1 보안 정책 정의 및 구성 요소

1 보안 정책-정의

- 보안 정책은 시스템을 위협하는 주요 위험요소로부터 기업의 자산을 보호하기 위한 정책임(AVT)

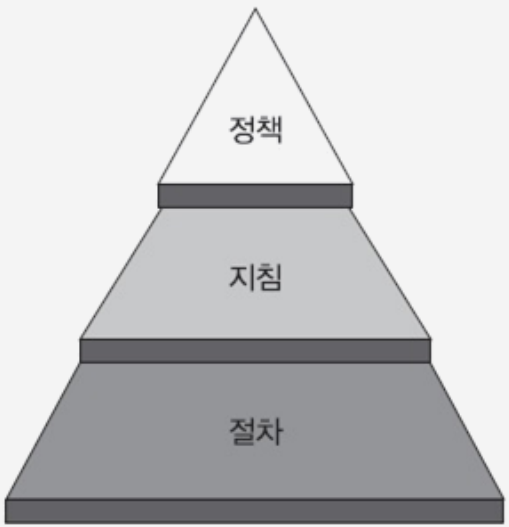
- 정보 위험도를 서열화한 문서, 수용 가능한 보안 목표 식별, 목표를 달성하는 메커니즘의 식별로 구성됨

2 보안 정책의 필요성

- 2003년 1.25 대란 등의 정보보안 관련
  대형 사고가 발생하고 ISO 27001 등 보안에 관한
  국제 표준이 생기면서 기업들이 저마다의 환경에
  맞는 보안 정책을 수립하기 시작함(SQL 취약점, 영국)

3 보안 정책의 구조

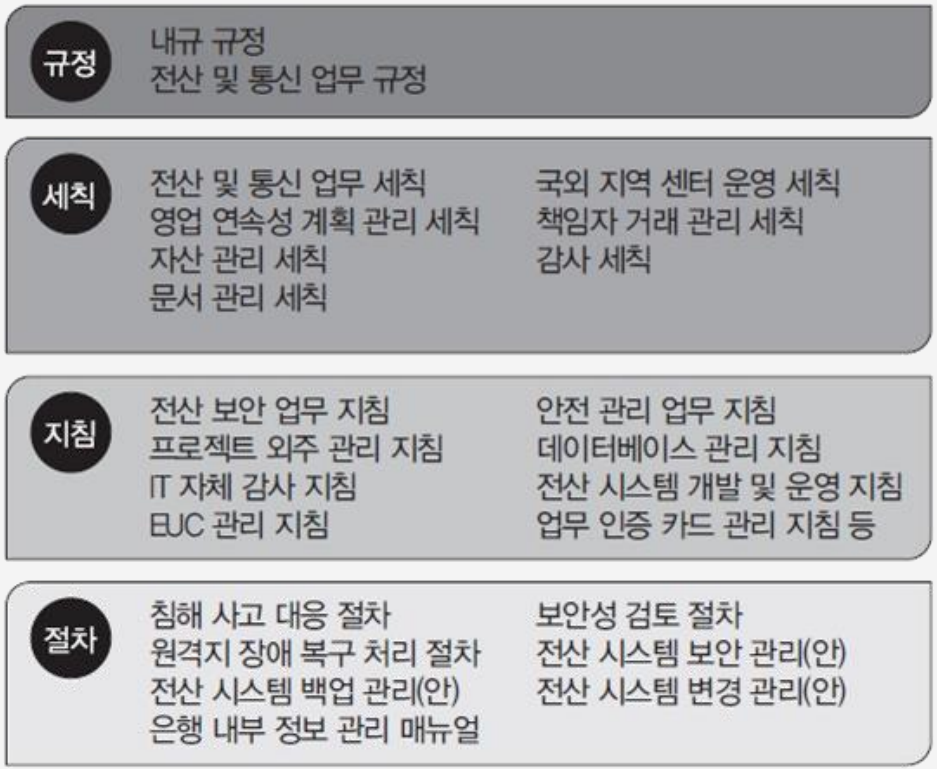
[일반적인 보안 정책 구조]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 보안 정책의 구조의 예

