

**پايان نامه**

**گرايش نرم افزار**

**موضوع:**

**اصول و مبانی امنیت در شبکه های رایانه ای**

**استاد راهنما:**

**نام دانشجو:**



**چکيده**

هدف از ارائه ی این پروژه معرفی اصول و مبانی امنیت در شبکه های کامپیوتری می باشد .در ابتدا به تعاریف و مفاهیم امنیت در شبکه می پردازیم .

در مبحث امنیت شبکه ،منابع شبکه وانواع حملات ،تحلیل خطر ،سیاست های امنیتی ،طرح امنیت شبکه و نواحی امنیتی به تفضیل مورد تحلیل و بررسی قرار می گیرد .

برای حفظ امنیت شبکه نیاز است تا مراحل اولیه ایجاد امنیت و سیتم های عامل و برنامه کاربردی مناسب لحاظ شود .در ادامه به انواع حملات در شبکه های رایانه ای پرداخته ایم و برای افزایش امنیت در سطح شبکه به AUDITING ، کامپیوترهای بدون دیسک ،به رمز در آوردن داده ها و محافظت در برابر ویروس پرداخته ایم .

و اما روشهای تامین امنیت در شبکه که عبارتند از : دفاع در عمق ،فایروال و پراکسی که به طور کامل تشریح شده است .و در ادامه سطوح امنیت شبکه ، تهدیدات علیه امنیت شبکه ، امنیت شبکه لایه بندی شده، ابزارها و الگوهای امنیت شبکه ،مراحل ایمن سازی شبکه ، راهکارهای امنیتی شبکه ،مکانیزم های امنیتی و الگوریتم جهت تهیه الگوی امنیت شبکه توضیح داده شده است .

