한국인터넷진흥원 침해사고 분석 절차 안내서

과제A03 NIST800-61과 공통점, 차이점 비교 정리

BoB7기 취약점분석 정성조

챕터 1의 초반부에서 말하는 내용은 두 문서가 비슷하다. 사이버 범죄는 인터넷이 발전할수록 계속해서 증가하고 있다. 이를 위해 KISA와 NIST 문서에서는 침해사고에 대응할 수 있는 방법을 소개한다. 다만 KISA 문서에서는 침해 사고에 대응할 수 있는 구체적인 도구를 집중적으로 소개하고 NIST 문서에서는 침해 사고에 조직적으로 대응할 수 있도록 하는 정책들을 소개한다.

공통적으로 각 직책별 행동 방안을 소개한다.

KISA 문서의 챕터 2에서는 사고대응 방법론부터 보고서 작성까지의 단계별 침해사고 분석 절차를 다룬다. NIST 문서에서는 담당자가 따라야 하는 OMB’s Circular, FISMA, FIPS 등의 지침을 소개하며 법 집행, 사고 보고 조직, 사고 대응 팀 모델 등을 간략하게 설명한다.

챕터3부터 두 문서가 확연히 갈린다. KISA는 침해 분석 도구를 이용하여 윈도우 사고를 분석한다. 반면에 NIST는 사고에 대응하는 방법을 소개한다. 구체적으로 사고를 처리하는데 있어서의 준비 과정부터 탐지, 분석, 회복을 반복한 후 보고서를 제출하는 방법까지 소개한다. KISA는 윈도우 쪽으로는 초기 분석에 있어서의 휘발성 증거 초기 수집법과 루트킷 분석, 해킹 툴 분석을 소개한다. 리눅스 쪽으로도 마찬가지로 초기 휘발성 증거 수집법을 소개하는데 리눅스 파일 시스템의 특징을 이용한 분석 방법을 소개한다. 네트워크 쪽으로는 네트워크 트래픽을 중점적으로 살펴보며 데이터베이스 쪽으로는 mysql에서 사용자가 얻을 수 있는 정보를 제한하는 방법을 소개한다.

챕터4에서는 NIST는 사고 대응 방법론에서 한 층 나아가 조정과 정보 공유 방법을 소개하며 KISA는 주요 해킹 사고를 분석한다. 악성코드를 통한 백도어 및 웹쉘 확인 방법을 소개하며 로그 분석과 제거 방법까지 분석한다. 이 외에도 악성 봇 C&C 서버, ARP spoofing 분석을 통해 대책을 마련한다. NIST는 조직간의 정보 공유를 통해 분석 능력과 대책을 좀더 향상시킬 수 있는 점을 강조한다.