- 정책에 준 하는 문서를 '규정'이라 하고, 지침에 해당되는 문서를 '세칙'과 '지침'으로 구분



[A은행의 보안 정책 구조]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 보안 정책의 구분

- 규칙으로 지켜야 할 정책(Regulatory)
- 하고자 하는 일에 부합하는 정책이 없을 때 참고하거나 지키도록 권유하는 정책(Advisory)
- 어떠한 정보나 사실을 알리고자 하는 목적의 정책 (Informative)
- 보안 수준에 따라 나누기도 함

6 Security Policy

- 조직의 상위 관리자가 만든 보안 활동에 대한 일반적인 사항을 기술한 문서
- 일반적으로 5쪽 정도의 분량이며, 최대 10여 쪽을 넘지 않음

6 Security Policy

- 기록 내용
  - 보호하려는 자산(유형, 무형)
  - 정보 소유자와 그의 역할 및 책임 정의
  - 관리되는 정보의 분류와 기준 정의
  - 관리에 필요한 기본적인 통제 내용

7 Standards

- 일반적으로 지켜야 할
  보안 사항에 대해 기술한 문서

- 세부 기술까지 설명하지는 않고
  일반적인 표준 절차만 담고 있음

8 Baselines

- 조직에서 지켜야 할 가장
  기본적인 보안 수준을 기술한 문서

9 Guidelines

- 특정 상황에 대한 충고나 방향 등을 제시한 문서
- 부합하는 Standards가 없으면
  Guidelines를 참고하여 행동을 결정

10 Procedures

- 가장 하위의 문서로, 각각의 절차에 대한 세부 내용을 담고 있음
- 일반적으로 말하는 매뉴얼 수준의 내용을 포함

11 정보보호관리체계(ISO 27001)

- 영국에서 처음 만들어진 BS7799 Part1(실행 지침)과 Part2(규격)를 근거로 발전(영국, ISMS)
- BS7799 Part1은 2000년에 ISO/IEC 17799로, Part2는 2005년에 ISO/ IEC 27001로 국제 표준에 등록
- 2007년에 ISO/IEC 17799가 ISO/IEC 27002로 전환
- 이후 ISO/IEC 27001은 정보보호관리체계에 대한 국제 표준이자, 가장 권위 있는 국제 인증이 됨

11 정보보호관리체계(ISO 27001)

[ISO 27001의 통제 영역별 주요 내용]

통제 영역	개수	주요 내용
보안 정책	2	정보보호에 대한 경영진의 방향성 및 지원을 제공한다.
정보보안 조직	11	조직 내에서 정보보호를 관리하는 데 활용한다.
자산 관리	5	자산을 파악하고 이를 적절히 보호하는 데 활용한다.
인적 자원 보안	9	인적 오류, 절도, 사기, 시설의 오용에 따른 위험을 저감한다.
물리적 · 환경적 보안	13	사업장의 비인가된 접근 및 방해 요인을 예방한다.
통신 및 운영 관리	32	정보처리 시설의 정확하고 안전한 운영을 보장한다.
접근 통제	25	정보에 대한 접근을 통제한다.

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

11 정보보호관리체계(ISO 27001)

[ISO 27001의 통제 영역별 주요 내용]

통제 영역	개수	주요 내용
정보 시스템 취득, 개발, 유지보수	16	정보 시스템 내에 보안이 수립되어 있음을 보장한다.
정보보안 사고 관리	5	정보 시스템과 관련된 정보보안 사고와 취약점이 허용된 시기 이내에 적절한 교정 행동과 의사가 전달되는지 여부를 확인한다.
사업 연속성 관리	5	비즈니스 활동에 대한 방해 요인에 대응하며 중대한 실패 또는 재난으로부터 중요한 비즈니스 프로세스를 보호한다.
준거성	10	형법과 민법, 법령, 규정 또는 계약 의무 및 보안 요구 사항에 대한 위반을 피하기 위한 기준을 제시한다.
합계	133	

