금융투자업계 전산망의 통합보안관제에 관한 연구

정의연
도로교통공단
e-mail:iyeonjung@gmail.com

A Study on the Integrated Security Monitoring & Control in Financial Investment Industry Computer Networks

Eui-Yeon Jung
Road Traffic Authority

요 약

본 논문은 금융투자업계에 대한 보안관제 정책을 기준으로 업계가 공동이용 가능한 통합보안관제시스템이 구축 가능하도록 금융투자회사들이 구축 운용하고 있는 보안인프라를 비롯한 전산망의 보안관제를 위한 적용 기술과 운용체계 등을 조사하고, 이를 토대로 외부로부터 공격에 대비한 모니터링, 침입탐지 및 실시간 방어 등의 기능이 적절하게 수행되고 업계 차원의 종합적이고 체계적인 관리가 가능한 통합보안관제시스템 모델과 운영방안을 제시하고자 한다.

1. 서론

최근 정보통신기술의 발달과 초고속 인터넷의 보급 증가 등으로 행정 및 금융 서비스, 전자상거래 등 일상의 모든 분야에서 인터넷에 대한 의존도가 지속적으로 증가하고 이들 이용을 지연, 중단하는 등의 사이버 위협도 날로 증가되고 있다.

그중 가장 가시적인 피해양상을 나타내는 위협 중 하나는 서비스를 지연 또는 중단시키는 서비스거부(DDoS) 공격이다. 금융기관의 DDoS 공격으로 인한 피해는 금융거래업무 마비라는 핵심기능의 중단으로 나타나며, 특히 변동성이 큰 금융자산을 관리하는 금융투자시장의 특성상 보안인프라가 제대로 갖추어지지 않은 회사가 업계전산망을 이용할 경우 부정적 파급 영향은 지대하므로 업계 전체의 보안인프라체계 구축과 통합관리에 대한 관심이 더욱 커지고 있다.

본 논문에서는 금융투자회사의 보안시스템 구축 현황과 문제점을 파악하고 보안관제를 위한 제반 활용 기술과 대응체계 등을 연구하여, 업계가 공동이용 가능한 통합보안관제시스템 모델을 제시하고 효용성을 검증하고자 한다.

2. 보안관제에 대한 고찰

2.1 사이버 침해 행위 및 현황

사이버 침해 행위란 정보시스템을 대상으로 해킹, 컴퓨터바이러스, 웜, 스팸 메일, 서비스 거부 등 전자적 수단에 의하여 정보통신망을 불법침입, 교란, 마비, 파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.

사이버 침해는 그 행위 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있으며 각각 목적, 대상, 공격방법에 차이가 있다. 또한 위협에 사용된 기술의 유형에 따라 컴퓨터바이러스, 웜, 해킹, 피싱, 악성 봇(Bot), 분산서비스거부(DDoS)공격, 스팸 메일 등으로 분류할 수 있다.

최근 침해사고를 보면 2009년 7.7 DDoS 공격이후 계속해서 수많은 신규 취약점과 악성코드가 출현하고 상대적 소규모의 DDoS 공격과 개인정보 유출 등 인터넷 침해사고가 발생하고 있다. 금융결제원이 조사한 2010년 주요 정보보호 이슈를 보면 목표대상이 명확한 조직적 공격, 소셜 네트워크 서비스 위협, 악성 프로그램 및 가짜백신 증가가 우선순위를 차지하여 침해사고의 최근현황을 잘 보여주고 있다. 이러한 사이버 침해의 최근 공격 특징은 자동화, 공격도구의 능력 향상, 취약성의 신속한 발견, 침입차단시스템의 침투 증가, 비대칭적 위협 및 기반 공격의 위협 증가로 나타나고 있다.

