فصل سوم: جرایم رایانه ای و اینترنتی

امنیت در فا

- مبحث امنیت در فناوری اطلاعات از همیت بالایی بر خوردار است.
  - حفاظت از اطلاعات محرمانه شامل اطلاعات مشتریان و پرسنل
  - حفاظت در مقابل رفتار های بدخواهانه نظیر دزدی یا اختلال
  - اهمیت تعادل در صرف هزینه به منظور امنیت با سایر نیاز های سازمان

پیچیدگی سامانه ها و نیاز به افزایش امنیت

- امروزه سامانه های فناوری اطلاعات از نظر دامنه سامانه و افزایش خطوط برنامه نویسی نسبت به گذشته پیچیده تر شده است.
- به هر اندازه که یک سامانه توسعه یابد احتمال به وجود آمدن نقاط نفوذ به سامانه توسط بدخواهان افزایش می یابد.

افزایش انتظارات از کاربران

- امروزه در تمامی سطوح از جمله سطوح دفتری توقع استفاده از رایانه وجود دارد.این افراد ممکن است در صورت ندیدن آموزش مناسب یا به دلایل دیگر ضعف هایی در استفاده از رایانه از خود بروز دهند.
  - تایید هویت نادرست مراجعه کنندگانی که می خواهند از سیستم اطلاعاتی را دریافت نمایند.
  - کاربرانی که نام کاربری و رمز عبور خود را به دیگران می دهند تا وظایفی را به جای آن ها به انجام رسانند!

تهدید ناشی از فناوری جدید

- شبکه بندی
  - اتصال رایانه ها به میلیون ها رایانه دیگر می تواند منجر به نفوذ پذیری از طریق خطوط شبکه بندی بینابین آن ها شود.
- تغییرات پیوسته سیستم ها و به طبع آن تغییرات سازمانی گسترده در حوزه فا
- استفاده از سیستم های جدید که می توانند پتانسیل نفوذ پذیری یا دچار شکستگی (break) شدن را داشته باشد.

نمودار تعداد حملات مخرب سایبری

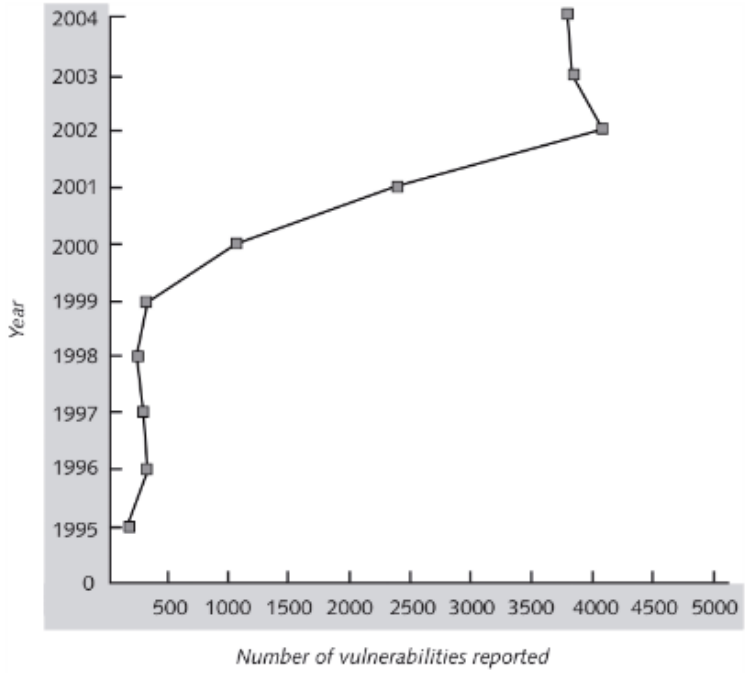


FIGURE 3-1 Number of vulnerabilities reported to CERT/CC

انواع حملات مرتبط با فا

- حملات ویروسی
- حملات کرم
- حملات تروجان
- عملیات فقدان سرویس دهی یا Denial of service

ویروس

- قطعه ای کد که معمولا با وانمود کردن خود به عنوان یک برنامه عادی بر روی سیستم اشخاص نصب می شود.
- منجر به نتایج غیر قابل انتظار می شود.
- معمولا به فایل ها متصل می شود.
- حداکثر توان سیستم را مصرف می نماید.

