기업 비즈니스 환경에서 효율적인 정보보호 프레임워크 구현을 위한 정보 처리 구조에 관한 연구

김민준*, 이경현**
*부경대학교 정보보호학협동과정
minjun@pukyong.ac.kr
**부경대학교 IT융합응용공학과
khrhee@pknu.ac.kr

A Study on Information Processing Framework for Implementing Efficient Information Security Architecture in Enterprise Business Environment

Min-Jun Kim*, Kyung-Hyune Rhee**,
*Interdisciplinary Program of Information Security, Graduate School,
Pukyong National University
**Department of IT Convergence and Application Engineering,
Pukyong National University

요 약

과거부터 기업의 정보보호 위험 관리에 대한 중요성은 계속해서 강조되었고 많은 투자도 이루어졌지만 RRO(투자 대비 위험 감소)에 대한 효과가 미흡한 주된 이유는 기술적, 물리적, 관리적 정보보호가 융합되지 못하는 것이다. 정보보호 프레임워크는 개별 정보보호 활동에 대한 공유로서 세 가지 정보보호 요소를 융합할 수 있는 환경을 제공하고 기업 환경에서 발생하는 위험 요소를 시각적으로 표현함으로써 체계적인 정보보호 위험 관리 활동을 장려한다. 본 논문에서는 이러한 환경을 구현하기 위한 필수 요소인 프레임워크 내 데이터 구조에 관한 연구를 통해 효율적인 정보보호 프레임워크를 구성하려는 기업들에 방향성을 제시한다.

1. 서론

기업의 자산이 점차 정보화됨에 따라 시스템의 정지나 오작동뿐 아니라 저장된 정보의 손실, 변형에도 기업의 경영 활동은 치명적인 영향을 받는다. 기업의 정보보호 조직은 정보의 손실 및 변형에 따른 위험에 대응하고자 표준화된 관리체계에 따른 정보보호 위험을 정의하고 감사를 통해 적정성을 검토하여 위험 요소를 사전에 탐지·대응하는 예방 활동을 수행해야 한다[1, 2].

이러한 체계적인 정보보호 위험 관리 활동을 위한 많은 연구가 있다[2-7]. 특히 NIST의 정보보안 프레임워크는 기업 보안 인프라 구성에 효과적인 가이드라인을 제시한다고 평가받는데 정보자산들로부터 발생되는 보안 이벤트의 실시간 분석 환경을 제공할 목적으로 개발되는 SIEM (보안 및 정보 이벤트 관리) 솔루션은 이러한 프레임워크를 적절히 반영하여 설계된다[7]

하지만 SIEM을 운영하더라도 비즈니스 환경 변화에 대응되는 전산화 부족으로 인한 수기관리, 각종 예외처리, 담당자 전문지식 및 임직원 보안의식 부족과 같은 복합적 요인으로 기술적, 물리적, 관리적 정보보호 활동이 상호작용하지 못하는 경우가 많아 조직을 위협하는 잠재적인 위험에 관한 식별이 어려워지면서 결국 정보보호 위험 안정적 경영 활동에 미치는 악영향을 줄 가능성이 증가한다[4]. 따라서 SIEM과 같은 프레임워크 내의 정보를 비즈니스적으로 표현·관리·분석하는 활동이 수반되어야 한다[8].

이 관점에서 체계적인 위험 관리 환경을 구축하기 위해 본 논문에서는 SIEM 프레임워크 내 비즈니스 정보를 구성하고 처리하는 접근방법에 관하여 연구한다. 본 논문의 구성은 다음과 같다. 2장에서는 비즈니스 정보를 SIEM 시스템에 반영하기 위한 정보 처리 구조에 관한 연구 내용을 다루고 3장에서 이러한 구조가 갖는 의미를 살펴본 후 4장에서 향후 연구 과제를 열거한다.

2. 제안 시스템

제안 시스템은 비즈니스 관점에서 핵심 정보를 수집·생성·관리하는 지식 시스템을 정의하고 내부 지식의 표현 방법과 처리절차에 관한 방법론을 다룬다.