2.2 보안관제 기능과 구성 시스템

전산망 보안관제는 24시간 서버와 네트워크를 통해 통신한 방대한 데이터에서 잠재적인 침입자의 공격시도를 규명하고 이러한 과정에서 분석된 내용을 토대로 불명확했던 침입시도를 규명하는 일련의 행위로, 각 보안관제의 기술 수준이나 관제 노하우 등에 따라 탐지, 분석, 대응 기능이 다양한 형태로 이루어진다. 탐지 기능은 전산망에 대한 트래픽 증감 및 내부 정보를 절취하기 위한 해킹시도, 악성 프로그램 유포 등과 같은 공격시도를 사전에 알아내는 활동이다. 분석 기능은 공격시도를 탐지한 뒤 최신 해킹기술 과 침해당한 전산망의 관련 로그정보를 수집하여 공격정보를 알아내고 피해규모를 파악하는 활동이다. 대응 기능은 분석 기능을 통해 파악된 공격자 정보와 취약점 정보를 활용하여 피해시스템이 정상적으로 운영될 수 있도록 전문기술을 제공하며 해당 공격탐지 기술을 개발하여 동일한 침해사고 발생을 사전에 방지하는 활동이다.

보안관제 기능 수행을 위한 보안시스템으로는 침입차단시스템(Firewall), 침입탐지시스템(Intrusion Detection System), 침입방지시스템(Intrusion Prevention System), 통합보안관리시스템(Enterprise Security Management), 위협관리시스템(Threat Management System), 가설사설망(Virtual Private Network) 등이 있으며, 총체적인 보안관리를 위해서는 네트워크에 대한 전반적인 상태 감시 이외에 취약점 진단, 위협정보 수집 및 전파, 사전 보안대책 수립을 통한 예방활동, 사이버 공격에 대한 경보 발령과 대응, 피해시스템의 피해정보 수집과 복구 등의 활동들이 함께 수행되어야 한다.

3. 금융투자업계 전산망의 통합보안관제

3.1 금융투자회사의 보안관제 현황

금융투자회사의 정보보안관리 체계는 업무시스템의 가용성과 내부정보의 기밀성, 무결성 보장을 목표로 전자금융감독규정, 정보통신기반시설보호법 등 관련 법규와 자체 규정에 따른 정보보안관리정책에 의거 보안시스템 및 침해사고 예방, 침해사고 대응, 보안품질 개선의 보안관제활동과 보안시스템, 보안조직 및 보안규정 운영의 보안인프라관리로 구성되어 있다.

회사별 보안장비는 '11년 기준으로 42개 금융기관의 76사이트, 약 500대가 있으며, 대부분의 회사들이 방화벽, IDS/IPS, DDoS 장비 등의 보안시스템을 갖추고 있으나 보유수량에 있어서는 회사별 규모 즉 트래픽 발생량에 따라 1대에서 수 십대까지 큰 차이가 있는 것으로 조사되었다. 한편 보안관제 내용을 보면 대형사 기준으로 한 두명의 담당자가 DDoS를 포함한 사이버 침해행위 관련 모니터링 및 상황전파 일 1건, 침해발생에 대한 실시간 방어 지원 및 보안정책관리 등은 월 1건, 기타 보안시스템 확인과 웹사이트 상태확인 일 2건 정도를 수행하고 있으며, 중·소형사들은 더욱 미진한 실정이다.

3.2 통합보안관제의 필요성

여러 형태의 사이버 침해로부터 정보자산을 안전하게 보호하고 업무의 연속성을 확보하기 위해서는 보안시스템을 체계적으로 운영 및 관리하여 신속하고 능동적인 침해예방과 대응을 할 수 있어야 한다. 그러나 네트워크 보안, 시스템 보안 및 데이터 보안과 같이 요구 기능별 보안시스템이 점점 전문화되어 각각의 전문지식과 관리방법을 필요로 하고 네트워크상에 산재되어 있는 보안시스템이 연동 및 호환성을 갖추어야 연관분석을 통한 침해대응력을 향상시킬 수 있음에 따라 통합보안관제의 도입이 확대되고 있다. 따라서 지금껏 개별 회사 단위로 보안관제시스템을 구축 및 운영하던 금융투자업계도 서비스의 안정화와 회사별 보안관제 수행에 대한 대응 한계 극복을 위하여 업계 차원의 보안관제시스템을 마련하고 이를 공동 이용하는 실시간 대응체계의 구축 필요성이 확대되었다.

3.3 통합보안관제의 기능

금융투자업계의 통합보안관제는 각 회사 사이버 트레이딩시스템 구간의 방화벽, 침입탐지 및 방지시스템, DDoS 대응시스템 등 보안시스템에서 발생한 보안 이벤트, 네트워크 트래픽 정보를 실시간 감시, 분석, 대응하는 업무로 다음과 같은 기능들이 요구된다.

