정보학연구 제7권 제4호 2004년 12월(pp.9-20)
The Journal of Information Technology. Vol.7. No.4

LAS Advanced & WRC 웹로그 분석을 활용한 ESM에 관한 연구

우승호* · 강순덕**

요 약

본 본 연구에서는 일차적으로 현재 네트워크에서 심각한 문제 유해바이러스를 해결하기 위해서 VirusWall을 실험해본 결과 Dos를 막을 정도 밖에 안되고 이 문제를 해결하기 위해서 이차적으로 ESM, CIS와 MIS면으로 지능화된 인터넷과 Multiple Protocol 등 상황에 맞는 대처를 하도록 로그 분석시스템을 구현하였다. 결과적으로 ESM의 다양한 해킹과 바이러스에 대응하기 위한 지능적인 전사적 보안관리 시스템과 CIS를 이용하기 때문에 정보보호 측면에 폭넓게 이용할 수 있게 되었고, Site Design, Packet 전송별로 클릭할 수 있고, 내부 인터넷(GroupWare)까지 사용되었으며, Smart View를 통해서 전체적인 웹과 보안의 관계도 모니터링 할 수 있게 되었다.

Ⅰ. 서론

현대 사회는 Mobile computing의 시대로 Distributed Computing, Nomadic Computing, Ubiquitous Computing, Wearable Computing으로 에이전트를 이용하여 에이전트를 통한 컴퓨터 간의 통신을 한다.

따라서 네트워크연결이 중단되면 모든 업무가 마비된다.

로버트 메칼프(Robert Metcalfe)박사는 네트워크의 가치를 매칼프의 법칙으로 수량화 했는데, 이 법칙에 따르면 네트워크의 유용성, 효용성은 사용자 수의 제곱과 같다[1]. 그만큼 인터넷은 현대사회에서 사람들의 생활에 깊이 관여하고 있으며, 중요한 매개체로 변화하였다[2].

인터넷과 네트워크 기술의 발달과 인터넷 사용량 및 사용인구의 급증, 정보통신 시스템에 대한 업무의존도 심화에 따라서 인터넷 웜 바이러스 등에 의한 피해 급증, 기밀정보 유출, 개인정보 침해, 정보자산 피해, 대외신뢰도 하락과 같은 정보화 역기능적 요소가 증가하고 있으며, 사회전반의 기반구조 및 경제 사회활동이 정보통신 인프라에 의존하는 비중이 커가고 있는 시점에서의 정보화 역기능은 이미 사회적이 문제로 대두되고 있다.

현실적으로 볼 때 기업들이 보유한 현재의 IT 인력이나 관리 운영 자원들로는 기업이 필요로 하는 보안 수준을 효과적으로 유지하기가 매우 어렵다[15].

해커의 공격이 경제적, 이념적, 이기적, 심리적인 것에서 한 단계 높여서 지능화된 시스템 공격으로 변화하고 있으므로, 현재의 보안관리 통합은 보안 수준을 효과적으로 유지하기 위해서 바이러스의 정교화, 해킹기법의 지능화와 같은 문제들이 Outsourcing으로 통제되어야 한다.

컴퓨터 시스템에 대한 범죄도 다양해지고, 인터넷 지능화 경쟁에 대비하여 CIS(Computer Information System)가 인터넷의 지능화 면으로 유용성의 도구로서 의사결정, 탐색, 브라우징, 검색

* 공주대학교 컴퓨터공학과

하여 전략적 의사결정을 한다. 또한 웹기반 전략 정보시스템으로 콜센터와 추적시스템 지능형 에이전트, 웹기반 교차 판매를 함으로 ESM면의 Service 요구가 계속 증가하고 있다.

외국의 실정은 발달되어 있지만 우리나라에는 일반화가 되어있지 않다. 외국제품을 도입하면 엔터 프라이즈 급이지만 우리나라 실정에서 망차체가 거대해서 노드가 많아져 그 역할을 다하지 못한다. 더욱이 국내 사정은 방화벽, IDS, VPN 공공 기관의 일부의 취약성이 네트워크와 보안관리자와 조화를 이루지 못한다.

심지어 NEIS조차도 정보가 암호화 되지 않은 채 공개되어 물의를 빚은 바 있다[19].

현재 세계는 디지털 경제로 경제적, 사회적 조직적 혁명으로 이행하고 이동한다. 따라서 통신 즉, 네트워크는 신경제의 정보기술의 핵심이 되었다. 정보 기술 지원은 근원이 조직간 비즈니스 제휴가 된다. CIS와 MIS의 필수인 인터넷 지능화 경쟁은 인터넷의 유용성도구로 prototyping, rapid application developing design 등의 기능이 있다[3].

CIS통제는 일반통제와 응용통제로써 일반통제는 물리적방법, 접근방법(생체인식과• 웹 통제-인증, 암호화, cable test, 방화벽, 바이러스), 데이터 보안, 통신 즉 네트워크, 관리방법 등이 있다. 응용통제는 소프트웨어의 구현으로 입력, 처리, 출력으로 나뉜다. 모든 위협에 대비를 한다는 것은 아주 어렵다. 방어전략으로는 예방, 지연, 감지 제한 복구 수정이 있다. 그리고 재난 복구 계획 요소는 효과적 통제와 보안관리를 통합하는 것이다. 보안관리는 재난 복구계획의 일부분이다[13].

