침해 사고 예방를 위한 대응 방안

CJ ENM 공진희

목차

Chapter I. 침해사고 예방 위한 사내 전략

0. Intro

경영진에게 제일 많이 듣는 질문 TOP 5

1. 우리 회사의 보안 상태는 어떻습니까?
2. 경쟁사들은 어떤 수준인가요?
3. A사가 해킹을 당했던데, 우리는 안전한가요?
4. 회사의 보안 솔루션은 잘 구축되어 있나요?
5. OOO에 대한 보안 솔루션을 도입했으니, OOO는 이제 침해 사고의 위험이 없어진거죠?

1. 보안 솔루션의 Coverage

현재 우리 회사에서 운영 중인 보안 솔루션에 대한 평가를 해야합니다.

Coverage 가시성

보안 약점이나 결함에 대해 “보호되는 영역”과 “보호되지 않은 영역 (Security Hole)”의 식별이 가능한가?

- 솔루션의 설치 및 유지 관리 뿐만 아니라, 보호할 자산과 위협에 대해 얼마나 효과적으로 방어할 수 있는지 평가하는 것 중요

보안 솔루션 Coverage 확인 – 3가지 관점에서 검토

- ✓ 자산(Asset) 커버리지 – 모든 자산이 적절하게 보호되고 있는가?
- ✓ 위협(Threat) 커버리지 – 알려진 공격에 대해 얼마나 효과적으로 방어하고 있는가?
- ✓ 규정 준수(Compliance) 커버리지 – 법규와 내부 정책을 준수하고 있는가?

2. 보안 강화를 위한 전략

보안 솔루션의 Coverage 가시성 확보 방안으로 “보안 아키텍처와 보안솔루션 Mapping”하는 방법을 제안합니다.

보안 아키텍처(프레임워크)와 보안솔루션 Mapping

보안 아키텍처(네트워크, 시스템, 데이터 흐름 등) 위에

현재 운영 중인 보안 솔루션들의 기능(방화벽, 웹 방화벽, EDR, DLP 등)을 겹쳐서(Mapping) 살펴보는 것은,

우리 회사의 방어 체계에 대한 가시성을 확보하고

Security Hole을 직관적으로 식별할 수 있는 중요한 활동

2.1보안 아키텍처-보안솔루션 Mapping

기대 효과와 고려사항

전체 현황 파악
나무가 아닌 “숲 " 을 봐야

- 개별 솔루션의 기능 초점 → (관점 확대) **전체 IT 인프라 내에서 각 솔루션의 역할과 상호 연계 상황을 파악**하는 것
- “어떤 구역은 방화벽으로 보호되고, 어떤 서버는 EDR로 감시되지만 저 클라우드 저장소는 보호 장치가 전혀 없군요?” → **보호받지 않는 영역 쉽게 식별**
- **중복 투자로 비효율적인 요인 식별 용이**

