조직의 보안 문제는 왜 반복될까?

보안전략연구소 박나룡

통제분야	통제영역	통제항목	결함
관리체계 수립 및 운영	2. 위험 관리	2.1 정보자산 식별	65
관리체계 수립 및 운영	2. 위험 관리	2.2 현황 및 흐름분석	129
관리체계 수립 및 운영	2. 위험 관리	2.3 위험 평가	50
보호대책 요구사항	5. 인증 및 권한관리	5.1 사용자 계정 관리	67
보호대책 요구사항	5. 인증 및 권한관리	5.6 접근권한 검토	61
보호대책 요구사항	6. 접근통제	6.1 네트워크 접근	26
보호대책 요구사항	6. 접근통제	6.2 정보시스템 접근	59
보호대책 요구사항	6. 접근통제	6.3 응용프로그램 접근	78
보호대책 요구사항	6. 접근통제	6.4 데이터베이스 접근	42
보호대책 요구사항	7. 암호화 적용	7.1 암호정책 적용	68
보호대책 요구사항	9. 시스템 및 서비스 운영관리	9.4 로그 및 접속기록 관리	55
보호대책 요구사항	9. 시스템 및 서비스 운영관리	9.5 로그 및 접속기록 점검	36
보호대책 요구사항	10. 시스템 및 서비스 보안관리	10.1 보안시스템 운영	121
보호대책 요구사항	10. 시스템 및 서비스 보안관리	10.2 클라우드 보안	57
보호대책 요구사항	10. 시스템 및 서비스 보안관리	10.8 패치관리	69
개인정보 처리단계별 요구	1. 개인정보 수집 시 보호조치	1.1 개인정보 수집 제한	21
개인정보 처리단계별 요구	1. 개인정보 수집 시 보호조치	1.2 개인정보의 수집 동의	86
개인정보 처리단계별 요구	2. 개인정보 보유 및 이용 시 보호조치	2.3 개인정보 표시제한 및 이용 시 보호조	54
개인정보 처리단계별 요구	2. 개인정보 보유 및 이용 시 보호조치	2.4 이용자 단말기 접근 보호	10
개인정보 처리단계별 요구	4. 개인정보 파기 시 보호조치	4.1 개인정보의 파기	121
개인정보 처리단계별 요구	5. 정보주체 권리보호	5.1 개인정보처리방침 공개	124

출처: ISMS-P 연도별결함통계(23.12)

1. 리소스 부족

- 인력이 양성되고 있는 시기

- 정보보호 인력의 숫자는 충분하지 않고,
- 전문인력은 더 부족하고,
- 법률이나 사회적 요구사항은 늘어나고,
- 예산은 항상 부족하고..

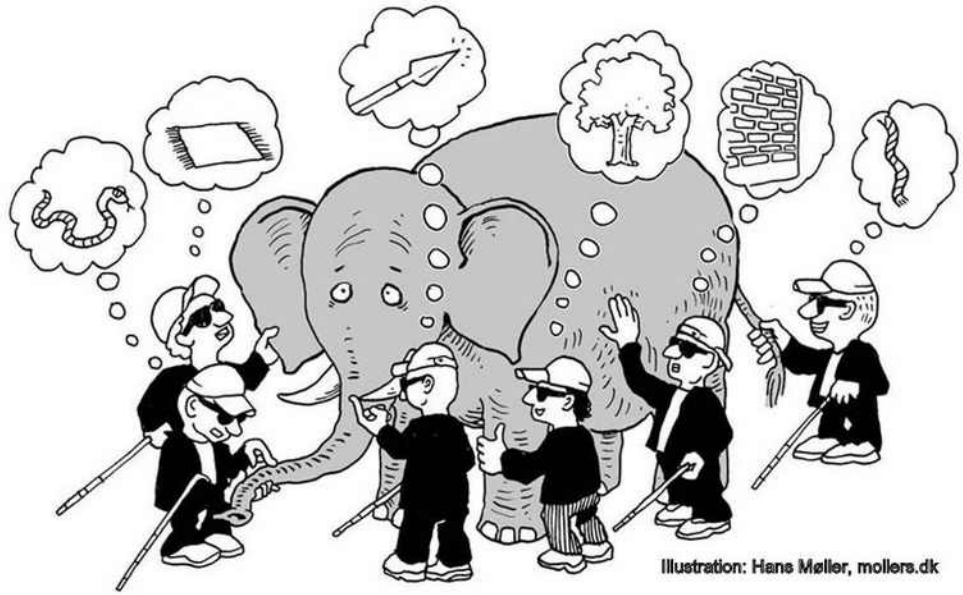
- 리소스는 보안 수준을 결정하는 중요 요소

2. CISO, CPO 역량

- 성장하고, 배우는 양성 단계
- 대표, 이사회 의지 확보
- 조직원 역량 확보를 위한 투자
- 조직간 힘 조절 (타 조직의 이해를 얻어낼 수 있는 지략 필요)

3. 커뮤니케이션

- DB에서 5년 지난 개인정보 삭제해 주세요.
  - 어떤 DB ? 어느 테이블 ?
  - 개인정보면 이름 ? 주소 ? 전부 ?
  - 5년 시점 ? 대상 서비스 ? 앱, 웹 ?
  - 삭제는 * 처리 ? Null 처리, Delete ?



4. 수평전개

- A 방화벽에서 불필요한 정책이 있어 확인하고 삭제했다.
  - B 방화벽, C 방화벽, D 방화벽은 ?
  - 정책(Rule)을 적용하는 다른 시스템은 ?

5. 프로세스

- 개인정보 3자 제공 업체 변경을 개인정보 조직에서 알 수 없다면 ?
- 시스템 유지보수 업체 담당자 정보의 변경을 알 수 없다면 ?

- 개발 시 보안성검토 프로세스
- 프로세스는 가시성 확보(식별, 검토, 확인 등)를 위한 필수

6. IT 환경의 복잡화

- 조직의 모든 IT 환경을 아는 직원이 있을까 ?
- 기존 레거시 시스템 + 신규 시스템 + 변경 시스템... + 클라우드 + Devops...
- 모든 리스크를 식별할 수 있는가 ?

7. 순환 근무

- 익숙해지면 다른 부서로 발령
- IT 내부 통제 방안으로 효과적인가 ?
- IT 환경에 맞는 전문인력 활용 방안 고민 필요

8. 그리고

- 조직원의 당연한(?) 무관심 : 내 일이 더 중요하다.
- 우선순위에 대한 조직원의 이해 : 그렇게 중요한 줄 몰랐다.
- 통상적인 업무 방식 : 예전부터 이렇게..

9. 그럼에도 불구하고

- 지속적 개선(대응능력)은 이루어지고 있다.

PASCON 2024

2024 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

감사합니다!

ISSSI@ISSSI.ORG