입법기관의 보안강화를 위한 네트워크 분석 및 보안 시스템 연구

남원희* ·박대우*
*호서대학교 벤처전문대학원 IT응용기술학과

A Study on Network Analysis and Security System for Enhanced Security of Legislative Authority

Won-Hee Nam* ·Dea-Woo Park*
*Dept. of IT Application Technology, Hoseo Graduate School of Venture
e-mail: dlbongmt@na.go.kr, prof1@paran.com

요 약

최근 7.7 DDoS 사건과 해킹 사건 등으로 국가기관의 정보보호에 관한 중요성이 대두되고 있고, 정보보호 관련 법률이 국회에서 논의되고 있다. 하지만 국회사무처의 정보보호컨설팅 결과 61.2점으로 매우 낮게 평가 되었으며, H/W, S/W분야의 평가에서도 보안성이 취약한 것으로 나타났다. 본 논문은 입법지원 기관인 국회사무처의 인터넷 네트워크와 사용 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 기밀성, 가용성, 무결성 등의 보안기준에 따라 파악하고, 이를 분석한다. 그리고 입법지원 기관이 갖추어야 할 인터넷 네트워크와 사용 시스템 등에 대한 보안 강화를 위한 설계를 연구한다. 본 연구를 통해 입법지원기관의 보안 현황을 분석하고, 사회적인 책임기관으로서 역할과 보안 강화를 위한 자료를 제공하고자 한다.

키워드

보안 강화(Enhanced Security), 네트워크 분석(Network Analysis), 보안 시스템(Security System)

I. 서 론

IT강국인 대한민국의 입법기관인 국회는 많은 부분이 전자화 되어 있으며 입법관련 많은 정보들이 DB화 되어 관리, 지원되고 있다. 세계 최초로 국회 본 회의장을 첨단 디지털 국회로 바꾸었고, 시각과 청각 장애 의원들을 위한 시설도 설치하였다[1].

국회홈페이지를 통해서 국회에서 진행되는 모든 회의록을 PDF 형식으로 확인할 수 있고, 국회의 본회의·예결위·상임위 및 주요 청문회·공청회, 국정감사 등에 대해 인터넷으로 생생하게 볼 수 있으며, 관련자료 또한 디지털 파일 형태로 제공 받을 수 있다[2].

국회의 특성상 국민을 위한 많은 정보의 제공을 목적으로 하고 있는 국회 네트워크 시스템은 개방성을 가질 수밖에 없을 것이며, 개방성은 외부의 불법적인 해킹[3]에 노출이 되는 취약점을 안고 있다.

최근 7.7DDoS 공격사건에서 문제가 되었듯 정보장애, 개인정보 유출이 빈번하게 발생되고 있다[4]. 또한 국회 네트워크의 개방적 특성상, 국회의원 및 그 보좌진 등에 대해서도 무차별 해킹과 정보침해 사례들이 발생할 수 있으며, 또한 입법기관인 국회의 행정을 주관하는 국회사무처에서 국회의 보안에 대한 책임을 가져야만 한다.

하지만 국회사무처의 정보보호컨설팅 결과 61.2점으로 공공기관의 보안성 평가 중에서도 매우 낮게 평가 되었다. 또한 H/W, S/W분야의 평가에서도 보안성이 취약한 것으로 나타났으며, 특히 정보보호 인식과 행동지침 준수 설문조사에 비추어 국회사무처 직원의 정보보안 인식과 행동지침 준수 정도는 낮은 것으로 평가되었다.

본 논문은 입법지원기관인 국회사무처 본 논문은 입법지원 기관인 국회사무처의 인터넷 네트워크와 사용 시스템 등에 대한 관리적, 기술적, 물리적 보안 요소에 대한 현황을 기밀성, 가용성, 무결성 등의 보안기준에 따라 파악하고, 이를 분석한다. 그리고 입법지원 기관이 갖추어야 할 인터넷 네트워크와 사용 시스템 등에 대한 보안 강화를 위한 설계를 연구한다.

본 연구의 결과는 국회의 보안에 대한 기초자료로 활용되어 국가의 사이버침해 등에 능동적으로 대처할 수 있는 방안을 마련하는 초석이 될 것

이다.

II. 관련 연구

2.1 보안요소

컴퓨터 범죄의 80% 이상이 조직원의 소행으로 나타나고 있고 내부의 운영요원이나 사용자에 대한 지속적인 보안 마인드 교육을 통해 인적 자원에 대한 보안기능의 유지해야 한다. 교육뿐만 아니라 사용자 ID 및 패스워드의 인증절차 및 생성절차의 안정성을 고려하고 전자서명과 지문인식 등을 통한 인증체계 강화하여야 한다. 또, 비밀번호 관리 및 부여체계를 정립하고 사용자 정보의 관리(변경) 체계도 정립시킨다. 그리고 보안감리는 전문가가 맡아야 하는 영역이다.