원활한 소통 도구
이해와 공감대 형성

- “보안 투자 계획을 설명하셨지만, 솔직히 잘 이해가 되지 않습니다. 마치 청구서를 제게 내미는 느낌이에요.” - 경영진 및 재무 불만

보안 전문가가 아니더라도 현재의 보안 상황과 필요한 조치를 **시각적 제시, 쉽게 이해하고 공감대 형성** 가능

고려 사항
커버리지 확인 시 함께 고려할 사항

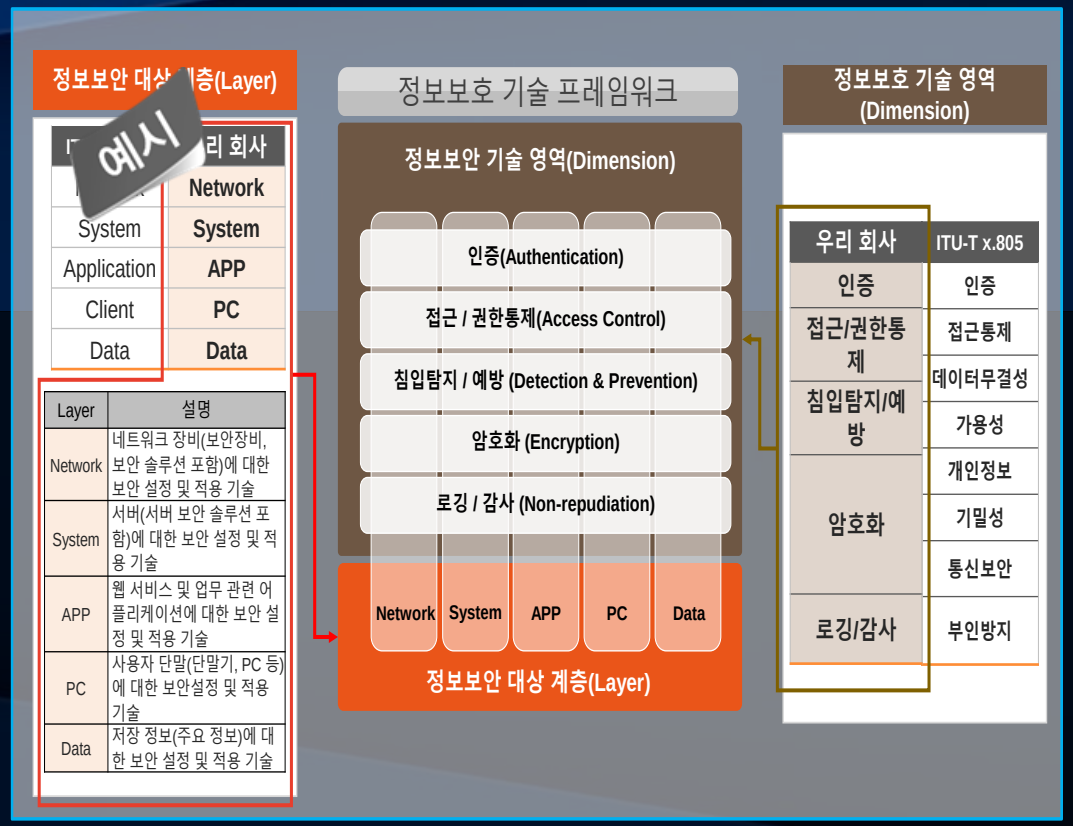
- **“솔루션의 기능 파악”**
  각 솔루션별 기능이 세부적으로 어떻게 되는지 확인
- **“보안 아키텍처의 최신성”**
  기존 아키텍처가 수립되어 있다면 현재 시스템의 상태와 관련 기준 등 최신 현황 반영
- **“자산의 최신성“**
  현재 자산에 대한 현황 파악 필수

3. 보안 아키텍처 수립 방법

Step 1. 범위 정의 (Scoping)

- 대상 선정: 보안 아키텍처 적용할 대상 정의.
  - ✓ 어떤 영역에 적용할 것인지 정의
    - 업무망 / 서비스 망 / 클라우드 등
    - 대외 서비스 시스템 / 대내 시스템 관련 모든 IT서비스/인프라
  - ✓ 계층에 대한 정의
    - Network, Server, PC, POS, DB, Data, System(Web service, Backoffice System etc.) 등

- 대상에 적용할 규제/기준 식별
  - ✓ 법률
    - 개인정보보호법 및 고시, 기준, 가이드라인 등 회사에 적용되는 보안 관련 법률 및 하위 문서
  - ✓ 사내 규정/지침/기준
  - ✓ 국내/외 보안 관련 표준/기준
    - ISMS-P, ISO27001, ISO27701, NIST 800-53, PC-DSS 등
  - ✓ 기타 회사 비즈니스 상 적용할 규제/기준



