

۹) حیرت‌انگیز است در هر سازمان شامل چهار گام اصلی زیر است:

گام ۱- امن سازی: با بهره‌گیری از ابزارهایی نظیر: سیستم‌های رمزنگاری، فایروال، افراز افعال و ...

گام ۲- پایش: یک سازمانی بایست به‌طور پیوسته ابزار تشخیص عملیات مشکوک و مورد پایش قرار گیرد. ابزارهایی نظیر سیستم‌های تشخیص نفوذ (Intrusion Detection) یا تله‌عسل (HoneyPot) systems می‌توانند در این گام کمک کننده باشند.

گام ۳- آزمون نفوذ و آسیب پذیری: در این گام سعی می‌شود ساعاتی مورد تست امنیتی قرار گرفته و در صورت وجود آسیب پذیری، نقاط آسیب پذیر گزارش شود. اصطلاح استاندارد در این گام تحت عنوان Pen test (تست نفوذ) شناخته می‌شود.

گام ۴- مدیریت ریسک: مناسب با هر یک از گام‌ها و سیاست‌ها سازمانی به‌طور پیوسته سعی می‌شود تا امنیت سازمان در حد مورد انتظار برقرار باشد.

۱۵) سیاست‌های امنیتی (Security Policy):

سیاست‌های امنیتی حاوی نیازمندی‌های امنیتی یک سازمان و یا یک سیستم اطلاعاتی/ارتباطی است. در تعریف سیاست‌های امنیتی بایست با رافعتهای زیر به‌طور شفاف تعیین شده باشد:

- انواع اطلاعات موجود در سازمان و میزان دسترسی افراد به آنجا،
- افراد مسئول در سازمان بر اجرای اوقات حفاظتی،
- نقاط جلسه امنیتی و میزان اقدامات حفاظتی مورد نیاز.

- هک (Hack): به معنای کنکاش به منظور کشف حقایق و نحوه کار یک سیستم یا سند.
به کسی که اقدام مکرر را انجام می دهد هکر (Hacker) اطلاق می شود.

- له (Attack): تلاش برای نفوذ به سیستم های رایان معنای می شود. به کسی که چنین اقدامی را انجام می دهد حمله کننده (Attacker) اطلاق می شود.

به عبارت دیگر حمله به عنوان هک محسوب می شود یا به فراموشی می تواند در نظر گرفته شود.

هکر فراکار = حمله کننده

- آسیب پذیری (Vulnerability): به مشکل شناخته شده و یا مشکوک در طراحی، پیاده سازی، بیکری و یا عملکرد سخت افزار/نرم افزار یک سیستم کامپیوتری که موجب نفوذ در آن می شود، آسیب پذیری اطلاق می شود.

- رخنه (Breach): به نقض سیاست امنیتی در یک سیستم اطلاق می شود.

- نفوذ (Intrusion): هر مجموعه از اعمال که نتیجه آن نقض به گونه امنیتی (محرمانه، صحت یا دسترسی پذیری) شود، گوئیم در یک سیستم نفوذ

اتفاق افتاده است.

نکته: مجموعه اعمال می تواند عمدی یا غیر عمدی باشد. آنچه در نفوذ مهم است نقض یک ویژگی از بهر گونه امنیتی است. اما همه یک نفوذ عمدی در یک سیستم اطلاعاتی را به معنی نیست.

- مکانیزم امنیتی (Security mechanism): به هر روش، ابزار یا رویه ای که برای

اعمال یک سیاست امنیتی به کار می رود، یک مکانیزم امنیتی اطلاق می شود.