2014년 지방직 9급 정보보호론 총평

-지안학원 조상진 교수

1. 문제분석

(가) 국가직 9급과 비슷한 출제범위를 제시

동일 출제기관여서 그런지 출제범위는 비슷하게 잡은 것 같습니다. 모든 영역에서 골고루 출제가 되었습니다. 특이한 문제는 특정 운영체제와 브라우저에 대한 내용이 1문제 출제되었는데, 이는 같은 날 시험본 교육청 문제에서도 동일했습니다(유닉스 문제 출제됨). 공부 범위가 계속 넓어지는 느낌입니다. 알기사(알기쉬운 정보보안기사, 조상진)에서 실무적으로 너무 깊게 들어가는 내용이라서 정보보호론에서는 빼냈는데 이번에 문제가 출제 되었습니다. 향후 개정판에서는 모두 포함시켜야할 것 같습니다.

(나) 법규 3문제/침해사고 대응 2문제 출제

국가직 9급시험과 동일하게 3문제가 출제되었는데, 개인정보보호법 1문제, 정보통신기반보호법 1문제, 정보통신망법 1문제씩 출제되었습니다. 서울시/지방직 대비 강의를 들으신 분들은 좀 수월했을 것 같습니다. 침해사고대응에서 2문제가 출제된 것은 이 부분을 중요하게 보고 있다는 것을 암시합니다.

(다) 난이도와 출제문제 분석

정보보호론 자체가 워낙 방대한 부분을 다루게 됩니다. 이번 시험도 깊게 들어가지는 안 했지만 상당히 방대하게 출제되었습니다. 국가직 9급시험과 다르게 약간 지협적으로 들어간 문제들이 몇 문제 보였습니다. 물론 탑스팟 교재에는 있었지만 과연 모든 수험생들이 맞추었을까 하는 의구심이 드네요. 전반적으로 난이도는 국가직 9급시험에 비해서는 높았습니다. 하지만, 강의를 통해서 법규문제가 어느 정도 정리되신 분들은 점수대가 국가직과 비슷하게 나왔을 것 같습니다.

2. 탑스팟 정보보호론 적중률 분석

(가) 적중률(93~98%)

PIMS와 Windows 방화벽만 동일 지문이 탑스팟 교재에 없었는데, 나머지 문항이 모두 교재에 있어서 역으로 추론해서 풀 수 있었을 것 같습니다. 나머지 문제들은 문제집이나 지방직 대비로 나누어 드린 자료에 모두 있었습니다. 자세한 내용은 해설에 적중된 페이지를 넣어놨으니 찾아보시기 바랍니다. 전체적으로 탑스팟 교재에서 93~98%정도의 적중률을 보였습니다.

(나) 이론편/문제편

60~70%는 문제편/이론편 지문과 동일한 내용이 많았고, 1~2문제가 수업시간에 강조하지 않은 내용인데 출제가 되었습니다. 침해사고대응과 관련해서 이번에 2문제 출제되었는데, 이 부분도 꼼꼼히 정리해봐야할 것 같습니다.

3. 향후 학습방향

(가) 범위를 넓게 공부하라.

국가직 9급 시험에 이어서 오늘 지방직 9급, 교육청 9급 시험이 있었는데, 출제범위를 상당히 넓게 잡고 있습니다. 법규문제는 일정 부분 계속 차지할 것 같습니다. 남은 시험에서는 침해사고 대응과 관련된 주제들도 꼼꼼히 살펴봐야할 것 같습니다. 교육청 시험에서는 유닉스 로그를 묻는 문제도 나왔습니다. 제가 강조한 부분만 재정리 해주세요.

(나) 회독수를 늘려라.

먼저 교재를 믿고, 다독을 해야 합니다. 단원별 문제풀이반이나 모의고사반에서 수업을 하다보면 점수는 회독수에 비례해서 점수가 나오는 것을 알 수 있었습니다. 남은 시험에서는 교재 구석구석 그동안 집중해서 안 읽어본 부분도 읽어주시길 부탁드립니다. 왜냐하면, 서울시/7급/국회사무처 시험 모두 난이도를 높이려면 지엽적인 부분에서도 출제할 가능성이 높기 때문입니다.

