TREND MICRO

하이브리드 클라우드 환경의 ‘Deep Security’

리눅스 서버와 컨테이너 보안 해법

SPECIAL REPORT

BylineNetwork

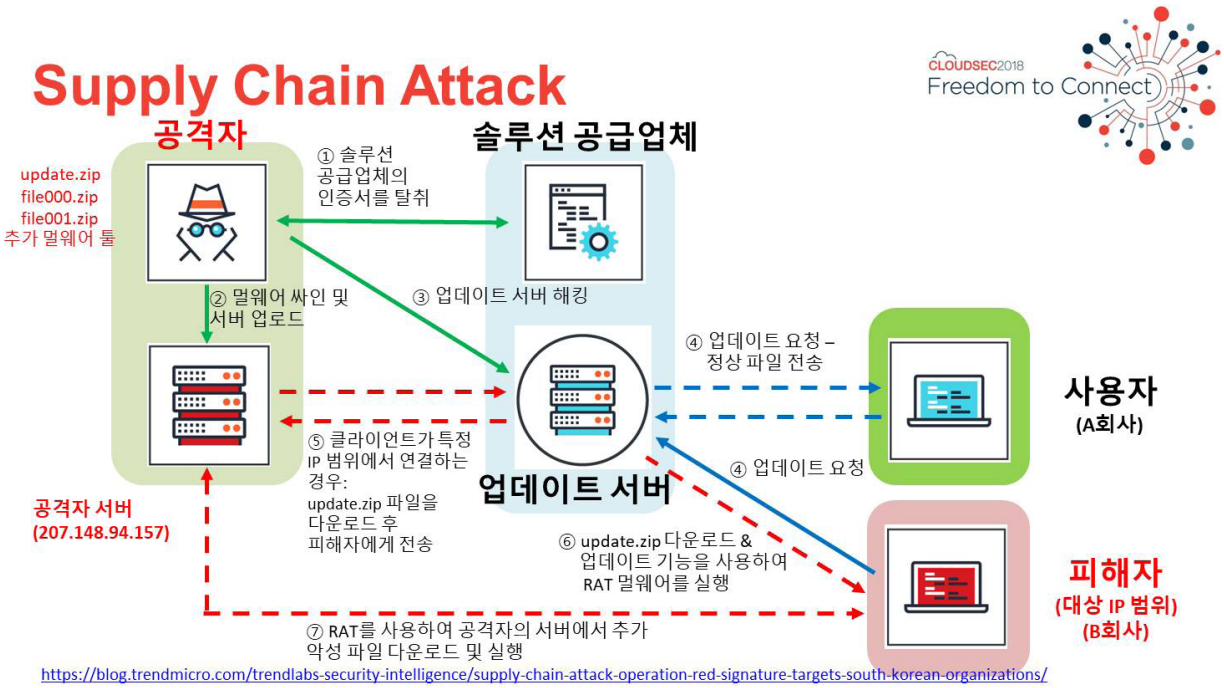
취약점 패치를 했든 안했든,
공격은 막아라

#1 지난해 6월 우크라이나 기반시설이 해커의 랜섬웨어 공격으로 마비됐다. 기업을 비롯해 공항, 정부기관 등 많은 조직이 심각한 피해를 입었다. 바로 한 달 전인 5월 전세계를 강타해 단숨에 100여개국 수십만대 컴퓨터를 감염시켜 큰 피해를 입힌 '워너크라이(WannaCry)' 랜섬웨어에 맞먹는 피해였다.

클라우드 환경에 보안을 적용하는 것은 쉬운 일이 아니다. 물리적 환경과는 달리 무형의 자산과 데이터에 보안을 적용해야 한다. 기존 데이터센터에 적용해온 보안 프로세스와 정책, 제품을 클라우드에 그대로 활용하고자 하는 경우 다양한 문제가 발생한다.

문제는 피해를 입은 우크라이나 기업이나 기관이 보안에 소홀해서 벌어진 일이 아니라는 점이다. 이 사태는 전형적인 공급망 공격이다. 공격자는 메드독(MedDog)이라는 회계 프로그램의 업데이트 서버를 해킹했다. 이 회계 프로그램 사용자가 정상적으로 업데이트를 했는데 악성코드에 감염됐다. 아무리 보안에 철저해도 이와 같은 정상적인 업데이트를 통해 설치되는 악성코드까지 막기는 힘들다. 고객사 입장에서 서드파티 소프트웨어 업체의 보안취약점까지 해결할 수는 없는 노릇이기 때문이다.

그러나 불행히도 소프트웨어 솔루션 벤더들은 보안에 많은 투자를 할 여력이 많지 않다. 특히 국내 소프트웨어 기업은 더욱 그렇다. 그러다보니 공급망 공격의 타깃이 되기 쉽다.



