Journal of The Institute of Electronics and Information Engineers Vol.53, NO.6, June 2016 http://dx.doi.org/10.5573/ieie.2016.53.6.069
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-6-8

보안사고 예보시스템

(Forecast System for Security Incidents)

이 동 근*, 임 종 인*

(Dongkun Lee and Jong In Lim©)

요 약

기업은 대부분의 경우 보안사고가 발생하면 내부 대응절차에 따라 신속한 사고처리에 집중하고 사고원인, 문제점 및 조치결과를 최고 경영진에게 보고하면서 사고를 마무리한다. 또한 외부에서 발생한 보안사고는 그때마다 관심을 가지고 적극적으로 내부와 연결하여 문제점을 발굴하고 조치를 하는 경우와 외부의 문제로 치부하며 잠시 관심정도만 가지고 넘기는 경우도 있을 것이다. 기업은 보안사고 발생 시점에 관심과 역량을 집중하여 대응하는 것 뿐만 아니라 보안사고가 발생하지 않도록 지속적인 사고예방 활동을 하는 것이 중요하며 이를 위해 체계적이며 일관성 있고 시스템적인 방법이 제공되어야 한다. 이와 같은 목적에서 본 논문에서는 보안사고 예보시스템을 제안한다. 보안사고 예보시스템은 기업의 내부에서 일어난 직접 보안사고 뿐만 아니라, 외부에서 발생한 간접 보안사고로부터 향후 보안사고 예측에 도움이 되는 사고발생 유발인자들을 모아서 데이터베이스화하고 기업에서 가지고 있는 축적된 사고 경험과 대응 프로세스들을 시스템화하여 상호작용을 하도록 만드는 것이다. 보안사고 예보시스템은 잠재적으로 발생할 수 있는 사고의 예방조치활동에 효과적인 대안이 될 수 있을 것이다.

Abstract

If the security incidents are occurred then, the company concentrates on the quick reaction to security incidents, reports the reason of incidents, it's problem, the result of measure to the top management team. There will be the case that actively finding problems and taking it's actions with linking the internal problems whenever external security incidents are occurred or that having only interest of problems at the moment. It is important that lasting the preventing action to prevent security incidents than not concentrating on only the security incidents are occurred. To do this, the systematical and consistent method for this should be provided. In this paper, we will provide a security incident forecast system. The security incident forecast system updates the incident induction factor which helping to forecast the potential security incidents on the database inferred from the direct security incidents which are occurred inside the company as well as the indirect security incidents which are occurred outside the company and makes interact with the incident experience and the measure process systematically. The security incident forecast system is the efficient measure about the potential security incidents in taking precaution.

Keywords : 보안사고, 보안관리. (Security Incident, Security Management)

Ⅰ. 서 론

핵티비즘[1]은 사회적 이슈나 정치적 목적을 달성하기 위한 수단으로 정부·기관·공공단체 등의 웹 사이트를 해킹하여 서버를 무력화시키는 형태의 보안사고이다. 최근에는 이러한 목적으로 기업을 대상으로 공격하는 사례가 점점 증가하고 있다.

이러한 해킹 사고들이 기업의 기밀정보나 개인정보를 포함한 고객정보의 노출로 이어지면 그 피해의 규모는 상당할 것이고 기업의 존폐를 위협할 수도 있다. 예를 들면, 2005년 금융기관의 인터넷 뱅킹을 최초로 해킹하여 명의를 도용했던 사례[4], 2007년 조선산업 기술을 중국으로 유출하려던 사례[5], 2010년 3월 1일 한일 사이버 전쟁을 통한 개인정보 3천만건 유출사고 사례[6]를 통해 알 수 있다. 특히, 그 대상이 기업의 기밀 정보 및 고객정보를 포함하는 개인정보라는 점에 주목해야 한다.

따라서, 기업은 이러한 개인정보를 포함한 기밀정보의 유출 및 그 피해를 방지하기 위해서 기업이 운영하

* 정회원, 고려대학교 (Korea University)
© Corresponding Author (E-mail : jilim@korea.ac.kr)
Received ; March 30, 2016 Revised ; April 6, 2016
Accepted ; May 2, 2016

고 있는 보안사고 대응 프로세스를 시스템적으로 결합하여 체계적으로 관리할 필요가 있다. 더 나아가서 기업 보안사고를 미연에 방지할 수 있게 미리 예측하는 시스템이 있다면 이상적인 보안관리 방법이 될 것이다.

1. 보안사고의 유형 및 대응방법

일반적으로 기업 보안사고의 유형은 제품의 취약점 때문에 발생하는 제품 보안사고, 기업이 운영하는 고객서비스 또는 사내 인프라가 해킹되는 침해사고, 기밀문서나 고객정보가 유출되는 정보유출사고 등으로 분류할 수 있다.

보안사고 발생 시 기업은 보안부서와 유관부서가 사고의 유형과 원인을 분석하고 위험수준을 판별하여 적합한 대책을 수립하고 적용한다. 이때 정보보호 정책과 법률 자문을 받을 수도 있으며 각 관련부서는 진행사항 보고, 조치사항 적용 등 보안사고 대응 프로세스를 따르게 된다.

2. 보안사고 대응 시 기본원칙

보안사고는 동일한 원인으로 인하여 반복되어서는 안 된다. 문제가 발생하여 대책을 수립하고 적용하였음에도 같은 원인으로 사고가 발생하게 되면 보안부서의 신뢰도가 하락할 뿐만 아니라 기업 차원에서는 이미지가 실추되고 경제적 손실의 위험성이 높아질 수 있다. 따라서, 정확한 원인을 분석하여 대책을 세우고 한번 발생한 사고에 대해서는 지속적인 관리하여 사고가 재발되지 않도록 해야 한다.

외부에서 발생한 보안사고 또는 언론이나 학술 컨퍼런스에서 이슈화 된 문제는 기업의 제품이나 서비스에 잠재적으로 영향을 줄 가능성이 있다. 이런 기업에 직접적인 보안사고로의 잠재성 갖는 유형의 보안 문제는 기업 내부에 취약한 부분은 없는지 분석하고 이에 대한 대책 수립과 예방조치를 시행하여 보안수준을 향상시켜야 한다.

