Journal of Digital Contents Society Vol. 9 No. 3 Sept. 2008(pp. 491-498)

기업정보 유출 방지를 위한 통합 로그분석 시스템 설계 및 검증

이재용*, 강수용**

요 약

최근 몇 년간 악의적 내부자에 의해 기업의 기밀정보가 유출된 사례들이 급속도로 증가하고 있으며, 이는 기업의 경쟁력 약화와 심지어 기업의 생존을 좌우하고 있음에도 불구하고 내부자에 의한 기밀정보 유출을 대비한 보안대책과 보안기술은 미비한 실정이다. 이에, 본 논문에서는 현재 구축·운영 중인 기업 내부 지향적인 보안 기술들에 대한 특징과 한계들을 분석하여 기업정보 유출 사고 발생 시 그 피해를 최소화하기 위한 통합 로그분석 시스템을 제안한다. 통합 로그분석 시스템은 사전에 분석된 위협 룰에 근거하여 내부 구성원의 기밀정보 유출 가능 행위들을 사전에 탐지하는 시스템으로, 보안 및 업무 단위 시스템을 연동하여 사용자의 모든 행위 로그를 수집하는 로그수집 모듈, 룰에 의해 비정상 유출 행위를 탐지하며 보안지수를 생성하는 로그분석 모듈, 탐지 결과 보고서를 생성하는 모듈로 구성된다.

Design and Verification of the Integrated Log Analysis System for Enterprise Information Security

Jaeyong Lee*, Sooyong Kang**

Abstract

The leakage of sensitive information by an insider within the organization becomes a serious threat nowadays. Sometimes, these insider threats are more harmful to an organization than external attack. Companies cannot afford to continue ignoring the potential of insider attacks. The purpose of this study is to design an integrated log analysis system that can detect various types of information leakages. The system uses threat rules generated through risk analysis, and monitors every aspect of the online activities of authorized insider. Not only should system have the ability to identify abnormal behavior, they should also be able to predict and even help to prevent potential risk. The system is composed of three modules, which are log collector, log analyzer and report generator.

Keywords : 내부정보보호, 정보유출, 로그분석, 정보보안, Enterprise Information Security, Log Analysis

1. 서론

오늘날 기업들은 전자문서 관리 시스템, 지식관리 시스템 등 IT기술을 활용한 지식 기반의 정보시스템을 구축하여 업무의 효율을 향상시키고 있으며 날이 갈수록 IT시스템에 대한 업무 의존도가 증가되고 있다. 그러나 해킹 및 악성코드 감염과 같은 외부 위협으로 기업의 사내 네트워크와 고객서비스가 중지되는 정보화 역기능이 도래했으며, 심지어는 국가 전반적으로 네트워크가 마비되는 인터넷 대란을 경험하였다. 이후 최근 몇 년간 국가와 기업들의 부단한 노력으로 외부 위협으로부터 시스템과 서비스의 가용성을 보장하기 위한 어느 정도의 보안 수준을 확보하였으며, 보안조직, 보안정책, 보안인력, 보안시스템 등의 보안체계가 확고히 정립되어 있다. 한편, 최근 들어 정보화 역기능의 한 유형으로 이동통신 표준기술인 Wibro, 철강 제조공정 특허기술 등 많은 시간과 비용을 투자하여 개발한 기술정보 및 영업정보, 고객정보들이 경쟁사나 해외로 유출되는 사례가 증가하고 있으며 이

※ 제일저자(First Author) : 이재용
접수일자:2008년08월12일, 심사완료:2008년09월10일
* 한양대학교 교육대학원,
ddobbasy@naver.com
** 한양대학교 정보통신학부(교신저자)

러한 천문학적인 피해 규모와 기업의 경쟁력 약화는 해킹이나 악성코드 같은 외부 위협이 아닌 기업 내부자의 부정 유출에 의해 발생하고 있다. 실제로 미국 CSI·FBI 보고서에 따르면, 2002년 미국에서 발생한 정보유출 사고 중에 약 80%가 내부자에 의한 것으로 파악되었다. 우리나라의 경우, 국가정보원 산업기밀보호센터는 2003년도부터 2006년까지 산업기밀 유출 적발사건이 92건에 이르며 총 피해 예상 금액은 95조 9천억원에 달한다고 밝혔으며, 연구원 매수를 통한 전·현직 내부자에 의한 기술정보 유출이 약 80%에 이른다고 밝혔다.[1][4]

