내부정보유출방지를 위한 DLP시스템 연구★

유 승 재*

요 약

현대의 정보통신 기술과 네트워크 기술이 발달은 기업의 운영환경을 스마트하게 변화시켰으며, 그 가운데서 수많은 데이터들이 생성되고 저장되고 사용되고 있다. 기업경영의 에너지원이 되는 중요한 정보는 경제적인 이윤과 가치를 생성하고 또한 강력한 영향력의 근거로 활용된다. 따라서 주요정보는 그 가용성과 편의성을 확보해야 함과 동시에 기밀성과 무결성을 담보해야 하는 것이며 이것이 바로 정보보호의 기본목표가 된다고 할 수 있다. 그러나 대부분의 기업들은 중요한 내부정보가 유출되어 심각한 피해를 야기하는 사고가 증가하고 있다. 이에 본 연구에서는 내부정보유출을 방지하고 안정적인 데이터보안 및 정보보호관리 구축을 위한 DLP(Data Loss Prevention) 기술과 솔루션에 대해 살펴본다.

A Study on DLP System for Preventing Internal Information Leakage

Seung Jae Yoo*

ABSTRACT

The development of modern ICT and network technologies has made the business environment smart.and under such circumstances, a great deal of data is being generated, stored and used. The important information that becomes an energy source for corporate management creates economic profit and value and is also utilized as a basis for strong influence. Therefore, important information must ensure its availability and convenience while ensuring confidentiality and integrity, which is the basic objective of information protection. However, most companies are seeing more and more incidents of serious damage due to the leakage of important internal information.

In this study, we deal with the Data Loss Prevention (DLP) technologies and solutions to prevent internal information leakage and establish stable data security and information protection management.

Key words : DLP, Endpoint Protect, Sensitive data

접수일(2018년 11월 29일), 수정일(1차: 2018년 12월 17일), 게재확정일(2018년 12월 31일)

★이 논문은 2018년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임.

* 중부대학교 정보보호학과

1. 서 론

현대의 정보통신 기술과 네트워크 기술이 발달은 기업(민간, 공공, 영리, 비영리를 포함한 일반적인 단체 일체 표현)의 운영환경을 스마트하게 변화시켰으며, 그 가운데서 수많은 데이터들이 생성되고 저장되고 사용되고 있다. 기업경영의 에너지원이 되는 중요한 정보는 경제적인 이윤과 가치를 생성하고 또한 강력한 영향력의 근거로 활용된다.

따라서 주요정보는 그 가용성과 편의성을 확보해야 함과 동시에 기밀성과 무결성을 담보해야 하는 것이며 이것이 바로 정보보호의 기본목표가 된다고 할 수 있다.[11]

그러나 대부분의 기업들은 중요한 내부정보가 유출되어 심각한 피해를 야기하는 사고가 증가하고 있다.

특히 이러한 내부정보의 유출사고는 내부 직원이나 외부협력업체 직원에 의해서 발생하고 있으며, 그 주요한 유출 경로로는 문서출력물, 모바일 디바이스나 휴대용저장장치로 복사 또는 이메일, 웹메일, 웹하드, 웹어플리케이션, 인스턴트 메시징(IM) 등 다양한 형태로 나타나고 있다.

개인정보 및 민감데이터에 대한 CIA확보는 정보서비스산업에서는 물론 4차 산업시대의 가장 기본적 요구사항이며 절대적 필요사항이라 할 수 있다. 이에 본 연구에서는 내부정보유출을 방지하고 안정적인 데이터보안 및 정보보호관리 구축을 위한 DLP(Data Loss Prevention) 기술과 솔루션에 대해 살펴본다.

2. 관련연구

‘2017 탈레스 데이터 위협 보고서에 의하면 글로벌 금융 서비스 기업의 49%가 데이터 유출 사고를 경험한 것으로 나타났다. 또한, 응답자의 90%가 데이터 위협에 대해 취약점을 느끼고 있으며 78%의 응답자는 주요 데이터를 보호하는데 더 많은 비용을 소비하고 있다고 조사됐다.

