Domain 4. 보안사고대응

Part 1. 업무지속성 계획

Chapter 1. 업무 지속성 관리 모델

1. 업무 지속성 관리

***1) 업무지속성 계획의 개념및 용어 정의

(1) **업무지속성 계획** (Business Continuity Plan): 조직이 재해,재난으로 인한 업무중단에 대응하여 핵심업무부문을 복구/재개할수있도록 하는 문서화된 정책및 절차

(2) **업무지속성 관리** (Business Continuity Management): 업무중단으로부터 발생할수있는 중대한 위험을 최소화하는 것을 목적으로 하는 총체적 접근법, 중대한 업무중단발생을 예방하고 업무중단발생시 핵심업무부문을 유지하거나 적기 복구하는 활동

(3) **업무중단** (Business Disruprition): 재해,재난으로 업무장소로 접근이 불가능하거나 현재 업무장소에서 업무수행이 불가능한 상황

(4) **업무영향분석** (Business Impact Analysis): 업무중단시 조직에 미치는 손실을 측정하고 재난발생시에도 수행되어야할 최소한의 업무를 정의하는 절차, 업무별 목표복구시간/ 복구우선순위/ 복구에 필요한 자원/ 필수인력등을 식별하는 활동

(5) **위험평가** (Risk Assessment): 위험요인을 평가하여 위험의 우선순위를 파악, 위험에 노출된 핵심업무를 파악하거나 위험에 대한 통제방법을 개선하여 업무중단을 예방하기위해 기존의 통제방법을 평가하는 절차

(6) **업무복구** (Business Recovery): 영업상 책무를 충분히 이행할수있도록 업무기능 복구하기위한 절차

(7) **업무재개** (Business Resumption): 영업복구후 새로운 영업상 책무를 이행할수있도록 업무기능이 회복된 상태

2) 업무지속성관리의 필요성:

업무지속성관리는 일회성 프로젝트가 아니라 지속적으로 조직의 경영 및 기술환경 변화를 즉각적으로 반영할 있어야 하는 일련의 관리 프로세스이다. 업부지속성관리에 대한 개념적 틀과 방법론 개발이 필수

3) 기타관리와의 관계및 범위

(1) 업무전략,기술전략과의 관계

(2) 업무지속성계획, 재해복구와의 관계

(3) 보안관리와의 관계

(4) 업무지속성관리 범위 결정요인

4) 업무지속성 관리단계

(1) **1단계. 개시단계:** 업무지속성 관리에 관한 정책 수립, 조직의 업무와 기술관련 정책과의 통합을 보장, 업무지속성 관리에 관한 제반 사항을 준비하는 프로세스

(2) **2단계. 전략수립단계**: 재해가 업무에 미치는 잠재적인 영향 및 위험을 평가하고 위험감소 및 업무프로세스 복구를 위한 여러옵션을 파악한 후 평가하여 업무지속성 관리를 위한 효과적인 전략을 수립하는 프로세스

(3) **3단계. 구현단계**: 업무가 지속적으로 운영되기위한 프로그램을 수립하는 단계, 업무지속성 전략에서 수립한 위험감소 조치및 재해복구를 위한 설비를 구현하며 필요한 업무복구를 위한 계획 및 절차를 작성하고 초기 시험을 수행하는 프로세스로 구성

(4) **4단계. 운영관리단계:** 업무지속성 전략, 계획및 절차를 계속적으로 시험, 검토 및 유지보수하며 적절한 교육및 훈련프로그램을 운영하는 프로세스로 구성되어 있다.

