POSTECH 사용자 PC 보안가이드

2014년 3월

학술정보처 정보기술지원팀

제•개정 이력

순번	제•개정일	변경내용	발간부서	연락처
1	2014. 03	제정	정보기술지원팀	279-2514
2				
3				

PC 보안관리 가이드

■ 개요

필요성

○ 최근 좀비PC를 통한 DDoS 공격 등 악성코드 감염으로 인한 침해사고 증가
○ 개인정보 탈취 등을 위해 사용자 PC에 대한 공격 증가
○ PC사용자의 중요 정보 및 개인정보 보호를 위해 개인 PC의 보안수준 향상의 보안관리 중요성 대두
○ 사용자 PC의 취약성 분석을 통해 불필요한 서비스를 제거하고 보안사항을 설정하여 내/외부 공격으로 부터 사용자 PC를 최대한 보호할 수 있는 사용자 PC 보안 점검 가이드가 필요

기대 효과

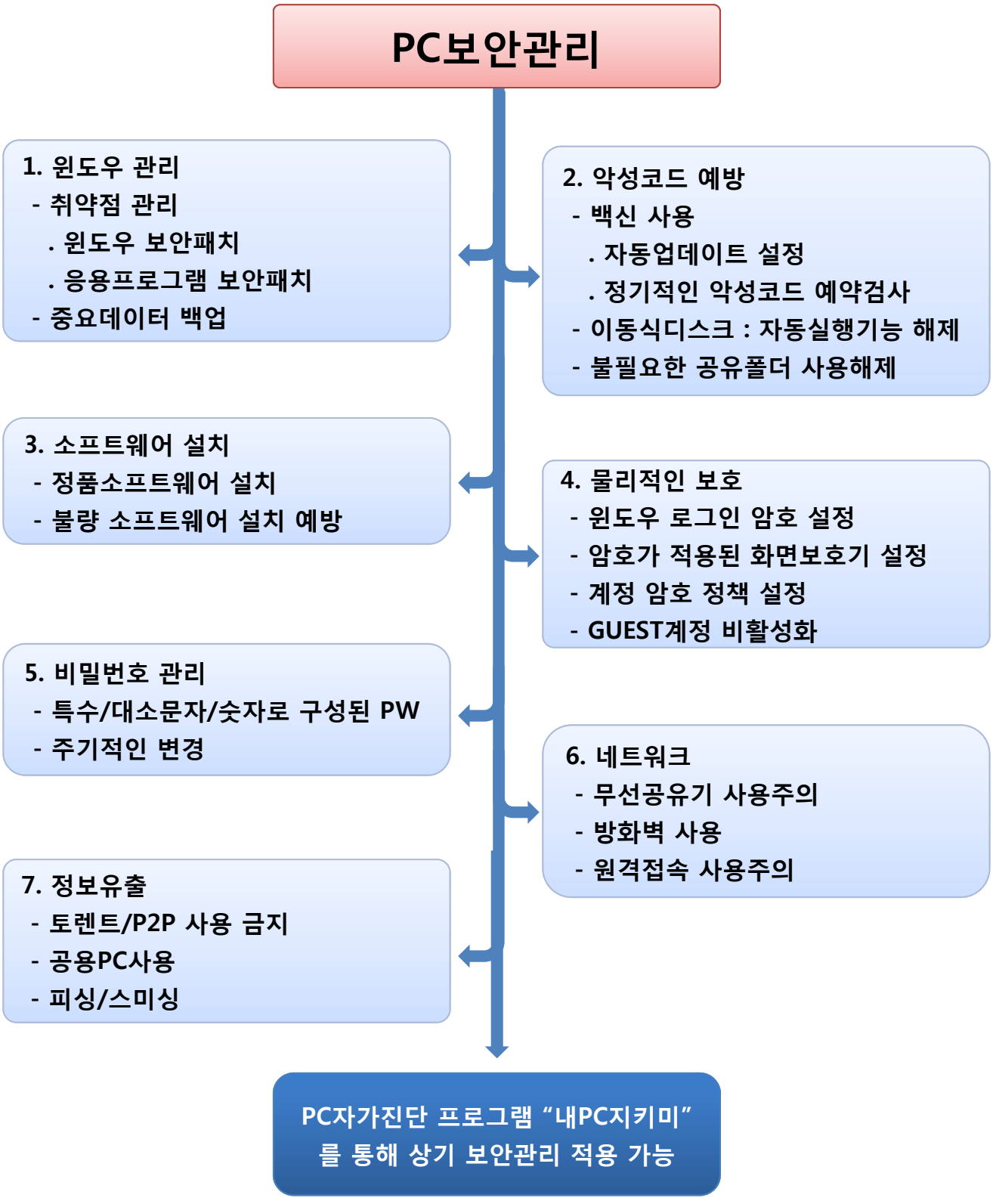
○ 취약점 발견에 대한 즉각적인 대응
○ 사이버 침해 사고 예방
○ 보안 요구사항에 대한 능동적 대처
○ 능동적인 정보보호 활동 수행을 통한 PC의 신뢰성 확보
○ 침해사고 발생 시 체계적인 대응으로 피해 최소화

