

과정명	
15차시	4차 산업 환경 속 정보 보안관리의 위협 요인과 대응 방안

<1> 정보 보안관리의 위협 요인

- 인터넷의 시작은 대학에서 연구실 간 데이터를 전송하기 위해 단순히 어떤 시스템과 다른 시스템의 통신 프로토콜을 만든 데서 비롯되었는데, 이 프로토콜들을 여러 회사에서 만들면서 서로 통신할 수 없어서 연결하기 위해 게이트웨이가 만들어지고, 더 많은 프로토콜을 연결하기 위해 게이트웨이의 숫자도 급격히 늘어났기 때문에 프로토콜의 표준화가 필요해짐
- 이렇게 점점 확장되고 네트워크 간의 연결이 자유로워지면서 보안에 대한 문제점도 대두되게 되었고, 보안의 위협 요인이 많아지며 이를 위한 대응 방안이 필요해짐

[1] 정보보안 관리의 위협 요인

(1) 보안 취약점(Security Vulnerability)

- 사전적 의미는 컴퓨터의 하드웨어 또는 소프트웨어 결함이나 운영체제 설계상의 허점으로 인해 사용자의 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람을 가능하게 하는 약점
- 넓은 의미로는 사용자나 관리자의 부주의 및 사회공학 기법에 따른 약점을 이용하여 공격 대상 정보시스템에서 공격자가 의도한 동작을 수행하게 하거나 특정한 정보를 탈취하게 되는 것
- 정보 보호 활동은 정보시스템이 가진 취약점을 찾아내어, 정보시스템을 위협으로부터 보호하기 위한 비용 효과적인 대책을 세우는 것
- 정보 보호 활동을 하는 이유는 보안 취약점 때문임
- 정보 보호 활동의 비용 효과적이며 실효적인 보안 대책을 세우기 위해서는 정보시스템 본래의 보안 취약점과 이를 공격하여 보안 문제를 일으키는 위협에 대해 정확히 진단하는 것이 필요

(2) 보안 취약점 분류

- 일반적으로 보안 취약점은 물리적, 기술적, 관리적으로 구분됨

구분		내용
물리적	물리적 취약점	침입자는 정보처리시설과 같이 정보시스템이 설치되어 있는 건물이나 워크스테이션 등과 같은 서버 및 개인용 컴퓨터가 설치되어 있는 사무실에 침입할 수 있다. 일단 침입에 성공하면 시스템 파괴, 부품 탈취 등과 같은 모든 수단의 불법 행위를 할 수 있음
	자연적 취약점	정보시스템은 화재, 홍수, 지진, 번개 등의 자연재해에 매우 취약함
	환경적 취약점	정보시스템은 먼지, 습도, 온도 등의 주변 환경에 취약함
기술적	하드웨어 취약점	하드웨어 오류나 오동작이 전체 정보시스템의 보안에 손상을 입힐 수 있음
	소프트웨어 취약점	시스템을 실패나 오동작으로 몰고 갈 수 있는 소프트웨어의 실패는 시스템을 취약하게 만들거나 시스템을 불안정하게 만들 수 있음
	매체 취약점	자기 디스크, 자기테이프, 출력물 등은 손실되거나 손상을 입을 수 있음
	전자파 취약점	모든 전자 장치는 전자파를 방출함 도청자는 정보시스템이나 네트워크 또는 휴대전화로부터 발생하는 신호를 가로챌 수 있음
	통신 취약점	컴퓨터가 네트워크나 모뎀에 연결된 경우 인가받지 않은 사람이 침입할 위험성이 증가함
관리적	인적, 관리적 취약점	보시스템을 사용하거나 관리하는 직원은 가장 큰 취약점을 보임. 관리자가 적절한 교육을 받지 않았거나 나쁜 유혹에 빠질 경우, 컴퓨터 사용자나 운영자 및 기타 직원들이 비밀번호를 누설하거나 주요 시설물의 출입구를 열어 두는 등의 행동을 할 수 있음

