금융기관 전산시스템 보안 강화에 대한 연구

김명수[*] · 최대영[**] · 서원우[***] · 김종배[****]
[*,**,***,****]숭실대학교

For the financial institution computer system security, research

Myung-Soo Kim[*] · Dae-Young Choi[**] · Won-Woo Seo [***] · Jong-Bae Kim[****]
[*,**,***,****]Soong-sil University
E-mail : [*]kmsoo8k@naver.com, [**]choidy219@naver.com [***]sw2trend@fnguide.com,
[****]kjb123@ssu.ac.kr

요 약

최근 금융권의 주요 이슈는 보안이었고 앞으로도 보안을 더욱 강조 될 것이다. 2013년 3월20일 전산 대란, 6월 25일 사이버테러 등으로 금융 당국은 ‘금융전산 보안 대책’ 발표와 2014년에 카드사 및 통신사 고객정보 유출 사고로 인해 ‘고객정보 유출방지 대책’을 공표하였고 당국은 매년 금융기관의 정보보호 실태 점검’을 실시하여 금융거래의 안정성 확보와 고객의 재산과 정보를 보호하는데 노력하고 있다

본 연구는 IT 시스템 관리자가 보안 강화를 위한 필요 사항에 대해 본론에서 전산 시스템기기 서비스 보안, 데이터 운영서비스 보안, 보안 관제 서비스 운영, 전산 시스템 운영 관리의 보안 사항에 대해 기술하여 정보보호를 위한 업무 운영에 도움이 됐으면 한다.

ABSTRACT

Last was the main issue of financial security in the future will be more emphasis on security. Such as March 20, 2013 Computational crisis, June 25 Cyber terrorism information to credit card companies and customers due to carrier spill in Financial computational security measures 'released in 2014 and the financial authorities' customer information leakage prevention measures "were published the efforts to protect customers' information assets and ensure the stability of the financial transactions carried out by financial institutions protected status check "the information annually authorities

This study business operations for the protection of information technology services for IT systems security equipment, data security operating services, security management services operations, operational management of IT systems security requirements from the point to the need for information security, IT systems administrator it would be great help.

키워드

financial authorities

Ⅰ. 서 론

최근 금융권의 주요 이슈는 보안이었고 앞으로도 보안을 더욱 강조 할 것이다. 이는 2013년 3.20 전산 대란, 6.25 사이버테러 사건이 발생하여 금융 당국은 '금융전산 보안 대책'을 발표했고, 2014년에 카드사 및 통신사 고객정보 유출 사고의 대책으로 '고객정보 유출방지' 대책이 마련되는 등 보안 정책이 그 어느 때보다 중요시 되고 있으며 금융당국은 매년 '금융기관의 정보보호 실태 점검'을 실시하여 고객의 재산과 정보를 보호하는데 노력하고 있다.

본 연구는 본론에서 IT 시스템 관리자가 보안 강화를 위한 필요 사항에 대해 금융기관 보안시스템 사례를 토대로 '전산 시스템기기 서비스 보안, 데이터 운영서비스 보안, 보안 관제 서비스 운영, 전산 시스템 운영 관리'의 보안 사항에 대해 기술하여 정보보호를 위한 업무 운영에 도움이 됐으면 한다.

Ⅱ. 관련 연구

1. 시스템 보안 업무 운영 현황

주요 금융기관, 공공기관, 대규모 고객 정보 서비스를 이용하여 업무를 하는 회사들은 종합상황실, 시스템 이중화, 보안 시스템 운영, 재해복구 시스템을 운영하여 보안 사고에 대비 하고 있다.

1.1 종합 상황 관리 시스템 운영

. 종합 상황실 운영 : SMS, NMS, 보안관련 장비, 음성관리시스템에 의해 상황판에 장애사항이 표시되고 이를 담당자에게 발생즉시 유·무선으로 전달되어 장애를 조치하게 하는 자동화 시스템 구축.

. 시스템 매니지먼트(SMS) 통합 운영 관리 : 시스템 관리를 통합으로 할 수 있도록 통합 정보 관리 체계를 구축하여 효율성 및 경제성, 운영의 용이성 확보하고 장애상황을 빠르게 파악 할 수 있도록 음성정보 시스템 및 종합 상황 모니터를 설치하여 운영

1.2 보안 시스템운영

기존에는 방화벽과 VPN장비를 도입하여 외부 해커 공격에 대비 했지만 최근에는 금융사 및 통신사, 정부기관 등이 지능형 지속 위협(Advanced Persistent Threat), DDos 공격에 대비하기 위해 디도스(Ddos) 방어 솔루션 및 망 분리 솔루션을 도입 하여 보안을 강화 하고 있다.