이에 따라 기업에서는 권한이 있는 내부자에 의한 기업정보 유출 사고 발생을 방지하기 위하여 통합 보안 조직의 강화, 내부 구성원의 보안의식 증진을 위한 교육뿐만 아니라 업무 시스템의 사용자 이력 보관, 단일화된 사용자 인증, 권한에 의한 시스템 및 정보 접근 통제 등 다양한 정보보호 방안과 대책을 수립하고 각종 보안활동을 수행하고 있으나 관리적·기술적 측면에서 현실적으로 이를 적용하여 운영하기가 쉽지 않다. 또한 DRM 기술을 이용하여 사용자의 매체 저장과 같은 행위를 모니터링하거나 기업 네트워크로부터 외부 네트워크로 유출되는 기밀정보의 패킷을 필터링하는 기술 등의 다양한 연구가 시도되고 있으나[2] 아직까지도 기업정보 유출을 효과적으로 탐지하기 위한 보안기술은 미비한 실정이며[5], 특히 정보유출 탐지 성능을 향상시키고 유출 손실을 최소화시키기 위해 정보가 유출되는 흐름을 통합적으로 분석하는 기능이 절실히 요구된다. 또한 기업의 정보보호 목표를 효과적으로 달성하기 위해 조직의 정보보호 수준을 정확히 평가해야 함에도[6] 불구하고 기업의 내부지향적 요소를 전혀 고려하지 않고 있다.

따라서 본 논문에서는 권한을 가진 내부자에 의해 발생하는 기업정보 유출 사고 방지를 위해 유출 가능성이 있는 비정상 행위를 정보가 유통되는 전 단계에서 통합 분석하며, 분석된 결과를 바탕으로 기업 내 보안 수준 제고에 기여할 수 있는 보안지수를 생성하는 통합 로그분석 시스템을 제안하고자 한다.

2. 내부정보보안 기술동향

2.1 보안전략

기업의 보안운영 조직은 외부의 침입뿐만 아니라 이제는 내부자에 의한 기업정보 유출을 심각하고 받아들이고 있으며, 이를 대비하기 위해 다음과 같은 신규 보안체계와 다양한 전략들을 제시하며 장기적인 로드맵을 구상하고 있다[3][7].

- 보안 조직의 강화
  다원화된 보안 조직으로 인한 보안 업무의 한계, 전문성의 한계, 위기 대응 능력을 향상시키기 위해 기업 비지니스의 성격, 경영원칙, 조직의 문화 등이 반영된 통합된 보안체계를 구축해야 한다.
- 단일사용자 인식 및 사용이력 체계 관리
  보안정책 및 사용자 통제의 일관된 시행, 감사 증적의 확보 등 기본적인 필수 보안 요구사항을 충족시키기 위해 단일화 된 사용자 인증 체계가 필요하며, 기업 내의 다양한 시스템에 대한 접근을 통제하는데 있어서 통합된 계정 관리 체계는 기업정보 유출 행위를 탐지하고, 유출 사고 발생 시 사고 조사를 위한 필수 조건이라고 할 수 있다.
- 정보의 암호화
  내부 구성원들의 단말에 존재하는 문서를 암호화하여, 단말에서 이루어지는 접근조차도 그 권한에 따라 열람을 불가능하게 하는 기능이 필요하다.
- 조사 및 추적 능력의 향상
  기업정보 유출 사고 발생 시 민형사상의 처벌 및 신속한 법률적 대응을 위하여 내·외부의 공조자를 명확히 가려내고 관련 증적을 확보하는 위기 대응 체계가 필요하다.
- 비정상 행위 모니터링 체계
  조사 및 추적능력 확보로 보안사고 피해를 최소화하기 이전에 유출 가능성을 사전에 탐지하고, 재발을 방지하는 활동은 더욱 더 중요하다. 사고 발생 가능성이 높은 위협요소를 인지하여 사전에 이를 예방하는 능동적 보안활동을 위해, 유출 가능성이 높은 비정상 행위를 모니터링하는 보안체계와 상시 전문 인력이 필요하다.

- 인적 요소에 대한 투자
  기업정보 유출 방지를 위해서는 내부 구성원들의 보안의식을 높아야 하며, 이를 위해서는 지속적 또는 강제적 보안 교육을 통해 구성원들의 전체적인 보안 수준을 향상시켜야 한다.

2.2 보안시스템의 운영 현황

내부자에 의한 기업 정보 유출 사고에 대비하기 위하여 기업들은 위와 같은 거시적인 보안 전략을 바탕으로 각 기업의 비즈니스 성격에 맞게 어느 정도 적절한 보안체계를 마련하였고, 이에 그 보안 체계에 합당한 보안 솔루션들을 도입하거나 자사 환경에 맞는 보안시스템들을 개발하고 있다.

