NIST Computer Security Incident Handling Guide Summary

Chapter 5. Appendix (A-G)

BoB7기 취약점분석 정성조

# 부록 A: 사건 처리 시나리오

사고 대응 팀 또는 구성원은 주어진 시나리오 및 관련 질문 목록을 통하여 가장 가능성 있는 대답을 결정함으로써 잠재적인 문제를 효과적으로 식별할 수 있다.

# A.1 시나리오 질문

- 이 활동을 사건으로 간주하면 어떤 조직의 정책이 활동을 위반하는가?

- 사건의 방지 혹은 제한을 위해 할 수 있는 조치는 무엇인가?

# 탐지 및 분석

– 선동자가 있다면 감지할 수 있는가?

- 조직이 발견 한 사건의 지표는 무엇인가?

- 사건 탐지를 위한 도구는 무엇인가?

– 사건의 분석 및 검증을 위해 누가 참여할 것인가?

– 사건 보고는 누가?

– 사건 처리 우선 순위 결정?

# 해결 및 회복

- 조직은 사건을 처리하기 위해 어떤 전략을 취해야합니까? 이 전략이 다른 사람들에게 더 좋은 이유는 무엇인가

- 사건이 포함되지 않은 경우 어떻게 될 수 있는가?

- 이 사건에 대응하기 위해 필요한 추가 도구는 무엇인가?

- 봉쇄, 박멸 또는 회복 과정에 관련된 인원은 어느 것인가?

- 증거의 출처와 획득 방법 및 유지는?

# 사고 후

- 누가이 사건과 관련하여 교훈을 얻은 회의에 참석할 것인가?

- 앞으로 유사한 사건이 발생하지 않도록 하기 위해 무엇을 할 수 있는가?

- 유사한 사건의 탐지를 향상시키기 위해 무엇을 할 수 있는가?

# 일반적인 질문

- 이 사건을 처리하는 데 몇 명의 사고 대응 팀원이 참여하는가?

- 사고 대응 팀 외에도 이 사건을 처리하는 데 조직 내의 어떤 그룹이 관련됩니까?

- 보고는 누가, 언제, 어떻게 할 것이고 보고할 정보와 보고하지 않을 정보의 구분은?

- 외부 당사자와의 기타 의사 소통은 어떻게 될 수 있는가?

- 이 사건을 처리하기 위해 팀이 사용하는 도구와 자원은 무엇인가?

- 사건이 다른 요일과 시간에 발생했다면 처리의 어떤 측면이 달라졌을까?

- 사고가 다른 물리적 위치에서 발생했다면 처리의 어떤 측면이 달라졌을까?

# A.2 시나리오

**DNS server DOS**

비정상적으로 많은 양의 패킷을 회사의 공용 DNS 서버와 주고받고 있는지 확인한다.

- 문제의 외부 IP 주소와 관련하여 조직은 누구에게 연락해야 하는가?

- 내부 호스트가 문제를 일으키고 있음을 감지했을 경우 영향은?

- 시스템 소유자가 확인되기 전에 9 개의 내부 호스트 중 2 개가 네트워크에서 연결이 끊어진다고 가정한다면 시스템 소유자 확인은?

**warm or DDoS 침입**

웜이 확산되기 시작한 지 몇 시간 후에 바이러스 백신 서명이 가능 해지 기 전에 이미 조직에 널리 퍼진 감염이 발생하였다.

- 사건 대응 팀은 감염된 모든 호스트를 어떻게 식별하는가?

- 바이러스 백신이 배포되기 전, 조직이 웜의 침입을 막으려고 시도하는가?

- 바이러스 백신이 배포되기 전, 조직이 웜이 감염된 호스트에 의해 전파되는 것을 어떻게 방지하려고 하는가?

- 조직이 모든 취약한 시스템에 패치를 적용하려고 합니까? 그렇다면 어떻게 되는가?

- DDoS 에이전트를 받은 감염된 호스트가 다음날 아침 다른 조직의 웹 사이트를 공격하도록 구성된 경우이 사건 처리가 어떻게 변경 되는가?

- 감염된 호스트 중 하나 이상에 조직의 직원에 관한 중요한 개인 식별 정보가 포함 된 경우이 사건 처리가 어떻게 변경되는가?

- 사고 대응 팀은 사고의 상태에 대해 조직 사용자에게 어떻게 알리는가?

- 네트워크에 현재 연결되어 있지 않은 호스트를 위해 팀에서 수행할 추가 조치는?

