실시간보안관리 프레임워크

김병학, 임채호
시큐리티맵(주)
{bhkim, chlim}@securitymap.co.kr

Framework of Real Time Security Management

Byunghak Kim, Chaeho Lim
SecurityMaP Co., Ltd

요약

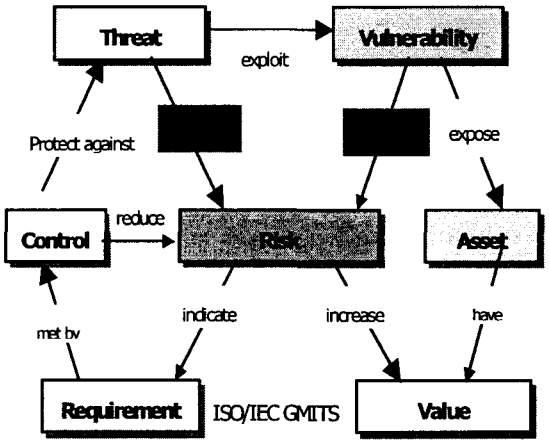
올해 발생한 슬래머웜 등 인터넷웜은 감염스피드와 피해영향으로 인하여, 정보보호의 전략을 급격하게 수정하게 만들었다. 가장 큰 문제는 기존의 정보보호제품이 신종 취약점과 공격에는 무용지물임이 증명되었고, 결국 Practice에 근거한 관리 및 프로세스에 의한 보안이 중요함을 보이고 있다. 또한 그동안 보안관리는 온라인화 되지 않은 자산에 근거한 모델이 많았지만 현재는 온라인화 된 자산에 대한 실시간보안관리 방법이 매우 중요해지고 있다. 실시간 취약점관리, 실시간위협관리, 실시간위험관리 등을 통하여, 실시간보안관리의 해외동향과 이론적 근거에 바탕을 둔 프레임워크 설계를 보이고자 한다.

I. 서론

정보사회에서의 기업은 IT 기술의 도입 및 성공화가 기업의 성공에 필수적이다. 모든 기업정보를 실시간(實時間)으로 중앙에 집중시켜 그 정보로 생산과 판매과정을 제어하는 것이 기업의 성공열쇠이다. 기업보안은 회사가 처한 보안의 문제점을 잘 알아서 최소한의 금액을 투자하여 최대한의 보안효과를 가지겠다는 것이다. 지금까지 경영자가 조직의 보안상태를 한번에 알고자 한다면 정보보호컨설팅을 통하여 위험관리를 위한 분석을 하였다. 하지만 모든 중요한 자산은 온라인화되어 있고 건마다 세계적으로 10억달러 이상의 피해를 입히는 인터넷웜과 같은 공격은 실시간으로 이루어지는데 매년 하게 되는 일시적 인컨설팅이 역할을 하지 않는다.

국제적인 표준의 "위험관리(Risk Management)" 문서에서는 취약점과 위협을 줄일 수가 있으면 위험이 줄어든다고 하였다. 하지만 현재 새로운 취약점(Vulnerability)을 이용한 새로운 공격(Threat)를 방어하고 탐지하여 대응책을 세워준 정보보호제품이 없고, 정보보호컨설팅이 대책을 완벽히 만들어 제시하고 있지 않는 것이 현실이다.

지금과 같이 정보보호가 많은 예산을 투입하고도 웜을 막아내지 못하는 것은 단순히 Firewall, IDS 등 정보보호제품, 즉 취약성과 위협을 분석하지 않은 제어(Control)만 선호하여 발생하는 것이다.



(그림 1) Security Management Framework

실시보안관리를 보는 우리의 요구사항은,

- 우리가 얼마나 취약한지 실시간에 아는 것,
- 우리에게 얼마나 많은 공격이 오는지 실시간에 아는 것,
- 대응 프로세스를 자동으로 수행하는 것,
- 우리에게 남겨진 위험에 대해서 아는 것
- 위험이 없어지도록 지속적으로 관리하는 것

등이다.

본 논문에서는 실시간보안관리 프레임워크를 도출하기 위하여 현재의 보안관리표준프레임워크, 위험분석, 정보보호컨설팅과 실시간보안관리 등의 동향을 분석하고 본 논문이 주장하는 실시간취약성관리, 실시간위협관리, 실시간위험관리, 그리고 실시간보안관리에 대한 프레임워크를 보이고자 한다.

