개인정보 보안솔류션 동향 연구

이태열
고려대학교 컴퓨터정보통신 대학원 컴퓨터정보통신공학과
email : kddt08@naver.com

Personal information security solution trend research.

Tae-Yeoul Lee
Computer & Information Technology, Korea University

요 약

요즘 현대사회에 들어 개인정보보호 개인정보유출 등 정보보호에 관하여 많은 기업들이 관심을 가지고 DRM(Digital Right Management) 및 pc보안 솔루션을 적극 도입하고 있다 기업의 이러한 투자에도 불구하고 많은 개인정보유출 사고가 지속적으로 발생 하고 있다. PC보안솔루션의 단순 구축이 아닌 기업에 적합한 보안 정책을 사전에 수립하고 정책에 맞는 시스템을 운영한다면 개인정보유출 사고를 미연에 방지 할 수 있을 것이다. 본 논문은 다양한 PC보안솔루션 중 개인정보유출 방지를 위해 PC에 필수 설치되는 보안솔루션을 정의하고, 필수보안 솔루션을 개인정보보호 관점에서 통합 운영하는 방안, 개인정보유출 사고 방지를 위한 효과적인 보안정책 및 동향을 연구하고자 한다.

I. 서론

우리나라는 개인정보유출 사고가 지속적으로 발생하고 있다. 2013년 12월 시중은행에서 고객 개인정보 13만 여건이 유출되는 사건이 발생하였고, 2014년 4월 시중 카드사에서도 1억여건의 정보가 유출 되었다 기업의 중요한 기밀정보와 개인정보의 유출 등 정보보안 사고와 공공기관, 금융기관, 방송사 등 주요 국가시설을 대상으로 한 DDoS 공격, 다양하고 고도화된APT 공격 등 최근의 사이버 테러는 기업 활동에 있어서 정보보안이 더 이상 부가적인 요소가 아닌 기업 활동을 영위하기 위한 필수적인 요소임을 극명하게 보여주고 있다. 이러한 이유로 최근 국내 기업에서의 정보보호 활동은 중요정보의 불법적인 유출 방지와 외부로부터의 공격에 대한 방어 및 차단에 집중되고 있으며 관련된 보안투자도 꾸준하게 증가하고 있다. 또한 기업의 IT 비즈니스 환경은 데스크톱 PC, 노트북, 스마트폰, 태블릿 PC, 가상화, BYOD 등 IT환경의급격한 변화에 따라 복잡화, 다양화되는 추세이며, 과거 인프라를 중심으로 한 외부로부터의 침입 방지에서 데이터를 중심으로 한 내부로부터의 정보유출방지로 패러다임이 변화하고 있다

II. 관련 연구

1.로그 분석

1.1 로그 분석

대부분의 회사에서 모든 시스템에서 생성되는 방대 한 양의 로그를 정기적으로 백업하고 있지만 양도 많을 뿐만 아니라, 무슨 내용이 담겨 있는지 모르며 막상 사용하려면 분석하기도 쉽지 않다. 그렇지만 사고가 발생했을 경우 추적할 수 있는 유일한 자료가 로그이기 때문에 로그 보존은 필수적 이다. 또한 로그 파일은 법적증거자료로 활용하는 것 도 가능하다. 더욱이 보안사고가 발생하기 전에 이상 증후 여부와 외부에서의 해킹시도 여부를 감시하여 알아낼 수 있는 유일한 자료가 바로 로그이며, 정기적인 취약점 진단과 함께 정기적으로 로그를 분석할 수 있다면 Proactive한 보안 대응체계를 구축하는 것이 가능해진다. 특히 방화벽(Firewall)이 나 침입탐지시스템(IDS)이 설치되

지 않은 기관에서는 침입시도여부를감지할 수 있는 유일한판단자료 가 시스템 내부의 로그파일이기 때문에 더욱 로그분석이 필요하다

1.2 최근 로그분석 동향

요즘에 보안시스템 로그 관리 분야의 동향은 통합보안관리(ESM)에서 위험관리시스템(RMS), 보안 정보 및 이벤트 관리(SIEM)에 이르기까지 지속적으로 진화하고 있다. 이중에서 로그 통합 관리를 위해 등장한 SIEM은 이기종 환경의 인프라 및 보안로그를 효율적으로 통합 운영하고 리스크를 낮추기 위한 해결책으로 받아들여지고 있다 방화벽, 침입방지시스템(IPS) 등의 네트워크 정보보호를 위한 보안솔루션들에서 쏟아내는 로그를 분석해 사고를 미연에 방지하는데 중점을 두고 있다. 그래서 요즘에는 유출 방지만이 아닌 비식별화, 암호화 등도 많이 개발되고 있어 개인정보 보호가 얼마나 중요 한지 알수 있다.

2.솔루션 동향

2.1 개인정보 검색 시스템

현재 일반적인 서비스 회사에서 수집하는 개인정보는 공통 필수정보, 상품별 필수정보, 선택정보로 구분되며 공통 필수정보에는 성명, 고유식별정보(주민번호, 여권번호 등), 집 (직장) 주소, 연락처(집, 직장, 휴대폰 중 선택가능), 직업군, 국적 등이 있다. 서비스에 필요한 필수정보는 서비스 상품의 체결 및 서비스에 필수적인 정보로서 해당서비스를 이용하는 고객에 대해서만 별도로 수집하는 정보이다. 이러한 정보를 정보보호하기 위해서는 정보(로그)파일의 검색 대상 항목, 검색 주기 및 검색 결과 통 지 방법에 따라 활용 방안을 분류할 수 있다. 검색 대 상 항목은 공통 필수 개인정보 중 정형화된 패턴으로 추출할 수 있는 고유식별정보 중 서비스에 가장 많이 사용되는 주민번호, 연락처정보 중 휴대폰으로 제한 한 후 필요 시 확대 적용한다. 주기는 관리자가 수동 검색방법, 시스템 자동검색 방법이 있으며 검색때 포머먼스 문제로 검색 스케줄이나 검색 내용등을 조절해야 한다.

