فهرست مطالب

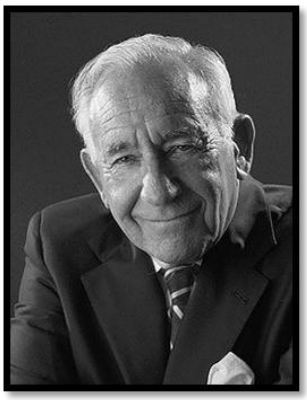
Chapter 1

امنیت اطلاعات

اهداف فصل

- مروری بر مفهوم امنیت
- معرفی پروسه امنیت اطلاعات
- آشنایی با مهندسی امنیت اطلاعات

1. امنیت اطلاعات



David Kahn
نویسنده معروفترین کتاب cryptography
(1967)The Codebreakers - The Story of Secret Writing
و اولین شخصی که مرکز کنترل شبکه اینترنت را شرح داد
National Security Agency (NSA)
و استاندارد Data Encryption Standard در 1970 تدوین نمود.

1.1. خلاصه فصل

از آنجا که امنیت شالوده ی هر نوع سیستمی است و با حضور خود در سیستم‌ها فارغ از نوع و هدف آن‌ها، می‌تواند برای مدیران و مسئولان زیربط، اطمینان خاطر در برابر انواع تهدیدات، آسیب‌ها، ریسک‌ها و حوادث را به دنبال داشته باشد.

و از دیگر سو هر سازمان، نهاد یا دستگاهی به موازات احساس نیاز به امنیت سیستم خود نسبت به تمامی تهدیدات موجود، به امنیت اطلاعات درونی و محرمانه خود به شدت نیازمند است و حتی شاید بتوان گفت امنیت اطلاعات می‌تواند پایه و اساسی برای حفظ امنیت در اکثریت جنبه‌های دیگر امنیتی سازمان باشد. لذا در این فصل سعی شده به اهمیت امنیت اطلاعات از زوایای مختلف پرداخته شود و مهندسی امنیت به‌عنوان یک روش طراحی، پیاده سازی، تست سیستم‌ها و تعدیل سیستم‌های موجود با هدف تکامل محیط آنها و نیز یک روش ساخت سیستم‌هایی که در مقابل سوء قصدها، خطاها و رویدادهای بد، مطمئن و قابل اعتماد باقی بماند، ارائه می‌گردد.

1.2. مفاهیم بنیادی در امنیت اطلاعات

یکی از ویژگی‌های اصلی شبکه در دسترس بودن آن برای تمامی افراد است بخصوص کسانیکه نوع کارشان بگونه‌ای است که باید به شبکه متصل باشند. در این حالت وقتی افراد به شبکه و یا خدمات خاص ارائه شده روی شبکه دسترسی نداشته باشند در واقع اختلال در سرویس دهی را عیناً تجربه می‌نمایند که این مسئله خوشایند نیست.

برای رفع این مشکل سازمان‌ها از دو اقدام اساسی *Authentication* و *Authorization* به منظور در دسترس قرار دادن اطلاعات استفاده می‌نمایند. در واقع " *Authentication* " نشانه‌ای برای اثبات ادعای فرد متقاضی برای دسترسی است. حال آنکه این نشانه می‌تواند مشتمل بر مواردی نظیر: چیزهایی که فرد باید بداند

(مانند password)، چیزهایی که فرد داراست (مانند smartcard) یا چیزهایی برای اثبات هویت فرد (مانند fingerprint) باشد و " *Authorization* " عمل تعیین اینکه آیا یک کاربر، کامپیوتر یا سیستم خاص حق انجام عملیات خاصی مانند خواندن فایل یا اجرای برنامه را دارد یا ندارد.

لازم به ذکر است این دو اقدام اساسی با یکدیگر و در کنارهم انجام می‌شوند بدین معنا که باید قبل از اینکه کاربران فعالیت‌هایی را که مجاز به اجرای آن‌ها هستند انجام دهند تأیید صلاحیت شوند.