가이드 제작 환경

○ 본 가이드는 Windows 7 운영체제를 바탕으로 작성되었습니다.

PC 보안관리 가이드

■ PC 보안관리 마인드맵



PC 보안관리 가이드

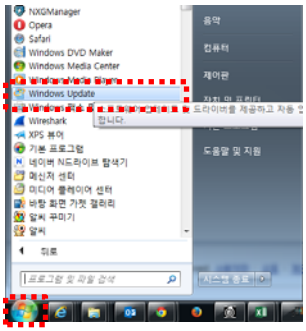
1. 윈도우 관리

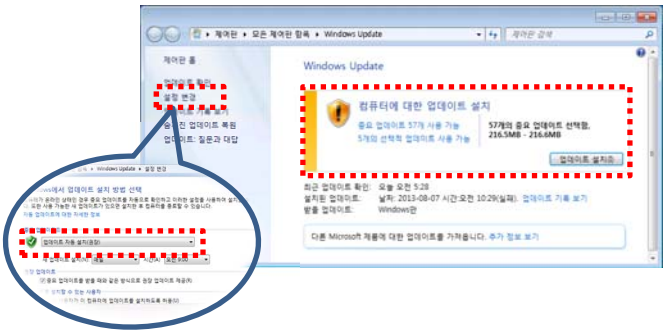
Windows 운영체제 및 MS Office 등의 주요 프로그램들은 알려진 주요 취약점들을 제거하기 위해 주기적으로 보안패치를 제공하고 있다. 따라서, 보안패치를 확인/설치하여 항상 최신보안패치상태를 유지해야 한다.

취약점 관리

○ Windows 운영체제 및 MS Office 보안패치

- 시작 – 모든 프로그램 – Windows Update 클릭하여 업데이트 실시





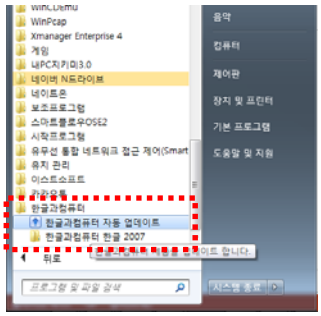
- 보안패치를 자동으로 설치하도록 “업데이트 자동 설치 " 로 반드시 설정

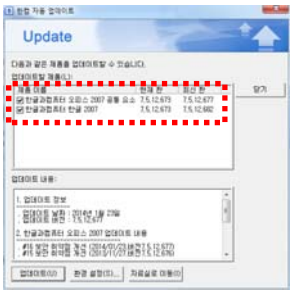
- Internet Explorer는 버전 9이상으로 반드시 업그레이드

> *Windows XP SP3 및 Office 2003에 대한 지원이 2014년 4월 8일 부로 종료됨에 따라 해당 OS 및 프로그램을 사용하는 구성원은 반드시 상위 버전으로 업그레이드해야 함*

