새로운 안티바이러스로 부상하는 IPS

코드레드로 발견 즉시 조처하는 솔루션 필요성 대두

이제 파이어월이나 IDS를 넘어 IPS의 시대가 열릴 것으로 보인다. 날로 극악해지고 영악해지는 바이러스는 DDoS의 대안으로 부상하던 IDS를 구시대 솔루션으로 만들어버리고 있다.

IDS가 문제를 파악했을 때, 이미 코드레드는 집안을 휘젓고 있기 때문이다. IPS는 이상 신호에 대해 발견 즉시 적절한 조처를 취한다는 점에서 IT 관리자들의 주목을 받고 있다.

미국 노스캐롤라이나주의 지방 은행인 퍼스트 시티즌 은행(First Citizens Bank)이 코드 레드 바이러스의 공격을 받았다. 하지만 이 공격은 실패로 돌아갔다. 왜냐하면 이곳의 네트워크 운영 팀이 최신 시큐리티 기술, 즉 그 악성 바이러스를 효율적으로 차단해낸 침입 방지 시스템(Intrusion Prevention System, 이하 IPS)을 설치해 뒀기 때문이다.

침입 경고 이전에 공격 중단에 초점

대부분의 관리자들은 IDS에 대해 잘 알고 있지만, 침입 방지 시스템은 분명 생소한 개념이다. 이 두 가지는 서로 밀접한 관련이 있고, IPS는 하나의 툴로서, IDS를 완전히 몰아내기보다는 서로 병행해서 쓰이고 있다.

하지만 이 두 시큐리티 기술 간의 근소한 차이점이 퍼스트 시티즌 은행의 워드를 비롯한 IT 관리자들에게 크나큰 차이가 나는 결과를 안겨줄 수 있다. IDS는 이미 알려져 있는 공격 시그니처를 감시하면서 수상한 네트워크 활동을 찾아내기 위한 목적으로 설계됐다.

IDS는 범상치 않은 네트워크 활동을 찾아냈을 경우 해당 운영 직원에게 경고 메시지를 보내고 침입의 진전 상황을 기록하고 보고한다.

하지만 IDS는 문제를 즉각적으로 처리하지는 못한다. 즉 진행되고 있는 공격을 막지는 못한다는 것이다. 바로 이 부분에서 IPS가 빛을 발한다. IPS는 공격 시그니처를 찾아내며, 네트워크에 연결되어 있는 기기에서 수상한 활동이 이뤄지는지를 감시한다. IPS는 서버가 비정상적인 행동을 실행하고자 하는 경우 자동으로 모종의 조치를 취함으로써 그것을 중단시킨다.

IPS를 판매하고 있는 오케나(Okena)의 마케팅 담당자에 따르면 "우리는 지금까지 그게 코드 레드인지조차 몰랐다. 그냥 비정상적인 활동이 이뤄지고 있었다는 것만 알고 있었다"며, "우리가 하는 일은 기기들의 작동이 어떤 식으로 이뤄져야 하는지를 파악한 후 그것을 실시간으로 실행시키는 것"이라고 설명했다.

벤더들 IDS에서 IPS로 발빠른 움직임

IPS가 감시하는 비정상적인 행동에 대한 예를 하나 들자면, 웹 서버가 텔넷이나 FTP 세션을 실행하려 하는데, 그 유일한 목적이 웹 페이지를 서비스하려는 것일 경우다.

또 하나 예를 들면, 한 도메인으로부터 들어오는 접속 시도 횟수가 비정상적일 경우, IPS는 해당 도메인에 대한 액세스를 모두 차단해버린다.

또는 메일 게이트웨이를 통해 들어와 마이크로소프트 아웃룩으로 하여금 주소록 안에 들어있는 모든 주소로 바이러스가 들어있는 전자우편을 자동으로 보내려 하는 모종의 코드가 될 수도 있다. 오그렌은 IPS를 이용할 경우 그런 시나리오를 모두 예방할 수 있다고 주장한다.

가령, 코드 레드의 경우 퍼스트 시티즌 은행은 이 바이러스가 자기 증식을 위해 인터넷을 뒤져 다른 취약한 서버를 찾아내려 한다는 것을 감지할 수 있었다.

이 은행이 배치했던 IPS는 엔터셉트 시큐리티 테크놀로지(Entercept Security Technologies)에서 개발한 것으로, 그런 활동을 즉각 중단시키고, 타깃이 된 서버들에 있는 에이전트를 통해 무단으로 송출되고 있는 포트 스캔을 중단시켰다.