불과 10여 년 전까지만 해도 기밀정보유출은 지금의 DLP에 대한 개념과 달리 주로 외부공격에 의한 피해로 인식하였었고, 이를 반영한 대응기술로서 Secure Content Management(SCM), Outbound Content Compliance(OCC), Information Leakage Detection and Prevention(ILD&P) 등이 IDC (International Data Corporation)에 의해 소개되었고, CMF(Content Monitoring and Filtering)가 가트너(Gartner)에 의해 소개되었다. 이러한 솔루션들은 내부자에 의한 정보유출 방지 뿐 아니라, 외부 공격에 의한 정보유출 방지를 모두 고려한 개념으로 다음과 같이 정의되었다.[1]

- SCM(Secure Content Management)은 웹, 이메일 및 인터넷 응용 프로그램을 통하여 내부 망에 유출·입 되는 비정상 콘텐츠에 대하여 바이러스 차단, 스파이웨어 차단, 웹 필터링, 메시징 보안 등의 4대 보안 기능을 포함하는 통합 콘텐츠 보안 솔루션이다. 특히 메시징 보안은 e-mail, IM, SMS 그리고 P2P를 통하여 유포되는 스팸 및 성인 콘텐츠를 필터링하는 기능뿐만 아니라, 내부 기밀정보의 유출을 탐지하고 차단하는 기능을 포함한다.
- OCC(Outbound Content Compliance)는 이메일, IM, P2P, FTP, 웹 포스팅 그리고 이외의 메시징 트래픽에 포함되어 내부로부터 유출되는 콘텐츠를 감시하고, 암호화, 필터링 및 차단 기능을 제공하는 솔루션이다. OCC는 공공기관과 산업체의 내부 규정(HIPAA, GLBA, SOX 등) 위반, 조직 내부의 이메일 정책이나 관행에 위반, 지적재산권 유출, 기밀정보 유출, 성인 콘텐츠 유포 등에 대한 방어 기능을 포함하고 있으며 크게 email filtering, secure email (encryption), multi-protocol content filtering, instant messaging security, ERM 등 5분야로 나눌 수 있다.
- ILD&P (Information Leakage Detection and Prevention)는 내부의 민감 정보의 불법 유출을 최소화하기 위하여 보안 솔루션을 포함하는데, ILD&P 시장이 성장할 수 있는 동력은 법적인 요인과 기술적인 요인이 있다. 기업 환경에서 인스턴스 메신저와 P2P 프로그램과 같은 네트워크 응용 프로그램의 증가에 따른 기밀유출 가능성의 확대와 정보 유출 사고의 증가 등 기술적인 요인과 Data Protection Directive (EU), SOX(미), HIPAA(미), GLBA(미), California SB 1386(미), 일본의 개인정보 보호 법 등 법적인 요인에 있다.

- CMF(Content Monitoring and Filtering)는 내부망에 유출·입 되는 트래픽의 패킷을 캡처링하고 세션관리를 통하여 언어 기반으로 내용을 분석함으로써, 사전에 정의된 룰이나 정책에 의해 기밀정보의 유출을 탐지 및 차단하는 기능을 제공한다.

3. DLP 솔루션 동향

기본적으로 개인 및 기업의 민감데이터의 누출은 막대한 금전적 피해는 물론 기업의 신뢰상실로 이어지는 심각한 문제를 야기한다. 내부 직원이나 협력업체들의 절도 또는 과실로 인하여 소스코드가 유출되는 경우가 발생할 수 있고 이어서 범죄자들이 소프트웨어에 악성코드를 심어 공격하게 때문에 민감데이터에서 소스코드의 위험성도 간과할 수 없다. 따라서 내부에 소스코드를 보호할 수 있는 기능을 탑재하는 것도 DLP솔루션의 요구사항이 될 것이다.[5]

유럽에서의 GDPR, HIPAA, FISMA 및 미국의 NIST와 같은 데이터 보호 규정의 증가로 규정 준수를 보장하기 위한 데이터손실방지 도구의 필요성이 증가했지만, 많은 기업들은 아직도 이를 채택하는 것을 주저하고 있다. 왜냐하면 그들은 DLP가 생산성을 떨어뜨린다거나, 중소기업에는 도입효과가 없다거나, 구현이 어렵고 오랜 시간이 소요된다는 라는 잘못된 인식이 처음부터 심어져 있기 때문이다.[2]

그리고 DLP 관련 밴더와 개발업체들의 접근방식 차이로 인해 나타날 수 있는 DLP에 대한 혼동이나 오해가 있을 수 있는데, 다음은 그 몇 가지 사례들을 언급해 놓은 것이다.