2.2 자료유출방지

보조기억매체 통제, 출력물 통제 방식 및 승인 절 차 등을 변경하여 통제 정책을 적용할 수 있다. 예를 들어 보조기억매체 읽기 허용/쓰기 차단 정책, 필요 시 내부 승인 절차를 통하여 보조기억매체를 통한 정 보유출을 방지할 수 있다. 또한 모든 문서에 워터마킹을 생성할 것인지, 문서 출력 시 마다 내부승인을 할 것인지, 모니터링 방식을 선택할 것인지에 대한 정책을 통해서 문서 유출을 관리할 수 있다. Table 3. 과 Table 4. 는 보조기억매체 통제 및 출력물 통제 시 수립할 수 있는 보안 정책이다. 보안을 레벨을 설정해 수동적인 정책에서 적극적인 정책으로 강화되고 있다. 정책 강화에 따라 사용자의 불편함이 증가될 수 있다.

2.3 저자권관리(DRM)

DRM은 문서 접근 권한 등 다양한 정책을 구현 할 수 있다. 연구소 등 인사이동 없이 지속적으로 근 무하는 환경에서는 사용자 또는 부서별 정책을 구현 할 수 있으나 금융회사는 정기/수시로 인사이동이 있으므로 사용자 또는 부서별 정책을 구현하는 데에는 한계가 존재한다. 그러므로 문서에 대한 접근 정책 보다는 DRM 해제 시 통제 정책을 강화하는 것이 대중서비를 하는 포털이나 금융쪽에 적합하다.

DRM 해제 정책을 강화화기 위해서는 기업 내 업무시스템이 DRM을 인식할 수 있도록 시스템이 변경되어야 한다. 예를 들어 DRM 파일을 업무시스템 내 업로드 시 자동 복호화 처리를 하지 않을 경우 사용자의 불필요한 해제 신청이 많아 실제 통제 하기위해 정책과 상이한 결과가 나올 수 있다.

2.4 다중 솔루션 통합

보안솔루션 간의 기능 통합을 이용하여 개인정보 유출차단을 위한 보안정책을 수립할 수 있다. 개인정보 검색시스템과 DRM을 연동하여 검색 결과를 자동 암호화하는 효과를 발생할 수 있다. 그리고 개인정보 검색시스템과 DLP솔루션을 연동하여 USB에 파일를 저장 시 개인정보 포함 여부를 검사하는 추가 보안정책을 적용할 수 있으며, 인쇄 시 개인정보가 포함된 파일만 통제할 수 있게 되어 출력물 통제 정책을 펼치는데 사용자의 이해 가능성이 높아질 수 있다. 솔루션 기능 통합 할때는 몇가지 유의사항이 있다. 개인정보 검색시스템과 DRM 연동 시 압축된 파일에 대한 관리적 대안이 필요하며 검색시스템은 압축된 파일(Zip 등)내 개인정보 포함여부를 검색하기 위해 압축된 파일과 동일한 파일을 추가로 생성하여 압축 해제 후 검색결과 정보를 수집한 후 압축해제된파일을 삭제한다. 압축된 파일내 개인정보 파일 정보를 DRM에 이관 하더라도 DRM은 압축된 파일 내 개인정보 파일을 자동 암호화 할 수 있는 기술적 방안이 존재 하지 않는다. 또한 결제가 필요한 시스템에서도 이슈가 있다. DRM, DLP 솔루

션들은 정보 유출 통제를 위한 솔루션으로 통제적용을 위한 절차가 필요하고, 암호 화문서 해제, USB 사용 권한 부여, 출력물 승인 등 통제 해제를 위한 절차도 있어야 한다. 이런 여러 가 지 해제 절차를 하나의 승인시스템으로 일원화하면 사용자 편의성도 향상될 뿐만 아니라 보안담당자의 모니터링 부담도 줄일 수 있어, 보안의 효율성도 향상된다.

III.결론

민간의 서비스를 하는 회사에서는 정보보안의 기준을 준수 및 개인정보 유출 방지를 위해 지속적으로 보안솔루션을 설치,운영하고 있으나, 개인정보 유출 사고는 끊임없이 발생하고 있다. 본 논문에서는 상용 PC보안솔루션 중 필수 설치 보안솔루션을 소개하고, PC보안 솔루션의 각 기능들을 개인정보 보호 관점에서 통합한 하나의 관리 툴로써 운영하는 방안을 두었다 본논문에 내용을 보면 알겠지만 높은 보안이라함은 업무의 효율이 낮아 진다는 것을 알수 있다 이문제는 정보의 중요성에 따라 등급과 승인 라인은 설정하여 업무의 효율을 높여 주는 부분도 관과해서는 안될 부분이다. 마지막으로 다중 솔루션을 활용해 필요 기능을 축족했다고 하지만 시스템간의 연동이 쉽지 않아 통합하는 필요기능을 뽑아 쓸 수 있는 기능의 플랫폼이 필요 할 것으로 사료 된다. 개인정보의 이슈는 점점 커지고 있어 보안 분야에서 지속적으로 발전에 효율과 보안이 균형을 찾을 것으로 예상 한다.

[참고문헌]

[1] 정보보호학회논문지 솔루션보안정책

[2] 정보보호학회논문지 기업용 보안프레임

[3] 솔루션기업의 역량모델링 사례