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

12 ISO/IEC 27001

- ISO/IEC 27001는 국제표준화기구 (ISO : International Organization for Standardization) 및 국제전기기술위원회 (IEC : International Electrotechnical Commission)에서 제정한 정보보호 관리체계 에 대한 국제 표준이자 정보보호 분야에서 가장 권위 있는 국제 인증으로, 정보보호정책, 물리적 보안, 정보접근 통제 등 정보보안 관련 11개 영역, 133개 항목에 대한 국제 심판원들의 엄격한 심사와 검증을 통과해야 인증됨

12 ISO/IEC 27001

- 한국에서는 한국품질재단(KFQ)과 같은
  인증기관이 ISO/IEC 27001인증을 제공하고 있음

13 개인정보보호

개인정보 유출 사고사례

사례	발생 시기	유출 규모	내용
KT	2012년 7월	870만 명	협력업체 직원이 5개월에 걸쳐 유출
SK컴즈	2011년 7월	3500만 명	해킹으로 네이트, 싸이월드의 고객 정보 유출
대부업체, 저축은행, 채팅 사이트	2011년 6월	1900만 명	개인 정보 DB 판매상이 중국 해커에게 의뢰하여 개인 정보 구입
신세계몰	2010년 3월	2000만 명	개인 정보 DB 판매상이 중국 해커에게 의뢰하여 개인 정보 구입
GS칼텍스	2008년 9월	1151만 명	GS칼텍스 상담 홈페이지의 고객 정보를 DVD에 저장하여 유출
옥션	2008년 2월	1863만 명	해커가 옥션의 웹 서버를 해킹하여 고객 정보 유출

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

13 개인정보보호

1 정책

- 개인정보보호정책(Privacy Policy)는 어떤 당사자가 고객의 개인정보를 어떻게 수집, 사용, 공개, 관리하는지를 밝히는 선언 또는 법적 문서를 말함
- 개인 정보는 이름 · 주소 · 생년월일 · 혼인여부 · 연락처 · ID번호 및 유효기간 · 재정정보 · 신용정보 · 의료기록 등 개인이 여행하거나, 매매계약을 체결하는 등의 상황에 있어서, 개인을 식별할 수 있는 정보들을 말함

13 개인정보보호

1 정책

- 어떤 개인정보들이 수집되고, 그것이 비밀로 유지되는지, 협력업체들과 공유하는지 또 다른 회사들에 어떻게 양도되는지 하는 등에 대하여 밝혀 놓고 있음(원래 공유, 양도 불가)

13 개인정보보호

1 정책

- 개인정보 보호정책은 그것이 개인의 신체와 도덕의 자치권에 기반하고 있으므로 현대국가에 있어서 중요한 의미를 지님, 그러한 이유로, 이것은 헌법적 보호를 받을 가치가 있음, 보호정책에 담겨야 할 내용들은 보호정책을 요구하는 관할 법률에 따라 달라질 수 있음, 대부분의 국가들은 누가 보호되고, 어떤 정보들이 수집되고 사용될 수 있는지에 대한 입법과 지침을 가지고 있음

13 개인정보보호

1 정책

- 일반적으로, 유럽에서의 데이터 보호법은 민간영역과 공공영역으로 나누어 정보를 보호하고 있음

13 개인정보보호

1 정책

- 이 법은 정부의 개인정보 관리에 뿐만 아니라, 민간회사들과 상업 거래에서도 적용됨(공공+민간), 북미에서 정보보호법은(퀘백 제외) 공공영역에서만 적용될 뿐, 민간영역에는 적용되지 않음
- 그러나, 북미의 민간 사업체들 대다수는 자신의 보호정책과 윤리강령을 발전시킬 동기를 가지고 있음(민간)