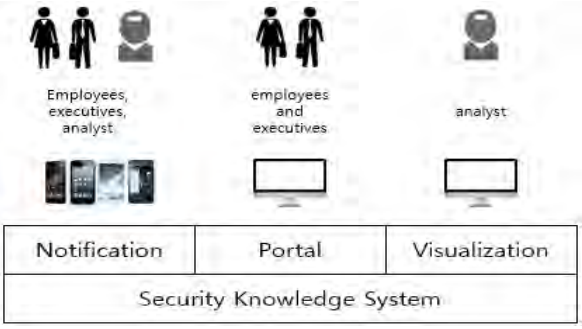
2.1 위험 관리를 위한 프레임워크

정보보호 위험 관리 프레임워크는 기업의 위험을 기술하고 평가할 수 있는 환경 제공을 위해 논문에서 제안하는 지식 시스템을 중심으로 아래 세 가지 시스템과 함께 구성된다.

1) 알람 시스템 : 위험이라고 판단되는 사건의 탐지 등 즉각적인 정보 전달이 필요한 상황을 담당자에게 정보 전달 매체로서 전달하는 시스템

2) 시각화 시스템 : 지식 시스템에서 생산하는 데이터를 요약하고 시각적인 데이터 분석환경을 제공하는 시스템

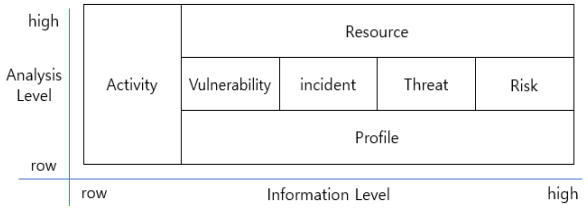
3) 포탈 시스템 : 비즈니스 관련 위험을 임직원에게 제시하여 기업 내 존재하는 위험 요소에 대해 인지 및 대응이 가능하도록 인터페이스를 제공하는 시스템



(그림 1) 프레임워크 구성 시스템

2.2 지식 시스템

정보보호 지식 시스템은 행동(Active), 자원(Resource), 취약성(Vulnerability), 사건(Incident), 위협(Threat), 위험(Risk), 프로파일(Profile) 모듈로 구성된다. 핵심 정보는 정보보호 지식 시스템에서 위험 관리 모듈을 중심으로 이 활동에 가치를 부여하는 다양한 모듈들이 상호작용하는 형태로 처리되며 다른 시스템들은 지식 시스템의 정보를 이용하여 목적에 따라 업무 처리한다.



(그림 2) 정보보호 지식 시스템 구성요소

<그림 2>는 지식 시스템을 이루는 각 모듈을 나타내는데 인접한 모듈은 서로가 다루는 정보에 대한 의존도가 높은 강한 상호작용 관계가 있고 가로축은 정보의 수준(데이터 가공 정도의 고저)을 세로축은 분석 수준(분석에 필요한 기술 수준의 고저)에 따라 모듈을 배치한다. 정보의 수준과 분석 수준이 낮을수록 기술의 깊이가 요구되는 전문가 영역, 반대의 경우는 관리 영역에 가깝다.

프레임워크의 핵심인 지식 시스템은 다섯 가지 관리 모듈로 이루어지고 각 모듈은 하나 이상의 정보 집합 산출물을 만들어낸다.

a. 활동 관리(Activity Management) : 정보자산으로부터 도출되는 활동 정보에 대한 수집, 가공, 처리를 수행하는 모듈

b. 자원 관리(Resource Management) : 보유한 자원(인적, 물리적, 논리적 자원)들을 취합하여 각 모듈에서 참고하기 용이한 형태로 유지, 관리하는 모듈

c. 취약성 관리(Vulnerability Management) : 자동화 스캐너, 퍼징 테스트 등으로 발견될 수 있는 취약점에 대한 확인, 조치 그리고 완화될 수 있도록 관리하는 모듈

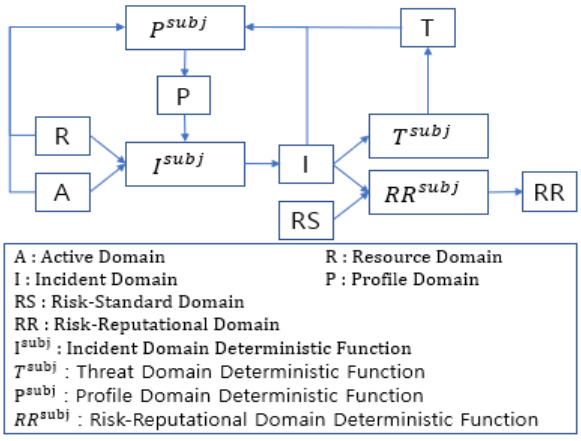
d. 사건 관리(Incident Management) : 활동과 자원 데이터를 조합하여 사전 정의된 위험을 판단할 수 있는 사건 데이터를 추출하는 모듈

e. 위협 관리(Threat Management) : 내·외부 사건 데이터를 조합하여 위협 데이터를 추출하는 모듈.

