바이러스 메일 차단은 신속한 업데이트가 생명

업데이트 문제 해결한 실시간 서비스 주목받아

박상준 코코넛 전략기획팀 과장

하루에도 몇 통씩 바이러스 메일을 받으며 스트레스를 받은 적이 있을 것이다. 점점 지능화되는 바이러스와 바이러스로부터 자유롭고자 개발되는 안티 바이러스 기술. 이제 기술이 아닌 서비스로 발전하는 트랜드에 대해 살펴보고자 한다.

「편집자주」

일반 가정과 기업에게 동시에 문제가 되는 보안 이슈는 무엇일까? 누구나 가장 먼저 머리에 떠올리는 것은 바이러스일 것이다. 국내뿐만 아니라 전 세계적으로 보더라도 매년 바이러스로 인한 피해가 급증하고, 이에 따른 백신업체의 매출도 덩달아 급증하는 추세다.

CERTCC-KR(2002년 6월)의 자료를 참조해 보면, 매월 평균 10-20개의 신종 또는 변종 바이러스가 지속적으로 발생하고 있다. 대부분의 바이러스의 생산지는 외국(약 80-90%)이고, 국산 바이러스가 다소 낮다. 그러나 바이러스 생산 후 전 세계로 전파되는데 하루도 걸리지 않는다는 점을 감안하면 바이러스의 생산지에 대한 논의는 별 의미가 없다.

새로운 형태의 바이러스 출현

올해를 포함해서 가장 주류를 이루는 바이러스 종류는 트로이목마로 전체 바이러스 종류의 약 40%가 넘는다. 그 뒤를 매크로 바이러스, 웜 바이러스, 파일 바이러스, 악성 스크립트가 따르고 있다.

외형적인 모양새로서는 새로이 발견되는 바이러스의 수는 일정하며, 그 중 대부분의 바이러스는 트로이 목마 바이러스와 매크로 바이러스이다. 그러나 바이러스로 인한 피해 동향을 살펴보면 오히려 웜 바이러스가 가장 문제되는 것을 알 수 있다.

웜 바이러스로 인한 피해액과 피해보고 건수는 타 바이러스에 비해 가장 높다. 웜 바이러스는 기존의 바이러스와 그 형태가 매우 상이해 별도로 구분된다. 새로 등장해서 작년과 올해 매우 큰 피해를 입혔던 웜 바이러스는 기본적으로 자기 복제기능이 있고, 독립적으로 활동하며, 메일 및 다양한 미디어를 통해 매우 빠른 속도로 감염 대상을 넓혀간다는 점이 가장 큰 특징이다. 빠른 속도로 감염을 넓혀간다는 특징 때문에 감염이 된 기업의 전산자원은 급속히 고갈되어 가고, 궁극적으로 기업의 가용성을 하락시키는 주요 원인이 된다.

이처럼 새로운 종류의 바이러스는 기존의 주로 1대의 컴퓨터의 기능을 마비시키는 데에서 전체 네트워크의 기능을 떨어뜨림으로써 기업의 업무 수행에 방해요인이 된다. 이처럼 바이러스의 유전자가 급속히 변화되고 있는데 반해, 이에 대응할 수 있는 백신프로그램의 발전은 상대적으로 느린 상황이다.

안티 바이러스 솔루션의 한계점

기존의 바이러스 방역의 유일한 방법인 안티 바이러스 솔루션에 의한 대응은 두 가지의 치명적인 허점을 갖고 있다. 첫 번째 문제는 신속한 업데이트의 어려움이고, 두 번째 문제는 안티 바이러스 솔루션의 능력에 대한 문제점이다.

바이러스 방역상의 가장 중요한 점은 신속한 업데이트이다. 바이러스가 최초 유포 후 하루 이내 전 세계에 전파된다는 점과 전파의 속도가 기존의 바이러스보다 훨씬 더 빨라졌다는 점을 감안하면, 바이러스에 대한 업데이트는 늦어도 하루를 넘어서는 안 된다.