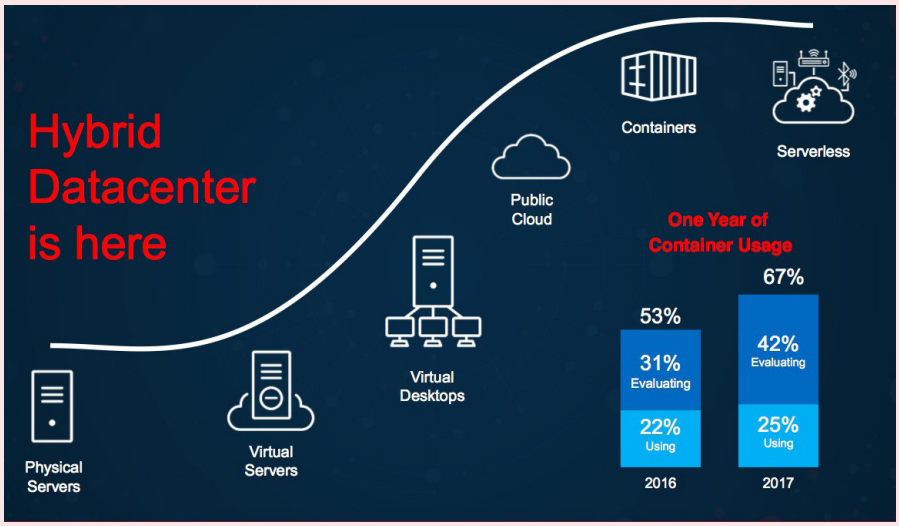
#2 지난해 미국 3대 신용평가회사 가운데 하나인 에퀴팩스에서는 1억4300만명의 개인정보가 유출되는 참사가 벌어졌다. 미국인 2명 가운데 1명꼴이다. 유출된 정보에는 생년월일, 주소와 같은 기초정보를 포함해, 운전면허증 번호, 신용카드 번호, 급여, 사회보장번호까지 포함돼 있었다.

이 참사는 에퀴팩스가 아파치 스트러츠(Apache Struts) CVE-2017-5638 취약점을 방치한 데서 비롯했다. 이 취약점은 앞선 3월에 이미 공개됐던 것이다. 취약점이 공개됐음에도 에퀴팩스는 2개월 이상 패치를 하지 않았고, 이 작은 실수가 기업의 운명을 좌우할 수도 있는 사태의 원인이 됐다.

그러나 IT시스템을 운영하다 보면 보안패치가 나왔다고 무조건 업데이트할 수 없을 때가 많다. 패치가 운용 시스템에 어떻게 영향을 미칠지 알 수 없기 때문이다. IT운영팀은 언제나 패치가 조심스럽다. 패치 전에 충분한 테스트를 거칠 시간이 필요하다.

그렇다면 취약점이 공개되고 시스템에 패치를 업데이트하기 전까지의 간극은 위험한 상태로 방치해둘 수밖에 없는 것일까? 또 소프트웨어 벤더의 솔루션에 취약점이 없기만을 기도해야 하는 걸까? 우리 기업이 제2의 에퀴팩스가 될 위험성을 내재한 채?

트렌드마이크로는 이에 대한 대책으로 '가상패치(Virtual Patch)'를 제시한다. 트렌드마이크로에 따르면, 버추얼 패치는 취약점이 알려졌음에도 패치를 하지 않았거나, 벤더가 패치 업데이트를 제공하지 않았을 때 대비하는 기술이다. 취약점이 발표됐을 때 소프트웨어 솔루션 벤더들이 해당 취약점을 해결한 업데이트를 항상 내놓는 것은 아니다. 패치가 나온다 해도 항상 우리 시스템이 최신 패치 상태를 유지하고 있는 것도 아니다. 가상패치는 실제로 패치를 하지는 않았지만, 패치한 것과 같은 효과를 일으키기 때문에 이런 상황에서도 최악의 상태를 막을 수 있다. 패치가 적용될 때까지 시간을 벌어주는 용도라고 볼 수 있다.



가상패치는 최근 급변하는 최신 IT환경에는 더욱더 필요하다. 현재 기업의 IT환경은 과거와 비교할 수 없이 복잡해졌다. 일단 기존의 레거시 시스템, 가상 서버, 가상 데스크톱, 퍼블릭 클라우드, 컨테이너, 서버리스 컴퓨팅 등이 혼재해 있다. 특히 컨테이너 사용률이 급증하고 있다.

이런 상태에서 패치는 더욱 복잡한 일이 된다. 다수의 클라우드 서비스를 이용하면서 하이브리드 클라우드 환경을 구현한 경우 어떻게 일관되게 보안정책을 유지할 것이냐가 큰 숙제다. 레거시 시스템에 대한 패치는 매우 어렵기 때문에 사실상 보안 취약점을 노출한 채 방치되는 경우도 많다.

한때 리눅스는 상대적으로 안전하다는 생각도 있었다. 그러나 근래에는 리눅스용 악성코드가 급증하고 있다. 트렌드마이크로에 따르면, 지난해 리눅스용 악성코드는 2만5000개가 발견됐다. 그런데 올해는 상반기에만 1만5000개가 이미 나타났다. 지난해 리눅스 기반 에레버스(Erebus) 랜섬웨어 감염으로 촉발된 인터넷나야나 사태 이후 해커의 공격이 엔드포인트에서 서버로 넘어오는 추세를 읽을 수 있다.

