Journal of Digital Contents Society Vol. 8 No. 1 Mar. 2007(pp. 69-76)

그룹웨어시스템상의 악성트래픽 차단 네트워크구조 설계방법

노시춘*, 방기천**

요 약

그룹웨어시스템 악성트래픽 차단이란 인트라넷 시스템상에서 악성트래픽의 확산과 유통을 차단하는 방법이다. 그룹웨어시스템 악성트래픽 차단방식은 전통적 구조에서 차단하지 못했던 다양한 경로와 유형의 유해트래픽을 그룹웨어 내부경로상에서 차단함으로써 보안처리 및 트래픽 과부하를 경감시킨다. 제안된 그룹웨어 시스템 방역을 시행할 경우 내부 게이트웨이와 연결된 Backbone Switch의 CPU상에는 부하율에 큰 변화가 나타났다. 내부 게이트웨이 설치전 트래픽 급증에따라 상승하던 CPU 부하는 내부게이트웨이 설치후 상당수준 감소되었다. 이것은 형태를 알 수 없는 다량의 유해 트래픽이 내부 네트워크를 통과하고 있음을 보여주는 것이며 평상시 네트워크 환경이 얼마나 많은 악성트래픽의 위협에 직면해있는지를 보여주는 것이다. 백본 스위치의 CPU 사용율은 일간 평균 17% 수준을 유지하다가 내부 게이트웨이 상에서 유해 트래픽을 제거한 후는 4% 로서 10% 정도 축소됨으로써 본 연구에서 제안한 내부게이트웨이 방역의 효율성을 입증해준다.

A Study on Methodology for Protection of Malicious Traffic in Groupware Network System

Si-Choon Noh*, Kee-Chun Bang**

Abstract

The blocking of malicious traffic in groupware network system is used to prevent the spread and distribution of malicious traffic. The method protecting from malicious traffic in groupware system is designed to handle the malicious traffic of various routes with the internal course of groupware, which leads to lighten the load of security and traffic. It was impossible to block this kind of traffic at the traditional structure. When the protection of the proposed groupware system is performed, there appears to be a great change for the rate of a load factor at the CPU of Backbone Switch which is connected to the internal gateway. The load factor of CPU, which was increased with the traffic, is now remarkably reduced after the internal gateway is set up. This is to show that a lot of malicious traffic pass through the internal network and that network environment is faced to the menace of many malicious traffics. This paper is to show the efficiency of protection of internal gateway proposed in this study, for the rate of CPU of Backbone Switch was about 17% a day, but was dropped up to the 4% after the malicious traffic was removed.

Keywords : Malicious Traffic, Groupware, Infrastructure

1. 서론

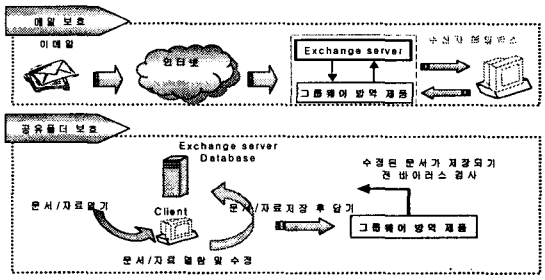
인트라넷 시스템상에서의 그룹웨어시스템 방역방식인 PC나 서버단위의 악성트래픽 삭제, 차단은 어느정도 기능적 취약요인이 내재되어있다. 순간적으로 전파되는 바이러스를 모든 서버나 PC단위로 일일이 삭제하고 차단하므로 비록 백신기술이 뛰어나고 자동화 방식이라 해도 정보시스템 특성에 따라 일정부분의 방역누수가 필연적으로 발생한다. 또하나의 문제점은 특히 심각한것으로 소위 네트워크 트래픽 경로를 따라 감염되는 내부네트워크 확산인바 거점 상에서의 바이러스 진단, 삭제, 유입 차단이라는 방역에 불구하고 방역망을 통과한 바이러스가 그

※ 제일저자(First Author) : 노시춘
접수일자:2007년02월13일, 심사완료:2007년03월15일
* 남서울대학교 컴퓨터학과
nsc321@nsu.ac.kr
** 남서울대학교 멀티미디어학과

