Journal of the Korea Industrial Information Systems Research Vol. 19 No. 6, Dec. 2014
http://dx.doi.org/10.9723/jksiis.2014.19.6.107

정보자산 침해방지를 위한 NAC 구축 사례 연구†

(A Case Study on NAC System Implementation for Infringement Prevention of Information Assets)

송 영 민[1], 홍 순 구[2], 김 현 종[3]
(Yung Min Song, Soon Goo Hong, and Hyun Jong Kim)

요 약 외부로부터의 웜·바이러스 및 악성코드와 해킹 등에 대한 위협이 증가하고 있어 기업의 정보자산 침해방지를 위한 네트워크 보안의 중요성이 커지고 있다. 따라서 본 논문에서는 기업 내부의 네트워크 보호 및 정보 자산 침해 방지를 위한 네트워크 접근 제어(NAC) 시스템의 구축사례를 통해 NAC 구현을 위한 절차 및 방법과 실제 적용에 따른 기업 보안의 개선 효과를 알아보고자 하였다. 이를 위해, A 기업의 NAC의 실제 구축 사례를 바탕으로 기업의 NAC의 구축 과정에서의 주안점과 구축 후의 성과 등을 심층 분석함으로써 기업의 네트워크 보안 효과를 높일 수 있는 방안을 제시하였다. 본 연구는 학문적으로 이 분야의 초기연구로 후속연구를 유발하였다는 점과 실무적으로는 NAC 도입을 위한 가이드라인을 제공하였다는 점에서 그 의의가 있다.

핵심주제어 : 네트워크 접근 제어 시스템, 네트워크 보안, 구축 사례

Abstract The importance of a network security to protect infringement of corporate assets has been issued due to the increasing various threats such as warm virus, vicious codes, and hacking. Thus, the goal of this research is to discover the procedure and methods for a NAC system implementation. In this case study, we suggest that the critical management issues during the implementing a NAC system as well as measure its performance in qualitative and quantitative perspective. The contribution of this paper is both to lead to the further research in this network security field and to provide a guideline for companies willing to introduce a NAC system.

Key Words : NAC, Network Access Control, Infringement Prevention, Case Study

1. 서 론

과거 기업의 IT 보안은 주로 외부로부터 유입되는 웜·바이러스 및 악성코드와 해킹 등에 대응하기 위해 침입차단시스템, 바이러스월, 침입방지시스템(IPS) 등의 네트워크 보안시스템을 도입, 배치하는 데에 집중되어 있었다. 그러나 발전하는 유·무선 네트워크 기술과 단말기의 다양화, 기업 비즈니스 환경의 확대 등으로 인터넷 관문에서 네트워크 침해를 막는 것에 한계가 생겼다. IT 및 보안 관리자들은 네트워크를 보호하기 위해 여러 정보보호 시스템을 구성해 왔음에도 불

† 이 논문은 동아대학교 교내 연구비지원에 의하여 연구되었음.
1) 동아대학교 경영대학원, 제1저자
2) 동아대학교 경영정보학과, 교신저자
3) 동아대학교 경영정보학과

구하고 유해 트래픽이 끊임없이 발생하는 상황에 직면하고 있으며 사용자가 안티바이러스, 개인 방화벽과 같은 보안체계를 마련한다 하여도 운영체계에 적절한 보안패치 및 보안제품 업데이트 미수행 등 보안관리가 취약해 내부에서 발생된 공격에 의해 업무 시스템의 침해가 발생하거나 내부 중요 정보자산이 유출되는 사례가 끊임없이 발생되고 있다. 2009년 7월에 발생한 7.7 DDoS 대란 역시 DDoS 공격을 유발하는 악성코드가 내부 네트워크 내 취약한 사용자 PC에서 활성화되어 업무 시스템을 마비시키고 외부 불특정 네트워크를 공격한 대표적인 침해사고이다[1].

이와 같이 내부네트워크 보안의 중요성이 커지고 있으나 기존의 연구에서는 공격에 대한 사후 대응 및 침입방지와 같은 보안 기술에 중점을 둔 연구가 주를 이루고 있다[2,3]. 이에 본 연구에서는 네트워크 접근제어(Network Access Control, 이하 NAC) 시스템의 개념과 주요 보안기능을 이해하고 기업 내부의 네트워크 보호 및 정보 자산 침해 방지의 관점에서 기존 사용자 기반 정보보호시스템과 연계하여 NAC을 구현하는 방안과 실제 적용에 따른 기업보안의 개선효과, 문제점 등을 사례연구를 통해 분석함으로써 NAC의 기업보안 적용에 효용을 극대화 할 수 있는 방법을 제시하고자 한다.

2. 이론적 배경

2.1 보안 위협과 NAC의 등장

인터넷의 발전으로 인해 DDoS 공격 등 사이버테러와 피싱・파밍 사고, 국내 S/W 취약성을 이용한 인터넷 보안사고 등이 증가하는 추세이다[4]. 기존의 기업 IT 보안은 외부 네트워크로부터 내부 네트워크를 보호하거나, 내부 사용자들의 접근 제한 방식에 한정하여 구축되었다. 또한 기존의 정보보호 시스템은 하나의 정보보호 알고리즘으로 특정한 응용에만 활용이 가능하였다[5]. 그러나 근래에는 원격지에서의 가상사설망접속, 협력사 사용자의 증가, 무선 네트워크 사용자의 자유로운 이동성 등에 의해 전체 네트워크 보안 및 사용자의 네트워크 접근관리가 매우 어려워졌다[6]. 또한, 오늘날 많은 조직이 외부로부터의 네트워크 접속을 허용하기 때문에 과거의 네트워크 보안 정책으로부터의 근본적인 변화를 요구하고 있다. 한국인터넷진흥원 조사에 따르면 정보보안의 위협 원천으로 '불법 해커 등 컴퓨터 범죄자(38.0%)'를 가장 많이 지적했으며, 그 다음 '퇴사한 직원(18.2%),' '현재 근무중인 직원(17.4%)' 순으로[7], 조직 내·외부에서 접근하는 네트워크 보안의 중요성을 보여주고 있다.

