사회공학 공격에 대한 기업조직의 위험 수준 평가 방안

박 영 후*, 신 동 천**

요 약

최근의 보안 관련 공격들은 시스템의 취약점을 악용하는 공격보다는 시스템을 운영하는 사람을 목표로 하는 공격들이 다양하게 발생하고 있다. 그러나 현재 사람을 주요 공격 목표로 하는 사회공학 공격들의 위험도를 분석하여 전략적으로 대응하고자 하는 연구는 매우 부족한 현실이다. 본 논문에서는 사회공학 공격의 위험도를 평가하기 위해 공격 경로, 공격 수단, 공격 단계, 공격 도구, 공격 목표 측면에서 사회공학 공격들을 분석한다. 아울러 동일한 공격에 대해 조직의 특성과 환경에 따라 위험도는 다름을 반영하여 사회공학 공격 위험도와 함께 조직의 특성과 환경을 고려한 조직의 위험도를 평가한다. 뿐만 아니라, 일반적인 공격 위험도 평가 방법인 CVSS, CWSS, OWASP Risk Rating Methodology를 분석하여 사회공학 공격에 대한 조직의 위험도 평가 방안을 제안한다. 제안한 방법론은 조직의 환경 변화에 따라 조직에 적절한 사회공학 공격에 대한 조치를 취할 수 있도록 평가 유연성이 있다.

A Risk Assessment Scheme of Social Engineering Attacks for Enterprise Organizations

Younghoo, Park*, Dongcheon, Shin**

ABSTRACT

Recently security related attacks occur in very diverse ways, aiming at people who operate the system rather than the system itself by exploiting vulnerabilities of the system. However, to the our best knowledge, there has been very few works to analyze and strategically to deal with the risks of social engineering attacks targeting people. In this paper, in order to access risks of social engineering attacks we analyze those attacks in terms of attack routes, attack means, attack steps, attack tools, attack goals. Then, with the purpose of accessing the organizational risks we consider the characteristics and environments of the organizations because the impacts of attacks on the organizations obviously depend on the characteristics and environments of the organizations. In addition, we analyze general attack risk assessment methods such as CVSS, CWSS, and OWASP Risk Rating Methodolog. Finally, we propose the risk access scheme of social engineering attacks for the organizations. The proposed scheme allows each organization to take its own proper actions to address social engineering attacks according to the changes of its environments.

Key words : Social engineering attack, Attack risk assessment, Organization risk assessment, Human-centric security, security strategy

접수일(2019년 2월 13일), 수정일(1차: 2019년 3월 25일), 게재확정일(2019년 3월 29일)

* 중앙대학교 대학원 융합보안학과
** 중앙대학교 산업보안학과(교신저자)

1. 서론

각종 보안위협들이 다양화, 복잡화, 그리고 지능화되어 가고 있는 오늘날 사람의 의사 결정 특성인 인지적 편견에 기초한 사회공학 공격들이 발생하고 있다. 즉, 공격자는 일차 표적인 사람의 행동, 동기, 경제적인 이득, 이기심, 복수, 외부의 위협 등을 자극하여 공격 대상의 의지나 동의와 상관없이 원하는 행동을 유도한다 [1][2] 사회공학자 케빈 미트닉은 기업의 정보보안에서 가장 큰 위협은 사람이며 보안 취약점을 이용하는 것보다 더 손쉽게 목표에 도달할 수 있는 방법이라고 설명하고 있다 [3][4].

