2014 년 지방직 9 급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
③	④	④	③	③	②	②	③	①	③
11	12	13	14	15	16	17	18	19	20
①	③	②	④	②	①	②	①	①	④

문 1. 정보보호의 주요 목표 중 하나인 인증성 (Authenticity)을 보장하는 사례를 설명한 것으로 옳은 것은?

- ① 대학에서 개별 학생들의 성적이나 주민등록번호 등 민감한 정보는 안전하게 보호되어야 한다. 따라서 이러한 정보는 인가된 사람에게만 공개되어야 한다.
- ② 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근 권한이 있는 의사가 이용하고자 할 때 그 정보가 정확 하며 오류 및 변조가 없었음이 보장 되어야 한다.
- ③ 네트워크를 통해 데이터를 전송할 때는 데이터를 송신한 측이 정당한 송신자가 아닌 경우 수신자가 이 사실을 확인할 수 있어야 한다.
- ④ 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 접근할 수 있어야 한다.

답 ③

③ 인증은 상대방이 진짜인지 아닌지(정당한 송신자인지) 확인하는 것이다.

<오답 체크> ① 인가된 사람에게만 공개되어야 한다는 것은, 아무나 보지 못한다는 것이므로 기밀성(Confidentiality)

② 정보가 정확하고 함부로 바뀌지 않아야 한다는 것은 무결성(Integrity)

④ 올바른 사용자가 안정하게 정보에 접근하고 이용할 수 있어야 한다는 것은 가용성(Availability)

허가받은 정보에만 접근할 수 있다는 표현이라면 인가(Authorization)이나 접근 통제가 될 수 있지만, '안정적으로 접근할 수 있어야 한다'는 것은 가용성을 말한다.

문 2. 시스템 계정 관리에서 보안성이 가장 좋은 패스워드 구성은?

- ① flowerabc
- ② P1234567#
- ③ flower777
- ④ Fl66ower\$

답 ④

④ 영어 대문자, 소문자, 숫자, 특수문자까지 4 종류의 문자열을 사용한 ④번이 가장 보안성이 뛰어나다.

♣ 스터디 플러스

『개인정보의 기술적·관리적 보호조치 기준』

제 4 조(접근통제) ⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운영하여야 한다.

- 1. 영문, 숫자, 특수문자 중 2 종류 이상을 조합하여 최소 10 자리 이상 또는 3 종류 이상을 조합하여 최소 8 자리 이상의 길이로 구성

문 5. 보안 공격 중 적극적 보안 공격의 종류가 아닌 것은?

- ① 신분위장(masquerade): 하나의 실체가 다른 실체로 행세를 한다.
- ② 재전송(replay): 데이터를 획득하여 비인가된 효과를 얻기 위하여 재전송한다.
- ③ 메시지 내용 공개(release of message contents): 전화통화, 전자우편 메시지, 전송 파일 등에 기밀 정보가 포함되어 있으므로 공격자가 전송 내용을 탐지하지 못하도록 예방해야 한다.
- ④ 서비스 거부(denial of service): 통신 설비가 정상적으로 사용 및 관리되지 못하게 방해한다.

답 ③

- ③ 메시지 내용 공개는 기존 정보의 흐름은 방해하지 않는 소극적 공격에 해당한다.

소극적 공격

도청(가로채기, interception), 트래픽 분석, 메시지 내용 공개 등

적극적 공격

차단(interruption), 변조, 위조, 신분 위장, 서비스 거부 공격(Dos), 재전송 공격 등

문 6. 피싱(Phishing)에 대한 설명으로 옳지 않은 것은?

- ① Private Data 와 Fishing 의 합성어로서 유명 기관을 사칭하거나 개인 정보 및 금융 정보를 불법적으로 수집하여 금전적인 이익을 노리는 사기 수법이다.
- ② Wi-Fi 무선 네트워크에서 위장 AP 를 이용하여 중간에 사용자의 정보를 가로채 사용자인 것처럼 속이는 수법이다.
- ③ 일반적으로 이메일을 사용하여 이루어지는 수법이다.
- ④ 방문한 사이트를 진짜 사이트로 착각하게 하여 아이디와 패스워드 등의 개인정보를 노출하게 하는 수법이다.

답 ②

피싱(phishing)은 인터넷 사용자에게 가짜 도메인을 알려주어, 가짜 사이트로 접속을 유도하는 공격이다. 진짜 사이트와 유사한 도메인의 가짜 사이트를 만들어 놓은 뒤, 이메일 등을 통해 가짜 사이트로 접속하도록 유인하여 개인정보 유출이나 계좌 이차나 요금 결제 등의 피해를 야기한다.

- ② WiFi Rogue Access Points(**Rogue AP**, 위장 AP)에 대한 설명이다. 해커가 악의적인 목적을 가지고 정상적인 AP 인 척 설치한 불법 액세스 포인트로, 사용자가 인터넷을 이용할 때 중간에서 사용자의 정보를 엿보고 가로챈다.

