکه در حمله فعال به قدرت سیستم های اشکار سازی حمله و واکنش سریع انها بستگی دارد.
((حملات غیر فعال))هیچ علامت اشکاری در شبکه از خود نشان نمی دهد و ممکن است برای ساعت ها و هفته ها باقی بمانند.حمله ی نوع((استراق سمع))از این دسته از حملات محسوب می شود و یک اخلال گر می تواند مدت های طولانی به شنود داده ها مشغول و از آنها به نفع خود بهره برداری کند.در حالی که هیچ ابزار تشخیصی قادر ببه کشف چنین حمله خاموشی نباشد.حملات غیر فعال بسیار خطرناک و موجب((آسیب))بسیار زیاد به موجودیت های شبکه هستند.برای پیشگیری از چنین حملاتی باید بین طرفین یک ارتباط کانالی امن ایجاد کرد.(حملات غیر فعال را می توان به تومور های پنهان تشبیه کنید که هیچ علائمی از خود نشان نمی دهند و عموما زمانی خود را نشان می دهند که کار از کار گذشته است.!

فرض کنید که بین هر دو موجودیت در شبکه یک کانال امن ایجاد و داده ها به نحوی رمز نگاری شوند که استراق سمع آنها هیچ ارزشی برای افراد غیر مجاز نداشته باشد و هیچ حمله ای طرفین ارتباط را تهدید نکند.آیا شنود داده هایی که از لحاظ محتوایی هیچ ارزشی ندارند برای یک بیگانه آشکار کننده هیچ اطلاعاتی نیست!فرض کنید یک اخلال گر به صورت خاموش و مستمر جریان تبادل اطلاعات بین دونقطه آ و ب در شبکه را استراق سمع کرده و متوجه می شودحجم تبادل پیام در ساعات10تا 12اولین شنبه ی هر ماه به ناگاه افزایش می یابد.آیا همین مشاهده نمی تواند بیانگر یک واقعیت و نمادی از یک رخدادجدید باشد!قطعا همین طور است و در اینجا حمله غیر فعال دیگری به نام ((حمله تحلیل ترافیک))مطرح می شود.((حمله تحلیل ترافیک عبارت است از:استراق سمع دنباله ی پیام های جاری بین دو نقطه از شبکه و استخراج شاخص های اماری این جریان به منظور آگاهی از نحوه ی تعامل طرفین ارتباط و تحرکات احتمالی آنها بدون آنکه محتوای پیام ها آشکار باشد.به عنوان مثال وقتی تعدادپیام هایی که بین نقطه آ که فرضا محل تجمع تروریست هاست و نقطه ب در پایتخت کشوری مفروض مبادله می شوند در یک مقطع زمان به ناگاه افزایش پیدا کند می توان نگران یک تحرک تروریستی بود!برخی از اخلال گران از این شاخص های آماری سوءاستفاده می کنند لذا برای جلوگیری از تحلیل ترافیک ضمن مراقبت های فیزیکی از کانال های انتقال باید توزیع ترافیک در طول زمان به گونه ای تنظیم شود که هیچ شاخص آماری مهمی از آن قابل استخراج نباشد.

چهارچوب دروس بعدی کتاب در توصیف سرویس های امنیتی

اولین گام در ارائهخدمات امنیتی و ایجاد کانال های امن استفاده از الگوریتم های رمز نگاری به معنای تبدیل پیام ها به دنباله ای نامفهوم از بیت ها است به نحوی که فقط و فقط گیرنده بتواند این دنباله ی نامفهوم را به شکل اصلی بازیابی کند.چنین الگوریتم هایی((سرویس محرمانه ماندن اطلاعات))را عرضه می کند و موضوع دروس 2تا 9این کتاب هستند.

درس دهم نیز به روش هایی می پردازد که بر اساس آن رمز شکن تلاش می کند تا دنباله ینامفهوم و رمز شده اطلاعات را بدون داشتن کلمه عبور (کلید رمز)به شکل اصلی برگرداند و از محتوای آن به نفع خود بهره بگیرد هرگاه چنین تلاشی به ثمر بشیند تمام سرویس های امنیتی در هم خواهد شکست!

دومین گام در ارائه خدمات امنیتی توسل به روش هایی است که گیرنده و فرستنده پیام بتوانند هویت یکدیگر و اصالت پیام و مکانیزم های احراز هویت تشریح خواهد شد.

سومین گام باید کاری کرد که نه فرستنده ی پیام بتواند ارسال پیام خود را منکر شود و نه گیرنده بتواند پیامی دروغین ساخته و ارسال آن را به کسی نسبت بدهند.این موضوع در درس دوازدهم بحث خواهد شد.

در چهارمین گام و برای پیشگیری از حمله ی وقفه باید تمهیداتی را اندیشید که بطور پراکنده در مابقی دروس بحث خواهند شد.

