엔드포인트 개인정보보호를 위한 복합적 상황인지 방식

용승림O, 김상오*
O인하공업전문대학 컴퓨터시스템과
*(주)인정보
e-mail: slyong@inhatc.ac.krO, sokim@ijbinfo.com*

A Collaborative Approach to Situational Awareness for Endpoint Personal Data Protection

SeungLim YongO, Sangoh Kim*
ODept. of Computer Systems & Engineering, Inha Technical College
*IJB Inc.

● 요 약 ●

EU의 GDPR(General Data Protection Regulation) 발효로 인해 유럽국가의 개인 정보 데이터를 활용하는 다국적 기업들이 규정에 맞는 데이터 보호정책을 수립하고 보안 투자를 강화하고 있다. 그러나 대다수의 기업들은 해커 등에 의한 사이버 보안을 위해서는 천문학적인 투자를 하고 있지만 기업 내 많은 직원들에 의한 실수나 고의에 의한 개인 정보 유출 방지에 대해서는 대처를 하고 있지 않다. 본 논문에서는 디지털 포렌식 기반의 앤드 포인트 실시간 모니터링 및 인간 행위 분석을 통한 앤드 포인트 개인 정보 보호 기능을 제공하여 기존의 사이버 보안에 국한된 통합 보안 관제의 효율성을 높이는 방안을 제안한다.

키워드: 개인정보보호(Personal Data Protection), 엔트 포인트 보안(End-point Security), GDPR(General Data Protection Regulation)

I. Introduction

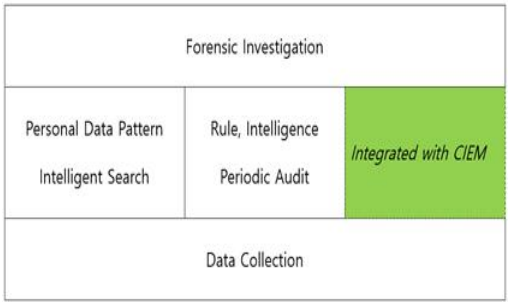
개인 정보 유출시, 최대 전체 매출액의 4% 또는 2천만 유로의 천문학적인 벌금이 부과될 수 있는 유럽의 GDPR이 2018년 5월15일 발효됨에 따라 전 세계 많은 기업들이 개인정보보호 및 사이버 보안에 대해서 많은 고민 및 투자를 하고 있다[1]. 우리나라의 경우에도 개인정보 유출사건이 지속되고 있으며 보안 선진국인 미국조차도 대규모 개인정보 유출등 문제가 발생되고 있다[2,3]. 국내외적으로 강화된 개인정보보호 필요성은 기존 제품에 좀 더 진화되고 넓은 범위의 감시를 요구하게 되었으며, 다음이 고려할 중요한 문제점들이다. 첫 번째, 데이터 유출에 대해서 바로 파악을 하지 못하는 것이다. 두 번째, 기존 시스템들은 주로 데이터베이스나 서버에 저장된 정형적인 데이터에 대해서만 집중하고 있고 PC에서 작성된 비정형 데이터에 대해서는 고려가 되지 않고 있다. 세 번째로는 내부 직원 등에 의한 악의적인 행위나 보안정책 등을 따르지 않는 실수 등에 의한 데이터 유출에는 속수무책인 경우이다.

본 논문에서는 비정형적이거나 문서안의 데이터 분석을 위해서 실시간 포렌식 데이터 기법을 도입한다. 사람들의 업무 행위를 실시간 분석함은 물론이고 표준화된 로그 생성으로 통합보안관제(SIEM, Security Information and Event Management) 시스템과 연동되는, 복합적인 상황 인지를 가능하게 하는 엔드 포인트 개인정보보호(EPDP, Endpoint Personal Data Protection)시스템을 제안한다.

II. Design of EPDP System

통합보안관제 시스템은 조직 내 여러 단위 보안시스템의 실시간 로그와 연동해서, 침입차단(IDS), 침입 방지(IPS), 바이러스 차단, 취약점 진단 등을 실시간적으로 지원하나[4], 사람이 포함된 엔드 포인트 단의 고려가 없어서 그 한계가 있다. 본 장에서는 엔드 포인트단을 고려한 복잡적인 상황 인지를 가능하게 하는 EPDP 시스템을 설계한다.

Fig.1은 EPDP 기능 블록이다. Fig.1의 각 기능들을 바탕으로 EPDP는 Fig.2와 같은 단계로 업무가 처리된다.