2. 국내외 표준 모델및 규정

1) **영국표준 BS25999**

(1) 정책의 의미: 영국 표준협회 (BSI)의 BCM표준으로 비즈니스 연속성을 이해, 개발,실행하기위한 기본 지침 제공하고 기업간 기업과 고객간의 거래에 신뢰를 심어주기 위한 것.

a. BS25999-1: BCM에 대한 일반적인 가이드와 프로세스 수립, 원칙, 용어등을 다루고 있으며 10개의 section으로 이루어져있음

b. BS25999-2: BCMS의 구축, 운영과 개선의 요구사항들을 명기하고 객관적이고 독립적인 심사를 위한 요구사항들을 기술하고 있으면 6개 section으로 구성

2) 금융감독원의 BCP 모범규준

(1) BCP수립범위

a. 핵심업무중단을 초래할수있는 가능성에 대비하는것을 전제로 BCP세울것

b. 주기적인 업부영향분석,위험평가,업무지속성관리전략수립 등 통해 기수립한 BCP, BCMS 를 지속적으로 개선하고 보완,유지해야

(2) BCP관련 조직의 역할

a. 이사회와 경영진: BCP수립/실행에 궁극적 책임을 지는곳은 이사회, 경영진, BCP는 일상적 경영관리에 통합되어야

b. 전담조직: BCP기능 전담조직 마련,운영

전담조직의 역할:

- 이사회/경영진의 BCP 책임수행 보조, - BCP관련 정책,절차마련등 문서화
- 각 영업,지원부서의 BCP관련 업무지원 - 핵심적 영업/지원부서에 대한 최소 BCP요건 설정
- 핵심 영업,업무중단에 대비한 보험가입여부 검토 -모니터링/통제 -경영진 보고/조치이행

c. 기타내부조직 및 외부기관:

BCP의 현실성,적정성과 관련부서의 정책/규정준수여부 점검

(3) 업무영향분석 (BIA)

a. **업무영향 분석**: 업무중단시 조직에 미치는 손실을 측정하고 재난발생시에도 수행되어야할 최소한의 업무를 정의하는 절차, 업무별 목표복구시간/ 복구우선순위/ 복구에 필요한 자원/ 필수인력등을 식별하는 활동

b. **복구전략**: 업무중단에 대비하기 위한 절차, 복구계획을 수립하여 이사회와 경영진의 승인을 받고 테스트를 수행해야한다.

c. **목표 복구시간(RTO):** 목표 복구시간은 특정 업무기능을 복구하기위한 목표시간으로서 특정영업기능 중단이 조직에 심각한 영향과 손실을 미치지않는 범위내에서 허용가능한 시간을 의미한다.

d. **목표 복구 시점(RPO):** 업무의 계속적 수행을 위해 손실된 데이터에 대한 손실허용시점을 의미

(4) **위험평가**: 위험요인을 평가하여 위험의 우선순위를 파악, 위험요인의 영향력에 따라 위험의 우선순위를 파악해야

(5) **BCM 전략의 수립:**

a. 재해로 인한 업무중단발생시에도 최소수준의 핵심영업, 업무를 지속하기위해 핵심영업,업무의 복구,재개방안등 업무지속성 관리를 위한 자체 전략을 보유하여야하며 전략마련시 영업환경, 리스크특성, 비용효익에의 적합도를 고려해야

b. **은행에 맞는 업무지속성관리모델**: 주사업장/ 백업사업장모형 , 상호주사업장/백업사업장 모형, 교대주사업장/대체사업장 모형, 위기시대체업무처리 모형

(6) **BCP 수립**

a. **위기 관리방안 마련:**

ㄱ. **위기관리 조직 구성**

- 위기관리팀 (CMT: Crisis Management Team), 위기관리위원회와 같은 위기관리 조직을 설치함으써 재해,재난으로 인한 업무중단 발생시 이에 대해 단계적으로 대응하고 지휘, 총괄할수있게해야

ㄴ. 위기관리 절차의 마련: 아래 사항에 대한 문서화된 절차 필요

ㄷ.의사소통, 정보교환 및 홍보 방안 마련

b**. 영업 재개 절차**

ㄱ. **동원단계(the mobilization phase)**: 영업,업무부서 복구팀에 통보, 업무재개에 필요 자원확보, 영업복구순서 결정

ㄴ. **대체 업무의 수행단계(the alternate processing phase)**: 대체사업장 이용한 핵심업무 재개

ㄷ. **완전 복구 단계(the ful recovery phase):** 원래 사업장으로 복귀

c. **기술 자원의 복구**

ㄱ. 어프리케이션,하드웨어장비,네트웍시설,전산시스템등 영업재개과정에 필수적인 기술자원을 효과적으로 보고/복원할수있는 방안을 마련하도록 하고있다.