(다) 법규를 잘 정리하라.

제가 안행부 질의 답변 내용을 게시해드렸는데, 출제범위에 법규가 들어가 있습니다. 교육청 시험에서도 법규 문제가 출제되었습니다. 만약에 아직까지 이 부분을 정리하지 않으신 분들은 남은 시험을 위하여 지방직/서울시 대비반(동영상)에서 꼭 정리하고 시험에 임하세요.

4. 지안 공무원 향후 수업진행내용

- 7급 대비(6주) : 요약강의 + 모의고사 + 교육청 문제풀이 + 감리사 기출풀이

  ★ 감리사 문제만 별도 해설 특강은 없음

- 개정판 강의 : 2014년 9월 ~

※ 기타 지안/탑스팟 가족이든 아니든 개인적으로 정보보호론 공부방법에 대해서 궁금한 내용이 있으신 분들은 kingsalt1102@naver.com으로 메일 보내시면 제가 아는 범위내에서 성심껏 답변드리도록 하겠습니다. 감사합니다.

지방직 9급 공개채용시험

–2014년 6월 21일 시행

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 정확하며 오류 및 변조가 없었음이 보장되어야 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.

정답 및 해설

◦ 인증성은 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용되는 성질이다.

오답피하기 ①은 기밀성, ②은 무결성, ④은 가용성에 대한 설명이다.

정답 ③

〈문제적중〉 문제편 5~6페이지 문제 및 해설 적중

2.

시스템 계정 관리에서 보안성이 가장 좋은 패스워드 구성은?

① flowerabc

② P1234567#

③ flower777

④ Fl66ower$

정답 및 해설

◦ 패스워드는 다음 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성한다.

가. 영문 대문자(26개)

나. 영문 소문자(26개)

다. 숫자(10개)

라. 특수문자(32개)

오답피하기 ④ ②번은 3종류로 만들어진 패스워드이고, ④번은 4종류로 만들어진 형태로 보다 더 좋은 패스워드라고 할 수 있다.

정답 ④

〈문제적중〉 문제편 156페이지 10번 적중

3.

다음은 정보통신기반 보호법 의 일부이다. 본 조의 규정 목적으로 옳은 것은?

보기

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

…중략…

2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스·논리폭탄 등의 프로그램을 투입하는 행위

제28조(벌칙)

① 제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

② 제1항의 미수범은 처벌한다.

① 명예훼손 방지

② 개인정보 보호 침해 방지

③ 인터넷 사기 방지

④ 웜 피해 방지

정답 및 해설

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

오답피하기 ④ 웜은 자가증식하며 시스템 자원을 고갈시킬 수 있으므로 주요정보통신기반시설에 매우 위협적인 공격이 될 수 있으므로 이를 방지해야한다.

정 답 ④

〈문제적중〉 서울시/지방직대비반 적중

4.

다음 설명에 해당하는 것은?

> 보기
>
> 기업이 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로서, 한국인터넷진흥원(KISA)에서 시행 중인 인증제도

① TCSEC
② CC
③ PIMS
④ ITSEC

정답 및 해설

오답피하기 ③ 개인정보보호 관리체계 인증제 (Personal Information Management System Authentication, PIMS 인증제) : 고객의 개인 정보를 안전하게 관리하는 기업에 주는 인증 제도. 개인 정보를 다루는 기업이 전사 차원에서 개인 정보 보호 활동을 체계와 지속 있게 하려고 필요한 보호 조치 체계를 구축했는지를 점검해 어느 정도 이상의 기업에 인증해 주는 것이다. 고객의 개인 정보 보호를 위해 필요한 법에 따른 요구 사항을 포함해 모두 3개 분야 119개 통제 항목으로 구성돼 있다.

정 답 ③

〈문제적중〉 이론편 813페이지 표와 819페이지 ISMS로 통해 쉽게 풀 수 있는 문제.

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) :전화 통화, 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.

정답 및 해설

◦ 위장 (masquerade)
① 시스템에 접근하기 위해 허가받은 사용자로 위장하는 것.
② 한 개체가 다른 개체처럼 흉내 내는 것.

오답피하기 ③은 소극적 공격에 해당된다.

정 답 ③

〈문제적중〉 문제편 232페이지 1번 적중

6.

