정보보호 관리자들이여, 좀 더 부지런해져라

▲ George Bakos (Northrop Grumman)

정보보호 담당자들은 하루가 다르게 변화해 가는 새로운 공격기법에 대응하기 위해 많은 시간과 노력을 투자하고 있다. 그러나 이런 고민은 국내 담당자들에게만 닥친 현실은 아닌 것 같다. 미국 Northrop Grumman의 정보분석가로 활동하고 있는 George Bakos를 통해 최근 등장하는 공격기법과 대응방법에 대한 해법을 요청했다. George Bakos는 Dartmouth College 연구소에서 웜 공격과 방어, 공격 모델링, 침입 탐지 등을 연구한 바 있으며, 현재는 Northrop Grumman에서 사내 데이터와 프로그램을 악의적인 공격으로부터 보호하는 업무를 맡고 있다.

정보보호뉴스 취재팀

최근 웹 애플리케이션 공격이 급증함에 따라 그에 대한 대책마련이 시급한 상황이다. 하지만 웹 애플리케이션 공격은 다양한 부분에서 공격이 가능하기 때문에 대응하기 어려운 점도 있다. IPS나 웹 방화벽과 같은 보안 솔루션 활용 이외의 대응방법이 있다면 소개해 달라.

대개 웹 애플리케이션 공격은 시스템 관리자나 개발자의 게으름에서 시작된다. 몇몇 특별하게 필요한 기능만을 허용하도록 하는 sysadmin 실행만으로도 대다수 공격을 방지할 수 있다. 또 웹 서버 모듈 및 패키지에서 불필요한 항목을 없애고, 취약점으로부터 웹 애플리케이션을 지속적으로 감시하는 등 관리자의 부지런함이 필요하다. 물론 이런 일련의 업무를 수행하기 위해서는 실력 있는 담당자가 필요하고, 때문에 기업은 비용을 감수하더라도 그들을 교육시켜야 한다.

기업의 시스템이나 네트워크가 외부 해킹에 노출됐다는 사실을 신속하게 알 수 있는 가장 효과적인 방법은 무엇인가.

복잡한 소프트웨어나 프로그램이 존재할수록 공격 가능성은 더욱 커지게 마련이다. 사고를 인지하지 위해서는 변칙 로그기록, 원인을 수 없는 성능저하, 외부로 나가는 네트워크 활동 등을 지속적으로 감시해야 하며, 이들 현상을 무조건 정상적이라고 간주하거나 또는 무시해서는 안 된다. 비록 정보보호 담당자가 모든 에러들을 찾아내 분석하는 것은 불가능할 지라도 사고 과정에 대한 기본적인 처리 절차는 기억해 둬야 하며 특히, 정상적일 때의 시스템 및 네트워크 구조를 머리 속에 그려놓을 필요가 있다. 그렇다면 훨씬 더 빠르게 사고를 인지할 수 있을 것이다. 그리고 한 가지 더 덧붙이자면, 대부분의 기업 정보보호 관리자들은 방화벽, IPS 등과 같은 보안장비들의 숫자가 IT 자산의 안전성과 비례한다고 생각하는 경향이 있는데 이는 잘못된 것이다.

운영체제와 여러 애플리케이션은 언제든 재설치할 수 있지만, 데이터는 그럴 수 없기 때문에 데이터 보호는

매우 중요하다고 생각한다. 효율적인 데이터 보호 방법을 알려 달라.