3. 보안사고 대응 시스템의 요구사항

기업은 보안사고 발생 위험성이 있는 분야를 미리 탐지하고 예방하기 위해서 보안사고 대응 시스템을 운영하기도 한다. 보안사고 및 대책에 대한 관리가 단순히 이력관리 수준에 그친다면 지속적이고 체계적인 관리가 어렵게 된다. 따라서 기업은 보안사고 발생 시 충분하고 세밀하게 사고분석을 해야 하며, 사고로부터 의미있는 데이터를 추출하여 이를 데이터베이스화하고 지속적으로 진화시켜 보안사고 예방활동에 활용할 수 있도록 해야 한다. 또한, 기업 내에 발생하지 않았던 새로운 유형의 사고 또는 간접사고가 있을 수 있기 때문에 예보시스템은 유사성을 갖는 보안사고로부터 정보를 분석하여 어떤 피해를 주는 유형인지 혹은 어떤 제품 및 서비스에 영향을 주는지 등 의미있는 결과를 도출하고 이를 이용하여 예보 할 수 있어야 한다.

4. 논문의 공헌도

본 논문에서는 향후 발생할 가능성이 있는 보안사고를 예측하는데 활용되는 예측인자라는 개념을 정의하였고 이를 데이터베이스에 축적하여 직접·간접 보안사고 발생 시 예측인자를 기반으로 다양한 분석을 통해 조치해야 할 사항을 알려 주는 보안사고 예보시스템을 제안한다.

예측인자는 직접사고 또는 간접사고로부터 사고 내용을 분석하고 평가하는데 사용하는 의미 있는 정보를 말하며 지속적으로 데이터베이스에 축적된다. 기업 내부의 보안사고 뿐만 아니라 외부의 간접 보안사고로부터 축적한 예측인자 및 새롭게 센싱한 예측인자를 보안사고 예보시스템에 입력하였을 때, 기업에 내재된 잠재적인 보안사고 위험성을 사전에 리포트 받아 예방 조치할 수 있다. 또한 재발사고나 예상하지 못한 사고를 최소화하는데 효과적으로 활용할 수 있다.

예측인자 정보를 보안사고 예보시스템에 입력하였을 때 데이터베이스에 해당하는 예측인자가 없는 경우 보안사고 예보시스템은 예측인자를 추가로 축적시키고 보안사고 예보시스템 내 정보들과 새로운 연관관계를 형성한다. 또한, 보안사고 예보시스템과 기업의 보안사고 대응프로세스를 어떻게 시스템적으로 접목하는지 그 방안에 대해서도 제안한다.

Ⅱ. 관련 연구

기업은 보안사고 발생 시 “즉각적인 대응절차의 발효”는 보안사고 대응방법에 있어서 피해를 최소화하여 조기에 정상적인 경영활동이 이루어질 수 있는 최선의 노력요소 중 하나이다. 2011년 두 회사에서 발생했던 개인정보 노출사고 피해 사건에서 보았을 때, 한 회사 A는 3일 다른 회사 B는 16일 이후에 사건을 공개하였다. 동일한 개인정보 노출사고였음에도 불구하고 빠른 대응으로 대응한 A회사는 업계 1위를 유지한 반면, 사건을 지연 발표한 B회사는 소비자 소송 및 주가하락

등의 결과를 초래하였다.[2]

이러한 사례를 통해 알 수 있듯, 보안사고 피해에 대한 기업의 대응절차와 즉각적인 대응능력은 점점 더 중요시되고 있다. 또한, 보안사고가 발생했을 때 의미있는 유효시간이내에 신속하게 대응하는 능력은 정보보호 목적의 3요소인 기밀성, 무결성, 가용성 중 가용성에 속한다고 볼 수 있고, 이는 기업이 기본적으로 보유해야할 역량이기도 하다.

1. 보안사고 대응절차

일반적으로 보안사고를 대응하는 절차적 방법론은 미국 NIST와 한국정보보호진흥원(KISA)에서 권고하는 가이드에서 찾아볼 수 있다. “NIST SP 800-61 Computer Security Incident Handling Guide[8]”의 침해사고 대응절차는 [사전준비]→[탐지 및 분석]→[억제, 근절, 복구]→[사고 후 활동] 4단계로 구성되어 있다.

한국정보보호진흥원(KISA)에서 발간한「침해사고 분석절차 가이드」에는 [사고 전 준비과정]→[사고 탐지]→[초기 대응]→[대응전략 체계화]→[사고조사]→[보고서 작성]→[해결] 7단계로 이루어져 있다.

이러한 보안사고 대응절차는 [예방], [탐지], [분석/대응], 그리고 [복구] 단계로 요약할 수 있다.

가. 예방 단계

악성 침해요인을 사전에 지속적으로 제거·감소시킴으로써 침해사고 발생자체를 억제·방지하기 위한 일련의 활동을 수행하는 단계이다.

나. 탐지 단계

기업에서 보안사고 탐지는 내부에서 인지하는 경우와 내·외부로부터 관련된 정보를 제공받는 경우가 있다. 이메일, 대표 홈페이지, 전화, 또는 기타 보안신고 채널을 통해서 정보를 제공받으며 이는 일반적으로 보안부서로 통보된다. 기업과 직접적으로 관련없는 외부의 간접사고(Indirect Incident)는 모니터링 대상이 되어 참고하는 수준이지, 당장 기업에 피해를 주지 않기 때문에 내부적으로 관련이 있는지 자체 확인해 보는 정도에 그치며, 관련자들에게 통보가 체계적으로 이루어지 않는 것이 현실이다.

다. 분석 및 대응 단계

접수된 사고는 보안부서(Security Department)로 이관되어 예상되는 피해 규모와 손실액 등을 분석하여 사고의 위험도를 상, 중, 하로 판단한다. 이후, 내부규정과 절차에 따라 관련부서와 협의하여 대응이 이루어지고 보안 위협요소를 제거하고 취약점을 조치한다.