피싱(Phishing)에 대한 설명으로 옳지 않은 것은?

① Private Data와 Fishing의 합성어로서 유명 기관을 사칭하거나 개인 정보 및 금융 정보를 불법적으로 수집하여 금전적인 이익을 노리는 사기 수법이다.
② Wi-Fi 무선 네트워크에서 위장 AP를 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.

전문 및 해설

◦ 피싱(phishing)은 개인정보(private data)와 낚시(fishing)의 합성어로, 개인정보를 낚는다는 의미를 가지고 있다.
◦ 사용방법은 수신자에게 E-Mail을 발송하여 Phisher들이 운영하는 위조된 사이트로 이동시킨 후 이들에게 사이트 개편 등의 이유로 고객정보(신용카드번호, 비밀번호 등)를 요구한다. Phisher들은 이렇게 수집된 정보를 다양하게 활용한다.

오답피하기 ② 위장 AP를 이용하여 중간에 사용자의 정보를 가로채 사용자인 것처럼 속이는 수법은 중간자공격의 형태로 피싱과는 거리가 멀다.

정답 ②

〈문제적중〉 이론편 253페이지 적중

7.

국내 기관에서 주도적으로 개발한 암호 알고리즘은?

① IDEA
② ARIA
③ AES
④ Skipjack

전문 및 해설

오답피하기 ② ARIA는 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안기술연구소(NSRI)[1] 주도로 학계, 국가정보원 등의 암호기술전문가들이 힘을 모아 개발한 국가 암호화 알고리즘이다.

정답 ②

〈문제적중〉 이론편 81페이지 적중

8.

공개키 기반 구조(PKI, Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보보호 방식이다.
② 인증서의 폐지 여부는 인증서폐지목록(CRL)과 온라인 인증서 상태 프로토콜(OCSP) 확인을 통해서 이루어진다.
③ 인증서는 등록기관(RA)에 의해 발행된다.
④ 인증서는 버전, 일련번호, 서명, 발급자, 유효기간 등의 데이터 구조를 포함하고 있다.

전문 및 해설

오답피하기 ③ 등록기관(RA; Registration Authority)은 사용자와 CA가 서로 원거리에 위치해 있는 경우, 사용자와 CA의 중간위치에서 사용자의 인증서 요구를 받고 이를 확인한 후, CA에게 인증서 발급을 요청하고, 발급된 인증서를 사용자에게 전달하는 역할을 한다.

정답 ③

〈문제적중〉 문제편 58페이지 해설 적중

9.

소인수분해 문제의 어려움에 기초하여 큰 안전성을 가지는 전자 서명 알고리즘은?

① RSA
② ElGamal
③ KCDSA
④ ECDSA

정답 및 해설

오답피하기 ① RSA는 소인수분해의 어려움에 기초한 공개키 암호의 대표적 알고리즘이다.

정 답 ①

〈문제적중〉 문제편 32페이지 55번 적중

10.

디지털 포렌식의 기본 원칙에 대한 설명으로 옳지 않은 것은?

① 정당성의 원칙:모든 증거는 적법한 절차를 거쳐서 획득되어야 한다.
② 신속성의 원칙:컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.
③ 연계보관성의 원칙:증거자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.
④ 무결성의 원칙:획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다.

정답 및 해설

〈디지털 포렌식의 기본원칙〉
- 정당성 : 디지털 자료증거는 적절한 절차를 거쳐 획득
- 재현성 : 피해 당시와 동일 조건에서 현장 검출 시 동일 결과 도출
- 신속성 : 휘발성 정보를 신속한 조치에 의해 수집
- 연계보관성 : 디지털 증거물의 획득, 이송, 분석, 보관, 법정 제출의 각 단계를 담당하는 책임자 명시
- 무결성 : 획득한 디지털 증거가 위조 또는 변조되지 않았음을 증명

오답피하기 ③번은 재현성에 대한 설명이다.

정 답 ③

〈문제적중〉 이론편 808페이지 날개 적중

11.

보안 공격에 대한 설명으로 옳지 않은 것은?

