NIST Computer Security Incident Handling Guide Summary

Chapter 2. Organizing a Computer Security Incident Response Capability

BoB7기 취약점분석 정성조

첫 번째로 고려할 것은 자신(기업)만의 사건에 대한 정확한 정의가 필요하다는 것이다.

특정 사건에 어떻게 대응팀이 대처할 것인지, 어떤 대응팀이 대처할 것인지가 중요하다.

계획, 정책, 절차는 내/외부의 대응팀과의 의사소통이 반영되어야 한다.

# 사건의 종류

* 대용량 연결 요청을 보내 크래쉬를 일으킨다.
* 스미싱
* 민감한 정보가 노출되고 돈을 내지 않는다면 공공에 노출시키겠다고 위협
* P2P를 통한 민감한 정보의 노출

# 사업의 담당자는 이를 따라야 한다

* OMB’s Circular No. A-130, Appendix III: 연방 기관은 시스템에서 보안 사건이 발생했을 때, 사용자에게 도움을 줄 수 있는 능력이 보장되어야 하고 우려되는 흔한 취약점과 위협의 정보를 공유해야 한다. 다른 기업들에게 정보를 제공해야 하고 Department of Justice guidance와 일치하는 적절한 법적 행동을 만드는 것을 지원해야한다.
* FISMA: 기관은 탐지의 절차, 보고, 보안 사건 응답, 그리고 연방 정보보안 집중 센터를 설립해야한다. ; 보안 사건을 탐지하고 다루는 정보보안 기술을 제공해야 한다. ; 취약점을 분석해야 한다. ; 현재와 잠재된 보안 사건과 취약점을 기관의 보안 담당자에게 알려야 한다.
* FIPS: 연방 정보 시스템의 소규모 보안 요구
* OMB: 개인 인식 가능 정보의 위반에 응답하고 위반을 보호하는 것

# 사건 대응 정책은 매우 개인화 되어있지만 대부분의 정책에는 동일한 키 요소가 포함되어 있다.

* 정책의 범위, 사건 혹은 단어의 정의, 사건의 우선 순위, etc..

# 계획의 요소

* 할 일
* 전략과 목표
* 상사의 허용
* 사고 대응에 기업적 접근
* 사고 대응 팀의 내/외부 의사소통
* 사고 대응 능력과 효용성을 측정하는 행렬
* 숙련된 사고 대응 능력을 위한 로드맵
* 기업 전반에 프로그램이 어떻게 맞는가

# 절차의 요소

* 절차는 정책과 계획을 기반으로 해야한다.
* SOP: 표준 절차를 다룬다. (standard operating procedure)
* 실제 테스트를 기반으로 유효함이 검증되어야 한다.
* 훈련이 꼭 제공되어야 한다.

# 외부 기업과 정보를 공유하는 것

* 사건의 탐지와 분석의 향상을 위해 적절한 사건 지표를 공유해야 한다.
* 하지만 민감한 정보를 공인되지 않은 단체에 제공할 경우 잠재적으로 추가적인 방해와 재정 손실로 이어질 수 있다.

# 미디어

* 기술적 세부 사항 등의 중요한 정보를 공개하지 않은 채로 미디어와의 상호 작용을 하는 것이 중요하다. (미디어와의 상호 작용에 대한 교육을 실시한다.)
* 논의 전 특정 문제와 심각성에 대해 접근한다.
* 일관성, 최신 유지를 위해 진술을 유지한다.
* 모든 직원에게 절차를 알린다.
* 사고 수습 훈련 중 모의 인터뷰와 기자 회견을 실시한다.

# 법 집행

* 보안 관련 사건들이 제대로 판결을 받기 위하여 사고 대응 팀은 사고 발생 전 법 집행 담당자와 사고를 보고해야 할 조건을 논의해야 한다.
* 법 집행 기관에 연락을 취하기 위하여 하나의 사고 대응 팀을 POC(Point Of Contact)로 지정하는 것을 추천한다.

# 사고 보고 조직

* FISMA는 연방 정부 기관이라면 USRT (US-CERT)에 사고를 신고해야 함을 요구한다. (1차 및 2차 POC를 지정한 후 모든 사고를 보고해야 한다.)
* 모든 조직은 적절한 CSIRT(컴퓨터 비상 대응 팀; USRT: 미국 컴퓨터 비상 대응 팀)에게 사고를 보고하도록 권장된다. 적절한 CSIRT가 존재하지 않을 경우 ISACs(정보 공유 분석 센터) 등에 보고할 수 있다.

# 기타 외부 당사자

* 조직의 ISP (for 공격 차단 및 추적)
* 공격 주소의 소유자(for 증거 수집)
* 소프트웨어 공급 업체(for 로그, 위협 수집)
* 기타 사고 대응 팀(for 사고 보고 및 정보 공유)
* 영향을 받는 외부 당사자(for 적절한 정보를 제공)

# 사고 대응 팀의 구조

**사고 대응 팀이란?**

* 사고에 대한 정보를 모든 사람들한테 제공해야 한다.
* 사고 위협, 영향 분석 및 복구 조치

# 사고 대응 팀 모델

* 중앙 사고 대응 팀 (단일 팀이 사고를 처리한다)
* 분산 장애 대응 팀(여러 팀이 사고를 처리한다)
* 조정 팀(Coordinating Team)(다른 팀에게 조언을 제공한다)
* 직원들(모든 사고 대응 작업 수행)
* 부분적 아웃소싱(사고 대응 업무를 위탁한다)

일반적으로 24시간 모니터링을 위탁한다. 이에 대해 조직의 사건 대응 팀은 보고를 받을 수 있다.