f. 위험 관리(Risk Management) : 위험을 사전 정의하고 각종 관리 모듈에서 제공하는 데이터로부터 위험 상황을 인지, 평가하여 위험을 관리해주는 모듈

g. 프로파일 관리(Profile Management) : 활동, 자원, 사건, 위협, 위험 데이터로부터 변화, 유사도, 주기성 등 특성을 추출하는 모듈

2.3 주요 정보 집합과 처리 흐름



(그림 3) 정보보호 지식 시스템 정보 처리 흐름

<그림 3>에서는 시스템에서 처리되는 지식의 도메인들과 처리 흐름을 보이는데 도메인들은 외부로부터의 입력을 통해 각자 영역에 기본적인 정보의 집합을 만들고 사건, 위협, 위험평가, 프로파일 도메인은 다른 도메인 간 상호작용을 통해 추가적인 정보를 생성하는 함수를 갖는다.

도메인 D에서 취급하는 주제($subj^D$)와 그 주제에 속하는 원 소 (d^{subj^D}) 가 $subj^D = \{subj^{D_1}, subj^{D_2}, ..., subj^{D_n}\}$ $d^{subj^D} = \{d_1^{subj^D}, d_2^{subj^D}, ..., d_n^{subj^D}\}$일 때, 결정적 함수는

$I^{subj^I}(a_i^{subj^A}, r_j^{subj^R}, p_k^{subj^P}) \rightarrow i_n^{subj^I} \in I$

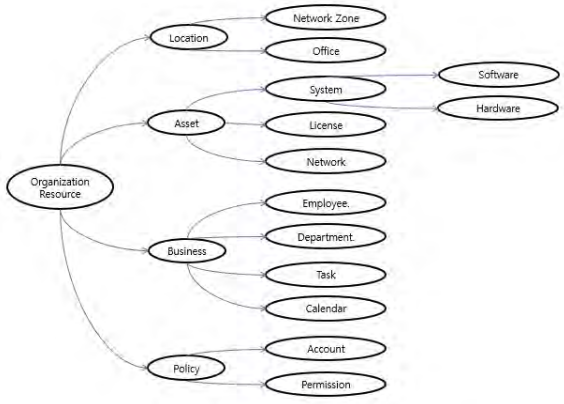
$T^{subj^T}(i_k^{subj^I}) \rightarrow t_n^{subj^T} \in T$

$RR^{subj^{RS}}(i_n^{subj^I}, rs_{n_R}^{subj^{RS}}) \rightarrow rr_n^{subj^{RS}} \in RR$

$P^{subj^P}(a_i^{subj^A}, r_j^{subj^R}, i_k^{subj^I}, t_l^{subj^T}) \rightarrow P_n^{subj^P} \in P$

2.4 상황인지와 자원 데이터 구조

앞서 정의한 다양한 형태의 도메인과 이들의 관계를 맺는 함수들을 이용하면 현재 상황에 대한 위험을 식별하고 미래 위험을 예측하기 위한 상황인지가 가능하게 된다. 여기서 자원 도메인은 상황을 만들어가는 주체와 대상으로서 속성과 허용된 권한 범위 내의 가능한 행위를 갖는다. 따라서, 자원과 행위 정보를 결합하면 정보자산으로부터 인지되는 상황에 대한 정보보호 위험도와 대응 우선순위를 결정 가능하여 문제에 대한 사전 인지 및 대응을 할 수 있다.



(그림 4) 자원 정보의 구성

<그림 4>는 기업의 자원 정보를 나타내는 한 가지 예이다. 이 정보 집합으로 이벤트에 대해 육하원칙에 따른 해석을 가능케 하여 이것을 활용한 각종 데이터 처리를 보다 고차원적이며 다양하고 신뢰성 있는 가치를 부여한다. 만일 이 데이터 집합이 존재하지 않거나 정보가 부족 혹은 부정확하다면 이후 시점의 정보 처리는 무의미하게 된다.

3. 지식 시스템 의의

잘 갖춰진 지식 시스템은 체계적인 정보보호 위험 관리 측면에서 아래와 같은 이점이 있다.

