**회의록**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 회의일시 | 2021년 04월 22일 | 팀명 | 대장님과 아이들팀 | 작성자 | 김한진 |
| 참석자 | 김한진, 공경선, 금소영, 김동관, 김범, 서용석, 최병섭 | | | | |

|  |  |
| --- | --- |
| 회의안건 | **1. 시나리오 요소 분석 | 클라우드 보안 부분**  **2. 시나리오 요소 분석 | 데이터 보안 부분** |

|  |  |  |
| --- | --- | --- |
| 회의내용 | 내용 | 이슈 / 비고 |
| **1. 가용성 및 네트워크 영역**  1) A저축은행 멤버스 및 서비스를 퍼블릭 클라우드로 마이그레이션  => A저축은행 멤버스 서비스 웹사이트 클라우드 이전과 보안  -> 데이터보안반  => A저축은행 고객 데이터 클라우드 이전과 보안  => 웹 사이트와 데이터베이스의 동기화 및 백업 전략과 재해복구 전략  -> 데이터보안반  => 2개 이상의 퍼블릭 클라우드를 통한 가용성 영역  2) 2개의 퍼블릭 클라우드 플랫폼으로 가용성 영역을 확보할 것  =>AWS + Azure 로 예상  3) 2개의 퍼블릭 클라우드 플랫폼에 문제가 있을 경우 A저축은행의 Backup 시스템에 의하여 시스템을 복구한다.  =>서비스를 복구할 동안 임시로 A저축은행 데이터센터에서 멤버스 서비스를 임시로 웹 서비스한다.  ->A저축은행의 온프레미스 시스템이 임시로 서비스를 이양받을 경우 데이터베이스는 A저축은행 데이터센터의 데이터베이스를 메인으로 사용한다.  =>비상시 클라우드 <--> 온프레미스 전환 기능이 요구되는 것으로 보이며, 이에 대해 구현방식에 대해 추가 논의가 필요해 보인다.  =>AWS + Azure 로 예상한다. |  |
| **2. 보안 및 감사영역**  1) DDoS공격과 SQL 인젝션 공격등에 대한 대비가 있어야한다.  2) 웹 사이트 및 데이터베이스에 대한 성능에 대하여도 1일, 1주, 1달을 주기로 성능 보고서를 생성한다. (컴퓨팅 자산 보고서 자동화)  =>WAF 상품 사용 및 설정  ->SQL 인젝션 치트 시트처럼 보편적인 WAF 룰설정에 대한 관련 자료가 있을 것으로 기대하고 있다.  =>AWS에 DDoS 방어 특화 상품 있는 것으로 알고 있다.  =>주기적 이라는 요소에 대한 방법에 대해 알아봐야할 듯 하다.  =>보고서 방식은 간단하게 CSV형식의 파일정도로 고려중이다.  3) 주기적으로 감사 보고서를 생성하고 이상 탐지가 있을 경우 자동 조치 후 보고서를 생성하여 메일로 관리자에게 보낸다. (비정상 이벤트에 대한 관리 자동화 및 주기적 보고서 작성 자동화)  =>WAF 및 방화벽 상품과 연동하는 방향으로 접근해야 할 것으로 보인다.  =>자동 메일서비스가 관건으로 보인다.  =>주기적 이라는 요소에 대한 방법에 대해 알아봐야할 듯 하다.  =>보고서 방식은 간단하게 CSV형식의 파일정도로 고려중이다.  4) 웹 사이트와 데이터베이스에 비 정상적인 접근 및 사용이 탐지될 경우 관리자에게 메일을 보내고, 이를 자동으로 간단한 조치를 취할 수 있어야 한다. (비정상 이벤트에 대한 관리 자동화)  =>WAF 및 방화벽 상품과 연동하는 방향으로 접근해야 할 것으로 보인다.  =>자동 메일서비스가 관건으로 보인다.  ->파이썬을 통한 메일서비스 관련 프로토콜(SMTP) 사용관련 자료를 확인  =>보고서 방식은 간단하게 CSV형식의 파일정도로 고려중이다.  [공통요소]  =>1일, 1주, 1달을 주기로 보안 보고서를 생성한다.  =>웹 사이트 및 데이터베이스에 대한 성능에 대하여도 1일, 1주, 1달을 주기로 성능 보고서를 생성한다.  -> python으로 구현할 것 같은데 멘토님의 도움 많이 필요할 것으로 예상된다.  -> 관리자에게 메일 : csv파일로 저장된걸 보내는지, 발생했다는 사실만 보내야 하는지에 대해 추가 논의가 필요하다. |  |
| **3. 개발환경영역**  7. A저축은행 내 개발 팀은 클라우드내에서 별도의 개발환경 및 테스트 환경을 사용하고 개발 및 테스트가 완료되면 실제 서버에 배포한다.  =>DevOps 관련 사항 (?)  =>배포까지 해야 하기에 컨테이너 기반으로 개발하여야 할 것으로 보인다.  ->가상의 웹서버 및 WAS(를 따로 구축한다면)도 컨테이너 형식으로 접근? |  |
| **4. 법률 및 정책**  1)고객데이터  =>고객데이터는 개인정보이기 때문에 국내법과 감사 정책등을 갖추어야 한다.  =>데이터센터 데이터베이스와 동기화 되어야 한다. 동기화할 때에도 보안과 감사 정책이 있어야 한다.  ->관리적 정책 + 기술적 정책  ->법관련 요소가 함유되어있음  ->**고객 데이터의 종류에 무엇이 있을지 고려해야함 <= 비식별화와 암호화 범위에 영향이 있을 것으로 보임** |  |
| **5. 이벤트 탐지 및 조치에 대하여**  1) SQL injection, DDoS 외의 우리들이 배운 요소들에 대해서도 탐지룰에 적용할 것  =>예) XSS, CSRF, SSRF, 스니핑, 스푸핑, TCP/SYN Flooding, apt 공격, http post attack, Slowloris attack  2) 이벤트 탐지를 이용한 자동보안 조치하는 방법에 대해 추가조사가 필요하다.  3) Secure Coding 이라는 항목에 대해 추가정보가 필요하다. |  |
| **6. 의문사항**  1) 과연 우리가 ELK 구축까지 감당할 수 있을까?  2) AWS에 두현할 모니터링 기능도 Azure에 동일하게 구현을 해야 하는가?  3) AWS에 구현한 모든 기능들을 Azure에 동일하게 구현을 해야 하는가?  4) DevOps 인가, DevSecOps 인가? <= 구현요소와 난이도에 영향이 있을 것으로 예상 |  |

|  |  |  |
| --- | --- | --- |
| 결정사항 | 내용 | 진행일정 |
| 1. 고가용성을 위해 멀티 클라우드로 구축 | 2021-04-22 |
| 2. 고객 데이터는 비식별화 한다. | 2021-04-22 |
| 3. 기획서 초안 작성 | 2021-04-22 |
|  |  |