FORTINET®

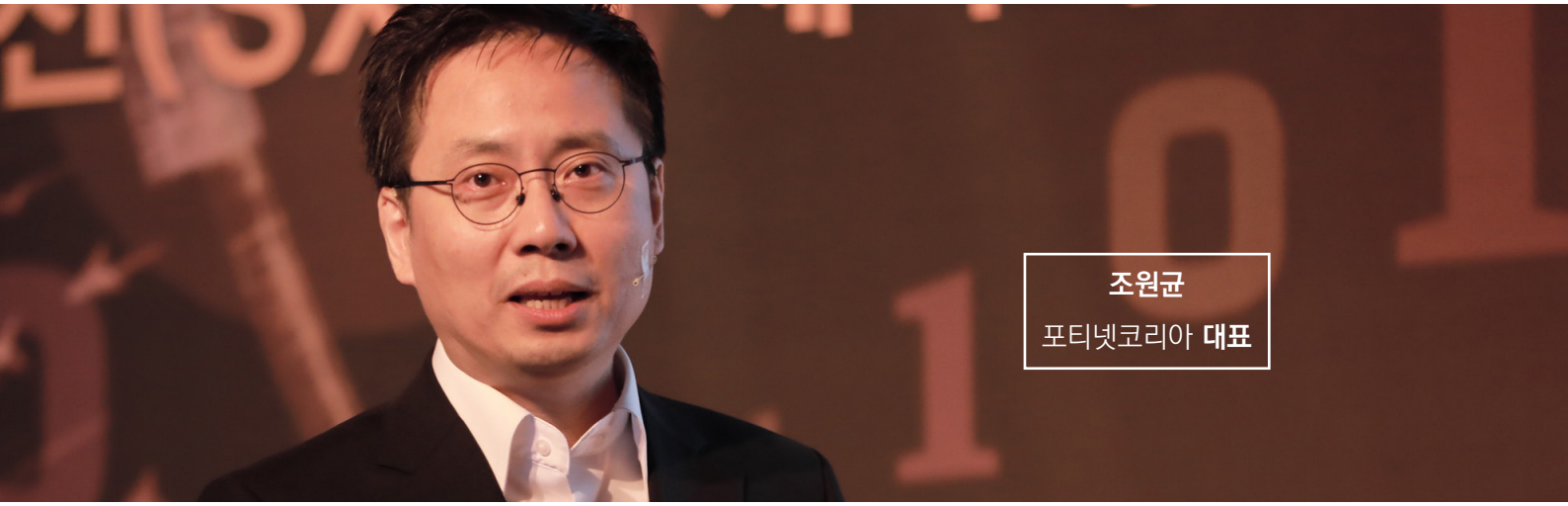
361 SECURITY 2018

디지털 트랜스포메이션 시대, 보안의 혁신을 제시하다

‘시큐리티 트랜스포메이션(SX)’이 필요하다 02
아파치 취약점 익스플로잇 공격과 암호화폐 크립토재킹 공격과 방어 시연 03
진화하는 사이버공격…“한국은 IoT가 위험” 04
패널토의_클라우드 환경에서의 보안 구축 방안 06
차세대방화벽·차세대IPS·SSL방화벽으로 기업 네트워크 보안 강화하기 10
시큐어 SD-WAN, 비용효과적인 지점 보안, 감사 방안 13
가성비 갑, APT 방어 시스템 고도화 14

SPECIAL REPORT

BylineNetwork



'시큐리티 트랜스포메이션(SX)'이 필요하다

디지털 트랜스포메이션 시대다. 전세계 기업들은 디지털 기술을 모든 사업영역에 통합시키는 '디지털 혁명'에 나서고 있다. 조직과 사업을 운영하고 고객들에게 가치를 제공할 수 있는 방법론이 근본적으로 변화한다.

디지털 혁명을 이루기 위해 필요한 핵심요소이자 기본은 기술이다. 물론 기술만 있다고 성공할 수 있는 것은 아니다. 기술 외에도 관리와 리더십 역량도 필요하다.

사물인터넷(IoT), 인공지능(AI), 클라우드 같은 기술을 활용하고 통합적으로 구현해 새로운 사업 패러다임을 창출할 수 있어야 한다.

무엇보다 기업이 성공적으로 디지털 트랜스포메이션 하기 위해서는 '데이터'가 매우 중요하다. 이제는 과거와는 달리 데이터가 '힘'이자 '전부'인 시대가 됐다.

갈수록 더 많은 데이터를 확보하기 위한 방법론이 모색되고 있지만, 많은 데이터를 확보하는 길을 열면 열수록 데이터 노출, 침해가 발생할 수 있는 길과 표면은 더 넓어진다는 아이러니한 상황이 발생한다. 그 점에서 데이터는 '양날의 검'이기도 하다.

그 이유로 디지털 혁명의 걸림돌이 '보안'이라는 말도 나오고 있다.

성공적인 디지털 트랜스포메이션을 위해서는 이제 보안도 트랜스포메이션이 필요하다.

어떠한 디바이스, 시스템, 클라우드에서도 빈틈없는 보안이 구현돼야 한다. 단시간에 이뤄질 수는 없겠지만 마라톤 경주를 한다는 마음가짐으로 나아가야 한다.

이를 위해 포티넷은 시큐리티 패브릭 아키텍처로 광범위하고 통합돼 있으면서도 자동화된 새로운 보안 아키텍처를 제시한다.

포티넷 시큐리티 패브릭은 ▲네트워크 보안(차세대방화벽, UTM)부터 ▲보안관제센터(SOC)/네트워크 관제센터(NOC)용 보안정보이벤트관리(SIEM) ▲클라 우드 보안 ▲웹 애플리케이션 보안 ▲이메일 지능형위협보 호(ATP) ▲ATP를 위한 샌드박스 ▲사용자 접속 보안(NAC, 무선AP보안, 보안스위치) ▲엔드포인트 보안(EPP, EDR) ▲데브옵스를 위한 오케스트레이터 연동용 API까지 전 영역을 지원한다.

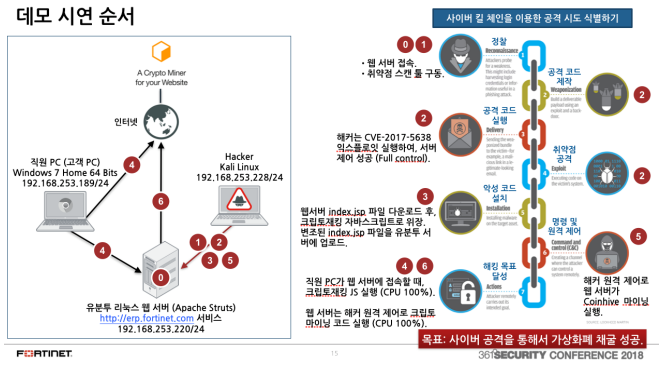
그 중심에는 '포티게이트'의 '포티운영체제(FortiOS)'와 위협 인텔리전스가 있다.

포티넷은 시큐리티 패브릭을 기반으로 기업들이 시큐리티 트랜스포메이션을 위한 보안 플랫폼을 전방위로 지원하고 있으며, 국내외 다양한 레퍼런스를 확보하며 확대하고 있다.By

아파치 취약점 익스플로잇 공격과 암호화폐 크립토재킹 공격과 방어 시연

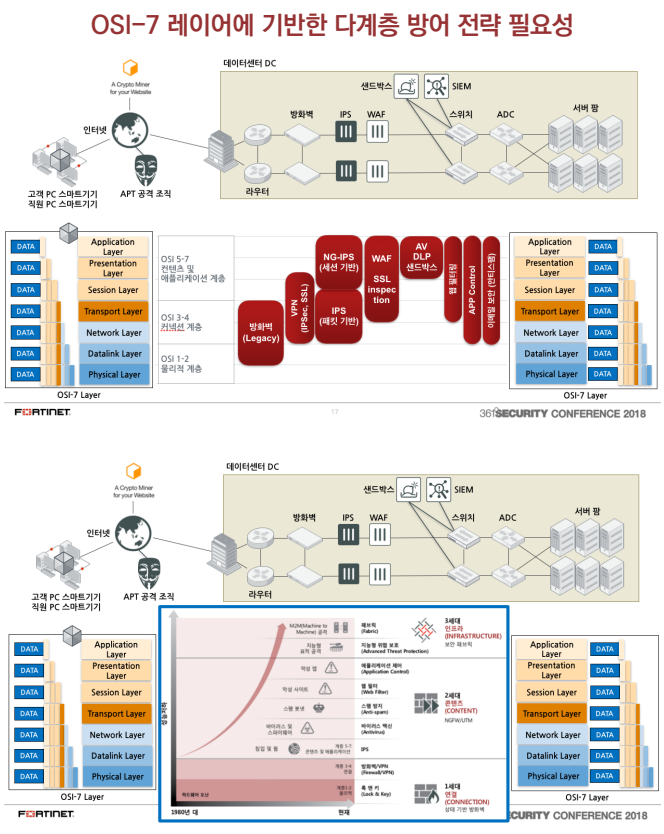
포티넷은 361° 시큐리티 행사에서 매년 화두가 됐던 주요 사이버보안 사고와 관련 라이브 데모를 진행해 왔다.

2018년 행사에서는 이퀴팩스(Equifax) 해킹 사건의 원인이기도 했던 웹 애플리케이션 플랫폼인 아파치 스트럿츠 취약점 익스플로잇의 공격 방법과 암호화폐를 탈취하는 크립토재킹의 침투 과정을 시연했다.