13 개인정보보호

2 역사

- 1968년 유럽평의회는 이전에는 널리 이용되지 않고 있던 방법으로 연결되고 전송될 수 있는 컴퓨터 기술에 의하여 야기된 새로운 위협을 인식하며, 인권에 미치는 기술의 영향에 대하여 연구하기 시작(컴퓨터 + 네트워크)

13 개인정보보호

2 역사

- 또한, 1969년 OECD는 개인정보 적용에 있어서 탈 국가화에 대하여 연구하기 시작
- 이러한 것들은 평의회가 개인영역과 공공영역에 걸쳐 개인정보의 보호를 발전시키도록 하는 정책을 추천하도록 이끔(개인 + 공공)

13 개인정보보호

2 역사

- 1981년, 개인정보의 자동적 처리에 관한 개인의 보호에 관한 협약(협약 제108호)이 도입
- 세계최초로 입법화된 개인정보보호법은 1973년의 스웨덴 데이터 법
- 뒤이어 1977년에는 서독의 데이터 보호법, 1978년 정보, 데이터 뱅크, 자유에 관한 프랑스법률이 잇달아 입법

13 개인정보보호

- 2013년 3월 23일부터
  안전행정부(현 행정자치부)는 개인정보보호법 시행

- 정부는 개인정보관리체계(PIMS) 도입(ISMS → PIMS)

14 PIMS에서 요구하는 주요 통제 영역

1 PIMS에서 요구하는 주요 통제 영역

분야	통제 영역	
보호 대책	1. 개인 정보 보호 정책	2. 개인 정보 보호 조직
	3. 개인 정보 분류	4. 교육 및 훈련
	5. 인적 보안	6. 침해 사고 처리 및 대응 절차
	7.1 접근 통제	7.2 암호 통제
	7.3 운영 통제	7.4 개인 정보 취급 시스템 개발 보안
	7.5 출력, 복사 통제	7.6 개인 정보 표시 제한
	8. 물리적 보호 조치	9. 내부 검토 및 감사
생명주기	1. 개인 정보 수집에 따른 조치	2. 개인 정보 이용 및 제공에 따른 조치
	3. 개인 정보 관리 및 파기에 따른 조치	

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

14 PIMS에서 요구하는 주요 통제 영역

2 PIMS

- 정보를 보호하기 위해 무엇을 어떻게 해야 하는지가 담김, 한국인터넷진흥원(KISA)이 정보 보호 활동을 계속하는 데 적합한 체계를 마련했는지를 살펴 인증해 줌(인증 기관)
- 기업으로부터 개인 정보가 대량으로 누출되는 사고가 늘자 보안 수준을 높이기 위해 마련한 제도
- PIMS 인증을 받으면 개인 정보 관련 사고가 일어났을 때 과징금 · 과태료의 절반(최대 경감치)까지 줄여 줌

14 PIMS에서 요구하는 주요 통제 영역

2 PIMS

- 그동안 방송통신위원회(인정 기관) 의결로 인증제를 운용했고, 2013년 2월 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 시행 근거를 마련함
- 제도를 활성화하려는 뜻
- PIMS 인증을 통해 시민이 개인 정보를 잘 관리하는 기업을 식별하는 효과를 기대

15 모바일 보안(BYOD)

- 기업에서 BYOD를 도입할 때
  보안 취약성을 최소화하기 위한 열 가지 방안

① **모바일 장치에 대한 보안 경험이 많은 컨설턴트 고용** : 보안 위반의 92%는 제삼자에 의해 발생하기 때문에 각 보안 기기의 연결 고리까지 보안 상황을 파악할 수 있어야 함

② **디바이스 제어 및 보안이 가능한 MDM/MAM 소프트웨어 도입** : 모바일 장치 및 앱 관리 소프트웨어는 매우 복잡하지만 상세한 사항까지 보안을 관리할 수 있음(MDM, MAM)

15 모바일 보안(BYOD)

