Symantec

케이스스터디

다계층 보안 전략으로 지능형 위협 차단,

kt '제로트러스트' 정보유출 방지 체계 강화

국내 대표 통신사인 KT는 정보보안단을 발족한 지난 2014년 8월을 기점으로 정보보안 체계를 대폭 강화해왔다. 다계층 보안 정책을 바탕으로 외부 해킹 위협과 내부 정보유출 통제, 협력사와 그룹사 보안관리까지 포괄적으로 수행하고 있다.
그 과정에서 KT는 시만텍의 SSL 가시성 솔루션인 'SSL VA', 네트워크 포렌식 솔루션인 'SA', 웹 보안 게이트웨이 '프록시SG', 네트워크 DLP를 도입해 수년째 활용하고 있다. 글로벌 위협 인텔리전스를 기반으로 이같은 다양한 보안 솔루션을 연계해 정보보안 체계를 강화하는데 효과를 거두고 있다.

시만텍 웹 보안 게이트웨이, SSL 가시성 솔루션, 네트워크 DLP 등 연계 활용해 효과적인 보안운영 환경 구축

암호화 트래픽까지 위협 가시성 대폭 확장, 내부 중요정보 세밀한 통제 정책 운영

KT 보안 이야기

Byline Network
byline.network

KT의
남다른
보안 이야기

KT 정보보안단은 지난 2017년 갈수록 증가하는 보안 위협에 보다 효과적으로 대응하기 위해 지능형 사이버 보안센터(Intelligent Cyber Security Center)를 개소했다. 사내 IT보안관제와 고객 네트워크 보안관제를 통합한 사이버보안센터는 단말부터 네트워크, 서버에 이르는 종합대응체계를 구축했다.

사이버보안센터는 외부에서 침입하는 사이버공격과 지능형지속위협(APT) 공격 탐지와 분석, 그리고 내부 정보유출 시도를 감시해 차단하는 1차 방어선 역할을 수행한다.

관문에 설치된 방화벽, 침입방지시스템(IPS) 등 1차 탐지·방어체계를 뚫고 위협이 내부로 들어오더라도 그 안에서 전파되지 못하도록, 또 중요 정보를 외부로 유출하는 활동을 탐지하고 차단하기 위해 다양한 보안 시스템이 가동된다.

여러 보안 솔루션들을 연계해 위협 가시성을 확보하고 양질의 위협 인텔리전스를 확보하는데 힘을 기울이고 있다. 바로 다계층 보안 정책을 통해 다양한 지능형 위협에 효과적으로 대응하기 위한 조치다.

KT 정보보안단의 유기무 보안기획담당 상무보는 "'신뢰하되 모든 것을 검증하라'는 모토로 관리적·기술적 보안을 강화하고 있다"라면서 "외부 공격과 APT, 내부정보유출 같은 내부자 위협, 협력사와 그룹사 통한 위협까지 대응하는 보안 프레임워크를 바탕으로 계속해서 탄탄하고 촘촘한 보안체계를 만들어 나가고 있다"고 밝혔다.

암호화 트래픽 위협 가시성 확보, 포렌식 솔루션과 연계

KT는 보안체계를 구축하는데 있어 위협 가시성을 폭넓게 확보하는 것을 중요하게 봤다. 특히 암호화된(SSL/TLS) 네트워크 트래픽 가시성을 확보하는 것이 외부 위협 대응에서 필수라고 보고 시만텍의 'SSL VA(Visibility Appliance)'를 도입했다.

인라인 복호화 솔루션인 'SSL VA'는 모든 암호화 트래픽을 복호화해 IPS와 연동해 위협 트래픽의 경우 차단 조치를 수행하고 있다.

유 상무보는 "보이지 않으면 관리되지 않는다. 외부에서 들어오는 공격 가운데 SSL 트래픽은 40% 이상이고, 계속해서 그 수치가 올라가고 있다"라면서 "SSL 트래픽 가시성을 확보해야 공격을 막을 수 있기 때문에 복호화를 수행해 차단한 후 분석을 위해 포렌식 장비에 저장하고 있다"고 설명했다.

KT는 시만텍의 포렌식 솔루션인 'SA(Security Analytics)'에서 악의적인 공격으로 판단되는 트래픽을 수집·저장하고 있다.

이를 바탕으로 위협에 대한 추가 분석을 수행한다. 주로 기존에 알려지지 않은 신종 위협이나 의심스러운 트래픽, 이상행위를 파악하고 조사하는데 활용하고 있다.

보안 웹 게이트웨이로 악성코드 유입 차단, 정보유출 통제

KT는 시만텍의 보안 웹 게이트웨이(SWG)인 '프록시SG'도 사용하고 있다. 시만텍 제품 가운데 가장 먼저 도입한 솔루션으로, 악성·유해 사이트를 차단하는 것은 물론 중요정보가 외부로 전송되는 것도 통제해 정보유출 방지체계를 강화하는데 효과를 거두고 있다.