외부공격을 차단하는 형태의 관문보안체계(Perimeter Security Architecture) 구조를 가지는 Firewall, IPS(Intrusion Prevention System) 만으로는 내부 사용자로부터 유입, 전파되는 바이러스 및 웜과 내부 사용자들의 권한을 초과한 주요 정보자산으로의 접근을 근본적으로 차단할 수 없다. 이러한 한계를 극복하기 위해 내부 사용자들이 네트워크에 접속하는 순간부터 사용자 인증 및 접근제어 정책을 강력하게 적용하여, 바이러스나 웜의 전파와 불필요한 정보자산으로의 접근을 적극적으로 차단하는 기술 즉, '예방'과 '차단'을 병행하는 적극적인 보안 아키텍처가 필요하게 되었다.

보안 위협의 변화로 필요해진 복합적 보안 기술의 요구사항에 대응하기 위해 가트너 그룹에서는 2004년 네트워크 접근 제어(NAC; Network Access Control)라는 새로운 네트워크 보안 모델을 정의하였다[8].

NAC는 IETF(Internet Engineering Task Force)의 NEA(Network Endpoint Assessment), TCG (Trusted Computing Group)의 TNC (Trusted Network Connect), Microsoft사의 NAP(Network Access Protection)라는 이름으로 표준화 혹은 업계표준이 진행되고 있고, 여기에 연동하는 개별 솔루션으로 시스코 시스템즈(Cisco Systems)의 Network Admission Control, 주니퍼네트워크스의 UAC(Unified Access Control), Microsoft의 NAP(Network Access Protection), 시만텍의 NAC 솔루션 등이 등장하고 있다[9].

이러한 NAC 기술이 대두된 배경에는 IT 기술이 빠르게 발전함에 따라 사용자의 네트워크 접속 형태가 무선을 포함한 보다 다양한 사용자 환경을 지원할 수 있도록 진화되어 왔고, 직접적 보안 침해사고에서 벗어나 웜·바이러스에 의한 간접적 사고 발생 건수가 두드러지게 증가했다는 사실에 기인한다. 국가사이버안전센터에서 발간한 2013년 국가정보보호백서에 따르면 2012년 침해사고는 악성코드 감염이 21,751건, 해킹사고가 19,570건이 발생하였으며, 악성코드의 경우

최근 5년 간 2배가 넘게 증가하였다[10].

2.2 NAC의 정의 및 필요성

NAC는 적절한 권한을 가진 사용자가 보안이 검증된 안전한 단말장치를 이용하여 내부 네트워크 자원에 접속할 수 있도록 제어하는 '사용자 접속 제어 시스템'이다[11]. NAC는 비정상 트래픽을 발생시키는 사용자, 즉 악성코드 및 웜·바이러스에 오염된 PC, 노트북, PDA 및 스마트 폰 등의 모바일 형태의 단말기가 네트워크에 접속하는 것을 원천적으로 차단하여 전체 네트워크가 교란되는 일을 미연에 방지하는 차세대 보안 시스템이다. 네트워크에 접근하는 사용자의 권한과 접속 단말들의 보안상태(바이러스 백신 소프트웨어의 설치 및 동작 여부, OS의 패치 여부 및 환경설정 등), 허가된 네트워크로의 접근여부를 실시간으로 감시·통제하는 등 기존의 보안 시스템들이 보안 위협이 발생한 이후의 사후 대응에 중점을 두었다면 NAC는 네트워크 접속 순간부터 사용 중, 접속이 끝날 때까지 전 부문에 걸쳐 예상되는 보안위협을 효과적으로 예방, 탐지, 통제, 치료할 수 있다.

IT 환경의 급격한 발전과 기업 비즈니스 환경의 확대로 기업내부 네트워크에 접속하는 개인 단말기가 PC, 노트북, PDA, 스마트 폰 등으로 다양화 되고, 내·외부 사용자들의 사내·외 유·무선 접속 등 접속 방식이 다양화 및 확대되어 보안 위협요인들이 증가함에 따라 기업의 내부 보안 관리 강화가 요구되고 있다

2.3 NAC의 주요 구성 요소와 기능

다양한 보안 위협에 대응하기 위하여 NAC는 세부 보안기능들을 통합하여 하나의 시스템으로 구성되어 있으며 주요 구성 요소와 보안기능은 <Table 1>과 같다[12].

3. NAC 구축 사례

3.1 구축 개요

3.1.1 구축 기업 소개

사례기업은 임직원 약 4,000 여명이 근무하며 본사와 지방 및 해외에 사업장을 두고 있는 대기업이다. 해당 기업이 NAC을 구축하게 된 사유는 사용자 PC의 보안을 강화하여 내·외부 비인가 사용자의 내부 네트워크 접속을 차단하고 일관적인 보안 정책을 강제함으로써 웜·바이러스 감염에 의한 내부 업무 시스템 침해 방지 및 내부 정보자산 유출 방지를 위함이다. 적용된 기업 환경은 <Table 2>와 같다.