본 연구에서는 보안문제를 재난복구계획의 일부분인 "보안 관리면"의 접근이다.

네트워크 트래픽을 발생시켜 서버가 동작할 수 없도록 하여 업무마비로 인한 인적 물적 자산 리소스를 손해보게 하는 유해트래픽을 해결하는 VirusWall를 ESM면으로 사용하기 위해서 (그림 1)~(그림 4)과 같이 구현하고 테스트 하였다. (그림 5)부터 (그림 12)까지는 실행된 결과를 보여준다.

테스트 결과, ESM면으로 실시간 관리와 Report는 되었지만 DDos문제와 CIS와 MIS면의 문제가 적용이 되지 않았다.

다음과 같이 7가지 기술로 웹 로그 분석을 CIS와 MIS면으로 고려한Report -center를 완성하여 개선된 ESM을 (그림 13),(그림 14)과 같이 구현했고, (그림 15)부터 (그림 18)까지는 Re -portcenter로 구현된 기능과 실행 결과를 보여준다.

1. Risk 관리를 포함한 특정 영역의 전문화 서비스(고객의 생산성 향상을 위한 URL Blocking, 웹 서버 Professional Service)

2. 응용 서버에 대한 Contents 위조에 대한 모니터링 (Web contents filtering & 모니터링)

3. 네트워크에 대한 주기적인 위약성 점검 및 대응 방안 제시 (Vulnerability Assessment)

4. HTTP/FTP/SMTP/POP3를 활용하여 게이트 웨이 방식으로 바이러스 유입 및 모니터링 차단 (Antivirus managent)

5. 다국적기업과 대규모 네트워크를 보유한 기업 간의 암호화 통신을 제공 (Managed VPN)

6. 스파이의 침입이나 비 인가된 침입 탐지, 분석 대응 (Intrusion Detection)

7. 가용성 모니터링과 장애 복귀와 트래픽 유행의 분석 소프트웨어 업데이트, 정책 변경 (Fire -wall Management)

결과적으로 ESM의 역할을 하면서 Web system audit역할, 인터넷 유용성 도구의 역할, 흩어진 정보시스템을 취합하여 관리하게 하며, 위협을 관리하는 좋은 예방조치, 외부와 내부 IT의 수백개의 이슈에 대비할 수 있고, 재난 계획 수립

을 위한 전문가 시스템과 재난 복구에 대비한 웹을 통제 할 수 있게끔 되었다.

II. 본론

본 연구에서는 다양화되고 지능화 되어가는 해킹기법과 바이러스 및 악성코드에 대응하기위하여 기존의 ESM보다 지능화되고 관리자가 신속한대응을 취할 수 있도록 도와주는 ESM (Enterprise Security Management)을 기초적인 네트워크 보안장비인 방화벽과 IDS, VPN의 기능을 Reportcenter와 연결하여 보다 보안된 ESM을 구현하는데 그 목적을 둔다.

다양한 변종 Virus의 증가로 인해서 장애 발생 요인의 사전 파악 및 장애 발생 시 신속한 대처가 요구됨에 따라 관제 시스템이 필요하게 되었다. 관제시스템은 실시간으로 VirusWall 시스템의 현황을 모니터링하고, 시스템 리소스의 임계치 설정에 따른 장애 요인 규정 및 장애 발생을 사전에 파악하며, 장애의 유형을 구분하여 그 원인에 따라서 신속한 대처가 가능해야한다. 따라서 본 실험에서는 KNU VirusWall을 구현하여 관제시스템의 역할에 적합하게 작동하는지 실행하였다.

1. KNU VirusWall

유해트래픽으로 인하여 네트워크 트래픽의 부하가 걸려 대역폭이 고갈되고, 서버가 동작할 수 없게 되며, 업무마비가 되어 인적, 물적, 자산 리소스가 낭비된다.

일반 PC, 서버시스템, 네트워크 등의 전산자원에 피해를 주어 전산정보에 손상을 주어 사용하지 못하게 하거나, 업무적으로 불필요한 정보를 전송하게 함으로써 내부자원을 소모시키는 것이 유해 트래픽이다.

(표 1)는 유해 트래픽의 종류와 대응방안을 보여준다.

결과적으로 IP, Port 차단으로 바이러스 차단이 가능하나, 웹, 메일 등 오픈된 서비스 포트로 유입되는 바이러스에 대한 대응 방안은 소극적이며, 스팸메일차단 시스템, 웹 사이트 차단 시스템은 바이러스의 차단기능이 없다[15].

〈표 1〉 유해 트래픽의 종류와 대응방안

유해 트래픽	보안 장비	차단 방식
바이러스	VirusWall	바이러스 패턴에 의한 차단
웜	VirusWall	웜패턴에 의한 차단
	IPS	
	방화벽	IP.Port에 의한 차단
(서비스 거부) Dos. DDos	VirusWall	트래픽 폭주감지 차단 IP. Port에 의한 차단
	IPS	시그너처. IP. Port에 의한 차단
	방화벽	IP. Port에 의한 차단
스팸메일	VirusWall	키워드. 메일ID. IP 출은 동작방식에 의 한 차단
	스팸메일차단 시스템	
유해사이트	VirusWall	
	웹사이트차단 시스템	유해 사이트 등록에 의한 차단

1) KNU VirusWall의 구현기술

VirusWall는 다음과 같은 기술로 구현되었다.

