

Security Education

Ver. 1



기초보안



GyungSoo Shin

CISSP, CISA

gss@kr.ibm.com

목차

1. 보안의 개념
2. 접근통제
3. 정보유출 피해사례
4. 침해위험의 유형과 대응법

1. 보안의 개념

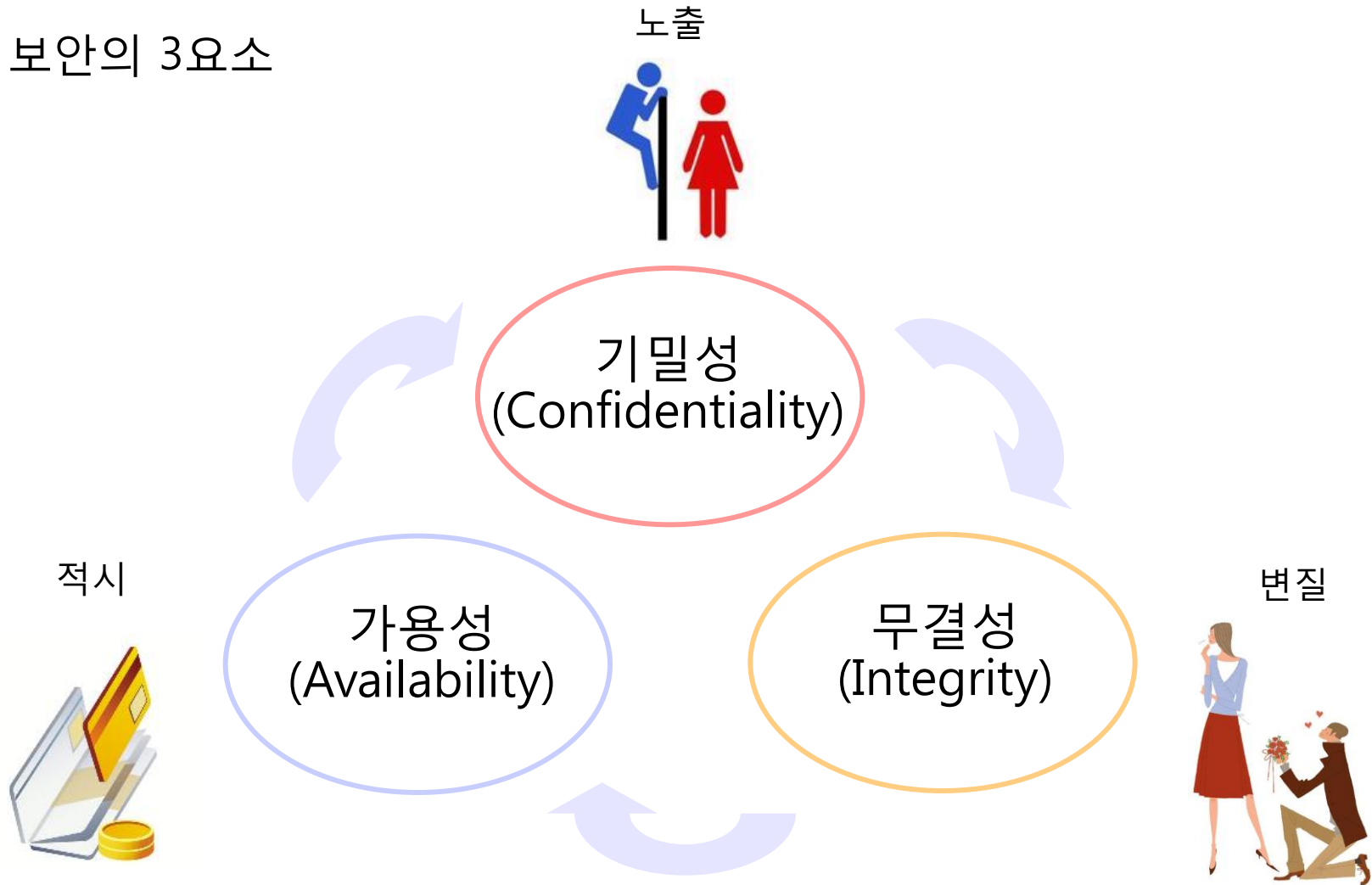
보안이란?



