

# 웹 피해 폭증...IPS로 악성코드 막는다

지난해 웹 바이러스로 인한 전세계 피해액은 330억달러(4655억)에 달하고 있다. 지난해 국내 웹 바이러스 피해액은 2007년 5333만, 2008년 1만5199만여 명이 지속적으로 늘어나고 있다. 웹 바이러스 피해건수도 2007년 1만5000건에서 2008년 3만6672건으로 늘었고, 지난해 8만5000건으로 폭발했다.

특히 웹은 기업에 대한 공격의 관건 역할을 증가시켰을 뿐 아니라 금융기관처럼 네트워크 안정성이 중요한 기업은 치명적인 결과를 초래할 수 있다.

금융기관은 당연히 힘을 기울여 수 있는 요건에 대한을 갖게 되었고, 자체 보안체계를 크게 강화하면서 웹이 차이를 갖고 있다.

금융권 IPS 시장은 최근 몇 년을 거점으로 매년 삼배 가까이 급성장할 것이라는 게 업계의 관측이다. 이미 국내의 3대 기업에 대해 10억 IPS 시장을 놓고 치열한 시장 경쟁전을 벌이고 있다.

## ▶ 웹해킹 65% 단절 보안

현재 일반적으로 사용되고 있는 보안시스템은 방화벽, 가상사상망, 침입탐지시스템, 침입방지시스템, 인터넷서비스단절이다.

방화벽은 가장 기본적인 형태의 보안장치다. 하지만 해커들은 방화벽을 통과할 수 있는 불로, 다시 말해 허가된 정보를 이용한 공격법을 개발, 네트워크를 뚫어내고 있다.

방화벽은 공격 전파되는 웹 바이러스의 피해가 크게 증가하고 있는 것도 방화벽에 대한 공격이 늘어나고 있기 때문이다.

웹 바이러스의 공격을 막아내는 방법으로는 네트워크를 운영시키는 악성코드를 찾는 역할을 하는 침입탐지시스템(IDS)이다.

IDS는 네트워크를 통해 발생하는 데이터의 패턴을 분석해 얻은 정보를 바탕으로 신뢰의 악성 유무를 감지한다. 하지만 IDS도 여러 장벽이 있다.

은 패턴의 공격을 막아내지 못하여 악성 코드를 탐지하지만 할 뿐 실시간으로 대응을 차단하지 못한다는 치명적 약점이 있다.

이에 따라 자체를 보안시스템으로 활용방지시스템(IPS: Intrusion Prevention System)이 주목을 받고 있다.

방화벽이나 웹 바이러스 등이 복잡해지고 고도화되면서 IPS는 자체 보안체제로 주목을 받고 있는 것이다.

IPS는 방화벽이나 바이러스 등 악성코드의 침입을 탐지하는 침입탐지시스템과 동시에 이를 실시간으로 차단하는 방화벽의 기능을 겸하고 있다.

IPS는 단순 네트워크 차단 기능을 지난 방화벽의 한계와 같은 인터넷과 사후 인터넷 침해 사고 분석 기능을 지닌 침입탐지시스템(IDS)의 단점을 보완, 실시간으로 웹 공격자를 저지하는

로 분석 차단해주는 보안제품이다.

한국정보보호산업협회(KISIA)는 올해 IDS가 포함된 국내 IPS 시장 규모를 600억원 규모로 예상하고 국내 IPS 시장의 성장률 기점으로 지속적으로 성장할 것으로 예상했다.

라드웨어코리아의 전용업 지사장은 "IPS가 웹, 바이러스 등을 100% 막아주는 맞춤형 웹 보호망 105를 도입하면 안전하다"며 "IPS가 기업부터 국내 보안시장의 차세대 기대주로 주목될 것"이라고 말했다.

지방자산이나 교육기관 등에 집중되던 수요가 통신과 금융 등으로 확대되는 추세다.

특히 지난해 1월 인터넷은행 이후 IPS가 핵심이나 반대로 가상사상망(VPN)에 대한 핵심 제품으로 급부상하고 있다.

금융권의 경우에는 아직 도입 초기 단계다. 개별 프로젝트로 꾸리는 하지만 은행을 비롯해 보험사와 증권사 등을 대하면 수가 30여 개를 웃돌기 때문에 최소 300여만 이상의 시장 규모로 예상되고 있다.

우선 - 현대은행, 우리 - 신한은행 등이 IPS를 도입했는데 제일 보강을 비롯해 금융기관이 도입 범위를 내부적으로 확장했다.