룹웨어 네트워크 내부경로를 통해 확산되는 경우이다. 수많은 서버와 PC에서 바이러스를 삭제해도 그룹웨어 네트워크 상에 바이러스가 존재하는 것은 바로 거점 차단 기능 자체가 가진 속성에 기인한 방역 누수가 근본원인이고, 백신 기술 발전에도 불구하고 바이러스의 네트워크 확산이 계속되는 것은 인트라넷 내부의 감염과 확산 악순환 때문이다. 결국 현재의 차단 체계 하에서는 어떠한 바이러스 백신과 솔루션을 적용해도 그룹웨어네트워크 바이러스 확산을 100% 차단할 수 없다. 이같은 상황에서 그룹웨어 네트워크 방역에 대한 해결책은 완전 예방과 완전 차단 대신 현실적 대안으로서 유통 바이러스를 네트워크 통과경로에서 차단 삭제해야 한다. 이를 위해서 현재의 거점 차단 구조를 사용하면서도 네트워크 경로상 확산차단기능을 추가하는 것이다. 이때의 대책은 방역솔루션 기술수준 문제가 아닌 네트워크 차단 구조의 문제이며 차단 위치 선정 그리고 차단시점에 관한 문제이다. 바로 이러한 이유때문에 방역 Infrastructure에 대한 새로운 구조가 도입되어야 한다. 본 논문은 오늘날의 방역 환경에 긴요한 방역인프라 구성에 관한 것이다. 즉 각종 악성코드 공격 패턴에 대응할 수 있는 방역 인프라는 어떤 구조로 개선되어야 하는 가에 대한 대안을 제시한다. 이를 위해 현재 널리 사용되고 있는 일반구조차단체계의 취약점을 진단하고 개선된 인트라넷 내부 차단체계를 제안한다.

2. 그룹웨어시스템의 방역 취약성 요소

그룹웨어네트워크 방역취약점 요인은 방역기술, 인프라구조, 관리나 운용 절차 3개 측면에서 원인을 찾을 수 있다. 방역 기술은 바이러스 침투 기술의 변화에 대응하여 항구적이며 지속적으로 개선해야 할 과제이며 방역 관리 방법, 운용 절차 등은 부분적인 문제점으로 거론될 수 있으나, 근본적인 문제 요인일 수는 없다. 따라서 기업정보시스템의 경우 다음과 같은 문제점을 인프라 구조적 측면의 문제점으로 도출한다.



(그림 1) 일반적인 그룹웨어 방역시스템 기능도

• 차단 기능의 취약성

지금 가장 문제되는 바이러스 침투 형태는 진단, 삭제, 유입 차단으로 해결할 수 없는 내부네트워크를 통한 확산이다. 현재까지의 방역 방식인 백신 기법은거점상에서의 진단, 삭제, 유입 차단에는 효과적이지만 네트워크를 통한 확산의 차단에는 극히 제한적 기능만을 발휘한다. 수많은 서버와 PC에서 바이러스를 삭제해도 네트워크 상에는 여전히 바이러스가 폭증하고 있다. 따라서 네트워크 확산 기능에 대한 대책을 강구하지 않는 기존의 차단 체계는 차단 체계상 커다란 결함 요인이 된다.

내부 네트워크에 접속된 수많은 PC 자원에 대해서는 하나하나의 PC마다 백신을 설치하고 업데이트하는 방법을 사용하여 왔으나 많은 수의 PC 자원에 대한 백신 설치와 업데이트는 너무나 많은 인력 소요가 발생한다. 무엇보다도 바이러스 방역에서의 생명인 방역의 신속성 도모 측면에서 바이러스 침투를 방어하지 못한다. 특히 PC 자원 규모가 증가할수록 이 같은 문제점은 상대적으로 커진다.

• 네트워크 인프라구조 취약성

네트워크 관문, 서버, PC로 고정된 방역 구조는 차단 Zone을 한정시킴으로서 내부네트워크 유통 바이러스 차단기능이 없다. 무엇보다도 1차 방어망을 통과했거나 내부 감염으로 서버, PC에 잠복한 바이러스가 인트라넷 내부를 통해 확산될 경우 서버, PC에 집중된 차단으로는 근본적 해결이 되지 않는다. PC나 서버 단위로 바이러스를 삭제, 차단하는 거점 차단은 순간적으로 전파되는 바이러스를 서버나 PC 단위로 일일이 삭제하고 차단하므로 자동화 방식이라 해도 수많은 작업이 동시에 이루어지는 과정에서 방역 누

수가 발생한다. 클라이언트 위주 방역은 트로이 목마 등 기승을 부리는 악성코드 감염 여부를 진단하고 치료하는 데는 효과를 나타내지만, 인터넷에 접속한 상태에서 공격용 패킷이 유입되거나 해킹 기술을 동반한 형태로 접속해오는 바이러스 움직임에 대한 대처기능이 없다.

