سمینار

امنیت در فناوری اطلاعات

انجمن مهندسین برق و الکترونیک ایران – شاخه اصفهان

بهزاد کشانی

خرداد ماه ۹۱

سرفصل مطالب

بخش اول : مفاهیم و مبانی امنیت

بخش دوم : تهدیدها و آسیب پذیریها

بخش سوم : پیشگیری و مقابله

بخش چهارم: مدیریت امنیت

بخش اول : مفاهیم و مبانی امنیت

۱– تعاریف
۲–لزوم امنیت در فناوری اطلاعات
۳– مباحث قانونی در فضای سایبر
۴– طبقه بندی اطلاعات رخدادهای امنیتی

بخش اول : مفاهیم و مبانی امنیت
۱– تعاریف

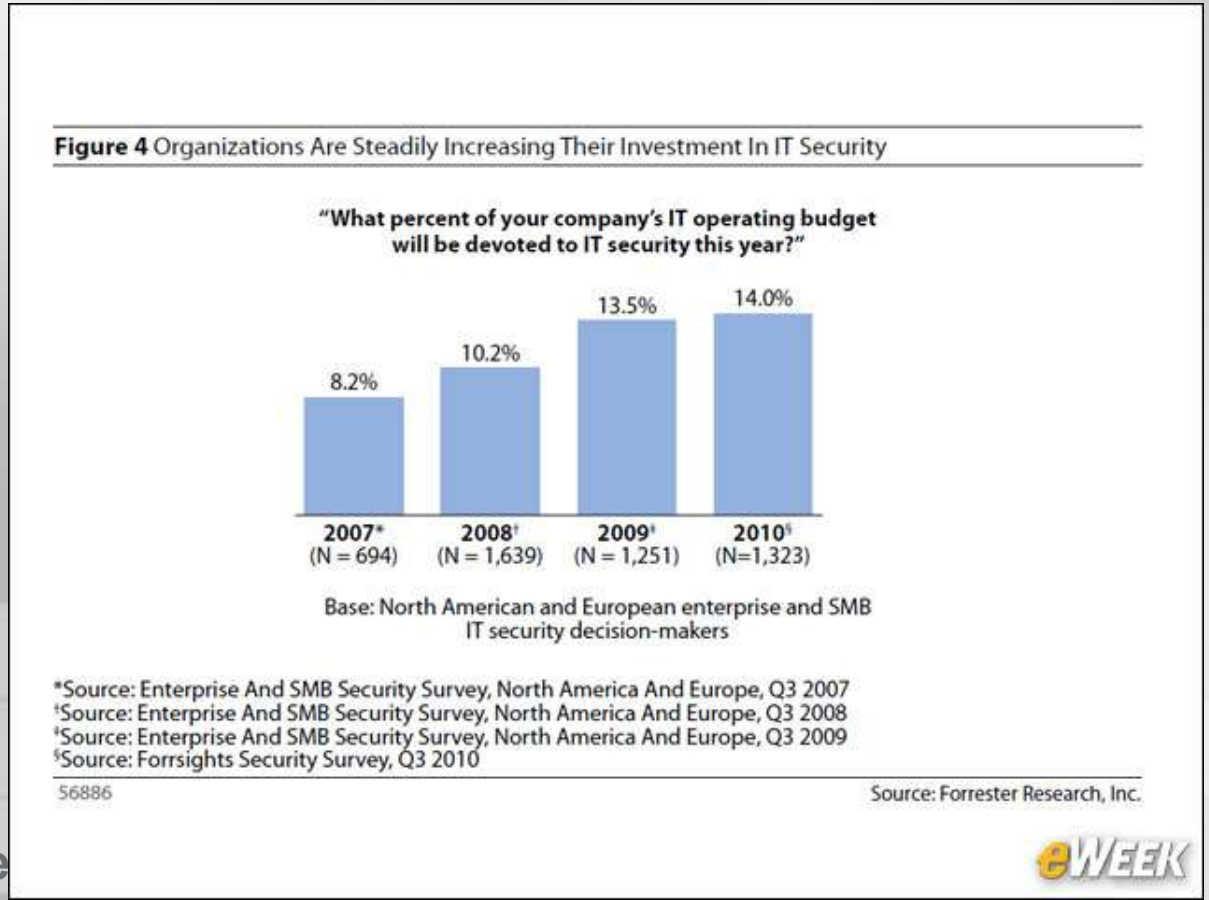
- **امنیت**
  - دوری از خطر، در معرض خطر نبودن
- **خطر**
  - در معرض آسیب دیدگی یا از دست دادن
- **فناوری اطلاعات**
  - جمع آوری، پردازش، ذخیره سازی، انتشار و انتقال اطلاعات از طریق سیستم های الکترونیکی و ارتباطی
- **فضای سایبر**
  - محیط ارتباطی الکترونیکی و شبکه های کامپیوتری