- ▶ 네트워크 연결방식 Plug & Use
- ▶ 네트워크 환경 변화가 없는 Gateway방식
- ▶ 대용량 트래픽 지원
- ▶ 분산 네트워크 구조에 의한 분산환경 지원
- ▶ 다양한 프로토콜 지원
- ▶ Packet Filtering 및 Worm, Dos, DDos 공격 차단
- ▶ 스팸 메일 차단 및 키워드 Filtering, Con-tent Filtering

▶ Virus 탐지
▶ 관련로그에 대한 검색 용이

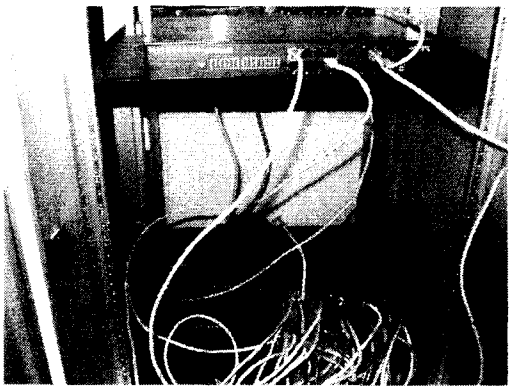
(그림 4)는 위와 같은 기술은 이용하여 구축한 KNU VirusWall의 시스템 아키텍처를 보여준다.

2) KNU VirusWall의 구현 및 결과

① 구현

본 연구에서 KNU VirusWall을 10월 15일부터 10월 22일까지 다음과 같이 실행 하였다.

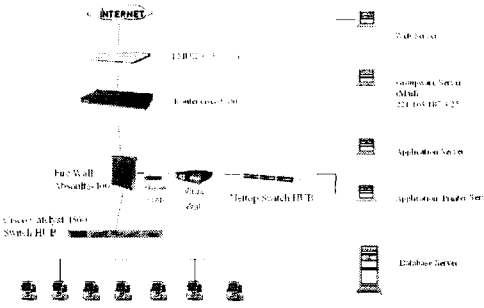
(그림 1)와 (그림 2)는 KNU VirusWall을 설치하는 과정을 보여준다.



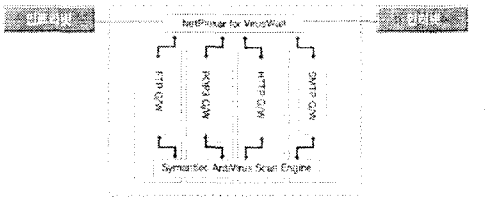
(그림 1) 실습실 스위치 허브에 연결

(그림 2) KNU VirusWall과 Client의 연결

(그림 3)은 KNU VirusWall의 구축된 그림이다.



(그림 3) KNU VirusWall의 구축



(그림 4) KNU VirusWall의 시스템 아키텍처

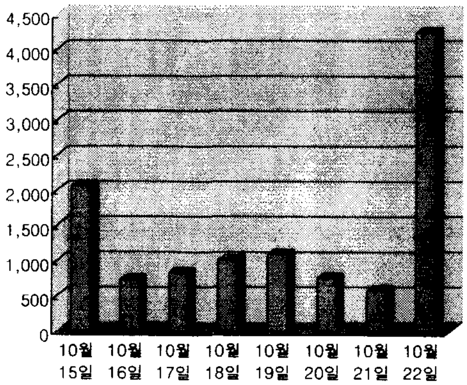
② 결과

▶ 전체 트래픽 검색 건수

〈표 2〉 전체 트래픽 검색 건수

전체	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	합계
전체	2,063	736	833	1,016	1,097	758	580	4,249	11,333

(표 2)은 전체 트래픽 검색 건수에 대한 표이고, (그림 5)은 전체 트래픽 검색 건수를 그래프로 나타낸 것이다.



(그림 5) 전체 트래픽 검색 건수 차트

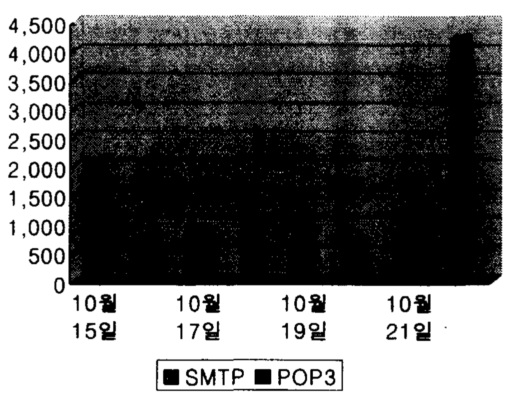
▶ 프로토콜별 검색 건수

〈표 3〉 프로토콜별 검색 건수

전체	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	[illegible]
SMTP	2,042	718	832	1,000	1,094	727	556	4218	[illegible]
POP3	21	18	1	16	3	32	24	31	[illegible]

(표 3)은 프로토콜별 검색 건수를 나타낸 표이고, (그림 6)은 프로토콜별 검색 건수에 대한 그래프이다.

