위험분석 보고서

아래 학번과 이름을 기재한다. 그 다음 양식 번호 1장에서 7장까지 내용을 작성한다. 빨간색으로 기술한 도움말(작성요령)을 참고하여 작성한다. 실제 보고서 제출 시에는 지금 이 설명 박스와 아래 빨간색 작성요령은 모두 삭제한다. 작성요령에서 설명 안 한 부분은 적당히 기업 상황을 가정하여(해당 가정사항을 1장 또는 2장에 기술해주세요) 작성한다. 판단하기 애매한 경우는 교수에게 질문 후 작성한다.

학번: 20190937

이름: 이혜린

1. 기업 배경 설명

선정한 기업은 은행이다. 은행의 비즈니스는 예금을 받거나 유가증권 또는 그 밖의 채무증서를 발행하여 불특정 다수인으로부터 채무를 부담함으로써 조달한 자금을 대출하는 것이다. 은행에서 가장 중요하게 생각하는 비즈니스 목표는 사람들의 자산을 관리해주는 것이고 사람들마다 보유한 자산이 다르기 때문에 이를 관리해주기 위해 정보시스템이 필요하며 이 정보시스템이 침해당할 경우 사람들이 각자의 자산을 정당하게 찾을 수 없게 되므로 은행에서 보안은 매우 중요하다.

2. 기업 환경 가정사항

1) 계정계 (Core Banking)

계정계란 계정(통장)을 관리하는 시스템을 일컫는다. 계정계 시스템은 공통업무, 수신업무, 신탁업무, 보험업무, 카드업무, 여신업무, 외환업무, 대행업무 시스템 등으로 구성된다.

한 사람이 여러 개의 통장을 만들 수도 있고, 죽은 사람의 통장도 있기 때문에 통상적으로 기본 데이터가 1억건을 넘는다. 통장별 거래 기록을 포함하면 수백억 건의 데이터가 보통 존재한다. 은행의 핵심 업무를 담당하고 있기 때문에 데이터를 2중, 3중으로 백업하고 보수적으로 운영된다.

대부분 마스터 테이블인 거대한 원장들이 있고, 다양한 업무를 처리하는 정형화된 트랜잭션들이 있다. 원장에 트랜잭션이 집중되는 구조이기 때문에, 안정적으로 트랜잭션을 처리하기 위한 미들웨어가 발달해 있다.

2) 정보계

고객정보, 분석정보, 영업정보, 기업전략 정보 등을 다루는 정보시스템이다. 거래활동 및 성과 측정 및 분석을 위한 목적으로 구축된다. 주요 시스템으로 수익관리, 고객관계관리, 성과관리, 위험관리 시스템 등이 있다.

기본적으로 정보연계, 통합조회, 통계분석 등을 많이 하기 때문에 관계형 데이터베이스 사용이 필수이다. 분석을 위한 데이터 동기화기술도 사용된다. Java 기반으로 구축되었으며, 최근에는 빅데이터 기술도 검토되고 있다.

3) 대외계

대외계란 은행 외부기관과의 연계업무를 처리하기 위한 시스템이다. 연계업무란 은행간 송금, 수표조회 같은 은

행간 업무를 말한다. 주요 연계시스템으로는 인터넷뱅킹, 텔레뱅킹, 펌뱅킹, ATM 등이 있다. 거래내역 기록 및 검증, 프로토콜 변환, 오류시 재전송 기능까지 매우 복잡한 구조로 만들어져 있다. 대용량 처리보다 정확성, 안정성에 중점을 준 트랜잭션 허브들이 도입되어 있다.

4) 운영계

운영에 관계된 시스템이 모였다. 통합관제, 네트워크 모니터링 등을 운영계라고 부른다.

5) 기업업무 시스템

회계, 인사, 세무 시스템 등이 있다. 백오피스라고도 부른다.

