[9-64]

조기경보시스템 기능 모델 연구

* 신승중 * 최운호 * 황경준 ** 진승할
* 한세대학교 * 한세대학교 * 한세대학교 ** 군포창업보육센터
* expersin@hansei.ac.kr, bzs320@hansei.ac.kr, harri@hanmir.com

A Study on Design & Function of Integrated Computer Emergency Response System for Implement of EWIS (Early Warning Information System)

* Seung-Jung Shin * woon-ho Choi * kyeong-joon Hwang ** sheong-hal Jin
* hansei university * hansei university * hansei university **kbi

요약

본 연구는 컴퓨터 시스템 및 네트웍, 어플리케이션, 인터넷 서비스 등으로 이루어진 전국적 혹은 전사적인 IT 인프라(Information Technology Infrastructure)에서의 자동화된 종합 침해사고 대응시스템 및 그 운영방법에 설계 및 기능연구에 관한 것으로, 보호대상에 위협이 되는 광범위한 침해사고요소(해킹, 바이러스, 웜, 사이버테러, 네트웍스파이, 정보전 등의 침해사고 및 취약성 정보)를 자동으로 수집/분류하고, 해당 조직별로 필요한 방식으로 정보를 가공/분석하여 이용할 수 있으며, 축적된 정보보호관련 정보의 안전한 공유시스템 및 네트웍 제공, 각 침해사고에 대한 공격평가와 조기 경보가 가능하며, 새로운 침해사고에 대한 테스트(시뮬레이션)를 수행하고, 조기경보시스템(EWIS(Early Warning Information System)의 설계와 기능에 대한 개념을 제시한다.

Ⅰ. 서론

인터넷 대란으로 네트워크 보안의 중요성이 부각됨에 따라 네트워크 감시시스템(NSS) 구축에 초점을 맞춰지고 있다. 해킹,웜(Worm) 바이러스를 차단할 수 있는 유해 차단시스템 도입을 확대하고 침입탐지시스템(IDS)보다 상위 개념인 NSS 를 설치해 인터넷 대란에서 문제가 된 네트워크의 이상징후와 침입탐지,IP 이상징후 등을 사전에 파악하는 것이다. 또 위험분석을 통한 조기경보시스템(TMS)을 구축,회원사들을 상대로 보안의 취약성을 신속히 알리는 방향으로 진행되고 있다. 이에 조기경보시스템들의 기능 모델을 연구하고자 한다.

Ⅱ. 본론

최근에는 이벤트를 구별하여 진짜 위험한 공격을 구별해내서, 위협 요소를 제거하는 연구가 시작되고 있지만 현실적으로 애로사항을 겪고 있으며, 실제 상황에서는 별다른 도움을 못 받고 있는 실정이다. 즉, 위험도가 높은 공격이 발생한 경우 이를 경보 또는