① Land 공격: UDP와 TCP 패킷의 순서번호를 조작하여 공격 시스템에 과부하가 발생한다.
② DDoS(Distributed Denial of Service) 공격:공격자, 마스터, 에이전트, 공격 대상으로 구성된 메커니즘을 통해 DoS 공격을 다수의 PC에서 대규모로 수행한다.
③ Trinoo 공격: 1999년 미네소타대학교 사고의 주범이며 기본적으로 UDP 공격을 실시한다.
④ SYN Flooding 공격:각 서버의 동시 가용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용할 수 없게 만드는 공격이다.

정답 및 해설

오답피하기 ① Land Attack은 공격자가 임의로 자신의 IP 어드레스와 포트를 대상 서버의 IP 어드레스 및 포트와 동일하게 하여 서버에 접속하는 공격방식이다.

정 답 ①

〈문제적중〉 문제편 236페이지 11번, 12번 적중

12.

웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법은?

① PGP
② SSH
③ SSL
④ S/MIME

정답 및 해설

오답피하기 ③ SSL은 넷스케이프사가 웹 브라우저 상에서의 보안을 위해 개발한 것으로서, 인터넷 전자상거래 시 요구되는 개인 정보와 크레디트 카드 정보의 보안을 위하여 가장 많이 사용되고 있는 프로토콜이다. 이는 IP(Internet Protocol) 프로토콜이 보안면에서 완벽하지 못하다는 문제를 극복하기 위해 개발되었으며, 현재 전 세계 웹과 같은 특정 응용분야 뿐만 아니라, 일반적인 인터넷 보안을 위하여 사용되고 있는 프로토콜이다. SSL은 WWW상의 보안 위협을 방지하기 위하여 SSL은 상호인증, 무결성을 위한 메시지 인증 코드(MAC, Message Authentication Code), 메시지 보안을 위한 암호화 기능 등을 제공함으로써 응용 프로세서 간의 안전한 통신을 제공한다. SSL의 주요 보안 서비스는 기밀성(Confidentiality), 상호인증(Mutual Authentication), 무결성(Integrity)이다.

정답 ③

〈문제적중〉 문제편 339페이지 21번 적중

13.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 정보통신 서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 정보통신서비스 제공자의 정보보호 최고 책임자가 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

정답 및 해설

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다.
② 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.

1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 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

오답피하기 ② 주요정보통신기반시설의 지정은 정보통신기반보호법의 내용으로 최고책임자의 업무와는 거리가 멀다.

정답 ②

〈문제적중〉 서울시/지방직 대비 적중

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.

정답 및 해설

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

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

오답피하기 ④ 개인정보에 대하여 열람을 할 수 있으나, 사본의 발급은 요구할 수 있다.

정답 ④

〈문제적중〉 서울시/지방직 대비 적중

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

정답 및 해설

오답피하기 ② 침해사고가 발생하였을 경우 조직 내의 모든 사람들이 신속하게 대처하여 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 것은 사고대응 7단계에서 초기 대응단계에 해당된다.

정답 ②

〈문제적중〉 이론편 802페이지 적중

16.

다음 설명에 해당하는 블루투스 공격 방법은?

보기

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 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)

정답 및 해설

〈블루스나핑(bluesnarfing)〉

- 휴대폰 보안 취약점을 이용해 블루투스 기기에 저장된 데이터에 접근할 수 있는 것이다.
- 사용자가 알지 못하게 전화번호 목록이나 일정표를 읽고 변형시키고 복사하는 등의 해킹을 말한다.
- 특별한 장치 없이도 10m 범위 안에서 해킹이 가능하며, 아무런 침투 흔적도 남지 않는다.

오답피하기 ① 블루재킹은 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼트리는 것이고, 블루버깅은 사용자가 알지 못하게 블루투스를 이용해 이동전화 명령을 이용하는 것이다.

정답 ①

〈문제적중〉 이론편 509페이지 적중

17.

데이터베이스 보안 요구사항 중 비기밀 데이터에서 기밀 데이터를 얻어내는 것을 방지하는 요구사항은?

① 암호화
② 추론 방지
③ 무결성 보장
④ 접근통제

정답 및 해설

오답피하기 ② 추론 통제는 간접적으로 노출된 데이터 노출을 통해 다른 데이터를 추론하여 다른 데이터가 공개되는 것을 방지하는 것이다. 통계적인 자료에서 많이 발생한다.

정답 ②

〈문제적중〉 문제편 363페이지 17번 적중

18.

가상사설망의 터널링 기능을 제공하는 프로토콜에 대한 설명으로 옳은 것은?

① IPSec은 OSI 3계층에서 동작하는 터널링 기술이다.
② PPTP는 OSI 1계층에서 동작하는 터널링 기술이다.
③ L2F는 OSI 3계층에서 동작하는 터널링 기술이다.
④ L2TP는 OSI 1계층에서 동작하는 터널링 기술이다.

정답 및 해설

오답피하기 ① IPSec(IP Security Protocol)은 IETF가 IP 계층(네트워크계층) 보안을 위하여 개방형 구조로 설계한 표준이며, 네트워크계층의 보안에 대해서 안정적이고 표준화된 기초를 제공한다.

정답 ①

〈문제적중〉 문제편 296페이지 9번 적중

19.

미국의 NIST와 캐나다의 CSE가 공동으로 개발한 평가체계로 암호모듈의 안전성을 검증하는 것은?

① CMVP
② COBIT
③ CMM
④ ITIL

정답 및 해설

오답피하기 ① 암호모듈 안정성 평가프로그램 중 미국의 NIST에서 실시하고 있는 CMVP(Cryptographic Module Validation Program)가 대표적이다.

정답 ①

〈문제적중〉 문제편 20페이지 22번 적중

20.

MS Windows 운영체제 및 Internet Explorer의 보안 기능에 대한 설명으로 옳은 것은?

① Windows 7의 각 파일과 폴더는 사용자에 따라 권한이 부여되는데, 파일과 폴더에 공통적으로 부여할 수 있는 사용권한은 모든 권한수정·읽기·쓰기의 총 4가지이며, 폴더에는 폴더 내용 보기라는 권한을 더 추가할 수 있다.
② BitLocker 기능은 디스크 볼륨 전체를 암호화하여 데이터를 안전하게 보호하는 기능으로 Windows XP부터 탑재되었다.
③ Internet Explorer 10의 인터넷 옵션에서 개인정보 수준을 '낮음'으로 설정하는 것은 모든 쿠키를 허용함을 의미한다.
④ Windows 7 운영체제의 고급 보안이 포함된 Windows 방화벽은 인바운드 규칙과 아웃바운드 규칙을 모두 설정할 수 있다.

정답 및 해설

◦ 윈도우 7 에서는 고급 설정을 통해, 인바운드 규칙과 아웃바운드 규칙에 각각 새 규칙을 넣어 포트를 개방하는 방식을 사용한다.

오답피하기 ① 파일과 폴더에 공통적으로 부여할 수 있는 사용권한은 모든 권한, 수정, 읽기 및 실행, 읽기, 쓰기, 특정 권한의 총 6가지이며, 폴더에는 폴더 내용 보기라는 권한을 더 추가할 수 있다.

② 윈도 비스타 이후부터 비트락커(Bitlocker)라는 기술을 제공하고 있다. 비트락커 기술은 하드웨어에 장착된 TPM(Trusted Platform Module, 신뢰할 수 있는 플랫폼 모듈)을 이용해 내장된 디스크를 암호화하므로, 해당 디바이스에서 하드 디스크를 추출하면 데이터 확인이 불가능해진다. 하드웨어를 분실하더라도, 안에 저장된 소프트웨어를 지킬 수 있게 하는 기술이란 의미다. TPM이 없는 경우 사용자가 지정해 입력한 암호를 통해 데이터를 암호화하므로, 해당 기술을 적용하지 않은 하드웨어에서도 이를 활용할 수 있다.

③ 개인정보 설정에서 낮음 단계와 별개로 모든 쿠키 허용이라는 단계가 있다. 낮음 단계는 압축된 개인정보 취급방침이 없는 타사의 쿠키를 차단하고, 사용자의 암시적 동의 없이 사용자에게 연락하는 데 사용할 수 있는 정보를 저장하는 타사의 쿠키를 제한한다.

정답 ④

〈문제적중〉 이론편 347, 349, 363, 370 페이지에서 추론 가능하지만 난해한 문제