진화하는 보안 위협, 다시 쓰는 보안 매뉴얼

사전/실시간/사후 대응으로 공격 전 과정을 빈틈없이 방어하는 시스코 시큐리티 서비스

Olaf G. Krohmann, Director, Global Security Solutions
Shyue Hong Chuang, Senior Security Architect, Global Security Solutions

사이버 공격은 갈수록 더 복잡해지고, 표적화되고, 집요해지면서 기업의 비즈니스를 위협하는 심각한 당면과제로 떠올랐습니다. 모든 것이 인터넷을 통해 연결된 '초연결사회(Hyperconnected World)'에서 진화하는 사이버 공격에 대처하려면, 위협에 집중하는 간결하고 확장 가능한 보안 모델을 갖춰야 합니다. 시스코의 새로운 보안 모델은 사이버 공격에 대한 사전, 실시간, 사후 대응을 하나로 묶은 보안 솔루션입니다. 이 모델은 총체적인 접근 방식을 통해 사이버 공격 전 과정에서 가시성을 확보할 수 있도록 지원합니다.

오늘날의 보안 솔루션은 최신 위협 동향과 총체적인 보안 모델을 구축하는 데 필요한 지원이 무엇인지 보다 철저하게 파악할 필요가 있습니다. 이에 따라 시스코는 사이버 공격 전 과정에 대응할 수 있는 보안 서비스를 개발했습니다.

전통적으로 기업 IT는 규제 준수와 위기 관리 요구사항 때문에 알려진 공격 범위를 최소화하는 보안 프레임워크에 무게를 두었습니다. 그러나 총체적인 보안 접근 방식의 경우 보안팀은 전 공격 과정에 보안 렌즈를 들이대고 철저하게 검사해 위협을 분석해야 합니다.

시스코는 시스코 Security Control Framework[1]를 네트워크 보안을 분석하는 기본 렌즈로 삼아 보안의 근본적인 두 가지 목표인 가시성과 제어력을 확보하기 위해 어떤 조치들이 필요한 지 분석하고 있습니다. 우회와 감염된 신뢰관계를 통해 공격 과정에서 그 경로와 수법이 끊임없이 진화하기 때문에 기업은 제어해야 할 보안 대상이 변하고 있다는 사실과 번번히 마주하게 됩니다.

사전 대응

당연한 말이지만 방어 대상이 무엇인지 파악하는 게 중요합니다. 접속된 애플리케이션과 시스템의 중요도에 따라 사용자 신뢰 수준을 분류할 필요가 있습니다. 모빌리티와 클라우드 서비스로 인해 분류 작업이 더 복잡해질 수 있습니다. 방어 대상을 규명하고 나면 모니터링 도구가 가동합니다. 모니터링 도구는 대략 두 가지로 구분되는데요, 전통적인 SIEM (security information and event management 보안 정보 및 이벤트 관리) 도구와 Open SOC(Security Operation Center) 모델을 따라 개발된 첨단 도구 세트가 있습니다. 이 단계에서는 다수의 기기와 애플리케이션 로그에서 데이터를 수집해 분석하는데요, 시그니처 기반 도구만큼이나 행동 분석이 중요해지고 있습니다. 대량의 데이터는 물론이고 데이터와 평판 로그와의 상관관계 정보까지 처리한다는 것은 곧 빅데이터를 처리한다는 의미입니다. 그래프 클러스터 알고리즘처럼 새로운 분석 방식이 필요한 이유가 여기에 있습니다.

고객의 IT 환경을 비즈니스 관점에서 적절한 수준으로 제어하기 위해, 우리는 다음과 같이 계층 방어를 제안합니다. 경계를 강화하고, 신뢰구간을 설정하고, 비즈니스 규정에 따라 각기 다른 보호 프로필을 지원할 수 있도록 인프라와 애플리케이션 전반에 걸쳐 구획을 설정하는 것입니다. 중요 자산이 무엇이고 그것을 어떻게 보호할 것인지 알기만 하면, 보안 제어 실행을 위한 규칙과 정책에 기반하여 화이트 리스트를 생성할 수 있습니다.

실시간 대응

네트워크가 공격받고 있을 때는 민첩성이 무엇보다 중요합니다. 공격 과정 중 사전 대응 단계에서 확보한 가시성과 제어 조치는 공격받는 대상을 감지하고 비즈니스에 미치는 위험을 신속하게 파악하는데 기여합니다. 시그니처 기반 침입 방지 제어 솔루션에 대한 적절한 업데이트를 설치했거나, 위협에 대한 실시간 보안 인텔리전스 제공 서비스에 가입한 경우라면 시그니처 기반의 공격은 대개 신속하게 차단됩니다.