ㄴ. 금융전산분야 위기대응 메뉴얼 : 금융전산시스템에 대한 위기대응은 메뉴얼을 따른다.

d. 중요 정보/기록의 관리 : 업무복구에 필요한 중요정보엔 즉시 접근하여 내용확인할수있게

(7) **대체 사업장의 마련**: 입지조건,목표복구시간을 감안하여 핵심업무와 기술복구위한 대체사업장소를 마련하도록 권고

(8) **BCP의 시범 테스트**

전형적인 시범시행(Full scale test), 데이터센터복구테스트, 영업점 복구테스트, 비상대응 테스트: 연 1회

(9) 모니터링 및 보고

(10) 예시...

3. 업무지속성 관련 기법 및 유형

1) **업무영향 분석 (BIA) :** 고객 사업수행에 어떤 위험요인이 잠재하고있으며 이러한 잠재적 위험요인이 미칠수있는 영향의정도

*** 업무영향 분석 흐름**

요약		방법
위험분석	전산시스템기능에 영향줄수있는 각종 위험요소 파악	위험의 개념 정립 위험대비의 필요성 전산장애/재해분석 사례분석
피해분석	전산로 인해 발생할수있는 피해내용 파악	피해종류 직/간접적, 총괄적 피해
업무중요도산정	장기적재해시 우선복구위한 중요도 분석	중요도 산정기준 업무별 중요도 계량화 업무별 등급화