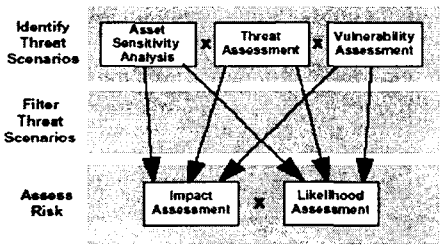
II. 동향분석

1. 보안관리표준프레임워크

BS7799(ISO17799) 및 ISO GMITS 등의 국제 표준이 있으며, 미국에서는 BSP 등의 전략과 최근 FISMA 등의 정보보안문서 보급체계를 가지고 있다.

2. 위험분석

위험분석은 정성적, 정량적 모델 등의 방법론이 있지만 결국 다음 그림과 같은 모델에 기반한다.



(그림 2) 위험분석 모델

원래 위험분석은 CRAMM, Buddy System, Analyze, COBRA, RiskPac, RiskWatch, Safe Suite Decision 등의 많은 제품이 존재하며, 최근 미국은 CIP 계획의 일환으로 IAM, IPAK, VAF, OCTAVE등의 위험분석 방법론을 개발하였다.

3. 정보보호컨설팅 및 ISMS

정보보호컨설팅은 고객의 조직에 대한 보안취약점과 위협을 알아내는 위험분석 등을 수행하여 고객의 위험의 값을 알아내고 결과 고객의 정보자산보호를 위한 대응방안을 제안하는 것이다. 국내외 많은 컨설팅업체들이 존재하며, 전문가 인력 위주의 낙후된 방법으로 컨설팅하고 있으며 결국 인건비 위주의 사업으로 진행 중이다. 전문컨설팅은 BS7799인증원 등에서의 인증을 받기 위한 것이라고 볼 수 있다.

4. 실시간보안관리

최근 해외에서는 실시간 보안관리를 목표로 제품이 발표되고 있다. 이는 대부분 IDS, ESM의 문제점을 바탕으로 개발된 위협관리시스템, MS 의 코드 불완전성을 기반으로 발전한 패치관리시스템, 또한 취약점관리시스템 등이 주류를 이루고 있다.

업체명	제품명	비고
Open	Security Threat Manager	위협관리
ArcSight	TruThreat	위협관리
eSecurity	SEM	위협관리
GuardedNET	NeuSecure	위협관리
Intellitatics	NSM	위협관리
netForensic	SIM	위협관리
PatchLink	PatchLink Update 5.0	패치관리
Shavilk	HFNetChkpro4.0	패치관리
BigFix	PatchManager	패치관리
StillSecure	VMS	취약점관리
ESecurityOnline	eSO Advisor	취약점관리
SecureInfo	EVM	취약점관리

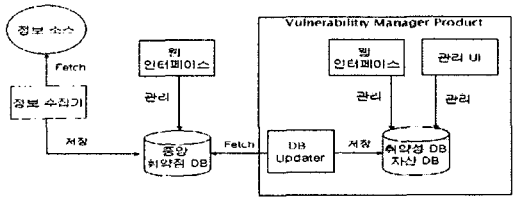
(표 1) 해외 실시간보안관리 제품 현황

III. 프레임워크

1. 실시간취약점관리 (Real Time Vulnerability Management)

VMS(Vulnerability Management System)은 조직에 가해지는 내외부의 다양한 위협에 사용되는 취약성에 대한 정보를 최신의 상황으로 유지함으로서 새로운 위협에 대처하는 가장 기본적인 프로세스라고 할 수 있다. 취약성 관리는 새로운 위협에 대처하기 위한 첫번째 관리 프로세스인 것이다. 취약성관리시스템은 아래 그림과 같이 정보소스로부터 발생하는 취약성과 자체 취약성을 수집하여 DB에 넣고 이를

종합적으로 관리하는 체계인 것이다.



(그림 3) 실시간 VMS 구조도

취약성 관리시스템의 기능은 다음과 같다.