표 1. 보안사고 분류[7]
Table1. Security Incident Classification[7].

The type of cyber crimes	Victim		
	Personal	Company	Government
Online Fraud	○	○	
Deceptive S/W	○		
Identity Theft	○		
Intellectual property infringement		○	
Espionage		○	
Loss of customer information		○	
Online Theft	○	○	
Online extortion		○	
Financial fraud		○	○
Hinder access		○	○

라. 복구 단계

사고관련 내용을 최고 보안책임자에게 보고하고 이력을 관리한다. 또한 사고 사례를 관련부서에 전파하고 교육하여 유사한 사고가 재발하지 않도록 관리한다.

2. 보안사고 분류기준

기업에 피해를 주는 사이버 범죄의 형태로는 온라인 사기, 지적 재산권 침해, 스파이 행위, 고객정보 손실 및 온라인 절도/사기 및 정상적인 서비스 방해가 있다. 이중 기업의 경우 가장 두드러진 사이버 피해 사고는 개인정보 노출 및 기술정보 유출이다. 이와 함께, 기업을 대상으로 가장 흔하게 발생하는 해킹의 형태는 DDoS 공격을 들 수 있고 이러한 공격은 시스템 장애로 기업 활동이 저해될 수 있다.

특히 앞에서 언급했던 핵티비즘 사례를 보면 그 나라의 사회적 이슈나 정치적 목적을 위해 관련이 없는 기업을 표적으로 해킹하기도 한다. 이러한 해킹의 피해는 [Table 1]의 피해분류와는 다르게 기업의 이미지 실추와 같이 무형의 피해를 포함하는 복합적 피해양상을 보인다.

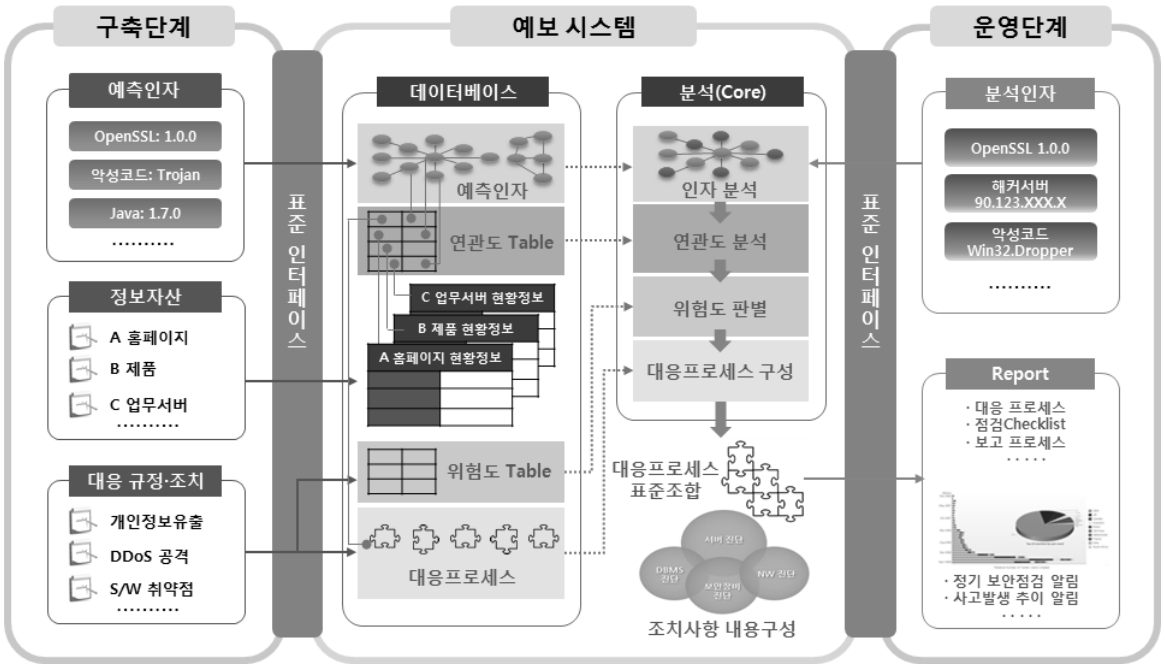

그림 1. 보안사고 예보시스템
Fig. 1. Forecast System for Security Incidents.

3. 정보보호 관리체제 및 인증제도

정보보호관리체계 인증제도는 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운영하는 종합적인 체계(정보보호 관리체계)의 적합성에 대해 인증을 부여하는 제도이다.[9, 12]

정보보호관리체계는 PDCA(Plan-Do-Check-Act) 프로세스를 통해서 보안위협요소를 일회적으로 대응하는 것이 아니라 지속적인 관리체계를 구축하고 강화하는 것을 목적으로 한다.[9, 12]

따라서, 기업은 정보자산에 대한 기밀성, 무결성, 가용성을 실현위한 절차와 그 과정을 체계적으로 수립하고 문서화하여 지속적으로 운영해야 한다.

개인정보보호 관리체제 인증제도는 기업이 개인정보보호를 위해서 필요한 보호조치 체계를 구축하고 이를 체계적이고 지속적으로 운영하는지를 인증해 주는 제도이다.[13]

이러한 정보보호관리체제와 개인정보보호 관리체제 인증제도를 통해서도 알 수 있듯이, 정보보호에 있어서 가장 중요한 요소는 보안사고가 발생하지 않도록 지속적으로 관리하고 예방 활동을 하는 것이 중요하다.

본 논문의 보안사고 예보시스템은 보안사고를 체계적이고 일관성 있게 시스템적으로 대응하는 것뿐만 아니라 과거 발생했던 사고들을 지속적으로 관리하고 이를 바탕으로 사고 예방을 하는 시스템 모델을 제시한다.

Ⅲ. 제안된 예보시스템

본론에서는 보안사고 예보시스템의 구성과 개념, 운영절차에 대해서 상세히 소개한다.