بخش اول : مفاهیم و مبانی امنیت
۲– لزوم امنیت در فناوری اطلاعات

- ارزش اطلاعات
  - اطلاعات شخصی
  - اطلاعات و تعاملات درون و برون سازمانی
  - تبادل اطلاعات مالی
  - اطلاعات سیاسی و اقتصادی
  - و ...

بخش اول : مفاهیم و مبانی امنیت
۲– لزوم امنیت در فناوری اطلاعات

- بودجه امنیت فناوری اطلاعات
  - بودجه فناوری اطلاعات سازمانها (۴ درصد گردش مالی)
  - بودجه امنیت فناوری اطلاعات



بخش اول : مفاهیم و مبانی امنیت
۳– مباحث قانونی در فضای سایبر

- قرارداد
  - توافق با کلیک در وب
  - امضای دیجیتال
- خرید مجوز استفاده
- سرمایه فکری
- حق الامتیاز
- علامت تجاری
- حریم خصوصی
- تهمت و افترا

بخش اول : مفاهیم و مبانی امنیت
۳– مباحث قانونی در فضای سایبر

- بی نزاکتی و هرزگی
- دعوی قضایی
  - جمع آوری شواهد و مدارک
  - حوزه صلاحیت دادگاه
- قوانین جزایی
- تحقیق و بازجویی
- توقیف رسانه
- مستندسازی

بخش اول : مفاهیم و مبانی امنیت
۴– طبقه بندی اطلاعات رخدادهای امنیتی

- رخداد
- حمله
- حادثه

بخش اول : مفاهیم و مبانی امنیت
۴– طبقه بندی اطلاعات رخدادهای امنیتی

بخش اول : مفاهیم و مبانی امنیت
۴– طبقه بندی اطلاعات رخدادهای امنیتی

بخش دوم : تهدیدها و آسیب پذیریها

۱– تهدیدات فیزیکی
۲– تهدیدات علیه کنترل دسترسی
۳– تهدیدات مرتبط با معماری سیستم
۴– تهدیدات علیه شبکه
۵– تهدیدات علیه برنامه های کاربردی و سیستم
۶–تهدیدات اینترنتی

بخش دوم : تهدیدها و آسیب پذیریها
۱– تهدیدات فیزیکی

- حوادث طبیعی
  - طوفان
  - سیل
  - زلزله
  - آتش سوزی
- تهدیدات انسانی
  - تروریست
  - خرابکار
  - دزدی
  - خطای انسانی عمدی
  - خطای انسانی غیر عمد

بخش دوم : تهدیدها و آسیب پذیریها
۱– تهدیدات فیزیکی

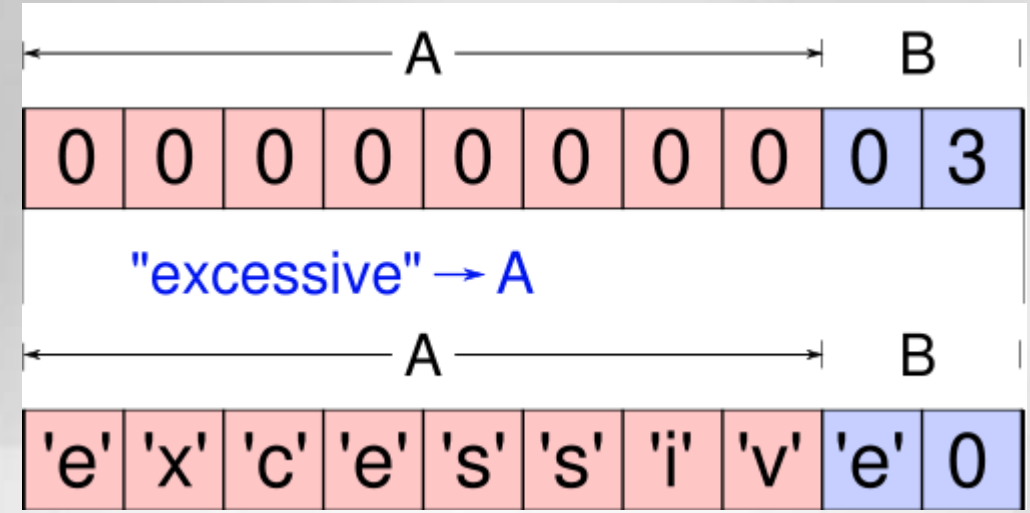
- شرایط اضطراری
  - قطعی ارتباط
  - قطع خدمات عمومی (برق، گاز، آب و ...)
  - خرابی تجهیزات

