ESM 시스템을 이용한 안정된 학내망 구축

이대식* · 윤동식* · 안희학**

요 약

오늘날의 네트워크는 여러 위협적인 공격에 취약한 상태에 있다. 특히 인터넷 서비스나 전자상거래와 같은 서비스를 제공하는 기업은 위험에 노출이 되어 있고 공격자의 타겟이 된다. 그리하여 기업들은 각종 보안솔루션을 사용하는 것이 현실적이다. 이것은 우리가 이용하고 있는 학내망에서도 예외일 수는 없음으로 학내망에도 FireWall, IDS, VirusWall, VPN 등 여러가지 보안 솔루션들이 존재한다. 관리자들은 이 여러 가지의 보안솔루션들을 관리해야 하는데 그러기에는 효율성이 떨어져 모든 솔루션을 관제 및 통제 할 수 있는 어떠한 관리 시스템이 필요하게 되었다. 본 논문에서 ESM이 관리하는 보안솔루션에 대한 기본적인 내용과 ESM을 사용했을 때의 장단점을 다룬다. 또한 그렇게 구현된 학내망에 ESM을 이용하여 관리자가 학내망을 더욱 효율적이고 체계적으로 관리할 수 있는 방안을 제시한다.

A School Network Construction using the ESM System

Dae Sik Lee* · Dong Sic Yun* · Heui-Hak Ahn**

ABSTRACT

Today, network is a fragile state in many threat attacks. Especially, the company serviced like internet or e-commerce is exposed to danger and targeted of attacker. Therefore, it is realistic that the company use the security solution. It exist various security solution in our school network. For example, FireWall, IDS, VirusWall, VPN, etc. The administrator must manage various security solution. But it is inefficient. Therefore, we need the Management System to controll every security solution. In this paper, we deal with basic contents of security solution to manage the ESM and merits and demerits when use it. Also we suggest method that the Administrator can manage his network more efficiently and systematically by using the ESM in our school network.

Key words : ESM(Enterprise Security Management), School Network

* 안동과학대학 사이버테러대응학과

** 관동대학교 컴퓨터학부

1. 서 론

현대 사회는 정보화와 정보공유 마인드로 인해 네트워크 및 인터넷 사용자가 증가하고 있다.

각종 해킹 및 크래킹, 바이러스웜등의 네트워크 피해들도 따라서 증가하고 있으며 이에 대한 피해는 점점 늘어가고 있는 추세이다. 이에 따라 네트워크 보안이 중점적 이슈가 되고 있으며 보안장비도 다양해지고 있다.

이런 보안장비는 네트워크를 서비스 하는 기업의 필수가 되어 가고 있으며 해당 기업의 취약한 부분을 보안하기 위해 설치해야 하는 보안장비의 종류는 많으나 모두 관리하기에는 효율성이 떨어졌다.

이러한 여러 보안장비를 하나로 묶어서 좀더 효율적이고 체계적으로 보안체제를 형성하고자 하는 의도로 구현된 것이 전사적 보안 관리 시스템(ESM : Enterprise Security Management)이다.

최근 공공기관이나 개인의 서버 또는 PC를 대상으로한 공격도 빈번히 일어나고 있으며, 이것은 학내망이라 해서 예외는 아니다.

국내의 학내망은 해커들은 놀이터나 또 다른 해킹의 경유지로 이용되고 있어 보안에 취약하다고 볼 수 있다. 또한 학내망의 경우 웜의 공격을 받았을 경우에 망전체가 마비됨으로 막대한 손실을 입을 수 있다.

본 논문에서는 큰 피해손실이 우려되는 학내망을 효율적이고 체계적인 보안 서비스를 제공하는 전사적 보안 관리 시스템(ESM : Enterprise Security Management)으로 구현해 보았다.

2. 관련 연구

본 논문에서는 안정된 학내망 구축을 위해 사용되는 관련 보안장비에 대해 간략히 살펴보기로 한다.

첫째 전사적 보안 관리 시스템(ESM : Enterprise Security Management)이란 IDS, FireWall, VirusWall 등 각종 네트워크 보안제품의 통합관리와 개별 침입에 대한 종합적인 대응을 위해 각 요소제품간에 인터페이스 및 교환되는 메시지포맷을 표준화하여 모니터링과 원격지 중앙관리 까지 가능한 지능형 보안 관리 시스템을 말한다.