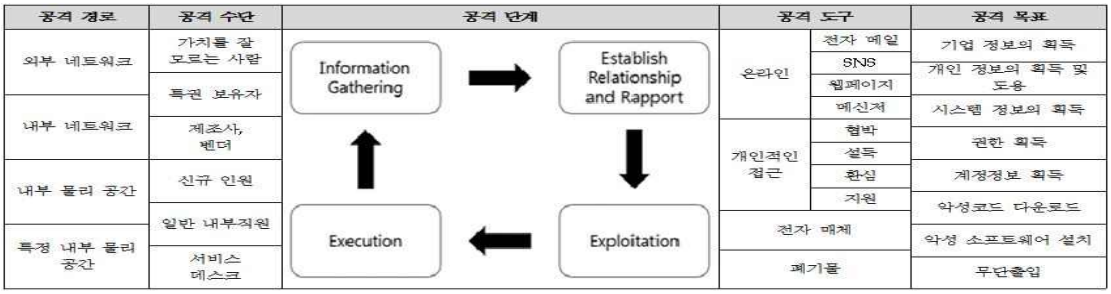
다양한 사회 공학 공격들이 있으며 사회공학 공격 사이클은 정보 수집, 관계 및 라포(papport) 형성, 공격, 실행과 같이 4단계로 이루어져 있다[5]. 그러나 공격 목표의 특성에 따라 각 단계에서 공격자가 발견되거나, 포기하거나 만족스러운 결과를 얻을 때까지 각각의 단계 또는 전체 단계를 반복해서 수행할 수 있다. 사회공학 공격이 계속적으로 증가됨에 따라 사회공학 공격의 위험성에 대한 인식은 많아지고 있지만 기존의 많은 보안취약점 평가 방법론들은 보안의 커다란 위협이 사람임에도 불구하고 사회공학 공격의 영역과 위험성을 평가에는 한계가 있다. 일반 공격 위험도 평가 방법론인 CVSS, CWSS, OWASP Risk Rating Methodology의 평가 항목들은 공격이나 취약점의 위험도뿐만 아니라 소프트웨어, 인프라 환경 및 응용 프로그램의 특성과 상태 등 목표가 되는 대상을 다양한 관점에서 고려하도록 설계되어 있다고 할 수 있다 [6][7][8][9].

사회공학 공격은 공격 자체의 위험도 존재하지만 공격이 적용되는 대상의 인식이나 특성 및 환경적인 부분 또한 고려해야만 유연하고 전략적인 사이버 공격에 대한 예측이 가능해 지며 공격에 대한 피해를 줄일 수 있다. 아울러 최근 사회공학 기법을 적용한 다양한 공격방법들이 등장하고 있으므로 공격 자체의 위험도 평가뿐만 아니라 조직의 환경까지 함께 고려하여 사회공학 공격이 조직에 미치는 위험도 평가방안이 필요하다[10]. 본 논문에서는 먼저 사회공학 공격이 조직에 미치는 공격 위험도 평가방안을 제시한다. 이를 위해 본 논문의 사전 연구 결과로 [15]에서 제시한 6개의 사회공학 공격 위험도 평가 지표를 활용하여 지표별로 객관적인 기준을 제시하여 균형 있게 공격 위험도 평가 방안을 제시한다. 한편, 사회공학 공격의 특징에 따라 같은 공격이라도 목표가 되는 조직이 보유한 환경에 따라 위험도가 달라질 수 있다. 따라서 본 논문에서는 조직의 환경을 함께 고려하여 사회공학 공격에 대한 조직 위험도 평가 지표를 도출하고 통합된 평가방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 [15]에서 제시한 사회공학 공격 위험도 평가 지표를 간략히 소개하고 이를 기반으로 한 공격 위험도 평가방안을 제시한다. 3장에서는 사회공학 공격의 목표가 되는 조직의 특성과 환경을 고려하기 위한 지표를 도출하고 4장에서는 통합한 평가방안을 제시한다. 5장에서는 결론을 맺는다.

2. 사회공학 공격 위험도 평가

이 절에서는 [15]에서 제안한 사회공학 공격 위험도 평가 지표를 간략히 소개한다. [15]에서는 사회공학 공격의 위험도를 평가하기 위한 지표를 개발하기 위해 일반 공격 위험도 평가 방법론인 CVSS, CWSS, OWASP Risk Rating Methodology를 구성하는 46가지의 항목을 분석한 후 공격 위험도 기준으로 9가지의 항목을 추출하였다. 아울러 10개의 사회공학 공격들의 특징을 분석하여 사회공학 공격에서 나타나는 구성 요소를 (Fig. 1)과 같이 공격 경로, 공격 수단, 공격 단계, 공격 도구, 공격 목표의 5가지 항목을 도출하였다[1][11][12][13][14].