1. 보안사고 예보시스템의 구성

보안사고 예보시스템은 정보를 축적하는 데이터베이스, 보안사고 예측을 위한 분석코어, 사용자가 정보를 입력하거나 결과를 열람하기 위한 표준인터페이스로 구성된다.

보안사고 예보시스템을 구축하는 단계에는 예측인자, 정보자산 현황, 보안규정 및 대응 프로세스, 보안사고 위험도 분류 정보 등을 표준인터페이스를 통해 입력한다. 예측인자 중심으로 정보자산 현황과 위험도, 대응 프로세스 등과 상호 연관 관계를 형성하여 연관도 테이블을 구축한다.

이후, 직·간접 보안사고가 발생할 때 이들로부터 분석인자를 센싱하고 시스템에 입력하면 입력받은 분석인자와 예측인자의 비교 분석을 통해 피해가 예상되는 정보자산을 도출하고, 사고의 위험성을 판별하여 적합한 대응 프로세스를 구성하여 조치사항들을 제공한다.

외부의 간접 보안사고로부터 센싱한 분석인자를 입력하면 기업 내부에서 보안사고를 발생시킬 수 있는 잠재적인 요소들을 찾고 이에 대한 조치사항들도 제공 받

연관도 Table 상세 예시

예측인자	값(Value)	피해유형	Relation		
			조치사항 (대응매뉴얼)	....	정보자산
OpenSSL	<= 1.0.1 ※ <= : 해당버전 이하	정보노출			
OpenSSL	<= 0.9.8zf	정보노출			
Adobe	21.0.0.182	악성코드 감염			
Adobe	11.2.202.577	악성코드 감염			
악성코드	KeRanger	자료파괴			
OS	Windows7 SP1	N/A			
OS	RedHat 9.0	N/A			
....	....	....	....	....	....

연관도 Table

예측인자	값	Relation
OS		
DB		
OpenSSL		
Java		
Adobe		
....		

그림 2. 연관도 테이블 예시
Fig. 2. The example of Relation Table.

을 수 있다. 보안사고 예보시스템은 내부적으로 가중치가 지속적으로 증가하는 예측인자들을 분석하여 내부의 정보자산 중에 조치가 필요한 부분을 발굴하여 정기적으로 리포트도 할 수 있으며 보안 패치·테마 점검·사용자 권한 정비 등 주기적으로 조치해야 할 사항들을 리포트로 제공할 수도 있다.

- ✓ 예측인자: 기존에 기업에서 발생했던 보안사고의 경험과 대응 노하우로부터 보안사고의 재발 방지를 위해 이용할 수 있는 인자들을 선별하여 축적하고 이후에 발생하는 직접·간접 보안사고로부터 의미있는 데이터를 추출하여 향후 보안사고의 발생 가능성이 있는 정보자산을 미리 찾아보는데 활용되는 인자이다. 예측인자는 예보의 정확도를 높이기 위해서 예보시스템에 의해 진화된다.
- ✓ 분석인자: 직·간접 보안사고로부터 보안사고의 특성을 평가하는데 활용되는 인자이고 예보시스템에 입력하는 값이다.
- ✓ 데이터베이스: 예측인자와 정보자산, 대응 프로세스 등을 사전 준비 단계에서 데이터베이스로 구축한다.
- ✓ 위험도: 예보시스템 구축 단계에서 보안사고로 인한 피해 규모와 피해의 심각성을 고려하여 기업 자체적으로 수립한 평가기준을 가지고 위험도를 미리 정의한다. 예보시스템은 분석인자와 예측인자를 활용하여 보안사고의 위험도를 평가한다.
- ✓ 피드백: 피드백이란 보안사고가 마무리되면 사고
- ✓ 결과를 분석하여 향후 예보시스템이 활용할 수 하도록 예측인자를 누적·반영하는 과정을 말한다. 피드백과정의 목적은 예측인자 항목을 지속적으로 업데이트하고 개선시켜서 보안사고 예측의 정확도를 높이기 위한 것이다.

2. 운영 절차

보안사고 예보시스템은 예측인자를 정의하는 방법에 따라 기업의 유형, 업무 환경에 유연하게 적용할 수 있다. 예를 들면, 고객의 개인정보를 주로 취급하는 기업인 경우 예측인자를 개인정보와 관련성이 깊은 전화번호, 주민번호, 이메일주소 등으로 정의하고 계속 진화시킬 수 있다. 또한, 보안사고 예보시스템 운영자는 개인정보와 관련된 외부 동향과 사고사례를 지속적으로 입력할 것이므로 본 시스템은 개인정보와 관련된 예보시스템으로 진화하게 된다.

가. 사전 준비 단계

보안부서는 사전준비단계에 데이터베이스를 다음과 같이 등록한다.

- ✓ 예측인자 도출: 기업 내부의 특성과 중요한 정보자산의 유형 그리고 보안사고 대응 노하우 등을 고려하여 예측인자를 도출한다.
- ✓ 대응 프로세스 등록: 기업에서 운영하던 사고대응 프로세스, 규정, 조치사항 등을 예보시스템에 등록한다.
- ✓ 정보자산 현황 등록: 보안사고 발생 시 피해규모와 대상을 파악하는데 필요한 서비스 현황, 시스템 현황, 제품현황 등의 현황정보도 예보시스템에 등록한다. 보안부서는 이러한 현황정보를 수시로 업데이트하면서 관리한다.
- ✓ 연관도 테이블: 정보자산 현황정보와 예측인자를

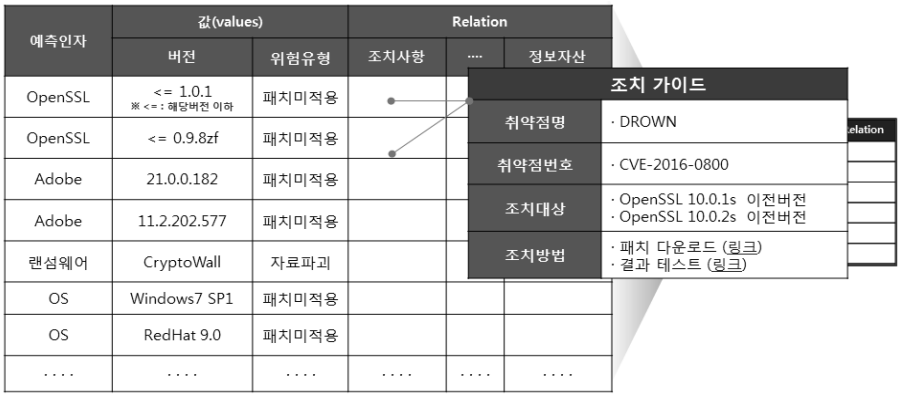

그림 3. 연관도 테이블 예시
Fig. 3. The example of Relation Table.