(표 4)는 바이러스 요일별 검색 건수를 나타내는 표이다.



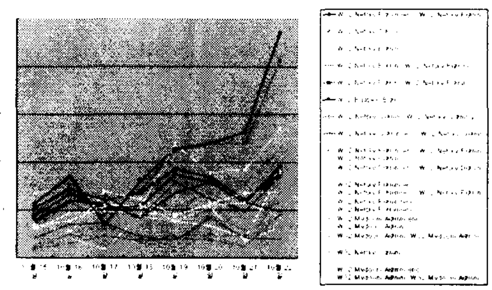
(그림 6) 프로토콜별 검색 건수 차트

▶ 바이러스 요일별 검색 건수

〈표 4〉 바이러스 요일별 검색 건수

바이러스	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	합계
[illegible]	57	85	35	80	114	120	132	235	858
[illegible]	45	75	46	70	112	119	120	206	793
[illegible]	68	73	57	52	118	89	93	135	685
[illegible]	49	63	51	46	104	93	78	114	598
[illegible]	52	72	60	68	93	84	61	88	578
[illegible]	43	67	52	54	87	79	58	96	536
[illegible]	36	59	65	42	79	62	49	85	477
[illegible]	39	60	57	41	68	79	58	49	451
[illegible]	31	58	43	58	53	68	48	58	417
[illegible]	29	47	48	47	44	57	68	69	409
[illegible]	35	27	69	61	45	55	58	43	393
[illegible]	33	39	54	55	38	34	21	89	363
[illegible]	28	46	33	48	34	60	16	89	354
[illegible]	19	35	28	40	51	53	28	58	312
[illegible]	13	31	18	33	48	43	18	44	248
[illegible]	10	21	9	43	38	53	17	33	224
[illegible]	21	35	36	22	18	42	21	20	215
[illegible]	11	20	31	23	11	44	29	44	213
[illegible]	9	25	34	17	7	26	10	69	197
[illegible]	15	31	23	21	17	23	11	45	186
W32 Beagle A@mm	12	25	13	21	23	25	23	33	175
W32 Netsky AB@mm	9	15	23	18	21	19	12	45	182

▶ 바이러스별 검색 건수



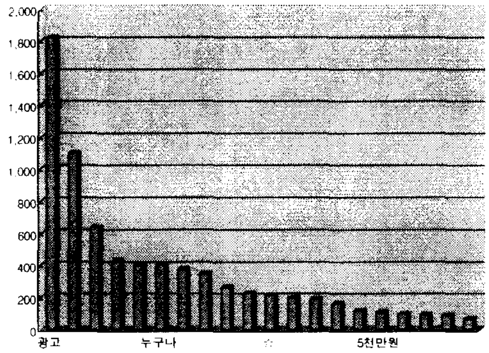
(그림 7) 바이러스별 검색 건수

(그림 7)는 바이러스별 검색 건수를 나타내는 그래프와 검색된 바이러스 종류를 보여준다.

▶ 키워드 검색 건수

〈표 5〉 키워드 검색 건수

키워드	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	합계
광고	1,072	95	69	79	80	41	64	320	1,820
대출	131	145	178	154	128	94	83	189	1,100
무료	62	96	72	99	51	33	38	169	630
1%대	36	20	41	51	54	22	37	165	430
공짜	335	1	2	10	8	11	4	34	405
누구나	32	48	45	68	85	60	14	53	405
◆	1	5	3	20	150	93	5	98	376
★	27	60	13	37	31	42	35	116	350



(그림 8) 키워드 검색 건수 차트

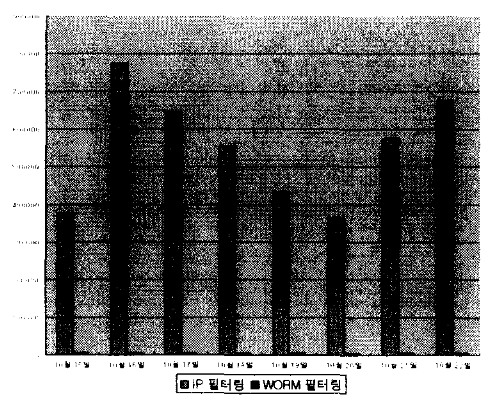
(표 5)은 키워드 검색 건수를 나타내는 표이고, (그림 8)은 키워드 검색 건수에 대한 그래프이다.

▶ 유해 트래픽 분류별 검색 건수

〈표 6〉 유해 트래픽 분류별 검색 건수

유형별	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	합계
IP 필터링	375427	775429	646263	563732	432583	364624	575363	675523	4397914
WORM 필터링	5759	5321	5516	5380	5580	5484	5399	5139	43,568

(표 6)은 유해 트래픽 분류별 검색 건수를 나타내는 표이고, (그림 9)은 유해 트래픽 분류별 검색 건수에 대한 그래프이다.



