심층방어 전략을 통한 통합보안관제 고도화 방안 연구

윤대원*, 류재철*
*충남대학교 컴퓨터공학과
e-mail:daewonyo@hanmail.net, jcryou@home.cnu.ac.kr

A Study on upgrading ESM Plan in a Defence In Depth Strategy

Dae-Won Yoon*, Jae-cheol Ryou*
*Dept of Computer Engineering, Chungnam National University

요 약

현재 개인정보보호법 및 정보보안에 대한 중요한 이슈가 되고 있다. 데이터 유출사고의 약76%가 외부조직에서 발견되었고, 피해조직의 내부에서 발견된 비율 중 절반 이상이 최종 사용자에 의해 발견되었다. 관제대상과 범위가 주로 네트워크 영역으로 한정되어 있고 외부로부터 유입되는 공격에 대한 모니터링에 집중하는 보안관제 체계가 사고의 원인으로 파악되었다. 즉 내부 PC를 대상으로 하는 공격이나, 패턴기반의 탐지를 우회하는 알려지지 않은 취약점을 이용한 APT공격, 사회공학적 공격 등에는 한계를 보이는 경우이다. 향후 사물인터넷(IoT)의 증가로 인하여 더 많은 취약점 공격과 대량의 비정형 데이터가 증가할 경우 내외부적인 공격에 보안 체계가 더 체계적이고 계층적 방어 보안 모델로 대응해야 한다.

1. 서론

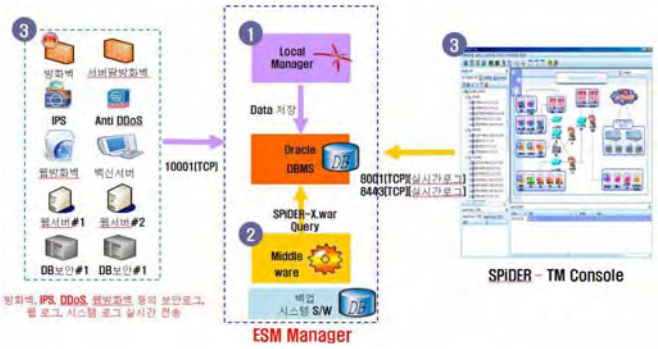
최근 전 세계와 우리나라를 뜨겁게 달궜던 소니픽처스 해킹과 한국 수력 원자력 해킹사태, 이러한 대형 해킹사건이 연이어 발생하면서 국내외 주요기관 및 기업의 다양한 보안 취약점이 드러나고, 이에 따른 보안 강화의 필요성이 대두되고 있다. 한국수력원자력 해킹 원인에는 국내외 전문가들과 정보 당국은 미국의 소니픽처스와 한국수력원자력 해킹 원인에 대해서는 북한 소행 가능성이 높은 것으로 보고 있다. 오랜 기간에 걸친 해킹으로 유출된 내부 자료가 한국수력원자력을 조롱하는 글과 함께 다섯 개 파일을 인터넷에 공개했다. 따라서 이러한 해킹 관련 사이버범죄로부터 핵심 자원을 보호하기 위해서는 지능적이고 다체계적인 심층방어(Defence in Depth)에 대한 관심이 절대적으로 필요하다고 할 수 있다.

2. 보안관제 개념 및 현황

단위 보안 시스템(방화벽, 침입 탐지/방지 시스템, Anti-DDoS, 웹방화벽 등)으로 부터 수집한 이벤트 로그를 관리, 분석, 대응하는 시스템을 보안관제시스템(ESM, Enterprise Security Management)은 이라고 정의한다. 기업 내부의 보안정책을 통합관리하기 위한 솔루션으로 기업의 경쟁력 확보와 영속성을 목적으로 주요 인프라에 대한 위협 요인을 사전에 분석 및 예방하고 위협 요인 발생 시 적절히 대응하는 절차를 수행한다. 최근의 지능화되고 다양한 취약점 공격과 사회공학적인 보안 위협은 정보보호 솔루션을 네트워크 경계에 배치하거나 내부 자산에 엔드포인트(end-point) 솔루션을 배치하여 대응하는 단층적인 방안으로는 실효성을 거두기가 어렵다. 결국 효과적인 정보보호 솔루션의 조합, 중요시스템과 데이터에 대한 접근차단 등과 같은 기술적인 보안과 더블어 정기적인 보안인식 교육, 시스템 사용에 대한 명문화된 보안 지침 등과 같은 정책적인 보안이 상호 보완해주는 계층구조로 정보보호 프로세스가 확립되어야 한다.