(3) 보안 위협

- 보안 위협은 자산에 손실을 초래할 수 있는, 원치 않는 사건의 잠재적 원인이나 행위자로 정의됨

- 위협의 유형은 자산에 영향을 미치는 방식으로 규정으로 위협에 대응하기 위한 보호 대책 선정에도 영향을 미치므로 가능한 구체적으로 표현하는 것이 좋음
- 보안 위협은 크게 자연에 의한 위협과 인간에 의한 위협으로 분류 가능

분류		내용
자연에 의한 위협		화재, 홍수, 지진, 전력 차단 등 자연에 의한 대표적인 위협으로부터 발생하는 재난을 항상 예방할 수는 없지만 화재경보기, 온도계, 무정전 시스템들을 설치하여 피해를 최소화할 수 있음
인간에 의한 위협	비의도적 위협	정보시스템의 보안 사고를 일으키는 가장 큰 위협으로 인간의 실수와 태만이 주된 원인 패스워드의 공유, 데이터에 대한 백업의 부재 등이 대표적인 부주의와 태만으로 간주되며, 이러한 위협은 언론매체에서 크게 다루어지지는 않지만 실제로는 정보 보호 문제를 일으키는 가장 중요한 요인임
	의도적 위협	컴퓨터 바이러스, 해커, 사이버 테러리스트 등으로부터 발생하여 도청, 신분 위장에 의한 불법 접근, 정당한 정보에 대한 부인, 악의적인 시스템 장애 유발 등이 있음

- 일반적인 보안 위협
 - 1) 내부자에 의한 중요 기밀정보 유출 위협
 - 2) 사회공학적인 공격 위협
 - 3) 스파이웨어의 위협
 - 4) 정보 도청 위협
 - 5) TCP/IP 프로토콜의 취약점 이용 위협
 - 6) 서비스 거부 공격(DDoS)
 - 7) 접근 통제 위협
 - 8) 정보 보호 정책 수립 및 이행 등 관리적 위협

(4) 최신 ICT 서비스 보안 위협

- 1) 스마트폰 보안 위협
 - 폭발적인 스마트폰의 보급과 이용으로 인해 스마트 기기를 대상으로 한 해킹 및 악성코드 감염 등 위협이 증가하고 있음
 - 악성코드의 주요 특징은 통화 기록이나 전화번호, 사진 등의 개인정보 탈취, 비정상 트래픽을 유발하여 과다 요금을 유도하거나 배터리를 소진하게 만드는 것
 - 휴대폰 단말 특성을 이용한 보안 위협
 - ① 사용자/단말기 보안 위협
 - 개인정보 또는 업무 정보의 유출, 불법 과금 발생, 업무용 서버에 불법 접속하여 업무 정보 유출, 스마트폰 소유자가 악의적으로 업무 정보의 외부유출
 - ② 네트워크 보안 위협
 - 무선 구간에서 패킷 스니핑, 상용인터넷망을 통한 해킹, 스마트폰을 거쳐 인트라넷 서버에 접속, 모바일 DDoS 등
 - ③ 응용 서비스 보안 위협
 - 모바일 SMS, बैं킹, VOIP 등 이용으로 해킹, 서비스 중단, 사회공학적인 공격이 증가와 악성코드 감염이나 악의적 목적의 앱으로 인해 위치, 개인정보 유출 등의 사생활 침해
 - ④ 모바일 콘텐츠 위협
 - 뉴스, 방송, 음악, 라디오, 영화 등 콘텐츠 DRM 해킹, 모바일 스팸, 불법 및 유해 콘텐츠 유통

2) 모바일 전자금융 서비스 보안 위협

- 모바일 전자금융 서비스는 금융 앱을 기반으로 서비스가 제공되기 때문에 앱을 배포하는 경로로 활용될 수 있는 앱 스토어, 블랫마켓, 웹 사이트, 문자메시지, 메신저 등을 이용한 공격과 단말기 자체 특성에 기인하여 PC 등 주변기기와 연동 시 발생할 수 있는 취약점을 이용한 공격이 이루어질 수 있음
- 모바일 전자금융 거래 시 공격 유형
 - ① 입력
 - 보안 카드나 이체 비밀번호 등 금융 앱이 실행된 상태에서 입력하는 중요 정보의 유출
 - ② 출력
 - 금융 관련 주요 정보가 화면에 출력될 때 화면 캡처 및 원격 제어를 통한 중요 정보의 유출
 - ③ 저장
 - 악성코드가 감염이나 단말기 분실 등의 생활에서 기기 내부에 저장된 중요 정보의 유출
 - ④ 전송
 - 유무선 통신 기능 이용 시 전송될 수 있는 중요 정보의 유출