کرم ها

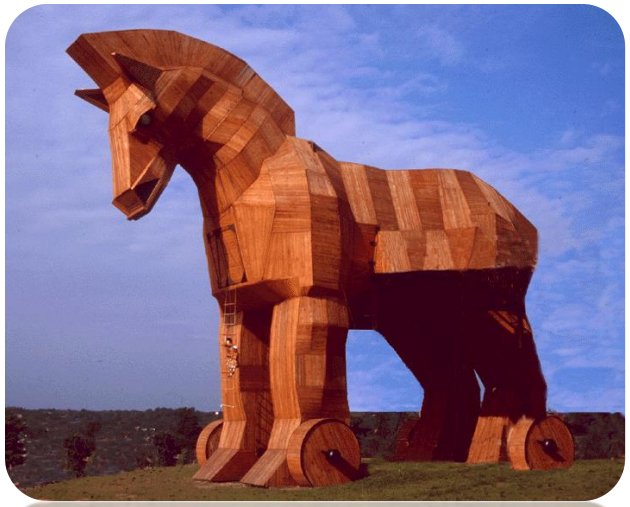
- بر روی حافظه رایانه تکثیر می شود.
- بدون اختیار اشخاص بر روی رایانه فرد نصب می شودو فعالیت می کند.
- اثرات مخرب بر روی رایانه فرد به جا می گذارد.
  - از دست رفتن داده های رایانه
  - از دست دادن توان سیستم

خسارت های ناشی از کرم

نام کرم	سال ایجاد	خسارت
iloveuou	2000	8.75 billion $
Code red	2001	2.62 billion $
sircam	2001	1.15 billion $
Mellissa	199	1.1 billion $

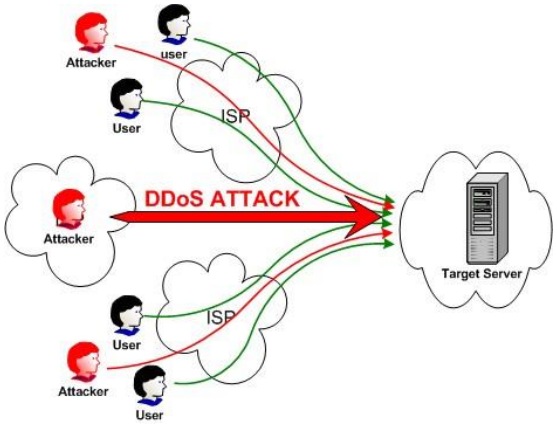
تروجان

- برنامه ای که هکر با فریب کاربر بر روی رایانه وی نصب می کند یا این که کاربر را ترغیب می کند که آن را نصب کند.
- بمب های منطقی
  - **برنامه هایی که تحت شرایط خاصی عمل می کنند.**



عملیات denial of service

- ارسال درخواست های زیاد از سوی گروه بدخواه به سوی سیستم تا سرور کاملا از کار بیفتد و کاربران واقعی نتوانند از سرویس استفاده نمایند.
- ارسال درخواست های سنگین به سرور از سوی گروه بدخواه به منظور از کار انداختن زود تر سرویس انجام می شود.



هکر ها و کراکر ها

- هکر : افرادی که محدودیت های سیستم را از روی حس کنج کاوی آزمون می نمایند.
- کراکر : به هکر بدخواه کراکر می گویند.در حقیقت کراک دو ویژگی خاص دارد
  - نوعی هک است.
  - به وضوح مجرمانه است.

کارکنان بدخواه!

- مهم ترین نگرانی امنیتی سازمان ها
- حدود ۸۵ درصد از جرایم مرتبط با سامانه های فا مشمول این رده می باشد.
- معمولا ناشی از رویه ضعیف در کنترل داخلی سیستم و سازمان است.
- یکی از موارد اتفاق این موارد سازمان هایی است که برای اعضا دامنه دسترسی به اطلاعات تعریف نشده است.

جاسوسان صنعتی

- دسترسی به راز های تجاری رقبا به صورت غیر قانونی
- هوش رقابتی : به شکل قانونی کسب اطلاعات تجاری رقبا می گوییم.
  - با استفاده از روش های قانونی
  - جمع آوری اطلاعاتی که در درسترس عموم می باشد.

تروریست سایبری

- راهکاری برای وادار کردن دولت به پذیرش اعتراضات سیاسی و یا اجتماعی
- یکی از انواع حملات رایانه ای
- تخریب سامانه های رایانه ای به نحوی که منجر به کشته شدن افرادی گردد.
- نفوذ به سامانه اطلاعاتی یک پادگان نظامی که منجر به انفجار پایگاه گردد.