<표 1> 보안관제 프로세스

정보수집 →	공격분석 →	침해대응
·보안이벤트 수집 ·방화벽 정책로그 ·IDS/IPS 공격 탐지 로그 ·Anti-Virus정보	·보안이벤트 분석 (공격 탐지/추이) ·로그 추적 분석 ·흐름 분석/시각화 ·공격현황 분석	·공격탐지/대응 ·보안정책적용 ·상관분석보고서 ·침해공동대응



(그림 1) 일반적인 보안관제 구조
(출처- http://www.igloosec.co.kr/)

현재 통합보안관제 ESM(Enterprise Security Management), 위협관리기반의 TMS(Theat Management System), 자산의 Risk적 보안에 중점을 두는 RMS(Risk Management System) 등이 통합된 차세대 보안관리 솔루션으로 앞다퉈 출시하고 있다. 이글루시큐리티는 차세대 컨버전스형 정보보호 관리 모델로 통합보안관리솔루션(ESM), 위험관리시스템(RMS), 복합형 종합 다차원 분석 시스템, 침해대응시스템 , 방화벽 정책관리 솔루션을 통합한 제품을 개발해 출시하였다.

제이컴정보도 ISMS(정보 보안 관리 시스템)기반의 정보보호관리체계 솔루션인을 개발 완료했다. ATMS은 ESM의 취약점을 보완할 수 있는 차세대 보안관리제품으로 예/경보, 위협관리, 취약성 점검 등 관리체계적인 통합 보안서비스를 제공하는 솔루션이다. SK인포섹도 ESM, IDS, TMS 등을 통합해 주는 시스템통합솔루션 투심(ToSIM)을 자체 개발해 출시하였다. 차세대 통합보안관리 제품을 통해 그동안 실시해 왔던 단편적이고 기술적인 보안 관리가 아닌, 더욱 진화된 정보기술 통합보안관리 체계를 갖추게 되며, 취약점 공격에 대한 상시적인 진단과 파악이 가능해져 지속적인 위험(Risk)관리를 할 수 있게 될 것으로 전망된다.

(그림 2) 차세대 보안관제 구조
(출처- http://www.igloosec.co.kr/)

<표 2>차세대 통합보안관리 제품 현황

회사명	특징	제품명
이글루시큐리티	차세대 컨버전스형 정보보호 관리 모델로 통합보안관리와 위험관리, 다차원분석, 침해대응시스템 등을 통합	eXTRiM
제이컴정보	ISMS(정보 보안 관리 시스템)기반의 정보보호관리체계	ATMS
SK인포섹	ESM, IDS, TMS 등을 통합해 주는 SI솔루션	투심(ToSIM)

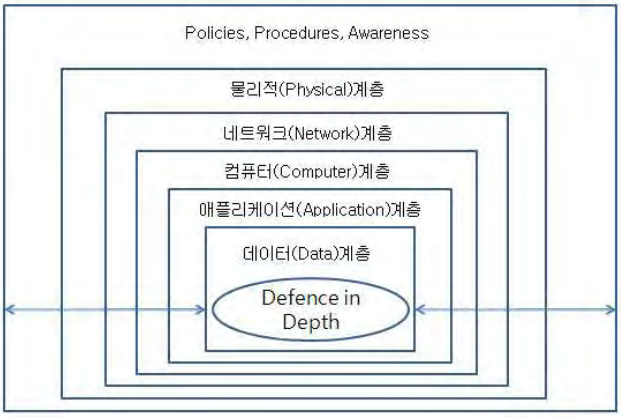
3. 계층방어 보안모델

심층방어(Defence in Depth)는 미국 국가보안국에서 2002년 9월 가이드라인을 제작하여 배포하면서 소개되었다. 배포된 가이드라인에 따르면 공격자의 공격 유형은 수동적 공격, 능동적 공격, 내부 공격, 근접 공격, 배포 공격의 5가지로 구분 할 수 있으며 5가지 공격 유형에 따른 계층 방어는 [표 3]와 같다.