بخش دوم : تهدیدها و آسیب پذیریها
۲– تهدیدات علیه کنترل دسترسی

- حمله رمز عبور (Password Attack)
- شکستن رمز عبور توسط واژه نامه (Dictionary Crack)
- Brute-Force Crack
- تایپ رمز عبور و لورفتن آن
- استراق سمع
- ثبت فعالیت صفحه کلید (Keylogger)
- حمله ممانعت از سرویس Denial of Service (DoS)
- مهندسی اجتماعی

بخش دوم : تهدیدها و آسیب پذیریها
۳– تهدیدات مرتبط با معماری سیستم

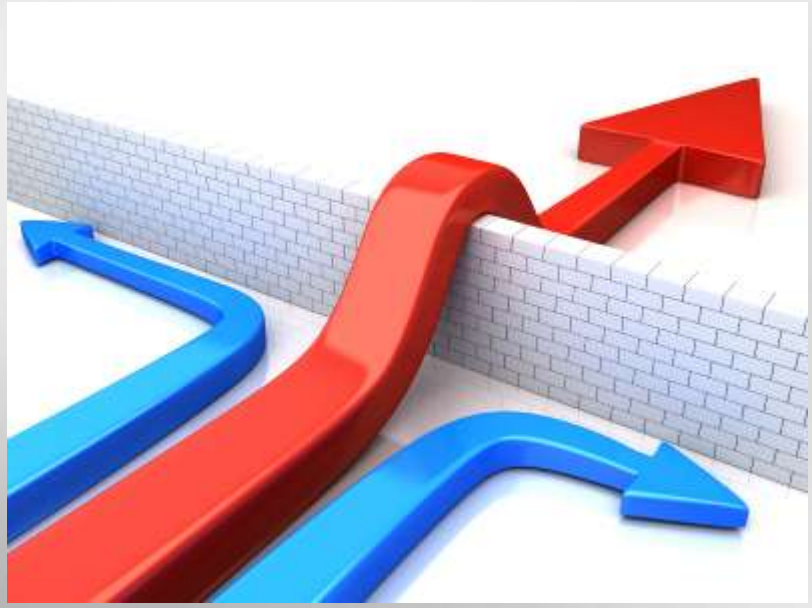
- سرریز حافظه (Buffer Overflow)
- کانال مخفی (Covert Channel)
- حمله افزایشی (Incremental Attacks)



بخش دوم : تهدیدها و آسیب پذیریها
۴– تهدیدات علیه شبکه

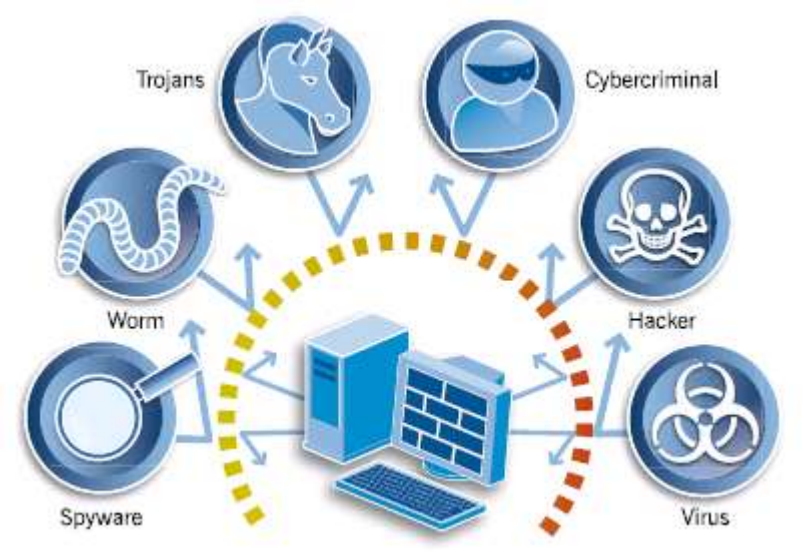
- حمله ممانعت سرویس
  - Ping of death
  - SYN Flood
- حمله های افشاء
  - بو کشیدن Sniffing
  - مسموم کردن ARP poisoning
  - حقه بازی DNS spoofing
  - War dialing
  - War driving