• 차단 대상 Zone의 제약성

일반적 차단 체계는 보호대상 자원 설정에서 하드웨어 Resource를 기준으로 하고 있고 따라서 트래픽 소통 경로나 저장 매체를 기준으로 하는 차단 Zone의 개념을 갖지 못한다. 또한 이메일 바이러스 방역에 초점을 맞춰왔고 이메일 이외 타 바이러스 경로에 대한 강력한 억제력을 갖지 못한다. 즉 네트워크 트래픽의 80% 이상을 점유하고 있는 웹을 통한 바이러스 침투대책이 취약하며 또한 파일 공유에 의한 바이러스 감염, CD-ROM, 디스켓 등 내부 매체 감염, 불법 제작 프로그램에 의한 감염 등 다양한 침투에 대한 시스템화된 대응 방안이 되지 못한다. 네트워크 트래픽은 통신 프로토콜과 TCP/IP 서비스별로 특성과 침투 패턴이 상이하다. 다원화된 네트워크 구조는 접속 지점 다양화로 인해 인트라넷 내부 침투 가능 취약 지점이 광범위하게 분포되어있다. 침투 기술은 바이러스 뿐만 아니라 해킹 기술과 결합된 복합 기술의 형태를 띠고 있다. 이같은 환경은 바이러스 백신에만 의존하는 방역 기능으로서는 결코 효과적인 대안이 될수없다.

3. 그룹웨어 방역 개선시스템

그룹웨어 방역은 차단기능설계,내부게이트웨이 설계,통합리얼타임방역망설계등 3개구조의 방역 메커니즘으로 구성한다. 개선된 그룹웨어 방역은 외부로부터의 악성트래픽 유입, 바이러스 감염 메일의 방역, 내부 네트워크 악성트래픽방역, 사용자간의 메일을 통한 바이러스 확산 방지 기능을 제공하며 궁극적으로 인트라넷의 그룹웨어시스템생산성을 높여주는데 적합하여야 한다.

<표 1> 차단 기능 구성

도메인	구간	차단 매커니즘	차단 기능	세부 차단 기능
내부 유통	침입 차단 내부 게이트웨이	게이트웨이 필터링	· SMTP 프로토콜을 통한 바이러스유출입 차단	-이메일 제목 -이메일 첨부물 -이메일 본문 -송신자, 수신자 -키워드 -스팸메일 -첨부물 제거 -메일 사이즈 제한
서버 방역	내부 게이트웨이 서버 방역	서버 바이러스 차단	· 서버군을 자동화 방역 바이러스 월을 구성하여 중앙 집중 관리형 차단	-별도 서버 또는 Embeded방식 -애플리게이션 서버 -파일 서버 -프린트 서버
			· 침입 차단	
			· 진단	-메일 바이러스 -웜 바이러스 -트로이 목마
			· 삭제	-메일 바이러스 -웜 바이러스 -트로이 목마
			· 치료	-감염 바이러스
클라이언트 방역	내부 게이트웨이 클라이언트	클라이언트 바이러스 차단	· 클라이언트군을 자동화 방역 망으로 구성하여 중앙 집중 관리형 차단 시행	-워크 스테이션 급 -PC급 -무선 LAN에 연결된 노트북
			· 침입차단	-내부유입차단
			· 진단	-메일 바이러스 -웜 바이러스 -트로이 목마
			· 삭제	-메일 바이러스 -웜 바이러스 -트로이 목마
			· 치료	-감염 바이러스

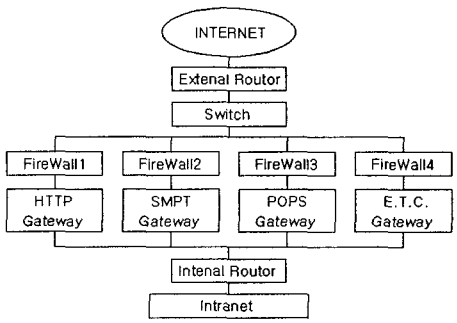
3.1 차단기능 설계

Traffic Node Protection 기능의 취약성에 대처할 수 있는 기능으로 경로 차단 구조를 도입하기위해 다단계 차단 기능을 적용한다. 다단계 차단 기능은 외부 네트워크와의 접점에서부터 인트라넷 구간 최종 접속 단계인 클라이언트 구간까지 단계 차단을 순차적으로 구성한다. 다단계 차단 구조를 도입하는 이유는 네트워크 전구간의 트래픽 소통 단계별로 차별화된 방역을 수행하고자하는 취지이며 또한 전단계의 방역 누수를 다음 단계에서 차단함으로서 방역의 완전성을 실현하는 것이다. 이같이 트래픽소통 구간을 구간별로 관리함으로서 전통적 네트워크 방역 방법론인 경계선 방어 즉, 1개 경로에서 모든 구간 방역을 전담하는 전수방역 방법을 수정한다.