3.1 DLP의 기능과 한계[3]

- DLP솔루션의 멀웨어 대응에 관한 의문이 있을 수 있다. Data Loss Prevention은 데이터 침해를 방지하고 데이터 일치, 규칙 및 정규식 일치, 키워드 등과 같은 특정 탐지 기술을 기반으로 엔드포인트에서 전송, 사용 또는 저장된 기밀 데이터를 탐지하는 기술이다. 따라서 멀웨어와 같은 외부위협에 대해서는 DLP가 아니라 바이러스백신솔루션을 통해 대응하는 것이 적절하다.
- 악성코드나 불법 콘텐츠 유통에 관한 문제가 심각하게 대두되고 있다. 이에 대해 DLP에서 특정 웹사이트의 탐색을 차단하거나 응용 프로그램 사용을 차단할 수 있는가에 대한 오해가 있을 수 있다. DLP의 목표는 직원들이 일상적인 업무를 수행하는 데 도움이 되는 웹 사이트 액세스나 응용 프로그램의 사용을 완전히 차단하는 것이 아니라 이메일, 인스턴트 메시징, 클라우드 스토리지 앱, 휴대용 저장 장치 등과 같은 도구를 통해 발생할 수 있는 기밀 데이터의 유출을 방지하는 것이다. 그러나 DLP 솔루션도 이러한 기능을 제공하지만 특정 웹 사이트와 웹 페이지의 탐색을 차단하는 것은 UTM솔루션의 일부로써 웹 필터링 솔루션을 통해 대응하는 것이 적절하다.
- 회사의 규모와 관계없이 개인정보를 포함한 비밀데이터는 존재하며, 의도/비의도적인 내부직원에 의해 유출될 수 있고, 정보유출에 대한 법적책임이 강화되는 현실에서 오히려 법적대응능력이 상대적으로 부족한 중소기업에서의 DLP 구현은 오히려 필수적이라 할 수 있다.
- 사용자가 다운로드하는 항목에 대한 가시성을 제공하는 DLP 툴이 있지만, DLP는 그렇게 하는 것이 일반적이지 않다. 이는 주로 솔루션의 목적이 무엇이 들어오는지를 제어하기 위해서가 아니라 민감한 데이터가 회사 네트워크 밖으로 나가는 것을 막기 위한 것이기 때문이다. 데이터 유출은 일반적으로 허가되지 않은 직원이 IT 부서의 제어가 제한된 클라우드 등으로 기밀 파일을 악의적인 사람 또는 개인 이메일 주소로 보낼 때 발생한다. 따라서 엔드포인트에서 다운로드하는 사용자를 DLP솔루션에 의해 제어/모니터링 할 수 있는가는 별개의 사안이라 할 수 있다.
- DLP속성에는 엔드포인트 위치를 포함하고 있지 않으므로 GPS 추적시스템이 있다하더라도 DLP솔루션에 의해 그 위치를 파악할 수는 없다. (참고로 컴퓨터의 위치를 파악하려면 WIFI 기반 위치를 파악할 수 있는 추적 장치나 소프트웨어가 필요하다.)

3.2 DLP제품과 효율성 평가기준

[1]에서는 기밀정보유출방지 제품의 평가기준으로 다음과 같이 제시하고 있다.