بخش دوم : تهدیدها و آسیب پذیریها
۴– تهدیدات علیه شبکه



- حمله تخریب، تغییر و یا دزدی
  - حمله به بانک اطلاعاتی
  - تغییر اطلاعات بانک اطلاعاتی
  - دزدی شناسه ها
  - افزایش سطح دسترسی
  - Session hijacking
  - نامه های ناخواسته Spam
- حمله های شناسایی
  - جستجوی آدرس IP Probes
  - پویش پورت Port Scan
  - پویش آسیب پذیریها Vulnerability Scan
  - آشغال گردی Dumpster Diving

بخش دوم : تهدیدها و آسیب پذیریها
۵– تهدیدات علیه برنامه های کاربردی و سیستم



- ویروس Virus
- کرم Worm
- اسب تراوا Trojan
- سرریز حافظه
- حمله ممانعت از سرویس
- ورودی نامناسب SQL Injection
- جاسوس افزار Spyware
- بمب منطقی Logic Bomb
- Adware
- Rootkit

بخش دوم : تهدیدها و آسیب پذیریها
۵– تهدیدات اینترنتی

- از بین بردن شهرت سازمان
- انتشار و استفاده از اطلاعات غلط
- گول زنک ها
- تهدیدها
- کدهای مزاحم
- نامه های ناخواسته
- نامه های زنجیره ای
- روشهای پولدار شدن
- طوفان پستی
- دزدی نرم افزار
- دزدی ادبی
- هک کردن تبهکارانه

بخش دوم : تهدیدها و آسیب پذیریها
۵– تهدیدات اینترنتی

- حراج شبکه ای
- قمار بازی شبکه ای
- خرید از طریق وب
- بازی ها
- جاسوس افزارها
- اعتیاد اینترنتی
- گروههای نفرت (افراطی)
- هرزه نگاری

بخش سوم : پیشگیری و مقابله

۱–پیشگیری و مقابله با تهدیدات فیزیکی
۲– پیشگیری و مقابله با تهدیدات علیه کنترل دسترسی
۳–پیشگیری و مقابله با تهدیدات مرتبط با معماری سیستم
۴– پیشگیری و مقابله با تهدیدات علیه شبکه
۵–پیشگیری و مقابله با تهدیدات علیه برنامه های کاربردی و سیستم
۶– عملیات امنیتی
۷– پشتیبانی داده ها و بایگانی