<표 3>계층 방어 예시

구분	공격형태	1단계방어	2단계방어
수동공격	네트워크 Sniffing (불법도청) 공격	네트워크 암호화	응용프로그램 보안
능동공격	인증정보Spoofing 공격,DoS공격,악성코드 삽입 공격	경계선(Perimeter) 보안	서버 및 PC 환경방어
내부공격	수정, 파괴, 비인가 정보 접근 공격	물리적, 인적 보안	접근통제, 감사
근접공격	물리적으로 근접한 곳에서 공격	물리적, 인적보안	기술적 감시
배포공격	악성코드가 탑재된 소프트웨어 배포	신뢰된 소프트웨어 배포	무결성 검증

성공적인 심층방어(Defence in Depth)을 구현하기 위해서는 3가지 주요 방어 요소인 사람(People)과 기술(Technology), 운영(Operation)이 있어야 한다. 과거에서 현재까지 심층방어(Defence in Depth)는 중요한 보안정책 중에서 설계에 해당하는 보안 아키텍처의 기본 구조로 자리 잡게 되었으며 [그림 2]와 같은 형태의 심층방어(Defence in Depth)체계를 구축하는 것이 일반화 되어 있다.



(그림 3) 일반적인 계층방어

물리적계층, 네트워크계층, 컴퓨터계층, 애플리케이션계층, 데이타계층 5가지 방어 체계는 보안정책, 인식개선, 보안절차가 기반이 되어야 비로소 심층방어의 모델로 완성된다. 5가지 방어 체계는 다음과 같이 각각의 계층에 필요한 보안 솔루션을 설치하거나 보안 기술을 이용하여 구현할 수 있다.

물리적 계층방어는 신뢰되지 않은 외부 네트워크와 내부네트워크의 경계로 경비나 출입문과 같은 물리적인 보안은 특정구역의 출입관리, 제어실에 대한 무단 접근을 차단한다.

네트워크 방어는 내부 네트워크를 보호하기 위해 라우터, 방화벽, 네트워크 침입탐지/차단시스템, 서버, 원격접근서버, 무선랜 보안, IPSec, 네트워크 세그먼트 기술을 사용하여 보안성, 가용성, 확장성, 관리성, 신뢰성 등의 서비스를 제공한다.

컴퓨터계층방어는 개인기반방화벽, 서버보안, 패치관리시스템(PMS), 안티바이러스(Anti-Virus) 감사 로그 등의 보안 솔루션을 설치하여 클라이언트 및 서버를 방어한다.

응용프로그램계층방어는 웹/앱서버, 데이타베이스서버, 이메일서버 등을 보호하기 위해 웹방화벽, 데이타베이스보안, 메일서버 보안 등의 솔루션을 설치하거나, 소프트웨어 개발 보안 등을 통해 중요자료에 접근 가능한 응용프로그램을 방어한다. 데이터방어는 암호화, 백업, 접근통제, 무결성 검증 등을 통해 시스템에 저장되어 있는 중요 자료를 방어한다.

심층 방어 체계가 기술적, 시스템적으로 완벽히 구축되었더라도 운영 중에 발생할 수 있는 시스템 오류, 관리자의 실수로 발생하는 에러들이 예측할 수 없는 곳에서 발생할 수 있다. 따라서 모든 상황 정보를 수집하고 정기적으로 분석하는 추가적인 절차가 필요하며 이를 보안관제 시스템과 연동해야 한다. 즉 시스템 현황을 한눈에 파악할 수 있어야 하며 접근통제 정책, 사용자 인증정책, 물리적 보안 등이 5가지 방어 체계에서 생산하는 다양한 로그와 함께 연동되어야 계층 방어 체계가 성공할 수 있다.

4. 계층방어 기반의 통합 보안관제 구축

효과적인 심층방어 통합보안관제를 위해서는 정보보안 거버넌스(Governace), 위험관리(Risk management), 컴플라이언스(Compliance) 등 통합적으로 지원 기능을 구축하여 유기적인 방어체계로 구축되어야 한다.

정보보안 거버넌스(Governace)에서 보안 최고 책임자는 법적 활동, 모니터링에 대한 책임, 보안관리를 위한 책임과 보안 요구사항에 대한 보증, 보안 정책을 승인하고 전략적 보안 목적을 정의한다. 가장 큰 특징으로 대내외 정보를 묶어서 보여주는 종합 대쉬보드 성격의 의사결정 포탈을 제공한다는 점을 꼽을 수 있다. 기존에는 ESM이나 TMS 기반 관제가 독립적으로 이뤄져왔으나 보안 포탈을 통해 이제 실무자들의 통합 관제가 가능해짐은 물론, 보안 최고 책임자가 쉽게 의사 결정을 내릴 수 있게 된다.