데모시연을 담당한 배준호 포티넷코리아 이사는 최신 사이버공격에 대한 가장 효과적인 방안으로 '다계층(Multi-Layer) 기반 방어 전략과 포티넷 시큐리티 패브릭 솔루션'을 제시했다.

또한 암호화폐 관련 최신 크립토재킹 사이버공격 대비 방안과 함께 '포티아이솔레이터(FortiIsolator)'와 '포티디셉터(FortiDeceptor)' 솔루션을 제안했다. By



포티넷의 연도별 사이버보안 사고 관련 데모 시연

연도	데모 시연 주제
2012	DoS & Website defacement attacks
2013	MITM, SSL Strip- steal facebook user/password even with HTTPs
2014	HeartBleed, CVE 2014-0160- one of the biggest internet vulnerability
2015	랜섬웨어 그리고 무선 와이파이 twin AP 해킹 시연
2016	Spear-phishing and Remote Access Trojan (RAT)
2017	IoT 사물인터넷 기기 해킹, 워너크라이 랜섬웨어 감염 시연
2018	Apache Struts 취약점 공격 그리고 크립토 재킹 공격 시연

진화하는 사이버공격… "한국은 IoT가 위험"

모든 범죄는 진화한다. 사이버범죄도 마찬가지다. 금전을 노린 범죄자들의 사이버공격은 점점 진화하고 있다. 이들은 심지어 첨단기술까지 무장해 나간다.

지금까지 사이버공격은 계획침투→감염→정보유출 등의 단계를 거쳤다. 이 때문에 공격을 위해서 수개월의 시간이 필요했다. 그러나 이제는 이와 같은 공격의 물리적 경계도 사라지고 있다. 보안 침해를 일으키기 위한 시간이 더 짧아졌다. 예를 들어 오토익스플로잇이라는 프레임워크가 있는데, 이는 최초 사물인터넷(IoT) 검색 '쇼단(shodan.io)'의 취약점을 자동으로 찾아내서 공격한다.

문제는 한국이 이런 공격에 더 취약하다는 것이다. 데릭 맨키 포티넷 글로벌 보안 전략가는 "한국 네트워크 공격 대다수가 IoT 기기에 집중돼 있었다"고 전했다. 라우터, CCTV, DVR 등이 대표적이다. 공격자들은 이런 기기에 인증받은 키값을 넣고 원격에서 실행시킨다.

데릭 맨키 보안전략가는 "IoT 타깃 공격은 감염대상 기기가 많고 관리가 어렵기 때문에 초보적인 방식의 공격이라도 대응이 쉽지 않다"며 "제로 트러스트 정책을 기반으로 모든 네트워크 접근을 감시하고 통제하는 정책이 필수"라고 말했다.

그에 따르면 ▲자동화된 패치관리 시스템을 이용한 취약점 제거 ▲네트워크 분할과 접근제어 ▲보안정보이벤트관리시스템(SIEM) 등을 이용한 위협관리 ▲IT 전반의 취약점 점검과 보안 위협 감시 등의 활동이 반드시 진행돼야 한다.

데릭 맨키 보안전략가는 아울러 포티넷이 최근 발표한 '글로벌 위협 전망 보고서'의 주요 내용을 공개했다.

이에 따르면, 올해 2분기 2만4000여개의 멀웨어 변종이 나타났고, 약 5000개의 멀웨어 패밀리가 탐지됐다. 암호화폐 탈취를 목적으로 한 크립토재킹 멀웨어가 그 중 23%에 달했다.

랜섬웨어는 갠드크랩(GandCrab)이 여전히 기승을 부리고 있으며, 개발조직과 유포조직이 분리되는 특징이 나타났다. 데릭 맨키 보안전략가는 "랜섬웨어 개발조직과 유포조직이 범죄 수익을 6:4로 나누고 있으며, 애자일 개발방식을 이용해 악성코드를 쉽게 개발하고 효율적으로 재사용하고 있다"고 설명했다.

7230개의 고유한 취약점이 탐지됐고, 이는 각 기업마다 811개의 취약점이 있다는 것을 의미한다. 96%의 기업이 서버에서 취약점이 있다.

봇넷의 경우, 265개의 고유한 봇넷이 발견됐다. 기업마다 1.8개의 봇넷이 있다. 특히 미라이(Mirai) 봇넷 변종인 위키드(WICKED)는 보안 패치가 안된 IoT 장치를 타깃으로 했으며, 스카다(SCADA)와 산업제어시스템(ICS) 환경을 타깃으로 삼는 가상사설망(VPN)필터는 데이터 유출뿐 아니라 장치를 작동하지 못하도록 할 수 있어 주요 위협으로 부상했다. 아누비스(Anubis) 변종의 경우, 랜섬웨어, 키로거(keylogger), 원격관리툴(RAT)

Volume of detections events South Korea vs APAC(Q4 2018)

Threat Type	Total in South Korea (million)	Total in APAC (million)	Percentage
Virus	0.1	5,017	2%
IPS	2113	58,786	3.6%
App	25255	431908	5.8%
Botnet	2	263	1%
Endpoint	0.007	0.213	3.2%

기능, 단문문자메시지(SMS) 가로채기(interception), 화면 잠금, 착신 전환 기능 등 몇 가지 기능이 추가됐다.

데릭 맨키 보안전략가는 "사이버공격자들의 공세가 더욱 강화되고 있으며, 점점 더 많은 공격자들이 그들의 툴 세트를 자동화하고, 잘 알려진 익스플로잇의 변종을 만들어내고 있다"면서 "또한 그들은 희생양을 찾기 위해 다수를 공략하는 접근보다는 보다 정확하게 타깃을 선별하고 있다"고 경고했다.

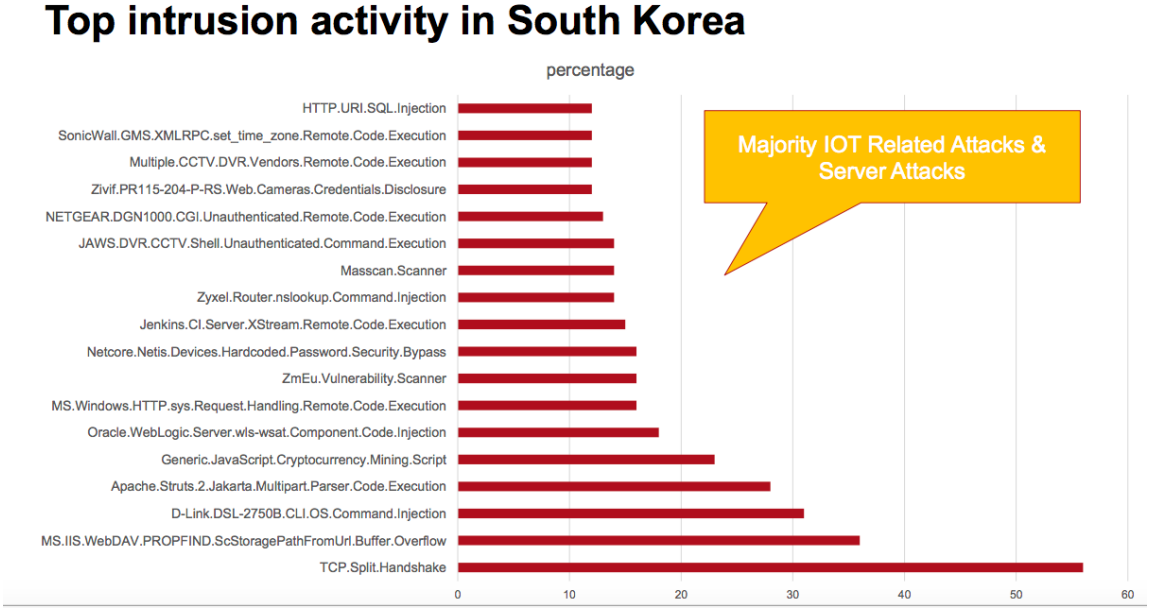
그는 "기업들은 공격자들의 이 같은 전략에 대응하기 위해 새로운 보안 전략을 수립해야 한다"면서 "자동화된 통합 방어 체계를 활용해 빠른 공격 속도 및 확대된 공격 규모의 문제를 해결하고, 고성능 행동 기반 탐지 기법을 활용해야 하며, 인공지능(AI) 기반 위협 인텔리전스 통찰력을 통해 중요한 취약점을 패치하는데 주력해야 한다"라고 말했다.

지난 분기 한국에서는 바이러스가 10만건이 발견됐고, 네트워크 침입 시도가 21억 1300만건 있었다. 애플리케이션 공격 시도 252억5500만건, 봇넷 2건, 엔드포인트 공격 시도 7000건 있었다.

한국에서는 아파치 스트러츠 등 알려진 취약점을 겨냥한 익스플로잇과 자바스크립트 기반 크립토재킹이 가장 많이 탐지됐다. 그 다음으로 디링크(D-Link), 링크시스(Linksys) 무선 라우터 장비 취약점을 악용한 익스플로잇이 보고됐다. 더불어 보안USB를 표적으로 한 틱(Tick) 공격과 이메일을 통한 피싱 공격인 '스카크래프트(Scarcraft)'도 발견됐다.

특이할 점은 한국에서의 공격 시도 상당수가 기술 관련 기업을 대상으로 했다는 점이다. 인터넷 포털사, 게임사, 커머스 회사 등이다. 심지어 보안관제서비스 업체도 한국에서는 공격자들의 주요 타깃이 됐다.