**واژه‌هاي کليدي**

امنیت ،حملات ، شبکه ، فایروال ، پراکسی ، الگو

**فهرست مطالب**

|  |  |
| --- | --- |
| **عنوان** | **صفحه** |
| مقدمه ............................................................................................................................................................. | 1 |
| فصل یکم : تعاریف و مفاهیم امینت در شبکه | 2 |
| 1-1) تعاریف امنیت شبکه | 2 |
| 1-2) مفاهیم امنیت شبکه | 4 |
| 1-2-1) منابع شبکه | 4 |
| 1-2-2) حمله | 6 |
| 1-2-3) تحلیل خطر | 7 |
| 1-2-4- سیاست امنیتی | 8 |
| 1-2-5- طرح امنیت شبکه | 11 |
| 1-2-6- نواحی امنیتی | 11 |
| فصل دوم : انواع حملات در شبکه های رایانه ای | 13 |
| 2-1) مفاهیم حملات در شبکه های کامپیوتری | 15 |
| 2-2) وظیفه یک سرویس دهنده | 16 |
| 2-3) سرویس های حیاتی و مورد نیاز | 16 |
| 2-4) مشخص نمودن پروتکل های مورد نیاز | 16 |
| 2-5) مزایای غیر فعال نمودن پروتکل ها و سرویس های مورد نیاز | 17 |
| 2-6) انواع حملات | 18 |
| 1-2-6) حملات از نوع Dos |  |
| 2-2-6) حملات از نوع D Dos |  |
| 2-6-3) حملات از نوع Back dorr |  |
| 2-6-3-1) Back ori fice |  |
| 2-6-3-2) Net Bus |  |
| 2-6-3-3) Sub seven |  |
| 2-6-3-4) virual network computing |  |
| 2-6-3-5) PC Any where |  |
| 2-6-3-6) Services Terminal |  |
| 2-7) Pactet sniffing |  |
| 2-7-1) نحوه کار packet sniffing |  |
| 2-2-7) روشهای تشخیص packet sniffing در شبکه |  |
| 2-7-3) بررسی سرویس دهندة DNS |  |
| 2-7-4) اندازه گیری زمان پاسخ ماشین های مشکوک |  |
| 2-7-5) استفاده از ابزارهای مختص Antisniff |  |
| فصل سوم ) افزایش امنیت شبکه |  |
| 3-1) علل بالا بردن ضریب امنیت در شبکه |  |
| 3-2) خطرات احتمالی |  |
| 3-3) راه های بالا بردن امنیت در شبکه |  |
| 3-3-1) آموزش |  |
| 3-3-2) تعیین سطوح امنیت |  |
| 3-3-3) تنظیم سیاست ها |  |
| 3-3-4) به رسمیت شناختن Authen tication |  |
| 3-3-5) امنیت فیزیکی تجهیزات |  |
| 3-3-6) امنیت بخشیدن به کابل |  |
| 3-4) مدل های امنیتی |  |
| 3-4-1) منابع اشتراکی محافظت شده توسط کلمات عبور |  |
| 3-4-2) مجوزهای دسترسی |  |
| 3-5) امنیت منابع |  |
| 3-6) روش های دیگر برای امنیت بیشتر |  |
| 3-6-1) Auditing |  |
| 3-6-2) کامپیوترهای بدون دیسک |  |
| 3-6-3) به رمز در آوردن داده ها |  |
| 3-6-4) محافظت در برابر ویروس |  |
| فصل چهارم : انواع جرایم اینترنتی و علل بروز مشکلات امنیتی |  |
| 4-1) امنیت و مدل |  |
| 4-1-1) لایه فیزیکی |  |
| 4-1-2) لایه شبکه |  |
| 4-1-3) لایه حمل |  |
| 4-1-4) لایه کاربرد |  |
| 4-2) جرایم رایانه ای و اینترنتی |  |
| 4-2-1) پیدایش جرایم رایانه ای |  |
| 4-2-2) قضیه رویس |  |
| 4-2-3)تعریف جرم رایانه ای |  |
| 4-2-4) طبقه بندی جرایم رایانه ای |  |
| 4-2-4-1) طبقه بندی OECDB |  |
| 4-2-4-2) طبقه بندی شعرای اروپا |  |
| 4-2-4-3) طبقه بندی اینترپول |  |
| 4-2-4-4) طبقه بندی در کنوانسیون جرایم سایبرنتیک |  |
| 4-2-5) شش نشانه از خرابکاران شبکه ای |  |
| 4-3) علل بروز مشکلات امنیتی |  |
| 4-3-1) ضعف فناوری |  |
| 4-3-2) ضعف پیکربندی |  |
| 4-3-3) ضعف سیاستی |  |
| فصل 5 ) روشهای تأمین امنیت در شبکه |  |
| 5-1) اصول اولیه استراتژی دفاع در عمق |  |
| 5-1-1) دفاع در عمق چیست. |  |
| 5-1-2) استراتژی دفاع در عمق : موجودیت ها |  |
| 5-1-3) استراتژی دفاع در عمق : محدودة حفاظتی |  |
| 5-1-4) استراتژی دفاع در عمق : ابزارها و مکانیزم ها |  |
| 5-1-5) استراتژی دفاع در عمق : پیاده سازی |  |
| 5-1-6) جمع بندی |  |
| 5-2)فایر وال |  |
| 1-5-2) ایجاد یک منطقه استحفاظی |  |
| 5-2-2) شبکه های perimer |  |
| 5-2-3) فایروال ها : یک ضرورت اجتناب ناپذیر در دنیای امنیت اطلاعات |  |
| 5-2-4) فیلترینگ پورت ها |  |
| 5-2-5) ناحیه غیر نظامی |  |
| 5-2-6) فورواردینگ پورت ها |  |
| 5-2-7) توپولوژی فایروال |  |
| 5-2-8) نحوة انتخاب یک فایروال |  |
| 5-2-9) فایروال ویندوز |  |
| 5-3) پراکسی سرور |  |
| 5-3-1) پیکر بندی مرور |  |
| 5-3-2) پراکسی چیست |  |
| 5-3-3) پراکسی چه چیزی نیست |  |
| 5-3-4) پراکسی با packet filtering تفاوت دارد. |  |
| 5-3-5) پراکسی با packet fillering state ful تفاوت دارد . |  |
| 5-3-6) پراکسی ها یا application Gafeway |  |
| 5-3-7) برخی انواع پراکسی |  |
| 5-3-7-1) Http proxy |  |
| 5-3-7-2) FTP Proxy |  |
| 5-3-7-3) PNs proxy |  |
| 5-3-7-4) نتیجه گیری |  |
| فصل 6 ) سطوح امنیت شبکه |  |
| 6-1) تهدیدات علیه امنیت شبکه |  |
| 6-2) امنیت شبکه لایه بندی شده |  |
| 6-2-1) سطوح امنیت پیرامون |  |
| 6-2-2) سطح 2 – امنیت شبکه |  |
| 6-2-3) سطح 3 – امنیت میزبان |  |
| 6-2-4) سطوح 4 – امنیت برنامه کاربردی |  |
| 6-2-5) سطح 5 – امنیت دیتا |  |
| 6-3) دفاع در مقابل تهدیدها و حملات معمول |  |
| فصل هفتم ) ابزارها و الگوهای امنیت در شبکه و ارائه ی یک الگوی امنیتی |  |
| 7-1) مراحل ایمن سازی شبکه |  |
| 7-2) راهکارهای امنیتی شبکه |  |
| 7-2-1) کنترل دولتی |  |
| 7-2-2) کنترل سازمانی |  |
| 7-2-3) کنترل فردی |  |
| 7-2-4) تقویت اینترانت ها |  |
| 7-2-5) وجود یک نظام قانونمند اینترنتی |  |
| 7-2-6) کار گسترده فرهنگی برای آگاهی کاربران |  |
| 7-2-7) سیاست گذاری ملی در بستر جهانی |  |
| 7-3) مکانیزم امنیتی |  |
| 7-4) مرکز عملیات امنیت شبکه |  |
| 7-4-1) پیاده سازی امنیت در مرکز SOC |  |
| 7-4-2) سرویس های پیشرفته در مراکز SOC |  |
| 7-5) الگوی امنیتی |  |
| 7-5-1) الگوریتم جهت تهیه الگوی امنیتی شبکه |  |