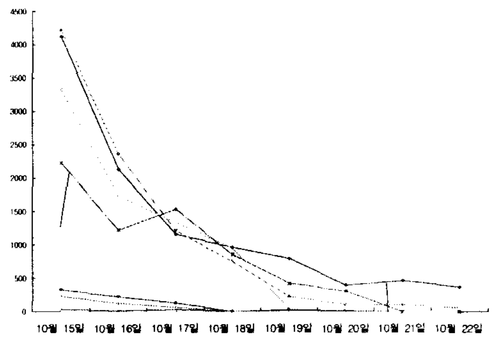
(그림 9) 유해 트래픽 분류별 검색 건수

▶ 웜 바이러스별 검색 건수

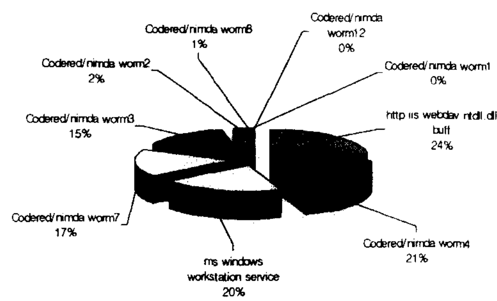
〈표 7〉 웜 바이러스별 검색 건수

웜바이러스 웜네임	10월 15일	10월 16일	10월 17일	10월 18일	10월 19일	10월 20일	10월 21일	10월 22일	합계
http iis webdav ntdll dll buff	4119	2134	1153	964	795	[illegible]	[illegible]	[illegible]	10,404
Codered/nimda worm4	4215	2360	1208	756	228	110	[illegible]	57	9037
ms windows workstation serv	4173	2572	1367	139	111	207	[illegible]	72	8872
Codered/nimda worm7	3326	1730	1332	956	25	12	0	0	7381
Codered/nimda worm3	2225	1227	1532	857	425	[illegible]	0	0	6579
Codered/nimda worm2	325	227	130	6	26	13	0	0	727
Codered/nimda worm8	225	128	61	6	25	13	0	0	458
Codered/nimda worm1	26	14	30	6	24	12	0	0	112
Codered/nimda worm12	0	1	1	0	1	0	0	0	3

(표 7)은 웜 바이러스별 검색 건수에 대한 표이고, (그림 10)와 (그림 11)은 각각 웜 바이러스별 검색 건수를 날짜와 종류별로 나타낸 그래프이다.

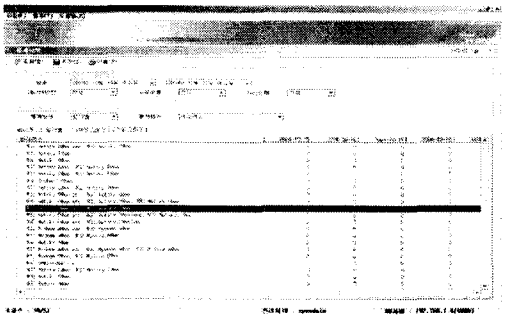


(그림 10) 웜 바이러스별 검색 건수 I



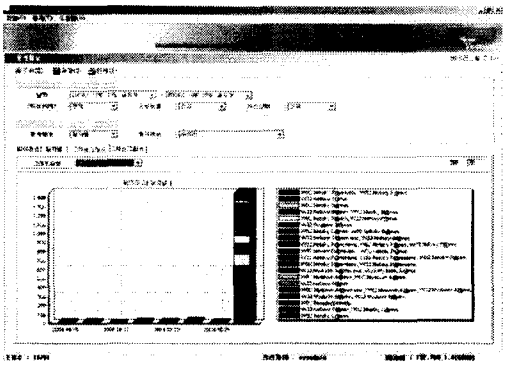
(그림 11) 웜 바이러스별 검색 건수 II

▶ 바이러스 차단 통계 화면



(그림 11) 바이러스 차단 통계 화면

(그림 11)는 바이러스 차단 통계에 대한 화면을 나타내며, (그림 12)는 바이러스 차단 통계에 대한 그래프를 보여준다.



(그림 12) 바이러스 차단 통계 화면 차트

3) KNU VirusWall의 테스트 결과 분석

실험 결과 메일바이러스에는 Netsky, My-doom 등이 많았으며, 인터넷을 통한 다운로드 시에도 바이러스의 유입 이 감지가 되었다. 특히 http IIS, MS windows workstation servce, Nimda등의 웜바이러스 에 의한 공격이 심한 것으로 나타났다. 이러한 위험성이 노출이 상태에서는 내부의 전산자원의 피해가 심각하게 우려되며, 내부 네트웍의 대역폭 낭비, 속도 저하, 네트웍 장애 등의 결과가 나타날 수 있다.

▶ KNU VirusWall의 장점

ESM의 기능인 실시간 시스템 관리 면과 Report를 산출할 수 있다.

① 다양한 경로에서의 유해한 바이러스 유입의 원천적 봉쇄 - SMTP, POP3, HTTP, FTP
② 내부 서버 및 클라이언트들의 바이러스 감염 방지 및 원천적인 차단
③ 최적의 네트웍 성능 유지
④ 인터넷 사용 시 바이러스 유입을 방지
⑤ 웜바이러스의 공격으로부터 내부 전산 자원 보호
⑥ 내부 네트웍 장애 방지 및 관리 비용 절감
⑦ 내부 업무 효율 증대
⑧ 정보 보안의 수준 향상 기대 및 대외적 위상 향상
⑩ 실시간으로 시스템의 자원 및 현황 전송
⑪ 장애 발생 시 알림과 동시에 조회성 정보 표시
⑫ 시스템의 임계치 조정에 의한 경고성 로그 표시
⑬ 장애 및 임계치에 따른 이벤트 발생과 시스템의 정상화 되었을 때 알림 메일 발송
⑭ 예약에 의한 보고서 출력과 Virus, 보낸 사람, 키워드, IP별로 보고서를 표와 그래프로 보기
⑮ Virus의 정보보안 메일 발송

▶ KNU VirusWall의 해결해야할 문제점

실험결과에서 보면 실시간 시스템 감시와 Report등으로 ESM을 지원하면서도 성능면에서 Dos 공격정도밖에 지원하지 못하고 DDos는 지원을 못했다.