- 기업에서 BYOD를 도입할 때
  보안 취약성을 최소화하기 위한 열 가지 방안

③ **모든 디바이스의 네트워크 환경에는 VPN 활용**
: 모든 네트워크 통신은 VPN을 통해 실행하고, 소프트웨어와 하드웨어에서의 VPN 사용법을 안내(VPN)

④ **디바이스에 패스워드 설정** : 많은 사용자가 디바이스의 암호화 설정을 '하' 등급으로 하고 있는데 이를 '상' 등급으로 높여서 설정함

15 모바일 보안(BYOD)

- 기업에서 BYOD를 도입할 때
  보안 취약성을 최소화하기 위한 열 가지 방안

⑤ **데이터 암호화 적용** : 개별 데이터 암호화와 전체 파일 시스템 암호화 중 장단점을 고려하여 회사의 정책에 맞는 암호화를 적용함(암호화)

⑥ **안티바이러스 소프트웨어 설치** : 각 디바이스는 기업의 네트워크에 작업을 진행하므로 MDM /MAM 안티바이러스 소프트웨어가 디바이스에 설치되어 있는지를 점검함

15 모바일 보안(BYOD)

- 기업에서 BYOD를 도입할 때
  보안 취약성을 최소화하기 위한 열 가지 방안

⑦ **ACLs(Access Control Lists)와 방화벽 설치**
: ACLs 및 방화벽은 소중한 데이터 및 파일을
취약한 시스템으로부터 보호하는 역할을 함
(ACL, 방화벽)

⑧ **데이터에 대한 감시 기능 확대** : 파일의 로그를
기록하는 등 감시 기능을 활성화하고,
SFTP(Secure FTP)와 같은 보안 기능 프로세스가
자동 실행되도록 함(로그, SFTP)

15 모바일 보안(BYOD)

- 기업에서 BYOD를 도입할 때
  보안 취약성을 최소화하기 위한 열 가지 방안

⑨ **로그 파일에 대한 통지 기능 설정** : 감시 로그, 시스템 및 이벤트 로그 등 모든 의심스러운 접근 시도에 대해 통지 및 저장 하는 기능을 설정함 (Alert)

⑩ **신뢰할 수 있는 사이트 제공 또는 앱 스토어의 다운로드 제한** : 사용자를 위해 승인된 앱 스토어를 화이트리스트에 등록 하거나 내부 앱 스토어를 통해서만 서비스를 제공받을 수 있도록 통제함(앱 스토어)

15 모바일 보안(BYOD)

- BYOD(Bring Your Own Device)
  - 회사 업무에 직원들 개인 소유의 태블릿 PC, 스마트폰, 노트북 등의 정보통신 기기를 활용하는 것을 일컫는 것으로, 2009년 인텔이 처음 도입
  - BYOD 업무환경을 조성하면 직원들이 업무용과 개인용으로 구분하여 여러 기기를 가지고 다녀야 하는 불편이 없어 생산성 향상, 회사의 기기 구입 비용을 줄일 수 있는 등의 효과(사적 영역 파괴)

15 모바일 보안(BYOD)

- BYOD
  - 그러나 개인이 자신의 기기로 회사 업무를 수행하기 때문에 기업의 보안을 유지하기 어렵고, 이를 이유로 보안을 강화할 경우 프라이버시가 침해될 수 있다는 단점(보안 유지 vs. 프라이버시)
  - 기업들의 도입이 전 세계적으로 확산되고 있으며, 우리나라에서는 2013년 10월 SK 텔레콤에서 BYOD 솔루션 'T 페르소나(Persona)'를 최초로 출시한 바 있음

16 사이버 보안(Cyber security)

- 정치적 또는 이념적 성향을 띤
  핵티비즘 형태의 해킹 공격이 자주 발생
- 기업 간 핵심 기밀을 해킹하는 사이버 첩보 활동이나
  국가 간 전산망을 해킹하는 사이버전 수준의 해킹
  공격도 빈번하게 발생
- 2012년 ISO에서는 사이버 보안을 위한
  국제 표준으로 ISO 27032:2012 발표