업데이트가 늦어지는 요소는 두 가지로 백신업체에서 바이러스 방역 엔진을 만드는 시간과 만들어진 방역 엔진을 실제로 고객이 업데이트 하는 시간으로 나뉘어진다. 첫 번째 요소인 엔진 제작시간은 각 백신업체에서 시간을 다투는 중요한 이슈로서 보통 최초 바이러스 발견 후 몇 시간 이내에 모두 수행되는 것으로 알려져 있다. 따라서 여기서 지연되는 시간은 상대적으로 적은 편이다.

그러나, 두 번째 지연요인인 고객의 업데이트 주기는 짧게는 하루에서 보통은 1주일 혹은 수개월이 걸리기도 한다. 사실 안티 바이러스 솔루션을 설치하고 수개월 동안 한번도 업데이트를 하지 않는 사용자가 부지기수이다. 이런 경우에는 바이러스 방역 솔루션이 설치는 되어 있으나 무용지물이 되곤 한다.

업데이트의 문제점에 대해서는 적극적으로 업데이트를 충실히 하

는 경우에도 약 2-3일이 걸리며, 요즘 바이러스의 특성상 내부 네트워크에 하나의 바이러스 감염 시 이를 치료하는데 많은 시간과 자원이 소요되고 있다.

두 번째 문제인 안티 바이러스 솔루션의 능력상의 문제점은 단 하나의 안티 바이러스 솔루션을 갖고서 바이러스 방역을 할 때 놓치는 바이러스가 발견된다는 통계에서 출발한다. 이 문제는 보통 알려지지 않은 바이러스 및 변형 바이러스에 대한 낮은 대처 능력은 당연한 것이며, 심지어는 알려진 바이러스에 대해서도 탐지를 못하는 경우가 생겼다.

NAI의 2001년 통계에 따르면, 단 하나의 안티 바이러스 솔루션을 사용했을 경우, 24종류의 알려진 바이러스에 대해 141번 바이러스를 놓치는 경우가 생겼다. 아울러 메일 바이러스 전문 보안업체인 메시지랩사(MessageLabs)의 통계에 따르면 잘 알려진 외산 솔루션의 경우 약 95% 내외의 탐지율을 보인다. 다시 말하면 알려진 바이러스 중의 약 5% 정도는 탐지를 못한 채 들어오고 있다는 것이다.

추가적으로 문제가 되는 것은 기존의 바이러스는 특정 호스트나 시스템에 장애를 일으키는 바이러스인 반면, 요즘의 바이러스는 앞에서도 이야기한 바 있듯이 네트워크와 시스템에 부하를 끼치는 문제점을 갖고 있기 때문에 바이러스 방역 대책이 단지 고객사 안에서 모두 해결되어야 하는 것은 매우 큰 위험을 안고 있는 것이다.

왜냐하면 어찌되었건 바이러스가 사내로 들어와서 차단이 되어야 하기 때문에, 해당 솔루션을 탑재한 시스템의 자원과 시스템에 연결되어 있는 네트워크의 대역폭의 막대한 손실은 어쩔 수 없이 받아들여야 하며 장비의 다운현상과 회선의 과부하는 업무의 마비를 의미한다.

솔루션에서 서비스로의 전환

이와 같은 이유로 가장 좋은 대안은 바이러스의 침입을 외부에서 차단하는 것이다. 외부에서 전문적으로 바이러스에 대한 차단을 제공하는 서비스가 존재한다면, 업데이트의 지연으로 인한 문제점을 최소화 시켜줄 수 있을 것이다. 또 고객 내부의 특정 호스트나 네트워크의 폭주 등으로 인한 문제점을 해결해 줄 수 있다.

이 경우에도 앞부분의 두 번째 문제인 하나의 안티 바이러스 솔루션을 사용하는 데에 따른 보안상의 허점과 알려지지 않은 바이러스 및 변형 바이러스로 인한 문제점은 여전히 숙제로 남아 있다.

