Akamai

백서

DDoS 방어에 관한 9가지 잘못된 통념

지난 2년 동안 DDoS(Distributed Denial-of-Service) 공격 규모는 두 배가 되었습니다. 공격 기법의 수와 조합 역시 크게 증가했습니다. 2020년에는 한 기업이 809Mpps(초당 백만 패킷)에 이르는 공격을 받으면서 초당 패킷 수 기준으로 사상 최대 규모의 공격이 기록되었습니다. DDoS 공격을 받을 가능성이 낮다고 스스로 판단하는 기업들도 있습니다. 하지만 모든 업계의 비즈니스 크리티컬 서비스 및 애플리케이션은 공격 대상이 될 확률이 높습니다. 인프라를 보호하지 않을 경우 모든 비즈니스가 다운타임에 노출되며 성능 저하 문제를 겪게 됩니다.

DDoS 방어는 전반적인 보안 전략의 핵심 요소가 되어야 합니다. 따라서 잘못된 통념을 인식하는 것이 DDoS 방어 체계에 중요합니다.

세상에는 DDoS 방어에 관한 수많은 잘못된 통념이 있습니다. 심지어 보안 벤더가 이러한 통념들 중 일부를 확대 전파하기도 합니다.

잘못된 통념 1. 총 용량은 사용 가능한 방어 리소스를 나타낸다.

단순한 네트워크 용량 수치만으로는 중요한 세부 정보가 전달되지 않습니다. 따라서 다음과 같은 질문을 던져야 합니다. '공격 트래픽을 처리하는 데 쓰이는 네트워크 용량은 어느 정도인가?' '공격 차단에 사용되는 방어 시스템의 리소스는 몇 개인가?' '플랫폼의 모든 고객 오리진에 정상 트래픽을 제공하기 위해 사용할 수 있는 네트워크 및 시스템 리소스는 몇 개인가?' 용량은 기술에만 국한되지 않습니다. 기술이 효과적으로 작동하지 않거나 방어를 최적화하지 못하는 경우 에스컬레이션, 인시던트 대응, 방어 조치 세부 조정 작업에 어떤 전담 인력을 활용할 수 있습니까?

팁: 서비스 제공업체의 전체 네트워크 용량과 플랫폼 안정성, 공격 방어에 제공되는 용량, 정상 트래픽 전송 사용률 간의 차이점을 자세히 살펴보는 것이 좋습니다.

잘못된 통념 2. 모든 공격 방어 시간 SLA는 동일하다.

공격 방어 시간은 정상 트래픽과 사용자에게 영향을 주지 않으면서 얼마나 빨리 악성 트래픽을 차단하는지를 의미합니다. 이 부분에서 다른 해석의 여지가 발생할 수 있습니다. 예를 들어, 어떤 벤더는 트래픽 급증이 최소 5분 이상 지속되지 않으면 이를 DDoS 공격으로 간주하지 않을 수 있습니다. 이 경우 공격이 시작된 지 5분이 지나기 전까지 SLA 타이머가 작동하지 않을 것입니다. 따라서 해당 벤더가 광고한 '10초 공격 방어 시간'은 실제로 5분 이상이 될 수 있습니다. 또 다른 벤더는 방어 규칙을 얼마나 빨리 배포할 수 있는지를 두고 공격 방어 시간을 정의합니다. 결론적으로 기업의 인터넷 기반 자산을 다시 가동하는 데 걸리는 시간이 가장 중요합니다. 벤더 SLA의 세부 사항을 주의 깊게 읽으시기 바랍니다.

팁: SLA에 나열된 공격 방어 시간에 대한 세부 정보를 확인해야 합니다. 이 세부 정보는 '공격 탐지에 걸리는 시간 + 방어 컨트롤 적용에 걸리는 시간 + 공격 차단에 걸리는 시간 + 방어 품질 = 실제 공격 차단에 걸리는 시간'을 나타내야 합니다.

잘못된 통념 3. 블랙홀링 및 전송률 제한은 적절한 방어 조치이다.

블랙홀링(Blackholing)은 일부 DDoS 방어 서비스 제공업체가 일반적으로 사용하는 방어 조치입니다. 자산이 공격을 받고 다른 고객이 위험에 처할 경우 서비스 제공업체는 해당 리소스의 트래픽을 가상 블랙홀에 폐기하여 부수적인 피해를 방지할 수 있습니다. 하지만 이 방법이 실질적으로 도움이 될까요? 공격자의 관점에서 블랙홀링이란 미션을 완수했다는 것을 의미합니다. 즉, 공격 대상의 자산이 효과적으로 오프라인 상태가 되었다는 것입니다. 서비스 제공업체의 인프라에 따라 다른 고객이 오프라인 상태가 되거나 성능 저하를 겪을 수 있습니다. 또 다른 대응책으로, 많은 제공업체는 공유 환경 내의 대응 조치로서 고객 트래픽 전송률을 제한하고 있습니다. 하지만 자산이나 서비스가 계속 가동되는 것처럼 보이기 위해 정상 트래픽의 20%~40%를 줄이는 행위는 공격을 받는 고객이 원하는 결과가 아닙니다.

