<9장>

02.다음 중 SNS 보안 위협에 해당되지 않는 것은 무엇인가?

1. 사이버 폭력
2. 피싱
3. SYN Flooding 공격
4. 악성 소프트웨어

03.소셜 네트워크에서 악의적인 사용자가 지인 또는 특정 유명인으로 가장하여 활동하는 공격기법은 무엇인가?

1. 악성 소프트웨어
2. 피싱
3. 이블 트윈 어택
4. 사이버 폭력

<10장>

03.다음 중 가장 취약한 사용자 인증 방식은 무엇인가?

1. 공인인증서
2. 생체 인증
3. 패스워드
4. 생각 인식

05.생체 인증 성능의 측정 기준 중에서 인증 권한이 없는 사람이 인증을 시도했을 때 성공하는 비율을 나타내는 것은 무엇인가?

1. EER
2. CER
3. FAR
4. FRR

06.접근 통제 모델 중에서 사람이 아닌 직책에 따라 권한을 부여하는 모델은 무엇인가?

1. HAC
2. MAC
3. RBAC
4. DAC

07.다음 중 관리적 접근 통제에 포함되지 않는 것은 무엇인가?

1. 직무 분리
2. 감독 구조
3. 보안 인식 훈련
4. 인터페이스 통제

08.입력 값 검증 코드 구현 방법에 대한 설명으로 바른 것은 무엇인가?

1. 알려진 악성 패턴에 한해서만 필터링을 하는 것은 화이트 리스트 방식 필터링이다.
2. 필요한 특정 입력 값만 받아들이고 그 외의 모든 값을 필터링을 하는 것은 블랙리스트 방식 필터링이다.
3. 웹 애플리케이션에서는 화이트리스트 필터링 방식보다 블랙리스트 필터링 방식을 선호한다.
4. 웹 애플리케이션에서 사용자 입력 값 검증 코드는 반드시 서버 측 프로그래밍 언어 내에 구현한다.

<11장>

01.IIS7을 설치했을 때 Default Web Site가 운영되고 있는 경우 기본적으로 설치되는 파일은 무엇인가?

1. Default.htm
2. Index.htm
3. Default.asp
4. Iissrart.htm

03. 다음 중 IIS에서 사용하는 로그 형식이 아닌 것은 무엇인가?

1. Microsoft IIS 로그 파일 형식
2. W3C 확장 로그 파일 형식
3. NCSA 공통 로그 파일 형식
4. HTTP 공통 로그 파일 방식

<12장>

02.다음 중 기업의 IT 보안 팀에서 수행하는 업무가 아닌 것은 무엇인가?

1. 정보보안 기획
2. 정보보안 관리
3. 정보보안 운영
4. 물리적 보안

03.방화벽과 침임 탐지 시스템의 기능을 조합한 솔루션은 무엇인가?

1. DRM
2. IPS
3. WebMail
4. SIEM

<13장>

02.아이폰에서 애플의 통제를 벗어나 임의의 소프트웨어를 설치할 수 있도록 만드는 것은 무엇인가?

1. 탈옥
2. 루팅
3. Security Off
4. Unpacking

03.안드로이드 운영체제를 사용하는 스마트폰에서 시스템 잠금장치를 해체하여 운영체제 관리자 권한을 얻는 것은 무엇인가?

1. 탈옥
2. 루팅
3. Security Off
4. Unpacking

04.안드로이드 앱 패키지 파일의 확장자는 무엇인가?

1. exe
2. jar
3. apk
4. bat
5. 접근 통제를 구현하는 세 가지 방법에 대해 설명하시오

접근 통제를 구현하는 방법에는 관리적 접근 통제, 논리적 접근 통제, 물리적 접근 통제로 총 세가지가 존재합니다.

첫번째로 관리적 접근 통제는 보안 정책을 구성하고 절차와 지침을 개발하는 것이 포함되어야 한다. 또한 정책과 지침 내에 어떤 통제가 사용되어야 하는지를 결정해야한다. 관리적 접근 통제는 크게 두 가지로 구분할 수 있다. 첫 번째는 정책 및 절차를 수립하여 조작에서 보유하고 있는 중요 정보가 무엇인지를 식별하고 그에 따른 통제 방안을 수립하는 것이다. 두 번째는 내부 임직원들이 회사의 보안 정책을 준수하도록 하기 위한 직원 통제활동이다. 직원 통제 활동에는 직무분리, 직무교대, 감독 구조, 보안 인식 훈련 등이 있다.