3. 자산 분석

표 1 - 자산 목록표

자산코드	자산유형	자산명	보관위치	자산평가 등급	책임자
A1	서버	계정계 DB 서버	상암 데이터센터	VH	강동원
A2	시설	부산 재해복구센터 A동	부산 재해복구센터	H	이재현
A3	네트워크 장비	통신망	분당 데이터센터	M	조규성
A4	토큰	고액 이체를 위한 OTP	판교 본사	H	이주연
A5	소프트웨어	인터넷 뱅킹 시스템	판교 본사	L	이진욱

표2 - 자산의 가치 평가 기준

가치평가	평가 적용 기준
VH	핵심 서비스 중단 및 개인정보의 상당한 노출, 경제적 손실이 매우 치명적인 수준
H	핵심 서비스 일부 중단 및 개인 정보의 노출, 경제적 손실이 어느 정도 치명적인 수준
M	핵심 서비스 중단이 없고 개인 정보의 노출, 경제적 손실이 크게 치명적인 수준은 아닌 경우
L	핵심 서비스가 관련되지 않으며 경제적 손실이 경미한 수준

4. 취약점 분석

표3 - 취약점 평가 기준

평가	평가 적용 기준
VH	핵심 서비스 중단 및 개인정보의 상당한 노출, 경제적 손실이 매우 치명적인 수준
H	핵심 서비스 일부 중단 및 개인 정보의 노출,

	경제적 손실이 어느 정도 치명적인 수준
M	핵심 서비스 중단이 없고 개인 정보의 노출, 경제적 손실이 크게 치명적인 수준은 아닌 경우
L	핵심 서비스가 관련되지 않으며 경제적 손실이 경미한 수준

표4 - 자산별 취약점 조사

자산코드	자산명	취약점
A1	계정계 DB 서버	네트워크 접근 통제 미비
A2	부산 재해복구센터 A동	지진 발생 가능
A3	통신망	망분리 안함
A4	고액 이체를 위한 OTP	출입 통제 관리 시스템 미비
A5	인터넷 뱅킹 시스템	침해사고 모의훈련 미비

5. 위협 분석

표5 – 자산/취약점/위협 연관표

자산코드	자산명	취약점	위협
A1	계정계 DB 서버	네트워크 접근 통제 미비	외부인에 의한 DB정보 탈취 및 변경 가능
A2	부산 재해복구센터 A동	지진 발생 가능	지진에 의한 백업 데이터 소실 가능
A3	통신망	망분리 안함	외부인의 내부망 침투 및 법적 과태료 부과
A4	고액 이체를 위한 OTP	출입 통제 관리 시스템 미비	외부인에 의한 OTP 탈취 가능
A5	인터넷 뱅킹 시스템	침해사고 모의훈련 미비	해킹으로 인한 인터넷 뱅킹 시스템 마비

표 6 - 위협 평가 기준

평가	발생주기 또는 발생 가능성
VH	시스템의 생명주기 동안 매우 자주 발생함 (3개월 이내)
H	시스템의 생명주기 동안 다섯 번 이상 발생할 수 있는 상태 (6개월 이내)
M	시스템 자산의 생명주기 동안 두세차례 손해를 입을 수 있는 상태 (1년 이내)
L	자산의 생명주기 동안 거의 발생하지 않음

6. 위험 평가

표7 – 위험분석표

순번	이슈구분	자산	취약점	위협	자산평가(가치)	취약점 평가 (심각도)	위협 평가(발생가능성)	위험도	위험등급	보호대책	해결방안
1	기술적 이슈	계정계 DB 서버	네트워크 접근 통제 미비	외부인에 의한 DB 정보 탈취 및 변경 가능	VH	VH	M	8	1	2.6.1 네트워크 접근	데이터베이스 서버의 IP 주소를 사설 IP 로 할당하고 네트워크 영역들을 분리하는 등 네트워크 접근 통제 정책을 적용한다.
2	물리적 이슈	부산 재해복구센터 A 동	지진 발생 가능	지진에 의한 백업 데이터 소실 가능	H	H	L	5	2	2.4.4 보호설비 운영	재해복구센터가 백업데이터를 잘 보관하게 하기 위해 건물을 면진설계하고, 항온항습기를 설치하고 2 중 전력망을 구성하는 등 보호설비를 운영한다.
3	법적 이슈	통신망	망분리 안함	외부인의 내부망 침투 및 법적 과태료 부과	VH	VH	M	8	1	2.6.7 인터넷 접속 통제	정보통신망법에 따라 인터넷 망분리 의무가 있으므로 안전한 방식으로 망 분리를 적용한다.
4	물리적 이슈	고액 이체를 위한 OTP	출입 통제 관리 시스템 미비	외부인에 의한 OTP 탈취 가능	VH	VH	M	8	1	2.4.2 출입 통제	보호구역을 지정하고, 출입 가능 임직원을 식별하고 관리하며, 출입통제장치를 설치하고, 출입 기록을 보존한다.
5	관리적 이슈	인터넷 뱅킹 시스템	침해사고 모의훈련 미비	해킹으로 인한 인터넷 뱅킹 시스템 마비	VH	H	M	7	2	2.11.4 사고대응 훈련 및 개선, 2.12.1 재해·재난 대비 안전조치	해킹이 이루어졌을 경우를 대비하여 모의훈련 계획을 수립하고 연 1 회 이상 실시하고 복구 절차를 계획한다.