지능형 지속공격 ATP(Advanced Persistent Threat)가 발생하면 행동 분석이 필요한데요, 이를 위해서는 해당 IT 인프라에서 비정상적 행동이 무엇인지 알고 있어야 합니다. 따라서

[1] http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/CiscoSCF.html

© 2014 Cisco and/or its affiliates. All rights reserved.

정상적 행동에 대한 가이드라인을 수립하는 사전 조치가 필요합니다. 이 단계에서는 해킹된 네트워크 내부에서 우회 공격을 시도할 수 있기 때문에 알려진 감염 노드 및 사용자에 대한 블랙리스트를 작성하거나, 네트워크 트래픽 흐름을 청소하는 것이 보안 목표가 될 것입니다. 블랙리스트의 신뢰성은 여러분의 보안 가시화 솔루션이 얼마나 정확하고 시의 적절하게 악성 트래픽을 식별해 내느냐에 달려 있습니다.

"악성코드 멀웨어(Malware)와 APT를 이용한 공격 수법이 점점 더 정교해지고 있습니다. 기본 보안 어플라이언스만 으로는 이런 위협들을 더 이상 해결할 수 없기 때문에, 대부분의 기업들이 보안 관리에 어려움을 겪고 있습니다."

Bryan Palma, Global Security Solutions,
Senior Vice President and General Manager

사후 대응

소동이 가라앉고 복구를 진행할 때 보안 목표는 다시 한 번 치료에 집중하는 것입니다. 치료에는 패치 및 복구 외에도 재발 방지를 위해 보안 가시성과 제어 수준을 점진적으로 개선시키는 일이 포함됩니다.

감염된 호스트나 사용자가 휴면상태에서 벗어나면 정찰, 명령 및 제어 통신용 채널을 가동하거나 데이터 탈취를 시도할 수 있기 때문에 네트워크가 이들을 신속하게 식별할 수 있어야 합니다. 감염된 노드와 사용자를 확실하게 식별해 격리시킬 수 있는 능력이 요구되며, 이때 무결성 검증과 트래픽 흐름 분석이 중요한 역할을 할 수 있습니다.

IT 인프라에 대한 가시성을 공격 전 과정에 걸쳐 지속적으로 확보하는 것이 보안 아키텍처를 수립하는 데 있어서는 매우 중요합니다. 공격 시뮬레이션 및 평가를 통해 IT 인프라에 대한 통찰력을 이끌어 내는 방안도 고려해볼 만 합니다. 보안에 있어서 기술적 제어를 구현하는 것도 중요하지만, 가장 효과적인 제어는 보다 숙련된 보안 프로세스 또는 능숙한 사고 조사에 달려 있다는 사실을 여러분도 아실 겁니다.

지금까지 공격과정에 따라 단계별로 설명해 드린 보안 관점을 이해하셨다면, 여러분은 아마도 현재와는 다른 보안 아키텍처를 염두에 두고 계시겠지요. 시스코 2014년 연례 보안 보고서(2014 Annual Security Report)에 언급된 것처럼, 이제 인터넷 범죄자가 네트워크에 침입하는 것은 '만약'이 아닌 '언제', '어떻게' 침입하느냐의 문제가 되었으니까요.

시스코 사이버시큐리티(Cybersecurity) 서비스

시스코 사이버시큐리티 서비스는 기업이 정보 보안 프로그램의 제어 수준과 가시성을 사전 대응, 사후 대응, 실시간 대응 등 보안 전 단계에 걸쳐 향상시킬 수 있도록 돕는 서비스로, 설계, 구축, 관리 서비스로 구성되어 있습니다. 시스코는 이상 감지 및 복원 기능을 지원하는 보안 네트워크 아키텍처를 기업의 위험 허용 범위를 반영하여 설계하고 구현할 수 있습니다. 고객사는 이 서비스를 통해 보안 운영을 직접 관리하거나 선별적으로 위탁함으로써 안전, 지적 자본, 재정, 프라이버시를 위협하는 현재의 공격과 새로운 공격에 유연하게 대응할 수 있습니다.

시스코 사이버시큐리티 서비스는 다년 간의 보안 서비스 구축 및 운영 경험을 가지고 있으며, 시스코 사내 보안 운영에 적용해온 보안 툴과 기술을 사용합니다.

2014년 시스코 연례 보안 보고서 다운로드
http://dcg.cisco.com/go/4h