16 사이버 보안(Cyber security)

- ISO 27032:2012에는
  사이버 보안 위험에 다음과 같은 요소들 추가
  - 소셜 엔지니어링 공격, 악성 코드, 스파이웨어,
    기타 잠재적으로 위험한 소프트웨어(사회 공학,
    스파이웨어)

- 사이버 보안 표준에서 고려하는
  아래 요소도 정책 수립할 때 참고하면 좋음
  - Web 2.0, P2P 네트워킹, 인스턴트 메시징,
    Voice and Video over IP, 피싱과 소셜 네트워크
    사이(VoIP, mVoIP)

17 사회 공학

- 사회공학(社會工學, 영어 : Social engineering)은 보안학적 측면에서 기술적인 방법이 아닌 사람들간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법을 일컬음(비기술적 수법)

- 컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단, 우선 통신망 보안 정보에 접근 권한이 있는 담당자와 신뢰를 쌓고 전화나 이메일을 통해 그들의 약점과 도움을 이용하는 것 (사장님 메일)

17 사회 공학

- 상대방의 자만심이나 권한을 이용하는 것, 정보의 가치를 몰라서 보안을 소홀히 하는 무능에 의존하는 것과 도청 등이 일반적인 사회 공학적 기술

- 이 수단을 이용하여 시스템 접근 코드와 비밀번호를 알아내 시스템에 침입하는 것으로 물리적, 네트워크 및 시스템 보안에 못지 않게 인간적 보안이 중요 (네트워크 보안, 시스템 보안)

18 VoIP

- 음성 인터넷 프로토콜(VoIP, Voice over Internet Protocol, voice over IP, IP telephony)은 인터넷과 같은 인터넷 프로토콜(IP) 네트워크를 통해 음성 통신과 멀티미디어 세션의 전달을 위한 기술들의 모임을 가리키는 용어(IPTV)

- VoIP 전화뿐 아니라 VoIP는 수많은 개인 컴퓨터와 기타 인터넷 접속 장치에서 사용할 수 있음, 전화 및 SMS 문자 메시지는 모바일 데이터나 와이파이를 통해 보낼 수 있음(mVoIP)

2 보안 조직 구조와 역할

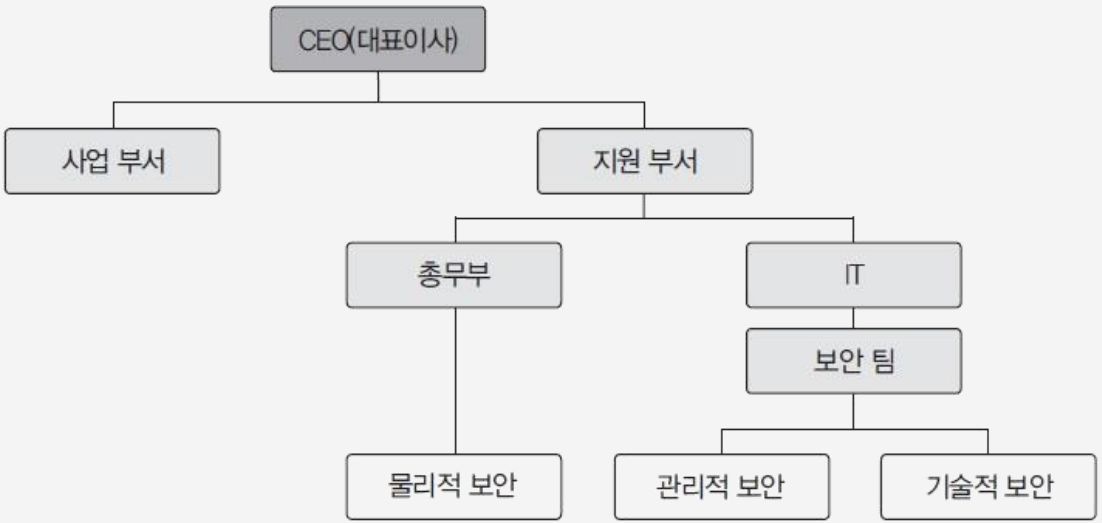
1 보안 조직의 필요성

- 2003년 1.25 인터넷 대란이 발생한 이후 2004년 국가정보원 산하에 국가사이버안전센터(NCSC) 설립 (SQL 취약점)