차단 기능이란 설정한 보안 도메인별로 차단 기능을 구성한 것이다. 설계한 차단 구조를 시행할 경우 설정 도메인별로 각각의 침투 유형이 존재하고 이를 차단하는 방법론 또한 각각 강구되고 있음을 보여준다. 차단 기능은 보안 도메인, 네트워크 구간, 도메인별 차단 매커니즘, 도메인별 차단 기능, 도메인별 세부 차단 기능으로 구성하였다. 이 같이 구성된 차단 기능은 기존의 차단 매커니즘을 설계개념으로 구성한 것으로서 기능 자체를 기술적으로 새롭게 개발하거나 설계한 것은 아니다. 다음의 <표 1>은 보안도메인별 차단 기능 매커니즘 구성 내용이다.

3.2 내부네트워크 차단구조 설계

바이러스 감염으로부터 데이터를 보호하기 위해서는 바이러스가 네트워크상 핵심 중요 정보에 도달하기 전에 실시하는데 웹 트래픽과 SMTP 트래픽을 대상으로 한다. 통계에 의하면 일반적으로 전체 트래픽에서 차지하는 비중은 웹 트래픽이 80%, SMTP 트래픽이 10%로 나타난다. 따라서 이 두개 종류의 트래픽에 대해 사전 방역을 실시하는 방안은 바이러스 차단과 Performance 향상 두 가지 측면에서 매우 긴요하다. 게이트웨이 방역의 기본 기능은 필터링 기능이다. 게이트웨이에서 적용할 수 있는 필터링 종류는 바이러스 필터링, 컨텐츠 필터링, 이메일 필터링, 파일 필터링, 스팸 필터링이다. 바이러스 필터링은 패킷 단위로 바이러스 감염 여부를 점검 삭제하며 컨텐츠 필터링은 이메일의 제목과 본문내용에서 특정 키워드가 발견되는 경우 이를 차단하는 기능이다. 이메일 필터링은 이메일 통과 허용 Size를 제한하는 기능이며, 파일 필터링은 특정 첨부 파일명이나 확장자를 미리 검사해 차단하는 기능이다. 스팸필터링은 지속적으로 발송되어오는 광고메일을 차단하는 기능이다



(그림 2) 내부게이트웨이 배치구조도

침입차단 시스템 구간과 내부 게이트웨이 구간 사이에 게이트웨이가 위치하면서 게이트웨이는 TCP/IP 응용 서비스별로 기능이 분담된다. 내부게이트웨이는firewall 이후, 내부 네트워크 진입 전 위치에 배치한다. firewall시스템에서 필터링 처리된 트래픽이 내부 네트워크에 도달하기 전에 게이트웨이 단계에서 바이러스 필터링을 하기 위해서이다. 이 필터링을 실시할 경우 게이트웨이 전 단계인 스위칭 구간, firewall 시스템 구간에서 여과된 안전 패킷 중 방역누수된 패킷이 있을 경우 내부 네트워크 진입 전 재차 필터링이 가능해지고 내부 네트워크로부터의 유출 트래픽에 대해서도 보안 필터링이 실시된다.

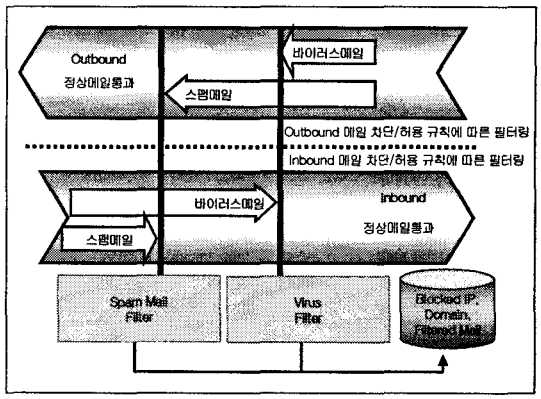
• HTTP Web Gateway

웹 게이트웨이 방역은 HTTP 프로토콜을 통한 바이러스 유입, 유출을 예방하며 사이트, 파일, 필터링으로 보안 위협이 되는 바이러스 유입을 차단하는 방역이다. 인터넷 상에서 제공하는 이메일 계정을 통한 바이러스 사내 유입이 증가하고 있고 외부 웹 서버와의 파일 Download, Upload, 바이러스 감염 이동 현상도 갈수록 증가하고 있다. 이 같은 현상은 종래의 메일 바이