'프록시SG'를 도입하면서 KT는 시만텍이 제공하는 글로벌 인텔리전스 네트워크(GIN)를 이용할 수 있게 됐다. 이 위협 인텔리전스를 기반으로 국내뿐만 아니라 해외 악성 웹사이트와 유해 사이트, 비업무 사이트로 구분해 관리를 수행하고 있다.

외부에서 웹을 통해 유입되는 악성코드 등 위협 차단은 물론, 내부에서 외부로 데이터를 유출하려는 시도를 실시간 탐지·차단한다. SSL 트래픽을 복호화 시킨 데이터를 포함해 모든 데이터의 크기와 목적지에 제한을 둬 드롭박스나 에버노트 같은 클라우드 서비스를 이용한 외부 유출을 통제하고 있다.

유 상무보는 "80, 443포트처럼 열어놓은 웹 프로토콜을 이용해 내부정보를 유출하거나 포트 정책을 위반한 공격이 들어오는 경우 '프록시SG'로 차단하고 있고, 토렌트같은 파일 공유 프로그램, 토르를 비롯해 다크웹도 자동 차단한다"라면서 "기존에는 단말단에서 일일이 조치하던 것을 시스템으로 막고 있다"고 말했다.

네트워크 가상 위협 동적분석(샌드박스)을 수행하는 APT 보안 시스템과 연계 구성해 보안운영 효율성을 개선하는 효과를 얻기도 했다. '프록시SG'가 샌드박스의 악성코드 분석 작업량을 감소시켰기 때문이다.

샌드박스, 네트워크 DLP와 연동해 보안운영 효과 향상

KT는 '프록시SG'를 샌드박스뿐만 아니라 시만텍의 네트워크 DLP(Data Loss Prevention)와도 연동해 보다 강화된 정보유출 방지체계를 구축했다.

시만텍 DLP가 제공하는 콘텐츠 분석 기술을 기반으로 PC와 서버, 웹 등 정보가 유출되는 모든 경로를 이용해 외부로 전송하는 데이터에 대한 가시성을 넓혔다. 예를 들어 외부로 나가는 파일에 개인정보나 중요정보가 포함돼 있는 것까지 파악할 수 있게 됐다.

혹시 모를 직원들의 보안정책 위반, 데이터 오남용 현황을 파악하고 점검, 통제할 수 있게 돼 개인정보보호와 기업비밀보호 수준을 한층 높일 수 있게 된 것이다.

KT는 내부정보유출 방지체계를 보다 강화하기 위해 클라우드 서비스까지 확장해 보호할 수 있는 방안을 고민하고 있기도 하다.

정보보안단 내에서 일부 사용자들을 대상으로 클라우드 서비스에 클라우드접근보안중개(CASB)를 적용해 개념검증(POC)을 수행하면서 테스트를 하고 있다.

보안 솔루션을 도입할 때 우선 고려하는 사항으로 유 상무보는 "안정성과 탄탄한 가용성은 기본이지만 매우 중요하다"라면서 "우수한 보안 솔루션들을 잘 연계하고 묶어 최대한 가치있게 활용하는데 힘을 기울이고 있다"고 전했다.

이어 "앞으로도 클라우드와 5G, 사물인터넷(IoT) 등 새로운 환경 변화에 대응하면서도 내부정보보안, 다중보안체계를 공고히 하는데 힘을 기울일 것"이라고 강조했다.

취재·글. 바이라인네트워크 〈이유지 기자〉
yjlee@byline.network

유기무 KT 정보보안단 IT기획실 보안기획담당(상무보)

보이지 않으면 관리되지 않는다.
늘어나는 SSL 트래픽 가시성을 확보해야
공격을 막을 수 있기 때문에 SSL VA 장비로
복호화를 수행해 차단한 후
분석을 위해 포렌식 장비에 저장하고 있다.
글로벌 위협 인텔리전스를 제공하는
보안 웹 게이트웨이로
정보유출방지체계를 구축했고,
네트워크 DLP까지 연동해 데이터 가시성을 넓혀
개인정보와 중요정보 유출을 통제하고 있다.
우수한 보안 솔루션들을 잘 연계하고 묶어
최대한 가치있게 활용하는데 주력하고 있다.

트래픽 암호화로 발생하는 보안 사각지대 해소하는
시만텍 SSL VA

시만텍 SSL VA(Visibility Appliance)는 암호화된(SSL/TLS) 트래픽에 대한 가시성을 제공해 기업 환경에 존재하는 보안 사각지대를 제거해준다. 암호화 기술을 사용해 은밀하게 활동하는 사이버공격을 탐지할 수 있어 지능형 보안위협으로부터 기업 환경을 보호할 수 있도록 지원한다. SSL VA는 모든 네트워크 포트에서 모든 SSL 연결 및 애플리케이션을 식별하고 복호화한다. 복호화된 결과물은 차세대방화벽, 침입방지시스템(IPS), 데이터유출방지(DLP) 솔루션 등에 전송해 정교한 보안위협을 탐지, 차단하는데 활용할 수 있기 때문에 보안효과를 높여준다. 또 고성능, 고가용성을 지원하는 SSL VA가 복호화 기능을 담당해주기 때문에 기업의 전반적인 네트워크와 보안 인프라 성능이 향상되는 효과도 얻을 수 있다. SSL VA는 기존 네트워크를 재구성하거나 IP주소 또는 토폴로지를 변경할 필요 없이 기존 인프라에 쉽게 구축할 수 있으며, 간단하게 중앙에서 여러 장비를 관리할 수 있도록 제공한다.