- 금융감독원은 전 금융권이 준수해야 하는 전자금융 감독 규정을 마련
  - 전체 임직원의 5%는 IT 인력으로 구성
  - IT 인력의 5%는 정보보안 인력으로 구성
  - 정보보안 관련 예산이 7% 이상이 되도록 권고

2 보안 조직의 구성 사례

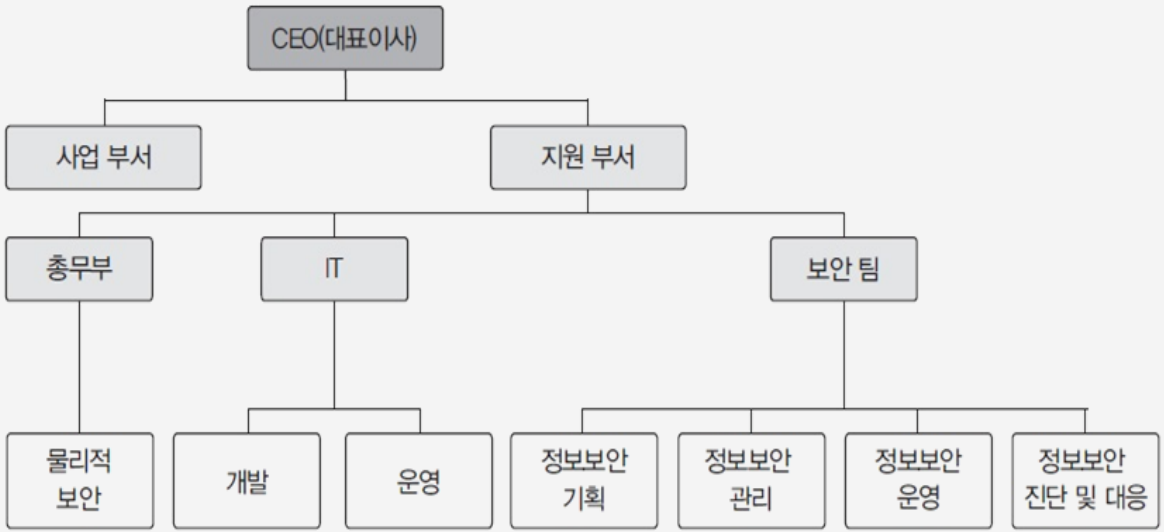
일반적인 회사의 보안 조직 구조



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 보안 조직의 구성 사례

보다 세분화된 보안 조직 구조



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 기획	정보보안 전략/계획 수립	• 전사 경영, IT 전략 및 위험 평가 분석, 동향 등과 연계된 단기/중 · 장기 정보보안 전략 수립 • 정보보안 동향 및 타사 현황 상시 파악, 보안 신기술 정보를 업데이트하여 향후 전략 및 사업 계획 수립에 반영 • 시스템 개발 또는 보안 장비 도입 시 보안 기술을 검토하고 그 적정성을 평가 및 검토한 결과를 협의하여 최종 결정 • 정보보안 투자 평가 기준에 따라 기술 검토와 예산, 효과 등을 평가하여 투자 우선순위를 결정하고 사업품의서를 작성하여 사업 진행
	정보보안 정책/지침, 표준 제정 및 관리	• 정책, 규정/지침 변경에 대한 환경 요인과 요구 사항을 검토 및 개정하여 ISMS (Information Security Management System)의 최신성 및 보안 인증을 유지하기 위한 활동 수행