첫째, 실시간 예·경보 기능으로 실시간 모니터링을 통하여 알려지지 않은 공격에 대한 징후파악(예보)과 알려진 공격의 발생현황(경보)을 생성하고 이를 전체 금융투자회사에 전파하여 실시간 대응토록 한다.

둘째, DDoS 탐지 및 분석 기능으로 DDoS 관련 침해사고 공동 대응을 위해 트래픽 및 이벤트 모니터링, 회사별 DDoS 상황 정보 제공, 패턴 업데이트 정보 및 대응 매뉴얼을 제공하고 공유한다.

셋째, 이기종 통합관제 기능으로 회사별 방화벽, 침입탐지시스템, 트래픽 수집 및 분석시스템 등 다양한 보안장비를 통해 수집된 이기종 보안 이벤트에 대해 모니터링, 트래픽 추이 분석, 이벤트 기반의 연계 분석 등을 실시한다.

넷째, 위협관리 기능으로 글로벌 위협정보와 국내 위협상황을 근간으로 회사별 수집된 프로토콜별 서비스별 트래픽 정보를 분석하고 의사결정수단과 대응방안을 제시한다.

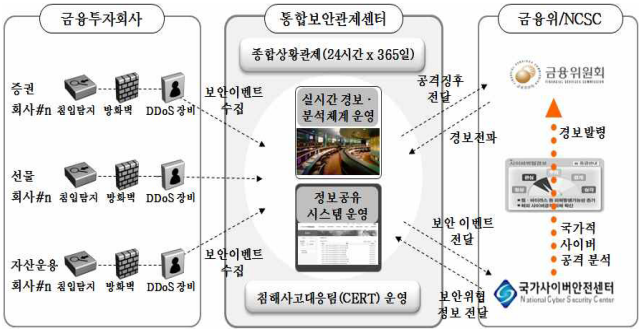
다섯째, 종합상황 분석 기능으로 실시간 단계별 예·경보, 주요 관제 정보, 통합보안관제 룰 셋 이벤트 정보, 회사별·포트별 트래픽 현황 등 종합적인 상황을 제공하여 직관적으로 업계전산망의 상황을 파악할 수 있도록 한다.

그 밖에 정보자산의 취약점을 진단하고 분석·평가하는 취약점 점검 및 분석 기능, 회사별 침해사고 접수 및 대응정보를 공유하고 침해사고 신고 및 정보제공 관리를 실시간으로 처리하는 보안관제 정보공유 기능 등이 포함된다.

4. 통합보안관제시스템 구현 방안

4.1 통합보안관제시스템 제안

금융투자업계 전산망의 통합보안관제를 위한 시스템은 회사별 보안시스템에서 발생한 보안 이벤트, 네트워크 트래픽 정보를 실시간으로 모니터링, 분석 및 대응할 수 있도록 하며, 탐지 및 분석 결과를 해당 회사 및 국가기관과 공유함으로써 금융투자분야 사이버 침해에 공동으로 대응 가능토록 한다.



(그림 1) 금융투자업계 통합보안관제 개념도

통합보안관제 업무는 기본 업무와 부가 업무로 나누어지며 기본 업무에는 침해행위 감시 및 모니터링 업무, 침

해행위 분석 및 대응 업무가 있으며, 부가 업무로는 우회 경로 제공, 좀비 PC 점검, 보안 컨설팅 및 보안 교육 등을 포함한다.

4.1.1 시스템별 구성 방안

통합보안관제는 DDoS 예·경보 시스템, 종합분석시스템, 통합보안관리시스템, 위협관리시스템 및 정보공유시스템 등으로 구성하여 수행한다.

DDoS 예·경보시스템은 전용망을 통하여 금융투자회사 DDoS 전용장비와 연동하고 DDoS 탐지정보, DDoS 전용장비 리소스 정보 등을 수집하여 DB에 저장하고 주기적인 분석활동을 수행하도록 한다.