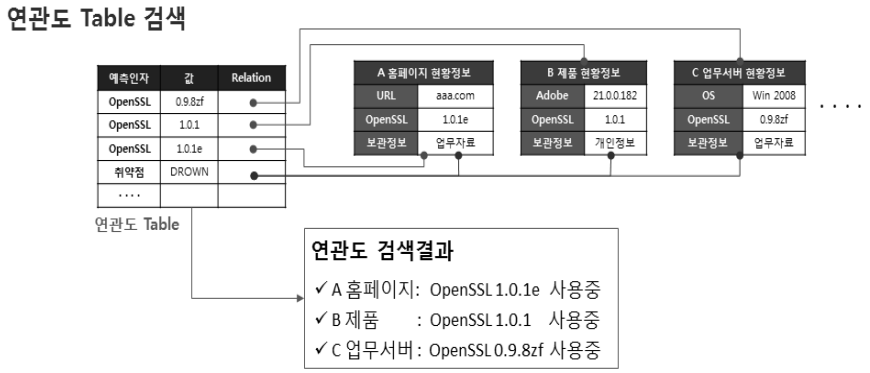

그림 4. 연관도 분석
Fig. 4. Analysis Relation.

입력하면 사고 발생 시 피해 범위 및 피해규모, 조치 대상을 명확히 제공하기 위해서 각 정보를 상호 연결하는 연관도 테이블이 구축되어 데이터베이스화 된다.

나. 예보시스템 운영 단계

(1) 분석인자 도출 방법

분석인자는 직·간접사고로부터 도출되며 예보시스템에 입력하여 정확한 조치사항을 얻기 위해 사용되는 인자이다. 예보의 정확도를 높이기 위해서 분석인자를 선정하는 판단력이 중요하다. 분석인자는 보안사고의 내용을 설명하는 키워드와 문장, 상세한 값으로 정의할 수 있다.

(2) 연관도 분석

보안사고 예보시스템은 입력된 분석인자를 예측인자 데이터베이스에서 검색한 후, 연관도 테이블을 통해 연관성이 있는 정보자산 현황정보를 도출한다.

예를 들면, [그림4]에서는 DROWN이라는 취약점의 경우, 예측인자 “OpenSSL 10.0.1s”와 “OpenSSL 10.0.2s”를 연관도 테이블에서 검색하여 “OpenSSL 10.0.1s” 등 특정 버전 이하에서 해당 취약점이 있으며 조치사항과 피해가 예상되는 정보자산을 찾을 수 있다.

(3) 위험도 판별

보안사고의 위험도 평가 기준은 관련법규와 기업 내부 특성에 맞는 내부 규정을 기반으로 수립된다. 위험도는 상, 중, 하로 구분되며 평가된 위험도에 따라서 사고 대응프로세스 및 조치사항들을 예보시스템이 제공한다. 다음은 위험도 분류 기준 예시이다. (표 활용)

✓ 고객 개인정보 노출사고 : 상
✓ 기업 기밀정보 유출사고 : 상
✓ S/W 보안 패치 미적용 : 중
✓ 악성코드 감염 대응 미흡 : 중

다. 피드백 단계

보안사고 예보시스템에서는 보안사고가 발생했을 때

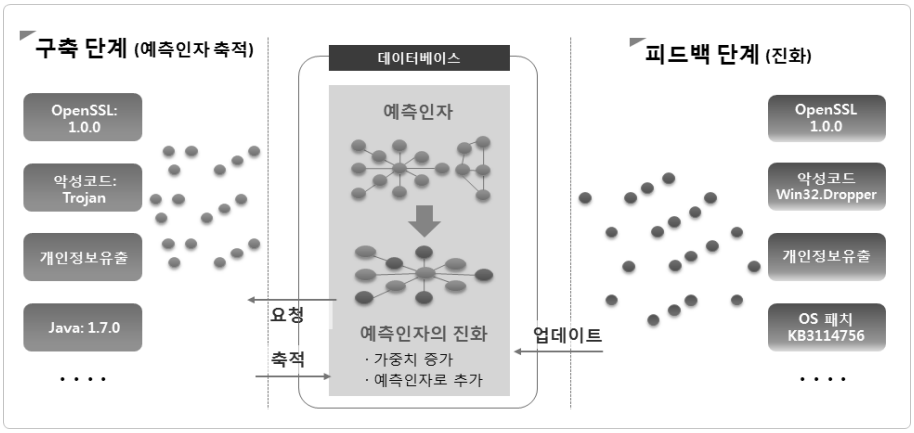

그림 5. 예측인자 진화
Fig. 5. Predictors Evolution.

사고 대응 프로세스를 제공하고, 발생하지 않은 사고에 대해서는 잠재적인 위험요소를 예측하여 리포트를 제공한다. 이러한 예측정보와 대응 프로세스 리포트의 정확도를 높이기 위해서는 예측인자, 정보자산 현황정보, 대응 프로세스, 연관도 정보 등 의미 있는 데이터를 데이터베이스에 지속적으로 보강하여 예보시스템을 진화 시켜야 한다. 이 단계를 피드백 단계라고 부른다.