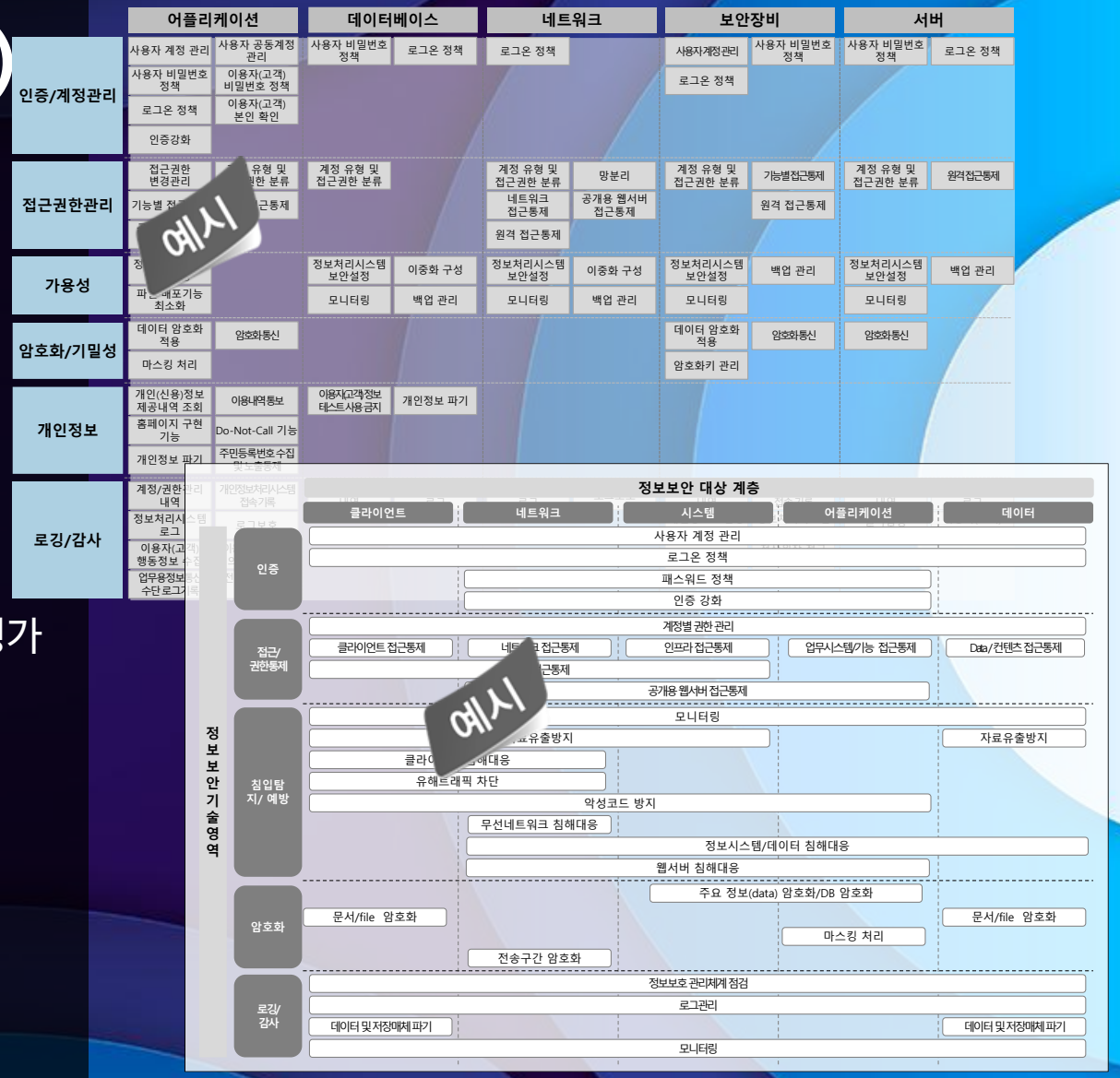
3. 보안 아키텍처 수립 방법(계속)

Step 2. 현황 분석 및 위험 평가

- **As-Is 분석**
  - ✓ Step1에서 정의하고 식별된 사항을 활용
    체크리스트 만들어 보안 현황을 파악함
    ex) ISMS-P 체크리스트(Base) +
    관련 규제/표준 규격 등 적용할 사항(Option)
- **위협 모델링 및 위험 평가**
  - ✓아키텍처 수립 대상 또는 회사(조직), 자산에 대한
    잠재적인 위협과 취약점 식별 → 발생 가능성과 영향도 평가
  - ✓위험에 대한 대응방안 및 우선순위 정함

Step 3. 목표 아키텍처 설계(To-Be)

- **기술적 보안 요소**
  - ✓ 정보보호 대상 계층별 적용되는 보안 기술을 정의
  - ✓ 각 요소들에 대한 구체적인 설계 필요
    - 구현되어야 하는 기능 / 프로세스