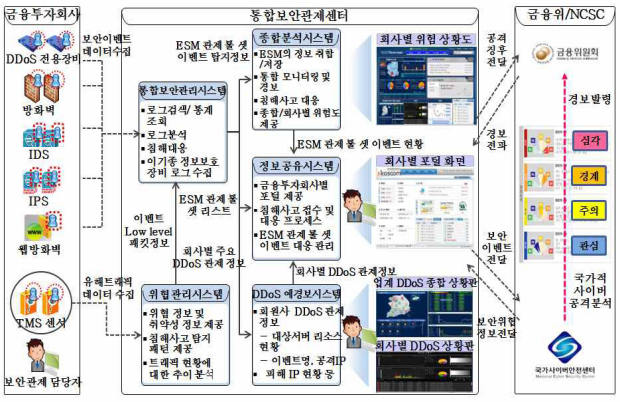
종합분석시스템은 금융투자회사의 보안시스템과 ESM에 수집된 정보를 바탕으로 단일시스템에서 관제하고 침해사고에 대응토록 구성한다. 또 각 회사 보안자산의 가치값과 취약점 수준, 위협 수준을 종합적으로 분석하여 회사별·자산별 위험도 등을 종합상황판을 통해 제공한다.

통합보안관리시스템은 관제대상 장비에 ESM 에이전트를 설치하여 보안데이터를 수집하고 이들 데이터를 기반으로 주기적인 분석활동을 수행하도록 구성하며 생산된 정보는 종합분석시스템과 정보공유시스템에 제공한다.

위협관리시스템은 업계 전산망에 TAP을 이용하여 TMS 센서를 구축하며 이를 통해 보안 데이터를 수집·저장하고 분석토록 구성한다. 수집된 데이터는 전송 데이터 프로토콜에 따라 금융투자회사와 통합보안관리시스템, 대외기관에 제공한다.

정보공유시스템은 금융투자회사 담당자와 보안관제 정보 공유 및 보안관제 이벤트 대응관리가 가능한 포털시스템으로 구축하고, 워크플로우 시스템을 내장하여 침해사고 대응처리 프로세스를 자동화하고 유형별·테마별 화면을 구성하여 보안관제 업무를 종합적으로 운영하도록 한다.

그 밖에 시스템 장애 시에도 업무 연속성을 확보토록 주요 시스템은 상호 연동 및 백업형태로 구성하며, 네트워크 장애에 대비하여 네트워크는 이중화한다.



(그림 2) 금융투자업계 통합보안관제 시스템 구성

4.1.2 보안관제 업무 운영 방안

통합보안관제센터에서는 금융투자업계 전산망의 침해시도 및 침해 발생여부를 실시간으로 모니터링하여 침해사고 관련 이벤트의 탐지 및 분석을 수행하고 금융투자회사와 공동으로 대응한다.

첫째, 이벤트 탐지 업무로 방화벽 이벤트는 방화벽 자체에서 지원하는 IDS 기능을 통해 발생시키는 이벤트를 모니터링하고 발생빈도가 높을 경우 해당 서버의 서비스 파악, 트래픽 캡쳐 및 모니터링 등 해당 트래픽에 대한 상세 분석을 실시한다. 또한 발생빈도가 급격히 증가하거나 주기적으로 발생하는 이벤트는 해킹이나 바이러스 등으로 인해 생성되는지를 분석하고 동일현상이 지속될 경우 세션차단, 블랙리스트 등록 및 대응보고 등 대응처리를 수행한다. 네트워크 및 서버 IDS에서 발생하는 이벤트는 패턴매치 방식으로 네트워크나 서버의 모든 활동을 탐지하므로 오탐률이 높아 신뢰성이 떨어지므로 네트워크 현황 및 각종 서비스 시스템들에 대한 업무분석을 토대로 트래픽의 특성을 사전에 파악하여 활용한다. DDoS 이벤트는 근거 이벤트의 결과값에 의해 탐지되므로 해당 경보 이벤트의 결과값을 확인하고 출발지IP 및 도착지IP를 확인한다. 발생빈도가 급격히 증가하거나 주기적으로 발생하는 이벤트는 방화벽, IDS 등에서 발생하는 경보에 대하여 상관분석을 실시하고 대응처리 한다.