그러나 많은 보안 소프트웨어 기업들이 리눅스 운영체제에는 소홀한 편이다. 리눅스에는 바이러스가 별로 없다는 편견 때문이다. 이 때문에 리눅스 서버가 위협에 노출되는 경우가 많다. 가상패치는 우선순위에서 밀린 리눅스 서버를 지키는 데에도 유용하다.

박상현 한국트렌드마이크로 지사장은 "가상패치는 예상되는 취약점 공격에 대응할 수 있는 룰을 만들어 방어한다"면서 "기업이 취약점 패치가 나와 있는데 하지 않은 경우, 레거시 시스템이어서 패치가 어려운 경우, 아직 등록되지 않은 취약점이 있는 경우 등 어떠한 경우에도 가상패치로 공격을 막을 수 있다"고 말했다.

박 지사장은 "지난해 인터넷나야나 사태 이후 클라우드나 데이터센터의 서버를 공격하는 사례가 늘어나고 있다"면서 "실수든 고의든 취약점이 패치되지 않아 위협이 노출되는 사태는 막아야 한다"고 강조했다. By

도커 컨테이너 보안,
DevSecOps 구현방안

최근 하이브리드 클라우드 환경에서 가상화 기술 외에 컨테이너 기술을 활용하는 비중이 크게 늘고 있다.

컨테이너는 애플리케이션을 보다 간편하고 효율적으로 구축해 빠르게 배포할 수 있는 기술이다.

컨테이너는 하이퍼바이저 위에 각각의 게스트 운영체제(OS)와 애플리케이션을 운영하는 가상머신(VM)과는 달리 공통 호스트 OS 위에 컨테이너 엔진을 설치해 애플리케이션을 구동한다.

VM보다 가벼워 효율적인 리소스 관리가 가능하고, 이미지 생성 배포·롤백이 용이하며 간편하게 애플리케이션 영역에 적용·배포할 수 있는 장점을 제공한다.

대표적인 컨테이너 엔진은 도커(Docker)다. 컨테이너 환경에서는 여러 컨테이너를 하나의 서비스로 구성하고 배포, 관리할 수 있는 오케스트레이션 툴을 사용한다. 대표적인 툴이 쿠버네티스(kubernetes)다.

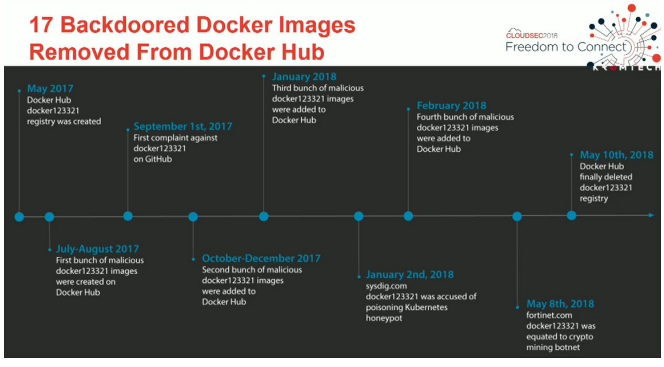
컨테이너 환경도 보안 대책이 필요하다. 최근 워크로드에 많이 사용하는 컨네이너가 취약점을 갖고 있거나 침해된 컨테이너 이미지가 배포되면 심각한 문제가 발생할 수 있기 때문이다.

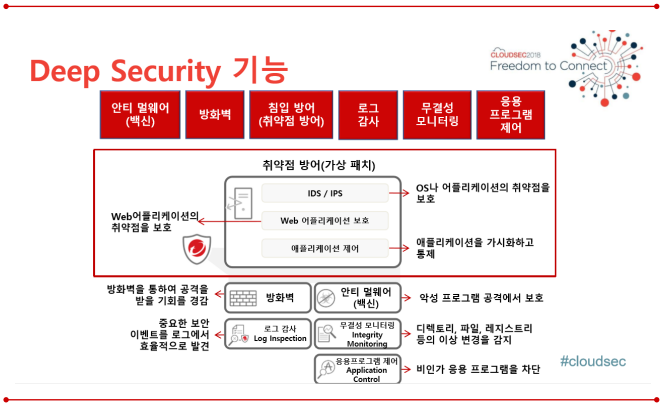
이미 지난 5월에 도커 허브에 올라온 컨테이너 이미지 중 17개가 악성코드에 감염된 채 배포돼 500만 건 이상의 컨테이너가 다운로드된 사례가 발견되기도 했다.

양희선 한국트렌드마이크로 부장은 "개발자가 오픈소스를 사용해 이미지를 가져오거나 수정해 배포하는 경우 취약한 컨테이너 이미지를 가져올 수 있다. 코드 재사용시나 공용 이미지를 가져와 사용할 때 잘못된 코드와 구성요소를 사용해 서비스를 만들고 배포할 경우 문제가 발생할 수 있는 소지가 있어 취약점을 점검하고 보완할 수 있는 요소가 필요하다"고 지적했다.

