5.8 전산망 보호 설비

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.8.1 정보통신망 보호 설비 마련

중요한 연구 정보 및 성과물을 저장·보관하고 있는 PC나 서버 등으로부터 정보를 유출하기 위해서는 정보통신망의 취약점을 이용하여 내부망에 침입하여야 한다. 내부 PC와 서버가 아무리 보안이 잘 유지되고 있다 하더라도 정보통신망의 불법적인 침해로 인해 중요한 정보가 유출되거나 소실될 가능성은 항상 존재한다. 따라서 정보통신망은 외부의 불법적인 침해로부터 보호해야 할 중요한 대상임으로 이를 위한 보호대책을 마련하고 보안시스템을 구축하여야 한다.

내용

· 외부망과 연계되는 구간에 정보통신망의 안전성을 제고할 수 있는 정보보호시스템을 설치하고 운영하여야 하며 정보보호시스템은 다음과 같다.
  - 침입차단시스템(Firewall)은 IP 주소와 접속 포트 등을 기준으로 접속을 선택적으로 차단/허가할 수 있도록 구현된 시스템을 말한다.
  - 침입탐지시스템(IDS: Intrusion Detection System)는 네트워크 상 또는 시스템 내부에 알려진 해킹시도나 비정상 행위가 발견될 경우 이에 대해 경보를 해주는 시스템을 말한다.
  - 침입방지시스템(IPS: Intursion Prevention System)은 인터넷 웜 등의 악성코드 및 해킹 등에 기인한 유해트래픽을 차단하는 시스템을 말한다. 침입탐지시스템의 공격탐지를 뛰어넘어 탐지된 공격에 대해 웹 연결을 끊는 등 적극적으로 공격을 차단하는 시스템이라고 할 수 있다.
  - 가상사설망(VPN: Virtural Private Network)은 공중망을 이용하여 개별망들을 하나의 사설망처럼 구성하여 안전한 통신을 할 수 있도록 보장하는 것으로 인증, 암호화, 터널링 등의 기술로 보안을 가능하게 하는 것을 말한다.

- 바이러스월(Virus-wall)은 외부망으로부터의 악성 바이러스 및 불법적인 공격을 사전에 차단함으로써 내부망의 자원을 보호해줄 수 있는 시스템을 말한다.
- 통합보안장비(UTM: Unified Threat Management)은 하나의 장비에서 여러 보안 기능을 통합적으로 제공하는 시스템을 말한다.

실행지침

1. 정보통신망 보안장비 설치

- 정보통신망에 영향을 주는 웜, 바이러스, 해킹 등의 침입을 방어하고 외부망과 연계되는 주요 회선의 안전성을 강화하기 위해 보안장비를 설치하여야 한다.
- 보안장비 설치에 따른 통신속도 저하 등의 문제가 발생하지 않도록 구성하여야 한다.
- 안전한 네트워크 서비스에 대한 지속적인 제공과 업무 연속을 위해 정보보호시스템에 대한 부하분산을 할 수 있도록(로드밸런싱 및 이중구조 등) 구성하여야 한다.

2. 정보통신망 보안장비 운영

- 정보통신망을 효과적으로 보호하기 위해 보안장비들을 통합 관리할 수 있는 세부지침을 마련하여야 한다.
- 보안장비에 적절한 필터링 규칙 등을 설정하고 적시에 기능을 할 수 있도록 주기적으로 확인하여야 한다.
- 보안장비의 보안 기능이 설정한대로 작동되고 있는지를 주기적으로 점검하여야 한다.
- 보안장비를 운영하는데 있어 가장 중요한 부분인 네트워크에 영향을 주는 웜, 바이러스, 해킹 등의 최신 공격 패턴에 대한 업데이터 및 시스템 자체에 대한 보안패치가 수시로 설치될 수 있도록 조치하여야 한다.
- 보안장비의 가용성을 적절히 확보하여 운영되고 있는지를 주기적으로 점검하여야 한다.

5.9 접근 제한

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	

5.9.1 내부망 연결 제한

외부로부터의 불법적인 침입을 차단하기 위하여 신원이 불분명한 사용자 또는 내부망의 보안관리정책을 준수하지 않은 시스템의 내부망 접근을 차단하기 위하여 내부망 접속 시 적절한 보안대책을 마련하고 이행하여야 한다.

내용

- 내부망에 연결된 정보통신장비를 비롯하여 전산장비와 중요한 연구관련 자료를 보호하기 위하여 불법적인 내부망 접속을 제한하는 대표적인 방법으로 라우터/스위치 네트워크 장비에 보안정책을 설정하는 방법과 네트워크 접근제어(NAC: Network Access Control) 전용 장비를 설치하는 방법이 있다.

① 라우터/스위치에 의한 내부망 연결 제한

- 외부망과 내부망을 연결하는 라우터/스위치 등의 네트워크 장비에 접근제어 설정 기능이 없다면 침해사고 발생 시 즉각적으로 대응할 수 없다. 이런 경우 특정 프로토콜 및 서비스를 허용하게 되는 상황이 발생하여 전체 네트워크 보안을 전반적으로 약화시킬 수 있으며 내부 네트워크 구성요소들을 외부의 공격으로부터 보호할 수가 없다.
- 라우터/스위치 등의 네트워크 장비는 단순히 데이터 전송을 위한 라우팅/스위칭 장비로서의 역할을 담당할 뿐 만 아니라 보안 기능을 탑재한 장비로서 다음과 같은 보안 설정 기능을 지니고 있다.
  - 불필요한 트래픽 및 프로토콜 필터링
  - 서비스 제거
  - 비인가자의 접속제한 조치 등

② 침입차단시스템에 의한 연결 제한

· 외부망과 내부망 사이에 침입차단시스템을 설치하여 허용되지 않은 사용자와 서비스가 내부망에 접근하지 못하도록 접근통제를 실시할 수 있다.

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	내부메일호스트	SMTP	허용
외부	Any	내부뉴스호스트	NNTP	허용
외부	Any	내부NTP호스트	NTP	허용
외부	Any(UDP)	내부DNS호스트	DNS(UDP)	허용
Any	Any	Any	Any	거부

[접근통제 규칙 설정 예]

· 이처럼 IP주소와 서비스 포트(Port)에 대해 접근을 허용할 것인지 거부할 것인지 설정하여 연구기관의 접근통제 정책에 따라 인가되지 않은 접근은 차단할 수 있다.

· 장비의 부하를 분산하고 내부망의 연결 제한을 효율적으로 운영·관리하기 위하여 라우터/스위치와 침입차단시스템의 보안 기능을 적절하게 혼용하여 사용하는 것이 좋다.

③ NAC을 통한 내부망 연결 제한

· 네트워크 접근제어(NAC)는 내부망에 접근하는 접속 단말의 보안성을 강제화할 수 있는 시스템으로 허가되지 않은 사용자나 웜 또는 바이러스, 악성 봇넷에 감염된 장비가 네트워크에 접속하는 것을 원천적으로 차단하여 전체 네트워크를 보호하기 위한 시스템을 말한다.

· 네트워크 접근제어 장비가 지원하는 주요 보안 기능은 다음과 같다.

- 접속제한

  신원이 불분명한 사용자와 네트워크 보안관리 정책을 준수하지 않은 장비에 대하여 내부망 접속을 제한하는 기능이다.

- 접속장비 무결성 검사

  내부망에 접속하고자 하는 단말기가 내부망에에 접근할 수 있도록 허용하기 전에 단말기의 보안상태(최신 보안패치 적용, 악성코드 감염여부, 주요 보안제품 설치여부 등)를 점검하고 필요한 경우 조치를 취하도록 한다.

- 차단/격리

  무결성 검사 결과에 따라 단말기의 내부망 접근을 차단/격리하고 문제를 해결하도록 하는 기능이다. 내부망 전체에 악영향을 미칠 수 있는 단말기가 내부망에 접속

하는 것을 원천적으로 차단하여 내부망의 시스템과 중요한 자료를 보호할 수 있다.

- 사용자 인증
  내부망 접속 사용자의 신원과 역할을 확인한다.

실행지침

1. 내부망의 연결 제한 지침 마련

- 외부의 악의적인 침입 및 불법적인 접근으로부터 내부망을 보호하기 위하여 내부망의 접속을 제한하기 위한 보안정책을 마련하여야 한다.
- 내부망의 연결을 제한하기 위한 보안장비들 간의 효율적인 운영 및 관리 지침을 명시하여야 한다.