<Table 1> Components and Security Function of NAC

구성 요소	보안 기능
사용자 인증 및 식별	사용자를 식별하여 접근 권한을 구분, 허가 받지 않은 네트워크 영역에 접근하는 것을 금지하도록 접근제어 정책(ACL)을 수립
정책 적용을 위한 네트워크 접점	사용자에게 네트워크에 연결할 수 있는 접점을 제공 '사용자별 접근 정책'을 실제로 적용함으로써 허가받지 않은 네트워크로의 접근 시도를 봉쇄
단말 무결성 검사	호스트 단말의 보안상태를 점검하고, 문제가 발견된 단말을 네트워크로부터 격리/자동치료 후, 사전 부여된 정책에 의해 네트워크 접속 허용
비정상 트래픽 감지	신규 웜이나 바이러스가 유입 시 발생되는 비정상적인 대량의 트래픽을 감지하여 자동으로 단말을 네트워크로부터 격리
호스트 상태 분석 및 네트 워크 접근 제어	현재 단말의 보안 위협요소를 검사한 후, 위협요소가 발견될 경우 단말을 격리하고 위협요소를 자동으로 해제
리포팅	사용자와 시스템의 네트워크 접근 이력 및 보안 위협요소 발견 상황, 조치 내역을 저장하여 내부 정보보호 관리에 유용한 정보를 제공

<출처: 전한수, 2008, 재구성>

<Table 2> Status of Case Company

구분	기업 환경
사업 분야	선박 제조 (컨테이너선, LNG선, 벌크선, 특수 목적선)
임직원 수	약 4,000명(지방・해외 사업장 포함)
네트워크 환경	고정 IP 환경
인증 체계	AD (Active Directory)를 통한 PKI 인증방식
NAC 구축 형태	Out of Band Controller 방식

3.1.2 구축 필요성 및 방향

사례 기업에서는 기존의 다양한 정보보호시스템을 도입하여 운영 중임에도 불구하고 시스템적 한계와 사용자의 관리소홀 등으로 내부 보안위협요소가 해소되지 않았다. 이를 해결하기 위해 네트워크 보안 시스템 구축의 필요성이 대두 되었다.

네트워크 보안 시스템의 구축 필요성으로는 다음과 같다. ① 비 인가자의 불법 네트워크 접속시도 및 해킹에 대하여 적극적으로 차단한다. ② 임의 IP 변경/부여 등으로 인한 시스템 장애를 예방하고, 악의적 사용자에 대한 End-Point Level에서 원천 차단한다. ③ 정확한 사용자 인식과정을 통한 네트워크 접속 권한을 차등 적용한다. ④ 네트워크 접속 후에도 사용자 권한에 맞는 서비스에만 접근토록 조치하여 불필요한 서비스 접속 시도를 차단한다. ⑤ 웜·바이러스의 보안위협으로부터 기간업무시스템의 보안을 강화한다. ⑥ 감염경로 및 방법의 다양화로 감염된 PC를 네트워크 접속 이전 단계에서 강제적 예방치료 또는 격리하여 감염으로 인한 자료 유출을 방지한다.

<Table 3> BMT Results

구분		G사	C사	Y사	M사	S사
동작방식	구성형태	Out of Band	Inline Out of Band	Inline Switch 연동	Out of Band	Inline Out of Band
	언어지원	한글, 영문	영문	한글, 영문	영문	영문
	Agent 구성	Agentless, Agent	Agentless, Agent	Agent only	Agentless, Agent	Agentless, Agent
	정책수행	ARP Manipulation	VLAN, Endpoint S/W	802.1x, Endpoint S/W	ARP Manipulation	Endpoint S/W
인증	사용자 인증	Web/agent 인증	Web/agent 인증	Agent 인증	Web 인증	Agent 인증
	DB연동	자체 DBMS 사용, RADIUS/MS Active Directory 등 연동지원				
위협관리	필수 S/W 통제·설치유도	필수 S/W 가제 자동설치, 설치 안내 등 적용방식 선택 사용 가능			설치 유도만 가능	
		필수 S/W 미설치 차단				
	PC 관리 통제기능	IP/MAC 사용통제	미지원	Agent 설치된 PC만	IP/MAC 사용통제	Agent 설치된 PC만
	치료/배포	자체 PMS 내장	3nd Party PMS	3nd Party PMS	3nd Party PMS	3nd Party PMS
	악성데이터 차단	Virus 미치료 PC 차단	QoS 지원	Virus 미치료 PC 차단	유해트래픽 탐지/차단	
		유해트래픽 탐지/차단		유해트래픽 탐지/차단		
	매체제어	USB,CD/DVD, FDD	미지원	미지원	미지원	USB,CD/DVD, FDD
접근통제	IP관리	제어/이력 관리	미지원	Agent 설치된 PC만	IP/MAC 사용통제	제어/이력 관리
	우회경로	Ad-hoc NET 탐지				
	탐지/차단	Illegal 라우팅 탐지	미지원	무선랜카드 제어	미지원	Wibro T-Logi
	IP 사용자	방문장/협력업체 등 사용자가 별 권한관리 기능				
	권한관리	ARP Manipulation	Agent F.W Driver	Agent F.W Driver	ARP Manipulation	Agent F.W Driver

<출처: 기업내부자료>

네트워크 보안 시스템의 필요에 따라 시스템의 구축 방향을 아래와 같이 수립하였다.

- 네트워크 차단 시스템의 필요성 및 적용 방법을 검토한다.
- 기 도입된 보안 시스템과 연동을 통한 보안 취약점을 개선한다.
- 사용자 식별기반 보안 프레임워크로 정확한 통제와 보안정책을 적용한다.