- 정확성 : file type이나 트래픽 양에 무관한 인식 및 정상작동
- 적용지점 : 네트워크와 엔드포인트 모두 감시
- 설정 : 정책생성지원 / 비구조화된 데이터의 판단
- 관리/보고 : 계층화(그룹화)된 접근권한정책지원 등
- 적용용이성 : 어플라이언스 형태의제품 지원/ 트래픽 감시장비 적응
- 증거보관 : 트래픽캡쳐 및 복원/로그자료 법적효력
- 적용방법 및 부가기능

다음으로 DLP를 구현하는 것이 효율적인지 확인하는 방법을 소개하였다.[4] DLP가 목적을 달성하는지 여부를 확인하기 위해 IT 관리자가 따를 수 있는 여러 가지 지표로써 기밀 데이터 전송 시도 횟수 및 심각도, 확립된 기준에 따라 보안 이벤트를 캡처할 수 있는 기능, 관리자의 불만 사항 수, 리소스 소비량 등을 사용하였다. 현재 위협 지형과 내부자에 의한 침해 건수를 감안할 때 Data Loss Prevention에 대한 수요는 지속적으로 증가하고 있다. 따라서 모든 기업들은 이용 가능한 적절한 DLP솔루션의 구축 · 운영을 위해, 소프트웨어의 효율성을 고려한 평가기준을 수립하고 적용해야 할 것이다.

DLP솔루션 도입에 따른 효율성 평가를 위한 기준이다. '투자 수익률 측정'과 'DLP의 효율성 판단근거'를 제시함으로써 이것을 근거로 DLP솔루션의 도입·운영을 결정할 수 있을 것이다.

무엇보다도, Data Loss Prevention의 목적은 침해가 발생하지 않도록 방지하는 것이다. 각 공급업체의 솔루션에 따라 IT 관리자는 서로 다른 채널을 통한 기밀 데이터 전송을 차단하고 모든 시도는 기록(case1)되도록 하거나 아니면 허용하고 모든 전송이 보고되도록 선택(case2)할 수 있다. 그러므로 DLP 솔루션의 성공 여부를 측정하는 것은 회사가 그것을 어떻게 사용하는지에 달려있다.

첫 번째 상황(case1)에서는, 시도 횟수와 심각도를 고려한다. 그것은 양적 데이터를 보는 것에 관한 것이지만 질적 정보에 관한 것이 때문에 DLP가 효율적인지 여부를 알 수 있는 데 좋은 지표가 될 것이다.

두 번째 상황(case2)에서는, DLP 솔루션이 실제로 위반을 방지하지는 못하고 단지 기밀문서와 관련된 사용자의 활동에 대한 가시성만을 제공하기 때문에 관리자는 상황이 변하는 것을 고려해야 한다. 이 경우 효율성은 지정된 기준과 관리자의 응답 시간에 따라 이벤트를 캡처할 수 있는 능력에서 비롯되며, 이를 통해 정책을 신속하게 변경하고 특정 데이터/파일 또는 사고 보고를 관리자에게 전송하여 추가 조치를 취할 수 있다.

DLP 소프트웨어 효율성을 나타내는 지표로서 직원들의 불만 건수도 고려된다. DLP배치로 일상 업무에 영향을 받는 사용자들의 불만이 증가한다면, 이는 DLP가 극도로 거슬리고 직원 생산성에 영향을 미친다는 것과 또한 이런 유형의 상황을 제거하기 위한 정책이 잘 조정되지 않는다는 것이다. Data Loss Prevention 효율성은 제공된 기능뿐만 아니라 원하는 목표에 따라 정책을 조정할 수 있는 능력에도 의존한다. 그래서 DLP는 규칙과 정책을 세밀하게 조정하는데 사용되는 기술만큼이나 효율적이다.

마지막으로, 총소유비용(Total cost of ownership, TCO) 측면에서 리소스 소비(DLP 정책을 관리하는데 포함된 인력 및 소프트웨어에 익숙해지는데 소요되는 시간과 보고서를 분석하는 데 소요되는 시간 등)는 DLP 시스템의 효율성을 결정할 때 중요하다. TCO는 도구 자체의 비용과 관련 비용을 기준으로 계산할 수 있는데, DLP의 관리 콘솔이 직관적일수록 학습곡선이 낮아져 필요한 리소스가 줄어든다.