2. 내부망의 연결제한 보안장비 운영 관리

- 불법적인 내부망 접근을 차단하기 위하여 라우터/스위치, 침입차단시스템, 네트워크 접근제어시스템의 보안 기능 설정에 대한 적합성과 타당성을 정기적으로 점검하고 관리하여야 한다.
- 보안장비의 네트워크 실시간 트래픽 및 로그정보를 정기적으로 분석하여 침해사실 여부를 모니터링하여야 한다.
- 보안장비를 보호하고 고유 기능을 완벽하게 수행하기 위하여 시스템 관리자 접속 인증을 강화하고 OS패치, 보안패치, 보안규칙(Rule) 패치 등 최신 버전(Version)로 항상 유지하고 관리하여야 한다.

5.9 접근 제한

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.9.2 무선통신망 관리

무선통신망은 유선통신망에 비해 이동성과 편의성이 뛰어나지만 외부로부터 불법적인 도청 또는 침입이 보다 수월하기 때문에 보안 측면에서 상대적으로 취약한 구조를 지니고 있다. 따라서 무선 구간에 대한 보안을 강화하여 연구정보의 기밀성, 가용성, 무결성을 높이기 위한 조치 방안을 마련하고 시행하여야 한다.

내용

- 무선(AIR)구간은 무선전송 방식으로 통신이 이루어지는 구간을 말한다.
- 사용자 인증은 무선랜에서 사용하는 802.1x의 프로토콜에 따라 인증방식이 다르지만 기본적으로 사용자 아이디와 비밀번호를 부여하는 인증방식과 인증서를 이용하여 인증하는 방식이 존재한다.
- 무선랜 스니핑은 무선랜에서 사용하는 802.1x 프로토콜중에서 일부 프로토콜은 기본적으로 통신에서 사용하는 데이터의 암호화를 제공하고 있지 않아 악의적인 목적을 가진 내부 사용자나 외부 사용자가 무선랜 상에 전송되는 데이터를 도청하는 것을 말한다.
- WPA2(Wi-Fi Protected Access)는 무선랜 데이터의 보안성을 제공하기 위해 Wi-Fi Alliance에 의해 정의된 보안 프로토콜이며 IEEE 802.11i 표준을 기반으로 AES 암호 알고리즘을 적용하고 있다. WPA2는 단말을 인증하고 데이터 프라이버시를 제공하는데 사용된다.
- WAP(Wireless Application Protocol)은 사용자가 무선 단말기를 사용해서 인터넷상의 정보를 신속하게 검색, 표시할 수 있는 통신 규약으로 WAP 게이트웨이는 무선망과 인터넷 사이에 설치하여 정보를 전송한다.
- 무선랜 서비스는 최근 이동성과 편의성으로 인하여 급속하게 사용되고 있지만 무선랜 프로토콜 상의 다양한 취약점으로 인하여 특별한 인증절차없이 엑세스포인터(AP)에 접속하여 비인가된 사용자가 주요 네트워크에 접근할 수 상황이 발생할 수 있으므로 다양한 보안기술을 적용하여 보안을 강화하여야 한다.

- 사용자는 항상 인증을 통해서 엑세스 포인터에 접속할 수 있도록 하고 전송되는 데이터의 암호화만 이루어져도 무선랜 구간에서 발생하는 대부분의 해킹을 차단할 수 있으므로 암호화 전송이 가능하도록 구성하여야 한다.
- 등록되지 않은 엑세스포인트의 사용에 대한 점검 등 무선랜 장비에 대한 관리적·기술적·물리적 보안대책 및 정기점검 방안을 마련하여야 한다.

실행지침

1. 무선통신망 보안관리 지침 마련

- 무선통신망의 효율적인 보안 관리 및 운영을 위하여 무선통신망 관리자를 지정·운영하여야 한다.
- 보안상 취약한 무선통신망의 신설 또는 증설은 최대한 자제하고 무선랜은 유선 네트워크 설치가 어려운 장소에 한하여 한시적으로 사용하도록 한다.
- 무선랜 서비스가 보안상 취약한 구간이 될 수 있음을 인지하고 이에 대한 보안방법과 이행절차, 사용자 인증, 무선구간 데이터 암호, 무선랜 장비 관리 등을 명시하여야 한다.