2.2 보안시스템

개인 및 기업의 중요 자원을 외부의 공격자로부터 보호하고 안전한 인터넷에 사용을 하기 위한 시스템을 보안시스템이라 한다. 따라서 침해가 발생하지 않도록 서버, 네트워크를 방어하는 역할을 한다. 이를 통해 관리자는 보안시스템으로부터 침입자 또는 침입을 시도하는 공격자에 대한 정보를 확인할 수 있고, 이에 대응하고 안전하게 관리할 수 있도록 한다[5].

2.3 F/W, VPN, IDS, IPS, ESM, Virus Wall

2.3.1 침입차단시스템(방화벽, Firewall)

인터넷에 인터넷 프로토콜(IP)로 접속되어 있는 네트워크를 불법적인 침입으로부터 보호하기 위하여 게이트웨이에 설치되는 정보보호 솔루션이다[6].

2.3.2 침입탐지시스템(IDS, Intrusion Detection System)

컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 정보보호 솔루션이다.

2.3.3 가상사설망(VPN, Virtual Private Network)

인터넷망을 이용해 사설망을 구축하여 직접 통신망을 제어하고 감시할 수 있는 네트워크망이다.

2.3.4 침입방지시스템(IPS, Intrusion Prevention System)

네트워크에서 공격 서명을 찾아내어 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 정보보호 솔루션. 수동적인 방어 개념의 침입차단시스템이나 침입탐지시스템과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다[5].

2.3.5 통합관제시스템(ESM, Enterprise Security Management)

침입차단시스템, 침입탐지시스템, 가상사설망 등의 보안 솔루션을 하나로 통합 관리하여 솔루션 간의 상화연동을 통해 전체 정보 통신 시스템에 대한 보안 정책을 수립할 수 있는 통합보안관리 시스템이다.

2.3.6 Virus Wall

인터넷 네트워크망을 통해 유입/유출되는 모든 패킷 트래픽에 유해한 바이러스를 검색, 차단 할 수 있는 솔루션으로 기업의 바이러스 병역과 내부의 기밀문서, 등 중요자원을 보호하기 위한 시스템이다.

III. 현재 입법기관의 네트워크 및 보안시스템 분석

3.1 네트워크 분석

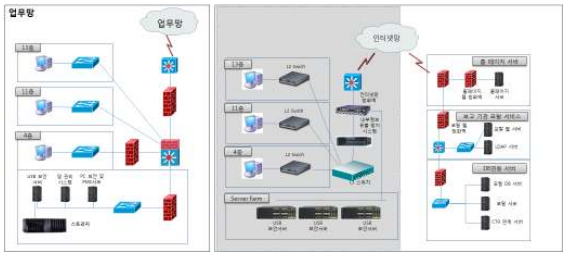

그림 1. 기존 네트워크 구성도

- 현재 사용 중인 네트워크는 업무전용망으로 전화
- 신규 인터넷망 1회선 구성 및 업무 망과 연계한 데이터 연동시스템 구성
- 인터넷망 외부 및 내부 DMZ 구간 구성
- 각 서버군의 공유 및 보안네트워크 구성
- 각 층간 신규L2스위치, 신규L3스위치- 물리적 네트워크 구성
- 내/외부 포탈 및 업무/비업무영역의 선택적인 공유 접근권한 및 경로확보
- 직속기관 및 외부기관 네트워크 접근 규칙에 의거한 네트워크 구성

3.2. 보안시스템 분석

- 보안 강화를 위한 업무망과 인터넷 망의 물리적 분리구성
- 망 분리로 인한 정보 보호의 효과 극대화를 위한 내부정보 관리 강화 구성
- 고의 혹은 부주의에 의한 내부정보의 유출 방지 구성
- 비인가 된 PC의 네트워크 이용 차단 환경 구성
- 외부와의 메일 송.수신을 위한 방안 마련
- 문화체육부의 공직자 통합 메일 시스템을 활용한 외부 메일 송.수신