بخش سوم : پیشگیری و مقابله
۱– تهدیدات فیزیکی

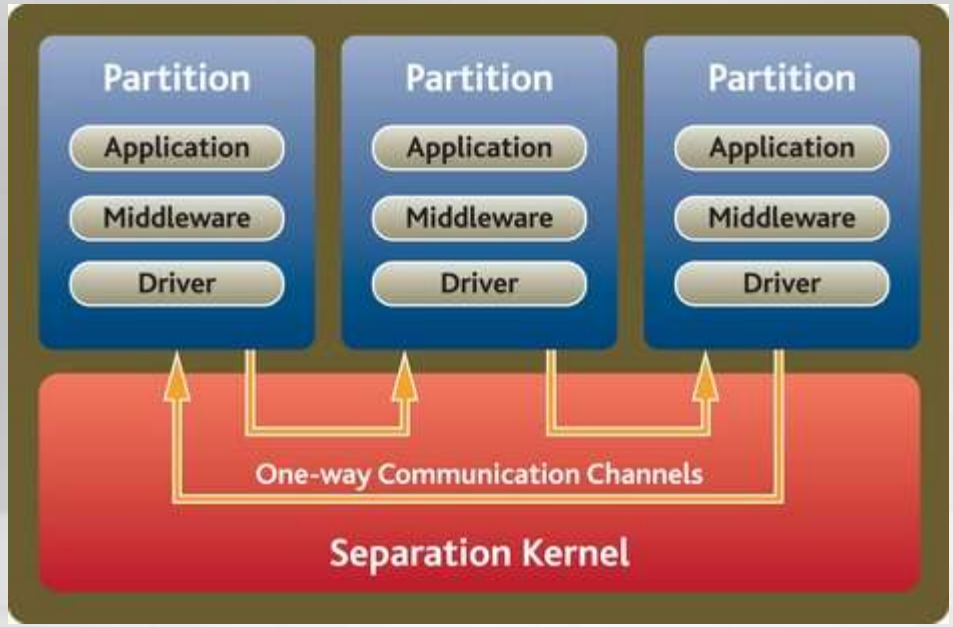
- پیش بینی سایت جایگزین
- ساختمان و ارتباطات مقاوم در برابر عوامل طبیعی
- روشهای حفاظت از ساختمان
- سیستم های کنترل و نظارت
  - دربها و ابزارهای کنترلی ویژه
  - دوربینهای مداربسته
- سیستمهای اعلام و اطفای حریق
- پیش بینی UPS ، ژنراتور و یا سرویس جایگزین
- نگهداری دوره ای انواع تجهیزات
- آموزش کارکنان

۲– تهدیدات علیه کنترل دسترسی

- احراز هویت
  - بر اساس آنچه می دانید نظیر نام کاربری رمز عبور
  - بر اساس آنچه دارید نظیر نشانه (Token) ، کارت هوشمند ،کارتهای مغناطیسی
  - بر اساس آنچه هستید نظیر مشخصه های زیستی (اثر انگشت، فرم دست، شکل قرنیه چشم و ...)
  - بر اساس آنچه انجام می دهید نظیر سرعت تایپ
- طبقه بندی اطلاعات و دسترسیها
- سیستمهای تشخیص نفوذ
- تست نفوذ
- Honeypot
- سیستمهای رمزنگاری تبادل رمز عبور
- آموزش به کاربران

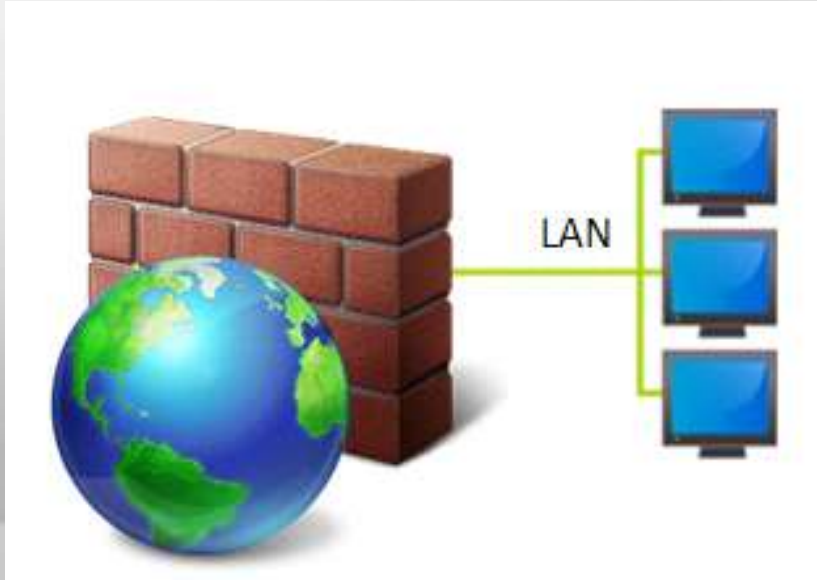
بخش سوم : پیشگیری و مقابله
۳–تهدیدات مرتبط با معماری سیستم

- مدیریت و کنترل حافظه سیستم
- جدا سازی پروسس ها
- توصیه های تولید کنندگان زیرساختی (نرم افزار و سخت افزار)
- مکانیزم تضمین اعتبار سیستم