3) 소셜 네트워킹 환경의 보안 위협

- SNS의 속성상 소속, 연락처, 취미, 활동내역, 사진 등 대부분의 개인정보를 공개된 상태에서 소통하기 때문에 이러한 과정에서 의도하지 않게 많은 개인정보들이 노출될 수 있음
- SNS 관련 보안 위협
 - ① 프라이버시 보안 위협
 - 개인 프로필 수집, 2차 데이터 수집, 안면 인식과 개인정보 연계로 인한 초상권 침해와 익명성 약화, 콘텐츠 기반 이미지 검색, 이미지 메타 데이터와 개인정보의 연계, 완전한 계정 삭제의 어려움
 - ② 네트워크상의 보안 위협
 - SNS를 이용한 스팸 증가, 크로스 사이트 스크립팅, 웜 및 바이어스 등에 대한 취약성 증가, 다양하게 통합되는 SNS 포털들이 정보수집기로 이용되어 보안 취약성이 증가할 수 있음
 - ③ ID 관련 위협
 - SNS를 이용한 특정 이용자 그룹에 대한 스피어 피싱, 침입을 통한 ID 정보유출, ID 도용을 통한 허위 정보 생산 또는 명예훼손 등 각종 범죄가 증가할 수 있음
 - ④ 사회적 위협
 - 사이버 스토킹, 사이버 괴롭힘, 산업 스파이 등에 관한 위협 등

4) 클라우드 서비스의 보안 위협

- 클라우드 서비스 가상화 플랫폼의 하이퍼바이저를 통해 가상 서버가 상호 연결된 구조적 특성에 따른 신규 공격 경로가 존재할 수 있으며, 특권을 가진 사용자의 접근제어, 데이터 무결성, 데이터의 분산 관리, 서비스의 가용성 보장 등이 중요한 보안 요소임
- 클라우드 서비스에서 일어날 수 있는 보안 위협 요소
 - ① 정보 위탁 및 자원 공유 문제
 - 고객 정보의 제3자 위탁 및 저장 방식으로 고객 정보를 저장 관리하는 제3기관의 보안 수준이 고객 정보 보호 수준을 결정하며, 클라우드 사업자 내부 직원의 고의, 설정 오류 등의 관리 부주의로 인한 정보 접근 및 유출의 위협 등이 존재함
 - ② 정보 및 서비스 집중화 문제

- 여러 고객사의 주요 정보 및 서비스가 집중됨에 따라 해킹, DDoS 공격의 표적이 되기 쉽고, 해킹 DDoS 사고 발생 시 모든 이용자 서비스가 연쇄적으로 중단되면 대규모 피해 야기 가능

③ 가상화 문제

- 물리적 자원을 논리적으로 통합 재분배하여 사용함에 따라, 1대의 물리적 서버에 여러 대의 논리 서버(가상 서버)의 구동으로 CPU, 메모리, 스토리지 등의 물리적 자원을 논리적으로 재분배, 전체 가상 서버 해킹 또는 악성코드 확산이 가능

④ 클라우드 오용과 비도덕적인 사용

- 악의적인 목적으로 클라우드를 도입하는 경우, 가상의 공간에 정보가 존재하는 특성이 있으므로 기존의 봇넷보다 더욱 높은 보안 위협이 있음

⑤ 불완전한 인터페이스와 응용 프로그래밍 인터페이스

- 부가 가치를 높이기 위해 기존 코드를 재사용하거나 합성 등을 통해서 응용 프로그램을 개발할 때 프로그램 복잡도가 증가하여 이에 따른 보안 취약성이 발생