사실 ESM은 오래전부터 사용되던 개념으로 보안관리라기 보다는 시스템 관리영역에서 출발했다. 이러한 시스템 관리영역을 보안이라는 전문적인 관리 도구로 특화한 것이 지금의 ESM이다.

모든 보안제품의 특징이 그러하듯 ESM 또한 보안을 위한 보조도구이며 모든 것을 자동으로 막아주는 마법사가 아니라는 올바른 인식을 갖는 것이 중점이라 할 수 있다.

따라서 도구와 사람이 해야 할 역활을 적절히 분배함으로써 결국은 전문인력이 시행해야 할 업무의 보조도구로써의 의미이다.

ESM은 IT기반 구조 환경 관점에서 보았을 때 두가지 영역으로 설명될 수 있다.

먼저 사용자 운영관리(User Administration & Management)방안으로 보안 또는 정책관리에 따른 사용자 및 접근관리에 비중을 두고 있는 범주이다.

Single-Sign-On의 기능을 대부분 포함하고 있으며 초기 유형의 ESM의 개념이 많이 반영되 있는 ESM으로 보안적인 측면보다는 시스템 관리의 성격이 강하다.

다음으로 위험평가(Risk Assessment)를 들 수 있다. 네트워크 및 시스템의 취약점이나 위험요소들을 분석하고 모니터링하는 관리도구의 형태를 취한다.

최근에 출시된 ESM제품들은 대부분 이영역이 주류를 이루고 있으며 기존 보안 제품들과의 통합이 활발히 진행되고 있다.

따라서 최근 ESM 추세로 보면 네트워크나

시스템 리소스들의 각종 위험 요소들을 분석하고 감시하는 FireWall, VirusWall, IDS 등의 여러가지 보안솔루션들을 통합 관리함으로서 관리의 효율성을 높으로 능동적인 보안대책을 세울 수 있도록 도와준다.

보안시스템의 통합적인 관리의 필요성대두, 이기종 보안시스템에서 발생되는 로그통합 관리를 목적, 중앙관리 및 대응이 필요하다.

둘째, IDS(Intrusion Detection System)는 침입 탐지 시스템으로 컴퓨터/네트워크에서 발생하는 일들을 모니터링(Monitoring)하고, 침입 발생 여부를 탐지(Detection)하고, 대응(Response)하는 자동화된 시스템을 말한다.

IDS의 자동 탐지 방식에는 비정상행위 탐지와 오용 탐지 방식이 있다. 비정상행위 탐지 방식 IDS의 장점은 새로운 침입의 유형에 대한 탐지 가능하지만 정상 행위를 모델링(예측) 하기 어렵고 방대한 사용자/네트워크 활동(training data) 필요하다 이러한 데이터로 탐지하는 것이 실제로 많은 시간이 요구되거나, 심지어 불가능한 것이 단점이다.

오용 탐지 방식 IDS의 장점은 상대적으로 낮은 오판 율과 침입에 사용된 특정한 도구/기술에 대한 분석 가능하고 이러한 사고에 신속하고 정확하게 대응하지만 새로운 침입 유형에 대한 탐지 불가능하고 이에 따른 DATA의 지속적인 업데이트가 필수적이다. 침입의 유형이 정해져 있으므로 언제나 우회가능성을 품고 있는 것이 단점이다.

IDS의 대응행동은 관리자에게는 침입 정보만 제공하는 수동적 대응과 실제 대응행동을 IDS가 자동적으로 수행하는 능동적 대응행동으로 분류할 수 있다.

IDS는 조직 전체의 보안 확립에 크게 기여하지만 완벽한 보안 솔루션은 아니다. 다단계 보안(*Defense in Depth*)시스템을 구축함으로서 높은 수준의 기술적 역량을 지닌 관리자의 지속적인 운영 및 관리 요구된다.