حصول اطمینان نسبت به اطلاعات در همه انواع سیستم‌ها (از قبیل سیستم‌های کنترلی، توزیع شده و ...) مهم و حیاتی است و در این خصوص تکنولوژی‌های اطلاعاتی انواع نفوذ به سیستم اطلاعاتی را که این سیستم مشتمل بر اجزای سخت افزاری ، نرم افزاری و انسانی است تضمین می‌نماید.

1.3. امنیت اطلاعات

امنیت و اطلاعات دو واژه مستقل از هم، معانی بسیار گسترده‌ای را در بر می‌گیرند. امنیت از نظر مفهومی به وضعیتی اطلاق می‌شود که نیروهای حفظ کننده‌ی وضع موجود ، توان محافظت را از نیروهای شناخته شده‌ی برهم زننده‌ی آن داشته باشند. ولی حفاظت کردن از هر چیزی نیاز به شناختن ماهیت آن و شناختن روش ها و چگونگی وقوع حمله ، به مورد حفاظت شده را خواهد داشت.

همچنین مهندسی به مفهوم انجام عملیاتی (به منظور تولید محصولی) با تبعیت از مجموعه قواعد مشخصی است که این عملیات به صورت سیستماتیک و قابل تکرار بتواند انجام شوند.

ترکیب این دو واژه می‌تواند تعاریف جدیدی داشته باشد ولی به صورت متعارف می‌تواند به مفهوم شناخت و بررسی مقوله امنیت از دید مهندسی و ایجاد نگرشی سازمان یافته‌تر برای افزایش امنیت باشد. در حقیقت مهندسی امنیت به بررسی اجزاء تشکیل دهنده امنیت به گونه‌ای که فرایند ایجاد امنیت و افزایش آن در مراحل گوناگون امری ساده‌تر و کم هزینه‌تر از بعد زمانی و ریالی باشد؛ می‌پردازد.

برای دستیابی به امنیت بالا باید از همان نقطه ابتدایی، موضوع امنیت به عنوان هدفی مهم مد نظر و به صورت امری ذاتی وجود داشته باشد، یعنی ماهیت اصلی هر آنچه که نیازمند امنیت است خود امنیت باشد.

بنابراین برای تولید نرم افزار هایی امن، به یک چرخه تولید نرم افزار نیاز خواهد بود تا نرم افزارهایی امن تولید کند. یعنی با داشتن یک Security Product Life Cycle می‌توان نرم افزار هایی امن نیز داشت.

یک Security PLC که امنیت را درون محصول خود تولید می‌کند باید در تمامی فازها به امنیت توجه و نگاه ویژه‌ای داشته باشد. مثلا در فاز Proposal و فاز Requirement باید امن بودن و منعطف بودن محصول از نیازهای اصلی و مهم تعریف شود و یا در فاز تست فشار بیشتری از این نظر بر روی محصول آورده شود.

در حالت کلی این موضوعات با پدافند غیر عامل نیز ارتباط مستقیمی دارند. پدافند غیر عامل به هر اقدام غیر مسلحانه‌ای گفته می‌شود که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان‌ها، تأسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد.

به بیان ساده‌تر پدافند غیرعامل، مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ، خسارات احتمالی به حداقل میزان خود برسد. هدف از اجرای طرح‌های پدافند غیرعامل کاستن از آسیب‌پذیری نیروی انسانی و مستحدثات و تجهیزات حیاتی و حساس و مهم کشور علیرغم حملات خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیر بنایی و تأمین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است. به عنوان مثالی ساده، از پدافند غیرعامل می‌توان به استتار، اختفا و ایجاد سرپناه برای تأسیسات مهم و استراتژیک اشاره کرد. در پدافند عامل مثل سیستم‌های ضد هوایی و هواپیماهای ره‌گیر، فقط نیروهای مسلح مسئولیت دارند. در حالی که در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری بر عهده گیرند.

