효과적인 위협관리를 위한 보안 위험도 평가기법*

강필용° 심원태
한국정보보호진흥원 인터넷침해사고대응지원센터
kangpy@kisa.or.kr, shim@kisa.or.kr

Security Risk Evaluation Scheme for Effective Threat Management

Pilyong Kang° Wontae Shim
Korea Internet Security Center(KISC), Korea Information Security Agency(KISA)

1. 서론

중요 IT 자산에 대한 보안성 강화를 위해서는 관련 위협(또는 취약점)의 식별 및 이에 대한 보안 대비책의 적정성 분석이 선행되어야 한다. 즉, 보안 관리자 입장에서는 중요 자산에 대한 최신 위협의 식별을 비롯하여 공격시도 탐지규칙 및 취약점 점검규칙 등 현재의 보안관리 체계가 적절히 적용 및 운영되고 있는지 사전에 점검하는 것이 무엇보다 중요하다. 그러나, 기존의 연구 및 제품들은 보안 로그만을 제공함으로써 운용중인 보안체계가 중요 자산에 영향을 줄 수 있는 공격을 얼마나 탐지할 수 있는지, 운용중인 보안 취약점 스캐너가 해당 위협을 얼마나 커버하는지 여부 등 총체적인 대응 수준에 대한 점검을 지원하기엔 미흡하다.

이에 본 논문에서는 중요 자산 및 위협(또는 취약점)별 보안 위험도 평가기법을 제안함으로써, 식별된 보안 위협에 대한 대응체계의 적정성 및 정량적인 위험도 계산을 통한 우선순위 부여 등 효과적인 위협관리를 지원하고자 한다.

2. 자산 및 위협 기반 위험도 평가기법

제안하는 기법은 침입경보 및 취약점 점검결과 등 다양한 보안 로그를 수집하여, 알려진 위협(또는 취약점) 및 중요 자산과의 상관관계 분석을 통해 보안 대응책의 누락여부 체크 및 정량적인 위험도를 계산하고, 우선순위 부여를 통한 적절한 대응을 지원한다.

본 논문에서는 위협 및 취약점 정보, 자산 정보, 침입탐지시스템, 취약점 스캐너 등이 운용되는 일반적인 환경을 고려한다. 그림 1은 중요 자산 및 알려진 위협에 대한 위험도 점검절차를 나타낸 것이며, 참고로 관련 보안장비가 더 있는 경우엔 해당 점검절차를 4단계 이후에 추가될 수 있다.

1단계 : 새로운 보안 위협/취약점 수집(즉, 위협 데이트베이스를 갱신)
2단계 : 관련 자산이 있는지 점검(즉, 위협과 자산을 매핑)
3단계 : 관련 공격시도 탐지규칙 적용여부 점검, 규칙을 운용하는 경우 탐지 횟수 조사(즉, 자산 관련 위협에 대한 침입탐지시스템의 탐지여부 및 빈도 확인)
4단계 : 관련 취약점 점검규칙 적용여부 점검, 규칙을 운용하는 경우 취약점 발견 여부 조사(즉, 자산 관련 위협에 대한 취약점 스캔 지원여부 및 스캔 결과 확인)
5단계 : 보안 점검표 작성을 통해 누락된 취약점, 탐지규칙, 점검규칙 등 추가(즉, 보안 대응체계 보완)
6단계 : 정량적인 위험도 및 대응도 계산

그림 1. 보안 위험도 점검절차

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2005-S606-02, 차세대 침해사고 예측 및 대응기술 개발]

본 논문에서는 제안한 기법의 분석 및 가능성 평가를 위해 위협 및 취약점 데이터베이스는 CVE(Common Vulnerabilities Exposures)*, 네트워크 기반 침입탐지시스템(NIDS)은 SNORT, 호스트 기반 침입탐지시스템(HIDS)은 A사의 제품, 취약점 스캐너는 NESSUS를 활용하고, 자산관리 모듈은 자체적으로 구현함으로써 시스템 프로토타입을 구현했다.