3.3 보안요소 분석에 따른 개선안

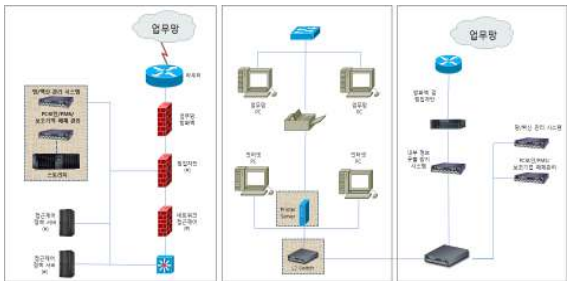

그림 2. 개선 된 네트워크 구성도

- 목표시스템 부합성 – 기능 및 성능 충족도
- 검증된 사이트 확보 및 국내 · 외 표준 준수
- 최신 기술 적용
- 향후 단계별 확장성 및 발전방향 반영
- 안정성을 제고한 대용량 트래픽 수용 장비 구성
- CC인증 및 국정원 인증 장비 및 솔루션 지원
- 우수한 시장 점유율 및 성능에 부합되는 장비

IV. 입법기관의 보안강화를 위한 네트워크 및 보안시스템 연구

4.1 네트워크 보안 강화

4.1.1 물리적 네크워크 분리(업무망, 인터넷망)

그림 1처럼 내부 망 분리는 논리적 망 분리로 구성한다. 서비스 연계 영역 부분은 정부통합 전산센터에서 구현하는 방식으로 서버에 랜카드 2개로 내·외부를 분리하고 방화벽으로 유해정보를 차단한다.

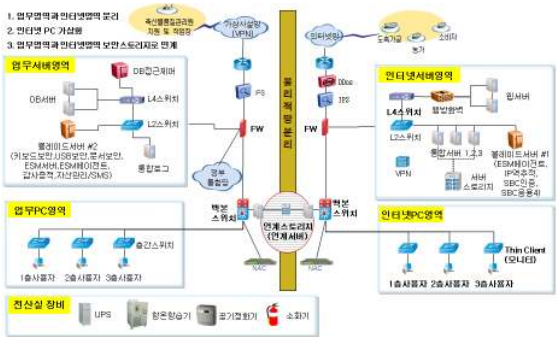

그림 3. 망 분리 시스템 구성도

4.1.2 네트워크 DDos 공격 대응

기간 중 주요 공격감지 및 차단하여 추가적인 감염 차단 및 연속적인 서비스 거부공격이 자동으로 탐지되고, DDoS의 숙주가 되는 봇넷(Botnet)시스템을 자동으로 차단 및 악성코드 전파를 위하여 주변 시스템으로 웜 및 ARP Spoofing을 이용한 전파 시도를 차단한다.

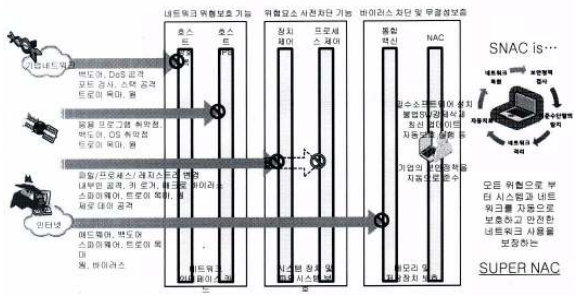

그림 4. DoS, DDoS 포트스캔 등 공격차단 및 확산방지

4.1.3 네트워크 Virus 공격 대응

바이러스, Worm, 트로이목마, 제로데이공격, 스파이웨어, 애드웨어, 루트킷, 해킹도구 등 다양한 악성코드로부터 시스템을 보호하고 자동으로 악성코드를 탐지 및 차단하며, 차단된 로그는 저장하여 관리한다.

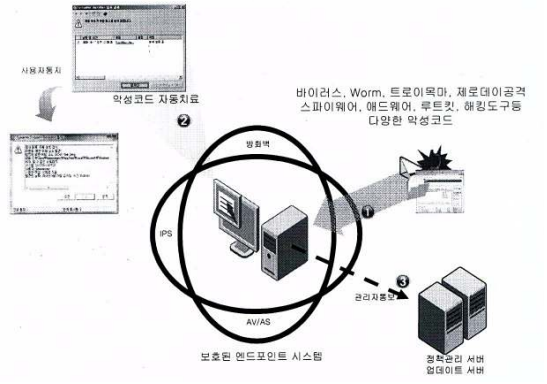

그림 5. 바이러스, 웜 등의 악성코드 차단관리

4.1.4 네트워크 해킹 공격 대응

- 사용자 인증기능

네트워크에 접근하는 사용자에 대하여 모든 네트워크 환경에서의 사용자 인증가능

- PC 보안점검 및 조치

백신/보안패치 설치 및 최신상태 유지, 필수/비인가 SW 설치 여부 등 사용자 단말기 상태 조사 및 자동설치, 설치유도 가능

- 네트워크 접근 제어 기능

유/무선 환경에서의 인가되지 않은 사용자 및 장비에 대해 탐지 및 차단하는 기능

- 비정상 트래픽 제어 기능

사용자 단말에서 발생하는 이상 트래픽(p2p, 불법 인스턴트 메시지 포함) 탐지 및 차단 가능

4.1.5 네트워크 인적 보안

통합센터는 참여인력에 대한 보안서약서 집행, 정보보호 교육 및 수시보안점검 등을 실시할 수 있으며, 사업자는 이에 성실히 응해야 한다.
계약업체는 보안인식 강화를 위해 주기적으로 (월

1회 이상) 실시해야 하며, 센터가 요구하는 보안교육에 참석해야 한다.