(1) 예측인자 업데이트

간접·직접사고에서 분석인자를 추출하여 예측인자 데이터베이스에서 비교한 후 예측인자 데이터베이스에 존재하지 않지만 의미 있는 데이터라면 예측인자로 선정한다. 예보시스템은 예측인자 데이터베이스에 없는 새로운 항목이 생기면 예측인자로 추가한다. 또한 예보시스템에서 보안사고 종결처리를 할 시점에도 사건 발생 시 입력했던 분석인자와 데이터베이스에 저장된 예측인자, 조치결과들을 비교 분석하여 새로운 예측인자를 도출해 낸다.

자주 발생하는 사고, 사회적으로 이슈화되고 있는 보안동향, 이와 연관된 사고들에 대해서는 각 예측인자에 가중치를 부여하여 분석코어에 반영한다. 가장 위험도 높은 문제 TOP 10을 선정하여 특별 관리하고 관련사고 및 유사한 사고를 포함하여 모니터링 한다.

(2) 예측인자의 진화

예측인자들은 피드백 과정을 통해 자주 검색되는 것들은 지속적으로 가중치를 부여받게 되고 같이 검색되는 것들 간에는 유사성, 연관성 가중치가 부여된다. 이를 바탕으로 예측인자들은 집합을 형성하게 된다.

예측인자 데이터베이스에 존재하지 않는 새로운 인자가 분석인자로 입력되었을 때 보안사고 예보시스템은 예측인자 집합에서 유사성, 연관성을 찾아 정보를 추출한 후 분석한다. 유리한 정보를 확보하기 위해서 분석인자를 예측인자로 업데이트 하고 연관도 테이블을 갱신하는 등 일련의 진화과정이 일어난다. 이러한 방법은 보다 정확하고 효율적이며 지능화된 보안사고 대응 시스템으로 운영될 수 있게 한다.

라. 직접 보안사고 대응

보안부서는 기업 내부에서 보안사고가 발생하면 사고정보를 분석하고 분석인자 형태로 도출하여 예보시스템에 입력한다. 보안사고 예보시스템은 위험도 수준에 따라 등급, 대응 프로세스, 조치사항, 적용대상 등이 포함된 리포트를 제공한다. 이를 기반으로 관련부서와 함께 사고 대응 프로세스에 따라 조치하고 진행사항들을 시스템으로 관리한다. 마지막으로 사고가 마무리되면 피드백 과정을 수행한다.

마. 간접 보안사고 대응

공개된 외부 보안사고 기사나 보안동향 정보를 수집하여 보안사고 예보시스템에 입력한다. 관련 정보 수집은 보안 담당자 혹은 자동화된 시스템에 의해서 수행할 수 있다.

보안부서에서는 수집된 정보로부터 분석인자를 도출하여 예보시스템에 입력한다. 예보시스템은 잠재적 보안사고가 예측되는 제품군, 서비스, 시스템 등을 대상으로 취약한 부분, 조치사항 및 대응 프로세스를 리포트한다. 보안부서는 이를 관련부서에 알리고 관련부서는 리포트에 따라 자체점검을 실시하고 그 결과를 보안부서로 통보한다. 보안부서는 관련부서로부터 받은 조치결과가 적절한지를 판단하고 피드백 과정을 수행한다.

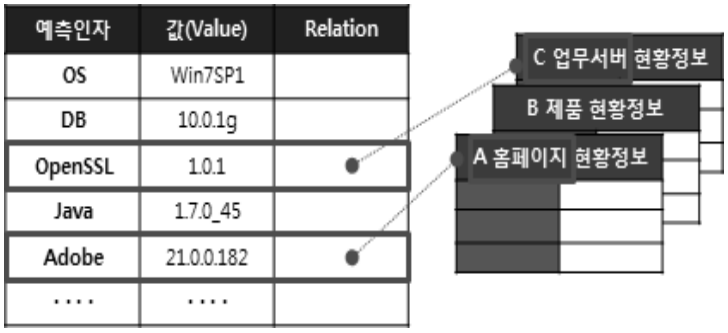

그림 6. 연관도 테이블 예시
Fig. 6. The example of Relation Table.

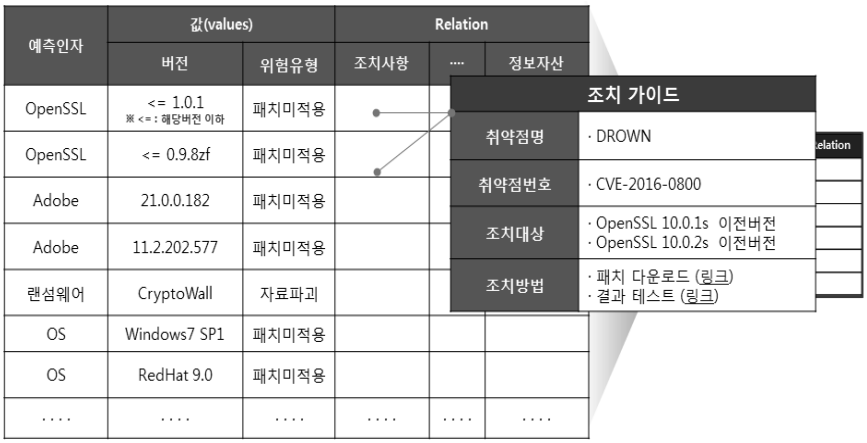

그림 7. 연관도 테이블 예시
Fig. 7. The example of Relation Table.

예보시스템은 피드백 받은 정보를 예보의 정확성을 높이기 위한 기반정보로 활용한다.

Ⅳ. 예보시스템 운영 예시

1. 사전 준비 단계

가. 예측인자 구성

고객서비스를 운영하고 있거나 홈페이지에 해킹공격이 자주 발생하는 기업에서는 다음과 같은 항목을 예측인자로 구성하여 예측인자 데이터베이스를 구성할 수 있다.

[예측인자 예시]

해커 서버, Java, 악성코드, OpenSSL, OS, Adobe, 취약점명, 관리자 ID, 비밀번호, 퇴직자 권한, 백신, 백도어, 루트킷, 웹셸, SQL DB, 한컴오피스, Android, 웹브라우저, CVE, URL 차단, IP 차단, 협력사계정, 제품 플랫폼, 등

나. 연관도 테이블 예시

예측인자, 정보자산 현황, 대응 프로세스, 조치사항 등은 연관도 테이블에 표준화된 형태로 구성된다.