악성코드를 담은 이미지를 그대로 애플리케이션에 반영해 서비스로 제공할 경우 고객들까지 감염시키고 피해를 크게 확산시킬 수 있다.

트렌드마이크로는 컨테이너 보안해법으로 두 가지 방안을 제시하고 있다. ▲안전한 컨테이너 환경을 운영하기 위해서는 취약점과 악성코드 공격으로부터 호스트 영역과 컨테이너 자체를 보호해야 하며, ▲데브옵스(DevOps) 환경에서 컨테이너 이미지를 배포하기 전에 악성코드나 취약점을 갖고 있는지 점검해 보호한다는 것이다.





트렌드마이크로의 대표 제품인 '딥시큐리티(Deep Security)'가 컨테이너가 탑재되는 호스트 영역의 보안을 제공할 수 있다.

'딥시큐리티'는 물리적 서버부터 도커와 같은 컨테이너를 포함해 가상·클라우드 환경까지 일관되게 통합 보호할 수 있는 하이브리드 클라우드 통합보안 제품이다. 안티멀웨어(백신), 방화벽, 침입방어, 로그감사, 무결성 모니터링, 애플리케이션 제어 등의 기능을 제공한다.

백신모듈·IPS·가상패치 기능으로 컨테이너 호스트 안전하게 보호

트렌드마이크로는 '딥시큐리티 에이전트(DSA)'를 도커 호스트에 설치해 안전하게 보호하는 동시에 모든 워크로드에서 일관된 보안을 유지할 수 있도록 제공한다.

실시간 백신모듈(AM)과 호스트 기반 침입방지시스템(IPS), 가상패치 기능 등이 도커 컨테이너가 설치·구동되는 호스트 영역 전체를 악성 공격으로부터 보호하는 기능을 제공한다.

특히 가상패치 기능은 취약점이 발견됐으나 정규 패치가 나오지 않았거나 사용자가 미처 패치를 하지 못했을 경우, 해당 취약점을 이용한 공격을 방어해 패치(보안업데이트)를 적용한 것과 동일한 효과를 낸다.

'딥시큐리티 매니저(DSM)'는 스마트폴더에서 도커 서비스를 하는 호스트 서버들에 대한 가시성을 제공한다.

컨테이너에서 악성파일, 취약점이 탐지돼 삭제된 경우 컨테이너 아이디(ID)와 이름, 이미지 이름까지 세부정보를 대시보드 화면에 표시해 제공한다. 이같은 정보는 REST 애플리케이션프로그래밍인터페이스(API)로 연동해 외부로 전달할 수도 있다.

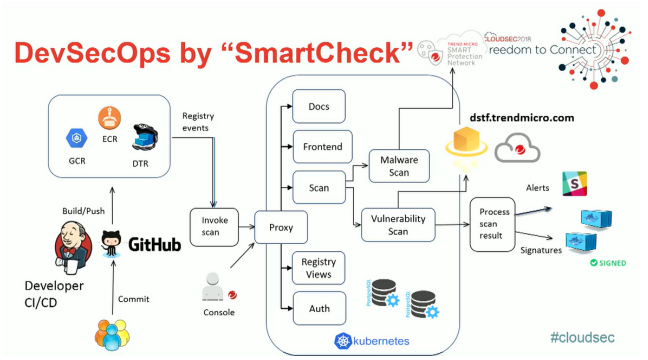
컨테이너 이미지 취약점·악성코드 점검, 데브섹옵스 구현 지원

트렌드마이크로는 컨테이너 서비스가 배포되기 전에 취약점과 악성코드 유무를 점검하는 '딥시큐리티 스마트체크(Deep Security Smart Check)'도 제공한다.

'딥시큐리티 스마트체크'는 실시간 개발과 운영이 이뤄지는 데브옵스의 개발·테스트 단계부터 운영돼 배포되기 전에 점검을 수행, API를 통한 자동화 방식으로 CICD(Continuous Integration and Continuous Delivery) 파이프라인을 보호할 수 있도록 지원한다. 이를 기반으로 개발과 운영이 실시간 이뤄지는 데브옵스 환경에서도 보안기능이 작동되게 하는 '데브섹옵스(DevSecOps, 데브시크옵스)'를 구현할 수 있다.

악성코드와 취약점 사전 점검은 트렌드마이크로 글로벌 사이버위협 인텔리전스인 '스마트 프로텍션 네트워크(SMAT Protection Network)'와 연동해 진행된다. 이 기능 외에도 레지스트리 콘텐츠에 대한 가시성 제공, 지속적인 모니터링과 신규 취약점·악성코드 패턴 업데이트에 대한 알림, 조사와 감사를 위한 점검 내역 검색 등의 기능을 제공한다.