**فهرست شکلها**

|  |  |  |
| --- | --- | --- |
| **عنوان** | **صفحه** | |
| شکل 3-1 مجوزهای مربوط به فایل ها و دایرکتوری اشتراکی را نشان می دهد. | | 3 |
| شکل 5-1 یک نمونه از پیاده سازی Fire wall را مشاهده می کنید | | 3 |
| شکل 5-2 یک نمونه از پیاده سازی Fire wall را مشاهده می کنید | |  |
| شکل 5-3 ارتباط بین سه نوع شبکه Perimeter را نمایش می دهد. | |  |
| شکل 5-4 دو شبکه Perimeter درون یک شبکه را نشان می دهد. | |  |
| شکل 5-5 یک فایروال مستقیماً و از طریق یک خط dial – up ، خطوط ISPN و یا مووم های کابلی به اینترنت متصل می گردد. | |  |
| شکل 5-6 روتر متصل شده به اینترنت به هاب و یا سوئیچ موجود در شبکه داخل مستقل می گردد. | |  |
| شکل 5-7 فایردال شماره یک از فایر دال شماره 2 محافظت می نماید. | |  |
| شکل 5-8 یک کارت شبکه دیگر بر روی فایر دال و برای ناحیه DMZ استفاده می گردد. | |  |
| شکل 5-9 Proxy server | |  |
| شکل 5-10 logging | |  |
| شکل 5-11 Ms proxy server | |  |
| شکل 5-12 SMTP proxy | |  |
| شکل 5-13 SMTP Filter Properties | |  |
| شکل 5-14 Mozzle pro LE | |  |
| شکل 5-15 DNS proxy | |  |
| شکل 5-16 | |  |
| شکل 6-1 | |  |
| شکل 6-2 برقراری ارتباط VPN | |  |
| شکل 6-3 پیکربندی های IDS و IPS استاندارد | |  |
| شکل 6-4 سطح میزبان | |  |
| شکل 6-5 Prirate local Area Network | |  |
| شکل 6-6 حملات معمول | |  |

**فهرست جدولها**

|  |  |  |
| --- | --- | --- |
| **عنوان** | **صفحه** | |
| جدول2-1- مقایسه تهدیدات امنیتی در لایه های چهارگانه TCP/IP | |  |
| جدول2-2- اهداف امنیتی در منابع شبکه | |  |
| جدول6-1- امنیت شبکه لایه بندی شده | |  |
|  | |  |

