웹애플리케이션 방화벽의 발달: 서버 보호에서 심층 방어까지

인터넷 기반의 네트워크 공격은 최근 20년 간 크게 정교화됐다. 오늘날의 웹 애플리케이션들은 그 다양성과 양방향성 때문에 보이지 않는 파괴적 사이버 공격의 경로가 되고 있어, 한 때는 유용했던 침입탐지시스템(IDS)과 침입방지시스템(IPS) 솔루션들로는 역부족인 상황이다. 대부분의 기업 네트워크 보안 침해 사고는 웹 애플리케이션에 존재하는 취약점들로 인해 발생한다. 기존의 보안 툴을 사용하고 있는 기업들도 사정은 마찬가지다. 반면, 보안에 주의를 기울이는 기업들은 IDS, IPS 및 기존 방화벽을 웹 애플리케이션 방화벽 솔루션의 신기술로 대체함으로써 이러한 보안 과제를 해결하고 있다.

WAF 1.0

1세대 웹애플리케이션 보안 기술이 IDS/IPS보다 앞선 두 가지 주된 기능은 HTTP 속성(방식, 주소, 파마미터)의 활용과 분석 전 데이터 전환(urlencode, base64)이다. 이 두 개의 기능은 서명 기반 방식을 사용했고, 서버 공격(RCE, Path Traversal, SQL Injection) 차단이 목표였다.

WAF 2.0

AJAX 를 비롯한 웹 2.0 기술 스택과 주요 웹애플리케이션의 폭발적 증가가 WAF 2.0 개발을 주도했다. 웹애플리케이션의 다양성과 복잡성으로 인해 서명 기반 기술로는 기하급수적으로 증가하는 오탐을 처리할 수 없게 되었다.

이에 동적 프로파일링 방식이 도입됐다. 지도적 기계 학습은 사람의 개입을 상당히 요하는 시간 집약적 프로세스였지만 서명 목록을 최적화할 수 있었다.

XSS, CSRF 등의 공격으로부터 사용자를 보호하는 방식도 2세대 WAF 솔루션에서 등장했다.

WAF 3.0

해커들은 서명 분석을 피하기 위해 제로데이 취약점으로 눈을 돌렸다. 이를 방어하기 위해서는 일반 애플리케이션 기능의 모델을 구축하여 비정상적인 행동들을 탐지하면서 동시에 오탐율을 줄여야 했다. 전자동 방식이 등장했으나 기계 학습의 원자료로서의 '클린(clean)' 트래픽이 부재했기 때문에 곧 사라지고 만다. 실질적인 트래픽에는 적법한 쿼리가 악의적인 쿼리와 함께 존재하기 때문에 대부분의 WAF 소프트웨어는 그러한 트래픽을 사용하여 좋은 트래픽과 나쁜 트래픽을 분류할 수 없다.

PT Application Firewall은 은닉 마르코프 모델(Hidden Markov Model) 기반의 사용자 행동 모델을 구축함으로써 혼합된 트래픽을 학습에 적용할 수 있고, 제로데이와 우회 시도를 차단할 수 있다.

새로운 위험 요인들

최신 애플리케이션의 보호는 엄청난 양의 클라이언트-서버 간 통신을 단일 창에서 통합해야 하는 극도로 복잡한 작업이다. 애플리케이션을 '스토어 프론트' 차원에서 보호하는 것으로는 부족하다. 모든 애플리케이션 시스템들과 컴포넌트들 간의 연결 또한 보호되어야 한다. 리테일러를 위한 애플리케이션, 산업 제어 시스템, 온라인 뱅킹, 전자 정부 등은 일반적으로 애플리케이션과 컴포넌트 간의 통신에서 XML 또는 JSON을 이용한다. 따라서, WAF는 XML 메시지에서 승인되지 않은 악의적인 데이터를 식별하며, SOA 호출을 인증하고 프로파일링 해야 한다.

능동적 보호

사용자는 공격을 기다리는 대신, 취약점을 집중적으로 처리할 수 있는 보호 시스템을 사용하는 능동적 방식으로 웹 애플리케이션 보안을 강화할 수 있다. 단순히 트래픽을 지정된 서명 목록과 비교하는 기존 방화벽에서는 불가능한 방식이다. 포지티브 테크놀로지스의 전문가들은 침투테스트 및 기타 기법들에 대한 경험이 바탕이 되어, PT Application Inspector에서 생성된 테스트 익스플로잇을 기반으로 하는 실시간 공격 성공 검증을 위한 동적 스캐닝과 자동 가상 패치 등 두 가지 중요한 취약점 차단 툴을 구현할 수 있었다.

3세대 WAF 솔루션은 비즈니스 로직에 대한 공격(사기 및 애플리케이션 수준의 DDoS) 차단에 중점을 두고, 특정 사용자 세션 내 일련의 이벤트들을 추적하고 재구성하는 사용자 추적 기능을 구현한다.