3.2 NAC 선정

3.2.1 BMT 구성

기업환경에 가장 적합한 NAC 적용모델 및 시스템 선정을 위해 NAC 제품군에 대해 BMT (Benchmark Test)를 수행하였다. BMT는 백본 내 테스트 VLAN을 구성하고 해당 포트를 NAC 센서와 연결(802.1X 기반 스위치 설정포함)하고 NAC를 통해 내부 단말에 대한 무결성 검증과 NAC 콘솔을 통해 정상적으로 보안정책 부여 및 수행이 가능한지를 검증 하였다.

3.2.2 BMT 결과 평가 및 제품 선정

BMT 평가는 환경구축, 사용자 인증, 사용자 접근통제(분산 방화벽), IP관리 기능, IP사용 신청기능, 유해 트래픽 탐지/차단, 사용자 정보수집 기능, 바이러스 백신 관리기능, 백신 연동 차단기능(Kaspersky 백신 서버 연동), 패치 관리기능 (PMS 연동), 부가기능(매체제어 및 통제), 사용자 정의 정책부여, 시스템 장애 복구, BMT 수행능력 평가의 14개 항목으로 <Table 3>과 같이 평가하였으며 5개의 NAC 제품군 중 영문만 지원되는 3개 제품은 부서별 및 그룹별 오브젝트 정의와 세밀한 사용자 정책 구성, 사용자 인증 창 처리, 조건 미 만족 PC에 대한 설치 유도 안내 등과 같이 BMT 과정에서 실제 운영 시 발견될 수 있는 각종 문제점이 도출되어 선정대상에서 제외하였으며 최종적으로 남은 2개 제품에 대하여 장·단점을 비교하였다.

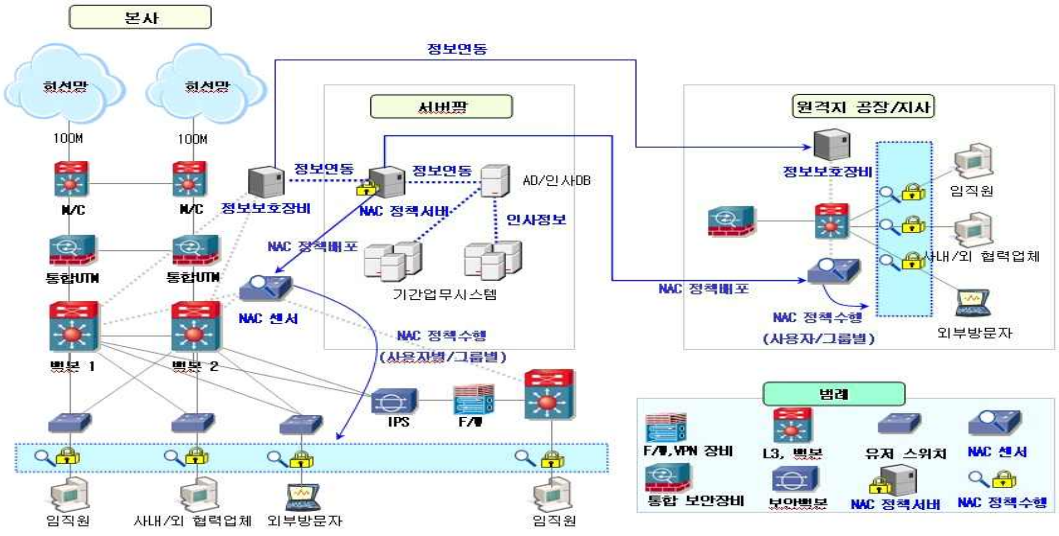
구축 기업의 네트워크 인프라 40%가 802.1X 미 지원 네트워크 장비로 구성되어 있어 최종적으로 구축 기업 환경에 가장 적합한 G사의 제품을 선정하였다.

3.3 NAC 구축

3.3.1 구축 목표 및 구성도

선정된 NAC를 구축하기 위해 아래와 같은 목표를 수립하였으며 이를 달성하기 위한 구성도를 작성하였다.

- 비 인가자 네트워크 접속과 IP 도용시도를 원천 차단한다(IP 실명제 적용).
- 비 인가자/인가자의 사용 권한 별 중요 시스템 접근 권한을 통제한다.



<Fig. 1> NAC Configuration Diagram

<출처: 기업 내부자료>

- PC의 사전 무결성 검사를 통해 웜·바이러스를 차단하고 업무피해 방지, 감염PC 또는 내부자 해킹으로 인한 내부 정보 유출 방지를 강화한다.
- 내부 악성 트래픽 발생 시스템의 추적 및 네트워크 격리를 통해 기간업무 시스템의 안정성을 향상시킨다.
- 기 도입 정보보호시스템과 사용자 정보를 연동하여 사용자 식별기반 보안 프레임워크를 구축한다.

<Fig. 1>은 수립된 목표를 달성하기 위한 시스템 구성도이며 시스템의 요구사항을 아래와 같이 도출하였다.

- 기업 내부 네트워크 중 802.1X 미 지원 장비가 40% 수준이므로, NAC 센서를 백본과 VLAN Trunk로 연동하여 내부의 모든 Client를 제어할 수 있도록 구성하였다.
- 본사에 설정된 NAC 정책서버를 통해 원격지 공장 및 지사에 설치된 NAC 센서 장비에 동일한 보안정책이 전달되도록 하였다.
- NAC 정보는 기간업무시스템의 인사정보 및 Active Directory 정보와 연동하여 NAC 사용자 식별정보의 정확성 및 보안성을 강화하였다.
- 수립된 보안정책 적용계획에 따라 임직원, 사·내외 협력업체, 외부방문자 등에 따라 접속 가능한 네트워크 및 서비스를 사용자 및 그룹별로 구분하여 차등 적용하고, NAC 인증에 실패하거나 보안 제약조건 불만족 단말은 내부망 네트워크 접속을 원천 차단하였다.