최신 보안위협 유입, 데이터 유출 막는
시만텍 프록시SG

시만텍 프록시SG(ProxySG)는 갈수록 정교해지고 확대되는 웹 트래픽 보안위협으로부터 기업 환경을 보호하는 웹 보안 게이트웨이다. 악성 페이로드가 담겨 있거나 사내 정책에 위배되는 웹 콘텐트를 검사해 필터링, 제거, 차단해 기업으로 유입되는 리스크를 낮추고 데이터 유출도 차단할 수 있다.
프록시SG는 시만텍의 클라우드 기반 글로벌 인텔리전스 네트워크(GIN)를 바탕으로 실시간 웹 콘텐츠를 평가해 최신 보안위협이 사내로 유입되는 것을 통제하고 보호한다. SSL 트래픽 모니터링을 지원해 암호화된 트래픽에 대한 가시성을 제공한다. 복호화된 콘텐트는 추가 분석이나 포렌식을 수행할 수 있는 다른 시스템으로 전송할 수 있고, 안티바이러스(AV)나 표준 ICAP을 통해 인증된 DLP와도 통합될 수 있다. 클라우드 애플리케이션을 포함해 회사에서 승인하지 않은 웹과 클라우드 애플리케이션(SaaS)을 모니터링해 사용을 제어할 수 있는 기능도 제공한다. 콘텐트 캐싱, 트래픽 최적화 기능으로 사용자가 필요한 시점에 중요한 클라우드 애플리케이션 가용성을 보장하고 성능과 용량을 최적화할 수 있다.

신속한 침해사고 대응과 포렌식 분석 지원하는
시만텍 SA

시만텍 SA(Security Analytics)는 네트워크 트래픽 가시성과 보안 인사이트, 실시간 위협 인텔리전스를 통합해 즉각적인 침해사고 대응과 향상된 네트워크 포렌식 분석을 지원하는 솔루션이다. 전체 네트워크 트래픽(패킷)을 수집, 캡처해 실시간 기록하고 분류, 조사함으로써 기업 환경에 침투한 공격을 빠르게 찾아낸다. 현재 네트워크 상황에 대한 컨텍스트 정보와 실행 가능한 인텔리전스를 제공하기 때문에 침해사고 해결에 소요되는 시간을 단축시킨다. 효율적인 포렌식 분석과 증거 추출 기능을 제공하는 SA는 공격 전과 후, 진행 단계에서 어떠한 일이 발생했는지 사건을 재연하고 재구성한다. 보안위협의 출처와 범위, 감염지점을 규명하면서 네트워크 트래픽에 대한 가시성을 제공해 기업은 위협에 노출되는 시간을 최소화할 수 있다.

기업의 중요 데이터 유출을 효과적으로 탐지, 분석해 보호하는
시만텍 DLP

시만텍 DLP(Symantec Data Loss Prevention)는 업계 최고의 데이터 유출 방지 기술을 제공해 기업 내부 기밀 데이터를 효과적으로 모니터링하고 통제할 수 있도록 지원한다. 엔드포인트 기기에서 사용 중인 데이터부터 네트워크를 통해 전송되는 데이터, 클라우드 데이터, 그리고 스토리지에 저장된 데이터까지도 보호하는 포괄적인 DLP 솔루션을 제공하고 있다. 그 중에서도 시만텍 네트워크 DLP(DLP for Network)는 이메일, 웹, FTP, 인스턴트 메신저(IM) 등 다양한 네트워크 통신 프로토콜을 통해 전송되는 중요 데이터 유출을 차단한다. 기업 네트워크 아웃바운드 트래픽을 캡처하고 분석해 중요 콘텐트와 메타데이터를 탐지한다. 모든 네트워크 통신에 대해 패킷 손실없이 심층적으로 트래픽과 콘텐트를 모니터링, 검사하고 분석해 직원이나 파트너에 의해 데이터가 유출되거나 도용되지 않도록 조치한다. 중요한 콘텐트나 메시지를 수정, 제거하거나 리다이렉션하고 차단할 수 있는 기능을 선택할 수 있다.

Symantec

시만텍코리아
서울시 강남구 테헤란로 152
강남파이낸스센터 28층

웹사이트 www.symantec.com/ko/kr
문의전화 02-3468-2026/2000
문의메일 sunhwa_choi@symantec.com

취재 및 제작
Byline Network
byline.network