교육기관 보안관제를 위한 효율적인 정보보호 수집체계에 관한 연구

권성호, 안재호, 윤성준
한국교육학술정보원
shkweon@keris.or.kr jhahn@keris.or.kr sjyoon@keris.or.kr

A Study On Information Security Data Collecting System For Security Monitoring Of Education Facilities

SEONG-HO KWEON, JAE-HO AHN, SUNG-JUN YOON
Korea Education Research & Information Service(KERIS)

요 약

최근의 국가·민간의 정보시스템을 위협하는 공격들은 점점 더 복잡해지고 정교해지고 있다. 이러한 공격들에 대응하기 위하여 범국가적으로 사이버안전센터들이 설립·운영되고 있다. 그러나 이러한 대량의 정보보호 데이터를 수집·분석·대응하는 것은 여러 가지 어려움들이 존재한다. 그 문제의 본질적인 부분은 바로 방대한 데이터의 양(量)이다. 다수의 보안관제 대상 인프라들의 모든 보안데이터를 수집 하는 것은 사실상 불가능하며, 대부분의 센터들은 네트워크 접점에 중앙관리형 보안인프라를 설치함으로써 그 해결점을 찾고 있지만, 이는 최근의 나타나고 있는 다차원적인 공격에 대응하기에는 한계가 있다. 본 논문에서는 이러한 다차원 분석시스템의 기본데이터가 되는 여러 보안정보를 효과적으로 수집할수있는 보안정보 수집체계를 제시하고자 한다.

1. 서론

현대사회에서의 정보의 힘은 곧 국가의 경쟁력과 연결되며, 이를 위협하는 요소들에 대해 효율적으로 대응하지 못할 경우 엄청난 대가를 치러야 한다. 최근에 발생한 7.7 DDoS 대란이 이를 잘 보여주고 있다. 이러한 대란을 겪으며 정보보호의 필요성과 함께 조직적인 대응체계의 중요성이 대두되고 있다. 그중에서도 사이버공격을 실시간 탐지, 분석·대응하는 보안관제업무의 중요성이 더해가고 있으며, 현재 국가 행정기관은 물론 민간기관에서도 사이버 보안관제센터를 설립, 운영하고 있다[1]. 이러한 보안관제 업무의 가장 근본적이고 큰 문제는 보안정보 데이터의 양이다. 수많은 기관에서 발생하는 방대한 양의 보안정보를 분석해서 대응하는 일은 현실적으로 불가능하다. 그렇기 때문에 어떤 데이터를 어떻게 수집할 것인가는 보안관제 업무에 있어 가장 중요한 부분이다. 아무리 고도화된 분석 방법론과 기법을 적용하여도 기본적으로 양질의 원시데이터를 수집하지 못하면 효과적으로 사이버 위협정보를 찾아내는 것은 불가능하기 때문이다. 본 논문에서는 대규모 데이터를 처리하고 특히 교육분야에 적합한 보안정보 수집체계를 제시하고자 한다.

2. 보안관제의 개념

보안관제는 여러 정보보호에 관련된 데이터를 수집하고, 이를 분석하여 결과물을 얻어내는 일련의 행위이다.[2] 보안관제 업무는 기본적으로 양질의 보안정보 데이터를 수집하지 못한다면 아무리 좋은 분석 방법론과 시스템도 무용지물이나 다름없다. 그렇기에 효율적인 보안정보 수집체계는 보안관제의 중심축이며, 사이버안전센터를 구축할 때 가장 많은 연구와 검증을 수행해야 하는 부분이다.

3. 교육기관 정보보호 수집체계

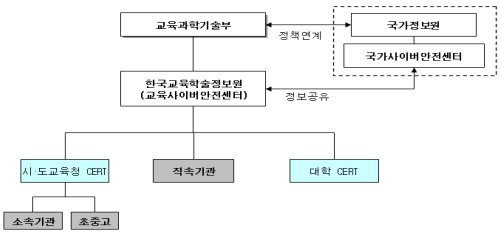
3. 1 교육기관 보안관제 현황

교육기관들은 과거 해커들의 놀이터라고 불릴 만큼 해킹사고가 많이 발생하였다. 교육기관의 해킹사고들을 분석해보면 자료의 유출·훼손등의 직접적인 1차 사고보다는 해킹 경유지, 좀비PC등 주요 침해사고의 중간 경유지로 이용되는 2차사고가 더 많이 발생했다[3][4].

