정보보호 개론

23. 기본에 충실한 정보보안

발표순서

- 해킹의 일반적인 성질
  - 해커의 범주
  - 해커 프로파일링 결과
  - 해커가 잡히기 힘든 이유
  - 사이버 범죄가 많은 이유
  - 사이버 범죄자의 수학
  - 심리적 요인과 대책
  - 보안시스템의 역할
- PC 보안
- 무선랜 보안
- 기업의 웹 보안

해킹의 일반적인 성질

- 미국의 핵심기반시설에 대한 모의 해킹 시험
  - 공격 대상 : 38,000대
  - 침투 성공 : 24,700대(67%)
  - 침투 감지(보안관리자 또는 운영자) : 988대 (4%)
  - 상급자에게 보고 : 267대(27%)
  - 결국 침투에 성공한 시스템 중 보고된 시스템은 1.1%에 불과

- 결론
  - 해킹은 쉽게 당할 수 있고,
  - 해킹은 잘 탐지되지 않으며,
  - 해킹 사실은 잘 보고되거나 공개되지 않는다

해커의 범주 (1)

- UN Crimes & Corruption의 해커 프로파일링

범주	설명	기술 수준	개인 / 그룹	대상	동기	시스템 파괴 여부
Wanna-be-lamer	9~18세, 해커가 되고 싶으나 능력이 안되는 사람	낮음	그룹 멤버	최종사용자	유행	파괴(의도적 혹은 실수 (비숙련))
Script Kiddie	10 ~ 18세, 알려진 해킹 도구 사용	낮음	그룹 멤버	알려진 취약성을 가진 약한 시스템	분노의 표출, 혹은 과시	파괴하지 않음
Cracker	17 ~ 30세, 파괴자, 시스템에 머물면서 파괴적 행동 가능	중간	개인	기업	능력을 보여주거나, 관심을 끌기 위함	항상, 일부러 파괴함
Ethical hacker	15~30세, 윤리적 해커	높음	개인 (그룹)	요청 받은 대상(대기업, 복잡한 시스템)	호기심, 학습, 보호	파괴하지 않음
Quiet, paranoid, skilled hacker	16~40세, 조용하고, 편집증이 있는, 전문화된 해커. 흔적 없이 해킹 가능	높음	개인	필요에 따라 선택	호기심, 학습, 에고이즘, 특정 동기	

해커의 범주 (2)

- UN Crimes & Corruption의 해커 프로파일링 (계속)

범주	설명	기술 수준	개인 / 그룹	대상	동기	시스템 파괴 여부
Cyber Warrior	18~50세, 돈을 목적으로 하는 용병	높음	개인	ISP,조직, 최종사용자	금전적 이득	파괴 가능, 명령에 따라 수정, 삭제, 탈취 등
Industrial Spy	22~45세, 산업스파이(내부자 포함)	높음	개인	기업	금전적 이득	파괴하지 않음 (정보만 탈취)
Government Agent	25~45세, 정부요원	파악 곤란	개인 또는 그룹	정부, 테러리스트, 전략적 기업이나 개인	직업	상황에 따라 다름
Military Hacker	25~45세, 사이버 전투요원	파악 곤란	개인 또는 그룹	정부, 전략적 기업	직업	상황에 따라 다름

해커 프로파일링 결과 (1)

- 성별
  - 2000년 이전 대부분 남성
  - 2000년 이후 여성 증가
- 연령
  - 대부분 10대
  - 일찍 시작한 경우 30 ~ 35세까지 지속
- 거주지
  - 대부분 도시
- 자신들에 대한 평가
  - 똑똑하고, 창의적이고, 열린 생각, 이상주의자
  - 실제로는 수줍음이 많고 순진
- 가정형편
  - 대부분 가난하고 문제가 있는 가정
- 학력
  - 컴퓨터, 과학 분야를 좋아하나, 정규 교육을 시간 낭비로 생각하고 중퇴하는 경우가 대부분
  - 창의적이고 지식에 대한 호기심, 문제 해결 능력이 뛰어남

해커 프로파일링 결과 (2)