⑥ 기술 공유 문제

- 인프라 서비스 사업자는 공유 기술을 바탕으로 시스템 확장성을 제공하지만, 다중 애플리케이션 아키텍처 사용을 위한 효과적인 자원의 분리가 이루어지지 않는 경우 클라우드 서버 내부의 가상머신 간 도청, 해킹 가능, 클라우드 인프라를 공격에 악용됨

⑦ 계정이나 서비스 갈취

- 클라우드 환경에서 계정 정보의 유출은 모바일 단말기 분실 또는 ID/PW 도용으로 타인 정보에 불법 접근이 가능함

5) 빅데이터 보안 위협

- 빅데이터는 대량의 정형 또는 비정형 데이터 집합 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술
- 빅데이터를 수집, 분석할 때 개인들의 사적인 정보까지 수집하여 관리하는 빅 브러더의 모습이 될 수도 있으며, 이렇게 모인 데이터가 보안 문제로 유출된다면, 이 역시 거의 모든 사람의 정보가 유출되는 것이기에 큰 문제가 될 수 있음

- 빅데이터 단계별 보안 위협

- ① 데이터 생성 단계
- ② 데이터 저장 운영 단계
- ③ 서비스 단계

6) 사물인터넷(IoT, Internet of Things) 보안

- 사물인터넷은 사람, 사물, 공간 등 모든 것들이 인터넷으로 서로 연결되어 모든 것들에 대한 정보가 생성 및 수집되고 공유 활용되는 것을 뜻함
- 사물인터넷은 여러 가지 요소 기술이 통합되어 특정 서비스를 구성하기 때문에 각 요소 기술 자체의 보안 취약점과 연동 시 새로운 보안 취약점이 발생할 가능성이 매우 큼

- IoT 서비스 환경에서 발생 가능한 보안 위협 시나리오

- ① 악성코드가 감염된 차량진단 앱을 통한 자동차 원격 제어
- ② 심박기 신호 정보 위변조를 통한 전류량 과징 공급
- ③ 홈서버 해킹을 통한 댁 내 가스밸브 원격 개방
- ④ 교통 정보 수집 센서 해킹을 통한 신호 제어
- ⑤ 항공기 내 와이파이를 통한 악성코드 감염 및 항공기 제어시스템 오동작 유발

<2> 정보보안 관리의 대응방안

- CPU 항공기 내 와이파이를 통한 악성코드 감염 및 항공기 제어시스템 오동작 유발 말함
- 보호 대책을 선택할 때는 위험 분석을 통해 조직의 환경과 문화에 맞는 것을 선택하는 것이 중요하며, 그 비용을 산정할 때는 구축비용에 운영에 따른 관리 비용도 반드시 고려해야 함

[1] 공격 패턴 및 대응 방법

(1) 앱 어플 공격

- 웹 어플리케이션 안전화를 위해서는 비밀번호 기반 인증 실시가 가장 중요
- 반복적인 로그인 실패 시 계정이 잠기도록 하여 무차별 암호 대입 공격을 제지
- 아웃바운드 접속 모니터링을 통해 서버에서 수백 만개의 패킷을 외국 정부 시스템에 전송해야 할 이유가 없다면 해당 기능을 잠금
- 사용자의 입력 유용성 검사 및 확인을 철저히 실시
- 제 3자(third-party) 플러그인에 대한 경계 필요

(2) POS 침투

- 다채롭고 강력한 인증 시스템의 복합적 사용
- 어떤 모니터링 옵션이 좋을지 결정 및 설치하는 것과 POS 환경을 분산 배치하는 것이 중요.
- POS 작업용 POS 시스템을 별도로 확보하여 직원이 웹 사이트 검색, 이 메일 확인 또는 게임 용도로 사용하는 것을 금해야 함

(3) 여러 종류의 실수들

- 다양한 종류의 실수들을 기록해야 하는 이유
 - 1) 보안 관련 교육, 연수 시에 자료로 만들어 사용
 - 2) 데이터를 통해서 실수가 일어나는 빈도 감소
 - 3) 일어났을 때 받을 데미지를 경감
- 데이터 셋이나 데이터 자산들이 처리되거나 해체되기 전에 IT부서에서 이런 자산들이 엄격한 절차에 따라 행해지는지를 확인해야 함