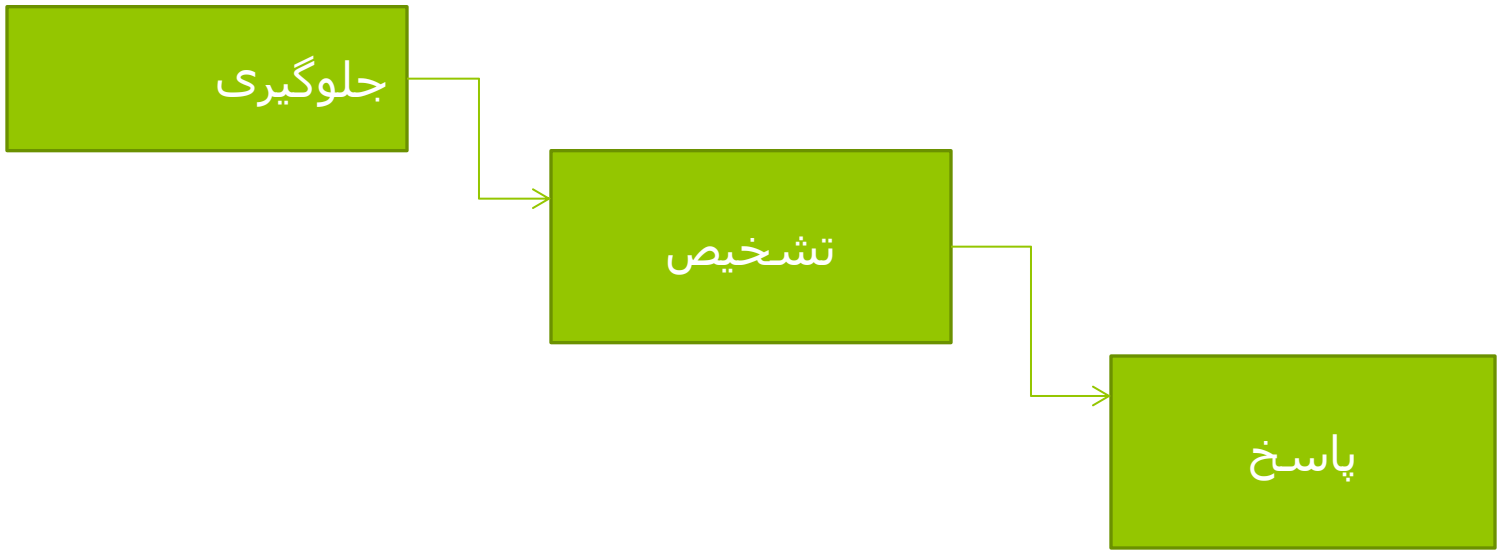
راهکار های کاهش آسیب پذیری

- امنیت
  - ترکیبی از مشی امنیتی و فناوری و کاربران
  - نیازمند گستره ای از فعالیت ها به منظور تامین امنیت
- معین کردن اعمالی که بیشترین خطر آسیب پذیری را برای سامانه فراهم می کند.
- آموزش کاربران
- ایجاد یک برنامه مدون برای پاسخ به خطر احتمالی

فراهم کردن خط مشی امنیتی

- خط مشی امنیتی دو مورد را در بر می گیرد:
  - نیاز های امنیتی سازمان
  - کنترل ها و محدودیت هایی که نیاز های فوق را تامین می کند.
- خطی مشی امنیتی معین نمی کند که چگونه یک راه کار امنیتی را پیاده سازی کنیم بلکه معین می کند چه راهکار امنیتی را باید پیاده سازی نماییم.
- باید خطی مشی های سامانه های اطلاعاتی که از سوی سازنده پیاده سازی شده با خط مشی های سازمانی ما هماهنگ باشد.

چارچوب یک خط مشی امنیتی



پیشگیری

- استفاده از آنتی ویروس
- تعیین نقش کارکنان شرکت و سطوح دسترسی اطلاعاتی آن ها با کمال دقت
- بستن روزنه ها
  - کنترل تمامی مجوز های دسترسی در پایگاه دسترسی سامانه(در سیستم های کوچک حذف تمامی کاربران سیستم به صورت دوره ای و لزوم در خواست مجدد آن ها برای دریافت اکانت توصیه می شود)

تشخیص خطا

- پایش فعالیت های شبکه و سامانه های اطلاعاتی
- مبتنی بر شیوه های رفتاری
  - مقایسه رفتار فعلی سیستم با رفتار مورد انتظار

تشخیص خطا(ادامه)

- مکانیزم کاسه عسل :
  - در معرض گذاشتن اطلاعات سازمان به صورتی که آن اطلاعات عملا اطلاعات درستی در مورد سامانه نمی باشد.
  - تصور هکران در این مورد که به اطلاعات مورد نیاز خود رسیده اند و از کاویدن بیشتر در سیستم صرف نظر می نمایند.

پاسخ دهی

- باید مکانیزمی کامل به منظور پاسخ دهی به هر گونه رخنه امنیتی وجود داشته باشد.
- در یک مکانیزم پاسخ دهی باید دقیقا معین شود که در هنگام رخداد یک نفوذ به سیستم:
  - چه کسانی باید مطلع گردند؟
  - چه کسانی نباید مطلع گردند؟

منابع

- Ethics in Information Technology, George W. Reynolds,3rd edition,2010.