2.2.1 문서보안

기업 내 생성되는 문서를 암호화하여 문서 생성, 편집, 출력, 폐기와 같은 문서의 전 생명주기 동안 인가된 사용자에게만 그 권한을 부여하여, 권한이 없는 사용자에게는 접근 자체를 차단함으로써 기업정보 유출을 방지하는 솔루션이다. 즉, 권한이 없는 사용자는 절대 문서를 해독할 수 없으므로 문서가 외부로 유출된 후에도 기밀성을 보장받을 수 있기 때문에 대부분의 대기업들은 문서보안 시스템을 구축하여 운영 중이다.

2.2.2 NAC (Network Access Control)

네트워크 접근 제어 솔루션은 보안 규정을 준수하지 않은 사용자나 비 인가된 사용자로부터 기업의 네트워크 및 서비스를 보호하기 위해 네트워크 접근 자체를 원천적으로 차단하는 기능을 제공한다. 예를 들어 인증 클라이언트 미설치, 윈도우 패치 미설치, 사내 보안 필수 프로그램 미설치, 또는 백신 엔진을 최신으로 업데이트하지 않은 경우 사내 네트워크의 스위치 단에서 접속이 차단된다. 따라서 사용자 인증과 접근 관리를 수행하며, 네트워크 접속을 수행하는 모든 단말의 보안성을 강제화 한다. 네트워크 접근 제어 솔루션은 모바일 환경이 일반화 되고 접속 단말이 다양해지면서 그 필요성이 대두되었는데, 특히 내부자에 의한 해킹이나 악성코드 위협을 방지하므로 기업정보 유출을 방지하는 솔루션으로 인식되고 있다.

2.2.3 DLP (Data Loss Prevention)

DLP는 사용자 랩탑을 이용한 클라이언트 기반의 유출, 또는 분리 가능한 저장 매체를 이용한 정보 유출에 대한 탐지가 불가능한 게이트웨이 전용 솔루션의 한계를 극복하고자 개발된 종합적 정보 손실 방지 솔루션이다. DLP는 기업의 정보 자산을 분류하고 각 보안 정책을 설정하여 데이터의 흐름을 트랙킹함으로써 내부, 외부로부터 기업의 정보 자산을 보호하는데, 이는 기업의 기밀정보 유출을 차단하고 피해를 최소화 하는데 있어 가장 진보된 솔루션이라고 할 수 있다. 그러나 아직 국내에 적용된 사례가 없어 그 효용성을 판단하기에는 이른 실정이다.

2.3 한계 및 시사점

현재 운영되고 있는 위와 같은 보안 시스템들은 다음과 같은 한계를 가진다.

첫째, 내부자에 의한 기업정보 유출 방지를 위한 각종 보안전략과 세부 방안들을 수립 시 내부 위협요소에 대한 위험분석 과정이 생략되었다. 즉, 기밀성에 따른 자산의 분류, 각 자산의 각종 위협 요소 분석, 위협에 따른 취약점 분석, 유출 사고에 따른 영향도 분석과 같은 사전 분석을 통해 기업 환경에 적절한 보안정책을 수립해야 함에도[8] 불구하고 단순한 솔루션 도입이나 허술한 보안체계로 효과적이지 못한 정보 보호 활동을 수행하고 있다. 이러한 사전 위험분석이 생략된 보안체계는 사용자 접근 통제에도 항상 보안홀이 발생하며, 보안홀의 발생은 결국 기업정보 유출 사고의 한 방법으로 이용된다.

둘째, 보안정책은 모든 내부 구성원들에게 예외 없이 엄정하게 시행되어야 함에도 불구하고 업무 편의상, 상사에 대한 도의상, 인간적 친밀감으로 인하여 보안정책의 예외가 항상 존재한다. 예를 들어 기업의 임원 및 팀장들에게는 많은 경우 모든 권한을 부여하여 운영하고 있으며, 업무 효율성을 높이기 위해 재택근무가 잦은 구성원에게는 랩탑을 사외로 상시 반출할 수 있는 권한을 부여한다. 이러한 예외 권한 부여 시 그 판단 근거를 객관적으로 측정할 수 없을 뿐만 아니라, 그 프로세스를 관리하는 것조차 엄청난 노력이 수반되기 때문에 예외 권한 관리와 같은 보안정책의 엄정한 시행은 현실적으로 상당히 어려운 문제를 가지고 있다.

셋째, 기업 내부 구성원들의 허술한 보안의식이다. 모든 내부 구성원들은 보안의 필요성을 인식하고, 각 기업의 전사적 보안 방침과 세부적 시행 지침 들을 파악하여 이를 실천해야 함에도 불구하고, 그 필요성조차도 인지하지 못하고 있는 실정이며, 이러한 내부 구성원들의 보안 의식에는 보안 업무는 보안 조직에서 수행하는 것이며, 본인의 도덕성에 문제가 없으면 보안사고 책임에 관대할 것이라는 기저가 깔려 있다. 따라서 내부 구성원들의 보안 의식을 증진시키기 위해 지속적이고 정기적인 보안 교육이 필요하며, 이를 통해 내부 구성원들이 자발적으로 관리적, 기술적, 물리적 보안 지침들을 수행할 수 있도록 해야 한다.