3.3 국내외 DLP상용제품 특징

공공과 민간을 망라하고 모든 기관에서는 엄청난 양의 정보를 안전하게 관리해야 하는 의무를 지니고 있다. 현재 대규모 정보시스템 운영 기관에서는 의무적으로 정보보호관리시스템을 구축하고

그에 따라서 정보를 안전하게 관리되도록 되어 있으나 실제로 개인정보를 포함한 주요정보유출의 위협은 점점 더 커져가고 있다. 이에 따라 각 기관에서는 기밀정보가 어디에 보유되어 있는지 식별하고, 식별된 기밀정보가 유출되는 것을 차단하며 유출(시도)의 사전 예방 및 감사를 통해 기관의 주요정보를 관리하는데 집중하고 있는데 이것을 DLP(Data Loss Prevention)라 하며, 주요정보 파악 및 식별, 기밀정보 사전 차단, 정보유출에 대한 감사 및 예방을 DLP 3요소라 할 수 있다.[7] DLP3요소를 실행하는 과정은 정보의 라이프사이클(수집-저장-관리-이용-파기)에 따른 다단계 전략이 필요하다.

기본적으로 개인정보자산의 식별 및 암호화 저장을 바탕으로 이용 및 제공의 과정에서 적절한 통제가 필요하다. 저장된 정보이용에 있어서 비정상적인 징후의 파악을 위해 DBMS와 각종 어플리케이션에서의 개인정보 조회나 접속기록의 분석이 요구된다. 또한 USB저장, 출력, 네트워크를 통한 유출의 통제가 필요하다.

이 때, 엔드포인트DLP의 경우 부분적으로 네트워크 통제기능이 부가된 경우도 있으나, 일반적으로 플랫폼과 OS환경에 따라 설치가 불가한 경우가 있고, 수많은 엔드포인트 각각에 유출패턴을 업데이트한다거나 또는 각각 DLP에이전트에서 생성되는 로그를 통합 관리하는 것은 절대적으로 무리여서 에이전트방식의 엔드포인트DLP로는 인터넷 전송을 통한 유출통제를 기대하기 어려운 상황이다.

따라서 이 과정에는 인터넷을 통한 정보유출을 차단하는 네트워크DLP의 설치 운영이 필요하다.

즉, 엔드포인트DLP는 PC나 노트북 등 유무선 단말디바이스에서의 파일이나 콘텐츠의 USB/OTG로 복사 또는 출력물을 통한 유출을 방지하고, 또한 블루투스/RF/테더링 등을 통한 정보유출은 차단하는 기능을 수행한다. 그리고 네트워크DLP는 개인정보유출 차단을 위하여 이메일, 메신저, 웹하드 등 네트워크에서 수집하고 차단하는 기능을 수행한다. [7]

네트워크 DLP의 경우 보통 어플라이언스 장비를 네트워크에 인라인 또는 탭 방식으로 설치해 네트워크를 통해 나가는 이메일, 메신저에 대한 데이터 유출을 차단하거나 모니터링 한다. 초기설치와 관리가 쉽고, 네트워크를 통한 유출방지에 특화 되어있다는 특성 때문에 인터넷을 통한 외부연결이 필수적인 현대 기업이 선호하는 DLP 방식이다. 네트워크 DLP는 사내메일, 포털 웹메일, 메신저, 웹하드, FTP, P2P를 통해 외부로 유출되는 데이터를 회사 보안정책에 따라 차단 및 기록을 수행한다. 상대적으로 전송량이 매우 많고 피해가 심한 네트워크 유출에 대해 전문적인 모니터링 및 차단을 지원한다.[8]

예를 들어, 국내 대표적인 DLP솔루션 업체인 D사의 솔루션(엔터프라이즈DLP)은 최신기술로서 GDPR (General Data Protection Regulation)의 기준을 준수하여 보안웹상에서의 DLP, 클라우드에서의 DLP, 빅데이터 검색방식 DLP 등 세부적인 기능을 수행하도록 두 가지DLP를 통합된 솔루션으로 개발되어 있다.[7]

또한, C사의 경우는 SSL통신으로 인해 해석할 수 없는 암호화 트래픽 복호화 문제 처리 그리고 콘텐츠 내용인식기반(Contents Awareness)으로 작동하는 통합된 DLP솔루션으로 개발·구현되어 있다.[8]

해외 대표적인 S사의 DLP솔루션은 아래 표[1]와 같이 상시 각종 저장매체나 네트워크 전송수단별 감시망을 구축하고 엔드포인트 집중관리 및 정보의 흐름가시성 확보를 주요 특징으로 한다. 또한 기밀데이터 면밀한 탐지를 위해 데이터를 서술된 데이터, 구조적데이터, 비구조적데이터, 비구조적 텍스트 , 문서양식 등으로 구분하고 콘텐츠인식기반 DLP로 구현되어 있다.[9]