	웜·바이러스	경유지악용	홈페이지 변조	자료훼손 및 유출	기타	계
2007	1,504	513	91	18	22	2,148
2008	1,210	454	82	73	48	1,867

<표 1> 2007~2008 교육기관 침해사고 유형

이러한 문제를 해결하기 위해서는 서버 및 네트워크 보안뿐만 아니라 사용자의 보안까지 포함하여 관제할 수 있는 데이터 수집체계가 필요하지만 대부분의 기존 수집체계들은 사용자단의 보안정보 수집은 전무한 실정이다. 이에 교육기관에서는 사용자단의 보안까지 고려한 보안관제체계를 수립하여 사이버 침해에 대응할 필요성이 제기 되었다. 이에 2008년 범 국가적인 보안관제 필요성에 맞추어 1차적인 단위 CERT 와 중앙의 콘트롤타위의 역할을 수행하는 교육사이버안전센터로 이루어진 [그림1]과 같은 보안관제 체계를 수립하였다.



[그림 1]교육기관 보안관제 체계도

3. 2 보안정보 수집체계

이제 앞서 언급한 보안관제 체계 안에서 중추적인 역할을 수행하는 교육기관의 특성을 고려한 체계적인 보안정보 수집체계를 제안 하고자 한다.

3.2.1 정보보호 데이터 수집항목 선정

현재 여러기관에서 많이 사용되고 있는 정보보호 인프라들은 보호하고자 하는 범위, 대상, 기능별로 매우 여러 가지 형태의 보안정보를 포함하고 있다. 이러한 보안정보들 중 효율적인 보안관제를 위해 5가지 보안영역내에 핵심적인 보안정보들을 분류하여 정의하고 이를 수집 할 수 있는 보안인프라 10가지를 <표 2>와 같이 선정한다.

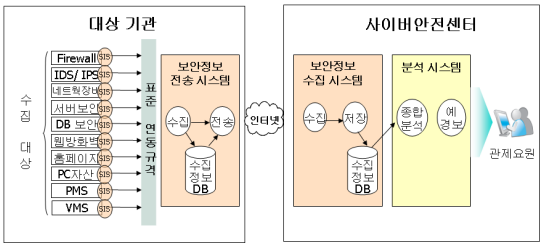
핵심 정보보호 데이터			보안정보 수집 시스템		비고
보안영역	제공 정보	세부 제공정보	정보소스 인프라	실제 수집 정보	
사용자 보안	침해발생정보	바이러스감염 정보	PMS/안티바이러스 매니저	PMS/안티바이러스 매니저 통계정보	단기
	침해대응정보	패치설치정보	PMS	PMS 매니저 통계정보	단기
		안티바이러스 설치 정보	PMS/안티바이러스 매니저	PMS/안티바이러스 매니저 통계정보	단기
APP 보안	장애정보	시스템 상태 정보	대표홈페이지시스템	시스템 구동 프로세스 및 서비스 현황	단기
	공격시도정보	Scan공격 통계 정보	Secure OS	Secure OS 이벤트(패턴정보, Deny정보)	단기/중기
	침해발생정보	공격유형별 통계 정보	웹방화벽	웹방화벽 이벤트(패턴정보, Deny정보)	장기
		홈페이지 침해 정보	Web컨텐츠보안	웹컨텐츠보안(패턴정보, Deny정보)	장기
	침해대응정보	Deny된 통계 정보	웹방화벽	웹방화벽 이벤트(패턴정보, Deny정보)	장기
네트워크 보안	위협트래픽 정보	네트워크 사용량 통계 정보	Transaction/Session 통계	네트워크시스템 Transaction/Session 정보	단기
		위협트래픽 정보	침입탐지·방지시스템	침입탐지시스템 이벤트(위협트래픽정보)	단기
시스템 보안	공격시도정보	공격시도 통계 정보	침입차단시스템	침입차단시스템 이벤트(패턴정보, Deny정보)	단기
			침입탐지·방지시스템	침입탐지시스템 이벤트(패턴정보)	단기
			Secure OS	Secure OS 이벤트(패턴정보, Deny정보)	단기/중기
	침해발생정보	공격유형별 통계 정보	침입차단시스템	침입차단시스템 이벤트(패턴정보, Deny정보)	단기
			침입탐지·방지시스템	침입탐지시스템 이벤트(패턴정보)	단기
			Secure OS	Secure OS 이벤트(패턴정보, Deny정보)	단기/중기
	침해대응정보	Deny된 통계 정보	침입차단시스템	침입차단시스템 이벤트(패턴정보, Deny정보)	단기
			Secure OS	Secure OS 이벤트(패턴정보, Deny정보)	단기/중기
DB보안	침해발생정보	공격유형별 통계 정보	DB Audit 시스템	DBAudit시스템 이벤트(패턴정보, Deny정보)	장기
	침해대응정보	Deny된 통계 정보	DB Audit 시스템	DBAudit시스템 이벤트(패턴정보, Deny정보)	장기