셋째, FireWall(방화벽)의 원래 의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는 것이다. 이 의미를 인터넷에 적용한다면, 이는 네트워크의 보안 사고나 위협이 더 이상 확대되지 않도록 막고 격리하는 것이라고 할 수 있다. 이는 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 적극적인 방어 대책이라고 할 수 있다.

방화벽 시스템의 기본 목표는 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공하는 것이다. 방화벽이 구축되지 않은 네트워크는 외부와의 투명한 접근을 허용하므로 서 내부망 전체가 위험 지대가 될 수 있지만 방화벽 시스템을 구축하면 불법적인 트래픽을 거부하거나 막을 수 있는 것이다. 물론 투명성을 보장하지는 않지만 내부 네트워크를 안전지대로 만들 수 있다.

넷째, VirusWall은 게이트웨이상에서 프로토콜을 실시간으로 감시, 치료하여 프로토콜의 시스템에 피해를 줄 수 있는 바이러스 및 악성코드를 차단하고 방역해 주는 보안솔루션을 말한다.

SMTP, HTTP, POP3, FTP 등 다양한 프로토콜을 지원한다. 설치시 네트워크의 환경변화가 전혀 없고 대용량 네트워크 트래픽 처리를 한다. Kault Tolerance, load balancing 기능의 고가용성 제공하고 Antivrus Vendors의 선택을 지원한다. URL/Category/IP를 이용한 다양한 Content Filtering 기능이 있다.Transparent Bridge 방식으로 투명성 제공하고, Smartfilter의 Contents Filtering 기능이 있고, Spam mail의 Anti-Spam 필터링 기능이 있다. Hardware and Software의 일체형 장비와 다양한 Reporting 및 Alerts 기능이 있다.

VirusWall을 사용하면 네트워크 레이어에서 취약점 분석/격리와 네트워크 접속시 보안패치

및 백신이 적용되지 않은 시스템에 대한 네트워크 접속을 손쉽게 차단, 이같은 문제점을 완화할 수 있다.

마지막으로 NMS(Network Management System)는 네트워크상의 전 장비들의 중앙 감시 체제를 구축하여 감시(Monitoring), 계획(Planning) 및 분석(Analysis)이 가능하여야 하며 관련 데이터를 보관하여 필요시 바로 활용 가능하게 하는 관리 시스템이다. 다시 말하면, NMS는 네트워크 관리자가 NMS제품을 사용하여 현재 운영되는 workstation으로부터 네트워크를 제어(control) 감시(monitor)할 수 있게 한다. NMS(network Management System)는 전반에 걸친 정보를 수집 관리하는데 그 목적이 있다. 현재 많은 NMS 상품들은 기본적으로 네트워크상의 전 장비들의 중앙 감시 체제를 구축하여 Monitoring, Planning 및 분석이 가능하여야 하며 관련 데이터를 보관하여 필요 즉시 활용 가능하여야 하는 것과 SNMP Protocol을 관리Protocol로 사용하며 CMIP으로의 전환 방안이 제시, Ethernet 및 FDDI네트워크에 접속되어있는 자원들의 관리, Graphic User Interface를 지향해야 하며 보안성이 우수하고 관리가 용이해야 하는 공통점을 갖는다. 통상 NMS는 Workstation급에 Network관리자가 사용하기에 편한 곳에 설치하며 단위 Network에 복수 개의 NMS를 병행할 수도 있다. NMS구동은 SNPM에 의해 작동하며 SNMP(Single Network Management Protocol) System은 NMS, NMS Agent, MIB(Management Information Base) 3부분으로 이루어진다.

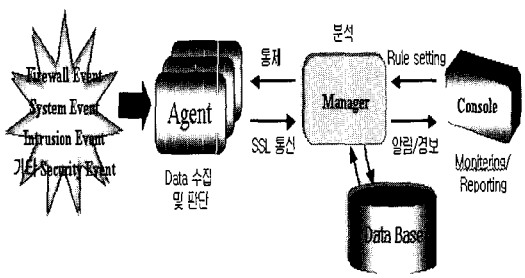
NMS는 SNMP Agent에 정보를 의뢰함으로써 Device들을 감시 제어한다. SNMP Agent는 NMS의 요구에 응답하고 Network상의 관리 대상 장비에 존재하는 S/W이다. Agent에는 장비에 관한 정보인 MIB(Routing Table Counter, status indication 등)이 있으며 이들은 Agent에 대한 NMS의 Poll과 Query에 대한 응답으로 NMS에 보내지고 이들은 다시 DB에 저장된다.