○ 한컴 오피스 보안패치

- 시작 – 모든 프로그램 – 한글과컴퓨터 – 한글과컴퓨터 자동 업데이트 클릭





○ JAVA/Adobe 등 보안패치

- 해당 응용프로그램의 업데이트 설정을 자동으로 설정하여 업데이트 실시

중요데이터 백업

○ 중요데이터의 정기적인 백업

○ PC와 별도로 분리된 디스크에 저장

2. 악성코드 예방

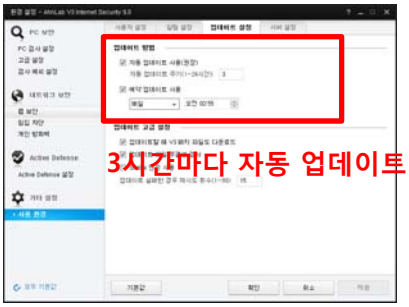
새로운 악성코드 등에 대응하기 위해 백신은 반드시 설치되어야 하며, 정기적인 업데이트 및 점검을 통해 사용자 PC를 보호하여야 한다.

백신 사용

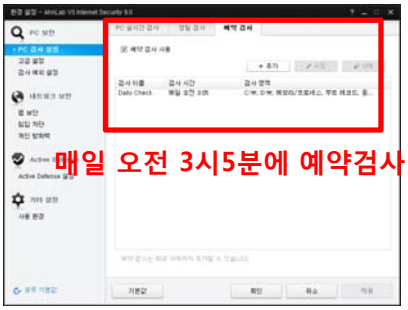
○ 백신프로그램 설치
- 대학 해모수사이트(hemos.postech.ac.kr)의 소프트웨어 배포에서 백신 제공
  . 교내 구성원을 대상으로 V3, 알약 백신 제공

○ 백신프로그램 자동업데이트 설정

○ 백신프로그램 예약검사 설정
- PC사용이 적은 시간에 정밀검사를 예약하여 정기적으로 검사 실시



[AhnLab V3 자동업데이트 설정화면]



[AhnLab V3 예약검사 설정화면]

이동식디스크 자동실행 해제

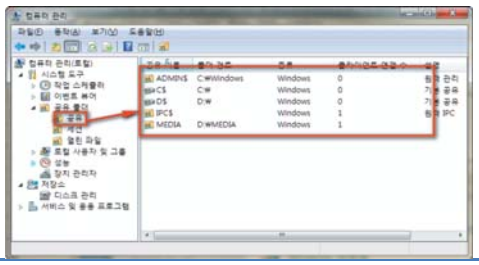
※ 이동식디스크 자동실행 기능으로 사용자 승인 없이 악성코드 자동 실행 가능하여 자동실행 기능을 해제하여야 함

○ 이동식디스크(USB등) 자동실행 해제 방법(Windows 7 기준)
- 시작 – 실행 – regedit 입력하여 레지스트리 편집기 실행
- 레지스트리에서 아래 항목 찾아 클릭
  "HKEY_CURRENT_USER₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩Explorer₩NoDriveTypeAutorun"
- NoDriveTypeAutorun 값을 "0xFF"로 변경하여 모든 유형의 드라이브 비활성화

불필요한 공유폴더 사용해제

※ 공유폴더는 사용자 동의 없이 악성코드를 복사할 수 있으므로 필요하지 않은 공유폴더는 반드시 제거 필요

○ 공유폴더 해제 방법
- "제어판 – 시스템 및 보안 – 관리도구 – 컴퓨터 관리 – 공유폴더 – 공유"에서 불필요한 폴더 제거
- "ADMIN$, C$, D$, IPC$"공유폴더는 관리용 기본 공유 설정됨



3. 소프트웨어 설치

불법 소프트웨어를 사용할 경우 악성코드 감염 및 저작권 위반 등의 위험이 있으므로 반드시 정품 소프트웨어를 사용하여야 한다.

정품소프트웨어 설치

○ 정품소프트웨어 설치

- 대학 해모수사이트(hemos.postech.ac.kr)의 소프트웨어 배포에서 대학 구성원이 사용할 수 있도록 정품소프트웨어 배포 중

[대학 배포 정품 소프트웨어 리스트]

구분	라이선스 보유 소프트웨어	구분	라이선스 보유 소프트웨어
OS	Windows 8 Enterprise 이하 버전	백신	AhnLab V3 Net for Windows Server 7.0 AhnLab V3 Internet Security 8.0 알약
OA	Microsoft Office 2013 이하 버전 한글 2010 이하 버전	Adobe	Photoshop CS 6 Flash Pro CS5.6 Illustrator CS6 Acrobat Professional XI
기타	SAS 9.2(교수 및 학생) Xmanager Enterprise 3.0 등 AlTools(알집, 알씨, 알드라이브(구 알FTP), 알송, 알툴바, 알캡쳐, 알쇼, 알약)		

※ Microsoft사의 라이선스 정책에 따라 사용 가능 SW 및 OS가 다를 수 있습니다.