دروس چهاردهم و پانزدهم به پیاده سازی عملی خدمات امنیتی در معماری لایه ای شبکه می پردازد وپروتکل های مهمی را در این زمینه معرفی می کند.

در درس آخر روش های ایجاد اختلال و نفوذ در شبکه از طریق حفره های امنیتی را مرور خواهیم کرد و به حملات شناخته شده علیه پشته ی پروتکلی TCP/IP نگاهی خواهیم انداخت.

زیر ساخت امنیت اطلاعات

وقتی ساختمانی را برای افتتاح یک موزه یا طلا فروشی پایه ریزی می کنند از همان اولین کلنگ بایستی به امنیت آن فکر شده باشد وگرنه قفل و زنجیر هیچ سودی ندارد.دیوار های بتونی مسلح به فولاد.کف سازی.تعیین و مسدود کردن تمام کانال های احتمالی پیش نیاز های یک ساختمان امن هستند.

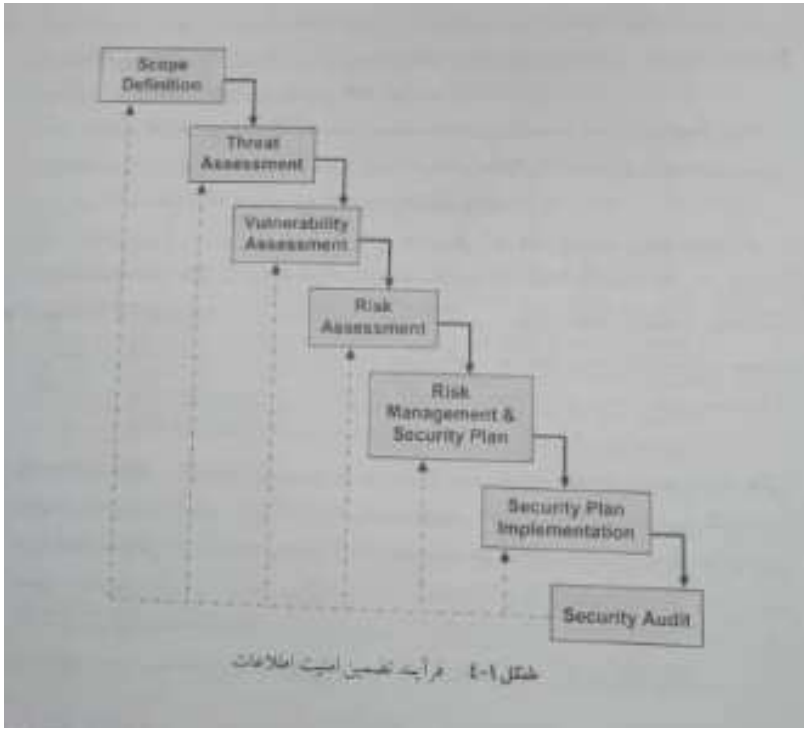
امنیت اطلاعات نیز از این مقوله مستثنی نیست.هرگاه قرار بر آن است که سرویسی در شبکه ارئه شود بایست ابتدا((تهدیدها))مشخص شده و((میزان خطر))براورد شود وسپس با تعیین حاشیه ی امنیت سرمایه گذاری لازم برای تمهیدات امنیتی محاسبه و بر اساس آن یک معماری متناسب پیش بینی شود.بدیهی است که امنیت در چندین سطح پیاده سازی و اعمال می شود.به همان اندازه که تشخیص هویت کاربران راه دور اهمیت دارد.جلوگیری از تردد افراد متفرقه به محل استقرار سرویس دهنده ها و حراست فیزیکی از آنها نیز مهم است.قدرتمند ترین روش رمز نگاری دنیا در مقابل کاربری که کلمه عبور خود را در دفترچه ی یادداشت خود در جایی گم کرده است زانو خواهد زد!لذا آموزش مدیران کارکنان و کاربران نیز به اندازه ی بهره گیری از سیستم های گران قیمت((کشف حمله))شایان توجه است.در شکل1-3الگویی از یک معماری امن برای اطلاعات ارائه شده است.