- ✓ 소중한 것을 지키기위한 수단
- ✓ 허락받은 자 만의 권리
- ✓ 모두의 관심속에 지켜져야 할 의무

2. 접근통제

보안의 3요소



2. 접근통제(cont'd)

접근통제의 3가지 분야

관리보안



- ✓ 보안정책
- ✓ 지침 및 절차
- ✓ 처벌

SECURITY

기술보안



- ✓ 해킹방어(CERT)
- ✓ 안티바이러스(V3)
- ✓ 방화벽(Firewall)

물리보안



- ✓ 출입통제시스템
- ✓ CCTV
- ✓ 경비원

2. 접근통제(cont'd)

접근통제의 3가지 분야- 중첩보안



3. 피해사례

2007" 두산중공업 핵심기술 유출사건



<그림. 동아일보>

- 두산중공업 핵심자료 900여건을 가지고 STX 산업플랜트 사장으로 전직
- 20여년간 연구해온 세계최고의 기술 유출
- 두산 피해액 1조7천억 원, STX 주가하락
- 2009년, 징역 1년6개월, 집행유예 2년 선고

3. 피해사례(cont'd)

2008" 옥션 고객정보 유출사건



- DB해킹으로 인한 1080만 명의 고객정보 유출
- 700여명이 개인당 50~70만원의 위자료 소송
- 소비자원 분쟁조정위원회에서 위자료를 지급하라고 하였으나 옥션 측에서 거부
- 14만 명 집단 소송
- 내년 2월로 1차 선고 연기
- 회사 이미지 하락

3. 피해사례(cont'd)

2009" 보이스피싱 (Voice Phishing)



<그림. 동아일보>

- 현금카드 보안정보가 유출되었으니 보안을 강화해야 한다면서 현금 요구
- 중국 내 조직화된 역할분담으로 보이스피싱
- 피해액 2441만 위안(약 43억 원)
- 중국 법원 두목 급 5명 무기징역, 나머지 25명 3~25년형

4. 침해위험의 유형과 대응법

물리적 위험과 대응법 – Tailgating



- 인가되지 않은 사람의 따라 들어가기를 허용 하는 것
- 비 인가자의 허가 받지 않은 정보 취득을 야기시킴
- 외부로부터의 위험에 노출



- 낯선 사람일 경우 “어떻게 오셨습니까?”라고 정중히 물어보며 신원을 확인
- 사원증 및 출입증은 반드시 패용하며
- 출입 시 리더기에 접촉시키는 것을 생활화

4. 침해위험의 유형과 대응법(cont'd)

물리적 위험과 대응법 - 사무환경

- 쓰레기통은 밝고 통행이 많은 곳에 비치
- 중요문서의 폐기는 분쇄기 사용
- Laptop과 같은 이동식장비는 보관에 주의(시건 장치 사용)
- 중요시설의 출입문은 외부에서 보이지 않도록 처리
- 출입문의 조명은 최대한 밝게 유지
- Desktop PC의 보이지 않는 뒷면에 불필요한 이동식 저장장치의 삽입여부
- 대외비 및 고객정보(고객명함 등)는 시건 장치가 되어있는 장소에 보관

4. 침해위험의 유형과 대응법(cont'd)

물리적 위험과 대응법 - 퇴직처리

- 실제 기업정보 유출의 대부분이 내부자 소행
- 직원의 정보기기 반납은 퇴사시점이 아니라 퇴사를 결심한 시점
- 전산직원의 퇴사시 사용자 ID회수 및 정지가 아닌 삭제조치
- 중요정보가 담겨있지 않은 정보기기과 권한이 제한된 임시 ID지급
- 출입문까지 Escort

4. 침해위험의 유형과 대응법(cont'd)

컴퓨팅 환경에서의 침해위험과 대응법 - 암호화

- Desktop, Laptop PC와 같은 정보기기는 BIOS, OS 암호화 필수
- P/W또는 힌트가 되는 메모를 눈에 띄는 곳에 붙여두는 행위 금지
- 생년월일, 전화번호 등 노출이 될 수 있는 비밀번호 설정은 취약함
- 1q2w3e, asdfgh와 같이 알기 쉬운 자판배열의 조합은 금물
- 민감한 정보(파일)는 자체 암호화로 보안성 증가
- 주기적인 비밀번호 변경

4. 침해위험의 유형과 대응법(cont'd)

인터넷 환경에서의 침해위험과 대응법 - 악성프로그램(Trojan Horse)