(Fig. 1) Components of social attacks

사회공학 공격 위험도 평가지표는 일반 공격 위험도 평가 방법론에서 공격 위험도 기준으로 추출한 9가지 항목과 사회공학 공격 기법 분석을 통해 <Table 1>과 같이 6개의 사회공학 공격 위험도 평가 지표를 도출하였다. 사회 공학 공격들은 평가지표인 공격 경로, 공격대상, 공격 복잡도, 공격 독립성, 공격파급효과(기밀성, 무결성)에 대한 위험도가 각각 다르게 된다. 따라서 제시한 평가 지표들에 대해 위험도 정도를 등급화 하고 등급에 따라 점수를 부여한다면 각 사회 공학 공격의 위험도를 상대적으로 판단할 수 있다. 예를 들어, low=1, medium=4, high=7, critical=10 등으로 위험도를 부여할 수 있다. 점수는 조직의 특성에 따라 독자적으로 부여하면 되며 각 지표들 간의 가중치 고려 등 실제로 정량화된 평가 방안 개발은 본 논문의 범위를 벗어난다.

사회공학 공격의 공격 위험도는 공격 경로, 공격대상, 공격 복잡도, 공격 독립성, 공격파급효과(기밀성, 무결성)에 대한 평가 점수로 계산된다. 각각의 평가지표들은 평가된 등급에 해당하는 점수를 가지며, 총점은 100점 만점으로 계산된다. 공격 위험도 점수의 산출 방법은 다음과 같다.

* 공격 위험도 = (공격 경로 + 공격대상 + 공격 복잡도 + 공격 독립성 + 공격파급효과) x 1.6667

(공격파급효과 = 기밀성 + 무결성)

따라서 공격 경로, 공격 대상, 공격 복잡도, 공격 독립성들을 나타내는 공격의 기본속성 그룹을 b_m 이라 하고 기밀성과 무결성을 나타내는 공격 파급효과 그룹을 p_n 이라 하면 공격 위험도(AR)를 산출하는 공식은 다음과 같이 일반화 시킬 수 있으며 새로운 지표 도입과 같은 각 그룹의 평가 지표 변화에도 적용할 수 있다.

<Table 1> Indices of attack risk

공격의 구성 요소	CVSS	CWSS	OWASP	평가 지표	
공격 경로	Access Vector	Access Vector	-	공격 기본 속성	**공격 경로**
공격 도구	Access Complexity	-	-		**공격 복잡도**
공격 수단	-	Level of Interaction	-		**공격 대상**
공격 단계	-	-	-		**공격 독립성**
공격 목표	Confidentiality Impact	Technical Impact	Loss of Confidentiality	공격 파급 효과	**기밀성**
공격 목표	Integrity Impact	Technical Impact	Loss of Integrity		**무결성**

$$AR = \sum_{k=1}^{b_m + p_n} a_k \times \frac{100}{\sum_b + \sum_p}$$

(b_m = 공격의 기본속성 그룹 b의 평가지표수,
p_n = 공격 파급효과 그룹 p의 평가지표수,
a_k = 평가지표 k의 평가점수,
$\sum_b, \sum_p$ = 그룹 b, p의 지표점수 합)

3. 사회공학 공격 조직 위험도 평가지표

조직 위험도 지표를 도출하기 위하여 공격위험도에 영향을 줄 수 있는 다음과 같은 공격 요소를 고려하였다.

- 조직의 구성원들의 수가 많을수록 공격 위험도가 변화된다.
- 사회공학 공격에 대한 인식과 대응 방법에 대한 교육 및 훈련도에 따라 위험도가 변화된다.
- 다른 조직들 간의 업무 공유 및 협업 수준에 따라 위험도가 변화된다..
- 조직 주변의 물리적인 환경에 따라 위험도가 변화된다.

따라서 같은 공격이라도 목표가 되는 조직이 보유한 환경에 따라 위험도가 달라질 수 있기 때문에 공격 특징, 공격 목표와 조직 환경 기준으로 분류한 일반 공격 위험도 평가 방법론의 개념을 바탕으로 <Table 2>와 같이 4가지의 조직의 환경을 평가할 수 있는 기본 속성과 4가지의 조직의 환경을 평가할 수 있는 자산 중요도를 선정할 수 있는 조직 위험도 평가 지표를 도출하였다.

일반 공격 위험도 평가 방법론인 CVSS, CWSS, OWASP Risk Rating Methodology에서 취약점을 악용한 공격들을 수치화 할 때 공격 대상의 시스템이나 인프라 환경을 고려하는 것을 알 수 있다. 추출한 모든 항목을 사회공학 공격에 모두 활용할 수 없으므로 성격이 비슷한 지표를 포함하거나 개념적인 부분을 고려하여 평가 지표를 도출하였다. 기본 속성은 사회공학 공격의 목표가 되는 대상이 보유하고 있는 환경적인 측면을 평가하기 위한 속성이다. 여기에는 물리적인 측면뿐만 아니라 조직의 프로세스 및 직원들의 인지정도 또한 고려하였다. 자산 중요도는 사회공학 공격으로 인해 발생하는 피해정도를 평가하기 위한 속성이다. 각 속성과 연관되는 측면에서 고려되는 손실 등을 고려하여 평가된다.