## ▶ 보안업계, 시장 불확실성도 지적

IPS 시장은 회사와 기관별로 치열한 시장 경쟁전을 벌이고 있다. 국내 최대 기업에는 LG, 엔시스, 윈스테크노와 지오펜, 알넷, 카이온 IPS를 출시하고 시장 경쟁이 나심다.

와국 업체 중에는 맥아리, 라드웨어, 피싱포인트 등 다수의 업체가 국내 시장을 통해 제품을 공급하고 있다.

LG엔시스는 주문형인터넷 기법의 하드웨어 제품인 케이프론 IPS를 통해 개인기 대응성 등에 주력할 계획이다. 또 중국 등 해외시장 공략에도 박차를 가하고 있다.

IDS 기법의 IPS 사업을 전개하고 있는 윈스테크노는 올 상반기 매출과 같은 규모로 IPS를 통해 운영한다.

윈스테크노는 관공서와 대학이 시장에서 성과를 거두고 있으며 대형 대기업, 부산 강서구청, 경기 16개 시군, 서울 6개 구청 등에 자사의 IPS 제품을 공급할 계획이다.

지오펜은 내부망과 프로세서기반의 고성능 IPS인 '웜블러커'를 내놓고 올해 매출 100억 원을 달성한다는 계획이다.

알넷은 최근 신제품을 내놓고 IPS 시장에 출시를 목표로 하고 있다. 시유어머전도 신제품 NXX IPS 시리즈를 출시했다.

한국맥아리, 라드웨어인사, 윈스테크노와 더불어 보안 업체들의 경쟁을 보이고 있다.

특히 한국맥아리가 SK텔레콤에 10여 대의 IPS를 공급한 것을 비롯해 SBS와 KTF에 제품공급에도 제품을 공급, 두드러진 성과를 보이고 있다.

라드웨어코리아는 금융권에서만 우리 편이든, 우리 신한은행 등에 IPS를 공급해 금융권에 강한 연계를 보이고 있다.

김희환

## 인력부족 - 라드웨어코리아 전용업 지사장

### "검증된 IPS 도입해야"

"IPS 도입을 통해 웹 바이러스로 인한 피해 폭주할 때에 네트워크의 안정성을 보장하는 것이 무엇보다도 중요하다"



지오펜 매출리케이스 스위치 전문업체인 라드웨어코리아의 전용업 지사장(사칭)은 인터넷 안전 네트워크를 운영하기 위해서는 IPS의 도입이 필수적이라고 말했다.

김 지사장은 금융기관은 다른 산업에 비해 보안분야에 많은 투자를 했지만 방화벽, IDS 등으로 막을 수 없는 웹의 경우 내부 시스템에 큰 타격을 주게 된다며 특히 최근엔 상황해고 있는 웹 바이러스를 막기 위해서는 IPS 도입이 불가피할 것이라고 설명했다.

그는 웹을 거래금액으로 확산되기 때문에 한 대의 컴퓨터가 웹에 감염되면 많은 경우에는 수만 명의 데이터를 발송한다며 이 때문에 갑자기 메일 발송이 많아 지메일 서버에 막대한 부하가 걸려 전체 네트워크는 마비된다고 설명했다.

김 지사장은 네트워크의 효율적인 관리와 내부망의 보안자산을 보호하기 위해서는 기존의 보안장치는 막을 수 없으며 웹 공격을 막기 위해서는 IPS를 도입해야 한다고 주장했다. 김 지사장은 국내 업체들의 경우에도 기술개발에서 뒤떨어지지 않자기 위한 것은 계속된 기술개발과 재투자 등으로 기술과 제품이 경쟁력 있다고 설명했다.

특히 금융기관이 IPS를 도입할 경우에는 기술과 제품이 검증된 솔루션을 선택하는 것이 고려돼야 한다고 말했다.

이는 국내 IPS 시장이 급성장하면서 관련업체들도 수요충족으로 한계 지점에 도달했다.

김 지사장은 최근 도입유형에서 IPS 도입과 관련 BMT에 참여인 업체는 14개 업체인데 그중 3~4개 업체만 통과했다고 설명했다.

한편 김 지사장은 IPS가 웹 바이러스 등을 100% 막을 수는 없다고 말했다.

그는 웹은 사내 네트워크를 통해서도 확산되기 때문에 웹에 걸린 컴퓨터는 사내 네트워크에 연결된 컴퓨터 다수가 감염되도록 확산될 수 있다고 지적했다.

라드웨어코리아는 금융기관에 수천 명이 우리은행, 신한 우리은행, 한국전선은행 등을 고객으로 확보하고 있다.

지사장은 "특히 해킹기부터는 금융기관 등이 사명을 주도할 것으로 예상돼 일부 영업에 집중해 IPS 시장에서의 주도권을 굳히나갈 예정"이라고 말했다.