[그림 7]에서는 예측인자 “OpenSSL 1.0.1버전”이 “C 업무 서버”와 연관을 갖는다는 것과 “Adobe 21.0.0.182 버전”이 “A 홈페이지”와 연관을 갖는다.

[그림 8]에서는 DROWN이라는 취약점에 대해서 예측인자 “OpenSSL 10.0.1s” 와 “OpenSSL 10.0.2s” 이하 버전에서 연관성이 있다는 것을 보여준다.

OpenSSL이라는 예측인자와 연관성을 갖는 정보자산은 DROWN 취약점을 보유한 정보자산이므로 취약점들이 모두 조치되어야 한다. 취약점으로 인하여 피해가 예상되는 정보자산은 연관도 테이블의 Relation 필드서 검색하여 제품, 서비스, 홈페이지, 업무PC 및 담당자의 정보를 상세히 얻을 수 있도록 해야 한다.

다. 대응 프로세스 시스템화

일반적으로 내부에서 보안사고가 발생하면 보안부서는 사고대응에 적합한 보안담당자를 지정하고 담당자

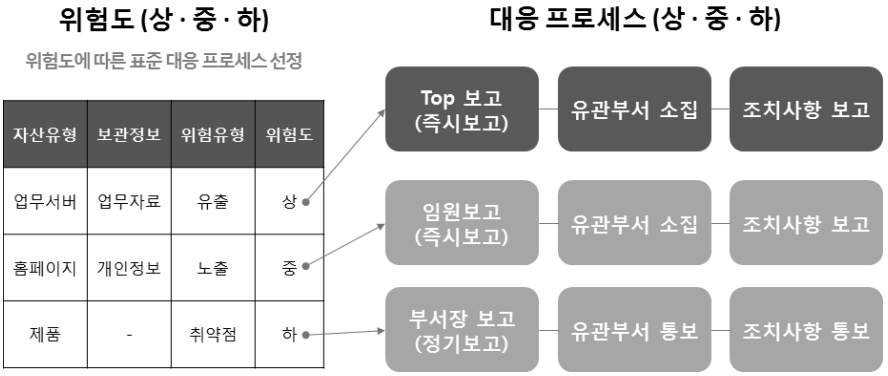

그림 8. 대응 프로세스 예시
Fig. 8. Counter Process.

개인의 능력에 의존하여 문서화된 사고 대응 프로세스에 따라 대처한다. 이러한 방식은 개인의 능력에 따라 조치결과가 달라질 수 있고 실수로 조치해야할 사항들이 누락될 수 있다는 문제가 있다.

보안사고 예보시스템은 분석인자와 예측인자를 기반으로 분석하여 시스템적으로 대응 프로세스를 구성하여 제공하므로 표준화된 방법을 통해 신속하게 대응할 수 있도록 한다.

이를 위해서는 기존에 기업이 운영하고 있던 보안사고 대응 프로세스를 위험도에 따라 세분화하여 표준화된 형태로 시스템에 입력해야 한다.

위험도를 상, 중, 하로 구분하여 위험도에 따른 대응 프로세스를 각각 구성할 수 있다.

[그림 9]를 보면 업무서버로부터 업무자료가 유출된 경우는 “위험도 상”에 해당하는 대응 프로세스를 따른다. 마찬가지로 홈페이지에서 개인정보가 노출된 경우는 “위험도 중”에 해당하는 대응 프로세스를 따른다. 제품 취약점에 대해서는 “위험도 하”에 해당하는 대응 프로세스를 따른다.

2. 예보시스템 운영단계

가. 분석인자 입력

보안사고로부터 의미 있는 분석인자를 추출하여 예보시스템에 입력한다. 아래 예에서는 분석인자로 “Drown”, “중간자 공격”, “OpenSSL 1.0.1s”, “OpenSSL 1.0.2g”를 입력한다.

나. 연관도 분석

보안사고 연관도는 직접·간접 보안사고가 발생했을 경우 기업 내 다른 제품과 서비스에는 영향이 없는지

그림 9. 분석인자 입력
Fig. 9. Input Analysis Factor.

판단할 수 있는 정보를 의미한다.

“Drawn”, “OpenSSL 10.0.1s”와 “OpenSSL 10.0.2s”에 대해서 연관도 테이블을 검색하여 하위 버전을 사용하는 제품 및 서비스를 찾아내고 Relation 필드를 검색하여 해당 제품 및 서비스 리스트의 정보를 얻는다.

연관도 테이블로부터 정보자산 “A홈페이지”와 “B제품”, 그리고 “C업무서버”는 취약점이 있다는 결과가 도출된다.

다. 위험도 평가 및 대응 프로세스 판별

예보시스템은 취약점이 있는 정보자산에 어떤 정보가 보관되어 있는지 판단하고 위험유형에 따라「위험도 평가 테이블」로부터 상, 중, 하의 결과를 판별한다. 본 예시에서는 “중”이라는 결과를 얻었다. 따라서 위험도 “중“에 해당하는 보안사고 대응 프로세스에 따라 사고를 대응하도록 한다.