코코넛이 영국의 메일 바이러스 차단 전문 서비스 업체인 메시지랩사와 제휴로 제공하고 있는 코코넛 스카이스캔 서비스는 이러한 문제점을 모두 해결한다. 코코넛 스카이스캔 서비스는 총 4가지의 서로 다른 안티 바이러스 솔루션을 사용하며, 이중 3가지는 McAfee, F-Secure, V-Find로서 전 세계적으로 인정받은 솔루션이다.

이들 솔루션은 알려진 바이러스에 대한 방역을 수행하되 서로의 취약성을 상쇄시켜 놓치는 바이러스에 대응한다. 아울러 메시지랩사에서 자체 개발한 Skeptic 기술은 인공지능 기술을 채택해 알려지지 않은 바이러스 및 변형 바이러스를 차단하는 역할을 수행한다. Skeptic 기술은 다양한 정보를 이용하여 메일의 행태를 분석하고, 각 행태별로 의심스러운 정도에 비례한 점수를 매긴 후, 이를 합산해 종합점수가 일정 수준이상 도달 시 바이러스로 탐지하게 된다.

메시지랩사는 이 Skeptic 기술을 이용해 러브 바이러스를 전 세계에서 가장 빨리 탐지하고 차단한 적이 있다. 업데이트의 문제점은 10분마다 업데이트를 수행함으로써 업데이트 지연문제를 해결한다.

바이러스로 탐지된 메일은 메시지랩사의 검역소에 보관하고, 고객의 요청이 있을 경우에 해당 메일을 알려줌으로써 장비 및 네트워크의 부하를 획기적으로 줄여준다. 아울러 모든 안티 바이러스 관련 구성을 코코넛에서 수행하기 때문에 고객은 신청서만 제출하면 되므로 매우 편리해진다.

바이러스 대응에 대한 효율적인 관리

대부분의 바이러스는 이메일을 통해 전파된다. 전체 바이러스 중 약 90%가 메일을 통해 전염되는 것으로 알려져 있다. 또한 IDC 통계(2000년)에 따르면, 전체 이메일 중의 20-30%에 바이러스가 감염돼 있는 것으로 나타났다.

아울러 지난 4년 동안 메일의 양이 2배로 증가했고, 그 증가 추세는 더욱더 급격히 상승할 것이다. 코코넛의 스카이스캔 서비스는 이를 감안해 이메일에 대한 바이러스의 차단을 지원한다. 그러나 침입차단시스템이 우회공격에 대해서는 차단을 할 수 없듯이, 코코넛의 스카이스캔 서비스도 이메일 외의 방법으로 공격하는 것은 차단할 수 없다.

따라서 고객사는 안티 바이러스 서비스 외에 별도의 안티 바이러스 솔루션을 갖추고 있는 것이 좋다. 대부분의 바이러스 침투는 안티 바이러스 서비스로 차단하고, 기타 바이러스 침투에 대해서는 안티 바이러스 솔루션을 종합적으로 대응함으로써 가장 효율적으로 바이러스에 대한 대응을 수행할 수 있다.

바이러스의 지능은 날이 갈수록 높아져 가고 있으며, 이에 따른 피해액도 급증하고 있다. 어느 특정한 한 솔루션이 모든 문제를 해결해 주는 시대는 지나갔으며, 해당 분야에 전문적인 업체에게 아웃소싱 형태의 서비스를 받는 시대가 도래하고 있다.

보안분야에서는 보안 관제서비스의 높은 이용률이 이를 증명하고 있다. 과거에는 소를 이용해 경작을 하는 시대였다면, 현재는 경운기를 이용해 경작을 하는 시대이다. 경작하고자 하는 논의 크기와 효율성을 따져서 적절한 방법을 선택해야 할 것이다. 급격히 지능화되는 바이러스의 효율적인 차단은 전문 바이러스 방역 솔루션업체의 전문 서비스를 받는 것이 가용성과 경제적인 측면에서도 분명 도움이 될 것이다.