3. ESM으로 구축한 학내망 설계 및 구축

본 장에서는 앞에서 살펴본 보안솔루션들과 기술들을 바탕으로 구현된 학내망을 ESM을 이용하여 좀더 통합적인 보안체계로 구현해 본다. 효율적이고 체계적인 보안서비스를 통합관리하기 위한 ESM시스템을 도입, 각 요소에 대한 설명과 그렇게 구성된 학내망의 장단점을 소개, 이후 최종적으로 시스템을 구현해 안정된 학내망을 보여준다.

3.1 ESM의 구성

ESM의 일반적인 구조는 (그림 1)과 같이 구성되어 있다.



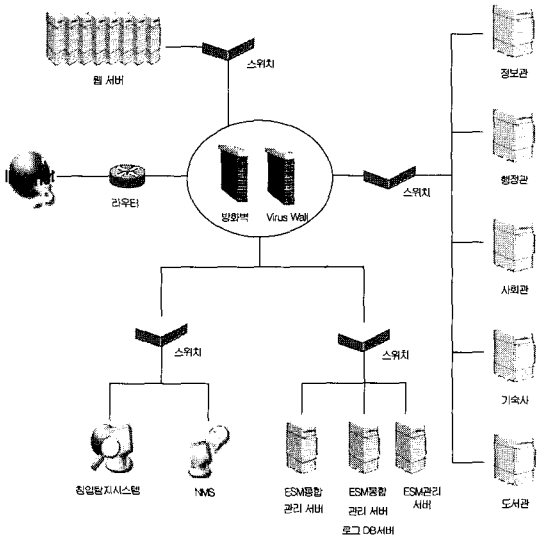
(그림 1) ESM의 구성도

Agent는 보안 장치에 탑재되서 운영되며 미리 정의된 규칙에 의해 각 event와 security policy를 적용합니다. 그리고 수집된 data를 manager server로 전달하고 통제 받습니다.

Manager는 정해진 규칙에 의해 data를 분석하고 저장하며, 각종 정책에 대한 저장, 분석, report 기능을 수행합니다.

Console은 분석 전달되는 자료, data에 대한 시각

적 정보 전달 및 상황 판단(인식) 기능과 manager server에 규칙을 설정하도록 지휘하고 통제는 업무를 맡습니다.



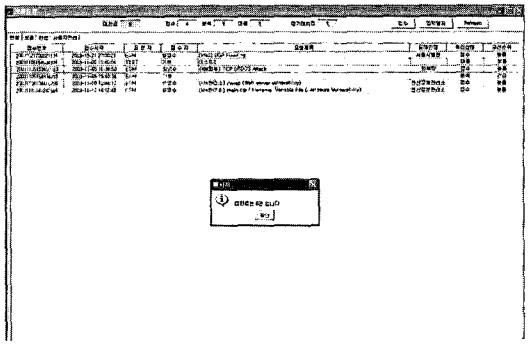
(그림 2) ESM으로 구축한 학내망의 구조

3.2 ESM의 기능

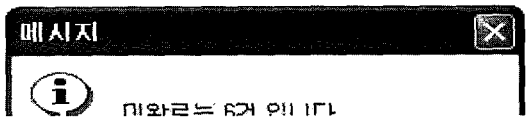
등록된 장비에 대한 Alive체크 및 그래픽적인 관리기능인 맵 관리 기능과 보안이벤트, 트래픽, 시스템 자원 등을 모니터링하는 기능이 있다.

저장된 이벤트의 검색 및 추이 분석을 하는 로그검색 기능과 로깅, 액션 등 사용자 및 시스템 이력 등을 관리하는 기능, 그리고 보안이벤트와 트래픽정보, 시스템 자원 정보의 상관분석 기능이 있다. 관리대상 H/W, S/W에 대한 자산정보관리 및 계약관리등을 하는 자산관리기능과 보안이벤트, 관제업무 전체에 대한 통계 및 보고서 작성 기능이 있다.

