**별첨5) 구현단계 보안활동에 대한 점검**

**개발환경 보안(네트워크) 구현사항 점검 목록 예**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **리뷰 항목** | **중요도** | **적용 여부** | **특이사항** | **보완 계획** | **비고** |
| 1. 네트워크 정책 운영 | | | | | |
| 경계영역 구분 정책 | 매우 중요 |  |  |  |  |
| 인바운드 및 아웃바운드 정책 | 매우 중요 |  |  |  |  |
| 최소권한 원칙 정책 | 매우 중요 |  |  |  |  |
| 히스토리 관리 정책 | 매우 중요 |  |  |  |  |
| 2. 네트워크 분리 및 DMZ 구성 | | | | | |
| 개발/운영 망 분리 | 매우 중요 |  |  |  |  |
| DMZ 구성 | 매우 중요 |  |  |  |  |
| 3. 침입탐지/침입차단시스템 적용 및 보안 관리 | | | | | |
| 침입탐지/침입차단시스템을 통한 접근통제 및 모니터링 | 매우 중요 |  |  |  |  |
| 침입탐지/침입차단시스템 Rule 보안 | 매우 중요 |  |  |  |  |
| 4. DB Zone 분리 진단 | | | | | |
| DB Zone 구성 | 매우 중요 |  |  |  |  |
| DB Zone 접근 통제 | 매우 중요 |  |  |  |  |
| 5. 데이터 전송 보안 적용 | | | | | |
| 중요 정보 암호화(SSL, VPN 등)적용 | 중요 |  |  |  |  |
| ○ : 적용됨 ◇ : 부분 적용 X : 적용 안 됨 N/A : 해당사항 없음 | | | | |  |

**개발환경 보안(서버) 구현사항 점검 목록 예**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **리뷰 항목** | **중요도** | **적용 여부** | **특이사항** | **보완 계획** | **비고** |
| 1. 네트워크 서비스 보안 관리 | | | | | |
| 불필요한 네트워크 서비스 중지 및 관리 | 매우 중요 |  |  |  |  |
| 2. 기본 시스템 보안 설정 및 보안 패치 | | | | | |
| Banner 수정 | 중요 |  |  |  |  |
| 시스템의 불필요한 권한 설정 제거 | 매우 중요 |  |  |  |  |
| 최신 시스템 취약점에 대한 대응조치 등의 시스템 Hardening | 중요 |  |  |  |  |
| 시스템OS 및 서비스 소프트웨어에 대한 최신 보안 패치 적용 | 중요 |  |  |  |  |
| 3. 사용자 계정 관리 | | | | | |
| 불필요한 디폴트계정 통제 및 사례 | 매우 중요 |  |  |  |  |
| 4. 악성코드 차단 | | | | | |
| 최신 백신 소프트웨어 설치 | 매우 중요 |  |  |  |  |
| 백신 실시간 감시 적용 | 매우 중요 |  |  |  |  |
| ○ : 적용됨 ◇ : 부분 적용 X : 적용 안 됨 N/A : 해당사항 없음 | | | | |  |

**애플리케이션 보안 설계 구현 사항 점검 목록 예**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **리뷰 항목** | **중요도** | **적용 여부** | **특이사항** | **보완 계획** | **비고** |
| 1. 보안 요구사항 | | | | | |
| 프로그램 입력 검토 | 매우 중요 |  |  |  |  |
| Race Condition 발생방지 | 매우 중요 |  |  |  |  |
| 버퍼 오버 플로우 발생 방지 | 매우 중요 |  |  |  |  |
| 소스코드내부에 민감한 정보 삽입 금지 | 매우 중요 |  |  |  |  |
| 소스코드내부에 악성 코드 삽입 금지 | 매우 중요 |  |  |  |  |
| 실행결과의 예외 처리 | 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 2. 로그인 관리 | | | | | |
| 로그인 실패시 원인 표기 제한 | 매우 중요 |  |  |  |  |
| 잘못된 패스워드 입력 회수 제한 | 중요 |  |  |  |  |
| 최근 로그인 정보 표시 | 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 3. 패스워드 관리 | | | | | |
| 패스워드 최소 길이 제한 | 매우 중요 |  |  |  |  |
| 추측 가능한 패스워드 사용 제한 | 매우 중요 |  |  |  |  |
| 패스워드 변경 및 확인시 보안 적용 | 중요 |  |  |  |  |
| 패스워드 사용기간 적용 | 중요 |  |  |  |  |
| 인증강화 | 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 4. 사용자 계정 관리 | | | | | |
| 추측 가능한 디폴트 계정 사용 통제 | 매우 중요 |  |  |  |  |
| 불필요한 계정에 대한 주기적 검토 밑 삭제 | 매우 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 5. 데이터 및 DB보안 관리 | | | | | |
| 주요 데이터 및 자료 파일 등 DB 저장 유무 | 매우 중요 |  |  |  |  |
| 데이터의 보안 등급 분류 설정 | 매우 중요 |  |  |  |  |
| 암호화 Key 관리 정책 | 매우 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 6. 애플리케이션 접근 제어 관리 | | | | | |
| 사용자 그룹별 접근 제한 통제 | 중요 |  |  |  |  |
| 관리자 접근 통제 | 매우 중요 |  |  |  |  |
| 다중 접근 제한 | 매우 중요 |  |  |  |  |
| 인증절차를 우회한 접근 통제 | 매우 중요 |  |  |  |  |
| … | … |  |  |  |  |
| 7. 로그 관리 및 접근 통계 | | | | | |
| 보안 등급별 로깅 설정 | 매우 중요 |  |  |  |  |
| 보안 등급별 로그 보관 기간 설정 | 매우 중요 |  |  |  |  |
| 로그 접근 통제 | 매우 중요 |  |  |  |  |
| … | … |  |  |  |  |

○ : 적용됨 ◇ : 부분 적용 X : 적용 안 됨 N/A : 해당사항 없음