결과적으로 LAS Advanced & WRC 웹 로그를 활용한 ESM을 구축하는 것이 지능형 도구

및 CIS와 MIS면으로 완벽한 보안이 될 수 있음을 알 수 있었다.

2. LAS Advanced & WRC 웹 로그를 활용한 ESM구축

현재 사용되고 있는 보안장비는 Gateway방식을 사용하고 있다. 현재 다양한 프로토콜에 의한 위협에 대처하기에는 무리가 따른다. 지능형 보안 장비의 개발이 불가피해 진 것이다. 현재 CIS는 전략적 의사결정 도구로서 웹기반 전략 정보시스템으로 사용자의 중요한 정보를 담고 있기 때문에 보안은 필수이며, 이에 따라서 ESM의 사용이 절대적으로 필요하다. 현재 우리나라의 보안실태를 보면 DDos공격하나 막아낼 수가 없다. 외국의 경우 ESM시스템이 발달되어 있지만, 우리나라의 방대한 네트워크망에 이식하기에는 기술적인 문제가 따른다.

본 연구에서는 LAS Advanced & WRC 웹 로그 분석기인 Reportcenter를 활용하여 우리나라 실정에 맞는 지능형 ESM을 구축하였다.

보안관리 분야는 최근 어려움에 직면하고 있다. 전문적이고 세분화되는 보안 제품의 개발의 추세에서 이를 적용하고 유지 관리하기가 점점 더 어려워 지고 있는 것이다.

1) Reportcenter의 구현 및 결과

사이트와 CIS와 MIS면으로 Content와 전문서비스를 위해서 주 메뉴를 다음과 같이 설정하였다.

- ▶ ESM
- ▶ 마케팅
- ▶ 상거래
- ▶ 사이트 디자인
- ▶ 사이트 성능
- ▶ 시나리오 분석

기능면으로 보면 방문자 현황, 검색엔진 사용통계, Smart View, 시나리오와 같은 기능이 있고 (그림 17)의 경우 Smart View의 기능을 나타낸다. Smart View는 그림에서 보는 바와 같이 왼쪽에 있는 웹을 분석하여 보안체크를 할 수 있게 하였다. (그림 18)의 경우는 시나리오로서 사용자가 각양각색의 시나리오를 만들어서 다양한 접근에 대한 대처를 함으로써 ESM으로써의 성능을 개선하였다.

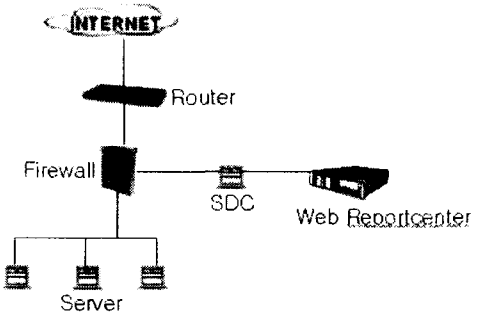
① Reportcenter 구현

Reportcenter의 구현은 다음과 같은 환경에서 구현되었다.

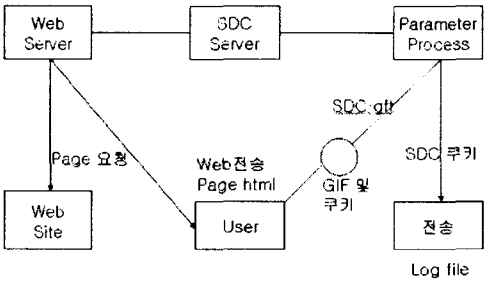
- ▶ Intel P4
  - 2800 Mhz 이상의 프로세서
  - 2 Gbyte Memory
  - 1 Gbyte 디스크 공간(SCSI 디스크들이 추 천됨)

- ▶ Sun
  - 400Mhz UltraSparc-Ⅱ프로세서 이상 (UltraSparc-Ⅲ 프로세서가 추천됨)
  - 1 Gbyte Memory
  - 1 Gbyte 디스크 공간

ESM과 CIS와 MIS를 위한 Web Reportcenter를 (그림 13)과 같이 설치하고, (그림 14)와 같이 동작하도록 구현하였다.