تمهیدات متناسب با برنامه های کاربردی	
مدیریت تمهیدها شامل تحلیل پیشگیری	
امنیت زیر ساخت شبکه	

طبق استاندارد های جهانی فرآیند تضمین امنیت اطلاعات در چندین فاز بدست می آید.شکل1-3این فرآیند را به تصویر کشیده است این فاز ها به ترتیب عبارت اند از:scape Definition

1)در این مرحله فهرست دقیقی از تمام عوامل انسانی و دست اندرکاران شبکه که به هرنحو در امنیت اطلاعات دخیل اند تهیه می شود.نباید فراموش کرد که در بسیاری از سازمان ها و موسسات اطلاعات مهم ترین دارایی آنهاست و عوامل متعددی باید در حفاظت و مراقبت از دارایی آن سازمان یا موسسه همکاری کنند.عواملی که باید فهرست دقیق آنها استخراج شود عبارتند از.تک تک کارمندان مدیران و مسئولین اجرایی سهام داران وسرمایه گذاران بیمه کنندگان یکایک مشتریان شرکای تجاری مصرف کنندگان(در صورت وجود)رقبا مراکز دولتی مرتبط کارآموزان احتمالی وهرکسی که به هرنحو از طریق شبکه(یعنی از راه دور)یا به صورت فیزیکی به منابع و تجهیزات شبکه دسترسی دارد باید در این فهرست به دقت تعیین شده spncadباشد.برای موسسات مالی و اعتباری یا مراکز تجارت الکترونیکی این فهرست می تواند بسیار طولانی باشد یاابزار های مناسب استفاده کرد. وبرای تهیه آن باید از نرم افزار های sbcet

تمام عواملی که به هرنحو با موسسه یا سازمان در ارتباطند ولی هیچ نیازی به دسترسی به منابع شبکه ندارند باید در استراتژی امنیتی کاملا از دسترسی فیزیکی یا دسترسی از راه دور دور نگه داشته شوند.پس از تعیین عوامل درگیر باید حوزه عملکرد آنها ونوع تعامل آنها با منابع شبکه مشخص شود در ضمن ماموریت سازمان و موسسه وتعهدات قانونی و یکایک عوامل و کارکنان باید مشخص گردد.



2) دراین مرحله باید تحلیل و براورد جامعی از طبیعت تهدید هایی که علیه منابع شبکه و اطلاعات وجود دارد و همچنین منشاء این تهدید ها و موقعیت این تهدیدها به عمل اید.
((طبیعت هر تهدید))می تواند بسیار متفاوت باشد:افشای اطلاعات حساس وسرمایه ای در اثر دسترسی اشخاص غیر مجاز تغییر مخفیانه در اطلاعات یا نابودی کامل اطلاعات.
((منشا تهدیدات))میتوانند در اشتباهات عمدی یا سهوی عوامل داخلی و کارکنان یاسوءاستفاده آنان باشد.از طرفی عوامل اخلال گر بیرونی که هیچگونه دسترسی مجاز برای آنها در نظر گرفته نشده ممکن است بتواند به هر نحو در سیستم ها نفوذ کرده و به منابع حیاتی شبکه دست پیدا کنند.
((موقعیت تهدید ها))می تواند از محل فیزیکی استقرار منابع شبکه شروع شود و این منابع به صورت فیزیکی دزدیده شوند.منظور از منابع فیزیکی ماشین های سرویس دهنده.تجهیزات مسیریابی .دیسک های سخت و نرم و ابزار های ذخیره سازی اطلاعات (شامل دیسک های فشرده .نوار های مغناطیسی و دی وی دی .نرم افزار ها یا بانک های اطلاعاتی است.
ماشین یکایک کارکنان نیز می تواند یک نقطه تهدید باشد چون نفوذ در کامپیوتر یکی از کارکنان می تواند راه را برای نفوذ به درون بقیه ماشین ها باز کند خصوصا وقتی که آن کاربر خود دارای سطح دسترسی بالا به منابع شبکه است و جزو کاربران ویژه تلقی می شود.
ایجاد اختلال عمدی یا سهوی در هریک از منابع جانبی مثل آنتن های شبکه های بی سیم منابع تغذیه خطوط انتقال داده و نظائر آن جزو نقاطی است که همیشه تهدیداتی علیه آنان است.

3) ((تهدید)) الزاما به((حمله))و((آسیب))نمی انجامد.((تهدید ها همیشه فرض می شوند ولی گاهی در عمل هرگز اتفاق نمی افتند)پس از تعیین تهدید ها باید نقاط آسیب پذیر سیستم بدقت براورد شود.منظور از نقاط آسیب پذیر هرگونه مولفه سخت افزاری نرم افزاری یا سیستم عامل است که بروز یک اشکال بالقوه در آنها منجر به حمله و خسارت خواهد شد.

4) متاسفانه امنیت امری نسبی است و چیزی به نام امنیت صد درصد(امنیت مطلق)قابل تعریف نیست از طرفی هزینه طراحی وپیاده سازی یک الگوی امنیتی می تواند بسیار گران تر از خود شبکه تمام شود.از انجا که تهدیدها احتمال وقوع یکسانی ندارند و از طرفی تبدیل هرتهدید به حمله خسارت های یکسانی را بجا نمی گذارند لذا در چهارمین مرحله بایستی میزان خسارت مالی در اثر تبدیل هر تهدید به حمله تخمین زده شود و هزینه پیشگیری و مقابله با آن تهدید نیز مورد ارزیابی قرار بگیرد تا بتوان بر اساس این دو ارزیابی بودجه لازم و امکانات مورد نیاز را پیش بینی کرد.

