기업환경을 위한 보안 요구사항 연구

박민우*, 김남욱*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:mwpark@imtl.skku.ac.kr

A Study on Security Requirements for Enterprise Environments

Min-Woo Park*, Nam-Uk Kim*, Tai-Myoung Chung**
*Dept of Electrical and Computer Engineering, Sungkyunkwan Univ.
**School of Information Communication Engineering,
Sungkyunkwan University

요 약

최근 발생한 사이버 범죄 경위를 살펴보면 범죄 목적이 분명하고 이를 달성하기 위한 수단이 치밀하여 비교적 높은 보안 수준을 가진 기업이라도 사이버 범죄 행위에 노출되어 피해를 입는 사례가 빈번히 발생하고 있다. 특히 기업환경에서 업무 효율을 높이기 위해 전자결재나 스마트워크 등을 도입하여 업무의 많은 부분이 컴퓨팅 장치에 의존적이 되면서 사이버 범죄에 대한 위협이 늘어나고 있다. 본 논문에서는 악성코드 또는 이를 이용한 악성행위로부터 기업 환경을 보호하기 위한 보안 시스템의 이상적인 요구사항에 대해 제안한다.

1. 서론

제어 시스템을 마비시키며, 오작동을 유발하기 위한 목적으로 물리적으로 단절되어 있는 네트워크에 침입하여 악성행위를 수행하는 악성코드가 출현하면서 전 세계적으로 컴퓨터 보안에 대한 관심이 증가하고 있다[1]. 최근 발생한 사이버 범죄들을 살펴보면 공격행위가 분명한 목적을 가지며, 목적을 달성하기 위해 시스템 취약점과 이를 사용하는 사용자의 습관, 관심사, 개인 장치 등을 이용한 사회공학적 공격을 수반하면서 사이버 범죄 행위가 보다 정교해지고 있다[2]. 사실상 알려진 공격들에 대해 탐지 또는 방어 할 수 있는 기존의 보안 시스템을 가지고는 최근 발생하는 사이버 범죄로부터 기업환경을 보호하는 것은 한계가 존재한다. 특히 최근에는 정치적 이념을 위해서 이루어지거나, 단순한 경제적 이득을 위한 행위보다는 특정 기업이나 기관을 무력화할 목적으로 이루기 위한 사이버 범죄들이 일어나고 있어 사이버 범죄에 노출될 경우 그 피해가 막대하다. 이에 따라 사이버 공격으로부터 기업환경을 보호할 수 있는 새로운 유형의 보안 시스템의 개발이 필요해졌다.

본 논문에서는 이러한 표적공격(target attack)으로부터 기업환경을 보호할 수 있는 새로운 유형의 보안 시스템을 제안한다. 본 시스템은 강제적인 보안 정책을 갖고 시스템으로 유입되는 위험한 트래픽을 통제하여 내부 시스템을 보호하는 보안 시스템이다. 본 논문에서는 제안하는 시스템이 기업환경을 보호하기 위해 필요한 필수적인 보안 요구사항을 제안한다.

2. 현 보안 시스템의 한계

기존의 공격패턴을 이용한 악성코드 탐지 또는 침입탐지 기술은 알려진 공격을 탐지하는 대에 높은 성능을 보인다. 과거에는 사이버 범죄의 빈도가 낮고, 뚜렷한 목적 없이 불특정 다수의 사용자들을 대상으로 공격이 이루어졌다. 그 결과 새로운 공격 기술에 대한 빠른 발견과 분석 후, 이를 신속히 보안 시스템에 적용하는 것이 보안 수준을 높이는 길이였다. 하지만 별다른 지식이 없이 손쉽게 악성코드를 제작할 수 있는 공격툴(attack tool)이 늘어나고 사이버 범죄에 관련된 커뮤니티가 형성되면서 컴퓨터 사용자가 손쉽게 악성코드를 생성·배포할 수 있게 되었다. 그 결과 하루에도 수 만개의 악성코드가 제작되어 인터넷으로 쏟아져 나오게 되었다[3]. 새로운 형태의 악성코드의 양적 증가는 알려진 공격패턴에 의존적인 기존의 보안 시스템의 성능을 떨어트리고 있다. 이와 같은 시대적 변화에 따라 기업환경을 보호하고 있는 다양한 보안 시스템들은 다음과 같은 공통적인 한계점을 갖게 되었다.