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 관리	시스템 구축 및 보안 장비 도입	• 시스템 신규 개발 시 통합 구매를 통해 업체를 선정하고 보안성 심의를 통과한 시스템을 테스트 및 검수한 후 구축에 필요한 보안 적용 • 구축 완료 후 설계에 반영된 보안 대책이 적용되었는지 여부를 점검하고, 조치가 필요한 경우 적절한 조치를 취한 후 테스트 결과 보고 • 보안 장비 도입 시 보안 정책 적용이 잘되었는지 여부 확인 • 개발 전에 시큐어 코딩에 대한 가이드를 제공하고 교육 실시 • 개발 이후 설계에 반영된 보안 대책대로 구현되었는지 점검하고 시큐어 코딩 가이드를 기반으로 코딩이 수행되었는지 확인

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 운영	인프라 보안 운영 및 보안 장비 운영	• 모니터링 장치를 이용하여 정보보안 관련 시스템의 상태를 정기적으로 모니터링하고, 정보보안 관제에서 모니터링 업무를 수행할 수 있도록 정보보호 시스템에 대한 유지보수 등의 운영 관리 활동 수행 • 서버/네트워크/DB 보안 운영 업무 수행
	위협 및 취약성 관리	• 데이터, 애플리케이션, 시스템, 네트워크를 보호하는 데 필요한 프로세스, 기술, 서비스의 취약한 부분을 관리하기 위한 활동으로, 보안 취약성 진단 대상을 선정하고 진단 • 발생 가능한 보안 위협(해킹)에 대한 시나리오와 Baseline 방식으로 모의해킹을 수행하여 발견한 취약점에 대한 보호 대책 제시
	보안 관제	• 24시간 365일(24×365) 각종 보안 이벤트 모니터링과 alert에 따른 조치 및 분석 등의 활동 수행

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 운영	보안 교육	• 보안 교육 계획에 따라 대상별로 일정에 맞춰 주기적인 보안 교육 실시 • 교육 실시 결과를 평가하여 내년 교육 계획에 반영
	정보보안 사고 대응 관리	• 보안 사고 발생 또는 징후를 발견하여 신고/접수를 하면 긴급성을 판단하여 긴급한 경우 선조치, 아닌 경우 보안 사고를 분석/대응 • 보안 사고 재발 방지 대책을 수립하고 외부 관련 기관에 보고

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 모니터링	정보보안 성과 모니터링 및 성과 관리	• 정보보안 업무를 부여받은 자가 규정/정책대로 활동을 모두 수행했는지 체크리스트를 통해 활동 내역을 평가하고 그 결과를 임원에게 보고한 후 받은 지시 사항을 정리하여 정보보호 계획 수립 및 정보보안 정책/지침에 반영 • 주기적으로 정보보안 시스템 운영 현황과 변경/조치가 있는 건에 대한 분석 및 대응 결과를 보고하고 임원의 지시 사항을 정리하여 정보보호 계획 수립 및 정보보안 정책/지침에 반영
	정보보안 내부 감사	• 기업 내부 감사 인력에 의해 이루어지는 경영 활동의 일환으로 계획 수립, 실사, 리포트, 모니터링 등 네 단계로 이루어진 감사 활동에 참여

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 보안 업무의 역할과 책임

일반적인 정보보안 조직의 업무와 역할

구분	수행 업무	설명
정보보안 모니터링	아웃소싱 보안 관리	• 아웃소싱 서비스를 계약한 업체의 서비스 항목(SLA에 의해 이행해야 하는 사항)을 주기적으로 점검하는 활동으로, 이행 점검 기준을 수립하고 이행 점검 수행에 따른 조치 사항이 완료될 수 있도록 지속적으로 관리
	컴플라이언스 관리	• 외부 기관 감사 시 수검 준비, 조치 사항에 대한 조치 계획 수립, 그에 따른 조치 이행 관리 • 정보보안 내부 통제 계획에 따라 해당 부서의 수행, 조치 사항에 대한 지속적인 관리 수행

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017