라드웨어는 이제 국내 3대 기업의 해커스 확보와 노하우를 바탕으로 금융권 시장에 대한 본격적인 공략에 나선다는 계획이다.

김희환 기자 khh@joong.com

## LG엔시스

### 자체 개발한 ASIC 탑재

LG엔시스(대표 박계형)의 침입방지시스템(IPS) 케이프론 IPS는 주문형인터넷(ASIC)기반 하드웨어 제품이다.

특히 네트워크 프로세서를 사용해 도당 2.3기가바이트의 대용량 트래픽을 처리하거나, 나노초의 손실없이 완벽하게 처리할 수 있도록 한 인텔이온 제품이다.

최근 인텔이온 프로세서와 웹 바이러스 등 공격대응, 업데이트, 서비스 등 제정방기 공격 대응을 지원함으로써 각종 사이버 공격에 대한 실시간 자동 업데이트 기능이 강화되고, 인증 관제 등으로 네트워크를 더욱 효과적으로 보호해 준다.

LG엔시스는 올 상반기까지 매출을 20억 달러에 달하는 50여개의 고객사들을 공급하는 성과를 거뒀다.

이에 따라 LG엔시스 측은 케이프론 IPS 및 신규 확대를 위한 해외시장 추가공급, 해외기 매출신장에 주력할 계획이다.

또 상반기에 좋은 반응을 얻었던 '캡슐' 신형의 운영 호스트 및 프로그램을 다수 적용하는 등 전체에 걸쳐 고객사에서의 신뢰



를 통한 제품 경쟁력을 높일 계획이다.

이 제품은 높은 성능을 국내 업체 최초로 자체 개발한 ASIC을 탑재했다는 점에서 차별화될 수 있다.

LG엔시스는 이와 같은 안정성을 기반으로, 또 해외업체가 주도하고 있는 하드웨어 제품들과 경쟁, 케이프론 IPS를 글로벌 제품으로 육성할 계획이다.

최근에는 중국 광안부 인증을 통해 IPS 제품으로 최초로 해외 진출했다. 2008년 중국 내로 수출된 정보보안용 보안기를 대안사에서 자체 네트워크 보안 솔루션을 대안사에서 자체 네트워크 보안 솔루션을 대안사에서 자체 네트워크 보안 솔루션을 대안사에서

## 지오펜

### 고성능 NPU 기반...높은 기술력으로 승부

자체 네트워크 보안용부인 개발업체인 지오펜(대표 김성현)은 국내 최초로 지난해 네트워크 프로세서(NPU) 기반의 고성능 IPS 웹블러커(WormBlaker)를 개발했으며 이를 통해 성능개선으로 발문공격기인 악성 코드를 분석하고 있다.

특히 이 회사는 최근으로 국가 안전에 K4 인증 획득에도 성공하는 등 기술력을 갖추고 있다.

지오펜은 지난 2008년 4월에 유선망과 방화벽(FW)과 가상사상망(VPN), 침입탐지시스템 등 자체 개발 기술을 갖춘 기업이며 특히 이러한 기능을 통합한 침입탐지시스템(IPS) 웹블러커를 솔루션을 개발하고 지난해 9월에 시장에 선보였다.

이후 한진, 경기도청, 과천시청, 강원구청, 광명구청, 파주시청, 남양주시청과, 무석구청 등 16개 시, 군, 구청에 공급, 주목성을 얻어 현재 전국적으로 수십 개 기관에서 BMT를 진행하고 있는 상황이다.

지사장이 각광받고 있는 IPS 시장에서 웹블러커가 탑재된 IPS 선두기업으로



나일 수 있었던 이유는 가격이 낮은 제품으로 승부하되 보다는 최고의 성능에 두드러진 점과 안정적인 성능이 특징이다.

이 회사가 자랑하는 웹블러커는 NPU기반으로 경쟁사에 비해 고성능을 표방하고 있으며, 악성(ASL), 주문형 침입탐지에 최적화된 능력이 뛰어나서 프로그래머와도 편리하고 고전압도 아서에서 매우 유연한 프로그램 변경이 가능해준다고 하는 고성능 IPS 솔루션이다.

지오펜은 올해 매출 100억 달성을 목표로 하고 있으며 미국, 유럽, 일본, 중국 등 해외를 겨냥한 글로벌 마케팅 및 제품 개발도 본격적으로 추진하고 있다.

실제로 중국과 필리핀이사와 등 현지법인 및 조인벤처를 설립하는 등 한중 글로벌 제품 개발을 통한 시장 개척에 나설고 있다.

김희환 기자 khh@joong.com