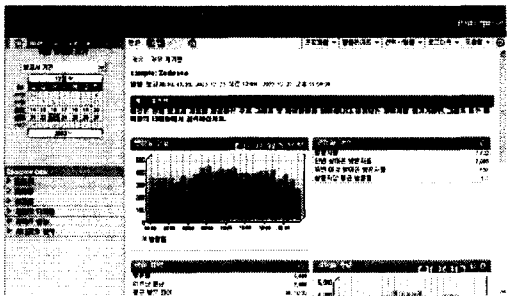
(그림 13) Web Reportcenter의 위치



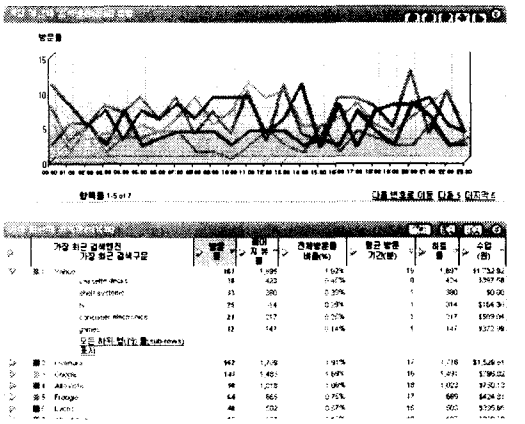
(그림 14) Web Reportcenter의 구조

② 결과

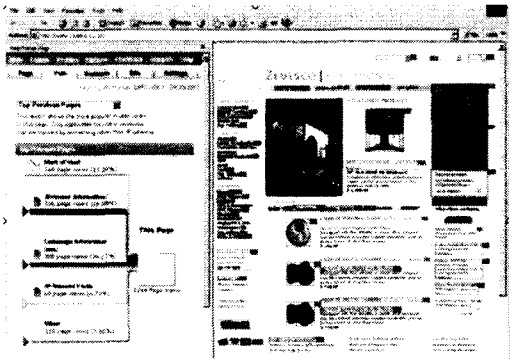
(그림 15)는 Web Reportcenter의 시작 화면며, 첫 화면에서 방문자 현황을 보여준다. (그림 16)은 검색엔진별 사용통계를 나타내고, (그림 17)은 Smart View를 보여주며, (그림 18)은 Web Reportcenter의 흐름을 보여주고 있다.



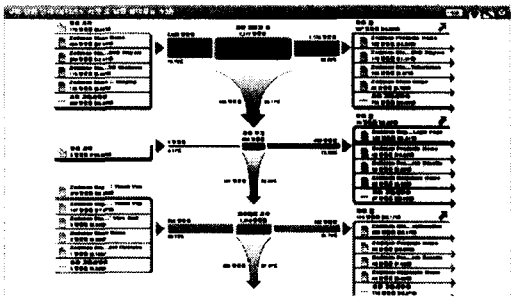
(그림 15) Web Reportcenter의 시작 화면



(그림 16) 검색엔진 사용 통계



(그림 17) Smart View



(그림 18) Web Reportcenter의 흐름

2) Reportcenter의 구축 결과 분석

결과적으로 다음과 같은 7가지 기능을 얻을 수 있었다.

① Web Reportcenter는 ESM면으로 Packet

전송별 검색을 할 수 있다.

② CIS, MIS면으로 내부 인터넷 즉 Groupware를 구현 할 수 있도록 하였다.

③ 대규모 트래픽 사이트를 플랫폼에 구애 받지 않고, 여러 사용자 및 부서들 을 브라우저를 통해 원격 관리 보고서의 환경 설정 및 수정을 할 수 있게 되었다.

④ 프록시 서버 분석, 모니터, 경고 및 복구와 정보기술 구현과 관리 기능을 할 수 있다.

⑤ 방화벽 및 프록시 서버 로그파일들을 분석하고 모든 내부로의(incoming) 및 외부로의(outgoing)활용, 멀티프로토콜 사용, 보안 문제점들, 직원생산성, 대역폭 사용 등에 대해 보고할 수 있게 하였다.

⑥ 취약점들을 탐지하고 해결할 수 있게 되었다.

⑦ 의사결정을 위해 정보기술 사용하는 결정 요인이 된다.

이로써 관리자는 보고서만으로도 빠른 사태파악과 대응을 통하여 피해를 최소화할 수 있을 것이다.

차후에 메모리관리 면과 실시간 비실시간 data를 주고받는 문제와 미디어를 통한 자원 발견에 대해서는 더 연구를 해야 할 것이다.

Ⅲ. 결론

정보 사회로 발전함에 따라 사회 전반의 인프라와 경제 활동이 정보 통신 기술에 의지하게 되었다. 정보 통신 기술이 계속 발전하면서 기술상의 문제점이 나타나게 되었고 이러한 취약점을 이용한 해킹 기술도 단순한 실력 과시용으로 시작되었지만 점점 조직화 및 범죄화 되어 가고 있다. 1980년대의 해킹 기법은 단순히 사용자 계정과 패스워드를 알아내 시스템에 침입하는 형태였다. 1988년에 출현한 인터넷 웜 바이러스와 버퍼 오버플로우 공격기법은 해킹 기법에 새로운 방향을 제시하였다.

현재 정보보호 기술도 다양하게 연구 발전되고 있다.

우선 기본적으로 설치하는 보안장비로 방화벽과 IDS(Intrusion Detection System), VirusWall이 사용되고 있으며, 통합보안 기술로 IDS와 VPN, NAT의 기술을 접목하여 개발하기도 한다.

