빅데이터 시대의 지능형 보안시스템에 관한 연구

김지현* · 이동훈*

* 고려대학교 정보보호대학원

The survey on Intelligent Security System in the age of Big Data

Ji Hyun Kim* · Dong-hoon Lee

*Graduate School of Information Security,Korea University

E-mail : mmlpl@korea.ac.kr

요 약

최근 IT분야의 화두 중 하나가 빅데이터이다. 과거의 보안이 경계지역에서의 방어였다면 현재에는 그 경계가 확장되어 점점 파트너사, 고객사, 원격지 직원까지 위협에 노출되었다. 따라서 전통적으로 경계지역을 방어하기 위해 사용했던 보안툴들이 이제는 유효성이 없어졌다. 갈수록 지능화, 고도화 되고 있는 보안이슈와 클라우드 시대에는 이에 걸맞는 지능형 보안시스템의 구축이 필요하고 이를 위해서 빅데이터가 최상의 역할을 할 것이다. 본 논문은 빅데이터 관련 기술을 고찰한 후 빅데이터를 활용한 지능형 보안시스템에 대하여 논의해 보겠다.

ABSTRACT

Recently one of the hot topics of IT field is big data.The security's meaning changed a lot, so security tools which were used to protect the limit area traditionally,now don't have any effectiveness. In the age of Cloud Computing, big data will do the best work. This paper discusses the technology related to big data and the intelligent security system utilizing big data.

키워드

지능형 보안시스템, 빅데이터, 빅데이터 분석기술, APT위협, BYOD위협

Ⅰ. 서 론

최근 IT분야의 화두 중 하나가 빅데이터이다[1]빅데이터는 '현재 시스템으로 처리 가능한 범위를 넘어서는 데이터'로 정의된다.[2] IT융합, 소셜미디어,서비스 산업 고도화,기업들의 고객 데이터 수집활동멀티미디어 콘텐츠의 폭발적 증가와 스마트폰 보급SNS활성화, 사무통신망의 저변확대로 데이터량은 그 종류와 수 또한 급격히 증가하고 있는 추세이다. 따라서 모든 기업이 보유한 빅데이터가 '거대한 가치추출이 가능할 만큼충분한 규모에 도달해 누가 먼저 그 가치를 추출해 내느냐가 향후 기업의 성패를 가늠할 상황에 직면하고 있다. 이에 대하여 갈 수록 지능화,고도화되고 있는 보안위협에 대응하는 지능형 보안 시스템 구축을 위해서는 빅데이터 분석이 필요하다는 것이 현재 보안 분야의 이슈가 되고 있다.아트 코비엘로 EMC RSA사장은 2012년 3월 8일 "현재의 시대에서 완벽한 보안은 없다. 과거의 기술과 사고의 연장선상에서 대응해서는 안되며 보다 창의적인 보안 대응방법이 필요하다"며 빅데이터가 새로운 보안모델을 완성하기 위한 새로운 모델로 부상하고 있다고 주장했다

Ⅱ. 빅데이터 관련기술 고찰

빅데이터를 데이터 용량에 따른 분류가 아닌 기존 데이터베이스 처리 방식으로 해결할 수 없는 데이터의 집합으로 정의하고 이를 처리할 수 있는 기술이나 역량을 보유한 국가가 미래의 경쟁력을 갖게 될 것이다.

* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정"지원 사업의 연구결과 지원사업의 연구결과로 수행되었음

1. 빅데이터 분석기술

1.1. 텍스트 마이닝(Text Mining)

텍스트 마이닝은 비/반정형 텍스트 데이터에서 자연어 처리 기술에 기반하여 유용한 정보를 추출가공하는 것을 목적으로 하는 기술이다 텍스트 마이닝 기술을 통해 방대한 텍스트 뭉치에서 의미 있는 정보를 추출해 내고, 다른 정보와의 연계성을 파악하며, 텍스트가 가진 카테고리를 찾아내거나 단순한 정보 검색 그 이상의 결과를 얻어낼 수 있다 컴퓨터가 인간이 사용하는 언어(자연어)를 분석하고 그 안에 숨겨진 정보를 발굴해 내기 위해 대용량 언어자원과 통계적, 규칙적 알고리즘이 사용되고 있다 주요 응용분야로 문서 분류, 문서 군집, 정보 추출, 문서 요약 등이 있다.