논리적 접근통제는 논리적 접근 통제는 기술적 통제라고도 불리며, 보호해야 할 정보에 접근하는 것을 제한하기위해 사용하는 하드웨어와 소프트웨어 도구를 말한다. 가장 많이 사용하는 논리적 접근 통제는 IP 주소 또는 MAC 주소에 따른 접근통제이다. 특정 애플리케이션에 접근할 수 있는 사요 자의 IP 주소 외에 다른 주소는 접근을 차단하는 방법이 이에 해당한다. 무선 AP의 경우에는 무선 노트북의 MAC 주소에 기반을 두고 인증된 장치 외에는 아예 접근하지 못하도록 하는 방법도 있다.

또 다른 논리적 접근 통제 방법으로 인터페이스 통제가 있는데, 이는 필요한 기능만 사용할 수 있도록 메뉴나 셸의 형태로 인터페이스를 제공하는 것을 말한다. 가장 쉬운 예는 은행의 현금지급기이다. 현금지급기는 입금, 출금', '통장 정리 등의 간단한 기능을 하는 버튼 몇 개 외에는 조작할 수 있는 메뉴가 없다. 따라서 이용자는 주어진 메뉴 외의 다른 조작이 불가능하다.

물리적 접근 통제는 물리적 접근 통제의 대표적인 활동으로는 네트워크 분리(망 분리), 경계선 보안, 전산실 동세, 데이터 백업 등이 있다. 네트워크 분리(망 분리)는 특정 네트워크를 물리적으로 다른 네트워크와 분리하는 것을 말한다. 민감하고 중요한 네트워크를 사용하는 기업이나 외부 해킹의 기업이나 외부 해킹의 위힘이 큰 기업에서는 물리 보안은 네트워크를 분리해서 사용하는 경우가 있다. 그리고 경계선 제한 구역이나 통제 구역에 들어갈 때 신원을 확인하는 것을 말한다. 물리적 통제의 다른 예로는 스위치나 라우터의 설치 장소를 들 수 있다. 대부분의 장소에서 네트워크 IP나 PC에 대한 통제를 하는데 스위치나 라우터 장비는 그대로 노출시키는 경우가 많다.이런 경우 임의의 라인을 꽂아 해킹에 이용할 수 있으므로 네트워크 장비에 임의로 접근할 수 없도록 잠금장치 등을 설치해놓아야 한다.

1. 아파치 웹 서버의 보안 설정 항목을 쓰시오.

아파치 각각 httpd, passwd, httpd.conf 디렉토리에서 설치된 것을 확인할 수 있으며 모든 소유자는 root로 되어있고, httpd는 root 그룹이며 나머지는 noboby그룹에 해당됩니다. 각각의 접근권한은 httpd는 511, passwd와 httpd.conf는 640의 접근권한을 가지고 있습니다. 아파치 웹 서버 보안설정에는 서버 이름과 IP 포트설정, 서버 실행 계정과 그룹설정, 웹 페이지 디렉토리 설정, 기본 문서 설정, 디렉토리 리스팅 설정, FollowSymLinks 설정, 접근 제어의 확인과 설정, ServerSignature 설정이 있습니다.

서버 이름과 IP 포트설정은 특정 IP와 포트, 서버 이름을 통해서만 접속할 수 있도록 설정하는 기능입니다.

서버 실행 계정과 그룹설정은 아파치 웹 서버는 noboby계정을 아파치 웹 프로세스의 권한으로 할당합니다. Guest 계정과 비슷한 권하능 가진 nobody계정은 로그인도 허용되지않습니다. 페도라 17에 설치된 아파치느 nobody라는 이름 대신 apache라는 별도의 계정을 nobody 권한으로 만들어 아파치 웹 프로세스에 대한 권한으로 할당합니다.

웹 페이지 디렉토리 설정은 웹 페이지 디렉토리는 공격자가 추측하기 어려운 경로로 만들거나 중요한 디렉토리에는 접근할 수 없도록 제한된 하위 디렉토리로 지정해야합니다.

기본 문서 설정은 디렉토리 인덱스 값을 이용하여 실제 사용하는 파일이 가장 높은 우선순위가 되도록 설정해야합니다. 기본설정은 index.htm이 가장 높은 우선순위로 되어있습니다.

디렉토리 리스팅 설정은 디렉토리안에 있는 모든 파일 목록이 노출될 수 있으므로 디렉토리의 option 에 indexes가 설정되어 있다면 삭제해야합니다.

FollowSymLinks 설정은 FollowSymLinks를 설정하면 그 디렉토리 안에 있는 심벌릭 링크를 따라갈 수 있으므로 사용하지 않는 것이 좋습니다.

접근 제어의 확인과 설정은 아파치도 IIS처럼 접근하는 클라이언트의 이름이나 IP주소등을 이용한 접근제어가 가능합니다. 또한 아파치에는 웹 페이지가 저장된 디렉토리별로도 접근 제거가 가능합니다.