불법/불량 소프트웨어 설치 예방

○ 불법소프트웨어 설치 금지

- 라이선스 구매 없이 또는 라이선스 정책에 위반되는 사용으로 소프트웨어 저작권 침해 발생
- 저작권 침해로 사용자 뿐만 아니라 대학에도 피해보상비용 발생(저작권법 제141조 양벌규정)

[소프트웨어 라이선스 정책 위반 사례]

- 개인 사용자에게만 무료로 배포하는 소프트웨어를 대학 소유의 PC 또는 개인 소유의 PC에 설치하여 연구/업무용으로 사용할 경우 모두 라이선스 사용권 위반

→ 개인 사용자용 무료 소프트웨어는 대학에서 절대 사용 금지

○ 불량소프트웨어 설치 예방

- 공식사이트에서 다운로드
- 설치전에 사용자들의 평판이나 인지도를 확인
- 사용하지 않거나 출처/용도가 불분명한 프로그램은 삭제
- 같이 설치되는 제휴프로그램 확인하기
- 가짜 백신 주의

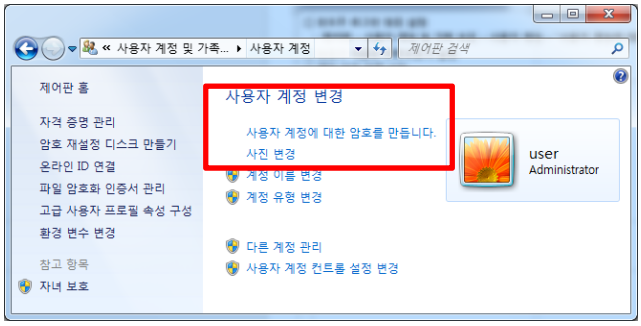
4. 물리적인 보호

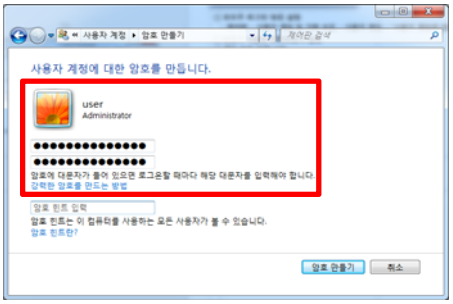
본인의 PC에 다른 비인가 사용자가 접근하지 못하도록 물리적인 보호를 통해 PC에 저장되어 있는 중요 데이터를 보호하여야 한다.

윈도우 로그인 암호 설정

○ 윈도우 로그인 암호 설정

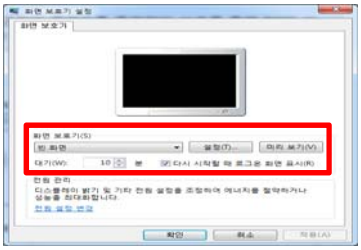
- 제어판 – 사용자 계정 및 가족 보호 – 사용자 계정 – "사용자 계정에 대한 암호를 만듭니다." 클릭





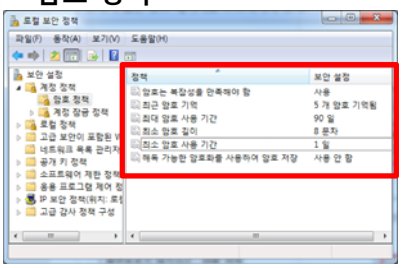
○ 암호가 적용된 화면보호기 설정

- 제어판 – 모양 및 개인 설정 – 개인설정 - 화면보호기 변경
  - 화면보호기 사용 여부 : 사용
  - 화면보호기 대기시간 : 10분 이하
  - 암호 보호 사용 여부 : 다시 시작할 때 로그온 화면 표시 체크