3.3.2 구축 일정

NAC는 구축 기업의 보안 및 네트워크 업무 담당자와 공급사의 전문엔지니어들이 TFT를 구성하고 약 3주에 걸쳐서 6단계로 나누어 NAC 서버 구축, 보안정책 수립, Agent 배포, 정책적용, 기존 정보보호시스템 연동 등의 기본설치를 시행하였으며 이후 약 2개월의 안정화 단계를 거쳤다. 이때 안정화 기간은 기존 정보보호시스템 연동 방법 및 수량과 구축 기업 업무담당

<Table 4> Validation Results of NAC

항목	세부항목	점검내용	결과
보안정책	시스템정책	MS계열, 자동 보안패치 진행사항, 필수/악성프로세스 실행여부, 하드웨어 자산정보, 소프트웨어 설치 등의 수집	양호
	네트워크 정책	사용자 역할, 무결성 확인에 따른 네트워크 제한여부 확인	양호
	위험정책	내부 네트워크에 사용하지 않는 IP에 대한 포트스캔, 비정상서비스 요청 등 유해 행위 탐지 허용 되지 않은 서비스 제공 사용자, Add-Hoc 네트워크, 우회경로 등의 이벤트 발생 여부	양호
감사기록	감사기록 확인	감사기록에 Critical 한 위험에 대한 내용 여부	양호
	감사기록 설정확인	일일로그 발생량과 Disk 용량 적정 여부	양호
	통계자료 확인	보안정책에 위반 사용자 및 호스트 목록 확인	양호
시스템환경	시스템 성능	사용량과 시스템의 H/W의 적정성 확인	양호
	네트워크 설정	interface의 설정호가인 Routing Table 확인	양호
	무결성	자료 무결성 확인 및 파일 권한 확인	양호
	시스템 패치	보안S/W의 모듈의 최신 버전 적용 여부, O/S에 최신보안 Patch 적용	양호
	시스템 메시지	네트워크 카드 속도 적정 여부, (10/100, half/full)시스템 H/W에 대한 critical 메시지 존재 여부 시스템 boot 일자 확인	양호
	시스템 파일	시스템에 불필요한 실행 파일이 있는지 확인	양호
	서비스 데몬	보안 S/W 이외 네트워크 서비스 데몬 동작 확인	양호
	디스크 공간	충분한 여분의 디스크 용량확보 여부	양호

<출처: 기업 내부자료>

자의 참여도, 공급사의 신속한 문제 대응에 따라 많은 차이를 보일 수 있으므로 명확한 목표시스템을 설정하고 사전 준비를 철저히 해야 하며 특히 구축 기업 업무 담당자의 적극적인 참여가 요구되었다.

3.3.3 NAC 검증

NAC 구축 후 NAC의 정상가동과 주요기능에 대한 회사의 구축 목표를 만족하는지 점검한 결과 양호한 것으로 판정되었다. 다음 <Table 4>는 구축 후 NAC 검증 결과이다.

3.3.4 구축 및 운영 시 발생한 장애 및 대응

기업에서의 보안시스템의 운영은 사용자들의 불편을 전제로 한다. NAC 구축은 초기에 정확한 사용자 식별기반에서 네트워크 접속, 내부 자료의 접속권한 관리, 보안시스템간의 충돌 등으로 사용자들에게 많은 불편과 불만을 야기 시키므로 주의하여 대응하지 않으면 사용자들의 반발로 각종 보안정책 적용이 무산될 수도 있다.

구축 초기 발생한 주요 사항과 해결방안을 정리하면 다음과 같다.

첫째, Windows 인증, NAC 인증 등 NAC 웹인증에 대한 사용자 불편과 비밀번호 분실 시 Windows 인증인지 아니면 NAC 인증인지에 대한 사용자의 장애접수 내용이 분명치 않아 업무처리에 어려움이 있었다. 상기 부분은 NAC 인증을 AD(Active Directory) 인증과 통합하여 사용자 불편 및 관리업무를 경감시켰다. 이때 사내 협력업체 및 내부 상근 고객사 인원 등에 대해서도 AD 인증으로 일괄 AD 계정을 발급하여 전체적인 관리포인트를 단일화 시켰다.

둘째, 사내 협력업체, 내부 상근 고객사 인원 등 기업 인사DB에 존재하지 않는 사용자가 발견되었다. 기업 인사DB에 존재하지 않는 사용자에 대해서는 일괄적으로 계정을 생성, 발급하고 사용교육과 안내를 하였으며 이로 인하여 초기 업무로드가 가중 되었다.

셋째, NAC Agent 배포 시 기존 바이러스 백신에서 NAC Agent 설치 파일을 악성코드로 오탐하여 설치가 안 되는 사례가 발생하였다. Kaspersky 백신에서 설치 파일을 신뢰구역에 추가하여 문제를 해결하였으나 지속적으로 Agent를 관리해야 하는 번거로움이 발생하였다. 이는 Agent 배포가 필요한 정보보호장비 사용 시 공통적으로 나타난 현상이다.

넷째, 구축 후에도 일부 PC에서 NAC 펌웨어 버그, Agent 버그로 인해 사용자 정보를 정상적으로 전달하지 못하는 문제가 발생하였다. 상기 부분은 PC 이미지 툴로 작업 시 SID(Security Identifier)를 초기화하여 문제를 해결하였으나 지속적으로 버그 문제가 발생되므로 주의하여 대응해야 한다.

