2021년 지방직,교육청 9급 정보보호론

-2021년 6월 5일 시행

1. ○△× 21.지방.9급

보안의 3대 요소 중 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것은?

① 무결성(integrity)
② 기밀성(confidentiality)
③ 가용성(availability)
④ 접근성(accessability)

오답피하기 ① 정보는 정해진 절차에 따라, 그리고 주어진 권한에 의해서만 변경되어야 한다는 것이 무결성이다. 정보는 항상 정확성을 일정하게 유지하여야 하며, 인가받은 방법에 의해서만 변경되어야 한다.

정답 ①

2. ○△× 21.지방.9급

스트림 암호에 대한 설명으로 옳지 않은 것은?

① 데이터의 흐름을 순차적으로 처리해 가는 암호 알고리즘이다.
② 이진화된 평문 스트림과 이진 키스트림 수열의 XOR 연산으로 암호문을 생성하는 방식이다.
③ 스트림 암호 알고리즘으로 RC5가 널리 사용된다.
④ 구현이 용이하고 속도가 빠르다는 장점이 있다.

오답피하기 ③ RC4가 스트림 암호 알고리즘이고, RC5는 블록 암호 알고리즘이다.

정답 ③

3. ○△× 21.지방.9급

DES(Data Encryption Standard)에 대한 설명으로 옳지 않은 것은?

① 1977년에 미국 표준 블록 암호 알고리즘으로 채택되었다.
② 64비트 평문 블록을 64비트 암호문으로 암호화한다.
③ 페이스텔 구조(Feistel structure)로 구성된다.
④ 내부적으로 라운드(round)라는 암호화 단계를 10번 반복해서 수행한다.

오답피하기 ④ DES는 한 번의 암호화를 위해 10라운드가 아닌 16라운드를 거친다.

정답 ④

4. ○△× 21.지방.9급

다음 (가) ~ (다)에 해당하는 악성코드를 옳게 짝 지은 것은?

보기

(가) 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드
(나) 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성코드
(다) 외부에서 파일을 내려받는 다운로드와 달리 내부 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 악성코드

	(가)	(나)	(다)
①	드로퍼	익스플로잇	랜섬웨어
②	드로퍼	랜섬웨어	익스플로잇
③	랜섬웨어	익스플로잇	드로퍼
④	랜섬웨어	드로퍼	익스플로잇

◦ 다운로드와 유사하게 새로운 악성코드를 생성하지만 다운로더가 외부에서 악성코드를 다운받는 것에 비해 드롭퍼의 경우 자신 내부에 포함되어 있는 데이터를 이용하여 악성코드를 생성한다는 차이점이 있다. 드롭되는 악성코드는 일반적으로 드롭퍼 내부에 압축/암호화된 형태로 존재하기 때문에 백신 프로그램을 통한 탐지가 어렵고 실제 실행을 해보지 않고서는 확인이 어렵다.

오답피하기 ③ 랜섬웨어는 중요 파일 등을 암호화 후 금전을 요구하는 악성코드이다. 취약점 공격 또는 익스플로잇(exploit)은 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램을 말한다.

정답 ③

5. ○△× 21.지방.9급

ISO 27001의 정보보호영역(통제분야)에 해당하지 않은 것은?

① 소프트웨어 품질 보증(Software Quality Assurance)
② 접근통제(Access Control)
③ 암호화(Cryptography)
④ 정보보안 사고관리(Information Security Incident Management)

ISO 27001:2013 정보보호 통제 항목

요구사항	내용
정보보호 정책	정보보호에 대한 경영방침과 지원사항을 제공하기 위함
정보보호 조직	조직 내에서 보호를 효과적으로 관리하기 위해서는 보호에 대한 책임을 배정
인적 자원 보안	사람에 의한 실수, 절도, 부정수단이나 설비의 잘못사용으로 인한 위험을 감소
자산 관리	조직의 자산에 대한 적절한 보호책 유지
접근 통제	정보에 대한 접근통제를 하기 위함
암호화	기밀성, 인증 또는 정보의 무결성을 보호하기 위해 암호화의 적절하고 효과적인 사용을 보장
물리적 환경적 보안	비인가된 접근, 손상과 사업장 및 정보에 대한 영향을 방지하기 위함
운영 보안	정보 처리 설비의 정확하고 안전한 운영을 보장하기 위함
통신 보안	네트워크 및 지원 정보 처리 시설의 안전한 통신을 보장하기 위함
정보 시스템 개발 유지보수	정보시스템 내에 보안이 수립되었음을 보장하기 위함
공급자 관계	협력업체(공급자)에서 접근가능한 조직 내 정보보호를 보장과 협력업체와의 계약에 따라 정보 보안 및 서비스 제공에 합의된 수준을 유지하기 위함
정보보안 사고 관리	보안사고에 대한 대응 절차의 수립 및 이행을 보장함
정보보호 측면 업무 연속성 관리	사업활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위함
컴플라이언스	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보호요구사항의 불일치를 방지하기 위함

오답피하기 ① ISO 27001 정보보호영역(통제분야)에 소프트웨어 품질 보증은 없다.

정답 ①

6. ○△× 21.지방.9급

암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키를 사용하는 것은?

① SEED
② ECC
③ AES
④ IDEA

오답피하기 ② 암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키(공개키, 개인키)를 사용하는 알고리즘은 공개키 알고리즘이다. SEED, AES, IDEA는 대칭키 알고리즘이고, ECC는 공개키 알고리즘이다.

정답 ②

7. ○△× 21.지방.9급

DoS(Denial of Service)의 공격유형이 아닌 것은?

① Race Condition
② TearDrop
③ SYN Flooding
④ Land Attack

오답피하기 ① 경쟁 상태(race condition) 공격은 유닉스 시스템에서 관리자 권한으로 실행되는 프로그램 중간에 임시 파일을 만드는 프로세스가 있을 경우 임시 파일 이름의 심볼릭 링크(Symbolic link) 파일을 생성하고, 이 프로세스 실행 중에 끼어들어 그 임시 파일을 전혀 엉뚱한 파일과 연결하여 악의적인 행동을 수행하도록 하는 공격으로 DDoS 공격과는 거리가 멀다.

정답 ①

8. ○△× 21.지방.9급

다음에서 설명하는 방화벽 구축 형태는?

보기

- ○ 배스천(Bastion) 호스트와 스크린 라우터를 혼합하여 사용한 방화벽
- ○ 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고 스크린 라우터와 내부 네트워크 사이에 배스천 호스트를 설치

① Bastion Host
② Dual Homed Gateway
③ Screened Subnet Gateway
④ Screened Host Gateway

오답피하기 ④ 스크린드 호스트 게이트웨이 구조(Screened Host Gateway)는 듀얼-홈드 게이트웨이와 스크리닝 라우터를 결합한 형태로 내부 네트워크에 놓여 있는 배스천 호스트와 외부 네트워크 사이에 스크리닝 라우터를 설치하여 구성한다.

정답 ④

9. ○△× 21.지방.9급

다음에서 설명하는 보안 기술은?

보기

○ 해시 함수를 이용하여 메시지 인증 코드를 구현한다.
○ SHA-256을 사용할 수 있다.

① HMAC(Hash based Message Authentication Code)
② Block Chain
③ RSA(Rivest-Shamir-Adleman)
④ ARIA(Academy, Research Institute, Agency)

오답피하기 ① HMAC은 SHA-1과 같은 일방향 해시함수를 이용하여 메시지 인증코드를 구성하는 방법이다. HMAC의 H는 Hash를 의미한다. HMAC에서는 사용하는 일방향 해시함수를 단 한 종류로 한정하는 것은 아니다. 강한 일방향 해시함수라면 뭐든지 HMAC에 이용할 수 있다.

정답 ①

10. ○△× 21.지방.9급

스미싱 공격에 대한 설명으로 옳지 않은 것은?

① 공격자는 주로 앱을 사용하여 공격한다.
② 스미싱은 개인 정보를 빼내는 사기 수법이다.
③ 공격자는 사용자가 제대로 된 url을 입력하여도 원래 사이트와 유사한 위장 사이트로 접속시킨다.
④ 공격자는 문자 메시지 링크를 이용한다.

◦ 스미싱(SMishing)은 SMS와 Phishing 공격이 결합된 용어로써, SMS를 통해 사용자를 속여 트로이목마 등 악성 소프트웨어 설치를 유도하고, 설치된 악성 소프트웨어를 통해 민감한 개인정보를 빼내거나 소액결재 등을 실행하여 금전적인 손해를 입히는 신종 휴대폰 사기수법이다.

오답피하기 ③ 합법적인 사용자의 도메인을 탈취하거나 도메인 네임 시스템(DNS) 또는 프락시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤 개인정보를 탈취하는 파밍 공격에 대한 설명이다.

정답 ③

11. ○△× 21.지방.9급

디지털 포렌식을 통해 획득한 증거가 법적인 효력을 갖기 위해 만족해야 할 원칙이 아닌 것은?

① 정당성의 원칙
② 재현의 원칙
③ 무결성의 원칙
④ 기밀성의 원칙

디지털 포렌식의 기본원칙
◦ 정당성: 디지털 자료증거는 적법한 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 ④ 디지털 포렌식의 기본 원칙에 기밀성의 원칙은 없다.

정답 ④

12. ○△× 21.지방.9급

「개인정보 보호법」상의 개인정보에 대한 설명으로 옳지 않은 것은?

① 개인정보 보호위원회의 위원 임기는 3년이다.
② 개인정보는 가명처리를 할 수 없다.
③ 개인정보 보호위원회의 위원은 대통령이 임명 또는 위촉한다.
④ 개인정보처리자는 개인정보파일의 운용을 위하여 다른 사람을 통하여 개인정보를 처리할 수 있다.

◦ 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.
◦ 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
◦ 개인정보처리자란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

오답피하기 ② 가명처리란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다. 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

정답 ②

13. ○△× 21.지방.9급

DoS 및 DDoS 공격 대응책으로 옳지 않은 것은?

① 방화벽 및 침입 탐지 시스템 설치와 운영
② 시스템 패치
③ 암호화
④ 안정적인 네트워크 설계

DDoS 대응 방안

유형	설명
라우터의 ACL 이용	ACL(Access Control List)을 이용한 필터링 방법, 공격 주소, 포트를 등록하여 사용한다.
라우터의 Ingress 필터링	Ingress 필터링이란 지정한 IP 도메인으로부터의 패킷만이 라우터를 통과하게끔 패킷을 필터링하는 것이다.
라우터의 Egress 필터링	IP 주소가 위조된 패킷이 인터넷으로 나가는 것을 ISP 단계에서 막을 수 있다.
라우터의 약속된 접근비율(CAR) 기능	단위시간 동안 일정량 이상의 패킷이 라우터로 들어올 경우 일정량 이상의 패킷은 통과하지 않도록 하는 기능을 CAR(Committed Access Rate)라 하는데, 이 기능을 이용하여 DDoS 패킷을 차단한다.
방화벽	방화벽의 포트 필터링 등을 통해 방지한다.
시스템 패치, 핫픽스(Hot Fix)	취약점/버그를 이용하는 악성코드 및 침입을 방지한다.
안정적인 네트워크 설계	취약시스템이 존재하지 않도록 설계하고, 단일실패지점인 SPoF(Single Point of Failure)가 존재하지 않도록 설계한다.
IDS 이용	IDS(Intrusion Detection System)에서 DDoS 공격을 탐지한다.
로드 밸런싱 (Load Balancing)	이중화, 삼중화 등 대용량 트래픽을 분산처리할 수 있고, 네트워크 대역폭 및 성능을 강화시키는 방법이다.
서비스 별 대역폭 제한	서비스별 대역폭을 제한하여 공격에 따른 서비스 피해를 최소화한다.

오답피하기 ③ 암호화는 도청, 스누핑 등 기밀성를 위협하는 공격에 대한 대응책이다.

정답 ③

14. ○△× 21.지방.9급

국제 공통 평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① CC는 국제적으로 평가 결과를 상호 인정한다.
② CC는 보안기능수준에 따라 평가 등급이 구분된다.
③ 보안목표명세서는 평가 대상에 해당하는 정보보호 시스템의 보안 요구 사항, 보안 기능 명세 등을 서술한 문서이다.
④ 보호프로파일은 보안 문제를 해결하기 위해 작성한 제품군별 구현에 독립적인 보안요구사항 등을 서술한 문서이다.

CC

◦ 정보보호시스템의 공통평가기준으로 현재 국내외에 널리 사용되고 있는 CC인증은 국가마다 상이한 평가기준을 연동시키고 평가결과를 상호인정하기 위해 제정된 평가기준으로 1999년 6월 ISO/IEC 15408 국제표준으로 승인되었다. CC인증은 미국의 TCSEC, 유럽의 ITSEC, 캐나다의 CTCPEC 등을 기반으로 개발되었으며, 각국에서 활용되고 있던 다양한 평가기준을 단일화하여 공통의 언어와 이해를 기반으로 한 CC를 개발하게 되었고 개발자 및 사용자 등 IT 제품 시장의 요구사항을 반영하여 발전해 왔다.

◦ 보증 수준을 표현하는 것이 CC의 보증등급이다. 사용자의 요구가 너무 다양하여 보안 기능요구사항에 대해서는 기능 등급을 표현하고 있지는 않지만 보증에 대해서는 사용자의 편의를 위해 EAL(Evaluation Assurance Level)이라는 보증 패키지를 제시하고 있다. EAL 등급이 어느 정도의 보증을 하는지에 대한 수치적인 표현은 어렵지만, EAL 등급이 높아지면 그 만큼 보증의 수준(확신)은 높아진다.

오답피하기 ② 보증 수준을 표현하는 것이 CC의 보증등급이다. 즉 CC는 보안보증수준에 따라 평가 등급이 구분된다.

정답 ②

15. ○△× 21.지방.9급

생체인증(Biometrics)에 대한 설명으로 옳지 않은 것은?

① 생체 인증은 불변의 신체적 특성을 활용한다.
② 생체 인증은 지문, 홍채, 망막, 정맥 등의 특징을 활용한다.
③ 얼굴은 행동적 특성을 이용한 인증 수단이다.
④ 부정허용률(false acceptance rate)은 인증되지 않아야 할 사람을 인증한 값이다.

오답피하기 ③ 얼굴은 행동적 특성이 아닌 생체적 특성을 이용한 인증 수단이다.

정답 ③

16. ○△× 21.지방.9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등)에 따른 정보보호 최고책임자의 업무가 아닌 것은?

① 정보보호 사전 보안성 검토
② 정보보호 취약점 분석·평가 및 개선
③ 중요 정보의 암호화 및 보안서버 적합성 검토
④ 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치

제45조의3(정보보호 최고책임자의 지정 등)
④ 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 ④ 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 정보통신서비스 제공자(집적정보통신시설 사업자)는

정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다. 즉 보기는 정보보호 최고책임자의 업무가 아닌 집적정보통신시설사업자의 업무이다.

정답 ④

17. ○△× 21.지방.9급

정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은?

① 인증기관 지정의 유효기간은 2년이다.
② 사후심사는 인증 후 매년 사후관리를 위해 실시된다.
③ 인증심사 기준은 12개 분야 92개 통제 사항이다.
④ 인증심사원은 2개 등급으로 구분된다.

◦ 사후심사란 인증을 취득한 기관이 수립하여 운영 중인 개인정보보호 관리체계가 인증기준에 적합하고 지속적으로 유지되고 있는지를 확인하기 위하여 인증 유효기간 중에 매년 1회 이상 시행하는 인증심사를 말한다.

오답피하기 ① 인증기관 및 심사기관 지정의 유효기간은 3년이며 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정을 신청을 할 수 있다. ③ ISMS-P 인증기준은 관리체계 수립 및 운영(16개), 보호대책 요구사항(64개), 개인정보 처리단계별 요구사항(22개)의 102개 통제항목으로 구성된다. ISMS-P 인증 수행 시 102개, ISMS 인증 수행 시 개인정보 처리단계별 요구사항 22개 통제항목을 제외한 80개 통제항목을 적용하여 인증심사를 수행한다. ④ 인증심사원은 심사원보, 심사원, 선임심사원으로 3개 등급으로 구분된다.

정답 ②

18. ○△× 21.지방.9급

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

① RSA를 이용하여 메시지 다이제스트를 서명한다.
② 세션키는 여러 번 사용된다.
③ 수신자는 자신의 개인키를 이용하여 세션키를 복호화한다.
④ 세션키를 이용하여 메시지를 암·복호화한다.

오답피하기 ② 세션키는 메시지 암·복호화에 사용하는 대칭키로 한 번만 사용된다.

정답 ②

19. ○△× 21.지방.9급

다음에서 설명하는 블록암호 운영 모드는?

보기
○ 단순한 모드로 평문이 한 번에 하나의 평문 블록으로 처리된다.
○ 각 평문 블록은 동일한 키로 암호화된다.
○ 주어진 하나의 키에 대하여 평문의 모든 블록에 대한 유일한 암호문이 존재한다.

① CBC(Cipher Block Chaining Mode)
② CTR(Counter Mode)
③ CFB(Cipher-Feed Back Mode)
④ ECB(Electronic Code Book Mode)

오답피하기 ④ 운영 모드 중에서 가장 간단한 모드는 ECB(electronic codebook) 모드이다. 평문은 N개의 n비트 블록으로 분할된다. 각 평문 블록은 동일한 키로 암호화되며 모든 평문 블록이 다른 경우 암호문 블록이 다르다. 그러나 ECB 방식은 평문의 블록 패턴과 암호문의 블록 패턴이 동일하게 유지되는 문제점을 안고 있다. 이러한 이유로 동일한 키로 여러 블록의 평문을 암호화할 때에는 ECB 방식의 사용을 권고하지 않으며, 보통 난수 발생과 같은 특수한 경우에 사용한다.

정답 ④

20. ○△× 21.지방.9급

BCP(Business Continuity Planning)에 대한 설명으로 옳지 않은 것은?

① BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.
② BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.
③ BIA는 조직의 필요성에 의거하여 시스템의 중요성을 식별한다.
④ DRP(Disaster Recovery Plan)는 최대허용중단시간(Maximum Tolerable Downtime)을 산정한다.

재난 복구 계획(DRP, Disaster Recovery Planning)
◦ 장기간에 걸친 재해나 재난으로 인해 피해 입은 시설의 접근거부와 같은 이벤트를 다룬다.
◦ 비상사태 발생 후 대체 사이트에서의 목표 시스템, 응용프로그램, 컴퓨터 설비의 운영재개와 같은 IT 중심의 계획을 말한다.

오답피하기 ④ 최대허용중단시간(MTD, Maximum Tolerable Downtime) 산정은 사업영향분석(BIA, Business Impact Analysis)에서 수행한다.

정답 ④