1. 초기 대응 (Immediate Response)

1. 사실 확인 (Fact-Check)

- 기사의 출처, 작성일, 작성자, 인용된 증거 및 제3자 확인 가능 여부를 검토.
- 회사 내부 로그, 시스템 상태, 네트워크 트래픽, 관련 구성 요소들을 확인해 동일하거나 유사한 이상 징후가 있는지 조사.

피해 범위 파악 (Scope Assessment)

- 해당 문제가 어느 범위(부서, 시스템, 서비스)에 영향을 주는지 정의.
- 내부 사용자/고객/파트너 등이 어떤 데이터 혹은 서비스가 침해 또는 노출됐는지 확인.

긴급 차단-완화 조치 (Containment & Mitigation)

- 공격 또는 이상 발생 지점이 확인되면 즉시 접근 차단, 방화벽 설정 변경, 권한 조정 등의 조치.
- 만약 보안패치 미적용, 취약점 존재 등이 원인이라면 긴급 패치 적용.

커뮤니케이션 (Communication)

- 내부 경영진/팀원에게 현재 상황, 취약성 및 예상 위험을 투명하게 공유.
- 필요시 법무부서, PR/홍보팀 등과 협력하여 외부 공개 여부 및 메시지 조율.

2. 원인 분석 및 재발 방지 (Root Cause & Prevention)

1. 원인 조사 (Root Cause Analysis)

- 로그 분석, 네트워크 패킷 캡쳐, 시스템 설정, 소스코드 등을 조사하여 문제의 근본 원인 파악.
- 내부 보안 정책 미비 또는 인적 실수 여부도 체크.

취약점 평가 및 점검 강화

- 관련 시스템 및 서비스의 보안 취약점 스캔 및 점검 실행.
- 정기적인 침투 테스트(Penetration Testing) 및 내부 보안 감사를 실시.

보안 인프라 강화

- 방화벽, IDS/IPS, 로그 모니터링, SIEM(보안정보 이벤트 관리) 시스템 등의 운영 및 보완.
- 인증 및 접근 제어 강화 (예: 최소 권한 원칙, 2차 인증, 역할 기반 접근제어).

교육 및 인식 제고

- 직원 대상 보안 인식 교육 확대 (피싱, 무단 접근, 데이터 유출 등).
- 내부 보안 절차의 매뉴얼화 및 누락된 절차가 없는지 검토.

3. 법적, 규제적 대응 및 보상

1. 관련 법규 및 규제 준수 여부 검토

- 개인정보 보호법, 정보통신망법 등 적용 가능한 국내법/규정 준수 여부 점검.
- 피해 데이터가 개인정보라면, 개인정보보호위원회 신고 여부, 고객·당사자 통지 요건 등 검토.

계약 및 보험 영향 확인

- 서비스 수준 계약(SLA), 보안 관련 조항, 책임 및 보상 범위 확인.
- 사이버 보험이 있는 경우, 보험사와 연락하여 보상 가능성 및 청구 절차 시작.

피해자/이해관계자 공지

- 피해가 확인된 경우 고객이나 해당자에게 사실 및 대응 조치, 향후 방지 계

획을 투명하게 안내.

4. 장기적 보안전략 강화

1. 보안 정책 및 거버넌스 체계 구축

- 보안 책임자(CSO / CISO)의 역할 및 책임 명확화.
- 정기적인 보안 보고 및 감사 체계 마련.

모니터링 및 탐지 역량 강화

- 이상 징후 탐지(Anomaly Detection), 침해 탐지 시스템, 로그 분석 역량 보강.
- 지속적인 위협 인텔리전스 활용, 최신 공격 트렌드 대응.

위기 대응 계획 (Incident Response Plan) 정비

- 사고 대응 시나리오 및 체크리스트, 역할 분담, 커뮤니케이션 플랜 마련.
- 정기 테스트(모의 사고 drills) 및 개선 주기 확보.