보안사고 피해규모 1억6천2백만 달러에 육박

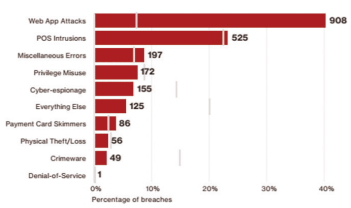
2013년, 미 유통업체 타겟(Target)은 윈도 구버전에서 실행 중이던 결제 시스템이 대규모 해킹에 피해를 입는 사건이 발생했다. 공격자들은 임의의 실행파일 업로드가 가능한 취약한 웹 서비스를 이용하여 POS 단말기들에 접근했다. 19일 간, 해커들은 4천만 개의 신용카드 및 직불카드 번호와 고객 7천만 명의 개인 정보를 유출해갔다. 이 사건으로 타겟은 1억6천2백만 달러 이상의 피해를 입었다.

단 하나의 취약점으로 인한 1억 파운드 규모의 피해액

2015년 10월, 영국의 통신사 TalkTalk에서는 해킹으로 고객 15만 명 이상의 은행 카드 및 개인 정보가 유출되는 사고가 발생했다. 취약한 웹애플리케이션이 원인이 된 당시 사건으로 TalkTalk은 4천2백만 파운드의 피해를 입었고 주주들은 6천만 파운드의 손실을 보고받아야 했으며 고객 약 10만 명이 이탈했다.

위협 #1: 웹 애플리케이션 취약점

Verizon DBIR에 따르면, 2015년 보안 침해 사고의 가장 큰 단일 경로는 웹 애플리케이션 취약점이었다



웹애플리케이션 방화벽의 발달

포지티브 테크놀로지스

설립년도: 2002년

사무실: 9개국에 소재

직원수: 550명 이상

애널리스트: ERP, SCADA, 은행, 통신사, 웹 애플리케이션 및 모바일 애플리케이션 보안 분야 200 여 명의 전문가

비즈니스 협력사: 100여 개의 IT 및 정보보안 통합 업체

기술 협력사: Cisco, HP, Microsoft, Oracle, SAP 등 50여 개의 글로벌 소프트웨어 및 하드웨어 제조사

WAF 360°

대부분의 WAF 솔루션은 웹 애플리케이션을 외부 공격으로부터 보호하는 데 초점이 맞춰져 있다. 그러나 오늘날의 분산식 인프라에서는 총체적인 접근 방식이 요구된다.

종합적 방식의 툴은 사용자와 시스템간 통신을 보호하고, 스마트 데이터 분석 기술을 사용하여 IT 보안 인력의 수동 작업량을 최소화한다. WAF 제품은 안전한 소프트웨어 개발 주기를 확장하고, 가령 웹 서버 업데이트 이후 운영 환경 때문에 발생할 수 있는 취약점들을 차단할 수 있다. 여러 개의 WAF(예: Cisco ACI 이용) 및 오픈 API를 종합적으로 지원하면 데이터 센터와 클라우드 서비스에 요구되는 비용이 절감된다. WAF 360°는 사기 차단 시스템들을 통합하여 데이터 유출 및 사용자 사기를 차단하기 때문에 기업과 정부가 웹 애플리케이션의 코드를 변경하지 않고도 클라이언트 관련 위험을 관리할 수 있다.

이러한 첨단 기술을 활용한 PT Application Firewall은 기업 보안 환경에 있는 모든 취약한 링크들을 처리함으로써 종합적이고 완전한 애플리케이션 보안을 제공한다.

업계에서 인정 받는 PT APPLICATION FIREWALL

가트너는 2015년에 이어 2016년에도 포지티브 테크놀로지스를 매직 쿼드런트 웹애플리케이션 방화벽 부문의 비저너리 기업으로 선정했다. 포지티브 테크놀로지스 PT Application Firewall의 기술 구현을 위한 비전과 역량의 완성도를 인정한 것이다*. PT Application Firewall은 전세계 주요 은행, 통신사, 리테일러, 석유 및 가스회사, 의료 기관, 언론 기관 등의 웹 서비스를 보호하고 있다. 자세한 내용은 af.ptsecurity.com에서 확인할 수 있다.

*가트너, 매직 쿼드런트 웹애플리케이션 방화벽 부문. Jeremy D'Hoinne, Adam Hils, Claudio Neiva. 2016년 7월 19일

포지티브 테크놀로지스

포지티브 테크놀로지스는 취약점 및 컴플라이언스 관리, 보안 사고 및 위협 분석, 애플리케이션 보호 솔루션 등 토탈 기업 보안 솔루션을 제공하는 업계 선도 기업입니다. 고객과 연구에 대한 헌신적 노력을 통해 세계적 분석 기관들로부터 ICS(산업제어시스템), 뱅킹, 통신, 웹 애플리케이션, ERP 보안 분야의 선두주자라는 명성을 얻고 있습니다. 포지티브 테크놀로지스에 대한 더 자세한 정보는 ptsecurity.com 에서 확인할 수 있습니다.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com