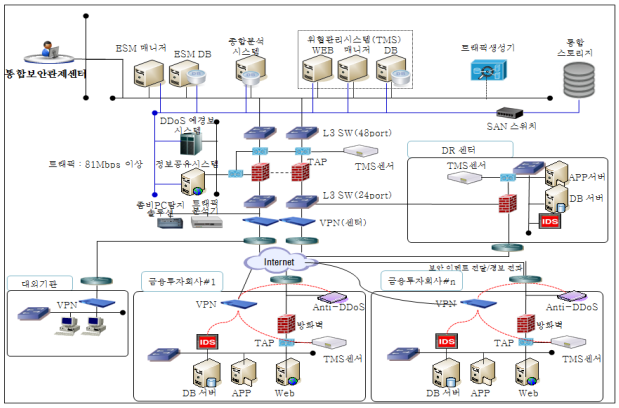
둘째, ESM 이벤트 분석은 개별 보안장비에서 발생하는 이벤트를 모니터링하여 그에 대한 상세내역(해당 네트워크 및 시스템, 출발지 및 목적지 IP/Port, 이벤트 룰)을 확인하고 발생건수, 중요도, 위험도가 다수 및 상위인 이벤트에 대해 상세 정보를 조회 및 확인하여 이벤트 유무를 판단한다. 비정상 징후, 침해시도 확인 및 웜 바이러스 유포 등으로 판단될 경우 방화벽 혹은 IDS에서 세션차단, 방화벽에서 차단 룰을 설정하고 ESM에서 블랙리스트 등록 및 세부 대응정보를 등재하여 DB화하고 동일상황 혹은 유사상황 발생시 신속하고 정확한 대응조치를 할 수 있도록 한다. 이벤트 분석은 오탐 여부를 확인하는 1차 분석과 실제 공격 여부를 확인하는 2차 분석으로 나누어 실시하며, 침해사고로 식별되면 침해사고 내용과 원인을 상세히 조사하여 원인과 영향을 제거하는 대응조치를 수행하고 정상적인 서비스가 가능토록 복구처리 한다.

그 밖에 Deepsight가 제공하는 ThreatCon 상황을 상시 모니터링하여 글로벌 위협사항의 변화추이를 확인하고 위협사항 발생시 관련 상황을 전파하여 대응토록 한다.

4.2 통합보안관제시스템 구축

통합보안관제센터와 금융투자회사는 VPN과 ESM 에이전트를 이용하여 보안 이벤트 및 로그를 전달하고 관제센터에서는 통합보안관리시스템, 위협관리시스템, 종합분석시스템을 통해 이벤트 모니터링 및 분석을 수행하며, 금융투자회사에서는 DDoS 예·경보시스템, 정보공유시스템을 이용하여 주요상황을 모니터링하고 대응토록 구축한다. 통합보안관제망은 방화벽에서 내부, 외부, DMZ, DR센터의 4개 네트워크 영역으로 분리하고 모든 네트워크 구성 시스템은 이중화하며, 국가사이버안전센터와 금융감독기관

과 연동토록 구축한다.



(그림 3) 통합보안관제센터 및 관련 시스템 구축 예

금융투자회사의 다양한 이기종 보안시스템에서 발생한 이벤트를 실시간으로 분석하여 위협 및 공격을 파악하고 대응하기 위해 이용회사의 보안장비에 공통적으로 적용할 수 있는 탐지기준(보안이벤트 표준 룰 셋)을 설정하고 통합보안관리시스템에 등록한다. 표준 룰 셋 적용을 통하여 보안이벤트 발생현황을 파악하고 이를 분석하여 각 회사에 최적화된 보안 이벤트 룰 셋을 확정한다.

<표 1> 보안이벤트 표준 룰 셋

구분	설 명
보안장비 리소스 기반	대상 장비의 CPU, Memory, Disk 사용량에 대한 표준 임계치
방화벽 이벤트 데이터 기반	Accept, Drop 등 방화벽 행위별 이벤트 데이터에 대하여 이벤트 평균 발생 건에 대한 표준 임계치
DDos/IDS/IPS 이벤트 데이터 기반	공격 패턴별 발생현황에 대하여 이벤트 평균 발생 건을 분석하여 TOP30 패턴에 대한 임계치
상관분석 기반	방화벽, DDoS/IDS/IPS 등 이기종 보안장비에서 탐지되는 이벤트 데이터 중 임계치 이상 발생되는 이벤트에 대하여 공통조건(출발지 및 목적지 IP 등이 동일할 경우)을 만족할 경우 보안이벤트가 발생
유해IP 기반	상황전파문, 악성코드 경유지 정보, 참가기관 침해사고 발생 및 글로벌 위협정보 등을 통하여 알려진 유해IP 접근시도 또는 접속시도에 대하여 임계치

표준 임계치는 리소스 경우 평균 사용량+20%, 이벤트 데이터 경우 평균 이벤트 발생량*1.5, 상관분석은 평균 이벤트 발생량*1.2, 유해IP 이벤트 1건 이상으로 산정한다.