* 완전히 아웃소싱

사고 대응 팀이 필요하지만 인력이 부족한 경우 사용될 가능성이 높다.

# 팀 모델 선택

* 실시간 가용성을 위하여 연중 무휴로 인력을 배치해야 한다. ( 24/7 Availability )
* 정규 시간 versus 파트 타임( 인력이 부족할 경우 임시 방편으로 사용 )
* 직원의 사기 ( 사고 대응 업무는 매우 스트레스를 주기 때문에 수행해야 할 행정 업무의 양을 줄이는 것은 사기에 큰 도움이 된다 )
* 비용 ( 광범위한 지식 체계를 위한 교육 비용 지원 )
* 직원 경험 ( 조직 내 기술 인력은 대개 외부 인력보다 조직의 환경에 대한 훨씬 더 많은 지식을 가지고 있다)

# 조직은 아웃 소싱을 고려할 때 다음 사항을 염두에 두어야 한다.

* 현재와 미래의 작업 품질
* 책임 부서(웹 서버 연결 끊기와 같은 문제를 담당자에게만 제공하기 위해)
* 조직 별 지식 부족
* 상관 관계의 부족(아웃 소싱 업체와 조직 간의 상관 관계는 매우 중요하다)
* 여러 곳에서 사고 발생 시 대처(예비 방문을 통한 효과적인 사고 대응)
* 장애 대응 기술 유지 보수

# 사고 대응 인원

1명 이상의 지정된 대체 인력을 가진 1명의 직원이 사고 대응을 담당해야 한다.

이 사람은 작업자의 작업을 감독하고 평가한다.

사고 대응 팀의 구성원은 시스템 관리, 네트워크 관리, 프로그래밍, 기술 지원 또는 침입 탐지와 같은 뛰어난 기술 능력을 갖추고 있어야 한다. 더불어 문제 해결 능력과 비판적 사고 능력도.

학습과 성장을 위한 기회를 제공함으로써 직원 이탈을 막는 것이 중요하다.

* 교육 자료 작성, 워크샵 실시, 연구 수행
* 직원의 교류 ( 충분한 인력 유치를 통해 직원이 없어도 휴가를 즐길 수 있도록 )
* 멘토링 프로그램
* 사고 처리 시나리오 개발 및 사고 처리 방법 논의

# 조직 내 의존도

모든 사고 대응 팀은 다른 팀의 전문 지식, 판단 및 능력에 의존한다.

* 경영진(사건 대응 조정, 피해 최소화, 보고)
* 정보 보증
* IT지원(IT기술 지원)
* 법무부(프라이버시에 대한 권리를 포함한 법률 및 연방 지침을 준수하는지 확인
* 홍보 및 언론 관계 (사건의 성격과 영향에 따라 대중에게 정보를 제공)
* 인적 자원
* 비즈니스 연속성 계획(비즈니스가 계속될 수 있도록 사고 대응 정책과 동기화를 해야함)
* 물리적 보안 및 시설 관리(손상된 워크스테이션을 복구)

# 장애 대응 팀 서비스

* 침입 탐지
* 자문 배포(새로운 취약성 및 위협에 대한 권고사항 발표)
* 교육 및 인식(취약점에 대한 교육 및 그에 대한 인식)
* 정보 공유(ISACs또는 지역 파트너십과 같은 정보 공유 그룹에 참여 후 기업 내에서 관련 정보를 공유)

# 권고 사항

* 공식적인 사고 대응 능력을 설정한다.(FISMA가 사고 대응 능력을 확립할 것을 요구한 것처럼)
* 사고 대응 정책을 만든다. (조직 구조 수립, 역할 및 책임 정의, 사고 보고 요구 사항 등)
* 사고 대응 정책에 따라 사고 대응 계획을 개발한다. (장애 대응 프로그램을 구현하기 위한 로드맵 제공)
* 사고 대응 절차를 개발한다. (사고 대응 정책에 근거하여 자세한 단계 제공)
* 사고 관련 정보 공유에 관한 정책과 절차를 수립한다. (이를 위해 법무부 및 경영진과 논의해야함)
* 사고에 대한 적절한 정보를 해당 기관에 제공한다. (연방 기관은 미국-CERT에, 다른 기관은 미국-CERT 또는 ISACs에 연락할 수 있다)
* 장애 대응 팀 모델을 선택할 때는 관련 요인을 고려해라.
* 사고 대응 팀에 적합한 기술을 가진 사람을 선택해라.(시스템, 네트워크, 프로그래밍, 기술 지원 및 침입 탐지)
* 사고 처리에 참여할 수 있는 조직 내 다른 그룹을 식별한다.(관리, 정보 보증, IT지원, 법무, 공공 업무 및 시설 관리 등)
* 팀이 제공해야 할 서비스를 결정한다.(주기능은 사고 대응이지만 대부분의 팀은 추가 기능을 수행한다. Ex) 권고 사항 배포, 보안 교육 등)