2) 백업센타 유형

(1) 운영형태별 분류

a. **독자구축 방식**: 독자적으로 백업센타 운영, 보안용이, 고가의 투자,운용비용

b. **공동구축방식**: 공동으로 백업센타, 비용 절감, 보안이 용이X, 투자형평성 조정 어려움

c. **상호구축방식:** 상호백업센터 역할, 비용절감, 절차협의가 어렵고 재해발생시 생산성 저하

d. **외부위탁방식**: 외부용역, 비용절감, 유지보수가 용이 , 보안이 용이하지 X

(2) 운영주체별 분류

a. 자체운영: 독자구축방식

b. 공동운영: 공동구축형, 상호구축형

c. 위탁운영: 위탁방식

****** (3) 기술형태별 분류**

a. **Mirror site** : 주전산센터와 동일한 시설, 최신성,안정성,신속성 높은비용 RTO:즉시

b. **Hot Site :** 주전산센터와 유사한 시설, 최신성,안정성,신속성 높은비용 RTO: 수시간

c. **Worm site**: 기본시설,중요전산기기,네트웍 비용저렴, 초기복구수준:부분적 RTO: 수일,수주

d. **Cold site:** 기본시설만, 재해발생시 전사기도입,네트웍구축 가장저렴, 복구에 긴시간 RTO:수주,

(4) **위치기준의 백업센터 유형**

a. 0km: 스프링쿨러발수,하론방전, 파이프동파,해킹,고전압장애,HW장애, data손실, 정전

b. 5km: 폭발, 화재, 전력공급중단, 낙뢰, 고의적 시설파괴

c.30km: 집중호우 및 홍수, 테러, 비행기 충돌, 화학물질 누출, N/W 기간망 장애

d. 100km: 지직, 전쟁, 태풍, 전염병

******(5) 백업방안 기준의 유형**

a. **Hot Stanby**: 미러시스템, 동일한 시스템 이미지

b. **DB Shadowing**: db 레벨의 상호백업, DB의 로그,저널이용하여 db를 백업센타에 생성

c. 원격백업: 시스템유무상관없이 on-line상의 DASD 및 테이프 백업

d. **Log/Journal 전송**: db 레벨의 상호백업, 원격백업방식/PTAM사용하여 로그,저널만을 백업센타로 , db는 복구시에만 생성

e. **OS백업**: 시스템구성만을 백업센터에 백업, PTAM방식으로 데이터 전송, 주기적 db생성

f. **단순백업**: ptam방식에의해 백업테이프만을 백업센타,원격지 테이프보관창고로 이동저장

Chapter 2. 업무 지속성 추진 절차

1. 업무 지속성 추진 절차

1) HP의 BCP 방법론

(1) 방법론 개요

(2) 방법론 세부내용

a. 1단계. 착수단계

b. 2단계. 평가및 분석

c. 3단계. 계획과 설계

d. 4단계. 실행

e. BC운영계획 수립

(3) 성공적 BCP수립 고려사항

2) 공공기관 업무지속성 관리 수립방안

(1) 방법론 개요

(2) 방법론 세부내용

a. 1단계. 개시단계

b. 2단계. 전략수립단계

c. 3단계. 구현단계
d. 4단계. 운영관리 단계
(3) 성공적 BCP수립 고려사항

2. 각종 고려사항 및 사례

1) 제해복구 센터 고려사항
(1) 재해복구센터 위치선정 고려사항
a. 주요자원의 동시공급중단 위험성 : fault tolerance확보
b. 동일 재해 영향권 위험성: 15~80km 이격
c. 테러의 위험성
d. 인력 가용성과 교통문제
e. 기술적 고려사항: mirror / hot site의 경우 데이터복제방식으로 인한 거리적인 제약존재
f. 비용고려사항:
(2) 재해복구센터 구축장소의 고려사항
a. 공간 확보 b. 보안성 c.경제성 d. 확장성
e. 확장성 f. 안전성 g. 지리및 기후조건 h.네트워환경 i.관리용이성
(3) 재해복구시스템 기술 결정 고려사항

2) 업무지속성 계획 정책 사례
(1) 업무지속성 계획 개요
(2) 업무지속성 계획 모형
(3) 업무지속성 계획 표준

Part 2. 보안사고 대응

Chapter 1. 보안사고 대응

1. 사고 탐지

1) 사고대응팀 (Incident Response Team)
(1) 정의: 위기대응팀(Emergency Response Team)이라고도함. 위기사고 대비, 사고발생시 대응하는 인력의 그룹, 대개 사고발생전 지정된 특정한 멤버로 구성됨
(2) 구성원: 사고조사자, 사고처리자, IT보안전문가
임시구성원: 업무대표, 법률자문가, 홍보담당자, 인사담당자, 기타보안관련자, 위험관리및 IT전문가
(3) 구성방식:
a. 중앙(centralized) 사고대응팀: 하나의 대응팀이 조직의 모든 사고를 다룸, 소규모,근거리
b. 분산(Distributed) 사고대응팀: 논리/물리적으로 분리된 지점에서 발생된 사고, 대규모, 산재조직
c. 조정(Coordinating) 사고대응팀: 중앙팀은 정책/표준개발, 분산팀: 사고대응하여 직접관리/수행
d. 외주(Outsouced) 사고대응팀: 완전 또는 부분적으로 외부조직에서 담당
(4) 훈련:
a. 특정상황에서 필요 역할을 완수할수있게 훈련되고 준비되야한다.
b. 소규모사고: 자발적/임시적 팀 대응, 대규모사고가능성: 지정/임시구성원이 연합지휘체계
c. 사전에 정의된 대응절차, 행동방식 숙지, 다양한 상황에 대비한 훈련
2) **보안사고의 종류**
(1) 위협 : 환경적 위협, 기술적 위협, 인적 위협

(2) 취약성

(3) 위험

(4) **보안사고의 개념및 분류**

a. 보안사고: 보안정책이나 지침에 어긋나게 위반하거나 위반의 가능성이 있는 위협, 다양한 사건에 대한 보고가 발생할때 우선순위를 정하여 시기적절하게 대응할수있도록 보안사고를 분류해 두어야 한다.