1

계정계 DB 서버의 자산평가는 VH이다. 계정계 DB 서버에는 사람들이 각자의 통장에 얼마나 자산이 들어있는지에 대한 정보가 들어있는 매우 중요한 데이터베이스이고, 해당 정보가 변경되면 은행의 의미가 무색해질 수도 있는 중요한 정보이기 때문에 VH를 주었다.

DB 서버에 공인 IP를 할당하고, 네트워크 접근 차단이 되어 있지 않은 취약점에 대한 평가도 VH이다. 사설 IP를

할당하지 않으면 외부인이 해당 서버에 접근하여 정보를 변경하거나 탈취해갈 수 있을 가능성이 생겨서 매우 중요한 취약점이라고 생각하여 VH를 주었다.

외부인에 의한 DB 정보 탈취 및 변경 가능 항목에는 위협 평가를 M으로 주었다. 아무리 공인 IP를 설정하였다고 하여도 은행 서버이기 때문에 정보를 변경하거나 가져가면 벌금을 물 수 있게 되기 때문에 쉽게 누군가가 해당 행위를 실천할 것 같지 않아서 M을 주었다.

2

부산 재해복구센터 A동에 대한 자산평가는 H이다. 아무래도 백업 데이터를 보관하는 곳이라서 VH까지는 무리가 있을 것 같고 그래도 백업 데이터가 재해 발생 시에는 중요한 역할을 하기 때문에 H를 주었다.

지진 발생 가능에는 취약점 평가를 H를 주었다. 아무래도 지진 진도가 작은 경우 위협적이지 않아 VH까지는 무리가 있을 수 있을 것 같다. 하지만 해당 건물에 위협적일 만큼 지진이 날 경우 백업데이터가 날아갈 수 있기 때문에 H를 주었다.

위협 평가는 L를 주었다. 아무래도 해당 건물이 흔들려서 안에 있는 서버, 백업 테이프 등 정보 자산들이 영향을 받을만큼 지진이 크게 날 가능성이 아직까지는 우리나라에 그렇게 자주 발생되는 것 같지는 않아서 L를 주었다.

3

통신망에 대한 자산 평가는 VH를 주었다. 통신망은 아무래도 기업이 항상 쓸 수 밖에 없는 자산으로 장애가 생기거나 보안이 취약하면 매우 위험할 수 있는 자산이므로 VH를 줄 수 밖에 없었다.

망분리 안함에 대한 취약점 평가는 VH를 주었다. 망분리를 하지 않으면 외부인이 내부 시스템에 침투하여 정보가 노출되거나 변경되거나 파괴될 수 있고, 망분리 의무 대상자의 경우 망분리를 하지 않았을 경우 법적으로 과태료가 3천마원 정도 부과될 수 있으며, 이는 기업이미지 하락 및 매출 손실로 이어질 수 있는 부분이기 때문에 VH를 주었다.

위협 평가는 M을 주었다. 아무래도 외부인이 함부로 은행 내부망을 침입하려는 시도 자체를 적게 할 것 같았고, 법적으로도 처벌을 받을 수 있는 행위이기 때문에 웬만해서는 잘 안할 것 같아서 M을 주었다.

4

고액 이체를 위한 OTP에 대한 자산 평가는 VH를 주었다. 아무래도 OTP가 정당한 주인이 아닌 사람에게 넘어가면 해당 사람이 자신의 자산이 아님에도 불구하고 돈을 함부로 쓸 수 있는 일이 벌어질 수 있기 때문에 VH를 주었다.

취약점 평가는 H를 주었다. OTP는 금고에 보관된다고 하는데, 이 금고가 있는 보호구역에 대한 출입 통제 관리 시스템이 미비하면 외부인도 들어가서 마음대로 OTP를 가져가거나 할 수 있게 되기 때문에 높은 취약점 평가를 주었다.

외부인이 OTP를 가져갈 수 있게 된다는 점에 대한 위협 평가는 M를 주었다. 아무리 출입통제시스템이 미비하다고 하더라도 은행 본사에 들어가서 보호구역까지 가서 금고에서 OTP를 꺼내가는 것은 아무래도 힘이 드는 일일 것 같아서 M을 주었다.