1.3 시스템 부분 이중화

. 업무 운영 서버 : 대외 고객 업무로 운영 중인 모든 서버는 HA(High-Availability) 구성으로 상호 Take-Over 기능이 구현되어 있어 장애 시 업무 중단 없이 처리.

. 데이터운영부분 : 주 전산센터의 데이터 입력 시 실시간으로 재해복구센터의 복제 기술을 적용하여 Data를 이중으로 관리

. 통신장비 : 스위치·라우터 등 주요 네트워크 장비에 대한 이중화 구성으로 Primary 장비 장애 발생시 Secondary 장비로 업무 수행

. 인터넷 이중화 : 인터넷 정보 제공 사업자(ISP) 및 망의 이중화로 인터넷 수행업무의 연속성 확보 (KT, DACOM, SK)

1.4. 재해복구시스템 구축

. 백업센터는 주 센터 시스템시설 설비, 장비 등과 동일한 구성으로, 실시간 복제솔루션이 적용되어 Data 손실 없이 업무서버 및 Network을 3시간 이내에 완전 복구가능

. 매년 1~2회에 걸친 종합테스트 수행을 통해 백업시스템에 대한 검증 실시

2. 보안시스템 강화 내역

종합상황실 운영, 시스템 이중화, 재해복구센터 운영 등 인프라 부분에의 보안 강화에 많은 인력과 비용을 투자하여왔다, 그러나 스마트폰, 테블릿 PC 등을 이용하여 업무를 처리하는 인터넷 고객의 급속한 증가, 외부 해커 공격의 다양화, 외국 서버를 통한 해킹 등으로 현재 상태의 보안 시스템으로는 보안 업무 처리에 한계가 있어 각 기관들은 네트워크 부분에서의 망 분리 및 DDos 차단 시스템을 운영하여 대비하고 전산 센터 내부 서버운영시스템 부분에는 다음과 같은 보안을 강화하고 있다.

2.1 시스템서버 보안 서비스 강화

. 기존에 시스템담당자가 운영 편의에 따라 보안 관리를 하고 있어 보안 문제가 종종 발생하고 있다. 이를 강화하기 위해서는 별도조직의 보안시스템 관리자를 운영하여야 하고,

. 보안 담당자는 전산기기, 백업장비 등에 대해 컨트롤 및 모니터링 기능이 있는 솔루션을 이용하여 보안업무를 수행하고

. 아울러, 사용자 승인, 접근권한 통제, 외부 해킹 및 내부 보안침해 방지 기능을 시스템에 적용하여 운영하여야 한다.

표 1. 시스템 보안 서비스 강화 내역

부문	내 역
계정/인증 강화	.사용자계정 및 패스워드관리, 사용자 추가/삭제 등 인터페이스기능 관리 .로그인 보안강화 기능(특수문자를 포함한 패스워드 10자리이상, 1개월 단위로 패스워드변경) .사용자접근 기록 관리 및 모든 접근 내역을 관리하는 감사기능
해킹 차단	.Anti-해킹기능(해킹의 실시간탐지) .기본적인해킹 방어 모듈이 작동하여 해킹차단 .백 도어, 트로이목마 웜 바이러스, 버퍼 오버플로우 등의 공격에 대한 실시간탐지 및 차단
접근 제어	.디렉토리별 사용자 접근 제어 .시스템 자원의 영역 구분 및 강제적 접근 제어 기능 .프로세스, 파일, 디렉토리 등 각각 레이블 링 하여 권한을 부여

2.2 데이터 보안 서비스 강화

.비인가자, 해커의 불법 접근을 방지하기 위하여 데이터의 내/외부 사용자 권한 및 접근/통제기능 운영과 데이터의 암호화로 데이터 유출을 방지하고

.보안 담당자들이 사용 내역분석과 사후 추적을 할 수 있는 기능을 적용하여 보안을 강화하여야 한다.

표 2. 데이터 보안서비스 강화내역

부문	내 역
접근 제어	.내외부의 인가되지 않은 사용자의 데이터 접근정책 마련 .컬럼 단위 접근, 제어 암호화 복호화 기술을 선택적으로 적용 .관련 사용자 IP, 시간대별 접근 제어
감사/로깅	.IT운영인력 및 개발자의 DB접근내역에 대한 감사/로깅 .비 암호와 컬럼에 대한 Audit Only 기능 수행 .일정 주기마다 감사로그 백업 .데이터 Key는 안전하게 보호 .DB운영과 보안 기능을 분리하여 전문적인 DB보안 관리
암호화	.DB에 저장된 데이터의 일괄 암호화 .컬럼에 대한 암호화 복호화 권한 분리로 접근 제어 보안성 확보 .데이터 유출시 암호화로 해독 불가 구조로 구성

2.3 보안 관제 서비스 강화

.회사 내에 분산되어 있는 보안 솔루션들을 ESM 시스템을 통하여 종합적으로 관리하고 모니터링을 실시하여 보안 위협과 침해사고에 대한 종합적 분석 및 대응체계 수립하고 보안 관리자는 이를 기반으로 일관된 보안정책 수립 하여야 한다.