- 일반적인 특성
  - 직업 또는 연구 목적의 합법적인 계정이 있더라도 자신의 계정을 사용하지 않음 (학생의 경우 학교 계정 사용 예가 있음)
  - IP 주소 스푸핑, 프록시 서버 등을 이용하여 신원을 감추고, 시스템 관리자에게 적발되지 않도록 흔적을 감추려 함
  - 주로 야간에 작업
  - 공격을 위한 정보 수집을 위해 사회공학기법 사용
    - 크래킹, 트로이 목마, 이메일, 쓰레기 뒤지기를 통한 패스워드 획득 노력
  - 상황에 따라 개인 또는 그룹으로 활동
  - 전문 공격자의 경우 상당한 시간을 들여 주의 깊게 계획을 수립, 재사용을 위한 명령, 행동 철저히 기록
  - 백도어, 스푸핑을 통한 주소, 확장자 속이기

해커가 잡히기 힘든 이유 (1)

- 사이버 범죄와 일반 범죄와의 차이점
  - 정보는 탈취되어도 복사가 된 것일 뿐, 사라지지 않는다.
  - 정보 유출로 인한 피해는 당장 일어나지 않고, 미래의 일

- 1차적으로 보안시스템 및 담당자의 부재, 담당자의 능력 부족 또는 근무 태만으로 감지를 못하는 경우

- 2차적으로 감지를 했어도 담당자가 은폐할 위험이 큼
  - 문책에 대한 우려
  - 정보가 100% 유출되었다고 확신하기도 어려움

- 담당자가 보고를 해도 상급자가 외부(관계기관)에 공개하거나 신고하는 것을 꺼릴 가능성이 큼

해커가 잡히기 힘든 이유 (2)

- 해커가 해당 기업을 협박하는 경우
  - 돈을 주고 무마할 것인가 ?
  - 관계기관에 신고할 것인가?
- 해커가 잡히는 경우는 ?
  - 해당 기업에 협박하는 경우 신고가 이루어져서
  - 공명심에 자신의 행위라고 밝히는 경우
- 피해자가 신고를 꺼리는 '성범죄'와 유사
  - 성범죄의 경우 10%만 신고

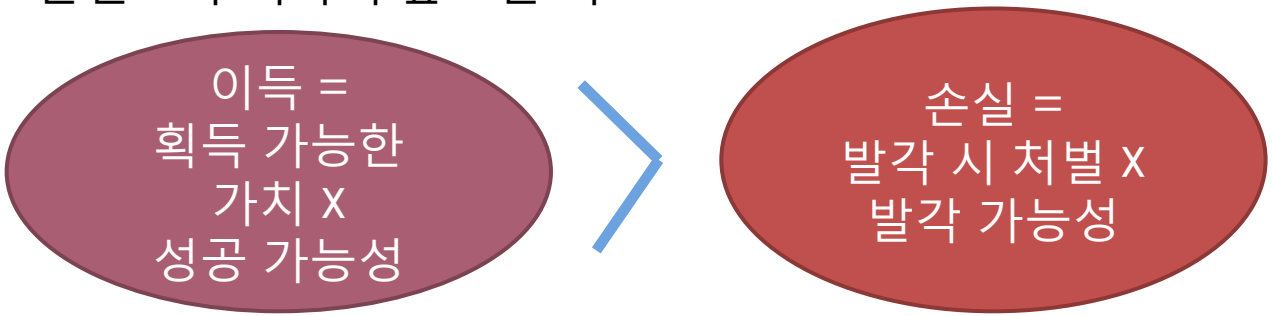
사이버 범죄가 많은 이유

- 미국 행동경제학자 댄 애리얼리(Dan Ariely)의 실험
  - MIT 기숙사에서 기숙사 공용 냉장고에 콜라 6개 팩과 1달러짜리 6장을 두고 관찰
    - 콜라팩은 72시간 내에 모두 사라짐
    - 지폐는 그대로 남아있음
  - '진짜' 돈을 훔치는 것은 꺼려함
  - '돈'의 추상성이 큰 대상일수록 부정 행위에 대한 유혹에 쉽게 넘어감