3.1 비즈니스 측면의 정보보호 활동 가시화

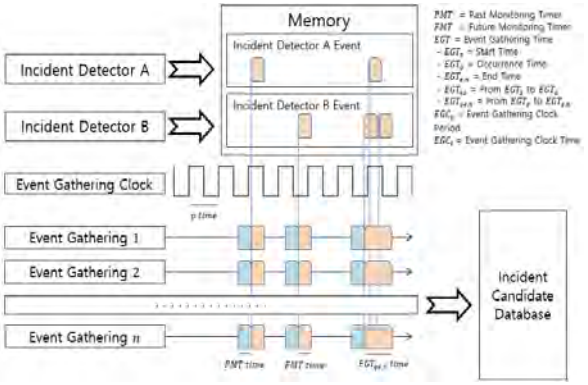
비즈니스 문화에 종속된 정보자산과 정보에 대한 보호는 그것을 다루는 구성원 간의 신뢰 없이는 이루어질 수 없다. 따라서, 비즈니스 측면에서의 정보보호 활동을 가시화하여 의미 있는 정보보호 활동이 이루어짐을 구성원들에게 표현하여 정보보호 활동에 참여할 것을 유도해야 한다. 프레임워크는 기업의 위험표준, 위험평가 정보와 상호작용할 수 있는 정보 구조의 표현으로 비즈니스 측면의 정보보호 활동을 가시화할 수 있다.

3.2 침해사고 대응 절차 자동화 & 고도화

정보보호 조직은 침해사고 발생을 인지하고 대응해야 하므로 국가기관에서는 기업의 침해사고 대응력을 높이기 위한 가이드를 제공한다. 침해사고 대응 절차 중 사고탐지와 조사 단계는 본 논문에서 제안하는 프레임워크 상에서 자동화 및 고도화될 수 있다.

사고탐지는 비즈니스적 위험(Risk)과 관련된 사건(Incident) 정보를 얼마나 정확하게 추출하는가를 고려해야 한다. 논문의 정보보호 지식 시스템에서 정보 간 피드백이 활성화되고 프로파일 체계의 완성도가 높아질수록 탐지 정확도는 증가할 것이다.

사고조사 시에는 사건 발생 주체에 대한 각종 정보(자원, 위협, 프로파일)를 융합한 타임라인 분석환경을 제공한다. <그림 5>는 분석환경 제공을 위해 사고탐지 시점 전후의 이벤트를 하나의 프로파일 공간 안에 담는 정보수집 방법론의 예를 보여준다. 이러한 사고탐지와 사고조사 영역의 자동화와 고도화는 침해사고 인지 및 대응 시간을 단축하고 분석 정확도를 높여 침해사고 대응 능력을 전체적으로 높여준다.



(그림 5) 사고조사 정보수집 방법론

3.3 알려지지 않은 공격에 대한 대응

지능형 지속 위협(APT)은 침투 형태가 매우 다양하고 정상적인 행위로 위장하여 공격이 성공할 때까지 지속적 침투를 시도하므로 기존 정보보호 시스템으로는 방어하는데 제약사항이 많다. APT 공격을 방어하기 위해서는 정상행위를 학습한 후 비정상행위를 찾아야 한다. 프레임워

크에서는 정상행위를 주체가 허용된 권한 내에서 비즈니스 로직을 따라 평소의 패턴대로 행동하는 것으로 보고 반대인 비정상행위를 찾아낸다. 이렇게 도출된 비정상행위는 APT공격의 한 형태가 아닐지라도 내적 또는 외적 요인에 의한 변화이므로 모두 관찰 및 소명 대상으로 간주한다. 이는 APT 공격 대응에 관한 본질적인 접근이자 효과적인 방어법일 수 있다.

4. 향후 연구 과제

이러한 여러 가지 이점을 구체화하기 위해서는 다음과 같은 관점에서 추가적인 연구가 필요하다.

4.1 정보 구조의 구체화

다양한 종류의 비즈니스 형태를 수용할 수 있는 정보 구조에 관한 연구가 필요하다. 모든 기업에서 최적화되는 정보 구조로 일반화하는 것은 현실적으로 어렵겠지만 적어도 이러한 정보 구조에 관한 연구는 프레임워크를 실체화하려는 기업에 가이드가 될 것이고 수많은 형태의 정보를 생산하고 소비하는 빅데이터 환경에서 정보와의 결합을 더 가볍고 효과적으로 수행할 수 있도록 한다.