b. **보안사고의 분류**

ㄱ. 서비스 거부: 자원의 고갈을 유발시키는 공격

ㄴ. 악성코드: 시스템을 감염시키는 바이러스,웜,트로이목마, 기타 악의적 코드

ㄷ. 비인가 접근: 허가없이 IT자원에 논리적,물리적으로 접근하는것

ㄹ. 부정사용: 네트웍/컴퓨터 정책에서 허용안되는 방식으로 접근하는것

ㅁ. 다중요소: 단일사건에서 다수의 보안사고를 포함하는것악성코드+비인가접속+부정사용

(5) **보안사고의 등급**

보안사고의 등급은 기밀성,무결성,가용성 측면에서 분류, 3~5 등급의 등급체계

1급: 조직에 심각한 영향을 미치는 기밀급 정보자산에 대한 유출:

서버,시스템,네트웍,데이터에 대한 침해, Ddos인한 서비스정지, 주요시스템 바이러스감염, 정보서비스와 관련된 사기/부정행위

2급: 대외비급 정보자산에 대한 유출:

서버,시스템,네트웍,데이터에 대한 시스템 권한의 단순오남용(비인가접근조회)

3급: 일반 정보자산에 대한 유출:

중요하지않는 시스템에 영향을 미치는 바이러스감염, 금전적 피해를 유발X는 보안사고

3) 보안사고 모니터링

(1) 시스템 로그 설정

a. 시스템 관리자는 추적성 확보위해 아래항목의 시스템 로그를 보관해야한다.

- 사용자 인증및 인증관련사항 -사용자 계정의 접속 관련 내용 -패스워드 관련내용
- 사용자인증 실패 -시스템관리자 계정으로 이루지는 활동 -네트웍을 통한 작업
- 시스템 다운과 재가동 -시스템 에러및 수정내용 -주요데이터 파일에 대한 접근
- 설정파일에 대한 접근권한 및 변경관련 내용 -장비에 대한 접근관련 내용

b. 단말기 통한 접근시 아래 항목의 로그가 포함되어야 한다

- 보안정책에 따라 허용되거나 거부된 접속, -보안시스템 구성요소로부터의 에러메시지
-다중 접근시도 -보안시스템의 정지/재가동

(2) 로그관리및 분석

a. 정보시스템 관리자가 로그를 기록할 때 준수해야할 관리지침

- 네트웍에 연결된 모든시스템의 내부시각은 일치 -로그기록을 매체에 백업
- 로그파일 정기백업, 로그변조 방지대책 수립 - 로그기록에 대한 접근통제, 감시
- 접속로그는 정보보호책임자의 공식적인 요청이나 법규에서 정한 경우외엔 공개불가
- 일반적인 로그는 정해진 기간보관, 이 기간동안 로그기록을 임의변경 금지

b. 서버/네트웍 보안담당자가 로그분석해야할때 준수해야할 지침

- 침해예방위해 로그를 정기/수시 점검
-서버,네트웍사용로그정보 주기적 분석, 정보보호 관리자에게 보고하여 불법접근,변조위험 방지
-접근기록분석결과 부적격사용, 불법시도일시 적절한 조치

(3) 시스템 모니터링

a. 서버운영담당자: 아래 사항에 대해 보안관리자에게 보고

- 정보시스템의 무단 사용, 파괴, 도난 - 정보의 임의변경, 회손
- 비밀정보의 유출,파괴, 변조 - 사용자 ID도용및 패스워드 유출
- 바이러스 감염및 악성프로그램 발견 - 기타 침해사고 및 침해흔적의 탐지로 판단될수있는 경우

b. 네트워크 운영담당자: 아래 사항에 대해 보안관리자에게 보고
- 네트웍 작동불능,파괴,변조 -비인가자의 불법적 접근 -기타 침해사고

c. 보안시스템 운영담당자: 아래 사항에 대해 보안관리자에게 보고
- 보안시스템 사용량 부하, - 사용자 접속현황 - 불법접속 및 변경시도
- 서비스 설정 - 접속허용및 거부된 IP주소설정 - 로그저장 공간 확보