(4) 내부자 특권 악용

- 보편적으로 '내부자의 특권 악용'은 중요 정보나 기밀에 접근할 수 있는 내부 관리자나 담당자에 의해 행해지기 때문에 이들에 대한 철저한 관리나 모니터링이 필요
- 근본적으로 중요 정보가 위치한 곳과 접근 권한을 준 사람과 정도에 대해 정확히 파악

(5) 물리적 도난 및 손실

- 모바일 디바이스, 이동식 미디어의 완전 암호화로 이동식 디바이스의 증가에 따른 도난과 손실 예방
- 정기적인 백업은 주요 데이터의 손실을 예방, 다운타임 감소, 보안 침해가 발생시 범죄 수사에 도움이 됨
- 모든 직원들이 보안 상황에 대한 인식을 확고하게 만드는 것이 필요

(6) 크라임 웨어

- 불법 온라인 활동을 위해 고안된 프로그래밍
- 판매사가 제공하는 OS 어플리케이션이나 보안 툴 등의 패치를 적극 활용하여 보안 취약성 방어
- 프로그램이 스크립트나 매크로를 실행하는 것을 막고, 이메일 서버에 첨부파일을 통해

실행파일이나 파일 확장 등을 제거하는 것이 중요함

(7) 사이버 스파이

- 사이버 스파이 범치는 단순한 툴들과 테크닉들로 시작하기 때문에 가장 기본적인 보호들이 이런 종류의 위협을 차단하는 것이 중요하며 특수화된 보호가 필요함
- 엔드포인트란 IT적인 관점에서 어떠한 소프트웨어나 제품의 최종목적지인 사용자로, 악의적인 소프트웨어는 이메일, 웹 드라이브 바이, 직접/원격 설치 등을 통해 전달되기 때문에 엔드포인트 보호는 중요함
- 피싱은 여전히 사이버 스파이 행위의 주요 공격 벡터이기 때문에 전달 매개체가 되는 이메일 등을 방어하는 것이 중요
- 사이버 스파이 범치의 거점이나 기반이 마련되었다 할지라도 내부 시스템을 보호하기 위해 네트워크 보호는 중요함
- 모든 해킹으로부터 교훈을 얻기 위해 시스템, 디바이스 그리고 어플리케이션의 내부 모니터가 필요함

(8) DoS 공격

- DoS 공격들의 빈도, 복잡성, 규모들이 계속 진화하고 발전 중
- 클라우드 서비스 공급자들은 서비스와 인프라를 보호하기 위한 솔루션을 보유해야 함
- DoS 공격에 대한 방어와 경감 능력에 대한 이해 필요
- DoS 공격이 실행되는 것을 막기 위해 철저히 핵심 자산을 분리 · 구분해서 관리

[2] 4차 산업혁명과 정보 보안관리

- 4차 산업혁명은 모든 분야에서 정보의 활용, 공유 그리고 전달 등이 과거보다 시공간을 초월해 동시다발적으로 이루어지며 더욱 많은 양의 정보들이 이용되고 있음
- 4차 산업혁명의 가장 중요한 자산은 정보 자원이며, 이런 정보 자원을 잘 보호하고 원활히 공유될 수 있도록 하는 것이 정보보안의 역할
- 정보보안을 위협하는 범죄 행위의 빈도가 증가하고 수법이 진화하면서 이것에 대한 대응 방법 마련이 시급함
- 정보보안의 위협 요인을 파악하고, 예방을 위한 구체적인 대책이나 방법을 마련함과 필요한 교육을 조직체 전반적으로 실시하는 것이 중요
- 예방 활동과 직원교육을 통해 공격에 대한 방어를 철저히 하고 실수를 통한 데이터나 정보 유실을 막을 수 있으며, 사이버 스파이나 내부자의 권한 남용 같은 비윤리적인 정보 관련 범죄 행위도 줄일 수 있음
- 정보 유출이나 지능화된 사이버범죄가 급증하면서 이를 예방하고 대비하기 위한 국경을 초월한 고도의 전문적인 조사 및 협력 등도 요구되고 있음