위험관리는 정보자원에 대한 취약성과 위험을 식별하고 위험을 수용 가능한 수준으로 감소시키기 위한 대응 방안을 목적으로 두고 있다. 정보자산 식별과 가치 산정, 위험분석(Risk Analysis), 통제 및 대응책 수립 등의 위험관리 프로그세스를 기반으로 해야한다. 시그니처, 룰기반 탐지 기법의 보안관제는 방화벽, IPS, IDS 등 단위 보안제품에 종속되어 있어서 정확도는 높으나 새로운 공격들에 대한 대응능력은 미흡하다. 위협관리시스템(TMS)의 경우 유해 트래픽 및 정상 트래픽 중심으로 공격을 탐지하며 보안관제와는 보완적으로 이용되고 있다. 위험관리(RMS)는 침해대응을 위한 핵심 단위 보안제품으로써 정보시스템에 대한 영향도와 중요도를 평가하고 정보시스템의 취약점을 찾아내 만든 위험도 매트릭스(평가지표)를 기반으로 위험관리가 가능해야 한다.

컴플라이언스(Compliance 규제준수)는 각종 법, 제도적 규제 및 권고의 철저한 대응을 위해 정보기술인프라로 구현하는 것을 말한다. 정보유출 사고를 효과적으로 막기 위해서는 컴플라이언스를 찾고 준수해야한다. 기술적인 관점에서 시스템상의 정보기술환경, 디자인, 정보의 물리적인 위치 등이 복잡하고 서로 유기적으로 연결되어 있다. 개인정보보호를 위한 Privacy, 중요한 자산보호 정책 Security, Governace를 연계하게 되면, 보안관제 자료를 토대로 분석한 후 침해사고 대응을 신속히 할 수 있다. 또 중요도 높은 시스템의 취약점을 발견하여 미리 공격에 대비하기 하기 위한 방법으로 잠재적 취약점을 찾아내는 자동화된 취약점 분석 기능과 보안침해에 대한 사후 분석을 가능케 하는 포렌식 기능은 효과적인 내부 통제를 지원한다.

(그림 4) 통합 보안관제 개념

5. 결론

최근 발생한 각종 해킹 및 정보유출 사건들로 정보 관리에 대한 관심이 고조된 상황에서 다양한 공격에 대응하기 위한 보안 관제 모델로 계층방어(Defence in Depth) 기반의 거버넌스와 위험관리, 컴플라이언스 기능을 포함한 통합보안관제체계를 제시하고 있다. 끝으로 강조하고 싶은 점은 통합보안관제를 효과적으로 구축하기 위한 정보보호 정책의 수립과 조직간의 협력, 정보보호 담당 직원들의 역량강화, 전 직원의 보안의식 고취 등이 동시에 만족 되어야 진화하는 보안 위협으로부터 기업의 중요자산을 안전하게 지켜낼 수 있다는 점이다.

참고문헌

[1] 빅데이터 분석으로 살펴본 IDS와 보안관제의 완성, 강명훈, 와우북스

[2] 보안관제 효율성 제고를 위한 실증적 분석 기반 보안 이벤트 자동검증 방법, 김규일, 박학수,최지연, 고상준, 송중석, http://dx.doi.org/10.13089/JKIECS.2014.24.3.507

[3] 보안관제 기술동향 조사 및 차세대 보안관제 프레임워크 연구, 신휴근,김기철, 정보보호학회지제23권 제6호, 2013.12

[4] 정보자산 침해방지를 위한 NAC 구축사례 연구, 송영민,홍순구,김현종, Journal of the Korea Industiral Information System Research Vol. 19 No.6, Dec. 2014

[5] 클라우드 환경에서의 통합 보안관제 모델 연구, 변연상, 곽진, The Journal of Digital Policy & Management 2013 Dec

[6] 국내 보안관제 체계의 현황 및 분석, 박시장, 박종훈, http://dx.doi.org/10.13067/JKIECS.2014.9.2.261

[7] 통합보안관제환경을 위한 아키텍처 및 활용연구 방안에 대한 연구, 황동욱, 이상훈, http://dx.doi.org/10.13089/JKIECS.2014.24.2.353