**정보보안기사**

**1장 정보보호 개요(~0720)**

시험 내용 전반에 적용되는 개념으로 출제 빈도도 높으니 확실하게 알아두자.

**최근 사이버 공격의 특징**

전파경로의 다원화, 공격의 초고속화, 분산화 및 에이전트화

**정보보호의 정의**

1. 정보의 수집, 가공, 저장, 검색, 송/수신 중에 발생하는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단, 또는 그러한 수단으로 이루어지는 행위
2. 정보보호는 기밀성, 무결성, 가용성, 인증성 및 부인방지를 보장하기 위해 기술적, 물리적, 관리적 보호대책을 강구하는 것이다.

**가장 쉬운 침투방법 선택 원리**

침투는 가장 분명한 수단으로 일어나는 것이 아니라 이용 가능한 모든 수단을 이용한다. 침투에 대한 강력한 대비책이 있어야 한다.

**정보보호 개념**

**기밀성**

|  |  |  |
| --- | --- | --- |
| **구분** | **개념** | **보안기술** |
| **기밀성(Confidentiality)** | 인가된(Authorized) 사람만이 허용된다. | 접근 제어, 암호화 |
| **무결성(Integrity)** | 정보는 절차와 권한에 따라서 변경한다. | 접근 제어, 메시지 인증, 침입 탐지, 백업 |
| **가용성(Availability)** | 인가된 사람은 정보를 적절히  이용할 수 있어야 한다. | 백업, 중복성 유지, 물리적 보호 |
| **인증성(인증, Authenticity)** | 진짜임을 확인/신뢰할 수 있어야 한다. | 메시지 출처 유효성 확증 |
| **책임추적성(책임성, Accountability)** | 개체의 행동을 추적해서 찾아낼 수 있어야 한다. 보안 침해의 책임이 있는 곳까지 추적해 활동 상황을 기록한다. 포렌식을 통해 보안 이슈를 해결 가능한 정도여야 한다. | **부인 봉쇄(부인 방지)**, 억제, 결함 분리, 침입 탐지 예방, 사후 복구, 법적 조치 |

**+ CIA Triad -> 기밀성, 무결성, 가용성으로 데이터 & 서비스 보호**

**OSI(Open System Interconnection) 보안구조**

* **보안 공격:** 정보 안전성을 침해하는 행위
* **보안 메커니즘:** 공격 탐지, 예방, 복구 절차
* **보안 서비스:** 하나 이상의 보안 메커니즘이 적용된 보안 강화 서비스

**세 종류의 보안 공격**

1. **기밀성 공격:** 스누핑, 트래픽 분석
2. **무결성 공격:** 변경(메시지 수정, Modification), 가장(Masquerading), 재연(재전송, Replaying), 부인(Repudiation -> 부인 방지(부인 봉쇄, Nonrepudiation)으로 방지 가능)
3. **가용성 공격:** 서비스 거부(Denial of Service), DoS 공격은 시스템 서비스를 느리게 하거나 차단한다.

**소극적 공격과 적극적 공격**

**소극적 공격:** 정보의 획득을 통해 기밀성을 침해하지만 시스템에는 영향을 미치지 않는다. 탐지보다 예방이 중요하다.

**적극적 공격:** 무결성과 가용성을 위협하는 공격. 데이터를 바꾸거나 시스템에 해를 입힌다. 방어보다 탐지가 쉽다.

|  |  |  |
| --- | --- | --- |
| **공격** | **수동/능동** | **위협 요소** |
| 스누핑, 트래픽 분석 | 수동 | 기밀성 |
| 변경, 가장, 재연, 부인 | 능동 | 무결성 |
| DoS | 능동 | 가용성 |

**기본 보안용어 정의**

* **자산:** 조직이 보호해야 할 대상. 자산 또는 데이터의 소유자가 가치를 부여한 실체
* **취약점(취약성, Vulnerability):** 허가되지 않은 접근자에게 오픈된 소프트웨어/하드웨어/절차 혹은 인력상의 약점. 기술적/물리적/관리적 약점을 말한다.
* **위협(Threat):** 가로채기(기밀성), 가로막음(가용성), 변/위조(무결성). 해를 끼치는 행동/사건의 집합
* **위험(Risk):** 자산 \* 위협 \* 취약점
* **노출(Exposure):** 위협으로 인해 손실이 발생할 수 있는 경우
* **대책/안전장치(Countermeasure/Safeguard):** 취약점을 제거하거나 노출을 감소시키기 위한 소프트웨어 설정, 하드웨어 장비, 또는 절차
* **다계층 보안/심층 방어(Defense in Depth):** Multi Layered(Level) Security라고도 불린다. 여러 계층의 보안 대책이나 대응 수단을 구성하는 것을 말한다. 한 가지 통제가 대응에 실패해도 전체 시스템을 위험에 빠뜨리지 않는 최선의 보호 방법이다. 보호, 탐지, 대응으로 이루어진다.
* **직무상의 신의성실, 노력(Due, Due Care, Due Diligence):** 특정 목적을 이루기 위한 의무, 주의, 노력을 말한다.
* **사회공학(Social Engineering):** 인간의 신뢰를 이용해 보안 절차를 깨트리는 침입 수단

**+보안은 불공정한 게임이다: 방어자는 모든 취약점을 다 알아야 하지만 공격자는 단 하나의 취약점만을 발견해도 된다.**

**+가장 약한 링크 원칙(Principle of weakness link): 보안은 가장 약한 링크보다 더 강할 수 없다. 단 하나의 취약점이 전체 시스템의 보안 실패로 이어질 수 있다.**

* **시점별 통제(Control, 빈출):** 예방통제, 탐지통제, 교정통제