2. 무선통신망 접근제어 및 암호화

- 접근을 제어하는 방법으로는 접근하고자 하는 정보기기 인증방법과 접속하고자 하는 사용자에 대한 사용자 인증방법이 있다.
- 무선 단말기가 엑세스포인트로 접속할 때는 만드시 사용자 인증을 거치도록 하여야 한다.
- 아이디와 비밀번호를 통한 기본 인증외에 접속권한을 가진 사용자의 MAC 주소를 등록하여 지정된 MAC 주소의 랜카드를 장착한 PC에서만 접속할 수 있도록 제한하여야 한다.
- 무선통신망의 특성 상 외부의 침입에 의한 정보유출의 가능성이 높은데 이를 방지하기 위하여 암호화하여 통신해야 한다. 암호화 방식에는 WEP, WPA, WPA2 등이 있는데 최신 버전인 WPA2 방법을 적용하여야 하며 128bit 이상 가능한 최대 크기의 암호키를 사용하도록 하여야 한다.

3. 무선통신망 관리

- 부서 이동, 휴직, 퇴직 등 인사에 변동사항이 발생할 경우에는 관리자는 해당 계정을 회수하거나 차단하여 접속할 수 없도록 조치하고 주기적으로 계정 사용자 목록을 점검하여 부적절하게 사용되는 계정은 없는지 확인해야 한다.
- 일정기간 (예; 3개월) 사용되지 않는 휴면 계정은 접속권한을 해지하여야 한다.
- 무선통신망의 설치 시에는 반드시 정보보안 관리자의 사전승인을 받고 인가된 것만 설치하도록 하며 정보보안 관리자는 인가되지 않은 무선통신 장치 사용 여부를 주기적으로 점검하여야

5.10 네트워크 자료 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.10.1 네트워크 자료 관리

내부 네트워크 관련 자료가 외부로 유출될 경우 불법적으로 내부망에 접속하고자 하는 비인가자는 이를 이용하여 내부망에 쉽게 침입할 수 있다. 따라서 연구기관 내부에 설치된 네트워크 구성 및 장비 등과 관련된 자료가 외부로 유출 또는 공개되지 않도록 특별한 보안대책이 요구된다.

내용

- 외부에 유출되지 않도록 보안조치가 필요한 네트워크 관련 자료는 아래와 같다.
  - 내부 네트워크 장비의 구성도
  - 내부 정보시스템의 네트워크 구성도
  - 내부 네트워크장비와 정보시스템의 IP 주소 현황
  - 내부 네트워크장비와 정보시스템 운영·관리 현황
  - 내부 네트워크장비와 정보시스템의 보안정책 자료 등
- 네트워크 관련 문서의 생성-활용-보관-폐기 등의 보안절차를 수립하고 문서관리자를 별도로 지정하여 외부에 유출되지 않도록 각별히 주의하여야 한다.
- 네트워크 관련 자료가 저장된 정보시스템은 물리적·관리적 보안대책을 마련하여 보호해야 하며 네트워크 관련 자료는 암호화 등을 통해 외부 유출 시에도 안전하게 보호할 수 있는 방안도 마련하여야 한다.

실행지침

1. 네트워크 자료의 보호대책 마련 및 이행

- 네트워크 자료를 관리하는 책임자와 담당자를 지정·운영하여야 한다.
- 네트워크 자료를 대외비로 지정하여 접권권한이 있는 자에 한하여 자료를 수정하거나 삭제, 열람할 수 있도록 조치하여야 한다.
- 네트워크 자료의 보존 형태에 따른 보안대책을 마련하여야 한다.
  - 전자파일 형태로 보존하는 경우에는 인터넷이 연결되지 않은 정보시스템에 자료를 암호화하여 저장하고 보관하여야 한다. 또한 이 정보시스템은 최소한의 인원만 접근 가능하도록 접근권한을 철저하게 통제하여 권한이 있는 자만이 사용할 수 있도록 물리적, 관리적 보호대책을 마련하여야 한다.
  - 문서 형태로 보존하는 경우에는 제한구역 또는 통제구역에 보관하되, 이중 잠금장치가 있는 캐비넷에 보관하여야 한다.

2. 문서열람대장 비치 및 관리

- 네트워크 관련 자료를 열람하는 자는 반드시 문서열람대장에 소속, 성명, 일시 등을 기입하여야 한다.
- 문서열람대장은 네트워크 문서관리자가 관리하여야 한다.

3. 네트워크 자료 폐기

- 네트워크 자료를 폐기하는 경우에는 복구가 불가능하도록 문서파쇄기로 파기하여야 한다.
- 네트워크 자료를 보관하고 있는 정보시스템을 폐기하고자 하는 경우에는 하드디스크를 복구할 수 없도록 물리적 또는 논리적으로 영구 삭제하여야 한다.