



을지병원 보안시스템 구축 사례

“환자들의 안전 진료위해 철벽 보안 실현한다”

포티게이트-300 도입으로 스팸메일 대폭 감소...개인정보보호법 개정에 맞춰 첨단 보안장치 마련계획

을지병원은 온라인 진찰이 현실화 되는 시점부터 방화벽, 바이러스 차단 등 기초적인 보안을 시작으로 최근 포티게이트-300을 구축하는 등 진찰 마비 같은 최악의 상황을 발생하지 않으려는 노력을 계속 벌이고 있다. 물론 EMR(전자의무기록)이 100% 구축된 상황은 아니지만 각종 트래픽을 차단시켜 원활한 병원 진료를 돕고, 환자들의 정보를 보호하기 위해 발 벗고 나선것.

자체 보안의식을 높이는 교육과 보안장비 구축을 강화하는 등 변화된 모습을 보이고 있는 을지병원 보안관리시스템 관리 현황을 취재했다.

글_한수진 기자 사진_장성협 기자



대형 병원은 하루에도 수 백에서 수 천명의 환자들이 입원과 수술, 진찰을 반복하는 유동인구가 많은 곳이다. 더욱이 어떤 산업분야보다 개인 보안이 중요시되는 진찰기록들이 보관되어있는 특수한 곳으로 분류되어 시스템 관리를 철저히 하는 것으로도 유명하다. 하지만 그 중요성에 비례하지 못하고 있는 것이 현재 병원들의 현실. 막대한 진료데이터들과 방사선 그림 데이터들을 한꺼번에 전산화 하는 작업이 쉽지 않기 때문이다. 또한 의사들 및 관계자들의 협조부분이 상당수 차지하는 만큼 오랜 시간에 걸쳐 보안 정책을 적용시킬 수 밖에 없다는 것이 일반적인 견해다.

이에 을지재단 산하의 을지병원(www.eulji.or.kr)은 빠른 변화보다는 보안의식 고취에 의한 점진적인 보안 시스템 구축

을 표방한다. 안전한 진료문화를 이룩한다는 취지에 방화벽, 바이러스 차단에 머무르던 낙후된 보안체제를 포티게이트-300을 전격 구축하면서 통합보안시스템의 시대를 열고 환자들의 정보보호에 나섰다.

통합보안시스템으로 '포티게이트-300' 시스템 채택

기존의 방화벽 하나로는 각종 해킹을 통한 보안 위협을 비롯하여 날로 지능화되고 있는 바이러스, 웜으로부터의 안전한 네트워크 운용과 스팸메일의 원활한 차단을 기대하기에는 역부족이었다. 이를 해결하기 위해 을지병원은 포티넷 코리아의 '포티게이트-300 통합 네트워크 보안 시스템'을 구축함으로써, VPN 기능을 제외한 안티바이러스, 방화벽, IDS, IPS, 트래픽 셰이핑, 콘텐츠 필터링, 이메일 필터링 등의 모든 기능을 사용하기로 결정했다. 이와 함께 기존에 사용하던 방화벽과 각 사용자 PC에 별도 백신을 설치하는 등 3중 보안을 통해 보안 위협에 대한 철저한 시스템을 구축해 놓았다.

이와함께 을지병원은 포티게이트-300 시스템으로 400여대의 클라이언트가 연결된 15대의 사내 서버를 통해 침입하는 바이러스 및 웜, 유해트래픽 등의 혼잡보안위협을 원천적으로 차단함으로써 안정적인 네트워크 구현은 물론 EMR 구축을 위한 안전한 보안 환경을 조성할 수 있게 됐다.

장호열 전산실 실장은 "바이러스 때문에 보안의 필요성을 느끼게 되었지만 위험요소로 인한 PC 다운현상으로 진찰에 막대한 손해를 초래하는 것을 보고 보안에 중점을 두자는 결단을 내리게 됐다" 며 "포티넷 장비는 비용이 상대적으로 저렴하면서도 종류가 다양했고, 구축 후엔 안티바이러스를 100% 걸러줘서 업무의 효율을 높여주었다"고 설명했다.

을지병원이 도입한 포티게이트-300 안티바이러스-IPS는 게이트웨이에서 완벽한 실시간 네트워크 보호 서비스를 제공하는 전용 하드웨어 플랫폼으로써 여러 가지 보안 기능을 네트워크 및 애플리케이션 단계에서 외부로부터의 바이러스·웜의 공격을 차단하는 차세대 통합보안 솔루션이다.

포티게이트 전 제품은 업데이트 된 바이러스 백신과 침입 감지 서명 데이터베이스를 전세계 포티게이트 시스템으로 자동 전송하는 포티넷의 배포 네트워크(FortiProtect Distribution Network)를 통해 항상 최신 업데이트된 보안 상태를 유지하고 있다.

