2014년 국가직 9급 정보보호론 총평

-지안학원 조상진 교수

1. 문제분석

(가) 첫 시험으로 출제범위를 제시

2014년 첫 시험였습니다. 출제기관에서는 대학교재를 기준으로 공부하라고 했지만, 과연 시험범위가 어디까지인지 가늠하기 상당히 어려웠는데, 어느 정도 윤곽은 잡힌 듯합니다. 일단은 정보보안기사 영역인 5개 법률 중에 2개 법률에서 3개문제가 출제되었습니다. 향후 정보보호론 시험은 이 영역까지 정리해야할 듯합니다.

(나) 정보보안기사 시험영역인 법률 3문제 출제

개인정보보호법 2문제, 정보통신기반보호법 1문제가 출제되었습니다. 개인적으로 가장 출제가능성이 높아서 개인정보보호법은 수업시간이 다루었지만, 정보통신기반보호법은 좀 의외였습니다. 혹시 출제 위원 중에 정보보안기사 문제냈던 분이 출제하지 안했나 하는 생각이 듭니다.

(다) 난이도와 출제문제 분석

정보보호론 자체가 워낙 방대한 부분을 다루게 됩니다. 이번 시험도 깊게 들어가지는 안 했지만 상당히 방대하게 출제되었습니다. 탑스팟 교재로 2~3회독을 하신 분들은 어렵지 않게 풀었겠지만 어느 정도 정리가 덜 된 수험생들은 어렵게 느껴졌을지도 모릅니다.

2. 탑스팟 정보보호론 적중률 분석

(가) 적중률(95%)

정보통신기반보호법을 제외한 모든 문제가 탑스팟 교재에서 출제되어 95% 적중률을 보였습니다. 자세한 내용은 해설에 적중된 이론편/문제편/모의고사의 페이지를 넣어놨으니 찾아보시기 바랍니다. 1문제는 알기쉬운 정보보안기사(조상진 저)에 나오는 내용입니다.

(나) 이론편/문제편

60~70%는 문제편 지문과 동일한 내용이 많았고, 수업시간에 강조한 내용들이 대다수 출제되었습니다. 나머지도 이론편 기본 개념만 정리하면 풀 수 있는 내용입니다.

3. 향후 학습방향

(가) 범위를 넓게 공부하라.

작년부터 시행되는 정보보안기사를 보게 되면 문제가 상당히 방대하게 출제되고 있습니다. 실제 이를 준비하는 수험생들이 가장 어려워하는 부분중에 하나였습니다. 정보보호론도 이에 못지 않게 범위를 상당히 넓게 잡는 것 같습니다. Unix/Linux는 안 나왔지만, 법률은 개인정보보호법만 나오기를 바랬습니다만, 공무원 준비생이 습득할 지식으로 판단을 한 것인지? 아니면 정보보안기사의 연장선상에서 한 문제 나왔는지 모르겠지만, 향후 수험생들에게는 상당한 부담으로 작용할 듯합니다.

(나) 회독수를 늘려라.

먼저 교재를 믿고, 다독을 해야 합니다. 단원별 문제풀이반이나 모의고사반에서 수업을 하다보면 점수는 회독수에 비례해서 점수가 나오는 것을 알 수 있었습니다. 카페에서 질문을 열심히하고 여러 번 본 수험생들은 점수가 고르게 일정하게 나옵니다. 그런 분은 이번 시험에서 분명 고득점을 받았을 것입니다.

(다) 법규를 잘 정리하라.

이번 시험의 출제범위는 대학교재+실무법률이 특징입니다. 실무법률의 범위는 정보보안기사 5개 법률 중에 2개 법률에서 출제되었습니다. 그렇다고 현 시점에서 정보보안기사 교재를 찾는 것은 옳지 않습니다. 왜냐하면 세 문제 중에 하나는 공공기관 개인정보에 관한 내용으로 정보보안기사 영역에도 없는 문제였습니다. 고로, 전산직에 특화된 법률 강의를 통해서 정리하는 것이 효율적일 듯합니다.

4. 지안 공무원 향후 수업진행내용

- 5월 지방직 대비(4주) : 법률 정리 + 요약강의 + 모의고사
- 7급 대비(6주) : 요약강의 + 모의고사
- 감리사 해설특강(7월 중순 예정) - 7급 대비 추천

※ 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.

국가직 9급 공개채용시험

–2014년 4월 19일 시행

1.

서비스 거부(DoS : Denial of Service) 공격 또는 분산 서비스 거부(DDoS : Distributed DoS) 공격에 대한 설명으로 옳지 않은 것은?

① TCP SYN이 DoS 공격에 활용된다.
② CPU, 메모리 등 시스템 자원에 과다한 부하를 가중시킨다.
③ 불특정 형태의 에이전트 역할을 수행하는 데몬 프로그램을 변조하거나 파괴한다.
④ 네트워크 대역폭을 고갈시켜 접속을 차단시킨다.

DDoS 공격은 여러 대의 컴퓨터를 일제히 동작하게 하여 특정 사이트/시스템을 공격하여 엄청난 분량의 패킷을 동시에 범람시켜 네트워크 성능 저하나 시스템 마비를 가져오게 하는 해킹 방법이다.

③ DDOS(Distributed Denial of Service) 공격은 해커가 감염시킨 대량의 좀비 컴퓨터를 이용해 특정 시스템으로 다량의 패킷을 무차별적으로 보내 과다 트래픽으로 시스템을 마비시키는 사이버 공격, 공격자는 다양한 방법으로 일반 사용자 PC(숙주 PC)에 봇을 감염시키고, 악의로 컴퓨터를 조종하여 표적 시스템의 데이터 베이스(DB) 삭제, 서버 마비 등 사이버 공격을 하는 것이 특징으로 데몬 프로그램 파괴와는 거리가 멀다.

정답 ③

〈문제적중〉 문제편 243p 문제/해설, DDoS의 개념을 묻는 단순 문제

2.

보안 프로토콜인 IPSec(IP Security)의 프로토콜 구조로 옳지 않은 것은?

① Change Cipher Spec
② Encapsulating Security Payload
③ Security Association
④ Authentication Header

◦ ESP(Encapsulation Security Payload) : 데이터 기밀성, 패킷 단위의 무결성, 데이터 원본 인증 및 Replay에 대한 보호(SPI 이용)를 제공한다. AH와 비교해 ESP는 암호화를 제공한다는 점이 다르다. ESP의 암호화는 공유된 대칭키를 사용한다.
◦ SA : IPSec은 공개키 암호화 방식을 사용한다. 통신 할 때 송·수신 측은 공개키를 교환하고, 인증 및 암호화 알고리즘과 암호키에 대한 정보를 교환해야 한다. 이러한 암호관련 프로파일(Profile)을 SA라고 한다.
◦ AH(Authentication Header) : AH는 IP 패킷에 대해서 무결성과 데이터 원본인증을 제공한다. 그리고 Replay에 대한 보호를 제공한다.

① Change Cipher Spec은 암호사양을 변경하는 SSL 프로토콜이다.

정답 ①

〈문제적중〉 이론서 598p~599p, 수업시간에 여러 번 강조한 내용임.

3.

DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?

① 디지털 컨텐츠의 불법 복제와 유포를 막고, 저작권 보유자의 이익과 권리를 보호해 주는 기술과 서비스를 말한다.
② DRM은 파일을 저장할 때, 암호화를 사용한다.
③ DRM 탬퍼 방지(tamper resistance) 기술은 라이센스 생성 및 발급관리를 처리한다.
④ DRM은 온라인 음악서비스, 인터넷 동영상 서비스, 전자책, CD/DVD 등의 분야에서 불법 복제 방지 기술로 활용된다.

정답 및 해설

DRM(Digital Rights Management)기술은 콘텐츠의 지적재산권이 디지털 방식에 의해서 안전하게 보호, 유지되도록 콘텐츠 장착에서부터 소비에 이르는 모든 유과정에서 거래 및 분배규칙, 사용규칙이 적법하게 성취되도록 하는 기술이다.

오답피하기 ③ DRM 탬퍼 방지(tamper resistance) 기술은 복제방지 등 위조에 대한 저항성으로 라이센스 생성 및 발급관리 처리와는 무관하다.

정답 ③

〈문제적중〉 이론서 56~57p, DRM의 기본 개념과 tamper resistance의 뜻만 알면 간단히 풀 수 있는 문제.

4.

다음 설명에 해당하는 접근제어 모델은?

보기

조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다. 사용자가 적절한 직무에 할당되고, 직무에 적합한 접근 권한이 할당된 경우에만 접근할 수 있다.

① 강제적 접근제어(Mandatory Access Control)
② 규칙 기반 접근제어(Rule-Based Access Control)
③ 역할 기반 접근제어(Role-Based Access Control)
④ 임의적 접근제어(Discretionary Access Control)

정답 및 해설

◦ 강제적 접근통제(MAC; Mandatory Access Control) : 주체가 객체로 접근하는데 적용되는 규칙은 보안전문가에 의해 생성되며, 운영자에 의해 설정되며, 운영체제에 의해 실행되고, 그리고 다른 보안기술들에 의해 지원된다.(중앙집중형 보안관리) 접근규칙은 운영시스템에 의하여 정의되기 때문에 Rule-based 접근통제라고도 한다.
◦ 임의적 접근통제(DAC; Discretionary Access Control) : 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 객체의 소유자가 접근여부를 결정한다. 구현이 쉽고 권한 변경이 유연한 점이 장점이다. 하나의 주체마다 객체에 대한 접근 권한을 부여해야 하는 불편한 점이 있다.
◦ 역할기반 접근통제(RBAC; Role Based Access Control) : 1970년대 다중 사용자, 다중 프로그래밍 환경에서의 보안처리 요구를 만족시키기 위해 제안된 방식으로 사용자의 역할에 기반을 두고 접근을 통제하는 모델이다.

오답피하기 ③ RBAC에 대한 개념 정의이다.

정답 ③

〈문제적중〉 문제편 88p 8번 문제 적중.

5.

공개키 암호에 대한 설명으로 옳지 않은 것은?

① 공개키 인증서를 공개키 디렉토리에 저장하여 공개한다.
② 사용자가 증가할수록 필요한 비밀키의 개수가 증가하는 암호방식의 단점을 해결할 수 있다.
③ 일반적으로 대칭키 암호방식보다 암호화 속도가 느리다.
④ n명의 사용자로 구성된 시스템에서는 $\frac{n(n-1)}{2}$ 개의 키가 요구된다.

정답 및 해설

◦ 공개키 인증서는 누구나 접근 가능한 공개키 디렉토리에 저장하여 공개한다.
◦ 공개키 암호는 대칭키 암호시스템의 키배송문제를 해결하기 위하여 등장 했다.
◦ 공개키 암호는 대칭키 암호에 비해 키의 길이는 길고, 속도는 느리다.

오답피하기 ④ n명의 사용자로 구성된 시스템에서는 2n개의 키가 요구된다.

정답 ④

〈문제적중〉 이론서 111p, 모의고사 1회 9번 적중

6.

웹 서버 보안에 대한 설명으로 옳지 않은 것은?

① 웹 애플리케이션은 SQL 삽입공격에 안전하다.
② 악성 파일 업로드를 방지하기 위하여 필요한 파일 확장자만 업로드를 허용한다.
③ 웹 애플리케이션의 취약점을 방지하기 위하여 사용자의 입력 값을 검증한다.
④ 공격자에게 정보 노출을 막기 위하여 웹 사이트의 맞춤형 오류 페이지를 생성한다.

정답 및 해설

◦ 파일 업로드 취약점(File Upload Vulnerability) : 게시판 등에서 스크립트 파일의 업로드에 대한 규제가 없을 경우 이를 악용한 해커에 의해 악성 스크립트 파일이 수행될 수 있는 보안 취약점이다. 게시판에서 파일 업로드가 가능한 경우 해당 게시판의 웹 어플리케이션과 동일한 언어의 스트립트 파일을 업로드한 후에 다시 이를 SSI(Server Side Interpreter) 특성을 이용하여 실행시킴으로서 웹 서버의 내부 명령어를 실행하는 공격이다.
◦ SQL injection, XSS 공격 등은 입력값 검증이 제대로 수행되지 않을 때 발생하는 공격이다.

오답피하기 ① SQL injection 공격은 데이터베이스와 연동되어 있는 어플리케이션의 입력값을 조작하여 DBMS가 의도되지 않은 결과를 반환하도록 하는 공격기법이다. 이는 해당 어플리케이션에서 사용자로부터 전송되어 오는 입력값에 대해 그 적정성을 검사하지 않았기 때문에 발생한다.(필터링이 없을 경우)

정답 ①

〈문제적중〉 문제편 346p 36번 적중

7.

개인정보 보호법 상 개인정보 유출 시 개인정보처리자가 정보 주체에게 알려야 할 사항으로 옳은 것만을 모두 고르면?

보기
ㄱ. 유출된 개인정보의 위탁기관 현황
ㄴ. 유출된 시점과 그 경위
ㄷ. 개인정보처리자의 개인정보 보관 · 폐기 기간
ㄹ. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

① ㄱ, ㄴ
② ㄷ, ㄹ
③ ㄱ, ㄷ
④ ㄴ, ㄹ

정답 및 해설

〈개인정보 유출 시 정보주체에게 알려야 할 사항〉

◦ 유출된 개인정보의 항목
◦ 유출된 시점과 그 경위
◦ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
◦ 개인정보처리자의 대응조치 및 피해 구제 절차
◦ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

오답피하기 ④ ㄱ. 유출된 개인정보의 위탁기관 현황, ㄷ. 개인정보처리자의 개인정보 보관·폐기 기간은 개인정보 유출 시 개인정보처리자가 정보 주체에게 알려야 할 사항이 아니다.

정답 ④

〈문제적중〉 문제편 480p, 13번 적중

8.

PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① PGP는 전자우편용 보안 프로토콜이다.
② 공개키 암호 알고리즘을 사용하지 않고, 대칭키 암호화 알고리즘으로 메시지를 암호화한다.
③ PGP는 데이터를 압축해서 암호화한다.
④ 필 짐머만(Philip Zimmermann)이 개발하였다.

정답 및 해설

〈PGP(Pretty Good Privacy)〉

◦ 1990년경에 필립 짐머만(Philip Zimmermann)에 의해 제안된 전자우편용 보안 프로토콜이다.
◦ 메시지를 속도가 빠른 대칭 알고리즘을 사용해 암호화하며, 대칭 알고리즘에 사용된 비밀키를 공개키 암호방식을 이용해 암호화하여 전달하는 키분배 방식을 사용한다.
◦ 암호화는 데이터를 압축 후에 암호화하고, 전자서명은 서명 후 압축한다.

오답피하기 ② PGP(Pretty Good Privacy)는 전자우편 메시지에 대해 IDEA 대칭키 암호 알고리즘과 RSA 공개키 암호 알고리즘을 사용한다.

정답 ②

〈문제적중〉 문제편 321p, 15번 적중

9.

컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은?

① 트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.
② 웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성프로그램이다.
④ 루트킷(Rootkit)은 감염된 시스템에서 활성화되어 다른 시스템을 공격하는 프로그램이다.

정답 및 해설

◦ 백도어(back door)/트랩도어(Trap door) : 시스템의 보안이 제거된 비밀통로로서, 서비스 기술자나 유지보수 프로그래머들의 접근 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 통로이다. 이런 통로를 만드는 이유는 현장에서 서비스 기술자나 공급사의 유지보수 프로그래머가 업무 편의성을 향상시키기 위함이다.

◦ 웜(Worm) : 초창기 형태의 악성 소프트웨어로서 컴퓨터 내의 다른 시스템에는 직접적인 악영향을 미치지 않고 기억장소 내에서 자가 증식하는 프로그램이다.

◦ 트로이목마 프로그램은 자료삭제 및 정보탈취 등의 목적으로 사용된다.

오답피하기 ④ Rootkit은 해커의 침입흔적을 삭제하거나 재침입을 위해 사용되는 백도어를 만들기 위한 도구들의 모음이다.

정답 ④

〈문제적중〉 문제편 101p, 11번 적중

10.

정보보호 관리체계 인증 등에 관한 고시 에 의거한 정보보호 관리체계(ISMS)에 대한 설명으로 옳지 않은 것은?

① 정보보호관리과정은 정보보호정책 수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현 등 4단계 활동을 말한다.

② 인증기관이 조직의 정보보호 활동을 객관적으로 심사하고, 인증한다.

③ 정보보호 관리체계는 조직의 정보 자산을 평가하는 것으로 물리적 보안을 포함한다.

④ 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위하여 관리적· 기술적 수단과 절차 및 과정을 관리, 운용하는 체계이다.

정답 및 해설

ISMS 인증제도란 정보통신서비스제공자, 정보통신서비스를 위해 물리적 시설을 제공하는 자, 민간사업자 등 인증대상기관이 수립 · 운영하고 있는 ISMS 기술, 물리, 관리적 정보보호대책이 인증심사기준에 적합한지를 한국인터넷진흥원(KISA)이 객관적으로 평가하여 인증하는 제도를 말한다.

오답피하기 ① 정보보호관리과정이란 정보보호 관리체계를 수립 · 운영하기 위하여 유지 · 관리하여야 할 과정으로 다음 5단계 활동을 말한다.

가. 정보보호정책 수립 및 범위설정
나. 경영진 책임 및 조직구성
다. 위험관리
라. 정보보호대책 구현
마. 사후관리

정답 ①

〈문제적중〉 이론서 819p, 모의고사 3회 18번 적중

11.

공격자가 자신이 전송하는 패킷에 다른 호스트의 IP 주소를 담아서 전송하는 공격은?

① 패킷 스니핑(Packet Sniffing)
② 스미싱(Smishing)
③ 버퍼 오버플로우(Buffer Overflow)
④ 스푸핑(Spoofing)

정답 및 해설

◦ 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하여 네트워크 트래픽을 도청(eavesdropping)하는 과정을 스니핑이라고 할 수 있다.

◦ 스미싱(SMishing) : SMS와 Phishing의 결합어로 문자메시지를 이용 피싱하는 방법. 해커는 핸드폰 사용자에게 웹사이트 링크를 포함한 문자메시지를 보내고 휴대폰 사용자가 웹사이트에 접속하면 트로이목마를 주입해 인터넷 사용이 가능한 휴대폰을 통제할 수 있게 된다.

◦ 버퍼 오버플로우(Buffer Overflow) : 버퍼에 입력되는 정보에 대해 한계 체크가 실행되지 않을 경우 데이터의 긴 문자열이 받아들여질 수 있다. 이로 인해 입력된 데이터가 할당된 메모리 버퍼보다 크다면 데이터는 또 다른 메모리 세그먼트로 흘러 넘치게 된다. 이를 통해 프로그램의 복귀주소를 조작, 궁극적으로 해커가 원하는 코드가 실행하게 하는 공격 방법이다.

오답피하기 ④ 스푸핑이란 해커가 악용하고자 하는 호스트의 IP 주소나 이메일 주소를 바꾸어서 이를 통해 해킹하는 것을 말한다.

정답 ④

〈문제적중〉 이론편 552p 적중

12.

정보보호의 주요 목적에 대한 설명으로 옳지 않은 것은?

① 기밀성(confidentiality)은 인가된 사용자만이 데이터에 접근할 수 있도록 제한하는 것을 말한다.

② 가용성(availability)은 필요할 때 데이터에 접근할 수 있는 능력을 말한다.

③ 무결성(integrity)은 식별, 인증 및 인가 과정을 성공적으로 수행했거나 수행 중일 때 발생하는 활동을 말한다.

④ 책임성(accountability)은 제재, 부인방지, 오류제한, 침입탐지 및 방지, 사후처리 등을 지원하는 것을 말한다.

정답 및 해설

〈책임추적성(Accountability)〉

◦ 사용자의 이용을 추적하고 그의 행동에 대해 기록하고 추적하는 활동

◦ 관여하지 않은 사람에게 책임을 물어 불이익을 당하지 않도록 함

◦ 식별, 인증, 권한부여, 접근통제, 감사 개념을 기반으로 수립됨

오답피하기 ③ 무결성은 데이터가 송신된 그대로 수신자에게 도착해야 한다는 것을 의미하고, 전송 중 데이터에 대한 고의적 또는 악의적인 변경이 없었다는 것을 의미한다.

정답 ③

〈문제적중〉 문제편 5p 7번 적중

13.

네트워크 각 계층별 보안 프로토콜로 옳지 않은 것은?

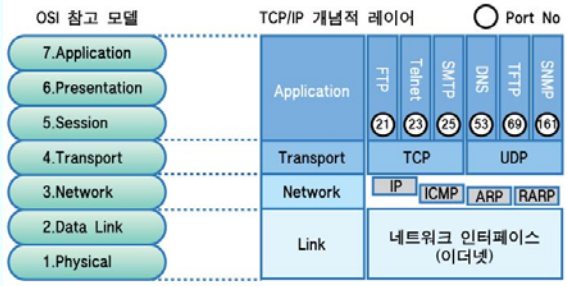
① 네트워크 계층(network layer) : IPSec

② 네트워크 계층(network layer) : FTP

③ 응용 프로그램 계층(application layer) : SSH

④ 응용 프로그램 계층(application layer) : S/MIME

정답 및 해설



오답피하기 ② FTP는 응용 프로그램 계층에 해당된다.

정답 ②

〈문제적중〉 문제편 171p, 22번 해설 적중

14.

방화벽(firewall)에 대한 설명으로 옳지 않은 것은?

① 패킷 필터링 방화벽은 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등을 이용한 접속제어를 수행한다.

② 패킷 필터링 기법은 응용 계층(application layer)에서 동작하며, WWW와 같은 서비스를 보호한다.

③ NAT 기능을 이용하여 IP 주소 자원을 효율적으로 사용함과 동시에 보안성을 높일 수 있다.

④ 방화벽 하드웨어 및 소프트웨어 자체의 결함에 의해 보안상 취약점을 가질 수 있다.

정답 및 해설

◦ NAT(Network Address Translation) : 라우터에 의해 적은 숫자의 유효 IP 주소만으로도 많은 시스템들이 인터넷에 접속할 수 있게 하는 네트워크 서비스이다. NAT에서 내부 네트워크와 외부 네트워크는 자연스럽게 두개의 네트워크로 분리된다. 외부에서 내부 네트워크로 직접적인 접근이 불가능하게 되므로 네트워크 보안효과를 가져올 수 있다.

◦ 패킷 필터링 방화벽(Packet filtering) : 관리자가 필터링을 위해 정의한 IP와 Port를 목록으로 작성하여, 차단 목록을 기반으로 네트워크계층과 전송계층에서 차단할 수 있는 필터링 기법이다.

오답피하기 ② 패킷 필터링 Firewall은 OSI 7 계층에서 3계층인 네트워크 레이어와 4계층인 트랜스포트 레이어에서 동작한다.

정답 ②

〈문제적중〉 문제편 282p 22번 적중

15.

해시 함수(hash function)에 대한 설명으로 옳지 않은 것은?

① 임의 길이의 문자열을 고정된 길이의 문자열로 출력하는 함수이다.

② 대표적인 해시 함수는 MD5, SHA-1, HAS-160 등이 있다.

③ 해시 함수는 메시지 인증과 메시지 부인방지 서비스에 이용된다.

④ 해시 함수의 충돌 회피성은 동일한 출력을 산출하는 서로 다른 두 입력을 계산적으로 찾기 가능한 성질을 나타낸다.

정답 및 해설

◦ 역상 저항성 : 주어진 임의의 출력값 y에 대해, y=h(x)를 만족하는 입력값 x를 찾는 것이 계산적으로 불가능하다.

◦ 두 번째 역상 저항성 : 주어진 입력값 x에 대해 h(x)=h(x'), x≠x'을 만족하는 다른 입력값 x'을 찾는 것이 계산적으로 불가능하다.

◦ 충돌 저항성 : h(x)=h(x')을 만족하는 임의의 두 입력값 x, x'을 찾는 것이 계산적으로 불가능하다.

오답피하기 ④ 해시 함수의 충돌 회피성은 동일한 출력을 산출하는 서로 다른 두 입력을 계산적으로 찾기 불가능한 성질을 나타낸다.

정답 ④

〈문제적중〉 문제편 38p 4번 적중

16.

정보통신기반 보호법 에 대한 설명으로 옳지 않은 것은?

① 주요정보통신기반시설을 관리하는 기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 그 사실을 통지하여야 한다.

② "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터 바이러스, 서비스 거부 또는 고출력 전자기파 등에 의한 공격행위를 말한다.

③ 관리기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 시설을 주요정보통신기반시설로 지정할 수 있다.

④ 주요정보통신기반시설의 취약점 분석·평가 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

정답 및 해설

◦ 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.
◦ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

오답피하기 ③ 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 시설을 주요정보통신기반시설로 지정할 수 있다.

정답 ③

〈문제적중〉 알기쉬운 정보보안기사(조상진 저) 3판 603p에 나옴.(정보보호론에는 없었음)

17.

개인정보 보호법 상 공공기관에서의 영상정보처리기기 설치 및 운영에 대한 설명으로 옳지 않은 것은?

① 공공기관의 사무실에서 민원인의 폭언·폭행 방지를 위해 영상정보처리기기를 설치 및 녹음하는 것이 가능하다.
② 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보 처리기기를 임의로 조작하거나 다른 곳을 비춰서는 안 된다.
③ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다.
④ 개인정보 보호법 에서 정하는 사유를 제외하고는 공개된 장소에 영상정보처리기기를 설치하는 것은 금지되어 있다.

정답 및 해설

누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

오답피하기 ① 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

정답 ①

〈문제적중〉 이론서 839p 적중

18.

국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① 정보보호 측면에서 정보보호 기능이 있는 IT 제품의 안전성을 보증·평가하는 기준이다.
② 국제공통평가기준은 소개 및 일반모델, 보안기능요구사항, 보증요구사항 등으로 구성되고, 보증 등급은 5개이다.
③ 보안기능요구사항과 보증요구사항의 구조는 클래스로 구성된다.
④ 상호인정협정(CCRA:Common Criteria Recognition Arrangement)은 정보보호제품의 평가인증 결과를 가입국가 간 상호 인정하는 협정으로서 미국, 영국, 프랑스 등을 중심으로 시작되었다.

정답 및 해설

〈공통 평가기준(CC, Common Criteria)〉

◦ 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 국제표준 평가기준이다. 국제표준(ISO/IEC 15408)으로 1999년 9월 승인되었다.

◦ 현존하는 평가기준과 조화를 통해 평가결과를 상호인정(CCRA)하는 구조로 정보보호시스템의 수출입에 소요되는 인증비용 절감으로 국제유통 촉진, 정보보호시스템의 보안등급 평가에 신뢰성을 부여한다.

오답피하기 ② 국제공통평가기준은 소개 및 일반모델, 보안기능요구사항, 보증요구사항 등으로 구성되고, 보증 등급은 7개이다.

정답 ②

〈문제적중〉 문제편 469p, 이론서 816p 적중

19.

위험관리 요소에 대한 설명으로 옳지 않은 것은?

① 위험은 위협 정도, 취약성 정도, 자산 가치 등의 함수관계로 산정할 수 있다.

② 취약성은 자산의 약점(weakness) 또는 보호대책의 결핍으로 정의할 수 있다.

③ 위험 회피로 조직은 편리한 기능이나 유용한 기능 등을 상실할 수 있다.

④ 위험관리는 위협 식별, 취약점 식별, 자산 식별 등의 순서로 이루어진다.

정답 및 해설

〈위험 회피(Risk avoidance)〉

◦ 위험 회피는 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다.

◦ 자산 매각이나 설계변경 등 다른 대안을 선택하여 해당 위험이 실현되지 않도록 하는 것이다.

오답피하기 ④ 위험관리는 자산식별, 위협분석, 취약성평가, 영향평가, 대책선정, 권고안 작성 순으로 진행된다.

정답 ④

〈문제적중〉 문제편 424p 37번 적중

20.

다음 설명에 해당하는 컴퓨터 바이러스는?

보기

산업 소프트웨어와 공정 설비를 공격 목표로 하는 극도로 정교한 군사적 수준의 사이버 무기로 지칭된다. 공정 설비와 연결된 프로그램이 논리제어장치(Programmable Logic Controller)의 코드를 악의적으로 변경하여 제어권을 획득한다. 네트워크와 이동저장매체인 USB를 통해 전파되며, SCADA(Supervisory Control and Data Acquisition) 시스템이 공격 목표이다.

① 오토런 바이러스(Autorun virus)

② 백도어(Backdoor)

③ 스턱스넷(Stuxnet)

④ 봇넷(Botnet)

정답 및 해설

자동 실행 바이러스(Autorun Virus) : MP3 플레이어나 USB 같은 이동형 저장 장치에 복사되어 자동 실행되도록 설정된 악성 코드. 'autorun.inf' 파일을 이용하거나 시스템 레지스트리에 등록되어 폴더를 숨기거나 더블 클릭을 방해하는 등의 악성 행위를 한다.

오답피하기 ③ 스턱스넷(Stuxnet)은 독일 지멘스사의 원격 감시 제어 시스템(SCADA)의 제어 소프트웨어에 침투하여 시스템을 마비하게 하는 악성 코드. 원자력 발전소와 송·배전망, 화학 공장, 송유·가스관과 같은 산업 기반 시설에 사용되는 제어 시스템에 침투하여 오동작을 유도하는 명령 코드를 입력해서 시스템을 마비하게 하는 악성 코드이다.

정답 ③

〈문제적중〉 이론편 211p 날개 적중