특징

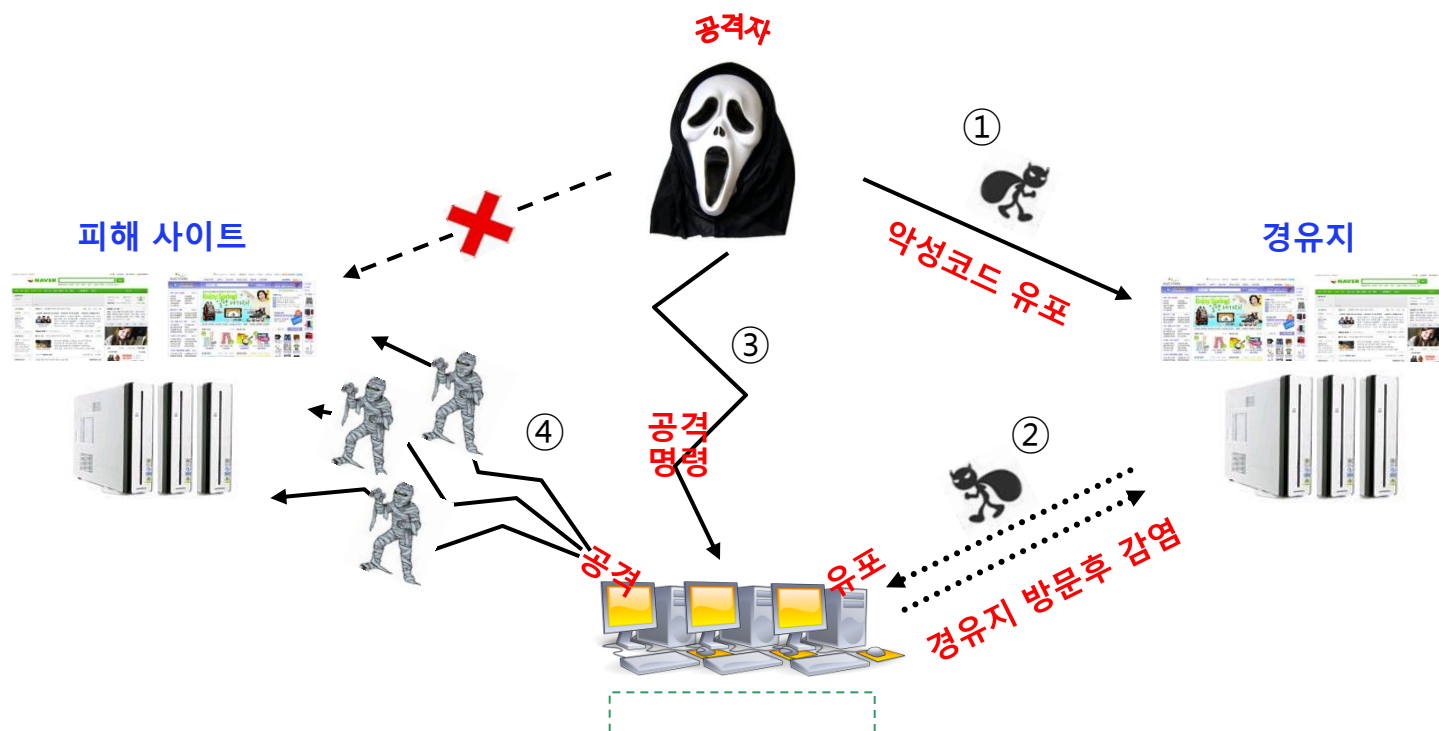
- 정상적인 경로로 사용자의 PC에 다운로드
- 사용자 개인정보 유출
- DDOS공격의 Agent (Zombie)역할
- 경우에 따라 사용자 PC 파괴



4. 침해위험의 유형과 대응법(cont'd)

인터넷 환경에서의 침해위험과 대응법 - 악성프로그램(Trojan Horse)

DDos 공격 개요도



4. 침해위험의 유형과 대응법(cont'd)

인터넷 환경에서의 침해위험과 대응법 – 악성프로그램(Trojan Horse)

원인

- 성인 음란물 또는 신뢰받지 못하는 불법 사이트가 주 원인
- 파일공유 사이트를 통한 침투(불법 다운로드)

대응법

- 보안패치(신뢰할 수 있는 패치 사용)
- Anti-Virus Scan설치(충분히 입증된 Scan 설치)
- 파일 공유사이트 접근차단, 파일 다운로드 시 사전검사 실시

4. 침해위험의 유형과 대응법(cont'd)

인터넷 환경에서의 침해위험과 대응법 – 악성프로그램(Adware, Spyware)

Adware

- ▶ 어떠한 프로그램을 설치할 때 사용자의 동의 하에 광고프로그램을 추가로 설치하게 되는데 프로그래머는 광고수익을 올리고 사용자에게 특별한 혜택을 주는 것에서부터 시작됨. 하지만 현재 Spyware성향을 띄고 있는 Adware가 늘어남으로써 사회적 문제가 되고 있다.

Spyware

- ▶ 미국 광고회사인 라디에이트(Radiate)에서 개인 사용자의 취향을 파악하기 위해 개발되었으나 최근 사용자의 이름은 물론 IP주소와 즐겨찾기목록, 개인 ID와 Password까지 알아낼 수 있게 발전되어 사이버 범죄에 사용될 소지가 많다.