"일단 관리가 쉬어 업그레이드나 설정하는 방법들이 크게 어렵지 않아 누구라도 관리할 수 있는 것이 장점이고, 스팸메일 체크기능과 트래픽 체크기능은 스팸메일의 수를 대폭 감소시켰고, 보안 예방을 하게 된 것은 보안장비 구축후 달라진 점"

이라며 "이젠 내부 정보 유출을 막고, 직원들의 보안의식을 고취시키는 일에 매진할 생각"이라고 장 실장은 덧붙였다.

진료레일 사라지는 완벽한 EMR 실현 목표

병원 직원들은 최근 EMR(Electronic Medical Record, 전자 의무기록) 구축과 관련하여 보안 위협에 대한 필요성을 절실히 느끼게 되었다.

장호열 실장은 "현재 병원 내 클라이언트의 평균 동시 접속이 200여대 정도로 포티게이트-300으로도 만족할 만한 네트워크 보안 효과를 보고 있지만, 추후 과도한 네트워크 트래픽에 대비하여 더 높은 성능의 시스템 도입을 검토 중에 있다"고 말했다.

울지병원은 EMR을 비롯하여 OCS(Order Communication System, 처방전달시스템), PACS(Picture Archiving Communication System, 의료영상저장전달시스템) 등의 전산 시스템 도입을 고려하고 있다. 따라서 보안 위협에 대한 중요성을 더욱 인지, ASIC 기반의 UTM 보안장비로 교체할 계획도 세워놓았다.

'보안 규칙' 만들어 체계적인 보안정책 만들어 나간다

울지병원의 보안정책을 총괄하고 있는 장호열 실장은 병원 내 보안책임자들이 모여 정보를 공유하고 사례 발표를 하며 보안정책을 논의하는 세미나에 참여해 활발한 활동을 펼치고 있다.

"어려움에 직면했을 때 해결해 나가는 노하우등을 교류해 보안 시스템을 운영하는데 많은 도움이 되고 있어 꾸준히 활동을 벌이고 있다" 며 "불과 수년 전까지만 해도 보안 의식들

Product 포티넷코리아 '포티게이트-300'



포티넷코리아(대표 김중덕, www.fortinet.co.kr)의 포티게이트-300 안티바이러스-IPS는 게이트웨이에서 완벽한 실시간 네트워크 보호 서비스를 제공하는 전용 하드웨어 플랫폼으로써 여러가지 보안 기능을 통해 네트워크 및 애플리케이션 단계에서 외부로부터의 바이러스 및 웜의 공격을 차단하는 차세대 통합 보안 솔루션이다.

또한 포티게이트 전 플랫폼에서 제공되는 포티가드(FortiGuard™) 배포 네트워크 서비스는 포티게이트 전 제품에 업데이트된 바이러스 백신과 침입 감지 서명 데이터베이스를 전세계 포티게이트 플랫폼으로 자동 전송하는 서비스다. 포티게이트 고객이라면 누구든지 포티가드 배포 네트워크(FortiGuard Distribution Network)를 통해 항상 최신 업데이트된 보안 상태를 유지할 수 있다.

포티게이트-300 제품군은 고성능, 가용성, 안정성을 만족 시켜 주며, 타 모델에서 제공하는 모든 기능(실시간 바이러스 차단, 방화벽, VPN, 침입탐지 및 차단, 대역폭 제어, 스팸 메일 차단)을 통합적으로 제공할 뿐만 아니라, 1Gbps의 고성능을 자랑한다. 자동 Fail-over 기능을 포함한 고가용성 기능 제공, 멀티존 설정 기능 등은 미션 크리티컬한 기업 망에 완벽한 보안 솔루션을 제공한다.

특히 포티게이트-300은 오늘날 성장하고 있는 중소기업의 사업장을 위한 성능과 확장성, 보안성을 제공하며, 10/100/1000의 속도를 제공함으로써 향후 기가비트 네트워크로 업그레이드 하더라도 사용할 수 있다.

이 전무하다시피 하고 시스템 투자가 미비했던것에 비하면 빠르게 발전하고 있는 것 같다. 하지만, 병원엔 여전히 보안을 하나의 보험으로 여기는 인식들이 남아있고, 사용자들의 보안 의식도 낮다."

울지병원은 사용자들의 보안 마인드가 구축되는 것이 더욱 중요하다고 여기고 보안 규칙을 정확히 만들어 명시해 놓고 정기적인 교육을 진행시키기로 했다. 또한 보안 컨설팅을 진행하고 부서를 전문화 시키는 등 체계화를 작성한다는 밑그림을 그려놓은 상태다.

한편, 울지병원은 내부 정보유출을 막는 보안 강화정책과 함께 DB 보안 솔루션 구축 등 보안장비의 다각화를 검토중이고 검증은 거쳐 적용시킨다고 밝히고 있다. 