○ 계정 암호 정책 설정

- 제어판 – 시스템 및 보안 – 관리도구 – 로컬 보안 정책 – 계정 정책 – 암호 정책
  - 암호는 복잡성을 만족해야 함 : 사용
  - 최근 암호 기억 : 사용자 선택(0~24)
  - 최대 암호 사용 기간 : 90일
  - 최소 암호 길이 : 8자리
  - 최소 암호 사용 기간 : 1일
  - 해독 가능한 암호화를 사용하여 암호 저장 : 사용 안함

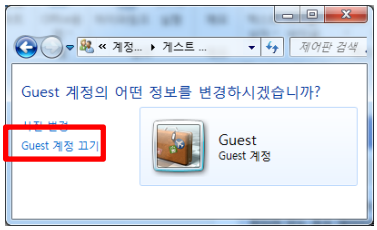


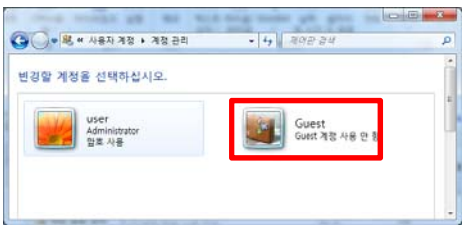
GUEST계정 비활성화

※ Windows에서 기본적으로 생성되는 Guest계정의 경우 관리소홀로 인해 보안취약점을 노출 할 수 있으므로 사용을 중지해야 한다.

○ GUEST계정 비활성화

- 제어판 – 사용자 계정 및 가족 보호 – 사용자 계정 – 다른 계정관리에서 GUEST계정 선택 – Guest 계정 끄기





5. 비밀번호 관리

사용자 계정 암호를 보안권고수준에 적합하게 설정하여 사용하는 것은 암호해독을 어렵게 하는 효과가 있어 시스템의 보안수준 향상에 기여한다.

비밀번호 구성

○ 권고 비밀번호

- 숫자, 대소문자, 특수문자 조합으로 최소 9자리 이상으로 설정

※ 최근 컴퓨팅 성능의 비약적인 향상으로 인하여 비밀번호를 크래킹하는 시간이 상당히 단축되고 있으며 이를 예방하기 위해서는 최소 9자리 이상으로 설정하여야 함.

※ 웹사이트 https://howsecureismypassword.net에서 비밀번호 길이 및 복잡도에 따른 크래킹 시간을 확인할 수 있으니 참고하지 바랍니다.

특수문자+대소문자+숫자 조합으로 9자리 생성시 크래킹에 1년 정도 걸림

[패스워드 길이와 크래킹 시간의 관계]

길이	패스워드 개수	크래킹 시간
4	14776336	2 초
5	916132832	2 분 30 초
6	56800235584	2 시간 30 분
7	3521614606208	1 주
8	218340105584896	1 년
9	13537086546263552	70 년

[다양한 문자 조합과 크래킹 시간의 관계]

패스워드 형식	문자 수	패스워드 개수	크래킹 시간
7-bit ASCII	128	72057594037927936	350 년
출력할 수 있는 문자열	95	6634204312890625	30 년
문자와 숫자 조합	62	218340105584896	1 년
문자	52	53459728531456	96 일
한 개의 대문자와 소문자	26/special	1670616516608	3 일
소문자	26	208827064576	9 시간
영어 단어 : 8 글자 또는 그 이상	Special	250000	1 초 이내

6. 네트워크(1/2)

무선공유기 사용 시 보안기능 사용 및 개인 PC의 방화벽 사용 그리고 원격접속에 대한 보안 설정을 통해 네트워크를 통한 보안위협을 최소화하여야 한다.

무선공유기 사용주의

○ 무선공유기 보안기능 설정하기
- 무선공유기 사용 시 암호화/인증 등 보안기능을 설정하지 않으면 외부인이 무단으로 무선랜을 사용할 수 있으며, 이러한 경우 이터넷 속도 저하 및 개인정보 유출 등 해킹 사고가 발생할 수 있음
- 암호설정 : WPA2, 암호알고리즘 : AES 선택