سیستم‌های اطلاعاتی به 3 بخش اصلی: سخت افزار، نرم افزار و شبکه تقسیم می‌شوند که این تقسیم بندی با هدف شناسایی و اعمال استانداردهای امنیتی اطلاعات تحت عنوان مکانیزم‌های حفاظتی و پیشگیرانه و در 3 سطح صورت می‌پذیرد:

- سطح فیزیکی
- سطح پرسنلی
- سطح سازمانی

اساساً این روش ها و سیاست‌ها بدین منظور پیاده‌سازی شده‌اند تا به مدیران، کاربران و اپراتورها چگونگی استفاده از محصولات را اعلام نموده و بدین طریق از وجود امنیت اطلاعات در سازمان‌ها اطمینان حاصل شود. امنیت اطلاعات به معنی حفاظت اطلاعات در برابر دسترسی، استفاده، افشا سازی، قطع، اصلاح و ... غیر مجاز است و علاوه بر این اثر قابل توجهی در حفظ حریم خصوصی - که در فرهنگ‌های مختلف بطور بسیار متفاوتی مشاهده می‌شود – دارد. و در حالت کلی اجزای اصلی امنیت اطلاعات را availability ، confidentiality ، integrity تشکیل می‌دهند.

در سال‌های اخیر توجه به امنیت اطلاعات بطور چشمگیری رشد نموده است و به حوزه‌های مختلفی نظیر:

1- امنیت شبکه‌ها و ساختارهای پیوسته
2- امنیت برنامه‌های کامپیوتری و بانک‌های اطلاعاتی
3- تست امنیت
4- ممیزی سیستم‌های اطلاعاتی
5- برنامه‌ریزی برای تداوم کسب و کار

...

تخصیص یافته است.

1.4. پروسه امنیت اطلاعات

امنیت اطلاعات یک فرآیند است نه یک محصول؛ فرآیندی است برای شناسایی و به حداقل رساندن ریسک به یک سطح قابل قبول در نظرگرفته شده، که لازم است این فرآیند تکرار داشته باشد و مدیریت شود. در واقع امنیت اطلاعات اثر یا پدیده واکنشی در مقابل یک پدیده فعال موجود است. اما در پاسخ به این سؤال که چرا امنیت مشکل است می‌توان اذعان داشت امنیت اطلاعات هیچ تفاوتی با زیرساخت‌های شبکه معمولی ندارد و تنها کافیست دقت و توجه کافی در این زمینه وجود داشته باشد و مشکل بودن امنیت اطلاعات بدین دلیل است که پس از وقوع حادثه‌ای برای زیرساخت‌های امنیت اطلاعات نشان دادن ارزش محسوسی برای آن، بسیار مشکل خواهد بود.

1.5. مهندسی امنیت

مهندسی امنیت به عنوان یک زمینه غیر رسمی در مطالعه، از سال‌های پیش وجود داشته است به عنوان مثال زمینه‌هایی همچون قفل‌سازی و چاپ امن، سال‌های زیادی است که وجود دارند و با توجه به وقایع مصیبت بار اخیر مهندسی امنیت به سرعت به یک زمینه درحال رشد تبدیل شده و شامل جنبه‌هایی از علوم اجتماعی، روان شناسی، اقتصاد، فیزیک، شیمی، ریاضیات و معماری می‌شود.

اندرسن مهندسی امنیت را اینگونه تعریف می‌کند:

"ساخت سیستم‌هایی که در مقابل سوء قصدها، خطاها و رویدادهای بد، مطمئن و قابل اعتماد باقی بماند."

تمرکز مهندسی امنیت بر ابزارها، پردازش‌ها و روش‌های موردنیاز برای طراحی، پیاده‌سازی، تست سیستم‌ها و تعدیل سیستم‌های موجود با هدف تکامل محیط آن‌ها است.

مهندسی امنیت یک زمینه تخصصی از مهندسی است که با توسعه طرح‌ها و برنامه‌های دقیق مهندسی برای تأمین امنیت، امکانات، کنترل‌ها و سیستم‌ها سروکار دارد و شبیه به دیگر فعالیت‌های مهندسی سیستم است که هدف اصلی آن پشتیبانی و ارائه راه حل‌های مهندسی است که این راه‌حل‌ها الزامات کاربری و تابعی از پیش تعریف شده را ارضاء می‌نماید. مهندسی امنیت مجموعه فعالیت‌هایی است که برای حصول و نگهداری سطوح مناسبی از :

- محرمانگی
- صحت
- قابلیت دسترسی
- حساب پذیری
- اصالت
- قابلیت اطمینان است.

محرمانگی: یعنی اطلاعات برای افراد، موجودیت‌ها یا فرآیندهای‌غیر مجاز در دسترس قرار نگیرد یا افشا نشود.
برای مثال کارت‌های تجاری اعتباری در اینترنت به یک شماره کارت اعتباری برای انتقال وجه از خریدار به فروشنده و از فروشنده به خریدار مجهز هستند و یک شبکه پردازشی مجهز نیازمند هستند.
در این حالت سیستم برای اجرای محرمانه‌سازی در زمان انتقال از عملیات رمزنگاری، محدود کردن موقعیت‌هایی که ممکن است به ذهن برسند (پایگاه‌های داده، فایل‌های ورود به سیستم، پشتیبان گیری و ...) و محدود کردن دسترسی به مکان‌های ذخیره سازی اطلاعات استفاده می‌نماید. قابل تأمل است اگر بخش غیر مجاز به هر نحوی به شماره کارت دسترسی پیدا کند عملاً نقض محرمانگی رخ داده است.
نقض محرمانگی به اشکال مختلفی می‌تواند رخ دهد:

- زمانیکه اطلاعات محرمانه به نمایش درآمده در صفحه نمایش کامپیوتر، توسط افراد غیر مجاز قابل مشاهده باشند نوعی نقض محرمانگی رخ داده است.
- به سرقت رفتن یا فروخته شدن لپ تاپ حاوی اطلاعات محرمانه کارمندان یک شرکت نیز نوعی نقض محرمانگی به حساب می‌آید.
- دادن اطلاعات، پشت خط تلفن به تلفن زننده ناشناس، نقض محرمانگی است.

توجه:
محرمانگی برای حفظ حریم افرادی که اطلاعات خاص یک سیستم را نگهداری می‌نمایند ضروری است ولی کافی نیست.
صحت : به معنای حفظ صحت سیستم و داده است.
در امنیت اطلاعات، یکپارچگی به این معنی است که داده نمی‌تواند به طور غیرقابل تشخیص تغییر یابد و کاملاً با یکپارچگی در بانک اطلاعاتی متفاوت است، البته می‌تواند به عنوان حالت خاصی از سازگاری همچون مدل کلاسیک ACID برای پردازش تراکنش در نظر گرفته شود.
زمانیکه یک پیام بطور پویا در حین عمل انتقال تغییر می‌یابد عملاً یکپارچگی از بین می‌رود لذا سیستم‌های رمزنگاری، یکپارچگیِ پیام را همراه با حفظ حریم خصوصی بعنوان بخشی از فرآیند رمزنگاری فراهم می‌آورند.
صحت داده : یعنی داده‌ها به صورت غیرمجاز تغییر پیدا نکنند یا از بین نروند.
صحت سیستم : یعنی فعالیت‌های مورد انتظار از سیستم بدون عیب و خالی از دستکاری‌های غیرمجاز (تعمدی یا تصادفی) در سیستم انجام شود.
اصالت: یعنی هویت واقعی یک موجودیت با هویت مورد ادعا یکسان باشد.

در کامپیوتر، تجارت الکترونیکی و امنیت اطلاعات لازم است در مورد واقعی بودن داده‌ها، تراکنش‌ها، ارتباطات و اسناد (اعم از فیزیکی یا الکترونیکی) اطمینان کامل حاصل شود. همچنین برای صحت اعتبار باید هویت واقعی یک موجودیت با هویت مورد ادعا یکسان باشد.

قابلیت دسترسی: یعنی منابع برای یک موجودیت مجاز در هنگام نیاز در دسترس و قابل استفاده باشد.

یکی از اهداف سیستم‌های اطلاعاتی این است که در هر زمان به اطلاعات نیاز باشد باید در دسترس قرار گیرند به‌همین منظور مفاهیمی نظیر مفاهیم مطرح شده در ذیل باید به درستی عمل کنند :

- سیستم‌های کامپیوتری که برای ذخیره و پردازش اطلاعات استفاده شده‌اند.
- کنترل‌های امنیتی که برای حفاظت آن‌ها استفاده می‌شوند.
- کانال‌های ارتباطی که برای دسترسی به آن‌ها استفاده می‌شوند.