- 신규 취약성 수집 기능
- 신규 취약성 알림 기능
- 자산에 대한 취약성 관리 기능
- 회사 전체, 자산 그룹에 대한 취약성 평가 기능
- 자산의 이력 관리 기능
- 취약성및 자산 데이터 베이스
- 취약성보고서 기능

지금까지는 시스템의 취약성은 스캐너(Scanner)라는 점검도구를 이용하였지만 많은 False Positive 즉 문제가 없는데도 취약하다고 보고하는 것, 서버에 이상을 줄 수도 있다는 것이 문제였으며, 기본적으로 감사를 위한 도구이지 관리도구는 아니었다. 결국 관리도구가 먼저일 것이다.

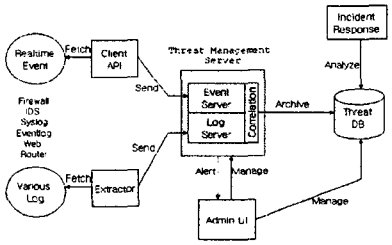
비교항목	스캐너	VMS
목표	Audit Tool	Management
형태	Sampling	전체관리점검
체크시간	정기점검	상시점검
신규취약성	벤더점검도구에 따라	실시간업데이트
잔존취약성	정기점검후관리없음	상시관리잔존크기
취약성갯수	1,000 - 2,000	6,000(매일10개)
정확도	오류많음	매우정확

(표 2) 스캐너와 실시간취약성관리비교

2. 실시간위협관리 (Real Time Threat Management)

전사적 통합보안관리를 함에 있어서 가장 핵심적인 역할은 무엇보다도 위협에 대한 종합적인 관리가 된다. 위협과 단순경고를 명확하게 분리해야 하며, 위협에 적절하게 대응하는 체계를 갖추기 위해서는 취약성에 대한 분석과 함께 위협을 발생시킨 장본인에 대한 즉각적인 조치를 통해서 달성할 수 있다.
TMS(Threat Management System)은 조직에 가해지는 내외부의 다양한 위협에 대해 즉각적인 대응까지를 포함하는 효과적 관리를 위해 개발된 위협 종합관리 시스템이다. 위협 관리는 실시간에 발생되는 모든 위협을 파악하고, 이 위협의 진위를 검사하며, 실제의 위협에 대해서는 바로 대응을 할 수 있는 시스템이다. 위협관리 시스템은 정보자산에 가해지는 위협들을 파악하고 자산을 보호하기 위해서 어떠한 보호대책이 수립되어야 하는가를 결정할 수 있도록 지원하는 시스템이다. 위협 관리는 보안 관리, 즉 위험을 줄이기 위한 노력에 있어서 가장 핵심적인 관리중의 하나이다. 위협 관리 시스템은 위협에 대한 대처를 할 수 있게 하는 지속적이고도 명확한 위협 관리 프로세스를 제공한다. 위협관리시스템은 전사적 보안관리체계의 핵심으로 Threat에 대한 종합적이고도 확실한 대책이 된다

위협관리시스템은 개략적인 구조는 아래의 그림과 같다.각종 정보자산으로부터 발생하는 이벤트를 분석하여 이를 종합적으로 관리하는 체계인 것이다.



(그림 4) TMS 구조도

구조상 주요모듈 각각의 간략한 역할을 살펴보면 다음과 같다.

모듈명	기능
Client API	실시간 이벤트를 서버로 전달
Log Extractor	각종장비의 로그를 서버로 전달
TMS Engine	Filtering, Corelation
Admin UI	관리자 콘솔
Threat DB	이벤트DB

(표 3) <표, TMS 모듈 기능>

TMS는 IDS, ESM 등과 비교를 할 수 있는데 다음 표와 같다.

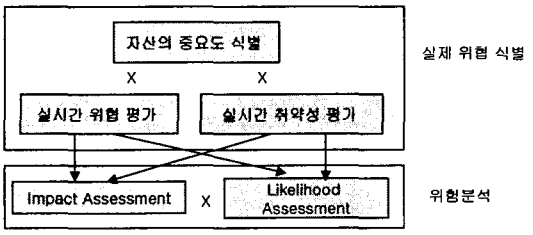
비교항목	IDS	ESM	TMS
이벤트수집	한가지형태	다양한형태	다양한형태
이벤트통합	없음	벤더에 의존	스크립트기반확장가능

이벤트처리	없음	필터링	필터링, corelation
이벤트대응	방화벽	방화벽	메일을 통한 대응프로세스
블랙리스트	없음	없음	대응결과리스트

(표 4) IDS/ESM과 TMS의 비교>

3. 실시간위험관리

실시간위험관리는 실시간으로 취약성과 위협을 관리하면 되는 것으로서 다음 (그림 5)과 같은 모델을 이해한다.