.이를 통해 보안 관리자의 개별 포인트 솔루션 운영관리 부담 최소화 할 수 있다.

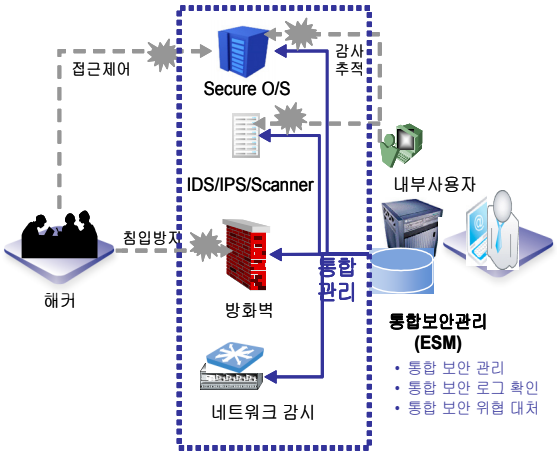

그림 1. 보안관제 서비스 개념도

표 3. 보안관제 서비스 내역

부문	내 역
통합성	.보안 관리서버와 종합분석서버의 별도 구성을 통한 대응체계 분리 .자산위협 취약성 정보에 대한 종합적 위험 분석 기능 .개별 포인트 보안의개별적이고 일관된 정보 보안 관리 .이상 징후 및 침해사고 원인의 실시간 분석 및 대응
이기종 인증 및 로그 관리	.다양한 보안시스템 및 장비에 대한 연동 구축 .보안 시스템의 최소한의 Resource 운영으로 보안시스템운영에 대한 영향 최소화 .대용량 로그 처리 기능 .로그저장 및 검색을 통한 사고분석기능
침해사고 분석	.종합적이고 신속한 24시간 모니터링 및 보안 핵심사항분석 .분야별 취약성 분석 .성능, 트래픽, 장애분석 위험평가

2.4 통합업무운영관리 서비스 강화

.클라이언트로부터 DB, 서버, 데이터베이스에 이르는 각 구간별 업무 트랜잭션 단위의 모니터링 체계를 구축하여 고객 업무의 트랜잭션 고유의 화면번호, Service Code, Transaction ID 등과 업무명의 매핑을 통한 시스템 Performance 및 Real-Time Transaction 관리 기능을 도입운영

. 즉, IT 인프라 요소와 어플리케이션 간 연관성에 따른 Process 모니터링 체계 구현하여 문제발생 시 이를 인지하여 해결하는 시스템 국축하여 운영하여야 한다.

표 4. 통합업무 운영관리 서비스 내역

부문	내 역
통합/업무관리 모니터링	.인프라위주의 관리체계에서 어플리케이션 관점의 모니터링(어플리케이션 연관성에 대한 Process모니터링) .주요 IT인프라의 이벤트 및 장애를 관리 (N/W, 시스템, DBMS일원화 관리)
End-To-End 모니터링	.트랜잭션 응답시간 통합관리(통합관점의 데이터 성능 실시간 수집분석 대응) .Client, Web, WAS, DB의 End-To-End 트랜잭션 통합관리 .운영을 위한 대시보드 체계 구축
사전예방 기능	.업무 장애 시 추적기능 및 원인파악 기능 .트랜잭션 고유의 화면 코드, Service Code, 트랜잭션 ID의 매핑을 통한업무 이상 유무 제공

Ⅲ. 결 론

본 논문은 보안 시스템에 구축에 있어 사용자 부분의 단말기와 회사 네트워크 부분의 방화벽, VPN, 망분리, DDos 시스템구축 등에 많은 자료가 있으나 데이터 저장 및 추출 서버, 프로그램 개발 관리 서버, 업무 프로세스 운영서버, 웹서버 등 보안사고 발생 시 회사 전체 업무에 영향을 줄 수 있는 시스템 운영 보안 부분의 자료가 많지 않아 금융기관 보안시스템 사례를 토대로 시스템 운영의 각 부분별 보안 강화 서비스 기능에 대해 기술하였다.

시스템관리자 또는 담당자가 보안 사고에 있어 빠르게 감지하고 이를 모니터링 할 수 있는 보안 시스템을 강화하기위한 프로젝트시 참고가 되었으면 한다.

향후에는 최근 이슈가 되고 있는 클라우딩 컴퓨터, 빅 데이터 등 보안사고시 엄청난 정보 누출이 예상되는 분야에 대한 보안 강화 사항에 대해 연구를 추가하고자 한다.

참고문헌

[1] 2022 GLOBAL TREND,2012, 네오넷코리아