**ليست علايم و اختصارات**

|  |  |
| --- | --- |
| (Secure dhell) | SSH |
| (Au then tication, Authorization and Accounting) | DMZ |
| Distributed denial of service) | DDOS |
| User service Remote Autheution Dial-in | RADIUS |
| Terminal Access controller Access control system | TACACS |
| Simple Mail Transfer protocol | SMTP |
| Simple Network Management perptocel | SN MP |
| Network Adsress Ttranclation | NAT |
| Port Address Translation | PAT |
| In for mation assurance Technical Farmwork From | IATFF |
| National security Agency | NSA |
| Key manage ment infrastructure | KMI |
| Public Key infrastructure | PKI |
| List Access control | ACL |
| Challenge Hhandshake Anthentication protocol | CHAP |
| Password Authentication protocol | PAP |
| Point to point tunneling protocol | pptp |
| Authenticated Header | AH |
| Encasugated secure payload | ESP |
| Secure sockets layer | SSL |
| TTransport layer security | TLS |
| Internet connection Firewall | ICF |
| File transfer protocol | FTP |
| Dpmin Name Server | DNS |
| Intrusion Detection system | IDS |
| Virtual Network computing | VNC |

# مقدمه

چنانچه به اهميت شبكه‌هاي اطلاعاتي (الكترونيكي) و نقش اساسي آن دريافت اجتماعي آينده پي برده باشيم، اهميت امنيت اين شبكه‌ها مشخص مي‌گردد. اگر امنيت شبكه برقرار نگردد، مزيتهاي فراوان آن نيز به خوبي حاصل نخواهد شد و پول و تجارت الكترونيك، خدمات به كاربران خاص، اطلاعات شخصي، اطلاعاتي عمومي و نشريات الكترونيك همه و همه در معرض دستكاري و سوءاستفاده‌هاي مادي و معنوي هستند. همچنين دستكاري اطلاعات- به عنوان زيربناي فكري ملت‌ها توسط گروههاي سازماندهي شده بين‌المللي، به نوعي مختل ساختن امنيت ملي و تهاجم عليه دولت‌ها و تهديدي ملي محسوب مي‌شود.  
براي كشور ما كه بسياري از نرم‌افزارهاي پايه از قبيل سيستم عامل و نرم‌افزارهاي كاربردي و اينترنتي، از طريق واسطه‌ها و شركتهاي خارجي تهيه مي‌شود، بيم نفوذ از طريق راههاي مخفي وجود دارد. در آينده كه بانكها و بسياري از نهادها و دستگاههاي ديگر از طريق شبكة به فعاليت مي‌پردازند، جلوگيري از نفوذ عوامل مخرب در شبكه بصورت مسئله‌اي استراتژيك درخواهد آمد كه نپرداختن به آن باعث ايراد خساراتي خواهد شد كه بعضاً جبران‌ناپذير خواهد بود. چنانچه يك پيغام خاص، مثلاً از طرف شركت مايكروسافت، به كليه سايتهاي ايراني ارسال شود و سيستم عاملها در واكنش به اين پيغام سيستمها را خراب كنند و از كار بيندازند، چه ضررهاي هنگفتي به امنيت و اقتصاد مملكت وارد خواهد شد؟  
نكته جالب اينكه بزرگترين شركت توليد نرم‌افزارهاي امنيت شبكه، شركت چك پوينت است كه شعبة اصلي آن در اسرائيل مي‌باشد. مسأله امنيت شبكة براي كشورها، مسأله‌اي استراتژيك است؛ بنابراين كشور ما نيز بايد به آخرين تكنولوژيهاي امنيت شبكه مجهز شود و از آنجايي كه اين تكنولوژيها به صورت محصولات نرم‌افزاري قابل خريداري نيستند، پس مي‌بايست محققين كشور اين مهم را بدست بگيرند و در آن فعاليت نمايند.  
امروزه اينترنت آنقدر قابل دسترس شده كه هركس بدون توجه به محل زندگي، مليت، شغل و زمان ميتواند به آن راه يابد و از آن بهره ببرد. همين سهولت دسترسي آن را در معرض خطراتي چون گم شدن، ربوده شدن، مخدوش شدن يا سوءاستفاده از اطلاعات موجود در آن قرار مي‌دهد. اگر اطلاعات روي كاغذ چاپ شده بود و در قفسه‌اي از اتاقهاي محفوظ اداره مربوطه نگهداري مي‌شد، براي دسترسي به آنها افراد غيرمجاز مي‌بايست از حصارهاي مختلف عبور مي‌كردند، اما اكنون چند اشاره به كليدهاي رايانه‌اي براي اين منظور كافي است.