(그림 5), 실시간위험분석 모델

또한 실시간취약성관리는 다음과 같은 모델을 이해한다.

$$Vulnerability = \sum Vulnerability_i$$
$$Vulnerability_i = \sum (Ij * Cj * Rj) * Tj$$

이때 I, C, R, T의 값은 다음과 같다.

I = 자산의 중요도 (자산의 중요도 분석)
C = 자산의 위치에 따른 중요도 (F/W 안쪽, 바깥쪽, ACL 고려) (확률분석)
R = 취약성의 위험도 (영향 분석)
T = 취약성 대처 정도 (0 or 1 - 확률분석)

또한 실시간위협관리는 다음과 같은 모델이다.

$$Threat = ((1- P_{fp}) * I + C * P_{fn}) * n / 3600$$

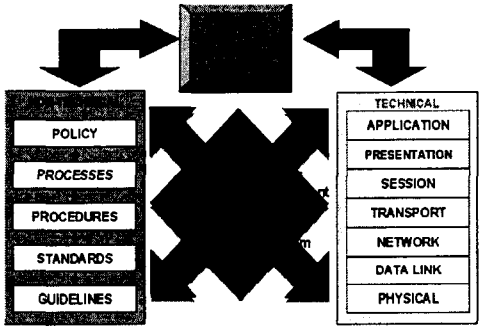
여기에서 사용된 값은 다음과 같다.

Importance = 위협의 크기
Pfp = False Positive일 가능성
Pfn = False Negative일 가능성 (확률분석)
n = 시간당 발생하는 이벤트 수 (영향 분석)
I = 자산의 중요도 분석
C = False Negative의 중요도
(False Negative는 자산에 대입 불가 - 자산의 중요도 분석)
(1- Pfp) = True Positive일 가능성(확률 분석)

4. 실시간보안관리

실시간보안관리는 중요한 정보자산에 대하여 실시간취약성관리와 실시간위협관리를 통한 실시간위험관리가 중요하다. 또한 실시간보안관리는 이러한 체계를 바탕으로 조직의 보안정책과 지침 등을 기술적인 정책에 의한 실시간보안관리로 자동적이 매핑이 요구되는 것이다. 또한 이 자동매핑에 요구되는 것은 다음이 있다.

- 정보보호전략
- 관리수행인정
- 보안관리구조
- 인식제고 프로그램



(그림 6) 실시간보안관리모델

IV. 결론

개정된 OECD 의 정보보안 가이드라인문서에는 ①Awareness, ②Responsibility, ③Response, ④ Ethics, ⑤Democracy, ⑥Risk assessment, ⑦ Safeguards, ⑧Security management, ⑨ Reassessment 등으로서 정보보안관리가 다수를 이루고 있다. 결국 정보보안에는 프로세스에 기반한 정보보안관리가 가장 중요하며, 최근 인터넷 웹등으로 지금까지의 보인기술에 의한 정보제품의 한계를 보였다. 최근 시큐리티랩(주)에서는 실시간보안관리제품을 선보이고 실시간위험관리, 실시간보안관리기술을 준비 중에 있다.

참고문헌

[1] The SANS Security Policy Project, www.sans.org
[2] Robert B. Fried, e-News: An 'Open' Portal Policy, sans.org

[3] Harold F. Tipton, Micki Krause, "Information Security Management Handbook, AUERBACH
[4] ISO/IEC, ISO17799,
[5] Sheldon Borkin, The HIPAA Final Security Standards and ISO/IEC 17799, September 4, 2003
[6] Ben Meader, Securing Internet Explorer Through Patch Management, October 30, 2003
[7] http://www.patchlink.com
[8] http://www.shavlik.com
[9] http://www.bigfix.com/website/index.html
[10] http://www.stbernard.com
[11] http://www.securitybastion.com/
[12] http://www.ecora.com/ecora/
[13] https://www.secureinfo.com
[14] http://www.esecurityonline.com
[15] http://www.stillsecure.com
[16] http://csrc.nist.gov/roi/ IT Security Capital Investment Planning Workshop, June 4, 2003
[17] http://csrc.nist.gov/asset/ Automated Security Self Assessment Tool