넷째, 기업정보 유출 방지 주요 시스템으로 대부분의 기업에서 운영 중인 PC보안과 문서보안 시스템에는 클라이언트의 통제 기능을 무력화 시키는 보안홀이 존재하며, 기술적으로 완벽하게 제어 가능한 방법이 없다. 예를 들어, 국내 문서보안 제품 중에 하나는 특정 확장자를 지정하여 다른 이름으로 저장 하였을 경우 암호화 문서가 일반 문서로 변경됨으로써 암호화된 문서를 무력으로 보안해지 할 수 있다. 또한 해킹도구를 이용하여 보안 클라이언트의 프로세스를 강제 종료하여 여러 매체에 대한 접근 통제를 무력화 시킬 수 있다.

다섯째, 많은 보안 시스템의 경우 제어 대상에 대한 종속성이 존재하여, 제어 대상의 환경이 변경될 경우 이를 빠른 시간 안에 업데이트해야 함에도 불구하고, 국내 벤더의 유지보수 능력은 환경의 변화를 신속하게 따라가지 못한다. 예를 들어, 문서보안의 경우 운영체제나 문서 편집기의 신규 버전이 출시되면 그에 따른 기능도 업데이트 되어야 본래의 제 기능을 수행할 수 있음에도 불구하고 그 변화를 따라가지 못하여 다양한 위협 가능성을 제공한다. 또한 문서보안 솔루션은 보안정책의 변화에 맞게 유연하게 설계되어야 함에도 불구하고, 기업 부문별로 보안정책을 달리 가져갈 경우 보안 클라이언트를 수정해야 한다는 한계가 있다. 즉, 솔루션이 제공하는 기능과 성격의 한계로 인하여 환경의 변화에 따른 유지보수가 필요하며, 신속하지 못한 대처에는 항상 보안 위협이 뒤따른다.

기업은 정보유출로 인한 피해의 심각성을 피부로 느끼고 있으며, 이를 대비하기 위해 다양한 보안 기술과 솔루션들을 이용하여 다양한 보안 전략과 보안 체계를 수립 중이다. 현재 많은 기업의 경우 기업정보 유출에 대비한 기본 체계는 마련하였으나, 보안 업무의 특성, 보안 기술의 한계, 보안 시스템 운영상의 어려움으로 인하여 앞으로도 극복해야 할 난제들이 많이 남아있다. 특히, 기술 구현의 측면에 있어서 두 가지 문제를 시급하게 해결해야 한다.

첫째, 기업정보 유출 사고를 사전에 차단하기 위하여 유출경로, 위협요소 대한 분석이 이루어진 후 그 결과를 기반으로 유출 가능성이 있는 사용자의 비정상 행위를 통합적으로 정확하게 분석하는 기능이 요구된다. 이는 권한이 있는 내부 구성원을 완벽하게 통제하는 기술은 현실적으로 구현하기 어려우므로, 정보 유출 행위를 사전에 모니터링하여 이를 가시화하는 기능이 필요하기 때문이다. 그리고 유출 경로를 토대로 비정상 행위를 분석하는 기능은 보안사고 발생 시 조사 및 추적체계에 도움을 줄 수 있다.

둘째, 마찬가지 이유로 현실적으로 내부 구성원의 모든 행위를 감시하는 것은 매우 어렵기 때문에 내부 구성원의 보안 의식을 향상시키는 기능이 절실히 요구된다. 이를 위해서는 적극적 보안 교육 활동이 요구되며, 내부 구성원의 보안 의식을 객관적인 수치로 판단할 수 있는 보안 수준 평가 체계와 보안 수준 자동 진단시스템이 필요하다.

3. 통합 로그분석 시스템

3.1 보안 시스템 분석

통합 로그 분석 시스템을 설계하기 위해서는 기존의 시스템에서 정보가 유출될 수 있는 모든 경로와 위협요소를 분석한 후, 분석된 결과를 바탕으로 정보 유출 가능성을 보이는 비정상 행위를 탐지하는 규칙을 작성하는 것이 필요하다.