<표 2> 보안관제를 위한 정보보호 데이터

선정된 보안정보 데이터중 실제 수집할 속성을 분류하고 다른 보안인프라 데이터와 상관성이 높은 속성에 우선순위를 두어 휴리스틱한 기법을 이용하여 효율적인 보안관제를 위한 데이터 속성만을 추출한다. 이것을 보안정보 연동규격화 하여 유연한 적용이 가능 하도록 한다. 이러한 연동규격은 개별 보안인프라에 모듈형태로 설치 되며, 보안정보 데이터를 정해진 규격을 통해 전송하는 역할을 수행한다. 이를 통하여 보안관제에 반드시 필요한 속성들만 전송함으로서 전송 효율성을 높일수 있으며, 이러한 연동규격을 자유롭게 변경함으로써 최신 보안위협을 효과적으로 분석할수 있다.

3.2.2 제안하는 보안정보 관리 시스템

본 논문에서 제안하는 보안정보 수집 시스템은 크게 두 가지로 구성된다. 먼저 연동기관에 설치되어 보안정보를 수집하여 교육사이버안전센터로 전송하는 보안정보 전송 시스템과 수집된 데이터의 검증을 수행하는 보안정보 수집시스템으로 구성된다. 이 두 시스템을 합쳐서 보안정보 관리 시스템 이라한다. 각 연동기관에 구축된 보안정보 전송 시스템은 단위 보안인프라의 보안정보 데이터의 속성들을 연동규격에 맞게 일반화 하여 전송 시스템으로 수집하고 이를 직접 전송(이벤트) 하거나 또는 DB에 1차 저장하여 필요한 통계정보를 생성 한 후 통계정보를 전송 한다. 이러한 데이터를 교육사이버안전센터의 보안정보 수집 시스템이 암호화 통신을 통하여 안전하게 수집하며 데이터검증을 통하여 보안정보에 대한 신뢰도를 높이고 상관분석이 용이한 형태로 데이터를 분석시스템에 이관하게



[그림 2] 보안정보 수집 구성도

된다. [그림2]는 이러한 보안정보의 수집 경로를 보여주고 있다.

국내 교육기관은 보안정보관리시스템이라는 수집체계를 통하여 각 단위 CERT 및 연동기관의 정보를 수집하고 있다. 이렇게 수집된 데이터들을 활용하여 교육사이버안전센터에서 24시간 보안관제를 통하여 침해사고 여부를 판단하고 대응을 하고 있다.

4. 결론 및 향후 발전방향

현재 본 연구를 통해 개발된 보안정보 관리 시스템을 통하여 시·도교육청, 초·중·고등학교 및 직속기관을 포함하는 11,000여개의 교육기관이 교육사이버안전센터에 연동되어 있으며, 일평균 약5천만건의 보안정보 수집·분석·대응 업무를 수행하고 있다. 불과 2,3년 전만해도 교육기관은 해커들의 놀이터라는 오명을 많이 들어야 했지만 현재는 체계적인 보안정보 수집체계와 보안관제 업무를 통하여 침해사고를 효과적으로 줄여나가고 있으며, 교육사이버안전센터는 이러한 교육기관 정보보호 활동에 중추적인 역할을 수행하고 있다. 또한 빠르게 변화하는 정보보호 트렌드에 대응하기 위해 수집체계에 대한 지속적인 문제점 도출 및 개선을 통해 보안정보 수집체계 고도화를 병행하고 있다.

향후에는 보안관제 과정에서 탐지되지 않는 신종사이버공격에 효과적으로 대응하기 위하여 새로운 유형의 사이버공격을 탐지, 차단할 수 있는 보안관제 기술의 지속적인 연구·개발이 필요하며, 타 보안관제센터들과 연계 및 정보공유를 통하여 이번 7.7 DDoS 사태처럼 국가 전산망을 위협하는 공격에 신속하게 공동 대응하는 사이버 공조체계를 강화해야 할 것이다.

참 고 문 헌

[1] 김영진, 이수연, 권헌영, 임종인, “국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구” 2009. 2 정보보호학회논문지

[2] R. Bejtlich, Tao of Network Security Monitoring, the beyond Intrusion Detection: What is Network Security Monitoring, Addison Wesley Professional, pp. 40-41. July 2004.

[3] 2009 국가정보보호 백서 2009. 4 국가정보원

[4] 2008 국가정보화백서 한국정보사회진흥원