2.1 보안 홀(hole)의 증가

인터넷을 이용하는 사용자 수의 증가, 인터넷에 접근 가능한 장치의 증가, 인터넷을 통해 제공되는 서비스의 증가는 보안 홀의 증가로 이어진다. 최근에는 미취학아동이 타블렛PC나 스마트폰을 이용해 인터넷에 접근하기도 하며, 실버 세대가 자신의 홈페이지를 꾸미거나 인터넷 커뮤니티 활동에 참가하는 등 인터넷 사용자가 다양한 연령대로 분포하게 되었다. 인터넷을 이용하는 사용자 수가 증가하면서 보안 지식이 부족한 사용자 수 또한 증가하였다.

그 결과 악성코드의 전파가 보다 가속화되고 감염된 장치의 증가로 인해 봇넷(bot-net)의 규모가 커지는 등 악성코드로 인한 공격행위가 보다 치명적이게 되었다. 인터넷에 접근 가능한 장치의 증가는 새로운 보안 취약점으로 이용되거나 보안 취약점을 지닌 낙후된 운영체제나 응용프로그램을 사용하는 시스템 수의 증가로 이어진다. 그 결과 인터넷 접근 가능한 장치의 증가는 인터넷 사용자의 증가와 유사한 현상을 유발한다.

인터넷을 통해 제공되는 서비스의 증가 또는 응용 프로그램의 증가는 시스템을 위협하는 보안 취약점의 수를 증가시켜 보안 홀을 만든다. 특정 응용 프로그램이 보안 취약점이 존재하는 경우, 이를 악용되기 이전에 개발자 혹은 보안 관련 회사에서 발견하여 보안 취약점을 수정하더라도 여전히 패치에 능동적으로 응하지 않은 사용자의 시스템은 위협에 놓인다. 또한 최근에는 발견된 보안 취약점의 패치가 이루어지기 이전에 공격에 악용되는 제로데이 공격이 이루어지면서 시스템의 안전을 위협하고 있다.

인터넷의 발달에 따라 보안 홀이 늘어나고 있다. 이러한 상황에서 알려진 패턴을 이용하여 공격을 탐지하는 기존의 보안 시스템은 한계를 갖는다.

2.2 암호화된 트래픽의 증가

최근 컴퓨터 사용자들의 보안 인식이 성장하면서 인터넷을 통해 제공되는 많은 서비스들이 보안 기능을 갖게 되었다. HTTPS를 이용한 로그인 과정, 메신저의 인스턴트 메시지의 암호화, 암호화되어 첨부된 파일, VPN 서비스 등 사용자 인증이 필요하거나 프라이버시 침해가 우려되는 서비스에 암호화 기능이 사용되고 있다. 이러한 트래픽 암호화는 개개인의 정보보호를 위해 효과적인 기능이지만, 기업환경에서는 오히려 역기능으로 작용한다. 기업환경에서는 내부 네트워크로 유입되는 트래픽들에 대해 유입 단계에서 일차적으로 검사하여 악성코드의 내부 네트워크 침입을 사전에 차단하는 것이 일반적이다. 하지만 암호화된 트래픽의 경우 이를 복호화하기 위해서는 암호화에 사용된 키(key)와 알고리즘이 필요하기 때문에 내부 네트워크로 유입되는 암호화 트래픽에 대해 검사하는 것이 불가능하다. 즉, 암호화된 트래픽은 내부 네트워크 유입 시 정해진 보안 정책에 예외사항으로 적용되거나 악성코드 검사 과정을 거치지 않고 내부 네트워크로 들어올 수 있다. 그 결과 치명적인 악성코드의 전파 경로로 작용하여 기업환경을 위협하는 요소로 작용할 수 있다.

2.3 공격패턴의 증가

통계에 따르면 매일 4 만개가 넘는 악성코드가 만들어져 인터넷으로 전파되고 있다[3]. 알려진 악성코드에 대한 패턴을 이용하여 악성코드를 탐지하는 보안 시스템의 경우 대조해야하는 공격패턴이 증가할수록 보안 시스템의 탐지 효율이 떨어지며, 공격패턴을 저장하기 위한 공간적인 효율도 떨어진다.