○ 무선공유기 패스워드 안전하게 관리하기
- 무선공유기에 관리자 권한으로 접근 시 패스워드를 통해 접근통제하여야 함

○ 제공자가 불분명한 무선랜 이용하지 않기

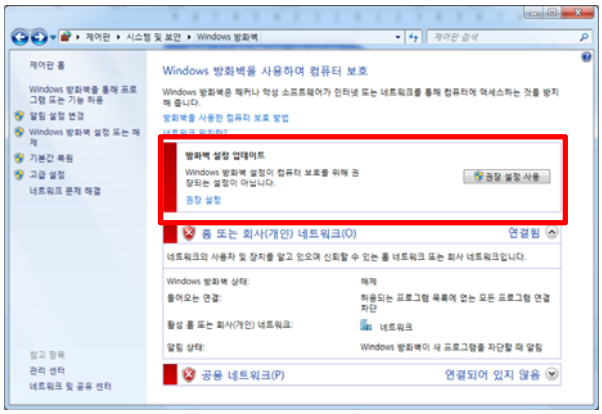
○ 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기

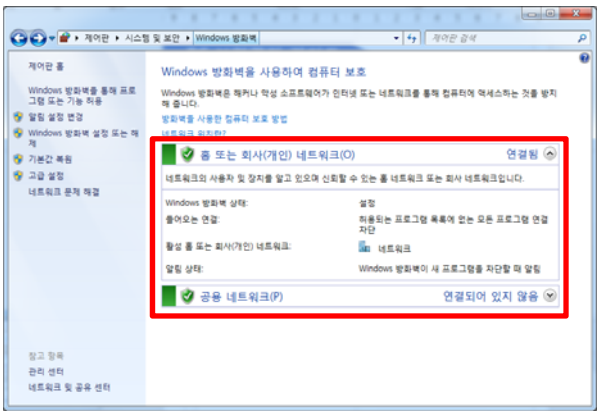
○ 무선공유기의 SSID를 변경하고 숨김 기능 설정하기

※ 보다 상세한 무선공유기 보안설정은 한국인터넷진흥원 “알기쉬운 무선랜 보안 안내서” 참고
URL : http://www.kisa.or.kr/public/laws/laws3.jsp 다운로드

방화벽 사용

○ 사용자 PC의 방화벽 사용 설정
- 방화벽은 시스템으로 시도되는 접근을 통제하여 악의적인 접근을 사전에 차단할 가능
- 제어판 – 시스템 및 보안 – Windows 방화벽 – 권장 설정 사용





6. 네트워크(2/2)

무선공유기 사용 시 보안기능 사용 및 개인 PC의 방화벽 사용 그리고 원격접속에 대한 보안 설정을 통해 네트워크를 통한 보안위협을 최소화하여야 한다.

원격접속 사용주의

○ "원격데스크탑 연결"은 Well-Known Port(3389포트) 사용으로 인해 외부에서 지속적으로 공격을 시도하고 있어 이를 사용하기 위해서는 보안설정이 반드시 필요

○ 원격데스크탑 연결 보안설정

1. 일반사용자 계정으로 연결
   관리자 계정(administrator)으로 원격데스크탑을 접속할 경우 관리자 계정이 공격 당해 노출되면 PC의 모든 권한을 공격자가 획득할 수 있으므로 일반사용자 계정이나 사용자계정을 제한하여 사용할 필요가 있다.
2. 계정 잠금 정책 설정
   원격데스크탑 해킹 도구는 알려진 계정(administrator, user 등)의 비밀번호를 무작위 공격(Brute-force Attack)하므로 접속 시도 횟수에 제한을 걸어 일정 횟수 이상 로그온 실패할 경우 계정을 잠금으로써 무작위강제공격을 예방할 수 있다.
   ※ 제어판-시스템 및 보안-관리도구-로컬보안정책-계정정책-계정잠금정책에서 계정 잠금 임계값 설정
3. 원격데스크탑 접속 포트 변경
   원격데스크탑 서비스는 잘 알려진 3389포트를 사용하고 있으므로 사용자가 임의의 포트로 변경하여 사용할 경우 공격자가 서비스 포트를 유추할 수 없어 위험성을 줄일 수 있다.
   ※ 시작-실행-regedit 입력 후 확인
   KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩TerminalServer₩WinStations₩RDP-Tcp₩PortNumber 에서 포트 번호 변경
4. 접속 가능한 IP주소의 제한
   윈도우 방화벽에서 원격데스크탑을 통하여 접속할 수 있는 IP를 제한하여 인가되지 않은 IP에서의 접근을 차단하여 해킹 시도를 막을 수 있다.
   ※ 제어판-Windows 방화벽-예외탭-원격데스크톱 편집-범위 변경-사용자 지정 목록 선택한 후 허용 IP 설정
5. 주기적인 접속 로그 확인
   윈도우 접속로그는 실패한 접속 시도나 계정잠금 정보를 저장하고 있으므로 주기적으로 접속 로그를 확인하여 공격 시도에 대응할 수 있다.
   ※ 제어판-관리도구-로컬보안정책-로컬정책-감사정책-계정 로그온 이벤트 감사에서 성공, 실패 설정
   제어판-관리도구-이벤트 뷰어-보안 항목에서 로그정보 확인