러스 감염 경로가 인터넷으로 이동하고 있음을 의미한다. 웹 트래픽을 방역하기 위해서는 웹 서버 전단에서 웹 트래픽 인식, 분류 기능이 필요하며 IP, URL을 기준으로 패킷을 필터링 하여 보안 위협이 되는 사이트, 개인 이메일을 통한 바이러스 유입, 유출을 방지 한다. 이를 위해 로드 밸런싱 장비인 웹 스위치를 활용하여 트래픽을 분리하여 소통시킨다. 강력한 IP/URL 필터링과 파일 필터링 기능으로 보안 위협이 되는 사이트나 개인 이메일을 통한 바이러스 유입, 유출 방지 업무 이외의 개인 용도의 인터넷 사용을 네트워크 게이트웨이 레벨에서 한발 앞서 차단한다. 외부 네트워크의 악성 웹 사이트의 컨텐츠로부터 내부 네트워크를 보호한다. 불필요한 외부 웹 사이트에 내부 호스트들이 접근하는 것을 차단한다. HTTP 컨텐츠 필터링에는 특정 URL에 대한 접근을 차단하는 URL 접근 제어 기능, 웹을 통한 내부 정보 유출을 방지하기 위하여 유해한 Scirpt, Applet, ActiveX컨트롤 등을 제거하는 스크립트 필터링 기능, 악성 쿠키를 통한 개인 정보 유출을 방지하는 쿠키 필터링 기능 등이 포함된다.

• SMTP/Virus Gateway

이메일 게이트웨이 방역은 SMTP 프로토콜을 매개로 실시간 감시를 수행하여 컨텐츠 필터링과 함께 네트워크 게이트웨이 레벨에서 바이러스 유입을 차단하는 기능이다. SMTP 스캐너는 Incoming, Outgoing, 이메일과 첨부물을 이메일 게이트웨이를 통과하는 시점에서 스캐닝 기능을 수행한다. SMTP 이메일 서버 단위에서 Server Based Solution을 동원하여 파일을 보호한다. 메일 게이트웨이 방역이 스팸메일 차단 기능과 함께 수행될 경우 보안 효율을 보다 높일 수 있다. 게이트웨이단에서 설치되는 메일 방역 솔루션은 유입 유출 이메일을 실시간으로 감시하여 이메일 바이러스에 의한 감염을 방지하고, 강력한 컨텐츠 필터링 기능과 스팸 차단 기능으로 보안 위협이 되는 이메일이 네트워크에 유입, 유출되는 것을 방지한다. SMTP 프로토콜을 매개로 하여 오가는 이메일을 실시간으로 관리하고 강력한 컨텐츠 필터링과 스팸메일 필터링 기능으로 보안 위협이 되는 이 메일 유입, 유출 을 내부 네트워크 진입전에 차단한다.



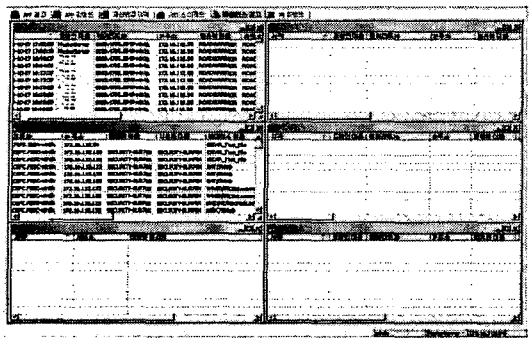
(그림3) SMTP 바이러스 필터링 기능도

• SMTP/SPAM Gateway

스팸메일을 차단하기 위해 송신자 및 수신자에 의한 메일 수신 방지 기능과 제목에 대한 키워드 필터링 기능을 수행하며, 스팸메일 자동차단을 실시한다. 내부 네트워크를 보호하기 위해 메일 송신시 송신자 필드 내용을 변환시켜 전송할 수 있는 기능, 메일 수신시에 첨부파일에 의한 부파일을 제거하는 기능, 내부 비밀 자료 유출방지목적의 전송 메일크기제한 기능을 적용한다. 심층 방어 전략의 일환으로 네트워크내에서 별도의 SMTP 게이트웨이를 사용하여 Exchange 서버를 SMTP 공격으로부터 보호한다. SMTP 서버의 작동을 중지하면 메일 전송이 불가능해질 수도 있지만 내부 이메일 전송은 여전히 가능하다. 하드웨어 일체형의 스팸메일 차단 시스템으로 스팸메일 차단, 바이러스 메일 차단, 메일 서버 보호 역할을 한다.