문 13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 정보통신서비스 제공자의 정보보호 최고책임자가 총괄하는 업무에 해당하지 않는 것은? (단, 이 법에 명시된 것으로 한정함)

- ① 정보보호관리체계 수립 및 관리·운영
- ② 주요정보통신기반시설의 지정
- ③ 정보보호 취약점 분석·평가 및 개선
- ④ 정보보호 사전 보안성 검토

답 ②

② 「정보통신기반 보호법」의 내용이다.

「정보통신기반 보호법」 제 8 조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설 중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제 45 조의 3(정보보호 최고책임자의 지정 등)

- ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다.
- ② 제 1 항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.
- ③ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.
 - 1. 정보보호관리체계의 수립 및 관리·운영
 - 2. 정보보호 취약점 분석·평가 및 개선
 - 3. 침해사건의 예방 및 대응
 - 4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
 - 5. 정보보호 사전 보안성 검토
 - 6. 중요 정보의 암호화 및 보안서버 적합성 검토
 - 7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행
- ④ 정보통신서비스 제공자는 침해사건에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제 1 항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.
- ⑤ 정부는 제 4 항에 따른 정보보호 최고책임자 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.

문 14. 「개인정보 보호법」상 자신의 개인정보 처리와 관련한 정보주체의 권리에 대한 설명으로 옳지 않은 것은?

- ① 개인정보의 처리에 관한 정보를 제공받을 수 있다.
- ② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 수 있다.
- ③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 수 있다.
- ④ 개인정보에 대하여 열람을 할 수 있으나, 사본의 발급은 요구할 수 없다.

답 ④

④ 열람 및 사본의 발급을 요구할 수 있다.

「개인정보 보호법」 제 4 조(정보주체의 권리)

정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

- 1. 개인정보의 처리에 관한 정보를 제공받을 권리 ---> ①
- 2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리 ---> ②
- 3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람 (사본의 발급을 포함한다. 이하 같다)을 요구할 권리 ---> ④
- 4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
- 5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리 ---> ③

문 15. 침해사고가 발생하였을 경우 조직 내의 모든 사람들이 신속하게 대처하여 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 단계는?

- ① 보안탐지 단계
- ② 대응 단계
- ③ 사후검토 단계
- ④ 조사와 분석 단계

답 ②

② 초기에 신속하게 대응하고 추가적인 손상을 막기 위한 단계는 '3 단계: 초기 대응' 단계이다.

< 정보보호 침해사고 대응 7 단계 >

1 단계: 사고 전 준비 과정

사고가 발생하기 전 침해사고 대응팀과 조직적인 대응을 준비

2 단계: 사고 탐지

정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해 사고의 식별

3 단계: 초기 대응

초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응팀 신고 및 소집, 침해사고 관련 부서에 통지

4 단계: 대응 전략 체계화

최적의 전략을 결정하고 관리자 승인을 획득, 초기 조사 결과를 참고하여 소송이 필요한 사항인지를 결정하고 사고 조사 과정에 수사기관 공조 여부를 판단

5 단계: 사고 조사

데이터 수집 및 분석을 통하여 수행, 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정

6 단계: 보고서 작성

의사 결정자가 쉽게 이하할 수 있는 형태로 사고에 대한 정확한 보고서를 작성

7 단계: 해결

차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획수립 등을 결정

문 16. 다음 설명에 해당하는 블루투스 공격 방법은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근 하는 공격 방법이다. 이 공격 방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP (OBEX Push Profile) 기능을 사용하여 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

- ① 블루스나프(BlueSnarf)
- ② 블루프린팅(BluePrinting)
- ③ 블루버그(BlueBug)
- ④ 블루재킹(BlueJacking)

답 ①

① 블루 스나프(BlueSnarf)

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.

공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP 기능을 사용하여 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근할 수 있다.

<오답 체크> ② 블루 프린팅(Blueprinting)

블루투스 공격장치의 검색활동을 의미한다.

각 블루투스 장치는 MAC 주소와 유사하게 6 바이트의 고유주소가 있다. 블루투스 장치는 장치간 종류를 식별하기 위해 SDP(서비스 발견 프로토콜)을 보내고 받는다. 그리고 이 SDP 를 이용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.

③ 블루 버그(BlueBug)

블루버그는 블루투스 장비간 취약한 연결 관리를 악용한 공격이다. 공격장치와 공격대상 장치를 연결하여 공격대상 장치에서 전화 걸기, SMS 보내기 등 임의의 동작을 실행하는 공격이다.

④ 블루재킹(BlueJacking)

블루투스를 이용해 스팸처럼 명함을 익명으로 퍼뜨리는 것. 다른 데이터의 이동이나 변조를 가하는 것이 아니며, 명함에는 주로 해커 메시지가 들어 있다.