**문서 도난**

도난된 문서가 해당 조직에 소속된 것으로 알려진 경우 FBI는 해당 문서의 합법과 누수 여부의 판별을 위해 사고 대응팀의 지원을 요청함

- 사고 대응 팀은 어떤 출처에서 증거를 수집 할 수 있는가?

- 팀이 조사를 기밀로 유지하기 위해 무엇을 할 것인가?

- 팀이 누수에 책임이 있는 내부 호스트를 확인한 경우이 사건 처리가 어떻게 바뀌겠는가?

- 팀이 누수를 담당하는 내부 호스트에 설치된 루트킷을 발견 하면 이 사건 처리가 어떻게 바뀌겠는가?

**데이터베이스 서버 손상**

특이한 디렉토리를 발견한 후 공격을 당했다. 조사 결과에 따르면 공격자가 루트를 획득하였다.

- 네트워크 암호를 계속해서 캡처하고 있는 경우?

- 중요한 고객 정보를 계속해서 전송하는 경우?

- 루트킷을 발견한 경우?

**알 수 없는 공격**

.RAR 파일을 통해 봇이 설치되었다.

- 팀은 .RAR 파일 내에서 가장 가능성이 높은 것을 어떻게 결정할 것인가? 어떤 다른 팀이 사고 대응 팀을 도울 수 있는가?

- 사고 대응 팀이 내부 호스트의 무선 네트워크 카드를 통해 초기 손상이 수행되었다고 판단한 경우 팀에서이 활동을 어떻게 조사 할 것인가?

- 인시던트 대응 팀이 내부 호스트가 기업 내의 다른 호스트의 민감한 파일을 처리하는 데 사용되었다고 판단한 경우 팀에서이 작업을 어떻게 자세히 조사 할 것인가?

**급여 기록 무단 접근**

급여 프로그램에 대한 마우스가 움직여져 있고 페이지가 바뀌어져 있다.

- 팀은 어떤 행동을 취했는지 어떻게 결정할 것인가?

- 임금 관리자가 전임 부서 직원으로 그녀의 사무실을 떠나는 사람을 인정한 경우이 사건의 처리는 어떻게 다른가?

- 팀이 그 사람이 현재 직원이라고 믿을만한 이유가 있다면 이 사건의 처리는 어떻게 다른가?

- 물리적 보안 팀이 사람이 사회 공학 기술을 사용하여 건물에 물리적으로 접근했다고 결정하면이 사건의 처리 방법이 달라질 수 있는가?

- 이전 주간의 로그에 급여 관리자의 사용자 ID를 사용한 원격 로그인 시도 실패 횟수가 비정상적으로 많았다면 이 사건의 처리 방법은 어떻게 다른가?

- 2 주 전에 컴퓨터에 키 입력 로커 가 설치되었음을 사고 대응 팀이 알게되면 이 사건 처리가 어떻게 달라 지는가?

**사라지는 호스트**  
IP 주소를 사용하는 호스트가 사라졌다.   
- 취약점 스캐닝 호스트의 ID와 관련된 점보를 포함할 수 있는 데이터 소스는 무엇입니까?  
- 팀은 취약성 검색을 수행한 사람을 어떻게 식별합니까?  
- 취약점 검색이 조직의 중요한 호스트에 대해 지시된 경우 문제를 처리하는 방법이 어떻게 달라집니까?  
- 취약점 검색이 회부 호스트를 대상으로 한 경우 이 장애의 처리 방법은 어떻게 달라집니까?  
- 내부 IP주소가 조직의 무선 게스트 네트워크와 연결된 경우 이 문제는 어떻게 처리됩니까?  
- 물리적 보안 담당자가 취약점 검사가 발생하기 30분 전에 누군가가 시설에 침입했다는 사실을 발견하면 이 사고를 처리하는 방법이 어떻게 달라집니까?  
**재택 근무**  
팀은 VPN 서버를 모니터링 하며 로그인된 ID와 행동 기록을 검토한다.  
- 팀의 다음 단계는 무엇인가?  
- 외부 IP주소가 공개 프록시에 속한 경우 이 사건 처리는 어떻게 다른가?  
- 사용자의 지식없이 ID가 여러 개의 외부 IP주소에서 VPN 연결을 시작하는 데 사용 된 경우 이 사건처리가 어떻게 다른가?

– 확인된 사용자의 컴퓨터가 가족 구성원이 다운로드한 게임의 트로이 목마를 통한 감염이라면?

– 백신 소프트웨어가 키 로거가 포함되어 있다고 판단한 경우 어떤 영향을 미치는가?