4) 보안사고 판단

(1) 보안사고 판단의 어려움

(2) 보안사고 표시기

a. 보안사고 indicator

ㄱ. **침입가능 표시기 (possible indicator)**: 보안사고가 야기될수있는 비정상적인 것, 수상한 파일, 알려지지않는 프로그램, 예상치않은 자원의 사용, 설명되지않는 시스템 고장

ㄴ. **의사침입 표시기 (probable indicator)**: 샐행시키지않는 행위가 시스템에서 실행, 예기치 않는 시간에 시스템이 동작하거나 새로운 계정의 출현, 공격의 신고, 침입탐지시스템의 탐지결과

ㄷ. **침입표시기 (definite indicator):** 해커신고접수, 공격에 의해 정보의 도난,가용성/성능저하가 초래된 것을 확인한경우, 침입이 확인되면 침입의 형태와 결과, 근절 대책 수립이 필요

b. 수작업: 알려진 유형의 침입은 자동화도구 이용가능, 새로운 침입방법은 수작업 조사 필요

ㄱ.탐지 방법
- 특별한 장소/행위로부터발생한 접속에 대한 로그파일 조사 -setuid, setgid 파일 조사
- 시스템바이너리 파일 변경조사 - 인가받지않는 네트웍 모니터링 프로그램 사용 조사
- cron과 at로 수행되는 모은 파일 검사 -인가받지않은 서비스 조사
- /etc/passwd파일조사, 변경부분 검사 -시스템,네트웍 설정파일의 인가받지않는 항목 조사
- 시스템숨김파일, ‘.’로 시작하는 특이한 파일 조사 - 지역네트웍의 모든 시스템 조사

2. 상황 보고

1) 의사소통의 중요성

(1) **보안사고의 신고:** 정보이용 사용자의 잘못되었다는 신고(정보의 손실,변경,삭제,시스템 오작동) 에 주로의존, 잘훈련된 사용자그룹가진 조직은 보안사고를 신속히 신고,대응 가능

(2) **보안사고의 공지:** 보안사고 공지절차는 사전에 수립

--> (누가공지? 공지포함내역? 언제공지? 공지대상?, 공지방법?)

* 보안사고공지가 사고처리 방해해서는 안됨, 토론한 필요없이 진행, 외부의 불필요간섭 배제

2) **조직내부 의사소통**

(1) 사고대응팀으로의 초기연락: 초동조치 매우 중요, 비상연락망, 예비담당자지정

(2) 사고대응팀 내부의정보공유: 신고접수후 상황파악,정보소유자,공지필요성 우선 평가 , 정보 공유

(3) 조치 사항 보고: 부문별 보안담당자의 보고: 보안사고보고서 포함내역
- 유형 -등급 - 발생일시 -조치완료시각 -대상자산 -영향범위
-사고내용 -사고원인 -조치내용 -사후대책 -기타 보안사고와 연관된 다양한 증적

3) 공격사이트 연락: 공격사이트 파악 후 해당지역 사고대응팀 연락

4) 언론공개 :

a. 공개시 고려사항
- 공공 관련 부서(홍보,공보)통해 언론에 접속

- 공공 관련 부서 부재시 언론배포할 보도자료 내용 충분히 검토

b. 공개지침

- 아주 낮은 수준의 기술적 정보 제공 - 언론보도는 추측의 범위를 넘어설수있음에 유의
- 증거보존위해 법률전문가와 상의 - 준비가 되기전에 언론인터뷰 금지
- 사건에 대한 언론의 지나친 관심을 허용하지않아야

3. 복구 대책

1) 사고범위 식별과 평가

(1) 확산방지및 원인제거

(2) 제어권의 회복

- 비밀번호 변경 -서비스중지 -백도어제거 -활동 감시

(3) 피해범위의 결정

a. 사건의 범주와 영향을 정의 하기위한 질문

- 다중 사이트사건인가? - 사이트에서 많은 컴퓨터들이 이 사건에 영향을 받았는가?
- 민감한 정보와 깊은 관련있나? - 사건의 침입지점은 무엇?
- 언론의 관심이 지대한가? - 사건의 잠재적인 손실은 무엇인가?
- 사건을 종결하기위한 추정 시간은? - 사건처리을 위해 요구되는 자원은?
- 법적인 요건과 관련있는가?