3.1.1 유출경로 및 위협요소 분석

위협요소를 분석하기 위한 첫 단계로 기업 정보가 보관되고 유통되는 모든 영역의 정보 자산을 중요도와 유형별로 분류 한다. 유통되는 영역에는 업무 시스템, 네트워크, 데이터베이스, 어플

리케이션, 배치프로그램, 내부 구성원의 업무용 PC, 그리고 각종 저장 매체를 모두 포함하며, 자산에는 영업정보, 기술정보, 고객정보 등의 기밀정보가 포함된다. 다음으로, 그 정보에 접근 가능한 모든 구성원들을 권한별로 분류하는데, 일반적으로 관리자, 운영자, 내부구성원, 협력업체 직원, 제휴 업체 직원, 기술 고문, 퇴직 예정자, 팀장 및 임원 등으로 분류할 수 있다. 이러한 분류와 함께 정보가 유통되는 경로를 분석한 후 <표 1>과 같이 위협요소 목록을 작성한다.

<표 1> 유출경로 및 위협요소 목록

주체	자산	영역	유출경로 및 위협요소
관리자	고객정보	고객DB	DB접근 후 파일 매체저장
운영자	고객정보	고객DB	DB접근 후 파일 매체저장
사용자	고객정보	App.	모니터 화면캡쳐
퇴직예정	고객정보	App.	모니터 화면캡쳐
협력업체	고객정보	App.	모니터 화면캡쳐
임원	고객정보	App.	모니터 화면캡쳐
관리자	특허기술	KMS 1	DB접근 후 파일 매체저장
운영자	특허기술	KMS 1	DB접근 후 파일 매체저장
사용자	특허기술	KMS 1	파일 내려받기 후 메일발송
기술고문	특허기술	KMS 1	파일 내려받기 후 메일발송
협력업체	특허기술	KMS 1	파일 내려받기 후 메일발송
임원	특허기술	KMS 1	파일 내려받기 후 메일발송
…	…	…	…
임원	설계도면	KMS 2	모니터 화면캡쳐

다음 단계로는 위협요소를 상세화하여 모든 유출 경로에 공통적으로 해당되는 위협요소들을 추출한다. 이는 유출행위를 탐지하는데 사용되는 규칙을 생성하는데 기초가 되는 정보이며, 그 중 일반적으로 추출할 수 있는 위협요소들의 일부는 <표 2>와 같다.

3.1.2 위협탐지 규칙 작성

상세 위협요소에 대한 분석이 완료되면 이를 기초로 정보유출 행위를 탐지하는 위협 규칙을 작성한다. 즉, 전 단계에서 분석된 위협이 발생했을 때 그 위협이 정상적인 행위인지 비정상적인 행위인지 판단하는 기준을 정의하는데, 이때 고려해야 할 요소는 유출 대상, 유출자, 특이한 행위, 유출 정보이다. 위협 규칙 작성은 시스템 구현을 위해 상세 위협요소를 구체화하는 작업으로, 유출 시나리오를 토대로 상세 위협요소를 쉐도우 코드 (shadow code)의 형태로 표현한다. 예를 들어, 암호화 문서를 해제하여 USB 저장매체에 문서를 저장하는 형태의 문서보안 위협을 규칙으로 구성하면, ① 지식관리시스템에 접속하여 문서를 다운로드 한 로그 검색, ② 문서보안에서 그 문서를 암호화 해제한 로그 검색, ③ PC보안에서 그 문서를 USB 저장매체에 저장한 로그 검색 등의 시나리오 형태로 규칙을 구성할 수 있다.

<표 2> 주요 상세 위협요소

구분	상세 위협요소
정보수집	특정서버에서 대용량 파일 다운로드
	업무시간 외 대용량 파일 다운로드
문서보안 PC보안	암호화해제 권한 획득 후 대용량 파일 복사
	암호화파일 해제 후 매체에 대용량 파일 복사
네트워크	VPN계정 발급 후 인트라넷 서버 과다 접속
	대용량 파일을 첨부한 메일을 외부로 전송
	인터넷 포탈사이트를 이용한 메일 전송
	FTP서버 접속 후 대용량 파일 전송
기타	P2P, 메신저, 업로드 컴포넌트 설치
	문서 과다 출력
	가상 및 듀얼 운영체제 설치

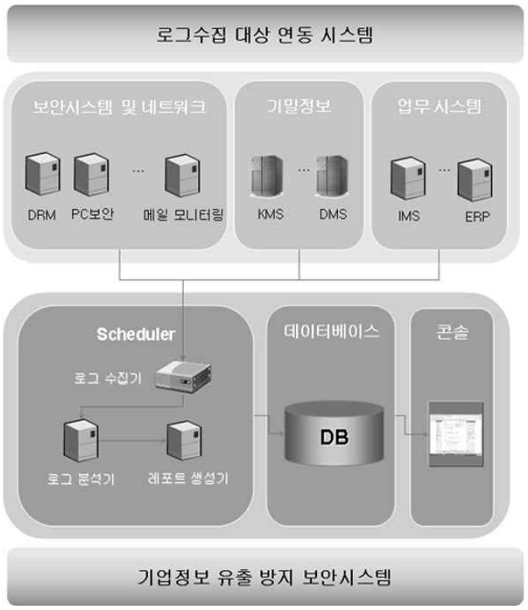
3.2 시스템 설계

3.2.1 시스템 구성

유출행위 탐지를 위한 기초 데이터로서 각 단위 시스템에서의 행위 로그들을 수집하기 위해서는 각 단위시스템의 연동이 필요하다. 단위시스템의 연동을 통해 확보할 로그는 크게 구성원들의 단말을 제어하는 문서보안, PC보안 등을 포함하는 각종 보안시스템과 네트워크 접근 및 사용 로그, 기밀정보가 보관된 지식관리시스템, 문서관리시스템 등의 인트라넷 시스템의 접근 로그, 그리고 사용자들의 정보와 행위를 분석하기 위해 인증서버 및 인사연동 시스템과 ERP시스템에서 생성되는 로그를 포함한다.

본 연구에서 설계한 보안시스템은 크게 3가지 모듈로 구성되며, 연동된 단위시스템으로부터 로그들을 수집하는 로그수집 모듈, 사전에 분석한 위협 시나리오를 기반으로 작성된 규칙을 이용하여 유출행위를 탐지하는 로그분석 모듈, 로그분석 모듈에 의해 산출된 각종 결과들을 데이터

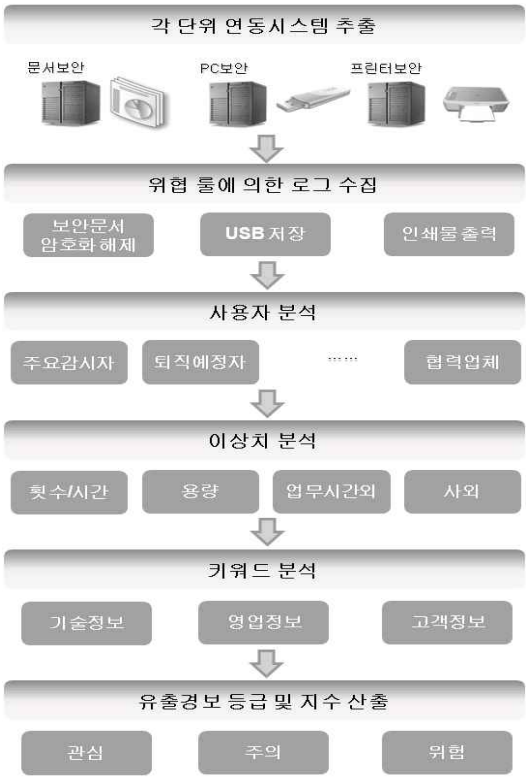
베이스에 저장하고 관리자가 이를 모니터링하거나 분석할 수 있도록 콘솔 정보에 맞게 가공하여 보고서를 생성하는 보고서 생성 모듈로 구성된다. 각 모듈은 스케줄러에 의해 실행되며, 산출된 결과를 저장하기 위하여 데이터베이스를 이용한다. 저장된 각종 결과들을 확인할 수 있도록 운영자 콘솔을 웹화면으로 제공한다. 전체 시스템의 구성도는 (그림 1)과 같다.



(그림 1) 시스템 구성도

3.2.2 시스템 워크플로우

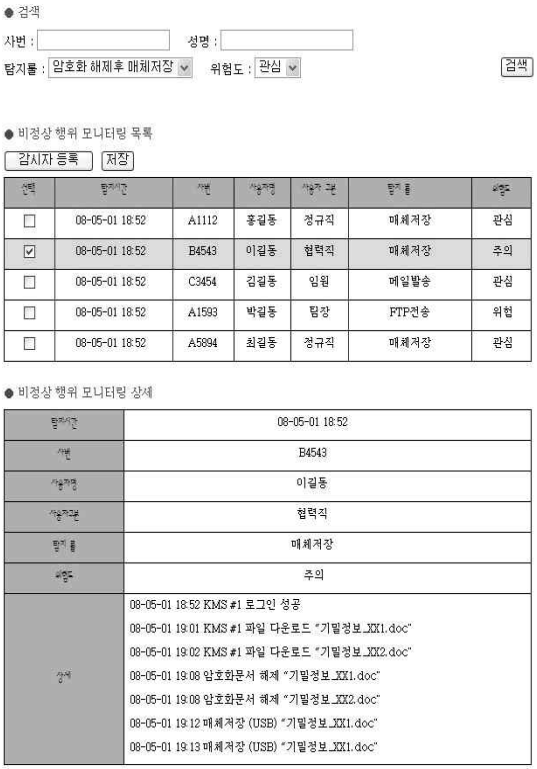
규칙 기반 기업정보 유출 탐지 과정은 다음과 같다. 단위시스템에서 로그를 수집한 후 해당 규칙에 의해 탐지된 위협은 사용자 분석, 이상치 분석 및 키워드 분석을 실행한다. 사용자 분석에는 우선 권한을 가지고 있는지의 여부를 판단하며, 일반 사용자, 퇴직 예정자, 주요 감시자, 기밀정보 관리자, 외부 인력인지를 파악한다. 이상치 분석에는 시간 단위 당 위협 회수와 시간대를 분석하며, 위협의 내용이 파일 복사인 경우 그 용량을 분석하고, 유출자의 위치가 사내인지 사외인지를 분석하며, 유출자 본인의 단말인지 판단하기 위하여 IP주소를 체크한다. 그 다음 단계는 유출한 내용의 키워드 분석을 통하여 유출 여부를 판단하며, 마지막으로 정보 유출 등급을 측정하기 위해 시스템 분석단계에서 산출된 심각도를 고려하여 보안지수를 산출한다. 전체적인 프로세스 흐름은 (그림 2)와 같다.



(그림 2) 프로세스 흐름도

3.2.3 화면 설계

비정상 행위 탐지 화면은 (그림 3)에서 보는 바와 같이 위협 행위 규칙에 의해 탐지된 비정상 행위들을 실시간으로 업데이트하면서 시간, 사용자 정보, 탐지된 규칙 명, 위험도를 보여준다. 이 때 운영자는 의심이 되는 사용자를 주요 감시 대상자로 설정할 수 있다. 특정 이벤트를 선택하면 화면 하단에 선택된 이벤트에 대한 상세 정보를 보여준다. 상세 정보는 각 단위 시스템에서의 단위 로그들을 모두 보여주어 분석이 가능하도록 한다. 또한 검색 기능을 제공하여 과거에 발생했던 비정상 행위들을 조회할 수 있도록 하였다.



(그림 3) 비정상 행위 탐지 화면

3.3 유용성 검증

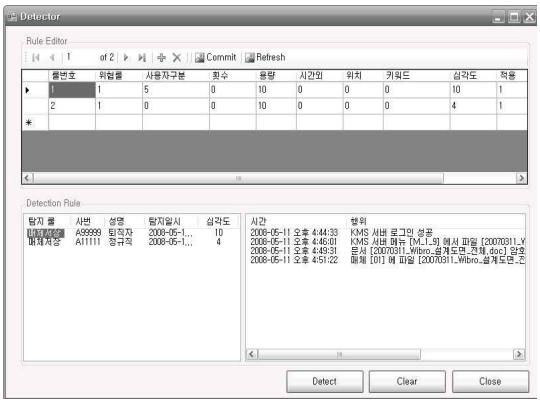
3.3.1 유출 시나리오

본 연구에서 제안된 시스템의 유용성 검증을 위해, 현재 운영되고 있는 보안시스템에서 정보유출 행위 탐지가 불가능하거나 기존 단위 시스템의 로그가 확보되어 있다고 하더라도 현실적으로 분석이 어려운 정보 유출 시나리오를 가정한다. 또한, 가정한 시나리오에 근거하여 하나의 위협 규칙을 작성한 후 설계에서 제안한 대로 탐지 모듈을 구현하여 유출행위 탐지 여부를 확인하였다. 대략적인 정보유출 시나리오는 (그림 4)와 같다.

(그림 4) 정보유출 가상 시나리오

3.3.2 탐지모듈 구현 및 탐지 결과

가상 시나리오에 적합하도록 KMS서버의 사용자 인증 로그 테이블, 파일 다운로드 로그 테이블, 문서보안 암호화 해제 로그 테이블, PC보안 매체 저장 로그 테이블을 임시로 작성한 후 위협 시나리오에 해당하는 위협 규칙을 코드로 구현하였다. 그리고 이상치 분석을 위한 기준치를 다양하게 설정하여 여러 개의 규칙을 구성한 다음 시나리오에서 가정한 정보 유출 행위를 탐지한다. 실제 정보유출 시나리오에 해당하는 로그를 생성한 후 정보 유출 행위를 탐지한 결과는 (그림 5)와 같다.



(그림 5) 정보유출 행위 탐지 결과

그림에서 볼 수 있듯이, 제안된 시스템은 각각의 위협 규칙에 의하여 탐지된 위협 행위에 관한 다양한 정보(관련 위협 규칙(룰), 행위자, 행위일시, 심각도, 관련 로그 등)를 실시간으로 관리자에게 알려주고 있다. 이러한 탐지 시스템은 정보가 수집되는 단계부터 실제 정보가 외부로 전송되는 전체 유출경로를 파악할 수 있게 하며, 이는 마지막 단계에서 유출 행위를 탐지하는 방식에 비해 보다 정확한 탐지 결과를 제공한다. 또한 위협 규칙을 작성하는 단계에서 설정한 보안지수를 제공하여 보안 관리 운영자에게 탐지 결과에 대한 초기 대응과 보안정책을 재정립하는데 도움을 줄 수 있다.

4. 결론

오늘날 권한을 가진 내부 구성원들에 의해 기업의 기밀정보가 유출되는 피해 사례가 증가하고 있으며, 기업에서는 이를 대비하기 위해 각

비즈니스 환경에 맞는 보안체계와 시스템을 구축하여 정보보호를 위해 노력하고 있는 중이다. 그러나 이 같은 노력에도 불구하고 기밀정보 유출 차단이나 탐지를 효과적으로 수행하고 있지 못하며, 특히 유출사고 발생 시 피해를 최소화하기 위하여 사고 경위를 효율적으로 추적할 수 있는 체계를 마련하지 못하고 있는 실정이다. 또한 기업의 보안 수준을 제고하기 위하여 여러 가지 보안지수를 반영하여 이를 판단하는데, 그 판단 근거로서 내부자에 위한 위협수준은 전혀 반영되고 있지 않다.

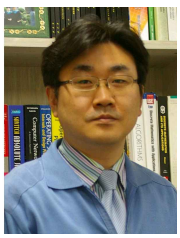
이에 본 논문에서는 내부자에 의한 기업정보 유출을 방지하기 위해 시행되고 있는 여러 가지 정보보호활동과 각종 보안기술의 한계를 분석함으로써, 제안하고자 하는 통합 로그분석 시스템의 설계 방향을 도출하였다. 기업 내 각종 단위 시스템으로부터 로그 자료를 수집하여 내부 구성원들의 기밀정보 유출 가능성 행위를 통합 분석하며, 이를 바탕으로 기업 내 각 부문의 보안지수를 생성하는 통합 로그분석 시스템을 제안하였다. 제안된 시스템은 내부 구성원에 의한 기업정보 유출 행위를 보다 효과적으로 탐지할 수 있으며, 생성된 보안지수를 이용하여 보안정책을 재정립하고 내부 구성원들의 보안의식을 향상시키는데 도움을 줄 수 있을 것이라 판단된다. 제안한 시스템은 내부 구성원의 각종 행위가 로그 자료로 보관되고 관리되는 기업 환경에 적용 가능하며, 실제 기업의 보안시스템으로 활용하기 위해서는 위협 시나리오를 상세화하여 위협 규칙을 정교화하는 연구가 필요하다. 또한 보안 수준을 판단하는 보안 지수의 정확성과 위협 경보의 오용 알람을 방지하기 위해 위협 경보의 단계 구분과 지수 측정을 위한 기준치 설정 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] “2008년 국가 정보보호 백서”, 국가정보원(2008)
[2] 김종원, 최종욱(2003), “기업정보 유출 방지를 위한 기술”, 정보보호학회지, 10권 2호, 한국정보보호학회
[3] 노시영(2007), “기술유출 방지를 위한 정보시스템 보안 방향”, 산업기밀보호센터
[4] “산업기술유출방지법 요해”, 산업기밀보호센터(2007)
[5] 이호균, 이승민, 남택용, 장종수(2006), “기밀정보 유출 방지 기술동향”, 정보통신연구진흥원
[6] 정희조, 김진영, 임춘성(2004), “기업의 정보보호수준 및 성숙도 진단을 위한 정보보호수준 통합평가시스템 개발에 관한 연구”, 정보보호학회지, 14권 4호, 한국정보보호학회
[7] IBM(2006), "Stopping Insider Attacks - How Organizations Can Protect Their Sensitive Information", IBM
[8] NIST(2001), "Risk Management Guide for Information Technology Systems", NIST

이 재 용

1999년: 아주대학교 일반대학원(공학석사)
2008년: 한양대학교 교육대학원 컴퓨터교육전공 석사과정
2002년~2005년 : 한국정보보호진흥원 연구원
관심분야 : 정보보호



강 수 용

1996년 : 서울대학교 수학과 (이학사)
1998년 : 서울대학교 전산과학과 (이학석사)
2002년 : 서울대학교 전기컴퓨터공학부 (공학박사)
2003년~현 재 : 한양대학교 정보통신학부 조교수
관심분야 : 운영체제, 저장시스템, 정보보호