**익명 위협**  
직원이 조직 시스템에 대한 익명의 위협을 받았다고 주장한다.  
- 위협의 알림에 대응하여 장애 대응 팀이 다르게 수행해야 하는 작업은 무엇인가?  
- 강화된 물리적 보안 제어가 사고에 대한 팀의 반응에 어떤 영향을 미칠 수 있는가?

**P2P 파일 공유**  
동일한 내부 IP 주소로 세 건의 파일 공유 흔적이 있다.  
- 이 사건의 처리 우선 순위를 지정하는데 사용해야 하는 요소는 무엇인가?  
- 이 사건의 처리에 영향을 미칠 수 있는 사생활 침해는 무엇인가?

– P2P 수행 중 컴퓨터가 개인 식별 정보를 가지고 있다면?  
  
**알 수 없는 무선 액세스 지점**  
노트북이 이상한 무선 액세스 지점으로 연결되었다.  
- 이 사건을 처리하는 첫 번째 주요 단계는 무엇인가?  
- 액세스 지점을 찾는 가장 빠른 방법은 무엇입니까? 액세스 지점을 찾는 가장 빠른 방법과 비밀스러운 방법은 무엇인가?  
- 외부 당사자가 일시적으로 조직 사무실에서 근무하는 접근 지점을 구축했다면 이 사건의 처리방식은 어떻게 다른가?  
- 침입 탐지 분석가가 건물 같은 층에 일부 작업대와 관련된 의심스러운 활동 징후를 보고한 경우 사고를 처리하는 방법은 어떻게 달라지는가?  
- 팀이 물리적으로 위치를 찾고 있는 동안 액세스 지점을 제거했다면 이 사건의 처리 방식이 어떻게 다를 수 있는가?  
  
부록 B – 사건 관련 데이터 요소  
조직은 사건 보고시 수집할 기본 요소를 지정해야 한다. 몇 가지 요인을 기반으로 자체 요소를 작성해야 한다.

**기본 데이터 요소**  
인시던트 리포터 및 처리기에 대한 연락처 정보 ( 이름 연락처, 이메일 등 )

**사건 처리자 데이터 요소**  
인시던트 응답의 현재 상태 ( 사건 요약, 처리, 원인, 영향 등 )

부록 C – 용어집

기준선 - 중요한 편차가 검출되도록 전형적인 사용 패턴을 결정하기 위한 리소스를 모니터링

컴퓨터 보안 사고 - ‘사고’를 참조하라

컴퓨터 보안 사고 대응 팀 - 컴퓨터 보안 관련 사건 대응을 지원하기 위한 기능

컴퓨터 사고 대응 팀(CIRT) 및 CIRC(컴퓨터 사고 대응센터, 컴퓨터 사고 대응능력) 라고도 합니다.

이벤트 - 네트워크 또는 시스템에서 발생하는 모든 이벤트

거짓 긍정 - 악의적인 활동이 잘못되었음을 나타내는 경고입니다.

사고 대응 - 컴퓨터 보안 정책, 허용되는 사용 정책 및 표준 보안 관행 위반, 임박한 위협

사고 처리 - 보안 정책 위반 완화 및 권장되는 방법입니다.

사고 대응 - ‘사고 처리’를 참조하라

표시기 - 문제가 발생했을 가능성이 있거나 현재 발생하고 있을 가능성이 있는 사건

침입 탐지 및 예방 시스템 - 컴퓨터 시스템이나 네트워크에서 발생하는 이벤트를 모니터링하고 이를 분석하여 발생 가능한 사고의 징후를 감지하는 프로세스를 자동화하는 소프트웨어입니다.

악성 코드 - 호스트에 성공적으로 감염시키는 바이러스, 웜, 트로이 목마 및 기타 코드 기반의 악성 개체

전구물질 - 공격자가 사건을 일으킬 준비를 하고 있을 가능성이 있는 신호

프로파일링 - 예상 활동의 특성을 측정하여 변경 사항을 보다 쉽게 식별할 수 있습니다.

서명 - 바이러스의 바이너리 문자열 또는 시스템에 대한 무단 액세스를 얻는데 사용되는 특정 키 입력 등 공격과 관련된 인식이 가능하고 구별되는 패턴

사회공학 - 시스템이나 네트워크를 공격하는데 사용될 수 있는 정보 (예: 암호)를 누군가 속이려는 시도

위협 - 잠재적인 부작용의 원인

취약점 - 악용 또는 남용되는 시스템, 응용 프로그램 및 네트워크의 약점