현재 정보보안의 최상의 보안은 ESM이다. 하지만 ESM은 보안장비일 뿐 정보자원관리의 책임은 ISD와 최종사용자에게 있다. 따라서 이들에게는 인터넷의 지능화 경쟁으로 사이트 방문 및 히트 필터의 추가, 프로파일은 필수적이 되었다[12].

현재 보안은 CIS와 MIS면으로 실시간 해커의 공격이나 바이러스의 감염 시 신속한 대처가 피해를 최소화하여, 관리자로 하여금 사태파악의 시간을 최소화하여 빠른 대응을 할 수 있도록 한다. 이외에도 웹 서버 트래픽 분석, 사용자 접근관리, 프로파일의 처리, 원격 환경 설정 등의 기능이 필수적이다.

또한 웹페이지에 포함된 바이러스 체크, 웹의 방향분석, 파라메타상태와 사이트 디자인, e-business, 인터넷의 인텔리전트를 가능하도록 하는 기능을 갖추고 있으며,. Web 기반 전략정보시스템으로써 Call Center, 추적시스템, 지능형 에이전트, Web 기반 교환판매와 Web 마이닝기능으로써 정보필터링, 감시, 웹접속로그마이닝, 브라우징, 인터넷 범죄예방의 기능능이 요구된다[3][11].

본 논문에서는 이 문제를 해결하기 위해서 VirusWall를 ESM면으로 구현해본 결과 실시간 시스템 대응과 Report만 지원했고, DDos공격과

CIS와 MIS면의 기능이 지원되지 않기 때문에 ESM기능과 웹 로그분석이 추가된 Repor -ting 시스템을 접목하여 네트워크와 시스템에 발생한 오류나 트래픽의 이상, 해커의 침입 징후 등을 보고서화 하여 관리자가 쉽게 알아볼 수 있도록 구현함으로써 ESM을 대체할 수 있도록 하였다.

따라서 사용자 Profile management agent로서 결과는 다음과 같다.

1. ESM의 역할
2. Web system audit역할
3. 인터넷 유용성 도구의 역할
4. 흩어진 정보시스템을 취합하여 관리
5. 위협을 관리하는 좋은 예방조치
6. 외부와 내부 IT의 수 백개의 이슈에 대비
7. 재난 계획 수립을 위한 전문가 시스템이 되도록 구현

현재 구현된 시스템은 메모리가 2Gb나 되는 대형 시스템이므로 이를 노트북과 같은 소형 Cli -ent한대로 Service하는 기술과 단계적으로 ESM과 웹상의 관계, Warehousing,을 CIS와 MIS면으로 기여하도록 하는 것, 실시간 비실시간 data를 주고받는 문제와 미디어를 통한 자원 발견에 대해서는 해결해 나가야할 과제이다.

참고문헌

[1] Andrew S. Tanenbaum Prentice Hall PTR, *Computer networks,* 2003.

[2] William Stallings, *Data & computer communications,* Prenice Hall Inc, 2004.

[3] TURBAN, *Information technology for management,* John & Sons Ins Wiley, 2002.

[4] 양대일, 이승재, "정보 보안 개론과 실습 네트워크 해킹과 보안", 한빛 미디어, 2004.

[5] 양대일, 이승재, "시스템 해킹과 보안", 한빛 미디어, 2004.

[6] http://www.selfcomselfnet.co.kr/net_firewall.htm

[7] http://www.comedu.pe.kr/infbook/book/chp5/chp5-2-1.htm

[8] http://kmh.ync.ac.kr/Hacking/netcademy/kisa/윈도우시스템원격DoS대책-kisa.files/frame.htm#slide0001.htm

[9] http://opendic.naver.com/100/entry.php?entry_id=91739

[10] interactive week,janauary.1998.p34

[11] http://www.nsca.com

[12] http://www.tis.com

[13] http://www.trendmicro.com

[14] http://www.cept.org

[15] http://www.symantec.com

[16] http://us.mcafee.com/default.asp

[17] http://www.iss.net

[18] http://www.knowx.com

[19] 우승호, 강순덕, "NEIS의 취약성에 관한 연구", 「한국정보기술전략혁신학회」, 제6권 제4호, 2003.

[20] 최양서, 최병철, 서동일 "Open Source를 활용한 S-ESM 개발" 한국전자통신연구원 사이버테러기술분석팀

[21] http://www.secuinfo.com/guide/Part3/part 3.htm 한국증권전산의 ESM구축사례

Research about Asynchronous LAS Advanced & WRC Weblog Analysis of Practical use ESM

Seung-Ho Woo* · Soon-Duk Kang**

Abstract

Result Dos that materialization KNU Virus Wall to solve serious problem Hurtfulness Virus in present network chiefly in this research to do not become and do correct disposal in situation such as internet and Multiple Protocol that is done intelligence anger for ESM, CIS and MIS side as secondary to solve this problem about out log analysis system embody.

As a result, could use comprehensively, and can click by Site Design, Packet transmission, and used to interior internet (GroupWare) in information protection aspect because intelligence enemy to face each other ESM's various hacking and virus uses Enterprise Security Management system and CIS, whole web through Smart View and relation of security could do monitoring.

Key words : KNU virus, ESM, WRC, MIS

* Division of Information & Communication Engineering, Kongju National University
** Division of Information & Communication Engineering, Kongju National University