4. 조직 위험도 평가 방안

4.1 평가 방안

사회공학 공격의 위험도에 영향을 주는 조직의 환경을 평가하기 위해 도출된 지표별로 객관적인 기준을 제시하여 평가한다. 지표에 대한 점수는 공격 위험도와 마찬가지로 low=1, medium=4, high=7, critical=10 등으로 위험도를 부여할 수 있으며 조직의 특성에 따라 독자적으로 부여할 수 있다. 각 지표별로 점수를 부여하는 방향의 예시는 다음과 같다.

■ 업무 연속성

업무 연속성은 조직이나 부서가 비즈니스의 목표를 달성하기 위해 다른 부서나 조직들과 업무적으로 공유하는 수준을 평가한다. 업무적인 공유 또는 협업이 자주 발생할수록 높은 점수를 받는다.

■ 인구 유동성

인구 유동성은 조직 주변 환경에 대한 위험도를 평가한다. 외부 인력의 출입 빈도와 주변의 인구 유동성 정도에 따라 점수가 평가 된다.

■ 공격 내구성

공격 내구성은 조직이 사회공학 공격에 대해 얼마나 준비가 되어 있는지에 대한 정도를 평가한다. 사회공학 공격에 대한 교육과 훈련 정도, 공격 대처 방안, 내부 지침 등을 평가한다.

■ 자산 중요도(기밀정보)

자산 중요도(기밀정보)는 성공적인 사회공학 공격이 조직이 보유한 기밀정보에 미치는 영향을 의미한다. 공격 위험도 평가와는 다르게 조직이

실제로 보유하고 있는 기밀 정보를 기준으로 한다. 기밀 정보에 미치는 영향이 증가할수록 높은 점수를 받는다.

■ 자산 중요도(비즈니스 신뢰성)

자산 중요도(비즈니스 신뢰성)는 성공적인 사회공학 공격이 조직의 비즈니스 신뢰성에 미치는 영향을 의미한다.

■ 자산 중요도(비즈니스 가용성)

자산 중요도(비즈니스 가용성)는 성공적인 사회공학 공격이 조직의 비즈니스 신뢰성에 미치는 영향을 의미한다.

■ 자산 중요도(시스템 자원 손실)

자산 중요도(시스템 자원 손실)는 성공적인 사회공학 공격이 조직의 비즈니스 신뢰성에 미치는 영향을 의미한다.

<Table 2> Indices of organizational risk

CVSS	CWSS	OWASP	평가 지표	
Target Distribution			조직기본속성	기업규모
Target Distribution				업무연속성
Target Distribution				인구유동성
	Internal Control Effectiveness Authentication Strength Likelihood of Discovery Likelihood of Exploit External Control Effectiveness	Opportunity, Ease of Discovery, Ease of Exploit, Awareness		공격내구성
Confidentiality Impact, Collateral Damage Potential, Confidentiality Requirement	Business Impact	Loss of Confidentiality	자산중요도	기밀정보영향
Collateral Damage Potential, Confidentiality Requirement, Integrity Requirement	Business Impact	Reputation Damage, Non-Compliance		비즈니스신뢰성
Collateral Damage Potential, Availability Requirement	Business Impact	Financial Damage, Privacy Violation		비즈니스가용성
Availability Impact, Collateral Damage Potential, Availability Requirement,	Technical Impact	Loss of Availability		시스템리소스

조직 위험도를 평가하기 위해 앞서 도출한 지표들을 환경 지표 그룹으로 분류하였다. 환경 지표 그룹은 사회공학 공격이 목표로 하는 공격 대상의 환경을 고려한 위험도를 평가한다. 기업 규모, 업무 연속성, 인구 유동성, 공격 내구성 요소들은 공격 대상이 가지고 있는 물리적, 업무적 환경들이 사회공학 공격에 대한 노출의 정도를 평가한다. 4가지 자산 중요도 요소는 공격 대상이 보유하고 있는 자산들에 대해 공격이 성공했을 경우 손상 정도와 조직의 우선순위를 판단하여 평가한다.