다섯째, 초기 사용불편으로 일부 고위 직급자들의 보안정책 예외적용 요청이 발생하였고 업무 및 조직의 급작스러운 변화 발생 시 신속한 보안정책 대응이 필요하였다. 전 직원에 대하여 내부 정보자산 보호에 대한 교육을 실시하였으며 특히, 팀장급 이상은 사전에 별도 교육과 관련 자료를 배포하여 이해를 구하였다. 회사의 보안정책 수립과정에서는 기획, 총무, 설계, 생산, 보안 등 회사의 전 주요 부서를 참여시켰고 주요 부서임원 및 최고경영자의 결재 후 회사의 규정으로 제정함으로써 신속한 대응이 가능해졌다. 그러나 업무 수행 시 발생하는 불편함으로 인해 예외적용 요청은 지속적으로 발생하였다.

3.4 NAC 구축 성과

3.4.1 구축 성과 개요

NAC 구축을 통해 NAC 사용자 인증, 각종 제약조건 검사, 내부 네트워크 및 정보자산에 대한 강력한 접근제어 기능을 활용하여 기존 단위 보안기능 중심으로 구축되어 있던 정보보호시스템과 연동하여 내부망에 존재하는 다양한 보안위협에 대응할 수 있는 종합적인 보안대응 체계로의 전환이 가능해졌다. 구체적인 성과는 다음과 같다

첫째, 내부 네트워크 제어 및 통제를 통해 운영 네트워크에 적합한 인증방식을 사용하여 비인가 사용자의 접속을 원천 차단하게 되었다.

둘째, 단말기 정책 준수 통제를 통해 바이러스 백신 및 최신 MS Patch의 강제 설치로 사용자 단말 PC의 안정성이 강화되었다.

셋째, 이상 시스템 탐지 및 격리로 내부 악성 트래픽 발생 시스템의 추적 및 네트워크 격리를 통하여 네트워크 안정성이 확보되었다.

넷째, 지능적 IT 인프라 관리를 통해 내부 네트워크 및 주요 시스템 변경사항 관리, IT 자산 및 IP 관리로 IT 인프라 관리 수준이 한 단계 발전되었다.

<Table 5>는 NAC 구축 전 보안 문제점에 대하여

<Table 5> NAC Deployment Effect of the Security Problem

항목	구축 전 문제점	구축 효과
네트워크 통제	• 비인가 사용자에 의한 각종 내부망 해킹 및 자료유출 시도 증가됨(악성코드로 인한 비자의적 행위 포함) • 비인가 사용자의 임의 IP 사용으로 정상적인 사용자와 IP 충돌 발생 • 비인가 사용자 PC의 강제 차단 어려움	• 사용자 별 접속 승인 과정을 거쳐 제한적 접속 허용
인가 사용자	• 접속 인가자의 권한 통제를 위해 방화벽 등을 이용하고 있으나 내부 간 서비스는 방화벽을 거치지 않으므로 사각지대 발생	• 인사DB 연동으로 사용자PC 및 IP/MAC 실명제 적용
비인가 사용자	• 비인가 사용자의 내부 네트워크 접속 탐지 어려움	• 비인가 사용자 네트워크 자동감지 및 원천 차단 정책 적용
권한/역할 기반	• 외부 방문자/협력업체 사용자에 대한 제한적 접근권한 부여 어려움	• 인가자 및 그룹권한 설정으로 업무상 필요한 서비스에만 접근 가능토록 조치
서비스 통제	• 각종 보안시스템의 정책 적용시 IP 정보 불일치로 인한 오류 발생	• 외부 방문자/협력업체 사용자에 대한 제한적 접근권한 부여 (기간 설정 포함) • 기 도입된 내부 정보보호시스템과 연동하여 기존 IP/MAC 기반 정책을 사용자 기반 정책으로 변경하여 정책 적용 대상의 정확도 향상
사용자 보안 상태 관리	• 사용자 PC의 보안S/W, OS 보안패치 등의 설치유무에 따른 자동 접속 통제가 어려움	• 보안조건 등 사전 정의된 조건 사항 불이행 PC의 네트워크 접근 차단 또는 소프트웨어 강제 설치 적용
웜·바이러스 확산방지	• 웜·바이러스 출현 시 자동 차단·격리가 되지 않아 이의 급속 확산의 위험성 존재	• 웜·바이러스 출현 시 이상 트래픽 유발을 감지하여 자동 차단·격리
내부 해킹방지	• 네트워크 접속 시 사용자 인증 과정이 없으므로 웜·바이러스 감염PC의 실제 소유자 파악이 어려워 조치 시간 증가됨 (비인가 장비일 경우 추적이 어려움) • 내부 사용자에 의한 스캐닝/해킹툴 공격 등 중요업무 서비스 공격탐지 및 방어가 어려움	• 네트워크 접속 시 사용자 인증을 이용하므로 웜·바이러스 감염PC의 실제 소유자 파악 가능 • 필요시 자동치료 기능 적용 • 내부 사용자에 의한 유해 트래픽 식별 후 네트워크 연결 차단 등 자동격리 정책적용

<출처: 기업 내부자료>

개선결과를 보여준다.