3.3 Real-time 통합방역망 설계

Real-time 방역은 수동조작을 가능한 축소하고, 자동화된 제어 매커니즘을 통해 Real-time의 방역망을 구성하는 체계이다. 구성내용은 Real-time 엔진 업데이트, Real-time 스캐닝, 종합 제어와 통제이며 이를위해 자동화 네트워크와 시스템을구성한다. Real-time 방역 체계로 바이러스 발생 지점 위치, 바이러스로 관련 정보, 바이러스 확산 정도, 바이러스로 인한 시스템 자원의 피해 정도, 바이러스 치료 여부, 백신 정보 등 주요 정보를 실시간으로 파악한다.



(그림 4) 통합Real-time 방역 시스템운용화면

서버와 클라이언트 레벨 차단 알고리즘은 양 도메인 모두 공통적인 원리와 기능을 바탕으로 한다. 공통의 원리란 구성된 보호 대상 자원 전체를 대상으로 관리측면의 통합 관리, 기능측면에서의 즉시성과 자동화를 기반으로 하고 있다. 클라이언트용 백신은 PC의 바이러스를 차단하거나 서버에 잠복해 있는 메일의 첨부 파일에 대해서는 검사하지 못한 채 서버의 DB가 감염될 경우 전체 네트워크에 치명적인 결과를 초래한다. 널리 배치된 많은 수의 클라이언트에 대한 개별적인 방역보다는 서버 단위에서 관리하고 방역을 수행하는 서버 차원 방역이 효과적이며 매우 강력하다고 할 수 있다. 특히 인트라넷 내부에 침투하여 확산되는 바이러스 박멸 대책으로서 서버 단위에서의 방역은 대단히 중요한 의미를 갖는다. 내부 네트워크 유통 경로 상의 바이러스 차단을 로컬 파일 서버의 전단에 별도의 바이러스 월 시스템을 설치하거나 각 서버 상에 소프트웨어 삽입(Embedded) 방식의 스캐너를 장치한다.

설치된 백신 엔진에 의해서 각종 바이러스의 내부 유통에 서버 전단에서 다시 한번 바이러스가 차단된다. 백신 엔진 설치 방법은 독립된 서버 형태로 하거나 소프트웨어 모듈(Module) 삽입의 방법을 각 사이트의 실정에 맞게 Customizing하여야 한다. 이렇게 장치된 바이러스 월은 침입차단시스템의 바이러스 월과 게이트웨이 레벨 방역과 조합을 통해 내부 유통 경로상의 바이러스 차단이 가능하다. 서버 레벨 방역 대상 자원은 로컬 파일 서버의 범위에 있는 애플리케이션 서버, 파일 서버, 프린트 서버와 이들 장비에 수용되어 있는 데이터, 애플리케이션, 그룹웨어, 공유폴더, 뉴스그룹이다. 최신 바이러스 침투에 대비하기 위해 백신 업데이트는 지정된 주기에 의해 자동으로 서버에 접속, 업데이트를 진행한다. 관리자에 의해 강제 업데이트도 가능하며 업데이트 장애 발생시 해당 장애를 분석 대처한다. 시스템 장애 발생은 물리적 손실과 직결되므로 이 경우에 대비한 장애 해결은 필수적이다, 백신을 이전 버전으로 복구하는 비상 환원(Rollback) 기능을 통해 문제를 해결한다. 또한 서버별 에이전트(Agent)에 대한 업데이트 기능은 개인별, 그룹별 통제가 가능하므로 문제 발생시 업데이트에 대한 장애를 최소화 할 수 있다.