1.2. 평판분석

최근 새로운 여론분석기술로 각광받고 있는 오피니언 마이닝은 웹사이트와 소셜미디어에 나타난 여론과 의견을 분석하여 유용한 정보로 재가공하는 기술을 말한다. 오피니언 마이닝 기술을 활용하면 네티즌들이 각각의 사건에 대하여 이야기하는 댓글이나 포스팅 등을 긍정 또는 부정으로 분류하여 더 객관적이고 정확하게 평판을 파악할 수 있다.오피니언 마이닝은 특정 서비스 및 상품에 대한 시장규모 예측, 소비자의 반응 등에 활용되고 있다. 정확한 오피니언 마이닝을 위해서는 전문가에 의한 선호도를 나타내는 표현, 단어 자원의 축적이 필요하다.

1.3. 소셜 네트워크 분석

소셜 네트워크 분석은 간단한 소셜 분석으로 나타내며, 수학의 그래프 이론에 뿌리를 두고 있다. 소셜 네트워크 연결구조 및 연결강도 등을 바탕으로 사용자의 명성 및 영향력을 측정하여, 소셜 네트워크 상에서 허브 역할을 하는 사용자를 찾는데 주로 활용된다. 이렇게 소셜 네트워크 상에서 영향력이 있는 사용자를 인플루언서(Influencer)라고 부르는데, 인플루언서 모니터링 및 관리는 마케팅 관점에서 중요하다고 할 수 있다.

1.4. 클러스터 분석

클러스터 분석은 비슷한 특성을 가진 개체를 합쳐가면서 최종적으로 유사 특성의 그룹을 발굴하는데 사용된다. 예를 들어 트위터 상에서 주로 사진/카메라에 대해 이야기하는 사용자그룹이 있을 수 있고, 자동차에 대해 관심 있는 사용자 그룹이 있을 수 있다. 이러한 관심사나 취미에 따른 사용자 그룹을 군집분석을 통해 분류할 수 있다.

III. 보안위협의 진화와 위협대응의 변화

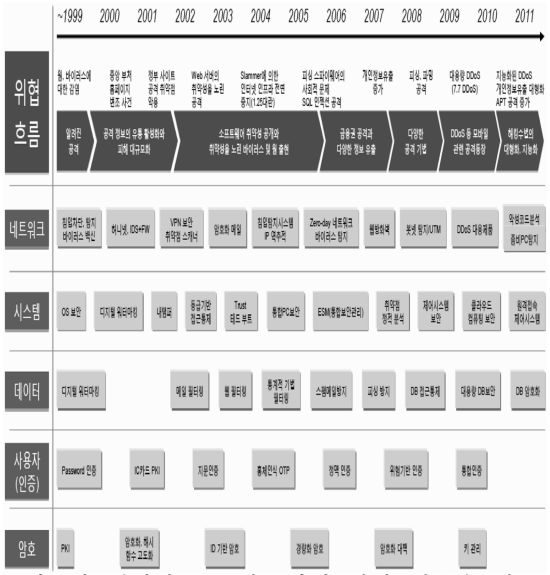
지난 10년간 위협의 진화와 대응기술을 요약하면 그림 2와 같이 구분할 수 있다. 사이버 위협은 알려진 공격 위주의 웜 바이러스에서 시작하며 웹 서버의 취약성 등을 이용한 공격 으로 진화한다. 그리고 어플리케이션의 취약성을 공격하고 피싱, SQL인젝션 공격이 발생하였고,지능화된 DDOS공격과 내부정보 유출을 노리는 APT공격으로 진화하였다. 공격의도는 실력과시에서 시작하여 금전적 이득과 핵티비즘으로 변형되어 정부기관과 사회기반 시설을 대상으로 변화하였다. 트랜드마이크로가 발표한 2011년 1분기 보안위협 보고서에 의하면 APT위협과 모바일 기기에 대한 사이버 범죄가 증가할 것으로 예상되었다. 이에 대표적 위협인 APT위협과 BYOD위협에 대하여 정리하였다.