데릭 맨키 보안전략가는 "한국에서 발생하는 위협 중 봇넷, 마이크로소프트(MS) 워드 문서 파일을 이용한 멀웨어 유포 등을 주목해봐야 하며, 특히 틱 공격과 스카크래프트 공격은 주요 기관을 노리는 타깃 공격일 수 있으므로 예의주시하면서 분석하고 있다"고 밝혔다. By



패널토의

클라우드 환경에서의 보안 구축 방안

패널 / 최주열 이사 (한국마이크로소프트)
장노륜 매니저 (네이버비즈니스플랫폼)
이수형 상무 (메가존)
권용 차장 (안랩)
최광순 이사 (포티넷코리아)

사회 / 이유지 기자 (바이라인네트워크)

클라우드는 대세다. 우리나라는 미국이나 일본 등 해외에 비해 클라우드 확산이 늦긴 했지만 이제 웬만한 기업들은 클라우드 서비스를 이용하고 있다.

정부에서 클라우드 활성화 정책을 시행하면서 이제 공공기관에서도 민간 클라우드 서비스를 이용할 수 있다. 보수적인 금융권에서도 비중요처리시스템에만 제한적으로만 허용했던 것에서 탈피해 앞으로는 개인신용정보, 고유식별정보를 처리하는 금융사 정보시스템도 클라우드를 사용할 수 있게 된다. 바야흐로 클라우드가 본격 확산되는 시대다.

많은 기업들이 데이터센터를 가상화해 프라이빗 클라우드 환경을 운영하고 있고, 또 퍼블릭 클라우드도 사용하고 있다. 하이브리드 클라우드 환경을 이용하고 있는 것. 여기서 나아가 여러 퍼블릭 클라우드 서비스를 사용하는 멀티클라우드 시대로 진입하고 있다. 그럼에도 불구하고 클라우드 보안에 대한 우려는 여전한 상황이다.

클라우드는 비용절감, 비즈니스 민첩성 향상과 같은 혜택을 제공하지만 보안 문제도 빠지지 않고 함께 얘기된다. 초창기에는 보안 문제 때문에 클라우드 서비스를, 특히 퍼블릭 클라우드를 사용하지 않으려는 경향도 있었다.

그러자 클라우드 서비스 제공업체들은 인프라에 있어서는 오히려 더 안전하다고 강변했다. 그렇다고 이들 업체들이 클라우드 보안을 모두 책임져주는 것은 아니다.

클라우드 서비스를 보다 안전하게 이용하기 위해 고려해야 할 보안 방안은 무엇일까.

과연 클라우드 서비스는 자체적으로 운영관리하는 인프라 보다 더 안전한가.

최주열 이사_클라우드 서비스가 절대적으로 안전하다는 얘기는 온당치 않을 것이다. 누군가는 뚫으려 하고 상대 쪽에서는 막으려는 조치를 한다. 보안위협을 막을 수 있는 기반 기술과 더불어 각 국가나 지역에 타당한 현재 규제에 맞출 수 있는 제도적 보안장치를 바탕으로 보안을 강화해 나갈 수 있다. 마이크로소프트를 비롯해 대부분의 퍼블릭 클라우드 서비스 업체들은 각국 정부나 산업의 표준 인증에 대한 준비가 돼 있다. 완벽한 서비스수준협약(SLA)은 쉽지 않기 때문에, 보완적 장치로 제도적 인증이 필요하다.

퍼블릭 클라우드 서비스 제공업체들이 채택하는 보안정책, '책임공유' 모델이란.

장노륜 매니저_클라우드에는 클라우드 서비스 제공업체의 관리영역 아래에 있는 인

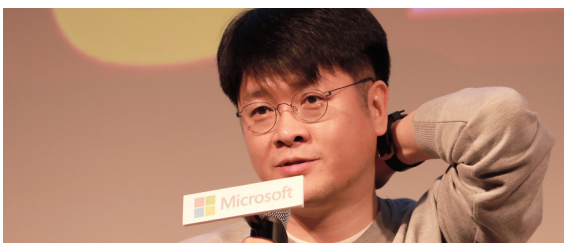
프라, 고객 관리영역에 속하는 인스턴스, 데이터가 있다. 고객의 인스턴스와 데이터는 사업자가 볼 수 없다. 때문에 사업자 관리영역은 사업자가 관리하고, 고객 책임하에 있는 인스턴스와 데이터는 고객들이 잘 관리하는 것이 '책임공유' 모델이다. 이 두 가지가 잘 공존해야만 보안이 잘 될 수 있다. 어느 한 부분이 소홀해진다면 보안의 벽은 약해질 수 있다.

클라우드 서비스를 이용하는 기업들, 보안 담당자들이 클라우드 보안을 구현하는데 있어 어려워하는 점은.

이수형 상무_많은 분들이 아마존웹서비스(AWS)를 사용하면 AWS의 인프라에서 모든 보안을 제공할 것이라고 생각한다. 이는 잘못된 추정이다.

클라우드 컨설팅은 마이그레이션(이전)부터 현재 고객이 가진 보안 취약점과 보안 프레임이 무엇인지에서 출발한다. 클라우드를 사용하기 전에 애플리케이션단 마이그레이션에 대한 재설계가 필요하다. 클라우드는 마법의 양탄자가 절대 아니다. 클라우드를 사용하기 위해서는 많은 공부가 필요하다. 데브옵스(DevOps)팀들은 지난 5년에서 10년 동안 많은 실수를 하고 교육을 통해 배워오고 있다. 보안팀은 약간 뒤처진 부분이 있다.

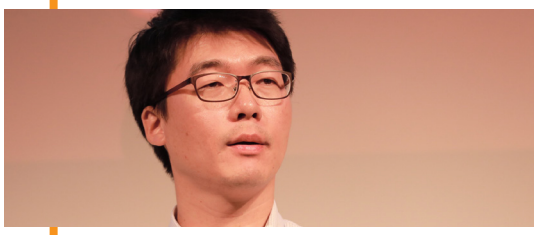
권용 차장_많은 분들이 기존(레거시) 환경에 적용해온 보안체계를 그대로 가상 환경에 똑같이 적용하려 한다는 점에서 어려운 점이 나타난다. 대개 서비스를 다 구성한 뒤에 보안관제서비스 업체나 보안 솔루션 업체에 연락을 한다. 이 경우 솔루션 가용성에 문제가 있다. 또 많은 보안 솔루션이 클라우드 제너레이션, 또는 클라우드 네이티브라고 이야기하지만 실제로 레거시 환경에서 제공되는 모든 기능을 지원하지 못한다. 클라우드 서비스를 잘 활용하려면 처음부터 클라우드와 보안 아키텍처를 함께 고려해 설계하고 구성해야 한다.



기존 온프레미스 환경에서 적용해온 보안체계를 그대로 클라우드에 적용하려는 접근방식은 문제인가.

이수형 상무_미국과 한국에서도 서비스하고 있는 한 유명 스트리밍 회사와 일했다. 이 회사는 데브옵스와 보안을 분리하지 않는다. 시스템 자체를 디자인할 때부터 보안팀이 함께 참여한다. 애플리케이션 아키텍처를 디자인하지만 각각의 아키텍처와 파이프라인에서 필요한 보안을 함께 디자인한다. 이를 고려하는 것이 중요하다.

또 이 회사 담당자들은 다들 매일 코딩을 하고 있다. 개발자나 운영 담당자 뿐 아니라 보안 담당자들도 매일 코딩한다. 그래야 데브옵스가 구현되고 데브섹옵스(DevSecOps)가 구현될 수 있다. 보안팀이 운영팀, 개발팀과 자유롭게 이야기하게 되고 이같은 문화가 정착되면 자연스럽게 데브섹옵스가 가능해질 것 같다.



빠르게 돌아가는 데브옵스 환경에서 보안팀이 뒤처지지 않고 데브옵스팀과 보조를 맞추기 위해서는 어떻게 해야 하나.

이수형 상무_올 초 어느 자리에서 '데브섹옵스'를 얘기했더니 어느 보안담당자가 이런 얘기를 하더라. 지금 보안팀은 두 세 명 뿐이고, 이들이 담당하고 있는 보안 솔루션이 20개 이상인데 어떻게 운영과 개발까지 할 수 있겠느냐고.

데브섹옵스는 보안담당자가 개발해야 한다는 의미가 아니다. 개발팀이 개발하고 운영팀이 운영해야 한다. 다만 세 팀이 동일한 언어를 갖고 통신할 수 있어야 한다. 데브옵스를 구현할 경우 시스템 간, 서비스 간에 애플리케이션프로그래밍인터페이스(API)로 통신해야하는 마이크로서비스아키텍처를 구현해야 한다고 제시한다. 이는 팀과 부서, 조직 차원에서도 이뤄져야 한다. 보안팀도 마찬가지다. 보안 프로세스도 자동화하고 진행된 모든 것들이 정보(knowledge)로 남겨져야 하는 것이 우선이다.

클라우드 서비스 제공업체 보안담당자 입장에서 어려운 점이 있거나 경험담을 소개한다면.