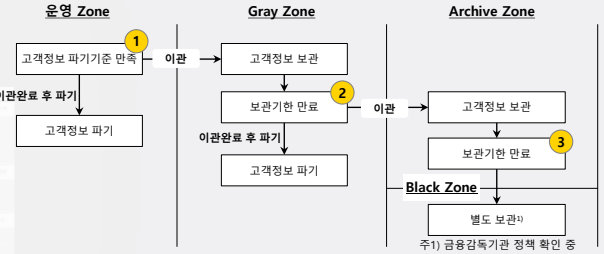
3.보안 아키텍처 수립 방법(계속)

(예) 보안 요소 설계 / 정의

1 고객정보 파기 Process

- 고객정보는 업무 목적이 달성되면 즉시 파기되어야 함(Archiving)
  - ✓ 법률 또는 문서관리규정에 별도로 보존연한을 규정한 경우에는 보존연한 만료 시까지 보관 가능
  - ✓ Archive Zone 보관 이후 Archiving을 통해 별도 보관하며 완전 삭제는 하지 않음

※ 고객정보 파기 절차



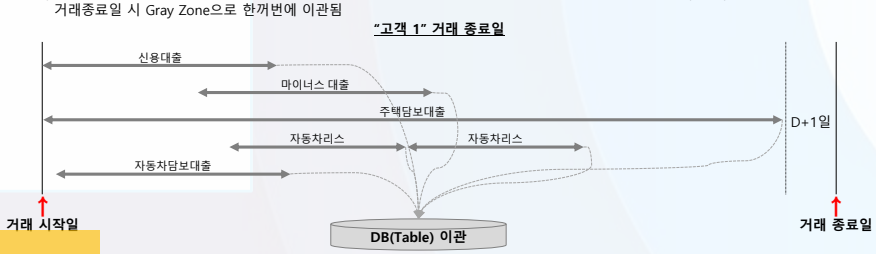
번호	설명	비고
①	고객정보 유입 유형에 따라 파기기준 적용	
②	운영Zone(Gray Zone 및 Archive Zone)	
③	운영Zone(Gray Zone 및 Archive Zone)	

- 접근통제 권한 관리
  - ✓ **Gray Zone**
    1) 접근 부서 및 접근자 : 고객센터 담당 부서 내 탈회고객 관리 담당자
    2) 접근 권한 승인권자 : 고객센터 담당 부서장
  - ✓ **Archive Zone**
    1) 접근 부서 및 접근자 : 준법감시팀 내 업무 담당자
    2) 접근 권한 승인권자 : 준법감시팀(준법감시인)

※ Gray Zone, Archive Zone의 고객 정보 복구 시에는 ***준법감시팀***의 통제에 따름

2.2 파기 시점 정의

- 고객정보 파기 시점
  - ✓ 고객정보는 통합고객DB에만 존재하며, 각 테이블은 고객ID만 이용하고 있음
  - ✓ **운영Zone → Gray Zone 이관 : 거래종료일 기준**
    1) **거래종료일 : 대출 잔액이 "0"원이 된 시점의 익일을 거래종료일로 정의함**
    2) 한 명의 고객에게 다수의 거래가 존재할 경우, 모든 거래에 대해 대출 잔액이 "0"원이 될 때 거래종료로 정의하며 익일을 거래종료일로 정의함
    3) 한 명의 고객에게 다수 거래 존재 시, 각 거래 별 대출 잔액이 "0"원이 되면 해당 거래 정보는 별도의 DB(Table)로 이관하며, 거래종료일 시 Gray Zone으로 한꺼번에 이관됨



- ✓ **Gray Zone → Archive Zone 이관 : Gray Zone 이관일 기준 2년 도래 시**
  1) 운영Zone에서 Gray Zone으로 이관된 날짜 기준으로 2년이 도래한 Data를 식별
  2) Archive 실행 시 해당 Data를 이관함
- ✓ **Archive Zone → Black Zone 이관 : Archive Zone 이관일 기준 3년 도래 시**
  1) Archive된 Data 중 Archive 수행일 기준 3년이 되는 Data를 식별
  2) 해당 Data를 Archive 실행하여 Black Zone으로 다시 이관함
- ✓ **Black Zone**은 Archive Zone에서 Archiving을 수행하는 것을 말함