(1)APT위협

지능형 지속위협은 단발성 공격이 아니며 공격 대상 네트워크에 침투하여 목적이 달성될 때까지 지속적으로 공격하는 고도화된 보안위협을 의미한다.[3] 이와 같이 APT공격은 특수목적을 가진 조직이 하나의 표적에 대해 다양한 IT기술을 이용하여 지속적으로 정보를 수집하고 취약점을 파악하여 이를 바탕으로 피해를 끼치는 공격을 의미한다.[4] APT위협은 악성코드, 취약점, 해킹 등의 IT기술에 의해 발생하는 위협으로 자동화된 툴이나 단순스캐닝 기술에만 의존하지 않고 사람이 직접 표적을 분석하고 이를 바탕으로 다양한 공격을 시도하는 사회공학적 기법을 모두 포함한다. 한 예를 들면 2011년 쉘, 엑슨모빌, BP, 마라톤오일, 코노코 필립스, 베이커 휴즈 등 미국의 글로벌 기업 5곳이 해킹을 당하는 일명 '나이트 드래곤 사건'이 발생하였다. 나이트 드래곤 사건에서 해커들은 사회공학 기법, 윈도 취약점, Active Directory, 원격관리도구(RATs)등의 기법을 사용하여 공격을 시도하였으며,그 과정은 다음과 같다.

-취약점이 존재하는 웹서버에 SQL인젝션 공격으로 악성파일을 업로드한다

-Spear-Phishing을 통해 접속을 위한 계정정보 획득, 악성파일에 대한 다운로드 및 감염을 시도한다



-획득한 계정정보로 시스템에 대한 접속을 시도하며, 시스템 내부의 사용자들의 계정정보도 추가적으로 수집한다.

-위의 단계를 거쳐 접속한 시스템을 공격자가 원하는 서버로 연결할 수 있도록 시도한다.

-수집한 계정정보 등을 사용하여 여러 중요정보에 대한 탈취를 시도한다.[4]

(2)BYOD위협

BYOD(Bring Your Own Device)는 개인 소유의 IT 단말기를 회사 업무에 활용하는 현상을 의미한다.[5] BYOD는 메인 PC를 주단말기로 유지하면서 개인의 태블릿PC,스마트폰을 보조적 수단으로 업무에 활용하겠다는 개념으로, 단순한 비용절감의 차원을 넘어 업무 프로세스를 변화시키고 새로운 수익창출의 수단으로까지 작용하고 있다.이러한 현상은 하드웨어와 소프트웨어의 발전이 더욱 가속시키고 있다. BYOD를 이용한 업무생산성, 편의성과 같은 긍정적인 요소 외에 잠재적인 보안위협이 존재한다.대표적 보안위협에는 기업의 IT통제권 상실,단말기의 취약점 및 악성코드로 인한 기업 내부정보 유출위협, 악성코드에 감염된 개인용 기기의 내부 접속으로 인한 기업 IT자산 위협, 단말기 도난 또는 분실로 인한 데이터 유출, 보안의식이 낮은 직원에 의한 계정유출 등이 있다. [2]

BYOD환경의 변화는 다양한 클라이언트 환경에 제약을 받지 않고 언제 어디서나 Email확인 및 회사 업무가 가능하게 되어 다량의 트래픽을 유발한다.또한 여러 환경에서 웹과 어플리케이션 취역점에 노출이 된다. 단위보안시스템들도 이에 대응하기 위하여 개발되고 다양한 보안시스템들이 구축되고 있다.이로 인하여 단위보안시스템에서 탐지하는 보안로그의 양도 급격히 증가한다. 오히려 보안데이터의 증가는 보안위협이 은닉하기 용이한 환경을 제공한다.

Ⅳ. 빅데이터를 활용한 지능형 보안 시스템

APT위협과 같이 보안위협이 점점 지능화되고 고도화되면서,기존 단위시스템만으로는 지능화된 보안위협을 탐지하고 방어하는데 한계가 있다.다량의 트래픽을 분석하고 수일 또는 수개월 이상의 장기간 동안 지속되는 공격을 탐지해야 하는 빅 보안 데이터 시대에 지능화된 분석 요구에 직면하게 되었다.