<표1> S사 DLP 동작프로세스

검색/식별	모니터링
- 데이터 검색 - 보유 목록 생성 - 정리 및 관리	- 데이터사용방식 확인 - 문장과 문맥 이해 - 전사환경 가시성 확보
보호	관리
- 정책위반 확인 - 예방적 보호 - 중요데이터유출방지	- 통합정책 정의 - 유출사고 대응 및 보고 - 중요정보 정화한 탐지

4. 결론

기본적으로 개인이나 기업의 민감데이터 누출사고는 금전적 손실은 물론 기업의 신뢰를 떨어뜨려 기업의 존폐까지 위협할 정도의 엄청난 문제를 야기할 수도 있음을 인식해야 할 것이다. 이와 같은 정보유출에 의한 피해를 막기 위한 대응으로써 본 연구에서 언급한 DLP 솔루션이 제공하는 일반적인 주요 기능으로는 접근제어, 암호화, 필터링, 모니터링이라 할 수 있다. 아울러 서버나 엔드포인트의 클라우드 기반 서비스의 확대에 발맞춰 기밀자료를 계속 주시하고 유출시도를 감시할 수 있는 시스템 환경을 위해 동작에 기반을 둔 콘텐츠 인식보호를 통한 DLP기술구현이 적절할 것으로 판단된다.[10]

내외부 인력에 의한 고의적 정보유출 시도나 우발적 데이터 유실/유출을 방지하고, 또한 인가되지 않은 인원의 부적절한 데이터 접근을 차단하고, 복사 및 붙여넣기를 비롯한 모든 데이터 전송을 모니터할 수 있도록 중요 콘텐츠 보호를 위해 외부장치, 어플리케이션, 온라인서비스 등을 통한 모든 데이터 전송 감시하고 위반 발견 즉시 차단 및 보고(증거확보)할 수 있는 신뢰할 수 있는 안전한 DLP시스템을 구현할여야 할 것이다.

물론 이렇게 한 것으로 위협이 해소되는 것은 아니므로, 모든 보안정책의 일환으로서 DLP 역시 일회성 구현이 아니라 과정이라는 사실을 인식하여야 한다.

참고문헌

[1] 이호균, 이승민, 남택용, 장종수, “기밀정보 유출 방지 기술 동향”, 정보통신연구진흥원 주간기술 동향, 제 1256호., 2006, pp.1-12.

[2] “Debunking the Top 3 Myths about DLP”, Andrada Coos, 2018, https://www.endpointprotector.com/blog/author/andrada-coos/)

[3] “Frequently Asked Questions about Data Loss Prevention”, Andrada Coos, 2018, https://www.endpointprotector.com/blog/author/andrada-coos/)

[4] “How to evaluate the efficiency of a Data Loss Prevention solution”, Andrada Coos, 2015, https://www.helpnetsecurity.com/2015/06/22/)

[5] “Keeping Source Code Safe with Data Loss Prevention” Andrada Coos, 2018, https://www.endpointprotector.com/blog/keep-source-code-safe-with-dlp/

[6] 내부정보 유출 방지 (DLP) -매체 제어, 개인정보 검색, 보안USB, MDM, https://www.endpointprotector.com/support/pdf/datasheet/Data_Sheet_Endpoint_Protector_4_CoSoSys_KR.pdf

[7] 소만사 DLP솔루션, https://www.somansa.com/solution/privacy-dlp

[8] 컴트루테크놀로지 DLP, http://www.comtrue.com/security/

[9] Symantec Data Loss Prevention, https://www.symantec.com/ko/kr/products/data-loss-prevention

[10] S-J Yoo, “Study on Improving Endpoint Security Technology”, 융합보안논문지 제18권 36호, 19-26, 2018.

[11] 양환석, 이병천, 유승재, “클라우드 컴퓨팅 환경을 위한 침입탐지시스템 특징 분석”, 융합보안논문지, 제12권 제3호.. pp.59-65, 2012.

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr