

Publication: iNews24

Date: 16/11/2011

Subject: In Big Data Era, 'Automation' is Key to Next-Generation Security Solution

http://news.inews24.com/php/news_view.php?g_serial=618698&g_menu=020200

빅데이터 시대, 차세대 보안솔루션의 핵심은 '자동화'

전통적인 솔루션 아닌 차세대 보안 솔루션 필요

2011.11.16. 수 18:56 입력

[김관홍기자] 스마트 기기의 폭발적 증가와 클라우드 컴퓨팅의 확산, 빅데이터 시대의 도래로 전 세계 네트워크 및 정보통신기술(ICT) 업계는 보안에 무게 중심을 두고 있다.

16일 대구 푸켓에서 열린 넷이벤츠 2011에서도 많은 참석자들이 빅데이터 시대의 도래와 그에 따른 보안 위협, 대응 방안에 대해 소개하고 자동화를 비롯한 해법들을 제시했다.

이날 아시아 태평양 기자간담회에 참석한 IDC의 팀 밀론 연구원은 "엔터프라이즈 환경에 대한 사이버 공격이 화두가 되고 있다"며 "모바일 기기의 확산, 클라우드, 빅데이터가 전통적인 보안 개념을 위협하고 있다"고 지적했다.

IDC 자료에 따르면 아태지역 스마트폰 시장은 2012년 2억3천만 대 이상을 형성할 것으로 전망된다. 스마트 기기의 폭발적 증가에 따라 각 기업들은 몇개의 디바이스가 조직 네트워크에 접속하는지, 몇명의 유저가 데이터를 사용하는지 알기 힘들어졌다. 보안에 그만큼 취약해지는 것이다.



◇ IDC 팀 밀론 연구원 (사진=넷이벤츠)

IDC는 또한 전세계 엔터프라이즈 소프트웨어 중 80%가 클라우드를 겨냥해 개발되고 있다고 분석했다. 데이터의 분할도 폭발적으로 증가, 2011년 1.8테라바이트(TB) 가량의 엔터프라이즈 데이터가 2014년에는 7테라바이트까지 증가할 전망이다. 그만큼 보안에 대한 위협도 증가할 것으로 관측된다.

팀 밀론 연구원은 "더 많은 디바이스를 업무에 사용중인데 기업들은 엔터프라이즈 네트워크에 대해 잘 이해 못하고 있다"면서 "가장 큰 문제로 무선네트워크가 지적되고 있으며 와이어(Wire) 및 와이어리스(Wireless) 네트워크 보안 솔루션도 중요해지고 있다"고 말했다.

팔로알토네트웍스의 니르 주크 최고기술책임자(CTO)도 최근의 소니, 삼성 등의 대규모 해킹 사태가 제한된 타겟을 짧은 시간에 최종 사용자 공격하는 현대화된 해킹 수법을 사용한터라 기존의 보안 기술로는 막을 수 없다고 강조했다.

그가 설명한 보안 위협 5단계에 따르면 해커는 최종 사용자를 유인해서 각종 문서나 MP3 파일, 영화 파일 등을 열람하는데(일명 스피어 피싱) 유인 방식이 전통적인 이메일이나 웹사이트뿐 아니라 메신저, 페이스북, 각종 문서 등 다양한 애플리케이션 등 다양하다.

해커가 보안 파일은 최종 사용자가 확인하게 되면, 조그마한 코드가 사용자 PC에서 활성화된다. 여기서 생성된 보안의 취약점은 네트워크를 통해 인터넷으로 나가게 되고, 트로이목마 같은 악성 프로그램이 사용자 PC에 설치된다.

이 프로그램은 외부 공격자와 연결하는 채널도 활동하는데, 외부 공격자는 사용자 PC를 통제할 수 있게 된다. 이때부터 해커는 최종 사용자의 PC를 활용해 자신이 원하는 모든 것을 마음대로 할 수 있게 된다.



◇ 팔로알토네트웍스 니르 주크 최고기술책임자(CTO) (사진=넷이벤츠)

하지만 이같은 최선의 해킹에 침입방지시스템(IPS)이나 안티 바이러스(AV)는 효과적으로 대응하지 못한다. 각각의 모든 단계를 보호하고 방어해야 하지만 현재의 솔루션들은 한계가 있기 때문이다.

니르 주크 CTO는 "IPS 없거나 AV 없이는 해킹 사건이 일어난 이후 한참 후에 솔루션을 내놓는 다"며 "솔루션 제공 업체들이 모든 문서와 해킹 타겟을 다 점검할 수 없고 해킹 공격이 소수의 유저에게 짧은 시간동안 이뤄져 원인을 파악하고 대책을 내놓기까지 오랜 시간이 걸린다"고 설명했다.

그는 "사람이 모든 문서의 타겟을 분석하기에는 한계가 있으므로 IPS와 AV의 자동화가 필요하다"고 지적하고 그에 대한 해답으로 샌드박스를 제시했다.

이 방법을 이용하면 최종 사용자가 애플리케이션을 확인하기 전 단계에 샌드박스를 구축, 미리 시뮬레이션과 검사를 진행한 후 최종 사용자에게 제공할 수 있다.

그는 또한 악성 프로그램을 차단하고 그에 대한 보안 솔루션을 생성하는 것에 대해서도 자동화가 필요하다고 주장하고 자사의 "와일드파이어" 솔루션이 샌드박스과 자동화 기능을 제공한다"고 소개했다.

푸켓(대구) = 김관홍기자 kky1441@news24.com >>>가짜뉴스대포기