بخش سوم : پیشگیری و مقابله
۴– تهدیدات علیه شبکه

- انتخاب صحیح توپولوژی و پروتکل شبکه ها
- سیستم های IDS و IPS
- دیواره آتش Firewall
- پروتکلهای رمزنگاری
- پیکربندی امن تجهیزات شبکه
- نگهداری و امحای امن تجهیزات و مستندات
- آموزش کاربران



بخش سوم : پیشگیری و مقابله
۵–تهدیدات علیه برنامه های کاربردی و سیستم

- انتخاب سیستم عامل و برنامه کاربردی مناسب
- به روز رسانی سیستم عامل و برنامه های کاربردی
- ابزارهای ضد ویروس و ضد جاسوسی و به روز رسانی آنها
- دیواره آتش شخصی Personal Firewall
- مدیریت بانک اطلاعاتی و توجه به امنیت آن
- استفاده از راهنماهای امنیتی تولید کنندگان

بخش سوم : پیشگیری و مقابله
۶– عملیات امنیتی

- سیاستهای امنیتی سازمان و کارکنان
  - استخدام
  - گردش مشاغل
  - جدا شدن کارکنان
  - مجوزهای قبلی
  - مرخصی اجباری
- بازرسی ، گزارش و نظارت
  - فیزیکی
  - شبکه
  - برنامه کاربردی
  - سرویسها
  - رعایت الزامات قانونی
- هک اخلاقی (Ethical Hacking)
- آموزش کارکنان

بخش سوم : پیشگیری و مقابله

۷– پشتیبانی داده ها و بایگانی

- ضرورت
- تهیه پشتیبان
  - تهیه پشتیبان موازی
  - ثبت وقایع
  - نرم افزارهای مربوطه
- مستند سازی
- نگهداری مناسب
- راهبردهای بازیابی
- رویه های جبران و مسئولیتها
- آموزش به کاربران

بخش چهارم : مدیریت امنیت

۱– سیستم مدیریت امنیت اطلاعات

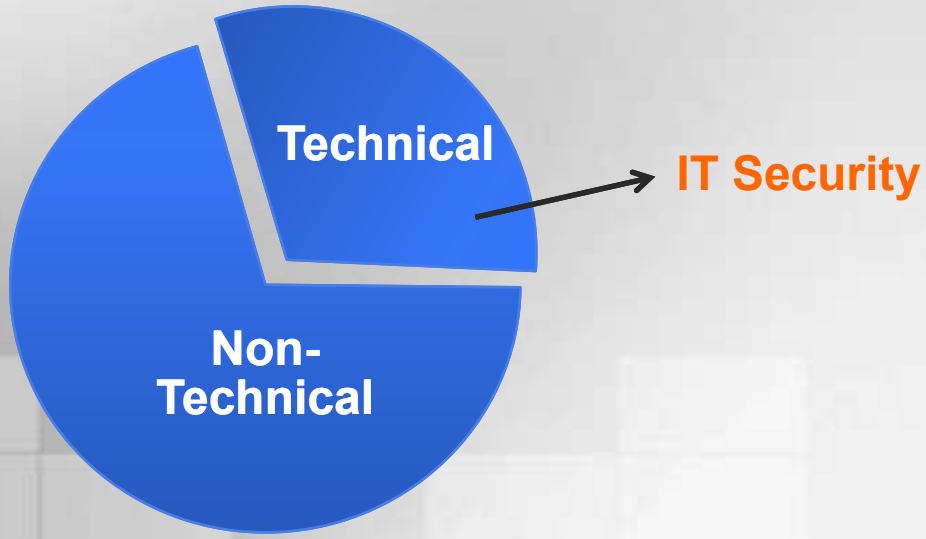
بخش چهارم : مدیریت امنیت

۱– سیستم مدیریت امنیت اطلاعات

- مؤلفه های امنیت اطلاعات
  - محرمانگی
  - در دسترس بودن
  - صحت
- سیستم مدیریت امنیت
  - قسمتی از سیستم مدیریت کلان، بنا شده بر دیدگاه مخاطرات کسب و کار، به منظور ایجاد، پیاده سازی، اجرا، پایش، بازنگری و نگهداری و بهبود امنیت اطلاعات

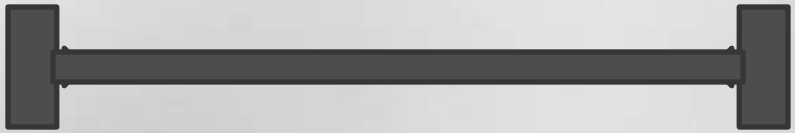
بخش چهارم : مدیریت امنیت
۱– سیستم مدیریت امنیت اطلاعات