3.4.2 내부 보안위협 감소 (정량적 성과)

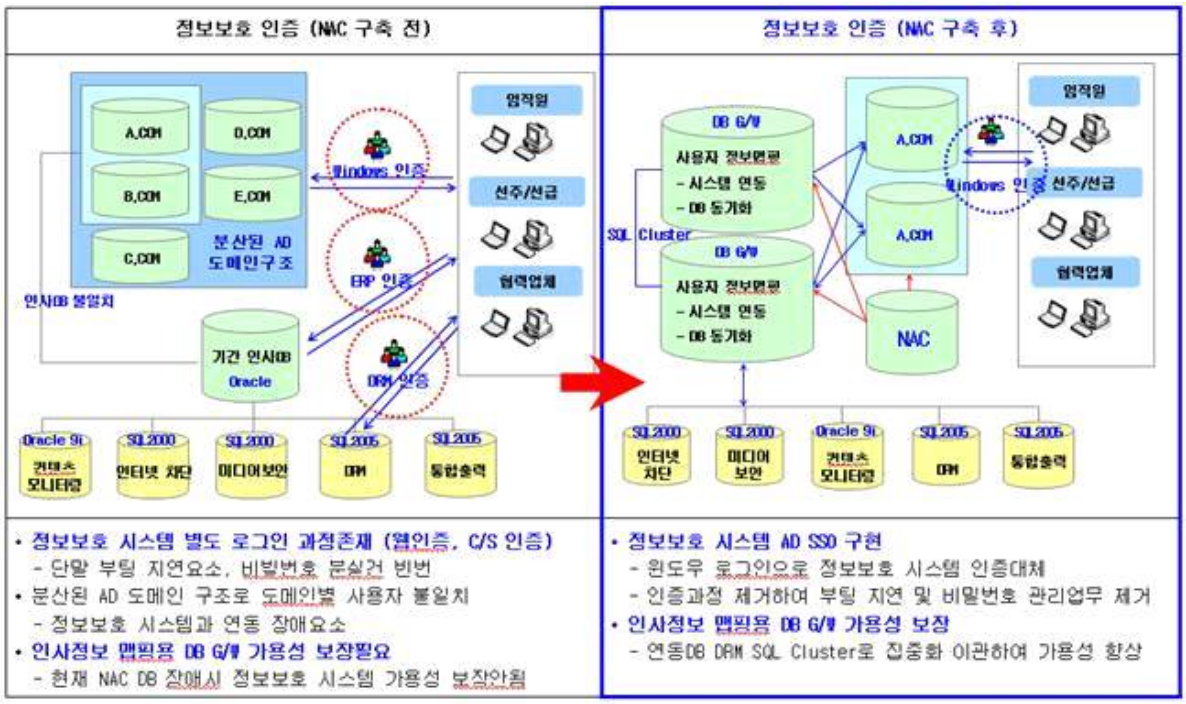
NAC를 도입하기 전 2007년도에 백신 및 보안패치 미설치 PC는 본사 기준 총 1,669대 PC 중 725대로 전체 PC의 43%가 보안위협에 노출되어 연간 221건의 바이러스 감염이 발생되었으나, 2008년도 NAC 구축 후 네트워크 접속 전 보안 제약조건 검사 및 보안위협의 사전 제거 정책 적용 후의 백신 및 보안패치 미설치 PC는 전체 본사기준 PC 1,420대 중 12대 수준으로 전체 PC 대비 1% 미만으로 감소되었다. 실제 바이러스 감염 PC 수도 2007년 221건에서 2008년에는 4건으로 감소되었고 그 이후로도 지속적인 감소 현상을 보이고 있다. 추가적으로 백신 및 보안패치 설치 작업과 바이러스 대응을 위한 지원 업무도 대폭적으로 감소되어 비용절감 효과도 얻을 수 있었다.

3.4.3 정보보호체계변화 (정성적 성과)

NAC 구축을 통해 기업의 정확한 보안 정책 구현이 가능하게 되었고, 사용자 인증의 정확도가 향상되었다.

가. 사용자 식별기반 보안 프레임워크 효과

NAC 구축 전에는 사용자 인증을 통한 통일된 식별 과정이 없으므로, 표준화 되지 못한 개별적 정보보호 시스템내의 사용자 정보에 의존하여 내부 정보 자산 접근 통제 정책을 수행 하였다. 그 결과 정보보호시스템의 통제 기능이 IP/MAC 등 사용자 정보의 변화와



<Fig. 2> Information Security Certification System

<출처: 기업내부자료>

유동성을 반영하지 못하는 형태로 통제됨으로써 각종 내부 정보 자산에 대한 접근, 열람, 복사, 출력, 외부 전송 등의 정보 유통 행위에 대해 상호 관계성을 가지고 일관된 정보보호 정책 부여 및 통제가 매우 어려웠다. NAC 구축 후 기존 개별 정보보호시스템간의 사용자 식별 정보가 일치됨에 따라 기업 내부 정보보호시스템 간 유기적 정보 결합을 통해 정확한 정책 구현이 가능하게 되었고, 업무 시스템에 대한 공격 및 정보 자산 유출 시도 등의 내부 보안 위협에 보다 신속 정확하게 대응할 수 있게 되었다.

나. 정보보호 인증체계 수준 향상

NAC를 구축하기 전 단위 시스템별 인증으로 인한 사용자 식별정보 불일치 및 보안권한 누수 현상이 발생하였으나 NAC 구축 및 AD 통합 작업을 병행 추진하여 일관성 있는 보안정책 및 권한관리가 구현되었으며 정보보호 인증 방식 간소화로 인증체계 수준 및 사용자 만족도가 향상되었다. <Fig. 2>에서 보면 NAC 구축 전에는 정보보호시스템과 인사DB를 연동하여 보안대상이 되는 사용자 정보는 일치시켰지만 실제 시스템의 보안정책은 IP/MAC 등의 정보 조합으로 구현되어 각 시스템별 IP/MAC 정보 불일치로 인한 전체 보안정책의 부정확성이 빈번하게 발생하였다. 또한 AD 환경구성이 통합되지 않아 AD별로 인증정보가 상이하여 도메인별로 사용자 정보가 불일치되는 문제가 발생하였고, 이러한 문제는 정보보호 장비와 연동 시에도 발생하였다. NAC 구축 후에는 AD 통합 및 NAC와의 연동을 통해 사용자 인증부분을 도메인 인증(Windows 로그인)으로 통합하여 사용자 인증의 정확도를 향상시켰으며, 실제 NAC 인증은 도메인 인증정보로 백그라운드로 처리하였다.