문서 및 전산자료 보안을 위해 정보통신망 구성도, 정보시스템 구성도, 용역사업 산출물 및 개인정보 등은 비공개 자료로 분류하여 관리해야 한다.

사업기간 중 과업수행에 필요한 전산장비(PC. 노트북. 디지털복합기)의 무단 반출.입을 금하며, 사업 참여 인력은 외장형 HDD, USB 및 CD/DVD 등의 보조기억 매체를 사용 할 수 없다. 필요시 통합센터의 사전 승인을 거쳐야 한다.

4.2 중요 시스템 보안

국회사무처의 중요 자료인 DB에 대한 보안을 강화할 필요가 있다. 보안 강화를 위한 일단의 방법은 DB 암호화이다. DB 암호화는 국정원에서 CC인증을 받은 국가용 암호제품으로 제공해야하며, DBMS 내 중요 데이터를 칼럼 단위로 선택적 암호화 기능을 제공한다. 초기 및 운영 중 암호화 적용 시 서비스가 중단되지 않아야 한다. 암호화 후 Index검색 기능을 통한 암호화 적용 후 Application 성능이 보장 되어야 한다. 암/복호화 시 시스템 부하를 최소화 하여야 한다. DBMS 이중화(RAC, HA) 및 분산 Application 환경을 지원한다. 다양한 암호화 알고리즘(SEED, TDES, AES, ARIA, SHA1)을 제공한다.

4.3 사이버침해대응센터

- 통합보안관제 시스템에서 생성되는 이벤트 모니터링 및 광역시도 단위의 침해등급 산정, 사고접수 및 대응 조치 이력 등을 종합적으로 관제 할 수 있는 침해분석대응 기반 구축
- 자산 및 취약점 연동 평가/관리, 위험지표 및 수준지표 평가/관리, 사고접수 단위로 위험등급 산정 및 기관 위험등급 산정 등의 종합적이고 체계적인 위험관리 체제 기반 구축

IV. 결론

본 연구결과 국가 주요기관인 입법기관의 정보보호를 위해서는 첫째, 지속적인 직원 정보보호 중요성 인지교육과 행동지침 인식의 활성화가 필요하다. 둘째, 연속적 계획에 의한 물리적 정보보호 기능 확충과 중요 정보에 대한 외부 접근 차단을 위한 내부서버와 외부 접속 서버의 분리가 요구되며, 중요 데이터에 대 한 백본망 등의 구축이 시급하다. 셋째, 정보보안을 위한 조직화된 정보보안 관제센터 등의 운영이 필요하다. 넷째, 입법기관 정보보안을 위한 국회정보보안 관련 근거 법규 제정이 요구된다.

향후 연구로는 국회사무처 직원들의 정보보호 인식에 관한 조사와 H/W, S/W적인 관리적, 기술적, 물리적 보안시스템에 대한 시설과 정보보호 제도의 준수 및 보안 시스템 운용에 대한 분석과 평가를 하여, 직원들에 대한 보안교육과 현장의 보안의무 사항 준수 지침을 만들어 실시한 후에 결과에 대한 분석이 필요하고, 이 결과를 통해 정보보호 관련법을 제·개정하는 것에 대한 연구가 필요하다.

참고문헌

[1] Young-Il Park, [Anniversary of founding a special interview] Won-Ki Kim Chairman, Daily Seoprise, Nov. 2005.

[2] Internet Broadcasting System, http://assembly.webcast.go.kr/, April 2010.

[3] Dea-Woo Park, Moon-Suk Jun, "The Analysis of New Video Conference System for Secure Communications," Journal of International Transaction on Computer Science and Engineering, Vol.2, No.1, pp.200-214, March 2005.

[4] Wan Choung, “A Study on Victims and Legal Response against the Internet DDoS Attack,” Vol.18, No.1, pp.207-228, 2010.

[5] Dea-Woo Park, Seung-In Lim, “A Study of the Intelligent Connection of Intrusion prevention System against Hacker` Attack,” Journal of The Korea Society of Computer and Information, Vol.11, No.3, pp.351-360, 2006.

[6] Dea-Woo Park, Woo-Sik Jung, “The study of performance evaluation between 32bit and 64bit K4 Firewall System,” Vol.8, No.1, Mar. 2003.