5) پس از تعیین فهرست تهدیدها و براورد ضرر و زیان ناشی از تبدیل آنها از قوه به فعل وهمچنین ارزیابی میزان بودجه موجود باید برای هرتهدید استراتژیهای زیر را اتخاذ کرد:
الف)استراتژیهای پیشگیرانه شامل استفاده از تکنولوژی های برتر.ابزار های مراقبت ونظارت.آموزش عوامل انسانی واخذ تعهدنامه های لازم(در خصوص رعایت نکات امنیتی)پیش بینی سخت افزار.نرم افزار یا سرویس دهنده های پشتیبان ونظائرآن.
ب)استراتژیهای مقابله شامل تعیین ابزار های کشف حمله.تعیین روش های بازیابی داده ها.بیمه تجهیزات و خدمات و نظائر آنها.
در این مرحله باید کلیه ی تمهیدات پیشگیرانه وراه های مقابله یا تهدیدها مشخص شود وآن بخش تهددیداتی که هیچگونه پیش بینی خاصی در مورد آنها نشده بدقت مشخص وبه صورت دقیق ورسمی مستند سازی گردد.خروجی این مرحله به شکل یک آیین نامه ومجموعه ای از طرح و نقشه خواهد بود:

1) پس از تدوین طرح و نقشه امنیتی باید آن را در عمل پیاده سازی کرد.بخش بزرگی از یک نقشه امنیتی فقط در گروی اعمال سیاست ها آموزش افراد و اخذ تضمین وتعهد در خصوص موارد امنیتی است .لذا به مدیریت قوی.پیگیری وارزیابی مستمر نیاز دارد.نصب وراه اندازی ابزارهای امنیتی وپیکربندی آنها بر اساس استراتژی تعیین شده در مراحل قبلی انجام می گیرد ومدیر پروژه بایستی هدایت صحیح این مرحله از عملیات را برعهده داشته باشد.عوامل درگیر در پیاده سازی طرح باید از متخصصین حرفه ای و خبره انتخاب شوند.

2) هیچ استراتژی کامل نخواهد بود مگر آنکه بطور متناوب و در مقاطع زمانی برنامه ریزی شده مورد بازبینی وارزیابی قرار بگیرد.گاهی در ارزیابی استراتژی امنیتی به مواردی ار تغییر.تکمیل با اقدامات جدید نیاز خواهد بود.بدیهی است که با گذشت زمان شزایط تغییر خواهد کرد لذا مدیر مسئول باید بطور مستمر استراتژی امنیت را مورد بازبینی و نقد قرار بدهد و رعایت دقیق و بی ملاحظه ی آن را در طول زمان تحت نظر بگیرد و نیاز های جدید را در آن لحاظ کند.

فرایند تضمین امنیت اطلاعات سازمانی (طبق روال شکل4-1)می تواند بر اساس استاندارد های شناخته شده جهانی مثل( )انجام بگیرد .رهنمود های این رده از استاندارد(که حاصل سالیان طولانی تجربه وتحقیق است)به گونه ای تدوین شده که پیروی از آن کمترین(خطر)وبالاترین امنیت سازمانی را ایجاد خواهد کرد.استاندارد امنیت سازمانی را در سه زمینه((محرمانگی))((صحت))و((تضمین دسترسی دائم))پیش بینی و تعریف کرده است.
استانداری مثل قالب مشترکی برای تدوین سیاست های امنیتی شامل((کنترل وطبقه بندی دارایی ها و ارزش اطلاعات سازمان))((امنیت فیزیکی فردی))((مدیریت ارتباطات))((کنترل دسترسی به منابع سیستمی))((روش های نگهداری وبهبود اطلاعات))((مدیریت و آموزش مستمر))امنیت مبتنی بر قوانین حقوقی وسازگار باآن تعریف کرده است.
سازمان ها وموسسات با هر وسعت وپیچیدگی قادرند با پیاده سازی دقیق این استاندارد ها.گواهینامه معتبر و بین المللی دریافت کنند.

بسیاری از موسسات و سازمان های بزرگ دارایی اطلاعاتی خود را بیمه میکنند.شرکت های بیمه به عنوان پیش شرط اخذ گواهینامه هایی مثل را الزامی می دانند.

پس از پیاده سازی بند های مصوب در استانداردی مثل (یا معادل آن)و اعمال سیاست های مصوب گروهی به نمایندگی از موسسه استاندارد.اجرای بدون نقص تمام بند های اخباری (که بالغ بر130مورد است را بازرسی و پس از تایید رعایت آنها برای سازمان مربوطه گواهینامه صادر میکنند .این گواهینامه باید بطور متناوب باز بینی و تمدید شود.