※ 고객정보를 **완전 파기 하지 않고 Archiving을 2회 수행하며 접근통제를 강화하고 있음**

❖ Tip. 보안 요소 설계 시

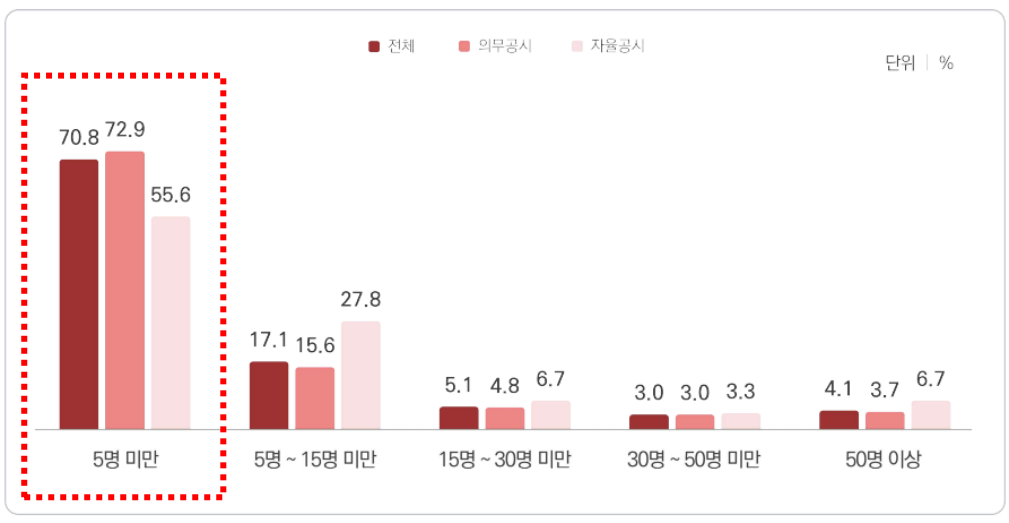
✓솔루션 / 시스템 개발 / 관리적 사항 구분

✓요소별 목표 수준 정의 → 단기/중기/장기 정보보호 로드맵 활용 가능

Chapter II. 조직운영 방안

우리는 항상 “인력이 부족하다”말합니다.

그리고 우리는 “조직의 규모를 어떻게 확대시킬 것인지”와 “현재의 조직 규모로 어떻게 효율적으로 운영할 것인지” 고민합니다.



* 출처: 2024 정보보호 공시 현황 분석(2024.12, 한국인터넷진흥원)

전체 기업의 “70.8%”

정보보호 전담인력 5명 미만

17.1% 기업, 정보보호 전담인력 15명 미만

1. 소규모의 인력 운영 방안

휴가, 외근, 외부 교육, 휴무 등으로 업무 담당자가 자리에 없을 때 관련 업무 처리가 지연되는 경우를 종종 봅니다.

규모가 작은 보안조직의 업무(보안활동)는 담당자 근무 여부와 상관 없이 수행되어야 하며, 관련 업무의 진행 상황은 조직내에서 언제든지 알 수 있어야 합니다.

T자형 인재

조직 문화

팀원들이 자신의 전문 분야를 넘어 다른 업무에도 관심을 가지고 서로 도와줄 수 있는 조직문화

조직 내부의 정보가 투명하게 공유되어 원활한 소통이 이루어지는 문화

자신의 의견을 솔직하게 나누고 새로운 시도를 서로 지지하는 문화

2. 성공적 조직 운영을 위한 제반 사항

리더의 역할 : 성장의 기회 제공

- 업무와 연관된 온/오프라인 교육 및 세미나 참여, 도서 구매 등 적극적인 지원
- 새로운 업무프로세스 도입 및 기존 업무프로세스의 변화에 대한 시도 지지/지원
- 구성원의 성장 방향에 대한 제시

기본틀 디자인

- 공통 역량 정의
- 공동 업무 정의
- 단순 반복 업무의 자동화
- 업무 프로세스의 표준화

환경 구축

- 조직 내 정보 공유를 위한 “협업툴”의 적극적인 활용
  – 자료/정보, 업무 수행 현황 등 공유
- 생성형 AI 등 적극적 활용하여 생산성 향상
  – 예, “개인정보보호법, 고시, 가이드 등”
  개인정보보호 관련 자료 정리 등 활용

Q&A

감사합니다.