ServerSignature 설정은 serversignature 설정을 통해 외부에서 아파치 서버의 버전과 운영체제 종류를 알아내지 못하도록 할 수 있습니다.

1. 보안 조직의 일반적인 정보보안 업무는 정보보안 기획, 정보보안 관리, 정보보안 운영, 정보보안 모니터링 등이다. 각각의 수행 업무는 무엇인지 설명하시오.

정보보안 기획의 업무는 정보보안 전략 및 계획 수립, 정보보안 정책 및 지침, 표준 제정 및 관리 업무가 있습니다.전사 경영 IT 전략 및 위험 평가 분석, 동향 등과 연계된 단기/중 장기 정보보안 전략 수립, 정보보안 동향 및 타사 현황 상시 파악, 보안 신기술 정보를 업데이트하여 향후 전략 및 사업계획 수립에 반영, 시스템 개발 또는 보안 장비 도입 시 보안 기술을 검토하고 그 적정성을 평가 및 검토한 결과를 협의하여 최종 결정, 정보보안 투자 평가 기준에 따라 기술 검토와 예산, 효과 등을 평가하여 투자 우선순위를 결정하고 업문의서를 작성하여 사업 진행, 정책, 규정/지침 변경에 대한 환경 요인과 요구 사항을 검토 및 개정하여 ISMS의 최신성 및 보안 인증을 유지하기 위한 활동 수행하는 업무가 있습니다.

정보보안 기획에는 정보보안 위험 관리를 수행하는데 이 업무는 정보 자산 관리 기준에 따라 자산을 식별 · 분류하여 목록을 작성하고, 관리하기 위한 목록과 실제 운영 목록을 주기적으로 확인하여 일치시키는 활동 수행. 정보 자산 운영 관리를 위해 정보 자산 반출 등 운영상의 변경에 따라 정보 자산 현황을 최신으로 관리하며 시스템 구축 및 보안 장비 도입 업무는 시스템 신규 개발 시 통합 구매를 통해 업체를 선정하고 보안성 심의를 통과한 시스템을 테스트 및 검수한 후 구축에 필요한 보안 적용, 구축 완료 후 설계에 반영된 보안 대책이 적용되었는지 여부를 점검하고, 조치가 필요한 경우 적절한 조치를 취한 후 테스트 결과 보고, 보안 장비 도입 시 보안 정책 적용이 잘되었는지 여부 확인, 개발 전에 시큐어 코딩에 대한 가이드를 제공하고 교육 실시, 개발 이후 설계에 반영된 보안 대책대로 구현되었는지 점검하고 시큐어 코딩 가이드를 기반으로 코딩이 수행되었는지 확인하는 업무가 있습니다.

정보보안 운영 업무는 인프라 보안 운영 및 보안 장비 운영, 위협 및 취약성 관리 업무가 있습니다. 각 업무에서는 모니터링 장치를 이용하여 정보보안 관련 시스템의 상태를 정기적으로 모니터링하고, 정보 보안 관제에서 모니터링 업무를 수행할 수 있도록 정보보호 시스템에 대한 유지보수 등의 운영 관리 활동 수행, 서버 네트워크 DB 보안 운영 업무 수행, 데이터, 애플리케이션, 시스템, 네트워크를 보호하는 데 필요한 프로세스, 기술, 서비스의 취약한 부분을 관리하기 위한 활동으로, 보안 취약성 진단 대상을 선정하고 진단 • 발생 가능한 보안 위협해에 대한 시나리오와 Baseline 방식으로 모의 해킹을 수행하여 발견한 취약점에 대한 보호 대책 제시를 수행합니다.

정보보안 모니터링정보보안 성과 모니터링 및 성과 관리 정보보안 내부 감사 업무가 있습니다. 각 업무에서는 정보보안 업무를 부여 받은 자가 규정/정책대로 활동을 모두 수행했는지 체크리스트를 통해 활동 내역을 평가하고 그 결과를 임원에게 보고한 후 받은 지시 사항을 정리하여 정보 보호 계획 수립 및 정보보안 정책 지침에 반영 · 주기적으로 정보보안 시스템 운영 현황과 변경/조치가 있는 건에 대한 분석 및 대응 결과를 보고하고 임원의 지시 사항을 정리하여 정보보호 계획 수립 및 정보보안 정책/지침에 반영,주기적으로 정보보안 시스템 운영 현황과 변경/조치가 있는 건에 대한 분석 및 대응결과를 보고하고 임원의 지시 사항을 정리하여 정보보호 계획 수립 및 정보보안 정책/지침에 반영, 기업 내부 감사 인력에 의해 이루어지는 경영 활동의 일환으로 계획 수립, 실사 리포트 모니터링 등 네 단계로 이루어진 감사 활동에 참여 등이 있습니다.