사회공학 공격에 대한 조직 위험도는 같은 공격이라도 공격 대상이 되는 조직의 환경에 따라 다른 평가 점수를 부여 받을 수 있게 2절에서 제시한 공격 위험도 평가 결과에 조직의 환경에 대한

평가 점수를 곱하여 조직의 위험도를 평가한다.

사회공학 공격의 대상에 대한 환경점수는 기업 규모, 업무 연속성, 인구 유동성, 공격 내구성과 자산 중요도에 대한 평가 점수를 더한 뒤 1점 만점으로 환산하여 환경 지표 그룹을 계산한다. 자산 중요도는 평가하고자 하는 사회공학 공격에 대해 기업이 보유하고 있는 기밀정보, 비즈니스 신뢰성, 비즈니스 가용성, 시스템 자원 손실에 대한 사항을 평가한다. 자산 중요도는 조직의 특성에 맞게 4가지 자산에 대해 위험도 가중치를 선택하여 부여하게 된다. 부여하는 위험도 가중치는 현재 조직의 상황에서 해당 자산에 대한 보호 수준에서 결정되는 가중치로써 본 논문에서는 위험도 가중치를 선택한 요소에 대해서는 평가 점수에 2배를 곱하여 계산하고, 선택하지 않은 요소에 대해서는 1배를 곱하여 평가하여 상대적인 중요도를 반영하는 것으로 제시하였다. 환경 지표 그룹을 계산하는 방법은 다음과 같이 나타낼 수 있다.

- 조직의 환경 = (기업규모 + 업무 연속성 + 인구 유동성 + 공격 내구성 + 자산 중요도) x (0.0125 ~ 0.0083)
- 자산 중요도 = 기밀정보 x S_1 + 비즈니스 신뢰성 x S_2 + 비즈니스 가용성 x S_3 + 시스템 자원 손실 x S_4 (단, S_i는 최대 4개까지 선택)

조직의 환경에 맞도록 평가를 일반화 하기 위해 기업규모, 업무 연속성, 인구 유동성, 공격 내구성을 나타내는 조직의 기본속성 그룹을 b′라 하고 기밀정보, 비즈니스 신뢰성, 비즈니스 가용성, 시스템 자원 손실을 나타내는 자산 중요도 그룹을 p′라 하자. 조직의 환경(OE)을 산출하는 공식은 다음과 같이 일반화할 수 있다.

$$OE = \sum_{l=1}^{b_m' + p_n'} a_l \times \frac{1}{\sum_{b'} + \sum_{p'}}$$

(b_m' = 조직의 기본속성 그룹 b'의 평가 지표 수,
p_n' = 자산중요도 그룹 p'의 평가 지표 수,
e_l = 평가 지표 l의 평가 점수,
$\sum_{b'}, \sum_{p'}$ = 그룹 b', p'의 지표점수 합)

본 논문에서는 사회공학 공격에 대한 조직 위험도는 같은 공격이라도 공격 대상이 되는 조직의 환경에 따라 다른 평가 점수를 부여 받을 수 있도록 사회공학 공격 위험도(최대 100점)와 조직의 환경에 대한 평가 점수(최대 1점)를 곱하여 공격 위험도가 조직의 위험도로 변환되도록 하였다. 공격 위험도를 조직의 환경을 고려한 위험도로 변환하기 위해 기본 지표 그룹에서 계산된 공격 위험도와 환경 지표 그룹에서 계산된 조직의 환경을 곱하여 최종적으로 사회공학 공격이 목표로 하는 조직에 대한 위험도를 평가할 수 있다.

최종적으로 사회공학 공격에 대한 조직 위험도는 공격 위험도 점수에 조직의 환경 점수를 곱하여 산출한다. 따라서 공격 위험도 점수(AR)와 조직의 환경(OE) 점수로 계산되는 조직 위험도(OR)를 아래와 같이 일반화할 수 있다.

$$OR = \left(\sum_{k=1}^{b_m + p_n} a_k \times \frac{100}{\sum_{b} + \sum_{p}} \right) \times \left(\sum_{l=1}^{b_m' + p_n'} e_l \times \frac{1}{\sum_{b'} + \sum_{p'}} \right)$$