2.4 사회공학적 공격

2010년에 발견된 악성코드 스턱스넷(stuxnet)은 인터넷으로부터 물리적으로 단절된 네트워크인 원격감시제어(SCADA, Supervisory Control and Data Acquisition)에 침투하여 제어 시스템의 오작동을 유발하도록 설계된 악성코드이다. 물리적으로 단절된 네트워크에 해당 악성코드를 전파될 수 있었던 것은 해당 네트워크에 접근 권한을 가진 사용자들에 대해 사전에 파악하고 그의 패턴을 분석하여 해당 사용자가 악성코드를 시스템으로 전달할 수 있도록 계획하였기 때문이다. 이처럼 사이버 공격이 분명한 목적성을 갖게 되면서 이를 달성하기 위한 사회공학적 공격이 이루어지고 있다. 아무리 튼튼하게 설계되어진 보안 시스템이라 할지라도 내부 사용자에 의해 검사과정을 우회하여 내부 네트워크로 전파될 경우 해당 악성코드에 의해 내부 네트워크는 속수무책으로 공격받게 된다.

2.5 새로운 서비스의 등장

새로운 서비스가 등장할 경우 해당 매체가 안전한지 여부를 판단하기 위해서는 많은 시간이 소요될 뿐만 아니라 판단 결과를 완전히 신뢰할 수 있는 것도 아니다. 예를 들어 스마트폰을 이용한 스마트워크의 경우 업무효율 증대 등을 이유로 최근 각광받고 있다. 하지만 스마트워크를 위해 개인의 단말에 저장된 주요한 문서들이 스마트폰의 백업과정이나 자동동기화를 통해 외부로 유출되거나 변조될 위협이 존재한다. 이처럼 새로운 서비스의 등장은 악성코드의 전파 또는 정보 유출의 새로운 경로로 작용할 위험이 존재한다. 기존의 서비스들을 대상으로 완벽한 보안 정책이 구성되어 있다고 할지라도 새로운 서비스의 등장으로 인해 기업환경이 취약해질 수 있는 것이다.

2.6 통신 우회 경로의 존재

최근 이동통신의 품질이 크게 증가하면서 이동통신을 이용한 테더링 서비스를 사용하는 것이 일반적이게 되었다. 와이브로와 와이-파이(wi-fi)를 테더링 해주는 장치 또한 일반화되면서 이를 이용한 인터넷 접속도 빈번히 이루어지고 있다. 내부 네트워크에 존재하는 시스템이 이동통신을 통해 인터넷에 연결될 경우 내부 네트워크로 트래픽이 유입되는 새로운 우회 경로가 탄생하게 된다. 이 경우 악성코드의 유입이나 공격자의 침입 여부를 탐지하기가 어려워져 결과적으로 내부 네트워크를 위협하는 요소로 작용할 수 있다.

3. 기업환경을 위한 보안 요구사항

기업을 대상으로 한 사이버 공격이 성공적으로 수행될 경우 기업은 천문학적인 경제 피해를 입게 되며, 소비자들의 신뢰도 상당부분 잃게 된다. 특히 사이버 공격으로 인해 유출되는 정보가 소비자들의 주요 개인정보나, 기업의 주요 기밀정보일 경우 그에 따른 파급효과는 굉장하다. 실

제로 일본의 유명 전자회사 소니(sony)의 PSN이 해킹당하면서 시스템에 등록된 약 7천 700만명의 사용자의 개인정보가 유출되는 사건이 있었다. 이 사건을 돌이켜 보면 기업의 규모가 크면 클수록 사이버 공격에 따른 피해 규모 또한 증가하며, 따라서 기업은 사이버 공격들로부터 안전하게 자신들의 네트워크를 지킬 수 있는 강력한 보안 시스템이 필요하다. 하지만 앞서 2 장에서 살펴본 것처럼 현 보안 시스템은 다양한 한계점들을 갖는다. 본 논문에서는 이러한 한계점을 극복할 수 있는 보안 시스템 개발하기 위한 주요한 보안 요구사항을 제안한다.

기업환경의 보안 시스템은 다음과 같은 요구사항을 충족할 수 있어야 한다.