대응법

- ▶ 신뢰할 수 있는 Spyware제거 툴 사용



4. 침해위험의 유형과 대응법(cont'd)

그 밖의 침해위험과 대응법 – 사회공학(Social Engineering)

사회공학(Social Engineering)

- 사람의 심리를 이용하여 부당한 방법으로 정보를 취득하는 방법

침해유형A. 직급을 이용

- 사내 Helpdesk로 한 통의 전화

“나 OOO이사야! 알지? 내 컴퓨터 비밀번호를 까먹었는데 뭐였지?”

특징: 직급을 이용하여 친분을 표시하며 자연스럽게 물어본다.

침해유형B. 고객으로 위장

- 고객센터로의 문의전화

“내가 내 전화요금을 묻는데 왜 개인정보를 말해야 돼!”

특징: 상담원의 질의에 응하지 않으며 무조건 화를 낸다. 상담원을 당황스럽게 만듦으로써 얼떨결에 정보를 말하도록 유도한다.

4. 침해위험의 유형과 대응법(cont'd)

그 밖의 침해위험과 대응법 - 사회공학(Social Engineering)

피싱(Phishing)

전화, 인터넷 메신저, 전자우편 등을 통하여 신뢰할 수 있는 사람으로 가장하여 기밀정보를 부정적인 방법으로 얻으려는 방법으로써 궁극적인 목적은 금전과 관련이 있다.

- ▶ 우체국직원, 검찰청, 보험회사직원 등을 가장하여 받을 물건이 있거나 금액을 환급해준다고 접근
- ▶ 최근 불특정 다수가 아닌 특정인물의 개인정보를 취득한 뒤 타겟을 정하고 접근하는 수법도 발생되었음(실제 자녀의 이름과 나이, 학교 또는 직장이름을 알아낸 뒤 보호자에게 전화를 걸어 XXX를 인질로 잡고 있으니 돈을 보내지 않으면 가해하겠다고 협박, 학교나 직장에 있는 사람이 아무 때나 전화를 받지 못하는 특성 이용)

4. 침해위험의 유형과 대응법(cont'd)

그 밖의 침해위험과 대응법 – 사회공학(Social Engineering)

대응법

- ▶ 블로그, 미니홈피등 개인게시판에 가족들의 전화번호 및 신상이 노출될 만한 정보들을 게시하지 않는다.
- ▶ 개인정보를 요구하는 전화는 신뢰하지 않는다. 실제로 공기업 또는 정부기관에서 전화를 걸어 개인정보를 요구하는 행위는 일체 하지 않는다.
- ▶ “확인 후 다시 전화를 드리겠다” 라고 말한 뒤 걸려온 전화를 끊고 신뢰되는 번호로 다시 전화를 걸어 정보의 사실을 판단한다.(Call Back)
- ▶ 자녀 등 가족에 대한 비상 연락처를 확보한다.



<참고자료: 한국인터넷진흥원>

4. 침해위험의 유형과 대응법(cont'd)

집성, 추론을 이용한 산업범죄



Dumpster Diving(쓰레기통 뒤지기)



직원이름
거래처목록 } 획득, 분석



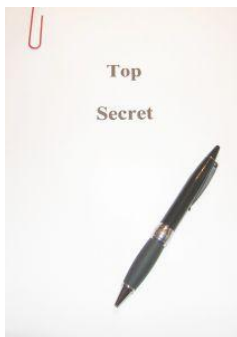
OOO직원이 XX거래처와 연관이?



OOO직원의 동료로 위장하여
XX거래처 담당자 정보를 획득



XX거래처 담당자로 위장,
OOO직원에게 전화를 걸어
제안서에 문제가 있다며
외부메일로 재 발송을 요청



정보획득

<그림: 동아일보>

Security is everyone's business!

-Thank You-

마침

본 자료는 보안의 기초지식을 토대로 누구나 배우기 쉽고 알아두어야 할 사항만을 거론하였습니다. 따라서 전문용어 및 Network관련 지식을 배제하였으며, 되도록 쉽게 접근할 수 있는 보안교육에 중점을 두었습니다. 그러므로 교육내용은 포괄적인 면이 다소 있으며 사무환경에서의 보안실무를 위주로 기술하였기 때문에 구체적인 해킹 방어법 및 심층연구는 이루어 지지 않았습니다.

IT강국인 대한민국은 정작 보안에 대한 인지도가 타 국가에 비해 현저히 떨어지는 것을 보고 아쉬움을 느꼈으며, 보안이 대기업이 아닌 중소기업의 기업에서도 널리 알려지고자 본 자료를 무료로 배포합니다. 단, 저자의 취지와 벗어난 무단수정은 삼가 바라며, 수정할 사항이나 기타 의견은 E-Mail을 통하여 전달해 주시면 감사하겠습니다.

Email: gss@kr.ibm.com / anthony_shin@naver.com