# فصل يکم –

# تعاریف و مفاهیم امنیت در شبکه

**1) تعاریف امنیت شبکه :**

بر اساس واژه نامه Webster امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می باشد. این تعبیر در دنیای الکترونیکی نیز صادق می باشد اما اگر بخواهیم تعریفی تخصصی در این زمینه داشته باشیم می توانیم بگوییم که، برقراری امنیت در حفظ و بقاء 4 اصل می باشد:

* محرمانگی : اطلاعات فقط و فقط بایستی توسط افراد مجاز قابل دسترس باشد.
* تمامیت : یک سیستم از عناصری متشکل است که در کنار هم برای رسیدن به هدفی یکسان همکاری دارند. حفظ تمامیت به معنای پیشگیری از بروز مشکل در این همکاری و پیوسته نگه داشتن عناصر یک سیستم می باشد.
* دسترس پذیری : اطلاعات بایستی به هنگام نیاز، توسط افراد مجاز قابل دسترس باشد.
* عدم انکار : به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکار کند.

## 2) مفاهیم امنیت شبكه امنیت شبكه یاNetwork Security پردازه ای است كه طی آن یك شبكه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می شود. مراحل ذیل برای ایجاد امنیت پیشنهاد و تایید شده اند:

1-شناسایی بخشی كه باید تحت محافظت قرار گیرد.

2-تصمیم گیری درباره  مواردی كه باید در مقابل آنها از بخش مورد نظر محافظت كرد.

3-تصمیم گیری درباره چگونگی تهدیدات

4-پیاده سازی امكاناتی كه بتوانند از دارایی های شما به شیوه ای محافظت كنند كه از نظر هزینه به صرفه باشد.

5-مرور مجدد و مداوم پردازه و تقویت آن درصورت یاقتن نقطه ضعف

برای درك بهتر مباحث مطرح شده در این بخش ابتدا به طرح بعضی مفاهیم در امنیت شبكه می پردازیم.

## 1-2) منابع شبكه

در یك شبكه مدرن منابع بسیاری جهت محافظت وجود دارند. لیست ذیل مجموعه ای از منابع شبكه را معرفی می كند كه باید در مقابل انواع حمله ها مورد حفاظت قرار گیرند.

1-تجهیزات شبكه مانند روترها، سوئیچ ها و فایروالها

2-اطلاعات عملیات شبكه مانند جداول مسیریابی و پیكربندی لیست دسترسی كه بر روی روتر ذخیره شده اند.

3-منابع نامحسوس شبكه مانند عرض باند و سرعت

4-اطلاعات و منابع اطلاعاتی متصل به شبكه مانند پایگاه های داده و سرورهای اطلاعاتی

5-ترمینالهایی كه برای استفاده از منابع مختلف به شبكه متصل می شوند.

6-اطلاعات در حال تبادل بر روی شبكه در هر لحظه از زمان

7-خصوصی نگهداشتن عملیات كاربرن و استفاده آنها از منابع شبكه جهت جلوگیری از شناسایی كاربران.

مجموعه فوق به عنوان دارایی های یك شبكه قلمداد می شود.

## 2-2) حمله

حال به تعریف حمله می پردازیم تا بدانیم كه از شبكه در مقابل چه چیزی باید محافظت كنیم. حمله تلاشی خطرناك یا غیر خطرناك است تا یك منبع قابل دسترسی از طریق شبكه ، به گونه ای مورد تغییر یا استفاده قرار گیرد كه مورد نظر نبوده است.برای فهم بهتر بد نیست حملات شبكه را به سه دسته عمومی تقسیم كنیم:

1-دسترسی غیرمجاز به منابع و اطلاعات از طریق شبكه

2-دستكاری غیرمجاز اطلاعات بر روی یك شبكه

3-حملاتی كه منجر به اختلال در ارائه سرویس می شوند و اصطلاحا Denial of Service نام دارند.

كلمه كلیدی در دو دسته اول انجام اعمال به صورت غیرمجاز است. تعریف یك عمل مجاز یا غیرمجاز به عهده سیاست امنیتی شبكه است، اما به عبارت كلی می توان دسترسی غیرمجاز را تلاش یك كاربر جهت دیدن یا تغییر اطلاعاتی كه برای وی در نظر گرفته نشده است، تعریف نمود اطلاعات روی یك شبكه نیز شامل اطلاعات موجود بر روی رایانه های متصل به شبكه مانند سرورهای پایگاه داده و وب ، اطلاعات در حال تبادل بر روی شبكه و اطلاعات مختص اجزاء شبكه جهت انجام كارها مانند جداول مسیریابی روتر است. منابع شبكه را نیز می توان تجهیزات انتهایی مانند روتر و فایروال یا مكانیزمهای اتصال و ارتباط دانست.