5

인터넷 뱅킹 시스템에 대한 자산 평가는 VH를 주었다. 보통 대면 은행이 상대적으로 일찍 문을 닫기 때문에 요

새 인터넷 뱅킹 시스템을 이용하는 사람들이 늘어나고 있는데 이것이 문제가 생기면 사회적으로도 큰 손실이 생길 것이기 때문에 VH 를 줄 수 밖에 없었다.

모의훈련 미비에 대한 취약점 평가는 H를 주었다. 아무래도 재해 발생 시에 대한 모의 훈련이 되어있지 않으면 아무리 예방을 철저히 해도 사고가 발생했을 때 당황해서 사고 대응 및 복구 절차를 제대로 실시할 수 없을 수가 있기 때문에 H를 주었다.

해킹으로 인한 인터넷 뱅킹 시스템 미비에 대한 위협 평가는 M를 주었다. 요새 인터넷을 사용하지 않는 기업들이 없어서 그런지 해킹 사고가 증가하고 있는 상황이지만 아무래도 기술이 어느정도 필요로 하는 사고라 자주 발생하는 것 같지는 않아서 M를 주었다.

표8 - 위험 등급 결정 기준표

등급	위험도 기준
1등급	8~10
2등급	4~7
3등급	1~3

DOA는 위험도 8로 하였다. 계정계 데이터베이스 서버가 공인 IP 할당을 하지 않고 네트워크 접근 통제 정책을 사용하지 않아 외부인에 노출이 될 수 있다는 점이라던지 망분리 의무 대상자인데 망분리를 하지 않아 외부인이 내부망을 침투할 수 있고 법적 과태료를 물 수 있는 상황이라던지, 출입통제관리시스템이 부족하여 외부인이 고액 이체를 위한 OTP를 가져갈 수 있는 상황에 대해서는 보호대책이 꼭 필요할 것 같아서 DOA를 8로 정하였다. 위험도 4~7은 위험은 하지만 보호대책이 당장 마련되어야할 정도는 아닌 것 같아서 2등급으로 설정하였고, 위험도가 1~3 은 위험하지 않은 것은 아니지만 그렇다고 크게 경제적 사회적으로 문제되지도 않을 부분이라 3등급으로 정하였다.

7. 보호대책 선정

1

보호대책: 2.6.1 네트워크 접근

계정계 데이터베이스 서버 등 일부 중요 서버의 IP 주소가 내부 규정과 달리 공인 IP 로 설정되어 있고, 네트워크 접근 통제가 적용되어 있지 않은 경우이다. 이 때 중요 서버는 사설 IP 를 할당하여 외부에서 직접 접근이 불가능하도록 설정하여야 한다. IP 주소 할당 현황을 최신으로 유지하고, 외부에 유출되지 않도록 대외비로 안전하게 관리한다. 외부에 내부 주소체계가 노출되지 않도록 내부 네트워크에서 사용하는 IP 주소와 외부에 드러나는 주소를 다르게 유지할 수 있는 NAT(Network Address Translation) 기능을 적용한다. 국제표준에 따른 사설 IP 주소 대역 중 C Class(192.168.0.1 ~ 192.168.255.255)를 사용한다. 네트워크 접근 통제를 위해 공개서버는 DMZ 에 두도록 하고, DMZ 를 경유하지 않은 인터넷에서 내부 시스템으로의 직접 연결은 차단한다. 서버팜, 데이터베이스팜, 운영자 환경, 개발 환경, 외부자 영역 등 네트워크 영역들을 분리한다. 분리된 네트워크 영역 간에는 침입차단시스템, 네트워크 장비 ACL 등을 활용하여 네트워크 영역 간 업무수행에 필요한 서비스의 접근만 허용하도록 통제한다. 물리적으로 떨어진 상암 데이터센터와 판교 본사 간의 네트워크 연결 시 전용회선 또는 가상사설망을 활용하여 안전한 접속 환경을 구성한다.

2

보호대책: 2.4.4 보호설비 운영

재해·재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 외부 집적정보통신시설(IDC)에 백업 데이터를 보관하도록 한다. 부산 재해복구센터에 진도 8.0 에도 견딜 수 있는 면진 설계를 한다. 또한, 외부의 바람을 이용해 수많은 서버의 열을 식히고 습도를 유지하는 풍도를 갖추도록 한다. 전력망을 2 중으로 갖추고, SKB, LGU, KT 등 세 회사의 통신망을 이용하여 한 회사의 통신망이 장애가 나도 다른 회사의 통신망을 이용하도록 한다. 그 외에도 화재감지 및 소화설비, 누수감지기, UPS, 비상발전기, 전압유지기, 접지시설, CCTV, 침입 경보기, 출입통제시스템, 비상등, 비상로 안내표지 등을 구비한다.