박상현 한국트렌드마이크로 지사장은 "2017년 기준 도커를 쓰는 기업은 25%, 평가 중인 곳 42%를 포함해 전체 67%에 달할 정도로 몇 년 새 클라우드 환경에 컨테이너 기술을 채택하는 비중이 급증했다. 이 컨테이너 환경에도 보안 홀이 있다"라면서 "워크로드에 많이 사용하는 도커·컨네이너가 취약점을 갖고 있거나 침해된 컨테이너 이미지가 배포되면 심각한 문제가 발생할 수 있기 때문에 보안 대책을 세워야 한다"고 강조했다. By



증가하는 위협 대응을 위한

리눅스 서버 보안 적용 가이드

2017년 리눅스 운영체제(OS)를 노린 악성코드가 2만5000개 넘게 발견됐다. 올해 상반기에만 이미 1만5000개를 넘었다. 지난 한 해 동안 발견된 리눅스 커널 취약점만도 453개에 달한다.

W3Tech 집계에 따르면, 웹서버 가운데 유닉스/리눅스 서버 비중은 67.1%다. 전체 유닉스 계열 서버 중 리눅스 서버는 절반 이상이다.

리눅스 서버 사용이 늘어나면서 사이버공격도 증가하고 있다. 더욱이 리눅스 서버는 취약점이 발견되더라도 가용성 문제나 업무 리소스 부족으로 업데이트가 제때 이뤄지지 않고 있는데다, 백신이나 침입방지시스템(IPS) 등 보안대책이 미비한 경우가 많다.

지난해 6월 10일 웹호스팅 기업인 인터넷나야나는 운영 중인 서버 153대가 리눅스 기반 랜섬웨어에 감염돼 3400여 고객 웹사이트가 연쇄 피해를 입었다. 암호화 해제 키를 받는 대가로 13억원의 막대한 비용을 지불해야 한다.

공교롭게도 이 사태가 발생했던 시점에 리눅스 악성코드는 크게 급증했다. 사고가 발생하기 직전인 지난해 5월 발견된 리눅스 악성코드는 3856개, 6월에는 5721개다.

최근에는 오래된 취약점을 이용, 쉘 스크립트를 다운로드, 실행해 리눅스 웹서버 자원을 암호화폐 채굴에 이용하는 사례도 발생하고 있다.

리눅스 보안대책은 이제 필수다. 그리고 백신을 사용하는 것만으로는 부족하다.

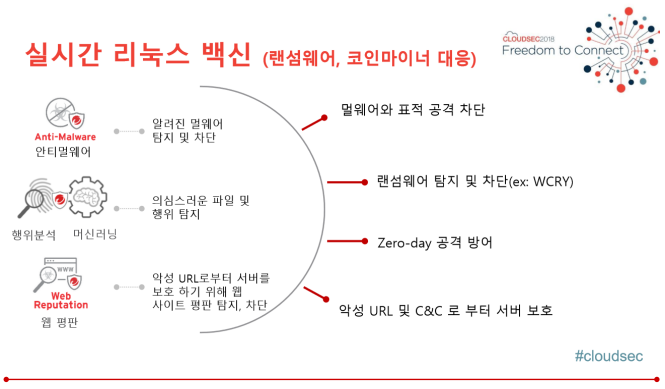
ISMS 기준 충족하는 보안 항목 : 백신, 호스트 기반 방화벽·침입방지

현재 정보보호관리체계(ISMS) 인증 항목에서도 '공개서버 보안'을 적용할 것을 요구하고 있다. 웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립해야 한다고 명시돼 있다.

리눅스 서버 보안을 위해서는 OS 패치를 정기적으로 적용해야 하는 것은 물론, 악성코드로부터 시스템을 보호하기 위한 대책이 필요하다. 취약점 점검과 네트워크에 대한 비인가 접근통제 정책도 운영해야 한다. 이같은 내용은 ISMS 준수를 위한 필수요건이기도 하다.

트렌드마이크로는 통합 서버보안 제품인 '딥시큐리티'에서 제공하는 실시간 리눅스 백신, 호스트 기반 방화벽과 침입방지 기능을 제공해 이같은 요건을 충족할 수 있도록 제공한다.

서버를 감염시키려는 악성코드 실시간 탐지, 차단 기능을 제공하는 리눅스 백신은 시그니처 기반의 알려진 위협 탐지·차단은 물론 행위분석, 머신러닝 기능을 활용해 의심스러운 파일과 행위까지 탐지해 알려지지 않은 제로데이 위협에 대처할 수 있는 기능을 탑재했다. 웹 평판 기능도 제공해 악성URL과 명령제어(C&C) 통신을 차단할 수 있다. 이같은 기능이 있어야 랜섬웨어와 서버를 암호화폐 채굴에 이용하는 크립토마이너에 대응할 수 있다는 게 트렌드마이크로의 설명이다.



CPU 사용량 설정, 버전과 실시간 감시 기능 지원 여부 확인해야

트렌드마이크로는 이밖에도 리눅스 백신이 제공해야 하는 기능으로 'CPU 사용량을 제한하는 옵션'이 필요하다고 지적했다.

윤명익 한국트렌드마이크로 부장은 "CPU 허용치나 임계치를 설정할 수 있어야 시스템 과부하를 통제하면서 악성코드를 탐지·차단할 수 있어야 한다. 다만 리소스 사용량을 낮춰 설정할 경우 검사에 오랜 시간이 걸릴 수 있어 적정치를 설정해야 한다"고 말했다.

또 리눅스 배포판과 커널버전을 얼마나 광범위하게 지원하는지도 중요하다고 강조했다. "리눅스 배포판 버전과 커널 종류가 많아 백신이 현재 사용하는 버전에 대한 실시간 감시 기능을 지원하는지 확인해야 한다. 커널후킹모듈을 지원해야 하는데 시중에 판매되는 리눅스 백신 중에서는 실시간 감시를 지원하지 않는 백신도 있다. 만일 리눅스 버전 커널버전을 지원하지 않은 백신을 도입할 경우 사용중인 리눅스를 다 업그레이드해야 할 수도 있기 때문에 배보다 배

꼽이 더 큰 상황에 처할 수도 있다"고 지적했다.

호스트 기반 방화벽은 양방향 스테이트풀 인스펙션(Stateful Inspection) 방화벽 기능을 통해 네트워크 트래픽을 제어한다. 서버 간 접근제어를 통해 불필요한 네트워크 트래픽을 차단한다.

사내 네트워크에서 감염 단말에 의한 사내 네트워크 서버로의 통신을 막기에는 한계가 있어 호스트 기반 방화벽이 필요하다는 게 트렌드마이크로의 얘기다.

방화벽은 프로토콜(TCP, UDP, ICMP 등), 소스와 목적지(IP·MAC 주소, 포트 등), 프레임(IR·ARP 등), TCP 헤더 플래그(SYN, ACK, FIN, PSH 등) 등 다양한 룰을 적용할 수 있는 솔루션을 선택하는 것이 중요하다.

호스트 기반 침입방지 기능은 들고나는 모든 트래픽을 분석해 공격 패킷을 탐지하고 차단한다. 표준 프로토콜을 따르지 않는 트래픽을 탐지·차단하며, 애플리케이션 사용을 탐지·차단하는 규칙도 제공한다. 크로스사이트 스크립팅(XSS), SQL 인젝션(Injection) 등 일부 기본적인 웹 애플리케이션 취약점 공격으로부터 보호하는 기능도 제공한다.

트렌드마이크로는 가상패치 기능으로 패치가 이뤄지지 않은 취약점을 활용한 공격으로부터 시스템을 보호하는 기능도 제공한다. 웹·DB 서버에 설치된 '딥시큐리티 에이전트(DSA)'가 자동으로 OS와 애플리케이션의 취약점을 검사(Scan)해 방어 룰을 적용한다.

윤 부장은 "가상패치를 적용하면 발견된 취약점에 대한 정규 패치가 발표되기 전에도 마치 패치한 것처럼 취약점 공격이 방어되는 효과를 얻을 수 있다. 가상패치는 정규패치를 긴급히 적용할 필요가 있을 때 이 패치가 서버 운영에 영향을 미치는 것은 없는지 여유롭게 테스트해볼 수 있도록 제공하기도 한다. 유지관리서비스가 중단된(EOS)된 제품의 경우에도 가상패치를 통해 공격을 방어할 수 있어 효과적"이라고 강조했다.

최신 사이버위협 동향과 보안 실전 팁

알버트 곤잘레스는 '세계 10대 해킹 사건'을 추릴 때마다 언급되는 유명한 악의적 해커다. 신용카드 정보를 탈취해 사기 거래로 검은 돈을 벌었다. 한 번은 현금계수기가 고장 나 손으로 34만달러를 셌다고 불평했다는 얘기가 일화로 전해질 정도다. 알버트 곤잘레스는 FBI에 체포된 후 다른 해커의 인텔리전스 정보를 캐내기 위한 이중 간첩으로 일한 것으로 알려졌다.

존 클레이(Jon Clay) 트렌드마이크로 글로벌위협커뮤니케이션 디렉터는 한국트렌드마이크로가 개최한 '클라우드섹(CLOUDSEC) 코리아 2018' 기조연설에서 "많은 이들이 해커를 어두운 지하실에서 일하는 10대의 모습으로 연상하는데 현실은 전혀 다르다"며 곤잘레스를 언급했다. 곤잘레스는 사람들이 해커와 해킹에 대해 갖고 있는 편견을 뒤집는 사례라는 것이다.

사이버공격의 위험은 곤잘레스가 한참 활약할 당시보다 더 커지고 있다. 더 많은 사람과 기기가 인터넷으로 연결되고 있어서다. 세상의 모든 것이 연결되면서 데이터가 엄청난 속도로 늘어나 더 많은 정보를 활용할 수 있는 세상이 열렸다. 이는 그만큼 사이버범죄자들의 공격대상이 많아졌다는 것을 의미한다. '안전하게 연결된 세상'이 필요한 시대가 왔다.

"인터넷으로 연결된 디바이스가 늘어나고 있다. PC 뿐만 아니라 토스터, 스피커, 프린터 같은 디바이스도 모두 연결이 되어 있고, 공격의 피해자이자 가해자가 되기도 한다."존 클레이 디렉터는 사이버공격이나 신원도용, 데이터 사기 같은 해킹 범죄의 증가율이 우상향 그래프를 그리고 있다고 설명했다. 이용자가 그 어떤 디바이스를 쓰든, 인터넷에 연결이 되어 있다면 곧바로 공격대상이 될 수 있는 시대이고, 또 그 어떤 이용자나 기기이든 절대 해킹이 불가능한 성역은 없다는 뜻이다.

그렇다면 최근 가장 위협적인 해킹 공격은 무엇일까?

트렌드마이크로 위협 인텔리전스를 통해 수집한 정보에 따르면, 2018년 상반기 차단된 사이버위협은 200억개에 달한다. 이메일 보안위협이 가장 컸다. 2분기 벌어진 사이버공격의 84%가 이메일에 의해 이뤄졌을 정도다. 특히 비즈니스이메일침해(BEC) 공격은 공격자들에게 큰 수익을 안겨다주고 있어 최근 몇 년간 꾸준히 늘어나고 있다.

암호화폐도 오늘날 가장 큰 위협 중 하나다. 존 클레이는 최근 언더그라운드 해커 포럼을 검색해 본 결과, 지난 한 해 이들의 커뮤니티에서 가장 많이 오고 간 키워드가 '암호화폐(Cryptocurrencey)'라는 것을 발견했다. 암호화폐 채굴을 위한 컴퓨팅 자원 해킹이 계속해 큰 위협이 될 것이라는 것을 짐작할 수 있는 부분이다.

암호화폐는 최근 가장 많이 언급되고 있는 랜섬웨어와 성격이 다르다. 랜섬웨어는 피해자의 데이터를 볼모로 돈을 요구한다. 이 때문에 피해자가 랜섬웨어 감염사실을 빨리 알아채야 한다. 그래서 해커

들은 팝업 메시지로 자신의 공격 사실을 피해자에 알린다. 그러나 암호화폐 채굴 공격은 은밀하게 진행될수록 좋다. 피해자가 감염 사실을 몰라야 더 오래 암호화폐 채굴 자원으로 피해자의 컴퓨터를 쓸 수 있다. 이같은 차이 때문에 이용자들은 자신의 컴퓨터가 암호화폐 채굴을 위한 자원으로 쓰이고 있는지, 감염 여부 자체를 알아내는 데만 수개월이 걸릴 수 있다고 존 클레이는 지적했다.

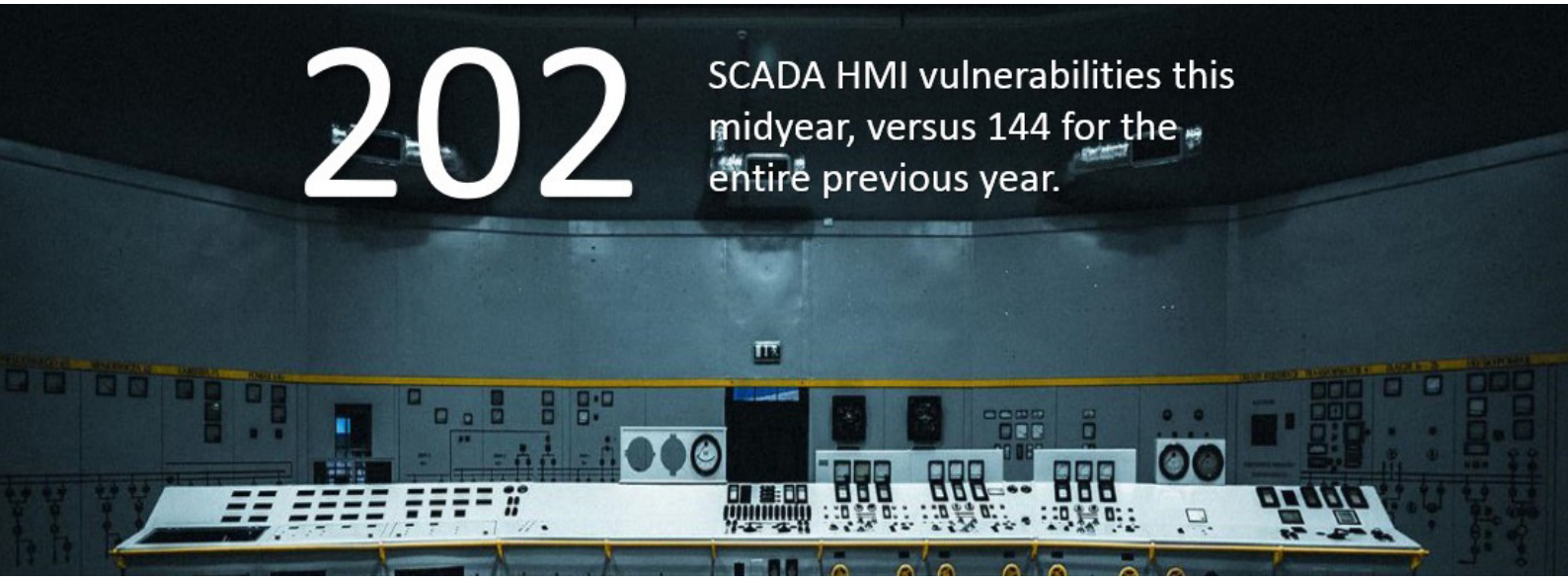
최근 사이버공격이 예전과 달리 '돈'을 중심으로 움직이고 있다는 점도 주목할 부분이다. 예전 해커들이 유명세를 얻기 위해 움직였다면, 랜섬웨어나 암호화폐 채굴을 위한 해킹 등은 결국 정보나 자원을 탈취해 더 많은 돈을 얻기 위한 위협으로 발전하고 있다는 것이다.

보안패치가 업데이트되기 전에 공격을 가하는 제로데이 공격도 기승을 부리고 있다. 트렌드마이크로에는 현재 3500명이 관련 버그를 연구하며 패치 작업을 하고 있다. 예를 들어 올 상반기 스카다(SCADA) 산업 자동화(HMI)에만 총 202건의 버그가 보고됐는데, 이는 직전 한 해 동안 발견된 버그 144개의 두 배에 가까운 수치다.

SCADA HMI는 수도나 전기 같은 매우 중요한 인프라에 쓰이고 있다. 트렌드마이크로 제로데이이니셔티브(ZDI)를 주축으로 최근 이같은 취약점 연구가 활발히 진행되고 있다. 지난해만 하더라도 관련 취약점이 발견됐어도 보고되지 않아 패치가 불가능했지만, 올 상반기에는 ZDI에서 그동안 발견 못했던 스카다 HMI 취약점을 발견해 모두 적용할 수 있게 됐다.

또한 트렌드마이크로는 알려지지 않은 사이버공격을 막기 위한 방안으로 인공지능(AI)과 머신러닝 기술도 연구, 적용하고 있다. 수십억개의 악성코드나 허니팟, 웹 URL 같은 정보가 결국은 상호 연결되는 데이터이기 때문에 이를 잘 분석해 패치 방법을 찾아낼 수 있다는 것이다.

클레이 디렉터는 "처음에는 피싱 메일 하나지만, 결국 네트워크 전체에 있는 정보를 탈취해가는 게 오늘날 공격 라이프사이클"이라며 "버그 파악 분석 프로그램인 가상패치를 적용해 우선적인 보호 조치를 취하고, 이후 완전히 공개된 패치를 적용하는 것도 하나의 대응방법"이라고 제시했다. By



전문가가 제시하는 보안 실전 팁

이용자의 데이터를 보호하는 첫 단계는 '비밀번호(password)' 관리다. 존 클레이 디렉터는 수십개의 계정마다 다른 비밀번호를 지정하는 것이 안전하지만, 이를 실제로 다 기억하기 힘드니 '패스워드 매니저'를 쓰라고 권유했다. 아울러 가족이나 직장 동료라고 하더라도 비밀번호를 공유하지 말 것을 권장했다. 비밀번호를 메모지에 적어 컴퓨터에 붙여 놓는 일도 당연히 금지다.

이메일 안전과 관련한 피싱 교육, 이중요소 인증 적용도 중요하다. 브라우저로 인터넷에 접근할 때 신뢰하는 링크라고 하더라도 검증이 필요하다. 클라우드 파일 공유에는 신중을 기하는 것이 좋다. 특히 기업 내부 직원들이 공유하는 클라우드 파일의 경우 수신인이 별다른 의심없이 주소를 클릭하게 되는데, 이때 악성코드가 딸려 올 수 있다. 사무실 외부에서 일할 때에는 공공 와이파이(WiFi)를 주의해 써야 하고, 업무 관련 대화는 가능한 피해야 한다.

이용자들이 모바일 기기를 공격 대상이라 인지하지 못해 별다른 보안조치를 취하지 않는 경우가 많은 것도 공격의 허점이 되기도 한다. 모바일 기기에도 비밀번호를 반드시 적용하고, 보안 소프트웨어와 이중인증을 적용하는 것이 좋다. 펌웨어 업데이트도 중요하다.

와이파이 라우터를 쓸 경우 로그인 정보를 주기적으로 바꾸는 것이 좋다. 원격관리는 가능한 쓰지 말고, 게스트를 위한 별도 액세스 아이디(ID)를 생성하라. 제품 구매시 기본 설정된 비밀번호는 즉시 바꿔야 한다. 그렇지 않을 경우 봇넷으로 악용되는 일이 발생할 수 있다.

TREND MICRO

하이브리드 클라우드 환경의 ‘Deep Security’

리눅스 서버와 컨테이너 보안 해법

By 바이라인네트워크

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

SPECIAL REPORT
BylineNetwork