هدف از ایجاد امنیت شبكه ، حفاظت از شبكه در مقابل حملات فوق است، لذا می توان اهداف را نیز در سه دسته ارائه كرد:

1-ثابت كردن محرمانگی داده

2-نگهداری جامعیت داده

3 -نگهداری در دسترس بودن داده

## 3-2) تحلیل خطر

پس از تعیین دارایی های شبكه و عوامل تهدیدكننده آنها ، باید خطرات مختلف را ارزیابی كرد. در بهترین حالت باید بتوان از شبكه در مقابل تمامی انواع خطا محافظت كرد، اما امنیت ارزان به دست نمی آید. بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهمترین آنها را تشخیص دهیم و از طرف دیگر منابعی كه باید در مقابل این خطرات محافظت شوند نیز شناسایی شوند. دو فاكتور اصلی در تحلیل خطر عبارتند از :

1-احتمال انجام حمله

2-خسارت وارده به شبكه درصورت انجام حمله موفق

## 4-2) سیاست امنیتی

پس از تحلیل خطر باید سیاست امنیتی شبكه را به گونه ای تعریف كرد كه احتمال خطرات و میزان خسارت را به حداقل برساند. سیاست امنیتی باید عمومی و در حوزه دید كلی باشد و به جزئیات نپردازد. جزئیات می توانند طی مدت كوتاهی تغییر پیدا كنند اما اصول كلی امنیت یك شبكه كه سیاست های آن را تشكیل می دهند ثابت باقی می مانند.در واقع سیاست امنیتی سه نقش اصلی را به عهده دارد:

1-چه و چرا باید محافظت شود.

2-چه كسی باید مسئولیت حفاظت را به عهده بگیرد.

3-زمینه ای را بوجود آورد كه هرگونه تضاد احتمالی را حل و فصل كند.

سیاستهای امنیتی را می توان به طور كلی به دو دسته تقسیم كرد:

1-مجاز (Permissive) : هر آنچه بطور مشخص ممنوع نشده است ، مجاز است.

2-محدود كننده (Restrictive) : هر آنچه بطور مشخص مجاز نشده است ، ممنوع است.

معمولا ایده استفاده از سیاستهای امنیتی محدودكننده بهتر و مناسبتر است چون سیاستهای مجاز دارای مشكلات امنیتی هستند و نمی توان تمامی موارد غیرمجاز را برشمرد.

## 5-2) طرح امنیت شبكه

با تعریف سیاست امنیتی به پیاده سازی آن در قالب یك طرح امنیت شبكه می رسیم. المانهای تشكیل دهنده یك طرح امنیت شبكه عبارتند از :

1-ویژگیهای امنیتی هر دستگاه مانند كلمه عبور مدیریتی و یا بكارگیریSSH

2-فایروالها

3-مجتمع كننده هایVPN برای دسترسی از دور

4-تشخیص نفوذ

5-سرورهای امنیتیAAA (Authentication، Authorization and Accounting) و سایر خدماتAAA برای شبكه

6-مكانیزمهای كنترل دسترسی و محدودكننده دسترسی برای دستگاههای مختلف شبكه

## 6-2) نواحی امنیتی

تعریف نواحی امنیتی نقش مهمی را در ایجاد یك شبكه امن ایفا می كند. در واقع یكی از بهترین شیوه های دفاع در مقابل حملات شبكه ، طراحی امنیت شبكه به صورت منطقه ای و مبتنی بر توپولوژی است و یكی از مهمترین ایده های مورد استفاده در شبكه های امن مدرن ، تعریف نواحی و تفكیك مناطق مختلف شبكه از یكدیگر است. تجهیزاتی كه در هر ناحیه قرار می گیرند نیازهای متفاوتی دارند و لذا هر ناحیه حفاظت را بسته به نیازهای امنیتی تجهیزات نصب شده در آن ، تامین می كند. همچنین منطقه بندی یك شبكه باعث ایجاد ثبات بیشتر در آن شبكه نیزمی شود.