<표 1> 보안 요구사항

신뢰할 수 있는 데이터만 사용자에게 제공
신뢰할 수 있는 데이터 판단
업무 실시간성 확보 : 검역 제외되는 트래픽 규정 : 검역 제외되는 파일 규정
내부 시스템 감시
내부 시스템 격리

3.1 신뢰할 수 있는 데이터만 사용자에게 제공

기업의 보안을 위해서는 데이터의 신뢰 여부의 판단을 최종 사용자에게 맡기기보다 기업의 보안 관련 전문가가 직접 판단할 수 있도록 해야 한다. 사회공학적인 분석을 통해 악성코드를 전파할 수 있는 것은 사용자가 잘못된 대상을 신뢰하고 있거나, 신뢰하지는 않지만 여러 가지 이유로 이러한 대상을 통해 데이터를 송·수신 하는 것에서 발생한다. 예를 들어 웹을 통해 자신의 친구에게서 받은 동영상이나 심지어 특정 소프트웨어의 자동 업데이트를 통해 자동적으로 다운로드되는 데이터 등도 충분히 악성코드를 포함하고 있을 수 있으나 대부분의 사용자들은 이러한 부분에 대해서 무작정 수용하고 있다. 따라서 특정 데이터가 신뢰할 수 있는 데이터인지 판단하는 것은 사용자 개인에게 맡기기보다 체계적인 검사 과정을 거친 이후 보안 전문가가 판단할 수 있도록 기업 환경이 구성되어야 한다.

3.2 신뢰할 수 있는 데이터 판단

3.1 에서 기술한 것처럼 데이터의 신뢰 여부는 기업의 보안 시스템 혹은 보안 전문가가 결정할 사항이다. 하지만 하루에도 엄청난 량의 트래픽이 발생하는 기업환경에서 모든 트래픽을 사람이 분석하는 것은 불가능하다. 따라서 특정 데이터의 안전성에 대해 판단할 수 있는 시스템이 필요하다. 이러한 시스템은 다음과 같은 사항을 반드시 만족해야 한다. 먼저, 모든 트래픽에 대해 안전성 여부를 판단할 수 있어야한다. 안전성 여부를 판단하는 단계를 우회할 수 있는 경로가 존재하는 경우 해당 경로가 보안 시스템의 안전성을 위협하는 취약점으로 작용할 수 있다. 하지만 실시간으로 발생하는 모든 데이터들에 대해서 오랜 시간 분석을 수행하는 것은 불가능하다. 따라서 트래픽이 실시간으로 전달되어야 하는지 여부를 판단할 수 있어야 한다. 이는 기업에서 다루는 업무의 특성에 따라 달라질 수 있으므로 기업에 맞도록 보안 전문가가 설정할 수 있어야 한다. 신뢰할 수 있는 데이터 여부를 판단하기 위해서는 패턴매칭에 기반을 둔 탐지 과정뿐만 아니라 행위에 기반을 둔 탐지 과정 또한 필요하다. 데이터의 정적분석 만으로는 패턴이 알려진 공격에 대해서만 검사할 수 있기 때문이다. 따라서 검사하고자 하는 트래픽의 목적지 시스템을 묘사할 수 있는 에뮬레이팅 환경 구성을 통해 행위를 기반으로한 악성코드 탐지 환경이 구축되어야 한다.

3.3 업무 실시간성 확보

기업의 업무는 실시간성이 매우 중요하다. 정보의 빠른 전달은 때로 사업의 성공과 실패를 좌우하기도 한다. 하지만 강력한 보안 시스템은 그만큼 업무 효율을 떨어트릴 수 밖에 없다. 따라서 이에 대한 충분한 대안이 필요하다. 업무 실시간성을 확보하기 위해서는 복잡한 검사 과정이 필요한 트래픽과 그렇지 않은 트래픽에 대한 구분이 분명하게 이루어져야 한다. 또한, 검사 과정을 받아야 하는 데이터의 경우에도 사전에 약속된 인증 체계를 통해 인증키를 가진 데이터에 대해서는 인증키 확인만을 통해 검사 과정을 무시할 수 있도록 하는 기능이 필요하다.

3.4 내부 시스템 감시

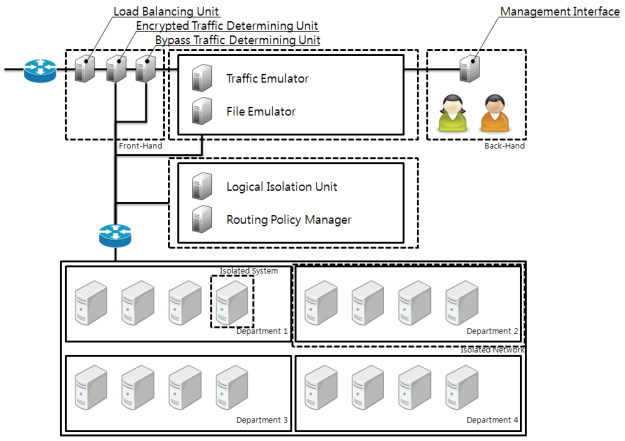
행위 기반을 통한 검사 과정으로도 데이터의 신뢰 여부를 완전히 판단하지 못하는 경우가 있다. 특정 악성코드는 안정적으로 악성행위를 수행하기 위해 특정한 상황에서만 악성행위를 수행하도록 설계된다. 이 경우 행위 기반 악성코드 검사를 수행한다 할지라도 특정 상황을 충족하지 못해 악성행위를 이끌어내지 못하고 검사를 끝마치는 경우가 발생할 수 있다. 이에 대한 대안으로 기업환경의 보안 시스템은 수시로 내부 시스템들을 감시할 필요가 있다.