7. 정보유출

사용자 부주의로 인해 PC내 중요데이터 및 개인정보가 노출될 수 있으므로 해당 서비스를 사용하지 않거나 각별히 주의하여 정보가 유출 되지 않도록 한다.

P2P 사용금지

○ P2P사용 시 중요 개인정보 또는 PC내 중요데이터를 공유설정하여 정보가 유출될 수 있음
○ 저작권 관련 파일을 불법 다운로드 시 저작권법 위반으로 인한 법적 처벌의 위험 존재
○ 토렌트/P2P 프로그램은 절대 사용 금지

공용PC사용 주의

○ 공용PC사용 전 악성코드 검사하기
○ PW등 중요 정보 입력이나 유출에 주의
○ 인터넷뱅킹 사용 주의
○ 자동 로그인 옵션 끄기
○ 웹사이트 사용 후 로그아웃

피싱/스미싱 주의

○ 스팸메일을 통한 사용자 계정정보 요구시 절대 회신 금지
- 대학은 구성원 HEMOS계정에 대해 메일을 통해 절대 계정정보를 요구하지 않습니다.
○ 단축 URL을 통한 접속 요구 시 절대 주의 필요
- 단축 URL의 경우 원본주소에 대한 정보를 확인할 수 없기 때문에 악성코드 유포에 악용되고 있음
○ 문자(SMS)메시지 내에 인터넷으로 연결되는 주소는 절대 누르지 말것

PC 보안관리 가이드

■ 내PC지키미 실행

내PC지키미는 Windows XP, Vista, 7 사용자 PC의 보안상태를 점검/개선하기 위한 개인용 PC 보안점검 프로그램으로, 앞서 설명한 PC보안관리를 한번에 할 수 있어 간단히 개인 PC의 보안수준을 향상 시킬 수 있다.

내PC지키미 설치

○ 내PC지키미 다운로드

- 해모수사이트(hemos.postech.ac.kr) 메인페이지에서 우측 하단의 사이버 보안 진단의 날 배너 클릭(링크)
- 매월 세번째 수요일 "사이버보안 진단의 날"에 POVIS사이트에서 팝업으로 안내 및 다운로드 가능

내PC지키미 실행/조치

○ 내PC지키미는 아래 10가지 항목에 대해 취약점 점검 및 조치 가능

항목 1	바이러스 백신이 설치되어 실행되고 있는가?
항목 2	바이러스 백신의 최신 보안 패치가 적용되어 있는가?
항목 3	운영체제, MS Office의 최신 보안패치가 설치되어 있는가?
항목 4	한글프로그램의 최신 보안 패치가 적용되어 있는가?
항목 5	Windows 로그인 패스워드가 8자리 이상으로 안전하게 구성되어 있는가?
항목 6	Windows 로그인 패스워드를 분기 1회 이상 변경하여 사용하고 있는가?
항목 7	화면보호기가 활성화되어 있으며 대기시간은 10분 이내로 설정되어 있는가?
항목 8	불필요한 사용자 공유 폴더가 설정되어 있는가?
항목 9	USB의 자동 실행이 허용되어 있지 않는가?
항목 10	미사용(3개월) ActiveX 프로그램이 존재하지 않는가?

※ 대학에서 발생하는 악성코드 감염 등의 침해사고 중 약 50%는 내PC지키미를 통한 정기적인 PC점검으로 예방 가능 함