4. 성능 분석

4.1 분석환경

내부게이트웨이 구간은 전단계에서 차단 조치가 이루어진 트래픽이 내부 네트워크로 진입되는 구간이며 한편으로는 내부 네트워크상에서 경로확산되는 유해 트래픽이 통과하는 구간이다. 이 구간에서는 내부네트워크 또는 진입 유해 트래픽에 대한 차단 실적이 측정되어야 한다. 내부 네트워크 방역구간은 메일 바이러스의 서버군 진입을 차단하는 구간이다. 따라서 메일 바이러스 차단 실적을 측정하고 바이러스 감염 숙주로 이용되는 메일서버상의 바이러스 차단과 시스템 Performance가 측정되어야 한다.

측정항목은 내부 백본네트워크의 CPU부하량, 내부네트워크에 접속된 메일시스템의 바이러스 차단성과 및 프로세스 처리량 등 자원성능이다. 측정에 사용된 시스템은 500대의 서버시스템과 5000대의 클라이언트를 구성한A기업 인트라넷시스템이다. 시스템구성은 외부라우터 와 웹스위치, firewall ,백본네트워크, 내부라우터로 구성되고 구조개선을 통해 내부게이트웨이 설치전후성능을 비교분석하였다.

4.2 분석결과

내부 유통 바이러스는 기존 구조의 방역에서 차단 기능이 수행되지 못하고 있던 부분이다. 검증을 통해서 내부 게이트웨이는 설계 사항에서 의도한 경로 확산 차단 기능을 수행하고 있음을

보여줬다. 즉, 내부 게이트웨이는 여러 경로와 원인으로 유통되는 바이러스나 웜을 차단하고 각종 유해 트래픽에 대한 차단 효과를 보여줬다.

측정 기간동안 내부 게이트웨이와 연결된 Backbone Switch의 CPU상에는 내부 게이트웨이 설치로 인해 CPU 부하율에 큰 변화가 나타났다. 내부 게이트웨이 설치전 내부 트래픽 처리로 인해 급증하던 CPU 부하는 내부 게이트웨이 설치후 급격히 내려갔다. 이 현상은 측정 기간중 정확한 형태를 알 수 없는 다량의 유해 트래픽이 네트워크를 통과하고 있었음을 보여주는 것이다. 이는 평상시 네트워크 환경이 얼마나 많은 위협을 받고 있는지를 나타낸다.

구축 전에는 사용자 응대, 감염 바이러스 치료 등 보안 담당자의 업무 비중이 과다했으나 설치 이후 중앙에서 전체를 관리할 수 있고 자동화 시스템의 역할로 인해 보안 담당자의 수작업이 현저히 줄어들었다. 그러나 산술적인 효과보다도 더 중요한 것은 시스템이 안전하게 보호되고 사용자들의 바이러스로부터의 해방감이다. 바이러스 방역 시스템은 어느 정도의 서버 부하와 이로 인한 성능 저하를 야기하지만 데이터 안전 보호, 대외 신뢰도 향상 등 수치로 환산할 수 없는 이익을 가져다준다는 점이다. 측정 기간중 백본 스위치의 CPU 사용율은 평균 17% 수준을 유지하다가 내부 게이트웨이 상에서 유해 트래픽을 제거한 후는 4% 수준으로 10% 축소되었다. 이 같은 현상은 주간 단위의 측정에서도 평균 14% 수준에서 13% 수준으로 하향 되었다. 측정 결과 분석은 바이러스웜 상에서의 바이러스로 인한 CPU 부하 변화 정도와 바이러스 치료 실패 수준을 구조개선 전후로 비교했다. 또한 바이러스 인한 시스템 처리 지연 발생으로 인한 송신 적체 건수를 비교했으며 시스템 최대 프로세스수를 비교 분석하였다. 분석 결과를 종합하면 방역 인프라 구조를 변경함으로서 전체 트래픽 중 절대 다수를 차지하는 웹 트래픽과 이메일 트래픽에서 적체되었던 바이러스 처리가 게이트웨이 구간에서 좀 더 신속히 치료되므로 인하여 트래픽 소통량이 원활해지고 전반적인 Performance가 향상되는 것으로 나타났다. 개선 성과가 나타난 항목은 바이러스웜, CPU 부하, 바이러스 치료성공률, 송신 적체수, 시스템 프로세스수 등이다.

① 바이러스웜 CPU 부하

바이러스로 인하여 메일 바이러스웜 CPU는 부하 수준이 순간 최대 100%까지 상승함으로서 프로세스 처리 지연이 발생하고 이로 인해 메일 송신 지연이 발생했다. 개선된 구조에서는 바이러스 차단에 의해 바이러스웜 부하가 60%이하로 안정되었다.