3

보호대책: 2.6.7 인터넷 접속 통제

정보통신망법에 의해 전년도 말 직전 3개월간 개인정보가 저장·관리하고 있는 이용자 수가 일일평균 100만 명 이상이므로 망분리 의무 대상자인데 망분리를 하지 않았다. 정보통신망법에 따르면 인터넷을 통한 정보유출, 악성코드 감염, 내부망 침투 등의 위험을 적절한 수준으로 감소시키기 위하여 망분리를 하여야 하고 그렇게 하지 않으면 3천만원의 과태료가 부과된다. 그렇게 되면 금전적 피해는 물론이거니와 대외 이미지 하락, 경쟁력 손상으로 이어질 수 있고 이는 매출 감소로 이어질 수 있기 때문에 해당 법령을 준수하도록 한다. 논리적으로 망분리를 하도록 하고 서버 가상화 방식 중 VDI 기술을 활용하기로 한다. 또한 망분리 우회 경로도 파악하고 차단하도록 한다. 망분리 환경의 적정성 및 취약점 존재 여부에 대한 정기 점검도 수행한다.

4

보호대책: 2.4.2 출입통제

은행에는 고액 이체를 위한 OTP를 본사 금고에 보관하고 있다. 해당 OTP가 탈취되면 정당한 권리를 가지고 있지 않은 사람이 고액 이체를 시도할 수 있으므로 금고가 있는 구역은 보호구역으로 지정해 놓는다. 보호구역에 출입 가능한 부서·직무·업무를 정의하고, 출입권한이 부여된 임직원을 식별하고 그 현황을 관리한다. 또한 출입통제 장치를 설치한다. 생체정보 기반 인증 방식인 정맥인증을 채택하기로 한다. 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 일정기간 보존하여 사후 모니터링이 가능하도록 문서적 또는 전자적으로 보존한다. 출입기록을 주기적으로 검토하며, 퇴직, 전배 등에 따른 장기 미출입자를 출입 가능한 임직원 목록에서 제외시키도록 한다. 또 비인가자가 출입을 시도했다면 사유를 확인하고 조치한다. 외부 협력 업체에게 과도하게 보호구역을 상시 출입할 수 있는 출입카드 등을 부여하지 않도록 주의한다.

5

보호대책: 2.11.4 사고 대응 훈련 및 개선, 2.12.1 재해·재난 대비 안전조치

기업에 악의를 가진 사람이 해킹으로 인터넷 뱅킹 시스템에 장애를 일으킬 수 있다. 이럴 때 아무리 기술적으로

훌륭한 임직원들이라고 해도 1년에 한번 이상 훈련하지 않으면 갑작스러운 사고 발생에 긴급히 대처하지 못할 수 있다. 따라서 침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 모의훈련 계획을 수립하고 계획서를 작성한다. 최신 침해 사고 사례, 해킹 동향, 비즈니스 특성 등을 반영하여 현실적이고 실질적인 모의훈련 시나리오를 마련한다. 정보보호, 개인정보보호, IT, 법무, 인사, 홍보 등 침해사고 대응과 관련된 조직이 모두 참여할 수 있도록 모의훈련 조직을 구성한다. 관련 내부 지침에 정한 절차 및 서식에 따라 모의훈련을 연 1회 이상 실시한다. 모의훈련에 따른 결과 보고서를 작성하고 이를 반영하여 대응체계를 개선하여야 한다.

해킹사고 발생 시 복구를 위한 관련부서 및 담당자에게 역할과 책임을 부여한다. 또 조직 내 관련 부서 담당자와 유지보수 업체 등 복구 조직상 연락체계를 구축하도록 한다. 서비스 및 시스템 중단시점부터 복구되어 정상 가동될 때까지의 복구 목표시간(RTO : Recovery Time Objective)과 데이터가 복구되어야 하는 복구 목표시점(RPO : Recovery Point Objective)을 정의한다. 재난 발생 시 업무에 끼치는 영향을 분석하고, 복구 목표시간 및 복구 목표시점 정의, 핵심 IT서비스 및 시스템이 무엇인지 식별하고, 복구 목표 시간별로 정보시스템의 복구 순서를 정의한다. 재해 발생, 복구 완료, 사후관리 등 단계에 따라 등 복구 절차를 마련한다.