4.3 통합보안관제에 대한 검증

통합보안관제시스템의 보안관제 수행 적합성에 대한 검증은 통합보안관제센터와 금융투자회사간의 송수신 데이터의 정합성 확인, 보안이벤트 발생시 정탐율을 최대화하는 탐지기준에 대한 검증, DDoS 모의공격을 활용한 모니터링, 분석 및 대응 프로세스 점검을 통해 실시한다.

이벤트 데이터 정합성 확인은 금융투자회사의 다양한 보안장비와 연동하기 위해 개발한 에이전트와 UDP를 이용하여 전송되는 이벤트 데이터를 시간정보 기준으로 비교한다. 탐지기준(보안이벤트 룰 셋) 검증은 금융투자회사의 보안장비별 표준 룰 셋에 대하여 2주간의 보안이벤트 발생 데이터를 수집 분석하여 분당 이벤트 평균발생량을 기준으로 실시한다. DDoS 모의공격에 의한 기능 점검은 외부 인터넷에서 금융투자회사 내부로 공격 트래픽을 발생시켜 네트워크 장비, 보안 장비, DDoS 장비 및 업무서버에 대한 모니터링, 대응 및 복구능력을 점검한다.

5. 결 론

인터넷을 통해 날로 자동화, 분산화, 복합화되는 해킹, 바이러스 및 DDoS 공격의 위협으로부터 개별 금융투자회사의 보안시스템으로 정보자산을 안전하게 보호하고 업무의 연속성을 확보하는 데는 한계가 있어 다양한 보안장비의 기능적 특성을 유기적으로 연결하여 종합적으로 분석·대응하기 위한 업계 차원의 통합보안관제시스템 구축·운영이 필요하다.

본 연구에서는 금융투자업계 전산망 환경에 적합한 통합보안관제 기능을 도출하고 이를 구현할 통합보안관제 모델 제시와 주요 시스템들의 구축을 통하여 실제 업무 활용성을 검증하였다. 그 결과 기본적인 보안관제 업무에 더하여 첫째, 보안시스템의 탐지율 최적화를 위한 탐지기준, 둘째, 관제 성능 향상을 위한 통합보안관리시스템과 위협관리시스템의 로드 분산 방안, 셋째, 네트워크 부하 감소와 주요 서버의 자원 낭비를 방지하기 위해 회사별 로그축약정책이 적용되어 금융투자업계 전산망에 적합한 통합보안관제 모델이 완성되었다.

이를 통해 침해사고에 대한 금융투자회사별 대응 한계를 극복하고 체계적인 예방 및 대응이 가능한 금융투자업계의 공동 관리체계가 마련되고, 나아가 범국가적 사이버 침해에 대한 대응체계 구축이 용이할 것으로 기대된다.

참고문헌

[1] E. Amosoro, “Fundamental of Computer Security Architecture, Design, Deployment & Operation”, Osbourne/McGraw-Hill, 2001

[2] 윤주호, 임현숙, 김용호, “보안 입문, 웹 해킹과 침해사고 분석-윈도우즈편”, 비팬북스, 2009

[3] “DDoS 공격유형 및 보안장비별 대응방법”, 정부통합전산센터, 2010

[4] “2010 해킹·바이러스 현황 및 대응”, 한국인터넷진흥원, 2011

[5] 김준학, “안전한 금융비즈니스 보호를 위한 보안관제 서비스 도입과 적용”, 금융보안연구원 금융정보보호컨퍼런스 자료집, 2011

[6] 금융결제원, http://www.kftc.or.kr

[7] 금융보안연구원, http://www.fsa.or.kr

[8] ㈜코스콤, http://www.koscom.co.kr

[9] 한국인터넷진흥원, http://www.kisa.or.kr