# 담당자용 침해사고 초기 대응 요점 정리

침해 사고에 대응하는 담당자에게 도움이 되는 팁 모음

## 사고의 배경 파악하기

사고의 내용은 무엇인가? 과거에 발견되었던 문제인가?

이 문제를 어떻게 발견했는가? 언제 누가 발견했는가?

사고가 난 환경에 배치된 보안 장비는 어떤 것이 있는가? (방화벽, IDS 등)

장비들의 보안 상태가 어떤가? 장비들의 취약성에 대한 조사는 얼마나 자주 있었는가?

어느 조직이 이 사고에 영향을 받는가? 그 조직은 사고에 대해 알고 있는가?

최근 그 조직이나 그 환경에서 다른 보안 사고가 발생한 적이 있는가?

## 연락 방법 정하기

이 사고를 알고 있는 사람들은 누구인가? 알고 있는 조직 혹은 회사의 이름은 무엇인가?

누가 사고 대응 최고 책임자인가?

누가 사고와 관련된 회사 방침을 결정할 수 있는가? (보통 이사가 담당한다)

사고에 대응하는 팀은 어떤 식으로 연락하는가? (이메일, 컨퍼런스 콜 등) 어떤 암호화 방식을 써야 하는가?

내부 조사 일정이 어떻게 되는가? 누가 일정을 조율하는가?

외부 조사 일정이 어떻게 되는가? 누가 일정을 조율하는가?

사고 현장을 조사할 사람은 누구인가? 이름, 직함, 전화번호(회사, 휴대폰), 이메일 주소를 기록해둘 것

누가 홍보, 경영, 법률등 회사내의 다른 팀들과 협의를 담당하는가?

## 사고의 범위 파악하기

어느 서버, 웹사이트, 네트워크 등이 이 사고에 직접적으로 피해를 입었는가?

침해 당한 장비에서 사용하던 애플리케이션과 취급하던 데이터는 어떤 것인가?

이 사고에 대한 법적 책임에 대해 알고 있는가?

사고에 피해를 받은 장비, 웹사이트 등으로 통하는 진/출입 경로가 어떻게 되는가?

최초의 사고가 발생한 원인은 무엇인가?

사고의 피해를 받은 장비들이 다른 조직에 위험을 끼칠 수 있는가?

## 사고에 관한 최초 보고서를 재검토하기

최초 조사를 하면서 사용한 분석 방법은 무엇인가?

최초 조사를 하면서 사용한 명령어와 도구는 무엇인가?

사고의 범위를 줄이기 위해 사용한 방법은 어떤 것인가? (예를 들어, 네트워크를 끊는 방법)

보안 장비에서 발생한 경고는 어떤 것인가? (IDS, 방화벽 등)

검토한 로그 중에 수상한 것이 있는가? 그 외에 수상한 이벤트나 상태 변경이 있는가?

## 사고 대응 준비 단계

사고에 피해를 받은 조직은 침해사고에 대응하는데 필요한 가이드라인이나 규칙을 가지고 있는가?

사고에 피해를 받은 조직은 라이브 조사나 포렌식 조사를 할 의향이 있는가?

공격을 받은 서버, 네트워크 장비 등을 모니터링 할 때 어떤 도구를 사용할 수 있는가?

분석을 할 동안, 어떤 방법으로 공격 당한 장비에서 파일을 이동 할 수 있는가? (네트워크, USB, 시디롬등)

공격 당한 장비들의 실제 위치는 어디인가?

복구 작업을 진행할 때 어느 정도의 백업/복원 능력을 사용할 수 있는가?

이 사고에 대응하기 위한 다음 방법은 무엇인가? (누가 무엇을 언제 하는가?)

## 사고 대응 핵심 단계

1. 준비: 필요한 도구를 모으고, 사용방법을 익힌다. 사고가 발생한 환경에 대해 익숙해진다
2. 확인: 사고 범위를 확인하고, 필요한 사람을 소집한다
3. 억제: 사고가 끼치는 영향이 최소화 되도록 조치한다
4. 퇴치: 공격을 퇴치하고, 필요하다면 복구 작업을 한다
5. 복구: 시스템을 정상 상태로 복구한다, 필요하다면 시스템을 재설치 하거나 백업본을 사용한다
6. 마무리: 사고의 상세한 내용을 정리하고, 수집한 내용과 사고로 배운 교훈에 대한 이야기를 나눈다

## 기타 침해 사고 대응 관련 자료

서버 관리자용 침해사고 대응 방법 요점 정리
http://nchovy.kr/forum/3/article/331

윈도우 시스템 침입 탐지 요점 정리
http://sans.org/resources/winsacheatsheet.pdf

윈도우 시스템 침입 흔적 찾기
http://www.ucl.ac.uk/cert/win_intrusion.pdf

리눅스 시스템 침입 탐지 요점 정리
http://sans.org/resources/linsacheatsheet.pdf

리눅스/유닉스 시스템 침입 흔적 찾기
http://www.ucl.ac.uk/cert/nix_intrusion.pdf

Authored by Lenny Zeltser, who leads a security consulting team at SAVVIS, and teaches malware analysis at SANS Institute. Special thanks for feedback to Jack McCarthy and Patrick Nolan.
 한국어 번역, 구동언 8con@nchovy.kr, 감수, 양봉열, xeraph@nchovy.kr