3.5 시사점

NAC 구축 시 발생할 수 있는 다양한 이슈 사항의 최소화를 위한 정책 가이드를 정리하면 다음과 같다.

첫째, “Keep security polices simple”은 초기에 사용자와 운영자 모두 NAC 환경에 대한 경험이 필요하므로 최소한의 인증이나 접속행위를 감시할 수 있는 수준의 보안정책이 적당하다.

둘째, “Walk-Before-Run”은 초기 운영 시 모니터링에 중점을 두고 정책 적용 대상은 한 두 곳으로 적

용해서 사용자들의 반응을 피드백 한 후에 적용 범위를 넓혀가야 한다.

셋째, 중요한 위반 사항 시에만 네트워크 접근을 차단한다. 다양한 규정을 점검할 수 있으나, 사소한 위반행위를 차단해서는 사용자들의 반발에 직면한다. 격리나 제한은 가급적 주요한 사항에 대해서만 수행하고, 나머지는 시스템에서 자동 또는 사용자가 수동으로 교정할 수 있도록 안내한다.

넷째, 사용자 예상 대응 시나리오를 작성한다. 가급적 온라인으로 통신할 수 있는 최소한의 통로를 열어두거나 사용자가 교정할 수 있도록 유도해야 한다.

다섯째, 전 직원 교육을 통하여 정보보호의 중요성과 필요성을 인식시킨다. 특히 팀장급 이상에 대한 사전교육과 참여 유도가 필요하다.

4. 결 론

유·무선 네트워크 기술의 발달과 단말기의 다양화, 기업 비즈니스 환경의 확대 등으로 내부 보안 위협이 크게 증가됨에 따라 기존의 외부 관문 보안으로는 기업의 내부 네트워크 보호와 주요 정보자산의 침해 및 유출 방지가 어려워지고 있다. 이에 본 연구에서는 NAC를 구축한 기업의 사례조사를 통하여 NAC의 구축 과정과 구축 후의 성과를 분석하였고 시사점을 도출하였다.

본 연구의 학문적 공헌도는 네트워크 보안 위협에 대한 조사 및 기업의 NAC 구축 과정에 대한 연구를 통해 이 분야의 후속연구를 유발하였다는 점이다. 실무적 공헌도는 향후 NAC의 도입을 고려하는 기업에게 실무적인 시사점을 제공하고 있다는 점이다.

한계점으로는 단일 기업의 구축 사례이므로 개별 기업의 다양한 보안요구 사항에 적합한 NAC의 선정 및 구축방안 제시 등 연구결과의 일반화 문제가 있을 수 있다.

References

[1] Samsung Electronics Security Group, "Loss Prevention Technology Direction for the Information Systems Security," 2007.

[2] S. S. J, "The Improved-Scheme of Two Factor Authentication using SMS," Vol 17, No 6, pp.25-30, 2012.

[3] H. W. Kim, "A Priority Analysis on E-Commerce Security Factors-Focused on Researchers and Practitioners," Journal of the Korea Industrial Information System Society, Vol 16, No 2, pp.163-171, 2011.

[4] Korea Internet & Security Agency, "2014 National Information Security," White Papers, 2014.

[5] Y. M. Lee, "Internet Security and Security Management System (ESM) Building Plan," Beaje University, Master Thesis, 2004.

[6] J. W. Cha, C. H. Kim, "Design of FPGA Hardware Accelerator for Information Security System," Journal of the Korea Industrial Information System Society, Vol 18, No 5, pp.1-12, 2013.

[7] Korea Internet & Security Agency, "Information Security Survey 2012," 2012.

[8] Mirage Networks, "Getting the Knack of NAC, 2006.

[9] National Information Society Agency, "2007 Trends in the Domestic Market and the Industry Survey," 2007.

[10] Korea Internet & Security Agency, "2013 National Information Security," White Papers, 2013.

[11] J. S. Kim, "A Study on the Method of Applying NAC to End-point Security in University Computer Network," Seoul National University, Master Thesis, 2008.

[10] H. S. Jun, "Effective Network Security Model for Dynamic Network Access Control," Korea University, Master Thesis, 2008.

송 영 민 (Yung Min Song)

- 정회원
- 동아대학교 경영대학원 경영학석사
- 관심분야 : 정보시스템, 네트워크, 보안

홍 순 구 (Soon Goo Hong)

- 정회원
- University of Nebraska-Lincoln 경영학과 경영학석사 및 박사
- 동아대학교 경영대학 경영정보학과 교수
- 관심분야 : 중소기업의 정보화, 웹 접근성, 정보시스템 평가, RFID, Co-creation

김 현 종 (Hyun Jong Kim)

- 정회원
- 동아대학교 경영정보학과 경영학석사
- 동아대학교 경영정보학과 박사과정
- 관심분야 : 정보시스템, Co-creation, 빅데이터

논 문 접 수 일 : 2014년 08월 22일
1차수정완료일 : 2014년 11월 14일
게 재 확 정 일 : 2014년 11월 17일