NIST Computer Security Incident Handling Guide Summary

Chapter 1. Executive Summary, Introduction

BoB7기 취약점분석 정성조

# Executive Summary

사이버 범죄와 관련된 공격은 더 다양하고 파괴적인 것이 되었다. 새로운 유형의 보안 사고가 자주 발생한다. 위험 평가 결과에 기초한 예방 활동은 모든 사고를 예방할 수 있는 것은 아니다. 따라서 장애에 대응하기 위한 능력이 필요하다. 이를 위해 본 안내서에서는 사고 관련 데이터를 분석하고 사고 처리 지침을 제공한다.

장애 대응 능력을 위해서는 상당한 계획과 자원이 필요하다. 따라서 공격을 지속적으로 모니터링하고, 사고 처리의 우선 순위를 결정하는 명확한 절차를 확립하며 내/외부 그룹과 적절한 통신 수단을 설정하는 것이 중요하다.

공격을 이해하고 초기 단계에서 식별하는 것이 향후의 타협을 방지하는 것의 핵심이며 사전에 조직간 이러한 공격의 신호를 공유하는 것은 공격을 식별하는 효과적인 방법이다.

조직은 공식적인 장애 대응 능력을 생성, 공급, 운영 해야 한다.

연방 법은 연방 기관이 사고를 USRT(미국 컴퓨터 비상 준비 팀)에 보고할 것을 요구한다.

FISMA(연방 정보 보안 관리 법)는 기관이 사고 대응 능력을 갖출 것을 요구한다.

장애 대응 능력의 설정에는 다음과 같은 조치가 포함되어야 한다.

* 사고 대응 정책 및 계획 생성
* 사고를 다루고 보고하기 위한 절차 개발
* 사고와 관련된 외부 파티와의 의사소통 지침 설정
* 팀 구조 및 인력 모델 선택
* 사고 대응 팀과 기타 그룹, 내/외부 간의 관계 및 의사소통 라인 설정
* 장애 대응 팀이 제공해야 할 서비스 결정
* 사고 대응 팀의 인력 배치 및 교육

문제가 발생한 후 대응하는 것보다 예방하는 것이 비용이 덜 들고 효과적인 경우가 많다. 대응에 필요한 자원과 용량이 부족한 경우 복구가 지연되거나 불완전해지고 더 큰 손실이 발생할 수 있다. IT직원에게 조직의 보안 표준에 대한 교육과 네트워크, 시스템 및 애플리케이션의 적절한 사용에 대한 정책 및 절차를 알려주어 장애 대응 능력을 보완하면 더욱 효과적으로 수행할 수 있다.

조직은 다른 조직과의 사고에 대한 상호작용을 통해 지침을 만들고 문서화 해야 한다.

사고를 처리하는 동안 조직은 외부 파티(법 집행 기관, 미디어, 피해자, etc)와 소통해야 한다. 신속해야 하기 때문에 통신 지침을 사전에 규정해야 한다.

본 안내서는 일반적인 공격 벡터에 기초하여 몇가지 유형의 사건을 정의한다. 공격 벡터는 다음과 같다.

* External3/RemovableMedia: 이동식 미디어 또는 주변 장치에서 실행된 공격
* Attrition: 시스템, 네트워크 또는 서비스를 손상, 저하시키는 공격
* Web: 웹 사이트, 웹 기반 응용 프로그램에서 실행되는 공격
* Email: 첨부 파일을 통해 실행되는 공격
* Improper Usage: 권한 있는 사용자가 사용 정책을 위반함으로써 발생하는 모든 사건
* Loss or Theft of Equipment: 컴퓨터 장치 또는 미디어의 분실 혹은 도난
* Other: 다른 공격

조직은 조직 전체에서 사고 감지 및 분석의 중요성을 강조해야 한다.

조직은 로그 및 보안 소프트웨어에서 적절한 정보를 수집하고 데이터를 정기적으로 검토할 수 있도록 로깅 표준 및 절차를 설정해야 한다.

조직은 사건의 우선 순위를 지정하기 위한 지침을 작성해야 한다.

개별 사건의 처리를 우선시하는 것은 사고 대응 프로세스에서 중요한 결정 사항이다. 사고는 사고의 기능적 영향과 같은 관련 요소를 기준으로 우선 순위를 매겨야 한다.

조직은 학습된 과정을 통해 사고로부터 가치를 얻어야 한다.

중대한 사고 후에는 회의를 개최하여 사고 처리 프로세스의 효과를 검토하고 개선 사항이 존재하는지 확인해야 한다. 이는 증거 목적 뿐만 아니라 향후 사건을 처리하고 새 팀원을 교육하는 데 참조용으로 중요할 수 있다.

# Introduction

* 1. 권한

NIST는 모든 기관 운영 및 자산에 적절한 정보 보안을 제공하기 위한 표준 및 지침을 개발할 책임이 있다. 이 지침은 자발적으로 사용될 수 있으며 저작권에 영향을 받지 않는다

* 1. 목적 및 범위

본 안내서는 사고에 대한 효과적이고 효율적인 대응을 위한 실질적인 지침을 제공함으로써 보안 사고의 위험을 완화하기 위한 목적을 가지고 있다. 문서는 사고 탐지, 분석, 우선 순위 지정 및 처리를 초점으로 맞춘다.

* 1. 관중

CSIRT, 시스템 및 네트워크 관리자, 보안 담당자, 기술 지원 담당자, 최고 보안 책임자를 위해 작성되었다.

* 1. 문서 구조

섹션과 부록으로 구성되어 있다.

* 2절에서는 사건 대응의 필요성, 대응 팀 구조, 사고 처리에 참여 가능한 조직 내 다른 그룹을 강조한다.
* .3절에서는 사고 처리 단계를 검토하고 사고 처리, 사고 감지 및 분석을 효과적으로 하기 위한 조언을 제공한다.
* 4절에서는 사건 대응 조정 및 정보 공유의 필요성을 검토한다.