국내 보안관제 제도, 정책의 현황과 필요성

김광혁, 박성익, 이영로
한국전산원 IT인프라구축단
{khkim, parksi, lyr}@nca.or.kr

A Study on Examination and Necessity of the Managed Security Control System and Policy

Kwang-hyuk Kim, Seong-Ick Park, and Yeong-Ro Lee
IT Infrastructure Division, National Computerization Agency

요 약

보안위협의 증가로 사이트를 적기에 취약점을 보완하고 안전하게 유지하기가 어려워지고 있어 전문화된 보안관제의 필요성이 증가하고 있다. 보안시스템의 도입은 설치, 최적화, 운영, 분석 및 후조치 등의 서비스도 개발되어 이용할 수 있다. 한편 이런 시장 현황에 비해 보안관제를 위한 제도는 일부에 지나지 않아 안정적 운영을 저해하거나 법적 위해소지를 안고 있는 부분도 존재한다. 본 논문을 통해서 보안관제 국내/외 현황을 살펴보고 제도화의 한계성을 살펴보기로 한다.

1. 서 론

정보는 다른 중요한 사업을 위한 자산과 같이 조직체에 있어서 중요한 역할을 하는 자산이므로 적절하게 보호되어야 한다. 정보 보안이란, 비즈니스의 연속성을 유지시키고, 비즈니스로부터 발생될 수 있는 손실을 극소화시키며, 투자에 대한 기대 이윤을 극대화시키도록 하고, 많은 비즈니스의 기회를 가질 수 있도록 다양한 위협으로부터 정보를 보호함에 있다. 보안관제는 불법 해킹이나 바이러스로부터 시스템과 네트워크 자원의 손상을 막기 위해 관제가 필요한 모든 시스템을 실시간으로 모니터링하여 즉각 대응할 수 있도록 하는 일련의 활동을 말한다[5]. 여기에는 보안솔루션의 기능을 최적화하고 원격지 보안 툴들의 로그 및 이벤트를 실시간 수집·분석하여 보안대책의 기본자료를 제공하며, 장애발생시 즉각적인 통보, 정해진 룰과 프로세스에 따라 조치를 취하며, 각종 보안 취약점 및 위험에 대한 위험 평가후 업데이트를 취하는 활동이 있다. 보안관제를 통해 얻을 수 있는 이점들은 다음과 같다[6].

·보안시스템의 성능/기능 최적화
·시스템, 네트워크의 실시간 이벤트/로그 수집, 분석, 대응
·유관기관과의 상호협력체계 유지
·보안 취약점 및 위험 분석, 평가
·보안대책의 수립 및 이행
·사전예방활동, 보안컨설팅 및 보안교육 등

한편, IT기술의 발전 및 통신망의 개방성, 상호의존성이 증대될수록 사이버 공격에 대한 위협은 점차 증가하고 있다. 특히 유·무선, 통신·방송이 융합되는 BcN환경에서는 현재 침해사고와는 다른 양상으로 전개될 것으로 예측된다. 즉, 지능화, 자동화되고 파괴력을 가지게 된 웜, 바이러스 및 해킹들이 초고속 통신·방송 융합망을 통하여 전국적으로 유포되고, 지금까지는 공격대상이 아니었던 영역까지 확대될 것으로 예측되어 이에 대비한 대응기술 및 체계의 검증과 발전된 보안관제가 필요하다.

본 논문에서는 국내/외 보안관제를 현황과 문제점을 살펴보고 효과적인 보안관제를 수행할 수 있는 정책, 제도 및 향후 해결해야 할 과제를 제시하도록 한다.

2. 관련 연구

2.1 국내보안관제 동향[7,8]

2.1.1 정부고속망 통합보안관제센터(행자부)

정부고속망 내·외부망 접속점을 경유하는 모든 트래픽을 수집하여 각종 현황 분석, 통계를 통한 전산자원의 효율적인 사용