یکی از مهمترین اهداف در سیستم‌های با دسترسی بالا این است که در همه حال اطلاعات در دسترس باقی بمانند. به این منظور باید از اختلال در خدمات بعلت قطع برق، خرابی‌های سخت افزاری و یا ارتقاء سیستم جلوگیری بعمل آید.

توجه: اطمینان از در دسترس بودن اطلاعات همچنین شامل جلوگیری از denial – of – service attaks می‌شود.

حساب پذیری: یعنی فعالیت‌های موجودیت‌ها در سیستم اطلاعاتی به صورت جداگانه قابل ردیابی و بررسی باشد.

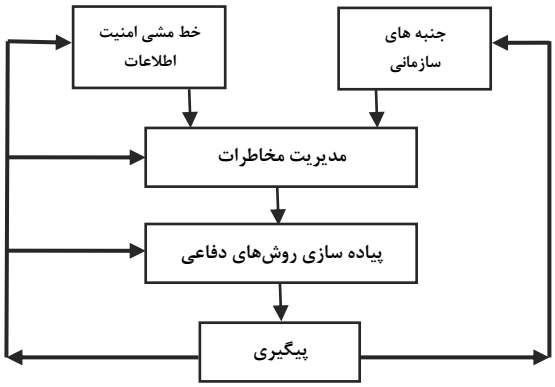
قابلیت اعتماد: یعنی رفتارها و نتایج مورد انتظار سازگار باشد.

1.6. اصول مهندسی امنیت

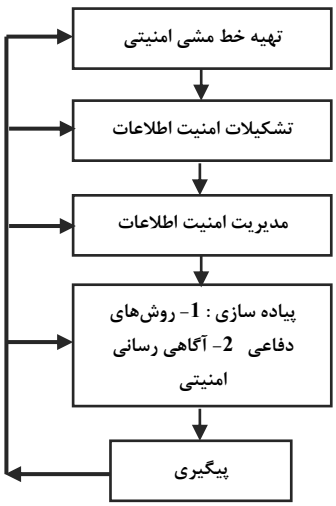
- امنیت فضای تبادل اطلاعات مفهومی کلان و مبتنی بر حوزه‌های مختلف دانش است.
- امنیت هر سیستم تعریف مخصوص به خود را دارد .
- امنیت ابزاری برای رسیدن به هدف سیستم است.
- امنیت نسبی است.
- امنیت سیستم طرحی یکپارچه و جامع را می‌طلبد.
- حیطه مسئولیت‌ها و مقررات امنیتی باید کاملاً شفاف و غیرمبهم باشد.
- طرح امنیتی باید مقرون به صرفه باشد.
- امنیت هر سیستم توسط عوامل اجتماعی محدود می‌شود.
- باید امنیت هر سیستم بطور متناوب مورد ارزیابی مجدد قرار گیرد.

1.7. چرخه حیات مهندسی امنیت

نمودارهای 1.2 و 1.3 ، چرخه حیات مهندسی امنیت را نشان می‌دهند.



نمودار1.2: چرخه حیات مهندسی امنیت



نمودار1.2: چرخه حیات مهندسی امنیت با جزئیات بیشتر

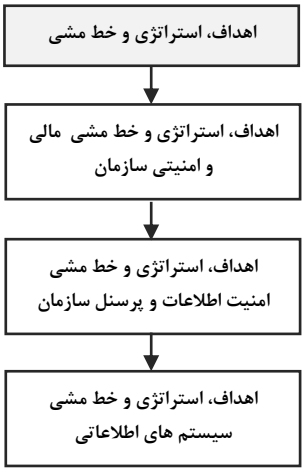
1.7.1. سلسله مراتب اهداف، استراتژی و خط مشی

برای ایجاد امنیت در یک سازمان، اولین قدم تدوین اهداف، استراتژی و خط مشی امنیتی سازمان است.