(b_m = 공격의 기본속성 그룹 b의 평가 지표 수,
p_n = 공격파급효과 그룹 p의 평가 지표 수,
b_m' = 조직의 기본속성 그룹 b'의 평가 지표 수,
p_n' = 자산중요도 그룹 p'의 평가 지표 수,
a_k, e_l = 평가 지표 k, l의 평가 점수,
$\sum_{b}, \sum_{p}, \sum_{b'}, \sum_{p'}$ = 그룹 b, p, b', p'의 지표점수 합)

4.2 평가방안 비교분석

본 논문에서 제안한 사회공학 공격 위험도 평가 방안을 일반 평가방법론들과 정성적인 비교한 결과를 <표 3>은 보여주고 있다. 제시한 평가 방안은 사회공학 공격의 특징을 고려함과 동시에 조직의 환경을 고려한 평가 방안이라는 차별성을 갖는다. 제시한 평가 방안의 특징은 다음과 같이 요약된다.

- 결과의 객관성 보장

제시한 평가 방안은 객관적인 위험도를 평가하기 위해 사회공학 공격이 지니고 있는 근본적인 위험도를 평가하기 위한 공격 위험도와 사회공학 공격이 적용되는 조직의 환경적인 특징을 고

려한 조직 환경의 위험도로 분리하여 평가한다. 따라서 공격 위험도 단계에서는 기존 사회공학 공격의 위험도를 평가함으로써 각 공격별로 상대적인 위험도를 확인할 수 있고 앞으로 나오는 새로운 사회공학 공격들에 대해서도 정량적인 평가가 가능해진다. 또한 조직의 위험도 단계에서는 조직의 상황과 환경을 고려한 조직의 환경 점수를 조직의 특성에 맞게 적용함으로써 조직 스스로 놓여있는 현실적인 위험도를 평가할 수 있다.

• 취약점 대비 수준 확인 가능

평가된 조직 위험도 점수를 데이터베이스화 하여 누적된 점수 데이터를 활용한다면 사회공학 공격에 어느 정도 수준으로 대비되어 있는지 변화를 확인할 수 있으며, 사회공학 공격에 취약한 조직의 특징을 더욱 명확히 파악할 수 있다. 또한 기업들의 향후 보안정책과 보안교육에 대해서도 어떤 부분에 우선순위를 두어야 하는지에 대한 방향을 제시해 줄 수 있다.

• 취약점 제거 이후의 상태 확인 가능

향후 취약점 제거 계획 수립에 특정 취약점을 제거한 후의 위험도를 미리 평가할 수 있어 취약점 제거의 우선순위를 정할 수 있기 때문에 효율적인 취약점 제거에 활용할 수 있다.

<Table 3> Comparison of Methodologies

방법론명	CVSS			CWSS			OWASP		사회공학 위험도 평가 모형	
주체	NIAC, FIRST			NCSD, DHS			OWASP재단		-	
특징	IT 플랫폼에 존재하는 취약점들에 대해 공통적인 알고리즘을 적용하여 위험도를 수치화			소프트웨어 상의 취약점을 일관적이고, 유연하고, 개방적으로 측정할 수 있는 메커니즘 제공			안전한 웹 및 응용프로그램을 개발할 수 있도록 지원하기 위한 애플리케이션 보안 프로젝트		사회공학 공격에 대해 대상 조직의 환경에 변화되는 위험도를 수치화	
평가대상	IT 인프라			소프트웨어			웹 애플리케이션		조직의 환경	
평가영역	기본	시간	환경	기본발견	공격표면	환경	공격 성공 확률	영향	기본	환경
평가항목	Access Vector, Access Complexity, Authentication, Impact(CIA)	Exploitability, Remediation Level, Report Confidence	Collateral Damage Potential, Target Distribution, Security Requirements(CIA)	Technical Impact, Acquired privilege, Acquired Privilege Layer, Internal Control Effectiveness, Finding Confidence	Required Privilege Required privilege Layer Access Vector Authentication Strength Level of Interaction Deployment Scope	Business Impact Likelihood of Discovery Likelihood of Exploit External Control Effectiveness Prevalence	Skill Level Motive Opportunity Size Ease of Discovery Ease of Exploit Awareness Intrusion Detection	Loss of CIA Loss of Accountability Financial Damage Reputation Damage Non-Compliance Privacy Violation	공격 경로, 공격 복잡도, 공격 대상, 공격 독립성, 영향도(C, I)	기업 규모, 업무 연속성, 인구 유동성, 공격 내구성, 기밀정보 영향, 비즈니스 신뢰성, 비즈니스 가용성, 시스템 리소스
항목수	14			16			16		14	
총점	10.0			100			Critical		100.0	
최신버전	3.0			1.0.1			-		-	
발표년도	2015.05			2014.09			-		-	