3.5 내부 시스템 격리

내부 네트워크에 존재하는 시스템이 우회 경로를 통해 인터넷에 접속하는 경우 해당 시스템을 내부 네트워크에서 격리시킬 필요가 있다. 우회 경로를 통해 인터넷에 접속하게 되는 경우 정당한 검사 과정을 거치지 않은 트래픽들이 내부 네트워크로 유입될 위험이 있으며, 그 결과 내부 네트워크에 악성코드가 전파될 수 있다. 이를 막기 위해서는 우회 경로를 통해 인터넷에 접속하는 시스템을 내부 네트워크에서 격리 시킨 후, 우회 경로를 통한 인터넷 접속이 종료된 이후 악성코드 감염 여부를 철저히 검사한 후 해당 시스템을 내부 네트워크에 연결한다.

4. 제안 시스템 구조

아래 (그림 1)은 기업환경을 보호하기 위한 보안 시스템의 제안 구조이다. 보안 시스템은 유입되는 트래픽들에 대해 다음과 같은 순서로 처리한다. 먼저, 유입되는 대량의 트래픽 처리를 위해 부하분산 장치를 거친다. 이 과정에서 암호화된 트래픽들은 검사할 수 있는 형태로 복호화하며, 정책에 따라 검사 대상이 아닌 트래픽은 복잡한 악성 코드 검사과정을 거치치 않고 내부 네트워크로 유입된다. 이후 검사 과정으로 전달된 트래픽들은 행위 기반의 트래픽 검사 및 파일 검사를 거친 뒤 이상이 없다고 판단된 경우에만 내부 네트워크로 전달된다. 이상이 있거나 판단이 부정확한 경우 반드시 보안 전문가에 의해 재검토되며 그 결과가 다시 다음 판단 기준에 적용될 수 있도록 피드백 된다. 이후 내부 시스템들은 이동통신을 이용한 인터넷 접근이나 USB와 같은 이동 저장장치 이용, 또는 불확실한 데이터를 수신하는 시스템에 대해 격리 조치를 취할 수 있으며 이를 감시하기 위한 장치가 존재하며, 수시로 내부 네트워크에 존재하는 시스템들을 감시한다.



(그림 1) 기업환경 보안 시스템

5. 결론

본 논문에서는 기업환경을 보호하기 위한 이상적인 보안 시스템의 보안 요구사항에 대해 제안하였다. 기업환경의 경우 단순히 알려진 공격들에 대해 능동적으로 대응하는 것이 아닌 알려지지 않은 각종 보안 위협으로부터 기업을 보호할 수 있는 수단이 필요하다. 따라서 기업환경의 내부 네트워크를 보호하기 위해서는 데이터의 신뢰 여부를 반드시 기업내 보안 전문가가 할 수 있어야 하며, 이를 위해 체계적인 판단 시스템이 필요하다. 이때 판단 시스템은 반드시 행위 기반의 악성코드 탐지가 가능해야 하며, 그 과정에서 탐지되지 않는 악성코드들의 추적을 위해 보안 시스템은 주기적으로 내부 시스템을 감시하며 필요에 따라 격리할 수 있어야한다.

향후 연구 내용으로는 이러한 보안 요구사항을 충족하는 보안 시스템 구축을 위해 먼저 행위 기반의 악성코드 탐지 기술의 연구 및 개발을 수행할 계획이다.

ACKNOWLEDGEMENT

본 논문은 중소기업청에서 지원하는 2011년도 산학연공동기술개발사업(No.000443010111)의 연구수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] “W32.Stuxnet Dossier”, Symantec Security Response
[2] ″2011 국가정보보호 백서“, 방송통신위원회
[3] 한국인터넷진흥원, 인터넷침해사고 동향 및 분석 월보, Dec. 2010.