최근까지만 해도 IT보안은 안전한 인터넷 세상을 만드는데 성공적인 역할을 해왔다.하지만 근래 들어 고객들이 디지털 세계의 자원을 활용하는데 익숙해진 만큼,신종 사이버 범죄자, 핵티비스트(Hactivist), 국가 단위의 범죄조직 역시 디지털 세계의 취약점을 이용하는데 능숙해졌다.침입자들은 업계가 고도로 연결된 인프라의 개방성에 적절히 대응하지 못하고 있는 점, 위협에 대한 자각과 대응속도가 느린 점을 공격의 회로 삼아 이전보다 훨씬 향상된 속도와 민첩성, 교활함으로 접근하고 있다.

이 논문에서는 빅데이터 시대에 보안업계가 나아가야 할 방향으로 다음과 같은 4가지 방향을 제시하겠다. 첫째, 보안에 대한 기존의 사고방식을 바꿀 것.둘째, 리스크와 문맥 기반의 민첩한 지능형 보안 시스템으로 변화해 나갈 것.'지능형 보안시스템'이란 컴퓨팅 환경에서 데이터 양이 폭증하고 있는 빅데이터 시대에서의 방대한 양의 정보를 면밀히 조사하고 미세한 공격 신호를 모두 감지할 수 있는 보안시스템을 의미한다.이는 이전의 방어 위주의 대응과 개별 사건을 추적하는 보안방식과 차별적인 개념이다.아트 코비엘로 EMC RSA 정보보안사업부문 사장은 지능형 보안시스템이 3가지 핵심 아이템을 기반으로 구성되어야 하며,이를 보다 효과적으로 구현하기 위해서 빅데이터 이슈가 발생하게 된다고 하였다. 아트 코비엘로 사장이 제안한 지능형 보안시스템의 핵심아이템은 ①리스크 기반이어야 한다법칙에 입각해 보안에 대한 캐퍼시티는 지속적으로 늘어나고 있고 속도도 빨라지고 있다. 리스크 관리는 리스크에 대한 철저한 이해에서 시작되어 내부에서 외부, 외부에서 내부 등 다양한 방향에서 이뤄져야 한다. ②기민한 대응이 필요하다③문맥 또는 상황을 인지할 수 있어야 한다.

셋째, 협업하고 정보를 공유할 것넷째, 지능형 공격에 맞서기 위해 차세대 보안 전문가를 양성할 것이다.

Ⅴ. 결 론

과거의 보안이 경계지역에서의 방어였다면 현재는 그 경계가 확장되어 점점 파트너사, 고객사, 원격지 직원까지 노출되었다. 그래서 전통적으로 경계지역을 방어하기 위해 사용했던 보안툴들이 이제는 유효성이 없어졌다는 것이다. 공격자들의 기술도 정교해지고 지적재산권에 대한 공격도 늘어나고 조직화되고 해커비스트들도 활동하게 된다. 공격을 감행하는 규모나 결과가 심각해지고 있다. 갈 수록 지능화, 고도화되고 있는 보안 이슈와 클라우드 시대에 걸맞은 지능형 보안시스템의 구축을 위해서는 빅데이터가 최상의 역할을 할 것이다. 최상의 보안을 구축할 수 있는 스토리지 양과 컴퓨팅 파워를 확보한 현재의 시점에서 보다 구체적인 액션을 취할 수 있는 유의미한 정보를 제공하기 위해서는 빅데이터가 중요한 요소로 자리매김하게 되었기 때문이다.

참고문헌

[1]강만모, 김상락, 박상무, “빅데이터의 분석과 활용”, 정보과학회지, 2012.06

[2]김정숙, “빅데이터 활용과 관련기술 고찰” 한국컨텐츠학회지, 2012.03

[3]최대수, 김용민,“빅데이터와 통합보안2.0”정보과학회지,2012.06

[4]남기효, 김윤홍, 권환우, 최신 정보보호기술 동향:APT 및 그 대응, 정보통신산업진흥원, IT기획시리즈

[5]김재필, “스마트 오피스의 새로운 트렌드 BYOD”, KT경제경영연구소,2011.11