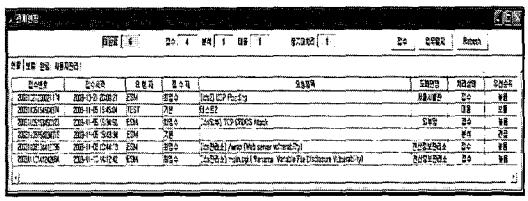
ESM을 구축함으로써 얻을 수 있는 보안효과는 보안관리 정책 및 절차가 정립이 되고 예방적 보안관리 체계가 수립된다. 그리고 효율적인 보안관리를 통한 위험감소 체계가 정립이 된다.



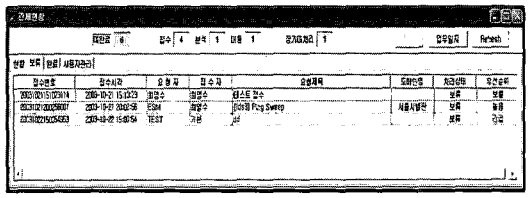
(그림 3) 관제현황 초기화면



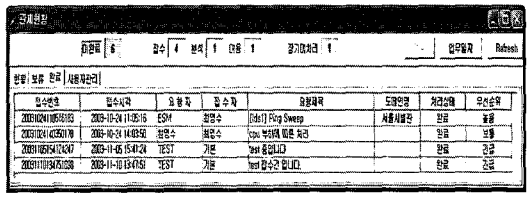
(그림 4) 미완료된 이벤트 알림 메시지



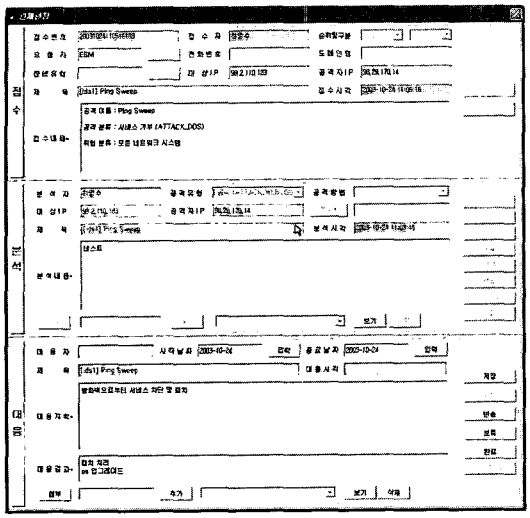
(그림 5) 이벤트 접수현황 화면



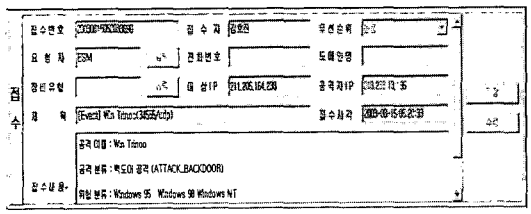
(그림 6) 처리 보류된 이벤트 현황 화면



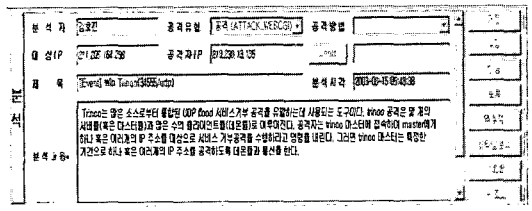
(그림 7) 처리 완료된 이벤트 현황 화면



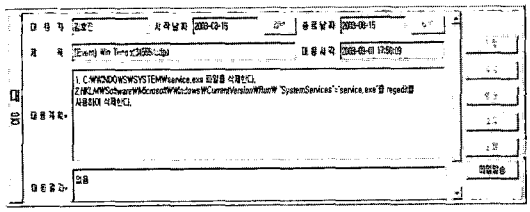
(그림 8) 이벤트 상세 정보



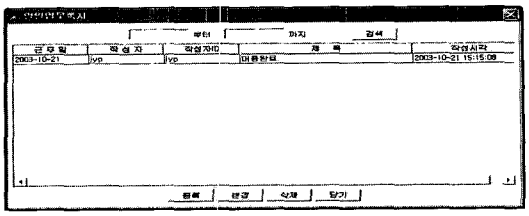
(그림 9) 접수 프로세스 처리화면



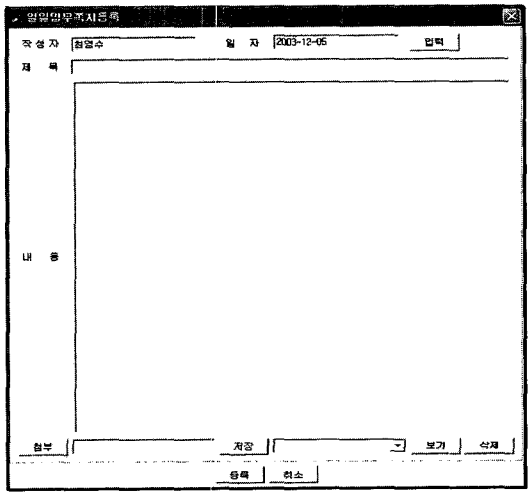
(그림 10) 분석 프로세스 처리화면



(그림 11) 대응 프로세스 처리화면



(그림 12) 업무쪽지목록 화면



(그림 13) 일일업무쪽지 작성 화면

4. 결 론

오늘날 여러 위협적인 공격에 취약한 기업이나 학내망을 여러 가지 보안 솔루션들을 이용해 보안하는데, ESM은 기존의 보안 솔루션들을 더 다루기 편하게 통합 관제해서 보다 효율적으로 관리하게 해준다.

ESM 보안을 통해 학내망이 안정적으로 관리되어 질 수 있고, 맵관리, 모니터링, 로그검색, 개체·이력관리, 상관분석, 자산관리, 통계 및 보고서 등과 같은 다양한 기능들을 통해 보안정책 및 절차가 정립되고 예방적인 보안관리 체계가 수립되었다. 그리고 효율적인 보안 관리를 통한 위험감소 체계가 정립된다.

참 고 문 헌

[1] John Bommers, "Practical Planning for Network Growth", Prentice Hall PTR, 1996.