라. 조치사항 및 리포트 발행

보안사고 예보시스템은 피해가 예상되는 정보자산과 위험도에 따라 조치사항을 제공하는 리포트를 발행한다. 본 예시의 경우 OpenSSL DROWN 취약점에 해당하는 패치를 적용하고 점검하라는 리포트가 도출되었다. 보

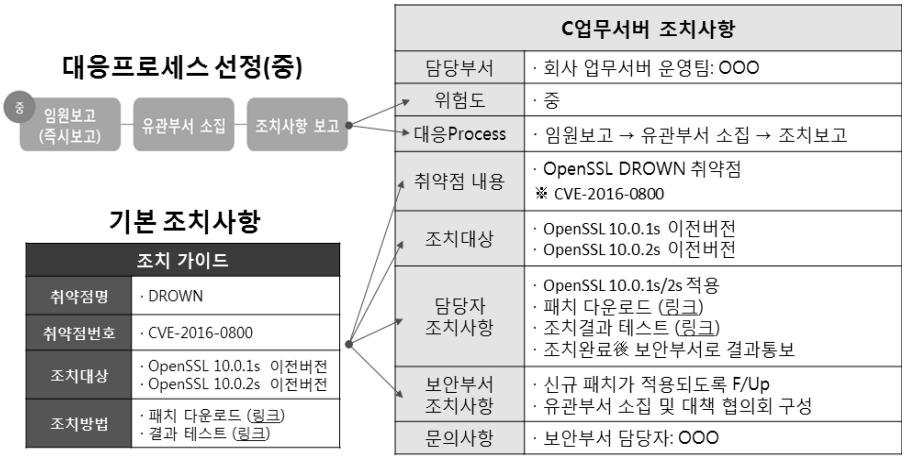

그림 10. 대응 프로세스 선정 및 조치사항 리포트
Fig. 10. Counter Process & Report.

자산유형	보관정보	위험유형	위험도
홈페이지	업무자료	패치미적용	중
업무서버	업무자료	패치미적용	중
제품	개인정보	패치미적용	중

그림 11. 위험도 판별결과
Fig. 11. Risk Result.

안부서와 각 담당자들은 조치사항 가이드에 따라 보안 패치를 적용하고 시스템을 통해 결과를 입력한다.

V. 결 론

본 논문에서 제안한 보안사고 예보시스템은 직접·간접 사고로부터 도출된 분석인자를 입력으로 받아 예측인자와 분석인자를 적용하여 위험도를 판별하는 한편, 보안부서와 유관부서에서 대응해야할 프로세스를 알려준다. 또한 리포트가 발행되어 세부적으로 조치해야할 사항들을 통보한다.

대응 프로세스는 보안사고 예보시스템에서 제공하는 표준 인터페이스*를 통해서 기업에서 문서화하여 운영하고 있던 사고 대응 프로세스들을 시스템으로 등록하는 것을 말한다. 사고가 발생하면 보안사고 예보시스템은 위험도에 따라 사전 단계에서 등록한 프로세스들을 조합하여 조치해야 할 프로세스들이 구성 된다.

기존에는 유관부서가 모여서 대응 방법을 논의하고 대책을 수립하느라 사고 대응이 지연될 소지가 있으며, 규모가 큰 기업 또는 프로세스가 복잡한 기업의 경우 프로세스 상의 조치사항들을 누락시키는 경우가 발생할 수 있었다.

보안사고 예보시스템은 위험도에 따라 대처하는 대응 프로세스들이 시스템적으로 신속하게 구성되고 유관부서로 동시에 리포트를 제공하여 체계적으로 대응할 수 있도록 한다.

특히, 간접 보안사고를 예보시스템에 지속적으로 접목하면 기업 내부와 관련 없어 보이는 사고를 통해서도 잠재적으로 내재된 보안사고를 사전에 리포트 받아 예방 조치할 수 있다.

* 사용자가 쉽게 운영 및 관리할 수 있는 인터페이스를 의미한다.

REFERENCES

[1] Anonymous attack http://www.datanews.co.kr/news/article.html?no=90099
[2] Dae-Young Lee, “A Study on Personal Data Hacking Case to build Corporate Security and Counter Strategy: Focused on HYUNDAI CAPITAL hacking case(2011)”, *Journal of Security Engineering*, v.10, n.4, 2013. 08.
[3] Dae-Young Lee, Jin-Hong Jeong, “A Case Study of Employee Privacy leaks and Fraud during B2B transaction -Focused on Man in the

Middle attack case-", *Journal of Security Engineering*, V.12, N.5, pp.501-514, 2015.
[4] The industrial espionage technology leakage situation of the domestic industry: http://m.blog.daum.net/torabora/13653348
[5] Shipbuilding technology leaks: http://www.boannews.com/media/view.asp?idx=8511
[6] March 1st Cyber attacks http://www.dt.co.kr/contents.html?article_no=2010030202010251739002
[7] NIST, Computer Security Incident Handling Guide.
[8] NIST, Cyber Security Framework, Cyber Security Issue, 2013.10.
[9] Jungduk Kim, "The Management System and Governance for Personal Information", Journal of the Korean Institute of Information Security and Cryptology, v.18, n.6, pp 1-5, 2008.12.
[10] Yoo, Jin-Ho ; Jie, Sang-Ho ; Lim, Jong-In, "Estimating Direct Costs of Enterprises by Personal Information Security Breaches", Journal of the Korean Institute of Information Security and Cryptology, v.19 no.4, pp.63-75, 2009.
[11] You, Seung Dong ; Yoo, Jinho, "Determinants of Willingness To Pay for Personal Information Protection." Journal of the Korean Institute of Information Security and Cryptology, v.24 no.4, pp 695-703, 2014.
[12] ISO, "ISO/IEC 27001-information security management", 2013: The ISO 27000 family of standards helps organizations keep information assets secure.
[13] KISA, "Personal Information Protection and Management System (PIMS) certification by bulletin (Broadcasting Communications Commission Notice No. 2013-17), http://isms.kisa.or.kr/kor/notice/dataView.jsp ?p_No=132&b_No=132&d_No=12, Mar.12. 2014"

저 자 소 개

이 동 근(정회원)
현 삼성전자 무선사업부
1990년 부산대학교 기계공학과 학사 졸업.
2010년～2013년 고려대학교 정보보호대학원 석사졸업.
2013년～현재 고려대학교 정보보호대학원 박사재학중.
<주관심분야 : 정보보호정책, 기업정보보호>

임 종 인(정회원)-교신저자
현 고려대학교 정보보호대학원 교수
현 대검찰청 디지털수사 자문위원회 위원장
현 한국정보보호학회 명예회장
현 금융보안원 보안전문기술위원회 위원장 전 대통령 안보특별보좌관
<주관심분야 : 정보보호정책, 개인정보보호, 사이버안보>