- 사이버 범죄에 대한 죄의식이 현저하게 낮음

사이버 범죄자의 수학

- 손실보다 이득이 높으면 시도



  - 획득 가능한 가치를 줄이는 방안
    - 가져가도 쓸모 없게 만드는 방안 (문서 암호화, 투명한 경영 등)
  - 성공 가능성을 줄이는 방안
    - 예방대책(기술적, 관리적, 인적)
  - 발각 시 처벌을 늘리는 방안
    - 해킹이나 정보 유출에 대한 엄벌
    - 심리학자의 연구 : 처벌은 미래의 문제이므로 생각 외로 큰 효과가 없음
  - 발각 가능성을 높이는 방안
    - 침입탐지시스템, 로그 분석 등
    - 초기 대응을 강화하여 발각 가능성이 높다는 메시지를 미리 전달할 필요가 있음

심리적 요인

- 불쾌감을 느끼면 자신의 비도덕적 행위를 쉽게 합리화한다.
  - 설문조사 후 5달러를 주기로 하고 설문 시작
    - Case 1 : 미안하다는 말과 자세한 설명 후 진행
    - Case 2 : 자세한 설명 없이 지루하게 진행
    - 5달러가 아닌 9달러를 주었을 때 회수율 비교
      - Case 1(불쾌감을 느끼지 않은 경우) 45%
      - Case 2(불쾌감을 느낀 경우) 14%
- 작은 부정이 큰 부정을 초래한다.
  - 자신이 정한 기준을 한번 깨면 더 이상 자기 행동을 통제하지 않는다.
  - “바늘 도둑이 소도둑 된다.”
- 다른 사람이 지키지 않으면 나도 지키지 않는다.
  - 주위의 다른 사람이 부정행위를 하면 혼자 있을 때보다 훨씬 더 많은 부정행위를 한다.
  - 특히 자신이 속한 사회집단의 일원이거나, 권위 있는 사람인 경우 매우 큰 영향

심리적 요인에 대한 대책

- 사람의 '감정' 요소를 관리
  - 사람의 마음을 잘 관리하라
  - 특히 내부자에게 중요
- 작은 부정에 단호해야
  - 초기에 대응이 없으면 점차 더 강한 공격으로 발전
  - 보안 정책을 초기 위반했을 때 신속하게 경고하고 대응해야
- 위에서부터 모두 동일한 보안 정책 준수
  - 예외자가 있는 경우 형식적으로만 지키게 됨

보안시스템의 역할

- 미국의 행동심리학자 댄 애리얼리(Dan Ariely)의 예화
  - 자물쇠 수리공의 말
    - 세상 사람의 1%는 어떠한 경우에라도 남의 물건을 훔치지 않는다.
    - 세상 사람의 1%는 어떻게든 자물쇠를 열어 물건을 훔친다.
    - 나머지 98%는 조건이 갖추어져 있는 동안에만 정직한 사람으로 남는다.
    - 자물쇠는 문이 잠겨있을 때 유혹을 느끼지 않는, 대체로 정직한 사람들의 침입을 막아준다.

- 하인리히 이론
  - 1:29:300의 법칙
    - 1번의 대형사고가 일어나기 전
    - 같은 요인으로 29건의 경미한 사고가 있었고,
    - 또 같은 사고를 낳을 뻔한 사소한 징후가 300번 있었다.

PC 보안 (1)

- 공격 타겟
  - 불특정 다수
    - 공격 방법
      - 주로 방문하는 사이트에 악성코드
      - 많이 다운로드 받는 컨텐츠에 악성 코드
    - 피해
      - 공격자는 PC 소유자가 할 수 있는 모든 일을 할 수 있음
      - 좀비화 -> DDOS 공격에 이용
- 특정 대상
  - 공격 방법
    - 지능형 지속 위협 (APT : Advanced Persistent Threat)
    - 전자우편 첨부파일을 통한 악성 코드 다운로드
      - 누드사진, 쿠폰
    - 첨부파일이 아닌 링크만 전송
  - 피해
    - 특정 개인 PC에 침투하여 개인 정보 절취
    - 특정 시스템에 침입하기 위한 전초 단계

PC 보안 (2)

- 대비책
  - 사용자가 출처 불분명한 파일은 다운 받지 않도록 교육
  - PC용 각종 보안 소프트웨어 설치 및 주기적 업데이트
    - 백신, 키보드 보안, 방화벽 등
  - PC 내 정보 암호화
  - 다양한 네트워크단, 서버단, DB단 보안 시스템 설치 및 모니터링

- "PC는 무조건 뚫린다"
  - 핵심시스템과 연결된 PC는 인터넷 연결 자체를 끊어야
  - PC 안에 중요 정보를 절대로 두지 말아야
  - 백신 설치 및 주기적인 업데이트 및 전수검사
  - 꼭 필요한, 출처가 분명한 프로그램만 설치

무선랜 보안 (1)

- 역사
  - 1999년 IEEE802.11b 제정
    - 인증방식 : Open System, Shared Key 인증
    - 데이터 암호 : WEP(Wired Equivalent Privacy)
  - 2001년 WEP에 대한 약점 논문 발표 및 오픈 소스 프로그램 발표
    - RC4 알고리즘 취약성으로 인해 10분만에 키 복구
  - 2001년 IEEE 802.11i TG 결성
  - 표준화 논의가 길어지자 2003년 WFA에서 WPA(Wi-Fi Protected Access) 발표
    - 인증방식 : Personal mode(PSK), Enterprise mode(IEEE 802.1x 인증서버 이용)
    - 데이터 암호 : Dynamic WEP, TKIP(Temporal Key Integrity Protocol)
  - 2004년 IEEE 802.11i 규격 제정
  - 2004년 7월 정식 IEEE 802.11i에 기반한 WPA2 발표
    - 암호 방식에 CCMP(Counter Mode Cipher Block Chaining Message Authentication Code Protocol)-AES 추가

무선랜 보안 (2)

- 단방향 인증 메커니즘의 취약성
  - 단방향 인증 : SK(Shared Key, 공유키) 방식
    - AP 입장에서 단말이 자신과 동일한 key를 소유하고 있는지를 확인하는 메커니즘
  - 단말 입장에서 AP가 자신과 동일한 key를 소유하고 있는지를 확인하는 절차가 없기 때문에 문제가 발생
  - 동일한 key를 소유하지 않은 불법 AP라 할지라도 단말에서 제공하는 인증 정보에 대해 OK 메시지를 전달하면, 단말 입장에서는 믿을 수 밖에 없음
  - 이를 개선한 것이 PSK(Pre Shared Key)이며, 상호 인증 형태로 이러한 문제를 해결

무선랜 보안 (3)

- PSK 인증 메커니즘의 취약성
  - Off-line 사전 공격(dictionary attack)이 가능한 메커니즘
    - 사전에 등록된 단어를 이용한 key는 크랙이 가능
  - key 배포 문제
    - AP와 단말에 수동으로 동일한 key를 설정하는 방식으로 모든 단말은 동일한 key를 설정
    - 해당 key가 유출되거나, 임직원이 퇴사하게 되는 경우 심각한 문제가 발생
  - IEEE 802.11i와 WAP2에서는 PSK를 개인 또는 SOHO에서만 사용하도록 권고(Personal mode)
  - 기업/기관 등 복수의 사용자가 이용하는 무선랜 환경에서는 IEEE 802.1x 인증 시스템을 사용할 것을 권고(Enterprise mode)

기업의 웹 보안

- 과거 주 공격대상
  - 회사의 네트워크나 시스템 장비
  - 방화벽, 침입탐지시스템 등의 도입으로 침입이 어려워짐
- 현재의 주 공격대상
  - 웹 서비스
    - 기업의 입장으로 운영할 수 밖에 없는 서비스
    - 글 쓰기나 사진 업로드 등 입력 허용
- 웹 서비스의 취약 원인
  - 다양한 언어로 개발 -> 표준화된 보안 대책 적용에 어려움
  - 개발 단계에서의 보안 적용이 필요
    - 도입 전에 보안이 강구되어야 함
      - 안전한 개발보다는 빠른 개발이 우선시
  - 잦은 변경
    - 초기 개발자와 운영자 상이 (기술 수준)
  - 사각지대 존재
    - 기술과 도메인 지식을 모두 알아야 하지만 현실적으로 불가능 -> 보안전문가, 업무담당자, 개발자들의 협동 작업 필요