[2] J. Case, M. Fedor, M. Schoffistall, and C. Davin, "The Simple Network Management Protocol(SNMP)", RFC 1157, May 1990.

[3] Leinwand, Allan, and Fang, Karen, "Network Management:A Practical Perspective", Addison-Wesley, 1993.

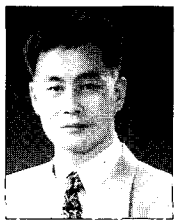
[4] Stephan Northcut, Judy Novak, Donald mcLachlan, "Network Intrusion Detection An Analyst's Handbook", Second Ed, New Riders September, 2000.

[5] 박종혁, "효율적인 보안 서비스를 위한 ESM 시트템의 구현"(고려대:석사논문, 2003).

[6] Clarkin Michael, "Comparison of Cyberwall -PLUS Intrusion Prevention and Current IDS Technology, Network-1 Security Solution", Waltham, MA 2001.

[7] William R. Cheswick and Steven M. Bellovin, "Firewalls and Internet Security" Addison Wesley, Reading, Massachusetts, 1994.

[8] Cisco Systems, Inc. "Cisco Secure Scanner Overview", Cisco Secure Scanner User Gui-de Version 2.0.29 June 2000.



이 대 식

1995년 관동대학교 전자계산공학과(공학사)

1999년 관동대학교 전자계산공학과(공학석사)

2004년 관동대학교 전자계산공학과(공학박사)

2003년~현재 안동과학대학 사이버테러대응학과 교수

윤 동 식

1992년 관동대학교 전자계산학과(공학사)

1994년 관동대학교 컴퓨터공학과(공학석사)

2000년 관동대학교 컴퓨터공학부(공학박사)

1999년~현재 안동과학대학 사이버테러대응학과 교수

안 희 학

1981년 숭실대학교 전자계산학과(공학사)

1983년 숭실대학교 전자계산학과(공학석사)

1994년 숭실대학교 전자계산학과(공학박사)

1984년~현재 관동대학교 컴퓨터학부 교수