그림 2는 위험도 점검절차에 따라 보안 점검표를 작성한 예제를 나타낸 것으로, 음영이 있는 부분은 관련 사항의 누락을 의미한다. 예를들어, 사례 ①은 위협이 부재한 경우로 관련 탐지 및 점검 규칙을 참조한 신규 위협의 추가가 요구되며, 사례 ② 및 ③은 각각 탐지규칙 및 점검규칙이 부재한 경우로 관련 위협 등을 참조한 신규 탐지규칙 및 점검규칙의 추가가 요구됨을 알 수 있다.

그림 3은 최신 취약점 10개에 대한 정량적인 위험도 시각화 예제를 나타낸 것으로, 취약점에 대한 보안도 구별 대응도 및 보안 이벤트 발생 정도를 함께 나타냄으로써 운영환경에 대한 직관적인 인지를 지원한다.

알려진 위협/취약점	1	2	3	4	5	6	①
관련 자산(OS, SW)	O	O	O	O	O		O
NIDS 탐지규칙	O(0)	O(5)	②	O(0)	O(3)	O(0)	O(9)
HIDS 탐지규칙		O(7)	②	O(4)		O(0)	
SCANNER-1 규칙	O(O)	O(-)	O(X)			③	O(O)
SCANNER-2 규칙	O(O)	2(O)		O(X)	O(-)	③	

※ ( )은 IDS의 공격시도 탐지횟수, 스캐너의 취약점 점검결과를 표시
[범례: 숫자(횟수), O(발견), X(미발견), -(미점검)]

그림 2. 취약점별 위험도 시각화 예제

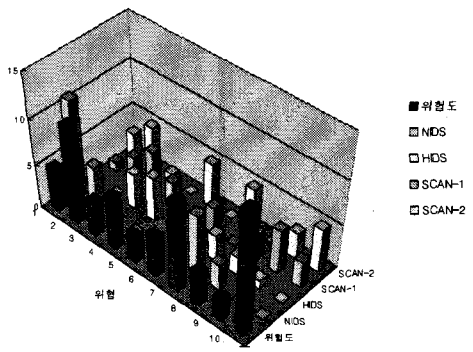

그림 3. 취약점별 위험도 시각화 예제

이와 같이 제안한 점검표 및 시각화를 활용하면, 탐지규칙 및 점검규칙 등 보안 대비책의 누락여부 체크를 비롯하여 보안 이벤트 발생빈도 및 위험도 시각화 등을 통해 시의적절한 대응체계 운용을 지원할 수 있음을 알 수 있다.

참고로 본 논문에서는 정량적인 위험도 산정을 위한 계산식을 제안하는데, 위협 t에 대한 위험도, $R_t(t)$는 다음의 수식과 같이 공격시도 정도를 나타내는 공격도(T)와 충격도(I), 자산가치(A)의 곱으로 얻을 수 있다.

$$R_t(t) = \sum_{i=0}^{n-1} T(i,t) \times I(t) \times \sum_{j=0}^{n-1} A(j,t)$$

3. 결론

본 논문에서는 중요 자산(네트워크 및 호스트 등)에 대한 위협관리의 적정성 및 위험도를 사전에 검증하기 위해 중요 자산 및 알려진 위협에 대한 위험도 평가기법을 제안했다. 제안한 기법은 식별된 알려진 위협에 대해 보안관리 환경이 공격시도 탐지 및 취약점 점검을 위해 얼마나 대비하고 있는지 정량화된 분석결과를 제공함으로써, 총체적인 보안 대응 수준을 보안 관리자가 사전에 점검 및 판단할 수 있도록 지원한다. 요컨대, 본 연구결과는 중요 자산과 관련된 보안 위협에 대한 사전 점검을 강화하고, 우선순위 부여를 통한 적절한 대응을 유도함으로써 보호 대상의 보안성 향상에 기여할 것으로 기대된다.

* 다양한 보안도구간 원활한 취약점 공유를 위한 것으로 8월말 현재, 153개 조직 및 기관에서 273의 제품 및 서비스가 호환성을 제공하고 있다.