- اهداف (Objectives)
- استراتژی (Strategy)

- خط مشی (Policy)

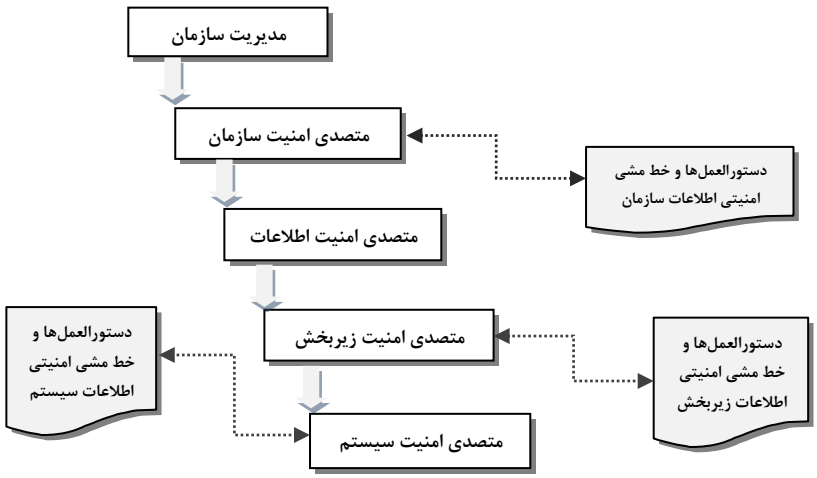
این سلسله مراتب در نمودار1.3 نشان داده شده است.



نمودار1.3: سلسله مراتب اهداف، استراتژی و خط مشی

1.7.2. جنبه‌های تشکیلاتی امنیت سازمان

به‌منظور پیاده‌سازی صحیح سیستم مدیریت امنیت اطلاعات در سازمان لازم است امنیت سازمانی دارای تشکیلات منظم و دقیق باشد. در رأس این تشکیلات مدیریت سازمان قرار می‌گیرد و همچنین هریک از رده‌های تشکیلاتی باید مقید به دستورالعمل‌های از پیش تعریف شده‌ای باشند. نمودار1.4 ارتباط بین این رده‌های تشکیلاتی را نشان می‌دهد.



نمودار1.4: تشکیلات امنیتی سازمان

1.8. مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع موجود در رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد. همچنین مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را برعهده داشته و درنهایت باید تلاش کند تا سیستم را همیشه به‌روز نگه دارد.

مدیریت امنیت اطلاعات مشتمل بر پیکربندی، مدیریت تغییرات و مدیریت مخاطرات است که در ادامه‌ی بحث هرکدام مورد بررسی قرار می‌گیرند.

فرآیندی است برای حصول اطمینان از اینکه تغییرات در سیستم تأثیر کنترل‌های امنیتی و به تبع امنیت کل سیستم را کاهش ندهد.

- مدیریت تغییرات

فرآیندی است که برای شناسایی نیازمندی‌های جدید امنیتی در هنگام بروز تغییر در سیستم IT انجام می‌شود. ایجاد روال‌های جدید، تجدید سخت افزارها، بروز رسانی نرم افزارها، اتصالات جدید شبکه و کاربران جدید از جمله تغییرات سیستم اطلاعات هستند.

- مدیریت مخاطرات

ریسک یا مخاطره عبارت است از احتمال ضرر و زیانی که متوجه یک دارایی سازمان (در اینجا اطلاعات) است. عدم قطعیت (در نتیجه مقیاس ناپذیری) یکی از مهمترین ویژگی‌های مفهوم ریسک است. طبعاً این عدم قطعیت به معنای غیر قابل محاسبه و مقایسه بودن ریسک‌ها نیست.

مدیریت مخاطرات فرآیندی است برای شناسایی و ارزیابی:

- دارایی‌های که بایستی حفاظت شوند
- تهدیدات
- رخنه‌ها
- آسیب‌ها
- مخاطرات
- روش‌های مقابله
- ریسک باقی مانده

1.9. ارزیابی کیفیت مهندسی امنیت

باید توجه داشت مهندسی امنیت تنها امنیت مربوط به کد برنامه (program) را بررسی نمی‌کند بلکه امنیت کل PLC و کلیه عوامل دخیل در آن را مدنظر قرار می‌دهد.

بنابراین برای ارزیابی کیفیت مهندسی امنیت باید در دو مرحله زیر صورت گیرد: