**별첨3) 위협모델링 방법**

**Microsoft SDL 설계 단계**위협모델링 방법

**Step 1**  
위협 모델링을 수행하기 위해 보안팀 구성.  
 🡪 보안팀의 리더는 해킹 / 침해사고 분석 및 대응 전문가가 적합

**Step 2**  
애플리케이션 분해 작업 수행.  
 🡪 위협 모델링을 수행해야 하는 애플리케이션에 대해   
 기능과 데이터 흐름을 기준으로 애플리케이션을 분해함.

**Step 3**  
위협 추출

🡪 STRIDE 위협 유형 기준으로 분류

|  |  |
| --- | --- |
| 신분 위장(**S**pooping Identity) | 거짓된 Identity를 이용하여 시스템 접근 권한 획득 |
| 데이터 변조(**T**ampering with data) | 불법적인 데이터 수정 |
| 부인(**R**epudiation) | 사용자가 자신이 수행한 특정 액션이나 트랜잭션을 부인. |
| 정보유출(**I**nformation Disclosure) | 유출되지 않아야 하는 개인 정보 유출 |
| 서비스 거부(**D**enial of Serice, DoS) | 시스템 또는 애플리케이션이 정상적으로 수행되지 않도록 한다. |
| 권한 상승(**E**levation of Privilege) | 제한된 권한을 가진 사용자가 다른 사용자의 권한을 습득하여 원하는 기능을 수행. |

**Step 4**  
도출된 위협에 대한 위험도 계산  
 🡪 DREAD 위험도 분류 이용, 가장 위협적인 요소들이 먼저 제거될 수 있도록 한다.

|  |  |
| --- | --- |
| 예상 피해(**D**amage potential) | 피해가 얼마나 클 것인가. |
| 재현 확률(**R**eproducibility) | 공격이 성공할 확률이 얼마인가 |
| 공격 용이도(**E**xploitability) | 공격을 위해 얼마나 많은 노력과 기술이 필요한가. |
| 영향을 받는 사용자(**A**ffected users) | 위협으로부터 얼마나 많은 사용자가 영향을 받는가. |
| 발견 용이성(**D**iscoverability) | 얼마나 쉽게 취약성이 발견되는가. |

**별첨3) 위협모델링 방법**

**Step 5**  
대응 기법 선택  
 🡪 위협모델링을 통해 해당 위협이 발생했을 때 대응 방법에 대한 정의도 함께 요구됨.   
 일반적으로 침해 사고가 발생한 경우 대응 방법은 아래의 대응기법 중 하나가 될 수 있다.

|  |  |
| --- | --- |
| 문제점 무시 | 문제점을 무시하고 아무런 대응도 하지 않는다. 불가피한 사유로 아무런 대응을 하지 않기로 했다면, 위협에 관련된 기능을 기본적으로 비활성화 상태로 설치할 수 있는지 고려해야 한다. |
| 문제점 알림 | 사용자에게 문제점을 알리고 사용자로 하여금 그 기능을 사용할 것인지사용하지 않을 것인지 결정할 수 있도록 한다. |
| 문제점 제거 | 문제점을 고칠 시간이 없고, 보안 위험도가 충분히 높다면, 그 기능을 삭제하는 것을 진지하게 고려해야 한다. |
| 문제점 수정 | 가장 분명한 해결책. 기술적으로 문제를 고치는 것이지만 현실적으로 가장 어려운 방법인 경우도 있다. |

**Step 6**  
대응 기술 선택  
 🡪 도출된 각 위협들을 제거하기 위해 요구되는 기술들을 도출

|  |  |
| --- | --- |
| 위협의 종류 | 대응 기술 |
| 신분 위장(Spooping Identity) | 적절한 인증(패스워드, 비밀키, 홍채인식, 지문 등)  패스워드는 저장하지 않음.  Cookie Authentication  Kerberos Authentication  PKI 시스템 (SSL/TLS 이용)  전자서명 |
| 데이터 변조(Tampering with data) | 해쉬  ACLSs  Message authentication codes  전자서명 |
| 부인(Repudiation) | 전자서명  감사로그 |
| 정보유출(Information Disclosure) | Privacy-enhanced 프로토콜  암호화  ACLs |
| 서비스 거부(Denial of Serice, DoS) | ACLs  필터링  Throttling  Quality of service |
| 권한 상승(Elevation of Privilege) | 최소한의 권한으로 실행  Group of role membership  Input validation |