4.2 프로파일 정보에 관한 연구

정보에 대한 특성을 추출하는 프로파일은 비즈니스적 안목과 수학적 방법을 등을 이용한 데이터 과학적 기법을 통해 얻는다. 프로파일을 수행하는 방법에 대한 힌트는 빅데이터, 머신러닝을 활용한 정보보호 이상징후 탐지에 관한 연구들에서 힌트를 얻을 수 있다[9-11]. 정보보호 조직은 이러한 연구결과를 활용하여 기업에 맞는 프로파일 전략을 세워나가야 한다.

4.3 위협정보 활용에 관한 연구

기업 내에서 발생한 위협정보는 이미 발생한 사건으로부터 도출되어 가치가 높으며 외부 사건으로부터 생성된 위협정보와 결합할 경우 위험을 감소시키기 위한 선제대응이 가능하다. 이러한 위협정보를 체계적으로 관리할 수 있고[12] 전문적인 보안기업이나 국가기관을 중심으로 위협정보를 공유하는 것은 공유 당사자 간 신뢰와 공유 범위에 관한 문제 등이 존재하지만 전략적, 전술적 위협정보도 얻을 수 있는 이점이 있어 추가적인 연구가 필요하다[13].

5. 결 론

의미있는 정보보호 활동을 위해서는 소속된 기업 비즈니스 관점의 영향도를 구성원에게 제공하여 신뢰를 얻는 과정이 필요하다. 프레임워크의 시스템 구성과 정보 처리 방법론은 그 과정에 도움을 줄 것이다. 제시한 향후 연구 과제와 같은 연구를 통해 정보보호 프레임워크를 구성하는 정보보호 기업에 도움이 되고자 한다.

참고문헌

[1] 장상수, 노봉남, 이상준, "정보보호 관리체계 운용이 정보보호 성과에 미치는 영향" 정보과학회논문지 정보통신 제40권 제1호, 2013

[2] 백남균, 정성민, 김태경, "확률적 분석에 기반한 위험평가 기법에 대한 연구" 보안공학연구논문지 제 10권 제 2호, 2013

[3] Youakim Badr and Jean Stephan, "Security And Risk Management in Supply Chains" JIAS 2 288-296, 2007

[4] 원종혁, 임욱빈, 박유진, "융합 보안관제시스템 구축 활성화 방안 연구" Journal of the IT&A Vol 12 No 4 Pages 535-552, 2015

[5] Ljiljana Ruzic-Dimitrijevic, "Risk assessment of knowledge management system" A Publication of the IIAKM, Volume 3, Issue 2, 2014

[6] 이수연, 유지연, 임종인, "주요기반시설 서비스의 안정적 운영을 위한 보안 프레임워크 설계에 관한 연구" JITS, 2016

[7] 차병래, 최명수, 강은주, 박선, 김종원, "Cybersecurity를 위한 SOC & SIEM 기술의 동향" 스마트미디어저널 Vol 6 No 4, 2017

[8] Reena Singh, Kunver Arif Ali, "Challenges and Security Issues in Big Data Analysis" IJIRSET Vol. 5, Issue 1, 2016

[9] 신익수, 송중석, 최장원, 권태웅, "기계학습 기반 IDS 보안이벤트 분류 모델의 정확도 및 신속도 향상을 위한 실용적 feature 추출 연구", 정보보호학회논문지, 제28권, 제2호, pp.385-395, 2018

[10] 하동욱, 강기태, 류연승, "기계학습 기반 내부자위협 탐지기술: RNN Autoencoder를 이용한 비정상행위 탐지", 정보보호학회논문지 제27권 제4호 pp.763-773, 2017

[11] 박진학, 권태웅, 이윤수, 최상수, 송중석, "다크넷 트래픽의 목적지 포트를 활용한 블랙IP 탐지에 관한 연구", 정보보호학회논문지 제27권 제4호 pp.821-831, 2017

[12] NakHyun Kim, Byung-ik Kim, Seulgi Lee, Hyeisun Cho, Jun-hyung Park, "Design of a cyber threat intelligence framework" IJIRTS Volume 5, 2017

[13] Thomas D. Wagner, Esther Palomar, Khaled Mahbub, and Ali E. Abdallah, "Research Article : A Novel Trust Taxonomy for Shared Cyber Threat Intelligence" Hindawi Security and Communication Networks Article ID 9634507, 11 pages, 2018