	Description
Data Collection	Endpoint 단의 데이터 유출을 실시간 감시하기 위해서 포렌식 기반으로 데이터를 수집
Personal Data Pattern Intelligent Search	나라별 개인 정보 데이터 패턴 라이브러리 및 서치 연동
Rule Periodic Audit	주기적으로 사내 컴퓨터내의 개인정보데이터에 대한 감사 수집된 데이터에 다양한 룰로 실시간으로 부정 사실 감지
Integration with SIEM	실시간 표준화된 로그를 생성하여 SIEM 등 다른 시스템과 쉽게 연동
Forensic Investigation	원격 포렌식 기능을 기본 탑재하여 이상 발생시, 상세 조사 및 법적인 증거 확보

Fig. 1. The function block of EDPD

EPDP는 Fig.2의 3단계에서 기존 통합보안관제 시스템 등과 연동되는데 기존 전통적인 센서 데이터들과 합쳐져서 정확하고 완벽한 데이터 유출 상황인지를 가능케 한다. Fig.3은 EPDP가 포함된 복합 상황 인지 방식의 개념도이다. 법적 증거물 수집 등이 가능한 원격 디지털 포렌식 기능을 추가하여 국내외 정부기관에서 요구하는 준법감시(Compliance) 업무는 물론 사고 후에는 여러 수사기관과의 효율적인 업무 협조가 가능하도록 되어 있다.

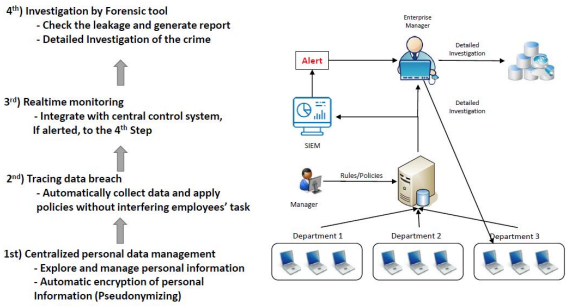


Fig. 2. The process of EPDP

기존에 할 수 없는 개인정보가 있는 문서 및 비정형 데이터 등의 유출에 대해서 실시간적으로 상황인지를 할 수 있게 되었고 현재 EPDP의 핵심 모듈을 협력사와 같이 MyNumber라는 제도가 도입된 일본에 공급하여 보험회사 등에서 엔드 포인트 단의 문서 및 비정형 데이터의 유출에 대해서도 감시하고 있다. 또한 해외 원전을 관리하는 회사에서는 개인정보는 아니지만 원전 내에서 근무하는 협력업체 직원들의 중요 데이터 유출 방지로 테스트되어 좋은 결과를 얻었다.

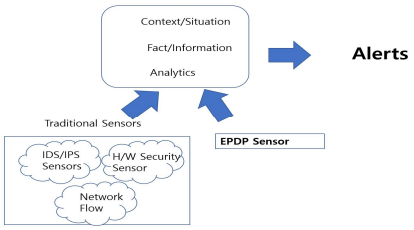


Fig. 3. Collaborative approach to Situational Awareness at SIEM

III. Conclusions

본 논문에서는 기존 사이버 보안에서 사용되는 전통적인 센서 정보를 바탕으로 한 정보유출 상황인지에 새로운 센서 정보를 추가하여 복합적인 상황인지를 가능케 하는 시스템을 제안하였다. EPDP는 인간과 인간이 사용하는 PC 간의 활동 상황을 실시간 고려하는 것은 물론이고 엔드 포인트 단의 비정형화된 데이터 또한 고려하여 다양한 개인정보 유출에 대한 방지가 가능하다. 향후, 인간 행위에 의한 유출에 대해서는 복잡한 업무내의 영역과 악의적인 영역을 자동으로 감지할 수 있도록 인공지능 기법의 응용 등에 대한 연구가 필요하다. 또한 개인 사생활 침해가 없도록 수집된 데이터는 다른 어떤 접근도 되지 않고 자동으로 심사되고 폐기될 수 있는 연구[5] 등이 필요할 것으로 사료된다.

REFERENCES

[1] Information Law Group. InfoLawGroup LLP, "GDPR: Getting Ready for the New EU General Data Protection Regulation", 2016.

[2] Korea E-Trade Researcher, "Analysis and Implications of Personal Information extrusion in Electronic Transactions", JungAng University, 2014.

[3] Solon, Olivia, "Facebook says Cambridge Analytica may have gained 37m more users' data", The Guardian, 2018.

[4] Swift, David, "Successful SIEM and Log Management Strategies for Audit and Compliance", SANS Institute. 2010,

[5] Kitchin, Rob, "The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences.",SAGE. 2014,