장노륜 매니저_사용자 고객들이 클라우드 서비스를 도입할 때 염려하거나 어려워하는 점은 두 가지다. 하나는 책임공유 모델 관련해 사업자가 관리하는 영역을 사용자가 투명하게 들여다볼 수 없다는 점이다. 예를 들어 IaaS 도입했는데 서버나 네트워크, 스토리지 레벨을 사용자가 온프레미스에서 장치를 운영하듯이 들여다볼 수 없기 때문에 사업자가 정말 잘하고 있는지, 믿고 써야되는지 염려한다. 두 번째는 온프레미스 환경에서 썼던 보안 아키텍처, 보안 방법론을 그대로 클라우드에 적용하려고 한다는 점이다. 사업자 의존성이 있기 때문에 이를 그대로 전환할 수 없다는 점에 염려한다.

기존 아키텍처를 클라우드상에 그대로 가져오는 것에 한계가 있긴 하지만 사업자들은 대체제를 많이 준비하고 있다. 마이그레이션 아키텍처 컨설팅을 받거나 서비스를 도입할 때 대체제가 무엇인지 서비스 사업자가 제공할 수 있는 영역도 꼼꼼하게 따져 맞는 서비스를 선택하는 것이 중요하다.

최주열 이사_사용자 환경마다 나름 특화된 부분도 있지만 공통된 환경도 있다. 100% 기존에 사용하던 방식을 클라우드로 옮긴다는 것이 가능할 수도 있지만 중복투자, 중복된 기술을 도입하게 될 수 있다는 점을 고려해야 한다.

기업 규모가 작으면 작을수록 보안담당자는 소수이거나 없을 수도 있다. 이 경우 특정 벤더의 기술에 전적으로 의존하게 된다. 클라우드로 옮기는 것을 먼저 고민하는 것보다는 그 전에 기술 내재화 관점에서 발생할 수 있는 장점과 단점을 고려했으면 한다.

대부분의 클라우드 환경은 기본으로 마이그레이션 환경 지원도구를 제공한다. 국내에서만 사업하지 않고 해외 사업까지 하는 경우엔 각 국가와 대륙에서 요구하는 보안 인증체계가 다른 부분이 있다는 점도 고려해야 한다. 보안을 누군가에 의존한다는 것보다는 이미 선결돼 있는 인증 시스템 내에서 책임을 나눠지거나 일부분을 클라우드 사업자가 맡는다는 관점에서 보안 접근방식을 채택하는 것도 나쁘지 않을 것이다.

하이브리드 클라우드 서비스를 사용하는 것을 넘어 멀티클라우드 환경에서 보안의 어려움은 가중되는가.

장노륜 매니저_멀티클라우드 채택시 나타나는 가장 큰 어려움도 기존의 온프레미스 환경의 보안정책을 똑같이 구축할 수 없다는 점이다. A사업자, B사업자가 제공하는 보안서비스가 다 다르다. 온프레미스에서 쓰던 것을 A사업자에 적용할 때, B사업자에 적용할 때 모두 달라진다. 사용자 입장에서 고려해야 할 사항이 많아진다. 서비스형 인프라(IaaS)도 그렇지만 IaaS 외에 서비스형 플랫폼(PaaS), 서비스형 소프트웨어(SaaS)까지 동시에 여러 클라우드 사업자 서비스를 썼을 때 애플리케이션과 서비스까지 고려해야 할 사항이 많다. 클라우드를 선택할 때 내가 지원받을 수 있는 정책과 기능을 짚어봐야 한다.

이수형 상무_앞서 언급한 스트리밍 업체의 경우, 가상머신(VM) 기반으로 서비스를 하고 있다가 도커 컨테이너 오케스트레이션 솔루션이 올라오면서 개발자가 코드 개발한 후 커밋하게 되면 운영팀에서 이를 가상머신으로 올릴 것인지, 컨테이너로 올릴 것인지 결정한다. 이와 함께 보안 태그도 같이 붙는다. 요구되는 보안레벨이 다름에도 구현한다. 컨테이너는 멀티클라우드에 쉽게 접근할 수 있는 방법이다. 혹시 모를 상황에 대비해 클릭 한 번으로 전환할 수 있도록 대비해놓은 것이다. 이 역시도 사람이 클릭하는 것이 아니라 서비스 품질이 떨어지기 시작하면 자동으로 VM이나 컨테이너를 늘려 자동으로 서비스 품질을 유지한다. 하나의 클라우드 서비스뿐 아니라 멀티클라우드 서비스까지 같이 테스트가 진행된다. 이 부분을 고려해볼 필요가 있다.

클라우드 서비스를 이용할 때 기업들이 가시성과 통제력을 잃어버린다는 우려가 있다. 이에 대한 방안은.

최광순 이사_클라우드 보안을 따져보면, 클라우드 플랫폼에서의 보안, 클라우드 플랫폼 위에서 제공되는 서비스단의 애플리케이션과 데이터 보안으로 구분해볼 수 있다. 가트너 보고서에 보면, 2020년까지 클라우드 보안 사고가 난다면 그 원인의 99%가 고객의 실수일 것이라고 전망돼 있다. 이는 클라우드 플랫폼은 99% 안전하다고 볼 수 있다는 것이다. 서비스나 데이터, 애플리케이션이 안전하지 않다는 전제에서 시작해야 한다.

SaaS 애플리케이션은 클라우드 보안에 있어 넘버원 이슈다. 사용자들이 직접 액세스하기 때문에 클라우드접근보안중개(CASB)와 같은 서비스가 필요하다. CASB는 API를 통해 가시성을 확보할 수 있도록 해준다. 사용자 행위나 컴플라이언스 준수 여부를 모니터링하고, 로컬에서 사용하고 있는 지능형위협보호(ATP), 데이터유출방지(DLP) 등 다양한 솔루션을 그대로 적용할 수 있게 한다.

포티넷도 '포티CASB' 솔루션을 갖고 있고, 시중에 여러 CASB가 제공되고 있다. CASB를 도입할 때에는 사용하고자 하는 지원하는 SaaS가 무엇인지 따져봐야 한다.

클라우드 서비스 제공업체들이 자체적으로, 또는 보안업체들과 애플리케이션단 보안을 강화하기 위해 제공하고 있는 기술방안은.

최주열 이사_보통 물리적 서버가 다운타임을 갖게 되는 가장 큰 원인은 팬이다. 그 다음은 하드디스크, 전원공급장치다. 이 세 요건을 뺀 나머지 가장 큰 이유는 사람의 실수다.

마이크로소프트 애저의 경우, 스토리지는 99.99%, VM은 99.95%를 SLA로 정하고 그에 상응하는 비용상계도 명시돼 있다. 하지만 뚫린 이후에 무슨 일이 벌어질 경우, 로컬에서 사용하는 파워포인트, 엑셀에서 유출된 경우 클라우드 사업자가 책임져주지는 않는다. 다만 이를 미리 미연에 방지하라고 마이크로소프트는 RCA(Root-Cause Analysis)을 제시하고 있다.

대형 네트워크 공격이나 특정 경로를 장악한 공격이 발생할 경우 대부분 사건이 발생하기 전이나 발생하고 있는 중간에 RCA 리포트가 나간다. 문제는 그 때 기업에서 패치하지 않는다는 것이다. 사업자는 적시에 리포트를 제공하기 때문에 고객이 이를 받아들여줘야 한다. 휴먼에러를 방지하기 위한 것이다. RCA는 여타의 클라우드 서비스 제공업체들도 제공할 것이다.

클라우드에서의 보안위협은 외부의 공격보다는 기업 관리자, 내부의 실수로 인한 위협이 더 큰 것인가.

이수형 상무_데브섹옵스를 잘 운영하고 있는 그 스트리밍 회사도 작년에 큰 보안 문제가 발생했다. 보유하고 있던 콘텐츠를 해커가 미리 가져가 일정 금액을 제공하지 않으면 이를 공개하겠다고 협박했다. 이는 데브섹옵스 프로세스의 문제가 아니었다. 이 회사는 굉장히 많은 회사들과 일을 한다. 내가 가진 보안 레벨이 많은 자회사나 파트너사들도 갖고 있을 것이라고 추정하는 것은 문제다. 해커가 들어와 콘텐츠를 훔쳐갈 수도 있지만, 더 중요한 것은 내 기업과 자회사·파트너가 같은 보안수준을 유지하는 것이다. 강력한 보안접근방식, 보안정책을 운영하는데 있어 보안담당자 분들이 고민이 많은 것 같다.

사람의 실수나 부주의로 인한 보안 문제를 보안기술뿐 아니라 보안관제서비스를 통해서도 보완할 수 있을 것이다. 클라우드 보안 관제서비스 필요성과 효과는.

권용 차장_보안관제서비스의 필요성은 차에 비유할 수 있다. 차만 좋다고 운전을 잘하는 것은 아니다. 운전자의 기술과 경험이 중요하다. 보안관제서비스는 전문성을 제공한다. 보안담당자의 수는 적은데 관리해야 하는 보안제품 수는 많고, 공격은 계속 새롭게 바뀐다. 관제서비스 입장에서 고객이 늘면서 관제인력만 늘릴 수 없어 정책을 자동화하거나 오케스트레이션 툴을 이용해 다양한 정보를 한 번에 받아 분석가들이 티켓 처리 시간을 계속 효율화시키는 방안을 계속 고민하고 있다.

장노륜 매니저_네이버 클라우드 플랫폼도 시큐리티 모니터링 서비스를 제공하고 있다. 한 가지 어려운 점은 서비스 받는 고객들은 사업자들이 A부터 Z까지 다 해줄 것으로 기대한다는 것에 있다. 하지만 판단의 결정권은 고객들에게 있다. 보안관제서비스를 제공할 때 서비스 업체는 공격 발생시 '공격이라고 90% 이상 판단된다, 이 공격을 막을까요' 라는 리포트를 고객에게 제공한다. 유효한 공격인지 판단해 '막아 달라' 또는 '예외해 달라'는 요청은 고객이 해야 한다.