2) 사고복구

(1) 우선순위 결정

(2) 취약성 관리

- 패치 적용 -서비스 보완 -절차 변경(보안과 연관된 기술, 업무상태, 법류등을 검토,변경)

(3) 보안대책 개선

(4) 복구절차

a. 비상복구 절차

-시스템별 복구절차및 방법 - 복구범위및 담당자 - 원인분석을 위한 증거자료 수집방법
-시스템 및 네트워크에 대한 취약점 제거등 사후관리 -재발방지위한 방안/기타 복구필요사항

4. 재발 방지

1) **후속처리**: 정보보안에서 가장 중요한 과정중 하나

사고후의 혼란스런 상황수습, 시스템 정상복구되면 이 시점에서 명확한 관점으로 후속분석시작

사고검토는 항상 일관성 유지, 조직의전부서에서 이루어져야, 결국 전체적인 품질향상을 가져옴

2) **사고의 문서화**: 후속처리시 가장 중요, 수립된 보안수준조정 및 향후 조치위한 근거(법적기소?)

(1) 시간대별 상황문서: log book, 대량의 정보 간추려 요약문서로 정리

(2) 기술적 요약서:

(3) 관리적 요약서: 사고의 범위,영향이해이한 내부적 관점제공, 보안관련 업무 의사결정시 결정적 역할

3) 사고평가

(1) 위험분석

(2) 업무영향 분석

(3) 사고분석: 대응과정 개선에 필요

a. 사고분석 질문: - 언제 무엇이 발생? -직원이 얼마나 잘 대응?
- 직원이 필요정보에 신속 접근할수있었나? - 다음사건엔 어떤것이 달라져야?

4) 법적 조치

보안사고는 여러가지 법률적 사항을 포함하고 있으므로 초기에 조직의 법률관련 부서나 관계자에게

사실을 알리고 법적으로 파생될 문제를 고려해야 효과적인 사고처리 가능, 공격에 사용된 방법이 일반인에게 잘 알려져있을 경우 소송제기가 특히 효과가 있음. (잠재공격자 방지에 도움?)

Chapter 2. 증거조사론

1. 포렌식 기법

1) **포렌식의 개념**

(1) 정의: 조사를 통해 법정에서 사용될수있는 사실을 확보하기위해 과학및 기술을 사용하는것. 컴퓨터 사고에 포렌식을 적용하는 중요한 목적은 가능한 최초 순간의 증거를 보존하기 위한것.

(2) 대상:

a. 컴퓨터가 대상인 범죄: 해킹

b. 컴퓨터를 매개로한 범죄: 전자상거래 사기, 음란물, 사이버 도박등...

2) **증거 수집:** 특별히 훈련된 포렌식 전문가가 수행하는것이 적합,

(1) 증거의 종류: 백업, 시스템로그,보안로그가 이용됨, 누가 언제 수행했는지 구체적 일지 매우 중요

(2) **증거의 신뢰도**: 증거의 신뢰도는 법원의 판사와 배심원에의해 판단, 다음을 고려해야

- 직접증거(강한 신뢰도)와 정황증거(약한 신뢰도)
- 증거에 대한 인증 : 주장하는 바에 대한 근거가 무엇인가에 의해 지원받아야
- 풍문규칙(Hearsay rule): 법정에서 배제됨
- 최적 증거규칙 (Best Evidence Rule) 원본이 법적에 제공되어야,
- 증거사슬(Chain of Evidence=Chain of Custody): 증거의 발생지, 책임자,내용,보호방법,변경여부등 일련의 기록을 의미, 증거가 수집되어서 법정에 가기까지 무결성을 유지해야)

(3) 로그의 유지와 보호:

- **보호기법: 전자서명, 안전한 타임스탬프, 임무분할,전용컴퓨터의 사용**

(4) 증거의 변조 방지

a. 변경,파손없이 전자적 증거를 포착하고 보존하는 기법

- 컴퓨터에 대한 물리적,원격 접근 제한
- 컴퓨터 작동중일때 화면이미지 촬영후 플러그 분리
- 복사본 디스크에서 포렌식 분석
- -컴퓨터가 꺼져있을때 켜지않음
- -키보드 건드리지않음
- 믿을수있는 OS사용하여 복사본 분석수행

3) 증거 유지

2. 증거분석

1) 분석방법

(1) 격리 분석:

- 대체시스템있어서 정상서비스 가능한 경우 나 분석할 동안 서비스 안해도될 경우
- 정확한 증거보존 필요한 경우, 아주 철저한 분석 필요한 경우,
- 격리이후엔 공격프로그램, 침입자 모니터링이 어려움

(2) 온라인 분석 (최소한의 자원으로 최소한의 분석만 원할때)

- 대체백업시스템 없어서 정상서비스 불가경우
- 공격프로그램, 공격자 활동을 지속 모니터링가능
- -원격지의 시스템을 빨리 분석해야할 경우
- 분석도중 침입흔적 손상가능, 정확분석 어려움

(3) 분석시스템 이용

- 피해시스템의 디스크이미지 복사해서 분석, 증거훼손없음, 보다 정확한 분서가능
- 분석시스템 준비, 디스크복사등 준비사항 많고 시간이 많이 걸림

2) 분석 준비

(1) 현장 동결

(2) 분석시스템 준비
(3) 디스크 이미지복사
3) 시스템 분석
(1) 시스템 상태에 따른 자료분석
(2) 공격시간대 중심의 분석
(3) 잘 알려진 공격기법에 대한 분석
a. /etc/passwd 파일 점검 b. cron, at 테잉블 점검 c. 백도어파일 점검
d. 트로이목마 파일점검 e. root소유의 SUID권한점검
(4) MAC시간에 근거한 분석: 반드시 분석시스템을 이용하여 분석해야 , TCT같은 분석도구-MAC획득
Mtime: 파일생성,파일변경한 시간 Atime: 파일읽거나 실행한 시간 Ctime: 속성변경된 시간
Dtime: 파일삭제된 시간
(5) 해킹프로그램 분석
a. 남겨진 잔해에 따른 공격의도
- 이진파일만 있는것: 흔적찾기 난해, 실력있는 공격자에 의한것
이진프로그램 분석:
* 정적 분석(공격프로그램 미실행, 도구이용)
* 동적 분석(공격프로그램 실행, 도구이용 바이너리변화,입출력값분석)
- 로그파일, 히스토리파일, 루트킷 설정파일: 스크립트키디
- 침입흔적없는것: 의심만 가는... 장시간 분석,모니터링 필요
(6) 로그파일 분석
(7) 지워진 파일 복구

3. 법적 처리

1) 증거의 문서화
(1) 증거사슬 양식
- 증거관리자의 이름/연락처 -증거내용획득/이동시점,이유,행위자 - 증거에 대한 세부 식별자
- 물리적, 논리적 저장위치 - 반환시점
(2) 기술자 관련 정보:
- 기술자의 증거획득위한 점검항목 - 증거획득위한 세부활동로그, - 기밀유지 서약서
(3) 소송 정보
-요청접수날짜, - 수사할당 날짜 -수사관,요청자이름/연락처
-소송번호 -소송/요건에 대한 내용,완료절차, - 완료시기
(4) 수사 보고 양식
- 수사관 이름/연락처 -수사일자,소송번호 -수사관련 인터뷰,의사소통 내역 -획득장비,데이터정보
-획득,분석에 사용된 SW/HW도구 -관련데이터 표본이나 복사본을 포함한 발견물과 저장위치
-담당 수사관의 표명
2) 법적 고려사항
- 법률적 기소의 일상업무에 어떤 영향을 주는지 검토할 필요가 있다.
- 내부인의 공격일 경우 조직의 신뢰성 저하등의 문제로 인해 조직내부에서 처리하는 경우 많음
- 재정적으로 이익이되고 무형적으로 조직에 도움이 될수있는지 파악하여 실행해야한다.