5. 결론

본 논문에서는 사회공학 공격이 조직에 미치는 위험도를 정량적으로 평가할 수 있는 방안을 제시하였다. 동일한 사회공학 공격 기법이라도 공격이 적용되는 조직 환경 또는 특성에 따라 위험도가 달라질 수 있다. 따라서 먼저 순수하게 사회공학 공격의 위험도를 평가할 수 있는 방안을 제시한 후 조직의 환경 요소를 함께 고려하였다. 공격의 순수한 위험도를 평가하기 위해 공격 경로, 공격 수단, 공격 단계, 공격 도구, 공격 목표를 고려 지표로 설정하였다. 아울러 조직의 사회공학 공격 위험도에 영향을 줄 수 있는 8가지 환경적 지표를 도출하여 조직의 특성과 환경을 고려하여 최종적으로 사회공학에 대한 조직 위험도 평가 방안을 제시하였다.

제시된 사회공학 공격에 대한 조직의 위험 수준 평가 방안은 사회공학 공격 기법들에 대해 공통적으로 적용할 수 있기 때문에 상대적인 정량적인 평가가 가능하다. 뿐만 아니라 조직의 특성과 환경을 반영하기 때문에 각 조직은 실제 상황을 반영한 사회공학 공격의 위험도를 조직의 환경에 맞추어 평가할 수 있다. 즉, 추가적인 공격 특징이나 추가적으로 고려되어야 하는 상황, 조직의 특성과 환경의 변화에도 적용할 수 있는 유연성을 갖는다고 할 수 있다.

참고문헌

[1] UK National Computer Emergency Response Team, 'An introduction to social engineering'. (https://www.ncsc.gov.uk/guidance/introduction-social-engineering)

[2] M. N. Sadiku, A. E. Shadare and S. M. Musa, "Social Engineering: An Introduction", Journal of Scientific and Engineering Research, Vol.3, Issue.3, pp.64-66, 2016.

[3] K. Mitnick, "How to hack peoplle" (http://news.bbc.co.uk/2/hi/technology/2320121.stm)

[4] C. Hadnagy, 'Social engineering: The art of human hacking', John Wiley & Sons, 2010.

[5] A. Nyirak, "The Attack Cycle", (http://www.social-engineer.org/framework/attack-vectors/attack-cycle)

[6] CVSS-SIG, 'Common Vulnerability Scoring System', (https://www.first.org/cvss)

[7] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System", IEEE Security & Privacy, Vol. 4, Issue. 6, pp. 85-89, 2006.

[8] CWE, 'Common Weakness Scoring System'. (https://cwe.mitre.org/cwss/cwss_v1.0.1.html)

[9] OWASP Foundation, 'The OWASP Risk Rating Methodology', (https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)

[10] Microsoft, 'How to Protect Insiders from Social Engineering Threats', 2014. (https://msdn.microsoft.com/en-us/library/cc875841.aspx).

[11] J. Long, 'No tech hacking: A guide to social engineering, dumpster diving and shoulder surfing',. Syngress, 2011.

[12] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks", Journal of Information Security and Applications, Vol. 22, pp. 113-122, 2015.

[13] D. Bisson, "5 Social Engineering Attacks to Watch Out For", (http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/)

[14] P. Chen, L. Desmet, and C. Huygens, "A study on Advanced Persistent Threats", IFIP International Conference on Communications and Multimedia Security, pp. 63-72, 2014.

[15] D. C. Shin and Y. H. Park, "Development of Risk Assessment Indices for Social Engineering Attacks", Journal of Security Engineering,, Vol. 14, No. 2,pp. 143-156. 2017.

〔저자소개〕

박영후(Younghoo Park)
2012년 8월 학사
2017년 2월 석사
2017년 6월~현재:시큐리티인사이드 선임 컨설턴트
email : pyh0206@gmail.com

신동천 (Dongcheon Shin)
1985년 2월 학사
1987년 2월 석사
1991년 2월 박사
email : dcshin@cau.ac.kr