- تامین امنیت اطلاعات فنی است یا غیر فنی؟
  - ۳۰ درصد فنی، ۷۰ درصد غیر فنی
- آیا امنیت یک محصول است ؟

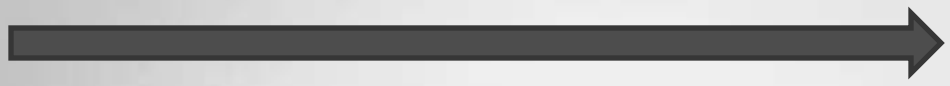


بخش چهارم : مدیریت امنیت
۱– سیستم مدیریت امنیت اطلاعات

- امنیت، پروژه یا فرآیند؟
  - Project : یک نقطه آغاز و یک نقطه پایان دارد

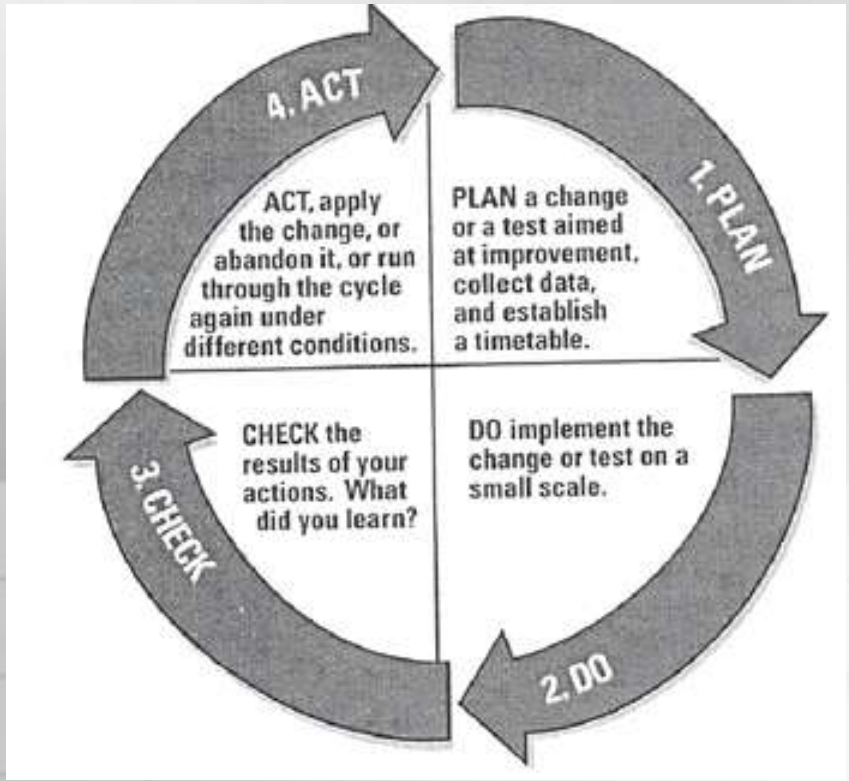


  - Process : شامل فعالیتهای مستمر بوده و فقط نقطه آغاز دارد



بخش چهارم : مدیریت امنیت
۱– سیستم مدیریت امنیت اطلاعات

- فرآیند تامین امنیت اطلاعات
  - استفاده از استانداردهای موجود
  - PDCA طراحی، اجرا ، ارزیابی ، اقدام
  - استاندارد ایزو ۲۷۰۰۱



بخش چهارم : مدیریت امنیت
۱– سیستم مدیریت امنیت اطلاعات

- **استاندارد ایزو ۲۷۰۰۱**
  - سند سیاست امنیت اطلاعات
  - سازماندهی امنیت اطلاعات
  - مدیریت دارایی
  - امنیت منابع انسانی
  - امنیت فیزیکی و محیطی
  - مدیریت ارتباطات و عملیات
  - کنترل دسترسی
  - تهیه, تولید و نگهداشت سیستم‌های اطلاعاتی
  - مدیریت حوادث مرتبط با امنیت اطلاعات
  - مدیریت تداوم کسب و کار
  - سازگاری با سایر قوانین و مقررات

با سپاس از حضور شما