이것만은 꼭 기억하자!

최주열 이사_퍼블릭 클라우드 서비스 업체 입장에서 '믿고 맡겨라' 라는 말씀을 드리고 싶다. 결국 언젠가는 기업의 환경에 기술 내재화를 해야 한다. 보안에 가장 우선되는 문제는 일단 믿고 맡기고, 그 사이에 또 다른 기술을 내재화 시키고, 그 다음 단계로 나아갔으면 한다.

장노륜 매니저_전통적인 IT아웃소싱할 때 서면계약서 검토를 거친다. SLA를 검토한다. 퍼블릭 클라우드를 쓸 때는 계약과정을 거치지 않는다. 이 부분을 많이 간과한다. 이용약관 동의는 계약과 동일한 행위다. 이 안에 사용자 고객분들이 받을 수 있는 서비스 범위, 사업자 면책범위 모두 나열돼 있기 때문에 이용약관을 꼼꼼히 살펴보길 권고한다.

이수형 상무_자동화를 강조했다. 보안팀에서는 자동화가 생소할 수 있지만, 이는 꼭 혼자서 해결하지 않아도 가능하다. 국외산 클라우드 서비스 제공업체들, 파트너인 메가존도 이 부분을 많이 고민하고 있다. 절대 혼자서 싸운다고 생각하지 말고 도움드릴 수 있으니 함께 했으면 한다.

권용 차장_일단 많이 써봤으면 좋겠다. 6개월 전에 미팅하고 다시 만났는데 클라우드에 대한 이해도에 변화가 없는 경우를 많이 봤다. 보안 솔루션 역시 인라인, 에이전트 형태 모두 다르다. 레거시 환경에서 제공되던 보안 기능도 다 지원되지 않는 기능이 있고, 클라우드 서비스에서 대체 가능한 방법도 있다. 경험해보는 것이 중요하다.

최광순 이사_퍼블릭 클라우드 도입을 고려하신다면 업무 워크로드를 마이그레이션하게 된다. 이 경우 공격면이 증가한다. 이 모든 것을 커버해줄 수 있는 클라우드 보안업체에 컨설팅을 받는 것이 중요하다. 포티넷은 마이크로소프트 애저, 구글, 알리바바, 오라클, IBM, 네이버까지 모든 클라우드 플랫폼을 지원한다. 제품들도 다양하게 구비돼 있기 때문에 적절히 고려할 필요가 있다. By

차세대방화벽·차세대IPS·SSL방화벽으로 기업 네트워크 보안 강화하기

박현희 포티넷코리아 부장

기업 네트워크 보안의 핵심 '차세대방화벽'

기존 방화벽은 애플리케이션 인지능력이 떨어진다. 기존 방화벽은 IP와 포트 기반으로 트래픽을 처리하는 방법인데 진화한 애플리케이션은 특정 IP와 포트에 고정되지 않는다. 웹에서의 위험성도 증가한다. 각종 악성 웹사이트, 바이러스, 웜, 스팸메일 링크 등을 통해 웹에서 감염이 되는 문제도 있다.

기존 방화벽은 통합된 보안 기능을 갖고 있지 않다. 방화벽에 침입방지시스템(IPS)이나 안티바이러스 기능을 통합할 경우 보안 효과가 극대화되지만 이러한 기능이 없고, 진화하는 지능형지속위협(APT)이나 제로데이(Zero-day) 취약점을 방어할 수 없다. 일반 방화벽은 앱을 볼 수 없으므로 현 보안 상황에 대한 가시성 역시 부족하다. 따라서 차세대 방화벽에 대한 요구가 높아지고 있다.

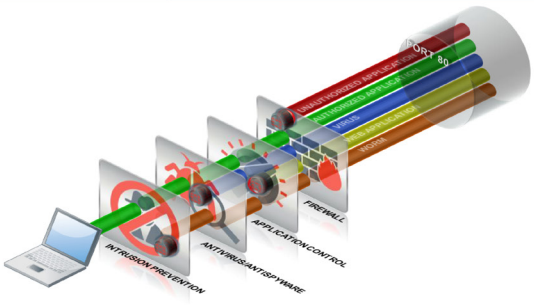
최근 분산된 보안 기능 통합, 새로운 위협 환경에 대한 대응, 데이터 유출과 보안 공격의 감소 등 여러 이유로 차세대 방화벽에 대한 요구가 높아졌다. 가트너는 2016년 일반 방화벽 대비 사용비율이 50% 수준인 차세대방화벽(NGFW)이 오는 2019년 90%까지 늘어날 것으로 전망했다.

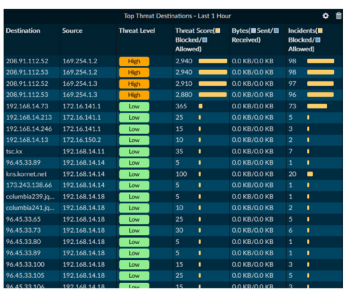
차세대방화벽은 일반 방화벽에 애플리케이션 컨트롤, IPS, 웹 필터링, 안티바이러스, SSL 트래픽 검사(Secure Sockets Layer inspection), ID 기반 방화벽을 통합한 개념이다. 그렇다면 NGFW 도입 효과는 무엇일까?

차세대방화벽 도입 대신 여러 장비로 보안을 구현할 수도 있다. 그러나 이 경우 네트워크 보안이 매우 복잡해진다. 차세대방화벽은 원포인트 솔루션으로 구성이 간단하고 행위분석 기반인 지능형위협보호(ATP) 솔루션이 통합되므로 깔끔하게 구축을 완료할 수 있다.

기존 방화벽의 한계는?

통합 보안 기능 부족	• 방화벽에 IPS와 Anti-Virus 기능을 통합할 경우 보안효과 극대화 • 진화하는 APT 및 Zero-day 취약점에 대한 방어 기능 필요
트래픽에 대한 가시성	• SSL을 이용한 암호화된 트래픽에 대한 가시성 제공 불가 • 어플리케이션 레벨의 실시간 트래픽 정보와 실시간 위협정보 제공 불가





차세대방화벽 도입시 고려사항

가트너 10대 전략기술 트렌드를 보면 2014년 이전까지는 보안 관련 내용이 없었다. 2015년 최초로 등장했고 2016년부터 공통적으로 적응형 보안 아키텍처(The Adaptive Security Architecture)가 등장하고 있다. 보안 아키텍처는 예측, 예방, 탐지와 대응 네 부분으로 구성돼 있다. 대부분의 기업들이 채용하고 있는 방식이다. 그러나 대응을 사람이 직접 하고 있었던 것이 문제다. 어떤 문제가 발생했을 때 장치가 스스로 대응하는 것이 '적응형' 보안 아키텍처다.

이는 몇 가지 조건을 포함하고 있다. ▲다단계 방어 체계를 갖출 것(알려진 공격과 그렇지 않은 공격을 방어하고 포렌식 분석까지 자동으로 이뤄지는 것) ▲보안 장비끼리 상호 연계해 자동으로 위협정보 DB를 공유하는 것 ▲보안사고 로그를 알기 쉬운 리포트로 만들어 가시성을 높일 것 ▲이런 네트워크를 심층 분석해 우회 공격을 피할 수 있을 것 등이다.

따라서 차세대 방화벽을 도입할 때는 ▲보안 효율성(광범위한 대응, 빠른 보안 위협 시그니처 업데이트 등) ▲트래픽 가시성(단일 화면을 통한 가시성과 풍부한 보고 기능) ▲성능과 신뢰성(원하는 기능을 실행할 때 제 성능을 유지할 수 있는 기능) 등을 갖춘 제품을 선택해야 한다.

차세대IPS의 핵심 기능

가트너는 차세대IPS(NGIPS)를 1세대 IPS에 애플리케이션 인지, 컨텍스트 인지, 콘텐츠 인지, 애자일 엔진 등을 추가로 갖추고 있는 것으로 정의한다. 보안 소프트웨어를 테스트하는 NSS랩스에서는 NGFW과 NGIPS를 거의 비슷한 기준으로 테스트하고 있다. 유저기반 정책, IPS 튜닝 커스텀 시그니처 외에는 거의 같은 방식이다.

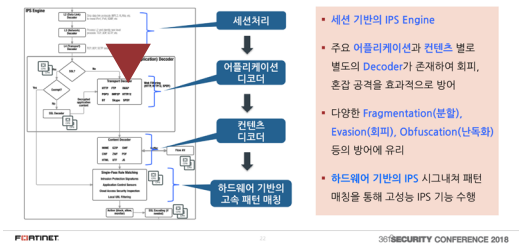
차세대 IPS는 어떻게 시작됐을까. 일반 방화벽은 원래 세션 기반으로 동작한다. 따라서 콘텐츠 검사 기능(L7 검사)이 없었다. 1세대 IPS는 콘텐츠를 봐야 하므로 L7 검사를 지원해야 했고, 동시에 세션을 지원해야 하므로 성능이 부족한 사태가 발생한다. 동시에 패킷을 기반으로 콘텐츠를 들여다본다. 그러나 방화벽과 같은 세션을 들여다보지는 않는다. 따라서 성능의 문제가 자주 생기고 해커들이 이를 우회하거나 회피하는 공격을 많이 만들어내게 됐다.

차세대 IPS는 1세대와 다르게 세션 기반, 애플리케이션 인지 기능 등을 탑재했다. 따라서 1세대에서 사용됐던 우회 공격 등을 디코딩해 콘텐츠로 만들어낸 후 검사 및 대응한다. 일반적으로 세션 기반의 IPS 엔진, 애플리케이션 디코더, 콘텐츠 디코더, 하드웨어 기반 고속 패턴 매칭으로 구성돼 있다.

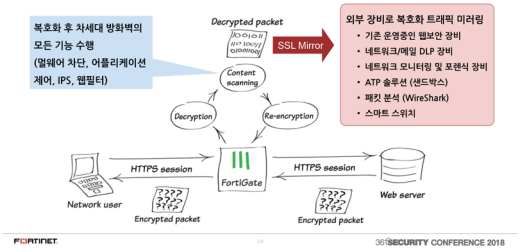
이에 따른 장점은 IPS 시그니처 개선이 있다. 1세대의 경우 인코딩 여부에 따라 매번 다른 패턴을 생성해야 했으나 차세대에서는 디코딩을 자동으로 한 뒤 검사를 한다. 따라서 우회·회피 공격(Evasion Attack)을 효과적으로 방어할 수 있게 됐다.

이러한 차세대 IPS를 도입할 때는 IPS 시그니처를 얼마나 빠르게 업데이트하는지, 정확성이 어떤지를 고려해야 한다. 또한 회피 공격을 얼마나 잘 막는지, 객관적인 성능은 어떤지 등에 대해서도 고민해야 한다.

차세대 IPS 엔진의 구조 (예시)



SSL 검사 및 활용방안



SSL방화벽 필요성과 활용

현재 SSL 트래픽은 이미 40%를 상회하고 있다. 암호화된 멀웨어 역시 50% 이상이다. 그런데 기업 중 SSL 트래픽을 검사할 수 있는 장비를 갖추지 못해 이를 그냥 방치하고 있는 곳들도 많다. 그러나 이제는 이 채널을 모두 검사해야 한다. 공격자들이 SSL 암호화 공격을 선호하기 때문이기도 하다. 따라서 암호화된 것과 아닌 것을 모두 처리해야 한다.

SSL 검사와 활용 방안은 절차에 따라 처리된다. 방화벽에서 SSL 암호화 트래픽을 복호화한 후 이를 장비 내부에서 처리한다. 이는 다시 암호화 후 클라이언트나 서버로 되돌린다. 차세대 방화벽에서는 복호화된 정보를 다른 웹 보안 장비나 정보유출방지(DLP), 포렌식, ATP 솔루션 등으로 미러링해준다. 보지 못하는 SSL 트래픽 정보를 별도의 암·복호화 장비를 투입하지 않고 자체적으로 처리하므로 효율적이다. 포티넷 장비의 경우 포트를 여러 가지로 사용할 수 있는 것이 특징이다.

SSL 방화벽 도입시 여러 고려 사항이 있다. SSL 트래픽에 대해서도 차세대 방화벽의 기능을 모두 수행해야 하며, 기존에 운영 중인 HTTP 보안 장비를 계속 활용할 수 있으면 좋다. 미러링 시 높은 성능이 필요하므로 성능 보장과 안정성이 중요하며, 미러링 시 수신장비가 이를 올바르게 받아들이는지 등의 호환성을 검증해야 한다.

포티넷 차세대방화벽의 강점

가장 큰 장점은 세 가지다. 포티넷 차세대방화벽 '포티가드(FortiGuard)'는 위협 분석 전문가가 모여 있는 연구소(포티가드랩)가 있어 위협 정보에 대한 인텔리전스가 뛰어나다. 전세계 장비에서 위협 정보를 인지하고 시그니처를 만들어낸다. 시그니처 업데이트 속도도 하루 한 번, 멀웨어는 한 시간에 한 번 정도로 매우 빠르다.

가시성 있는 운영체제(OS)인 '포티뷰(FortiView)'를 제공한다는 것도 특징이다. 포티뷰 화면으로 편리하게 상태를 인지하고 있으며 보안 전략을 짜는 데 많은 도움이 된다. 특히 멀웨어 관련 정보를 실시간으로 볼 수 있도록 한다.

성능도 뛰어나다. 포티넷은 현재 자체 설계한 칩인 '포티에이직(FortiASIC)'을 사용한다. 네트워크 프로세서와 콘텐트 프로세서로 구성돼 있다. 성능과 최적화, 트래픽 지연(Latency) 면에서 강점이 있다.

아울러 다양한 제품 포트폴리오를 갖추고 있다. 다양한 모델은 물론 모든 클라우드 플랫폼(아마존웹서비스, 마이크로소프트 애저, 오라클, 구글 클라우드)을 지원하는 가상화 제품도 갖추고 있다. 가상화 제품을 제외 모든 제품에는 자체 주문제작 반도체를 사용하므로 성능이 보장된다.

SSL 검사 기능도 모든 장비에 제공한다. 모든 장비에 SSL 트래픽을 기록한다는 의미다.

성능 검증은 NSS랩에서 이미 이뤄졌다. 2018년 NSS NGFW 테스트 결과 탐지율 99.13%. 회피공격 100% 차단, 처리성능(Throughput) 6.753Gbps, 방어/비용 효율성 1위를 달성한 바 있다. 레이턴시 역시 가장 작은 숫자를 기록했다. By

2018 NSS NGFW 결과

Product	Total Number of Attacks Run	Total Number of Attacks Blocked	Block Percentage
Fortinet FortiGate 500E V5.6.3GA build7858	2,074	2,056	99.13%

Test Procedure	Result
RPC Fragmentation	PASS
URL Obfuscation	PASS
FTP/Telnet Evasion	PASS
HTML Evasions	PASS
IP Packet Fragmentation + TCP Segmentation	PASS
HTTP Evasions	PASS
TCP Split Handshake	PASS
Resiliency[4]	
Attacks on nonstandard ports[5]	PASS

Figure 7 – Resistance to Evasion Results

Stability and Reliability	Result
Blocking under Extended Attack	PASS
Passing Legitimate Traffic under Extended Attack	PASS
Behavior of the State Engine under Load	
• Attack Detection/Blocking – Normal Load	PASS
• State Preservation – Normal Load	PASS
• Pass Legitimate Traffic – Normal Load	PASS
• Drop Traffic – Maximum Exceeded	PASS
Power Fail	PASS
Backup / Restore	PASS
Persistence of Data	PASS
Stability	PASS

Figure 16 – Stability and Reliability Results

- NGFW 테스트 결과 99.13% 방어
  - » 2056/2074 방어
  - » Evasion Attack 테스트 결과 pass
  - » 안정성 테스트 결과 pass
  - » 조사 대상 중 가장 낮은 Latency

Vendor	Latency (µs)					
	64-Byte Packets	128-Byte Packets	256-Byte Packets	512-Byte Packets	1024-Byte Packets	1514-Byte Packets
Barracuda Networks	76.26	79.07	80.37	98.33	77.67	99.99
Check Point	23.00	26.00	40.00	44.00	36.00	82.00
Cisco	94.72	108.55	94.51	92.73	107.96	111.89
Forcepoint	72.01	69.18	80.79	101.29	117.18	177.28
Fortinet	6.84	6.88	7.16	7.54	8.92	10.04
Palo Alto Networks	13.00	14.00	14.00	15.00	19.00	20.00
SonicWall	18.68	26.84	21.96	26.52	33.46	42.65
Sophos	162.11	166.43	175.19	174.71	163.00	145.50
Versa Networks	75.56	77.10	80.19	83.94	113.10	123.73
WatchGuard	44.88	83.65	86.96	106.71	125.71	123.52

Figure 6 – UDP Latency by Packet Size (Microseconds [µs])

FORTINET 38 361 SECURITY CONFERENCE 2018

시큐어 SD-WAN, 비용효과적인 지점 보안, 감사 방안

안경진 포티넷코리아 차장

최근 보안은 기업 IT부서의 최우선 과제로 자리잡았다. 기업들은 안티바이러스와 같은 기본적인 보안 프로그램에서 시작해 차세대방화벽, 침입방지시스템(IPS), 네트워크접근제어(NAC), 샌드박스 솔루션 등 복수의 보안기술 활용해 악의적인 침입을 막고자 하고 있다. 이와 같은 복합적인 보안 기술은 실제로 적지 않은 효과를 낸다.

그러나 대부분의 기업은 이같은 보안 솔루션을 본사에 주로 적용한다. 지점이나 대리점, 영업점과 같은 점포에까지 앞에서 언급한 보안 솔루션을 도입하는 것은 비용 면에서 매우 비효율적이기 때문이다. 예를 들어 편의점 프랜차이즈 기업이 모든 점포에 위에서 언급한 보안 시스템을 구축하고 관리할 수 있을까? 사실상 불가능하다.

이 때문에 기업의 지점이나 대리점은 공격자들의 놀이터가 될 때가 많다. 방화벽을 공유기처럼 쓰고 보안 정책은 다 무너져있는 경우가 있다. 심지어 PC에 안티바이러스 하나 제대로 없는 경우도 있다. 어느 정도 보안에 신경을 쓰는 점포라고 하더라도 IPS나 앱 컨트롤과 같은 높은 차원의 보안 기술은 적용되지 않는 경우가 대부분이다. 이는 지점뿐 아니라 본사에도 큰 위협요소다.

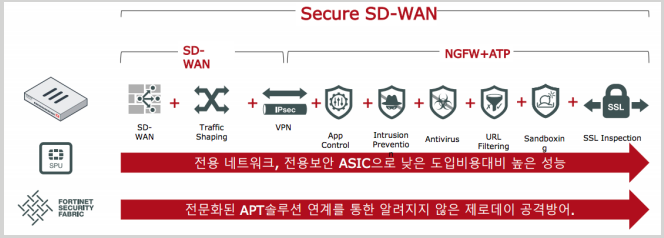
공격자들도 투자대비성과(ROI)가 중요하기 때문에 상대적으로 보안이 취약한 고리를 활용해 정보를 빼낸다. 일반적으로 기업의 지점이나 대리점은 전용망 또는 가상사설망(VPN)을 통해 본사와 연결이 돼있다. 지점의 IT시스템이 공격자의 손아귀에 들어갈 경우 해커는 이 망을 타고 본사시스템까지 침입할 수 있다. 그렇다고 지점에 앱 컨트롤, IPS, 샌드박스 등 본사와 같은 수준의 보안 시스템을 구축할 수도 없다.

포티넷 안경진 차장은 이에 대해 "지점이나 지사에도 보안시스템이 필요하다"면서 "그러나 모든 지점에 본사와 같은 규모의 투자를 할 수 없기에 최소한의 비용으로 최대한의 효과를 얻을 수 있는 솔루션을 찾아야 한다"고 말했다.

안 차장은 포티넷의 '시큐어 SD-WAN(소프트웨어정의광역네트워크)'이 이와 같은 요구를 충족시킬 수 있다고 설명했다. '시큐어 SD-WAN'은 SD-WAN과 차세대방화벽 보안 기능을 동시에 제공하는 것이 특징이다.

기존의 SD-WAN은 터널 역할만 했다. 오히려 외부에서 들여다볼 수 없기 때문에 지점의 취약점이 그대로 본사로 이전되는 통로가 되기도 했다. 하지만 '시큐어 SD-WAN'은 SD-WAN의 기능을 충분히 하면서, 앱 컨트롤, IPS, 안티바이러스, URL 필터링, 샌드박스, SSL 감시 등 다양한 보안 기능을 하나의 장비에서 제공한다.

복잡한 시스템이 아니라 단 하나의 박스에서 이 모든 기능을 제공하기 때문에 IT투자 여력이 낮은 지점이나 지사에서도 간단히 도입할 수 있다.



특히 '시큐어 SD-WAN'은 전문적인 보안관리자가 없는 지점에서도 손쉽게 활용할 수 있다는 점이 장점이라고 안 차장은 강조했다.

안 차장은 "'시큐어 SD-WAN'은 자체적인 보안 감사 기능이 있어 암호화되지 않은 접속권한이 허용됐는지, 방화벽은 열려있는지 닫혀있는지, 보안 프로파일이 설정이 돼 있는지, 알려지지 않은 공격을 막기 위한 샌드박스가 연결돼 있는지 등을 보안 컴플라이언스 기준으로 점수를 매겨준다"면서 "단순히 점수를 매기고 끝나는 것이 아니라 버튼 한 번 클릭만으로 조치까지 취할 수 있도록 설정을 지원하는 것이 가장 큰 장점"이라고 덧붙였다.

안 차장은 이어 "'시큐어 SD-WAN'은 또 전용선, 광랜, 3G, 4G 등 여러 형태의 회선을 단 하나의 인터페이스로 묶어주고 하나의 인터페이스에서 정책을 세우고 앱 단위로 트래픽을 전송한다"면서 "특정 회선에 문제가 생기면 다른 회선으로 우회하고, 레이턴시가 증가할 때는 사전에 설정해놓은 인터페이스가 아니라 다른 인트페이스로 트래픽을 보낼 수 있는 스마트한 SD-WAN 회선"이라고 강조했다. By

가성비 갑, APT 방어 시스템 고도화

최광순 포티넷코리아 이사

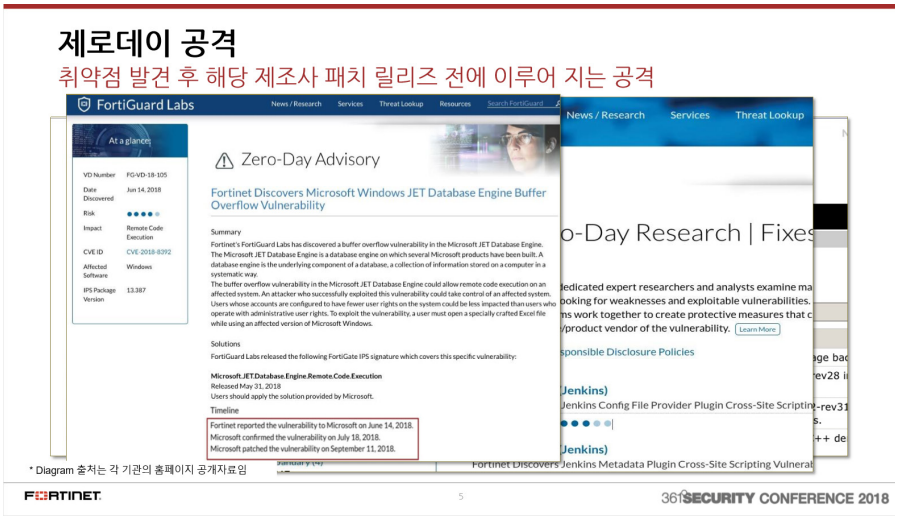
지난 6월 14일, 포티넷은 제로데이 공격과 관련해 마이크로소프트 윈도우 제트(JET) 데이터베이스 엔진에 버퍼 오버플로 취약점이 생겼다는 것을 발견했다. 관련정보는 즉시 전달됐고, 마이크로소프트는 7월 18일에 취약점을 확인, 9월 11일에 패치를 공개했다.

취약점 발견부터 패치 공개까지 걸린 시간은 석 달이다. 그러나 취약점이 공식 확인됐다는 것은, 해커들 역시 관련 정보를 알 수 있다는 뜻도 된다. 패치가 나오기 전에 얼마든지 보안 공격이 시도될 수 있다. 이 기간 기업은 어떻게 공격을 막아낼 수 있을까?

이미 많은 기업이 지능형지속위협(APT) 방어 시스템을 갖추고 있다. 지금 시점에서는 APT 방어시스템 구축을 논하는 것 보다는 시스템 고도화에 대한 이야기가 더 현실적이다. 다만 고도화를 위해 장비를 바꾸는 일은 비용적인 측면에서 어렵다. 기존에 어떤 업체의 제품을 썼든지 간에 상관없이 저렴하게 부족한 점을 메울 수 있도록 하는 게 보안업체들의 숙제다.

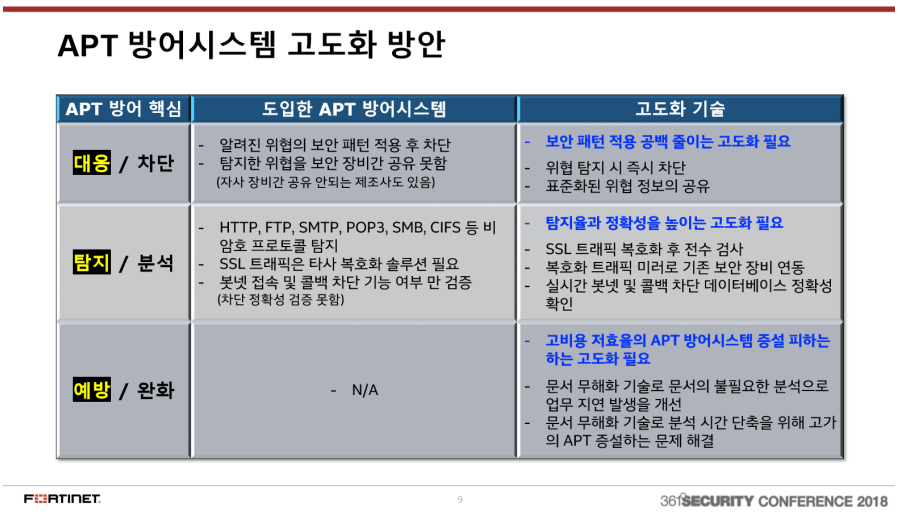
지금까지 구축돼온 APT 방어 시스템의 문제는, 마이크로소프트가 취약점을 인지하고 패치를 배포하기까지 생기는 저 석 달의 공백을 막을 수 없었다는 점이다. 최광순 포티넷 이사는 "기존 APT 방어 시스템은 분석과 대응에 초점을 맞추고 있는 것이 한계"라며 "실시간 대응과 정확한 탐지, 선제 예방이 삼위일체가 되어야 한다"고 APT 방지시스템 고도화 필요성을 설명했다.