워터마킹(Watermarking), 보안 라벨링(Security Labeling), 네트워크 페이로드 패턴 매칭(Network Payload Pattern Matching)과 같은 정보보호 솔루션들은 데이터를 갈취하는 공격에 효과적으로 대응할 수 있다. 하지만 데이터의 기능을 저하시키기 위한 상당한 수의 공격이 발생할 수 있고, 또 이런 공격은 기업의 침입탐지 시스템에도 발견되지 않을 수 있다.
일반적으로 기업을 대상으로 한 시스템과 네트워크 공격은 두 가지 형태로 구분된다. 특정 목표 없이 IT 자산을 공격하는 것이 하나이고, 다른 하나는 기업이 갖고 있는 특정한 자료를 목표로 하는 공격이다. 첫 번째의 경우는 전통적인 방법으로 얼마든지 대처할 수 있지만, 후자의 경우는 큰 손실을 야기할 수 있다. 우리 회사의 경우에는 시스템 속에 포함된 지적 자산을 공격하는 사례가 많다. 이런 공격에 대비하기 위해서는 시스템 초기부터 데이터에 접근제한을 해 둬야 한다. 네트워크를 잘 분할해 놓고, 접근제어를 실행하도록 하며, 사내 직원들에게는 이런 시스템의 구조를 설명해 보다 잘 이해할 수 있도록 하는 것이 필요하다.

최근 Google Phone이나 Smart Phone과 같이 다양한 운영체제를 사용하는 휴대전화기기들이 등장하고 있다. 기존의 시스템, 네트워크에 대한 공격 이외에 이들 휴대전화기기에 대한 보안문제도 적지 않게 대두되고 있는데.

솔직하게 말하면, 휴대전화기기의 보안에 대비하는 노력보다는 차라리 휴대전화기기 사용을 중지하거나, 휴대전화기기의 데이터 보안을 잊어버리라고 말해 주고 싶다. 현재 등장하고 있는 모든 휴대용 장비들은 운영체제, 메모리, 네트워크와 같은 모든 컴퓨터 기능이 내재돼 있음을 인식하고 있어야 한다. 즉, 이들 기기들은 컴퓨터만큼 중요하며, 또 그 만큼의 취약점을 가지고 있을 수 있다. 무선 네트워크 프로토콜은 가끔 암호화되지만, 그것은 데이터 전송 시에만 해당될 뿐이다. 그런데 휴대 전화기기나 PDA는 더욱 증가되고 애플리케이션 공격은 더욱 일반화되고 있다. 때문에 휴대용기기에도 일반 컴퓨터나 서버에 적용하는 것과 동일한 관리가 필요하다. 지속적으로 패치를 적용하고, 업데이트 시키고, 또 불필요한 서비스와 애플리케이션을 제거하도록 해야 한다. 무엇보다 사용자들은 데이터를 백업해 둠으로써 휴대전화기기의 공격이나 도난에 대비해야 한다.

최근 한국에서는 DDoS 공격이 많은 문제를 야기하고 있다. DDoS 공격은 한국뿐만 아니라, 세계적으로도 문제가 되고 있는데, 미국에서는 이와 같은 공격에 대해 어떻게 대응하고 있나.

잘 알고 있겠지만 DDoS 공격에는 네트워크 리소스를 모두 소진하게 하는 방법이 주로 이용되고 있다. 특히, 대부분의 DDoS 공격은 봇넷을 통해 이뤄지고 있으며, 수천 개의 좀비 PC를 통해 전 세계에서 동시에 일어나고 있다. 원론적이겠지만 최선의 대응방법은 상위 ISP와 함께 이에 대비하는 것이라고 생각한다. 비록 많은 비용이 소모될 수 있겠지만 ISP가 제안하는 Traffic Throttling, Diversion and Packet Scrubbing 등을 이용하는 것도 한 방법이 될 수 있다.

지난 2월 CONCERT가 주최한 SANS 교육을 위해 방한했던 것으로 알고 있다. SANS 교육을 통해 여러 국가의 정보보호 담당자들을 만나게 될 텐데, 국내 정보보호 담당자들과 해외 담당자들 간에 차이점은 무엇이라고 생각하나.

전 세계 많은 사람들로부터 질문이 담긴 이메일을 볼 때 이들이 가진 정보보호에 대한 열망을 느낄 수 있다. 그런 사람들에게 가이드라인을 제시하고, 교육받을 기회를 제공한다면 이들 대부분은 정보보호의 미래에 크게 기여할 것이다. 특히 기술적으로 앞서 있는 한국의 전문가들은 상당한 실력을 소유하고 있고, 또 자긍심이 있으며, 호기심이 왕성했다. 이런 사실은 정보보호 전문가가 되기 위한 중요한 자질이라고 본다. S