① مبانی امنیت داده:

امنیت داده مبتنی بر تحقق سه ویژگی

۱ محرمانگی (confidentiality) به معنای عدم افشای غیرمجاز داده‌ها،

۲ صحت (Integrity) به معنای عدم دستکاری افراد یا نرم‌افزارهای غیرمجاز،

۳ دسترس‌پذیری (Availability) به معنای دسترسی افراد مجاز به داده‌ها در هر زمان و مکان،

تعریف می‌شود. به سه ویژگی بالا در امنیت اطلاعات سه‌گانه امنیتی (Security Triad) گفته می‌شود.

② محرمانگی:

ویژگی امنیتی محرمانگی در حوزه زیر تقسیم‌بندی می‌شود:

- محرمانگی داده (Data confidentiality): این ویژگی ضمانت می‌کند که داده‌های محرمانه و حساس به افراد غیرمجاز افشا نمی‌شود.

- حفظ حریم خصوصی (Privacy): این ویژگی ضمانت می‌کند که افراد بر روی نحوه جمع‌آوری، ذخیره‌سازی و انتشار یا افشای داده‌های خصوصی خود توسط دیگران، کنترل و تأثیر دارند.

③ مرور - سوال: مفاهیم Security، Secrecy، Privacy، Confidentiality

نسبت به یکدیگر در چه جایگاهی قرار دارند؟

④ مکانیزم های متداول برای عینیت بخشیدن و تضمین محرمانگی، بهره گیری از ابزارهای رمزنگاری و کنترل دسترسی می باشد.

⑤ صحت:

در یک دسته بندی کلی، صحت به دو ویژگی زیر تقسیم می شود:

- صحت داده (Data Integrity): این ویژگی تضمین می کند داده ها و یا برنامه ها توسط افراد یا نرم افزارهای غیرمجاز دستکاری (یا تغییر) نمی شوند.

- صحت منبع (Origin Integrity): این ویژگی درستی و صحت منبع (فرستنده) اطلاعات را تضمین می کند.

⑥ مکانیزم های متداول برای ایجاد ویژگی صحت در سامانه، بهره گیری از ابزارهای امضای دیجیتال (رقمی)، کدهای احراز اصالت پیام و کنترل دسترسی می باشد.

⑦ دسترس پذیری:

وجود این ویژگی در یک سامانه تضمین می کند که دسترسی به داده و سرویس های مجاز در هر زمان و مکانی برقرار خواهد بود.

برخی مکانیزم های متداول برای ایجاد چنین ویژگی در یک سامانه عبارتند از: وجود نسخه های پشتیبان، داشتن سیستم های پایش و توزیع بالا، تکرار داده و سرویس و ...

۸) دلایل ناامنی سامانه‌ها

ناامنی در سامانه‌های کامپیوتری می‌تواند دلایل فراوانی داشته باشد (یا انفعال) در یک دسته‌بندی کلی می‌توان سه سبب زیر را برای آنها در نظر گرفت:

۱- ضعف فناوری: که می‌تواند ناشی از مولفه‌های نرم‌افزاری و سخت‌افزاری سامانه نظیر پروتکل‌های به کار گرفته شده، سیستم عامل مورد استفاده و یا حتی تجهیزات سخت‌افزاری باشد.

۲- ضعف تنظیمات: مواردی همچون رها کردن تنظیمات پیش‌فرض سایر مولفه‌های سامانه، انتخاب گذرواژه‌های نامناسب و غیرایمن، عدم توجه به اعمال تنظیمات امنیتی مربوط به سامانه (مقاوم‌سازی امنیتی) و بسیاری موارد مشابه دیگر می‌تواند سبب ناامنی سامانه شود.

۳- ضعف سیاست‌گذاری: مواردی همچون عدم وجود سیاست امنیتی، عدم وجود طرح و برنامه برای مقابله و بازیابی حوادث و نداشتن نظارت امنیتی پیوسته و مناسب می‌تواند سبب ایجاد ناامنی در سامانه گردد.

نکته ۱: از میان دسته‌بندی‌های ذکر شده در بالا، تنها ضعف تنظیمات و ضعف سیاست‌گذاری است که می‌تواند توسط سازمان‌ها مدیریت شود و ضعف فناوری در این میان خارج از کنترل و مدیریت سازمان‌ها است.

نکته ۲: «دلایل ناامنی سامانه‌ها صرفاً نگرش فنی نیست و نگرش مدیریتی به مسئله امنیت نیز لازم است.» مورد ۳ در موارد بالا، گویای این مهم است.