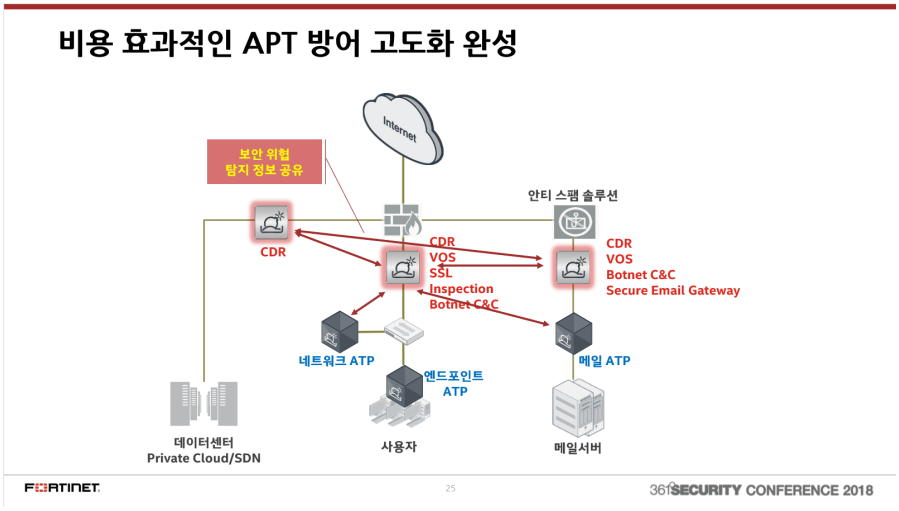
최 이사에 따르면 APT 방어 시스템 고도화는 보안 강화와 비용 절감, 기존 시스템 보완에 초점을 맞춰야 한다. 방어의 핵심은 실시간 대응과 정확한 탐지, 선제적 예방에 있다.



* Diagram 출처는 각 기관의 홈페이지 공개자료임

그렇다면 실제 고도화는 어떻게 이뤄져야 할까?





실시간 대응

새로운 위협이 출현했을 때 탐지 자체는 빠르게 이뤄진다. 문제는 탐지 이후 대응이다. 통상 보안 공격이 들어오고 난 후 3~4시간이 지나면 굉장히 많은 시스템이 감염되기 시작한다. 시그니처를 만들고, 오탐지를 막기 위해 시그니처에 대한 품질 검수를 거쳐 보안 장비에 다운로드 되기까지 통상 세 시간은 걸린다. 그 사이에 위협이 증가된다.

최 이사에 따르면 이 세 시간의 갭을 줄이자는 것이 포티넷 바이러스 확산 방지 서비스(VOS, Virus Outbreak Prevention Service)의 핵심이다. 시그니처의 품질을 검수하는 중이더라도, 혹시 모를 감염을 막기 위해 이미 탐지한 해시 정보를 바탕으로 글로벌 위협 정보 데이터베이스를 검색해 차단토록 하는 것이다.

이를 위해서는 글로벌 위협 정보 데이터베이스가 매우 풍부해야 한다. 아울러 시그니처나 글로벌 샌드박스 인텔리전스를 통해 얻은 정보 등 다른 데이터 소스들과 연동해 정보를 주고받아야 한다.

정확한 탐지

APT 방지 시스템이 처음 도입되던 5년 전만 해도 SSL 트래픽을 탐지하지 못하는 장비가 대부분이었다. 그러나 최근 들어 기업이 SSL 암호화를 많이 사용하는 환경을 감안하면 관련 트래픽을 분석하지 않는다는 것은 그만큼 위험을 떠안는 것이 된다.

탐지 고도화는 SSL 분석이나 실시간 봇넷 차단을 뜻한다. 정확한 탐지를 위해서는 SSL을 포함한 모든 트래픽을 분석하고 탐지할 수 있어야 한다. 다시 말해, 트래픽에 대한 전수 검사가 필요하다는 이야기다. 멀웨어가 암호화 형태로 전달될 수 있기 때문이다.

만약 암복호화 전용 장비를 단순히 암호화에만 쓰는 것이 아니라 이후 트래픽에도 책임을 지게 하는 방식을 고려한다면 문제 해결이 편해질 수 있다. 일차적인 보안 필터링을 하자는 이야기다. 알려진 멀웨어나 취약점 공격이 있다면 일차적으로 암복호화 전용 장비에서 차단하고, 이후 복호화된 트래픽을 분석 탐지 장비로 가져가서 전수검사를 통해 탐지율을 향상시키는 것이 중요하다고 최 이사는 설명했다.

실시간 변동하는 봇넷 C&C IP와 도메인 정보를 유지하고, 차단하는 것도 핵심이다 포티넷에 따르면 분당 봇넷 접속 차단 횟수만 3만2000번 이상이다. 대부분의 보안업체들이 봇넷 C&C 접속을 차단할 수 있다고 하지만 실제로 실시간 차단이 가능한지 그 성능을 검증하기는 어렵다. 그렇기 때문에 정확하면서도 많은 데이터베이스를 갖고 있는지 여부가 탐지율을 높이는데 중요한 요건 중 하나다.

예방 고도화

APT 방어 시스템 고도화의 중요한 포인트 중 하나는 선제적 예방이다. 그런데 예방을 하겠다고 모든 파일을 샌드박스에 넣어버릴 수는 없다. 샌드박스를 무한정 늘릴 수가 없어서다. 특별히 검사를 할 필요가 없는 파일을 미리 골라내면 좋은데, 기존 APT 방어 시스템 중에는 이런 기능이 없는 제품들이 있다. 그렇다고 새로 장비를 사자니 돈이 많이 든다. 최 이사는 "이 경우 예방 고도화를 위한 기술을 선택, 파일에 있는 액티브 콘텐츠를 제거해서 검수 트래픽을 줄이는 것도 방법"이라고 조언했다.

예방 고도화의 예로는 CDR(Content Disarm Reconstruction)이라는 기술이 있다. 이는 국내에서 '콘텐츠 무해화' 기술로 불리기도 한다. 선제적 예방의 핵심이 검사할 파일을 줄이자는 것이기 때문에 아예 '읽기 전용(read only)' 업무에 사용되는 파일은 검사에서 제외할 수 있게 활성화된 파일을 제거하는 방식이다.

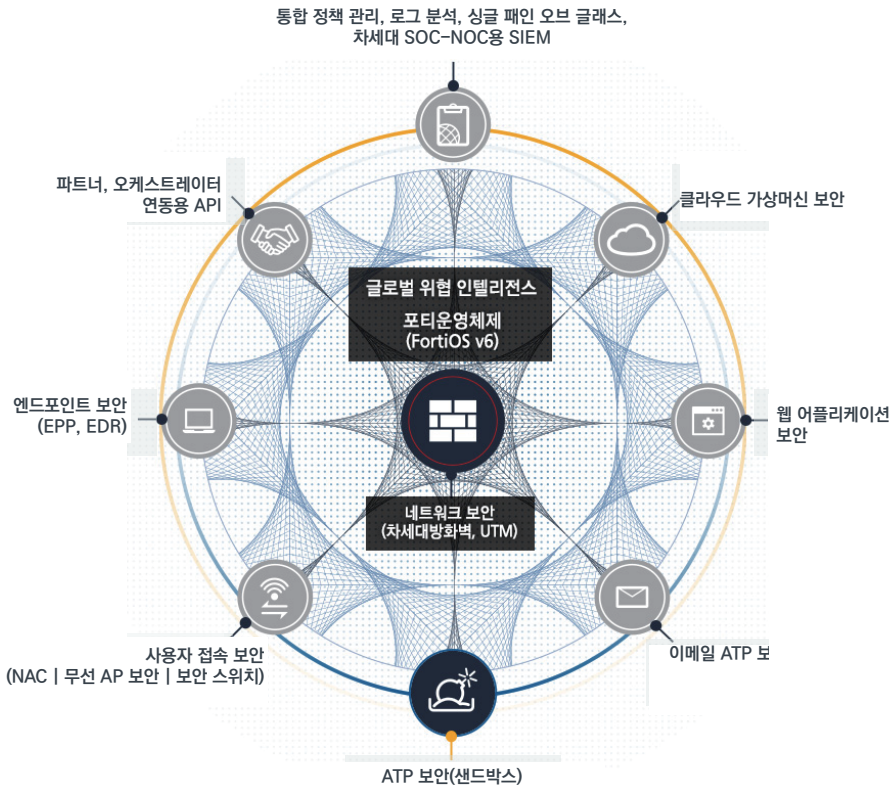
문서에 포함된 액티브 콘텐츠, 하이퍼링크, 매크로 등을 이용해 공격의 트리거로 이용하는 것은 해커들이 즐겨 사용하는 방법이다. 문서에 포함된 모든 임베디드 액티브 콘텐츠를 제거한 후 사용자에게 전달해 보안사고를 예방하고자 하는 것이 이 기술의 핵심이다. CDR 대응 장비를 도입하면 샌드박스를 계속 추가하는 것에 비해 비용이 많이 줄뿐더러 금융권같은 폐쇄망에서도 쓸 수 있다는 것이 장점이다.

최 이사는 "기존에 어떤 벤더의 장비를 도입했든 관계없이 핵심 기능을 비용 효과적으로 고도화 할 수 있는 게 포티넷의 강점"이라며 "고도화를 통한 분석 대기 시간단축으로 업무 지장을 최소화하고 예방과 탐지율 향상으로 보안 담당자의 업무량을 감소시킬 수 있다"고 강조했다.

FORTINET

361 SECURITY 2018

디지털 트랜스포메이션 시대, 보안의 혁신을 제시하다



BylineNetwork

발행 | 바이라인네트워크
배포 | https://byline.network/
취재/글 | 이유지 기자 yjlee@byline.network 심재석 기자 shimsky@byline.network
남혜현 기자 smilla@byline.network 이종철 기자 jude@byline.network
문의 | byline@byline.network

SPECIAL REPORT
BylineNetwork

문의처

포티넷 코리아

서울시 강남구 영동대로 325 (대치동, 해암빌딩 14/15층)
전화 : 080-559-8989 이메일 : kr-callcenter@fortinet.com
홈페이지 : http://kr.fortinet.com 페이스북 : https://www.facebook.com/fortinetkorea

FORTINET