② 바이러스 치료 실패 메일

바이러스 급증에 따라 바이러스 치료에 실패하여 바이러스 감염 메일이 메일 서버로 전송되는 메일이 10% 수준에 이르렀으나 구조개선후 3% 이내로 감소했다

③ 이메일 송신 적체

바이러스웜 부하 가중시 전송대기 메일건수가 일간 최대 56,000건에 이르렀다. 바이러스웜 부하경감 시 전송 대기 메일 숫자는 현저히 감소했다.

④ 시스템 최대 프로세스수

전송 적체로 시스템 CPU의 성능이 저하됨으로서 최대 프로세스 수는 3,000개 수준으로 하향 조정이 불가피했다. 그러나 시스템 구조개선후 프로세스 수는 10,000개로 정상 수준에 도달했다.

5. 결 론

슬래머 웜에서 경험했듯이 사이버 공격은 자연 재난과는 달리 사고 발생을 사전에 예측하게 하는 관련 변수가 극히 제한되어 있으며, 발생시 수십분 안에 전 세계로 확산되는 전파력을 보이고 있기에 무엇보다 사고발생 즉시 이상 징후를 발견할 수 있는 환경을 조성하는 것이 중요하다. 현재 인트라넷 시스템 운용 현장에서는 갈수록 빨라지는 바이러스 침투 시간, 침투한 웜 바이러스의 급속한 내부 네트워크 재감염, 다수 서버와 클라이언트 차원에 대한 개별 방역 처리 시간의 과다 소요 등 현재 사용하고 있는 방어 메커니즘으로는 극복하기 어려운 문제점들이 노출되고 있다. 본 논문에서는 이러한 문제점을 해결하고 보다 강력한 방어를 수행하기 위하여 그룹웨어 상에서의 내부게이트웨이구조의 정보보호 인프라스트럭처를 제안했다.

제안 인프라스트럭처는 새로운 설계사상을 기

반으로 하여 프레임워크를 도출하고 기능 메커니즘을 구성했으며, 기반 구조도를 설계했다. 그룹웨어 내부게이트웨이구조 인프라스트럭처는 다원화 차단, 다단계 차단, 차별화 차단을 실행하는 구조이다. 본 논문에서는 제안된 방법론에 대하여 성능분석 모델을 개발하고 사례연구를 통하여 성능분석 및 검증을 실시했다. 정보보호 인프라스트럭처의 효율성 여부는 사용자 또는 사용부서의 지속적인 진단과 튜닝을 필요로 한다. 본 논문으로 제안된 방법론은 향후 업무 현장에서 참고되고 응용될 수 있을 것으로 기대된다.

참고문헌

[1] Andrew Cook, "Building High Performance Firewall and Security Infra- structure", Nortel Networks, 2002.

[2] CCIMB, "Common Methodology for Information Technology Security Evaluation, Part1 ~ Part3. Version 2.1", 1999.

[3] CCIMB, "Common Methodology for Information Technology Security Evaluation, Part2, Version1.0", 1999.

[4] C. Edward Chow, "Introduction to Content

[6] David Baer, "Towards Compatibility with Firewall and Keyword search", Distributed Computing Group, 2002.

[7] David Harley, "Virus Bible", Kyohaksa, 2004.

[8] David Harley, "Virus Revealed", Kyohaksa, 2002.

[9] David Mitchell & Katherine Carr, "Best Practice for multi-tier virus protection", Oxford University, 2002.

[10] Department of Defense Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", August 1983.

[11] D. Peeples, "The Foundations of Risk Management ", 20'th National Information Security Conference, 1990. 10

[12] Dr.Thomas W.Shinder,Debra Littleejohn Shinder, "ISA Server 2000", Syngress Media, 2001.

노 시 춘

고려대학교 경영정보학(석사)
경기대학교 정보보호기술(박사)
KT IT본부 시스템보안부장
KT 충청전산국장
현재 남서울대학교 컴퓨터학과 컴퓨터전공 교수
관심분야 : 차세대통신망, 정보보호, 컴퓨터네트워크

방 기 천

1981년 : 서울대학교 전자공학과(학사)
1988년 : 성균관대학교 정보처리학과(석사)
1996년 : 성균관대학교 전산통계학전공(박사)
1984년~1995년: MBC 기술연구소
1995년~현 재: 남서울대학교 멀티미디어학과 교수
관심분야 : 멀티미디어콘텐츠, 멀티미디어 응용, 인터넷 방송 등