تهدیدات رایانه واینترنت

مفاهیم امنیت در شبکه

اصول امنیت:

۱. *محرمانگی*
۲. *احراز هویت*
۳. *صحت داده*
۴. *کنترل دسترسی*
۵. *در دسترس بودن*

حمله (Hack)

- **تعریف حمله**

هرگاه یکی از اصول امنیت نقض گردد

- **انواع حمله:**

۱. دسترسی غیرمجاز به منابع و اطلاعات از طریق شبکه
۲. دستکاری غیرمجاز اطلاعات بر روی یک شبکه
۳. حملاتی که منجر به اختلال در ارائه سرویس می شوند

تهدیدات رایانه وشبکه

- ویروس
- خطرات ایمیل
- شنودگرهاوکی لاگرها:
  - کنترل فعالیت کاربران
  - جمع آوری اطلاعات
- شناسایی و ردیابی کاربران
- حملات هکرها

ویروس

- **ویروس چیست؟**
- **اهداف ویروس چیست؟**
- **انواع ویروس:**
  - اسب تروا
  - کرم
  - بمب منطقی
  - ترس افزار
  - ...

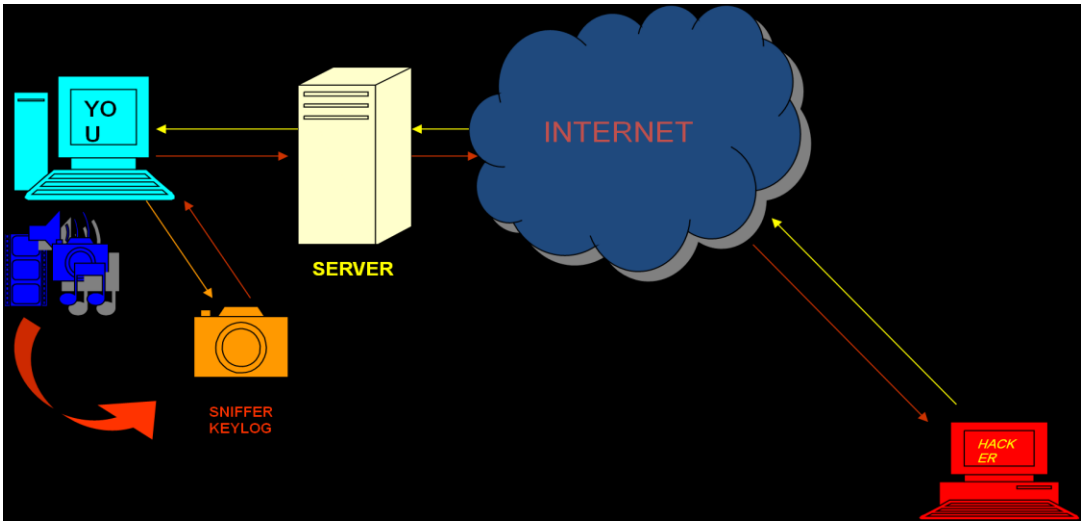
راههای نفوذ ویروس ها

- دیسکتهای آلوده (انواع مختلف)
- پست الکترونیکی
- برنامه ها ونرم افزار های آلوده
- شبکه های مختلف رایانه ای
- نقض قانون کپی رایت

تهدیدات ایمیل

- خطرات ویروسهای ایمیل و اسبهای تروا
- خطر نشت و فاش شدن اطلاعات
- خطر ایمیلهای دربردارنده محتویات بدخواهانه یا اهانت آور
- اسپم ها(ایمیلهای ناخواسته)

keylogger عملکردتروجان حامل



Spam

- ✓ Spam:نامه های الکترونیکی ناخواسته
- ✓ اسپم ((Spamیعنی نامه های الکترونیکی ای که از منابع نامشخص و یا ناشناخته ارسال و دریافت می شود.
- ✓ به آن دسته از نامه های الکترونیکی ناخواسته ای که به صورت «انبوه» برای افراد یا موسسات ارسال می شود.
- ✓ سیمانتک درخصوص گسترش هرزنامه ها (اسپمها) و برنامه های مخرب اطلاع داد که 90/4 درصد از مجموع نامه های الکترونیکی که کاربران دریافت می کنند هرزنامه هستند.
همچنین ارسال این هرزنامه ها در ماه می 2009 نسبت به ماه آوریل 5/1 درصد افزایش یافته است.

ضد ویروس

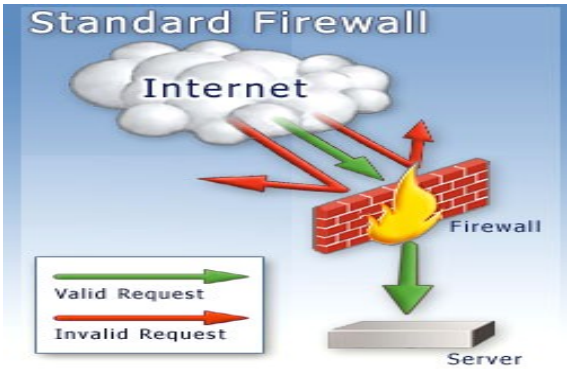
یک نرم افزار Anti Virus که به اختصار آنرا AV می نامیم با مشاهده و بررسی محتوای فایل ها به دنبال الگوهای آشنای ویروسها یا کرم های اینترنتی می گردند. در صورت مشاهده این الگوها که به آن Virus Signature گفته می شود، از ورود آن به کامپیوتر شما و اجرا شدن جلوگیری می کنند و یا به شما هشدار لازم را می دهند و از شما دستور میگیرند که آیا فایل را حذف کنند و یا سعی در اصلاح آن نمایند.

شرکتهای سازنده آنتی ویروس با آمدن ویروسهای جدید، الگوهای نرم افزاری آنها را کشف و جمع آوری می کنند و به همین علت اغلب لازم است تا این نرم افزارها هر چندگاهی به روز (Update) شوند تا الگوهای جدید ویروسها را بشناسند.

محافظت در مقابل خطرات ایمیل

- ایمیلهای ناشناخته را باز نکنید
- استفاده ازضدویروس یا دیوار آتشین

فایروال



کلمه عبور:

- کلمه عبور حداقل 6 کراکتر باشد.
- کلمه عبور ترکیبی از حروف کوچک و بزرگ، اعداد و کراکترهای ویژه باشد.
- کلمه عبور قابل حدس زدن نباشد.
- کلمه عبور در زمان تایپ کردن قابل تشخیص نباشد.
- کلمه عبور از کلمات عبور متداول نباشد.
- کلمه عبور مرتبا تغییر کند.

یازده نکته برای امنیت رایانه ها وشبکه ها :

۱ - استفاده از نرم افزارهای محافظتی
۲ - باز نکردن نامه های دریافتی از منابع ناشناس
۳ - استفاده از گذرواژه های مناسب
۴ - محافظت از کامپیوتر در برابر نفوذ توسط فایروال
۵ - خودداری از به اشتراک گذاشتن منابع کامپیوترواسناد دارای طبقه بندی در شبکه
۶ - قطع اتصال به اینترنت در رایانه های اداری و مواقع عدم استفاده در رایانه های شخصی
۷ - تهیه پشتیبان از داده های موجود بر روی کامپیوتر
۸ - گرفتن منظم وصله های امنیتی
۹ - بررسی منظم امنیت کامپیوتر
۱۰ -حصول اطمینان از آگاهی اعضای خانواده و کارمندان از نحوه برخورد با کلمپیوترهای آلوده
۱۱ -عدم ارائه آدرس پست الکترونیکی خود به افراد ناشناس