팁: 평상시 또는 공격을 받을 때 얼마나 자주 블랙홀링이나 트래픽 전송률 제한 조치를 취하는지 서비스 제공업체에 문의하시기 바랍니다. 서비스 제공업체가 어떤 상황에서 트래픽을 블랙홀링할 것인지, 서비스를 복원하기 위해 충족해야 할 기준은 무엇인지 알아보는 것이 좋습니다.

잘못된 통념 4. 클라우드 플랫폼을 누구와 공유하는지는 중요하지 않다.

모든 기업은 보안이 필요합니다. 도박, 음란물 웹사이트 등의 그레이 마켓(Gray Market)과 같이 논란이 많은 기업들은 자주 공격의 대상이 되며, 이러한 기업들 역시 방어를 필요로 합니다. 심지어 범죄 활동과 테러 공격을 장려하는 조직에서도 정상적인 클라우드 벤더로부터 사이버 보안 서비스를 구매했습니다. 일반적인 기업과는 상관없는 일처럼 보일 수 있지만, 불법 기업 또는 자주 공격을 받는 기업과 클라우드 보안 플랫폼을 공유하는 경우 부수적인 피해를 볼 가능성이 높습니다. 벤더의 리소스가 고갈되거나 사용할 수 없는 상태가 되어 기업이 위험에 노출될 수 있습니다.

불법 기업 또는 자주 공격을 받는 기업과 클라우드 보안 플랫폼을 공유하는 경우 기업이 부수적인 피해를 볼 가능성이 높습니다.

팁: 클라우드 보안 벤더의 제한적 사용 정책을 주의 깊게 읽고 보안 플랫폼 리소스를 고위험 대상과 공유하지 않을 것임을 확인하시기 바랍니다.

잘못된 통념 5. 올인원 보안 플랫폼은 더 나은 보안 경험을 제공한다.

일부 서비스 제공업체는 단일 클라우드 플랫폼에 다양한 추가 서비스를 제공합니다. 이는 단기적으로 보안 제어를 배포하고 통합하는 데 필요한 기술적 복잡성을 줄일 수 있음을 의미합니다. 하지만 운영 환경의 다른 부분이 중단될 경우, 동일한 백엔드 인프라와 네트워크를 공유하는 여러 서비스는 운영 중단, 부수적인 피해, 안정성 문제에 취약해집니다. 원스톱 솔루션 벤더에서 단일 플랫폼 접근 방식의 한계로 인해 기능을 희생시키는 경우가 많습니다. 특정 기술 및 보안 문제를 해결하기 위해 설계된 맞춤형 CDN, DNS, DDoS 스크러빙 클라우드의 투명한 조합은 방어 체계를 최적화하기 위해 높은 수준의 방어 및 성능을 대규모로 제공합니다.

팁: 통합된 보안 경험을 구현하기 위해 동일한 인프라를 공유하지 않아도 된다는 점을 염두에 두어야 합니다. 다양한 기반 아키텍처로 원활한 사용자 경험과 고성능 방어 기능을 모두 사용할 수 있습니다.

잘못된 통념 6. 온프레미스 솔루션으로 더 강력한 제어가 가능하다.

온프레미스 솔루션을 사용하면 기업에서 직접 제어를 할 수 있지만, 이는 착각일 수 있습니다. 모든 온프레미스 솔루션의 취약점은 주로 인터넷 대역폭의 용량입니다. DDoS 공격 규모가 점점 더 커지고 복잡해지면서(멀티벡터), 일반적인 4Gbps 미만의 공격도 인터넷 대역폭을 고갈시킴으로써 최고의 온프레미스 하드웨어를 갖춘 데이터센터에 DoS(Denial of Service)를 발생시킬 수 있습니다. 온프레미스 배포의 경우 결국 심각한 공격에 대한 방어 조치를 클라우드로 전환하기 위한 시간을 구매하는 것과 같습니다. 기업들은 보안 인력의 부족과 보안팀 운영의 부담으로 인해 사내 DDoS 방어 전문 지식을 개발하는 대신 클라우드 기반 플랫폼으로 DDoS 방어 솔루션을 아웃소싱하고 있습니다.

팁: 네트워크, IT, 사고 대응 직원의 부담이 가중되면 통제할 수 없습니다. DDoS 공격은 방어 전문가가 처리할 때 가장 잘 방어할 수 있습니다. 사내 부담을 최소화하고 전문가에게 아웃소싱하시기 바랍니다.

잘못된 통념 7. 여러 레이어의 방어는 필요하지 않다.

대부분의 기업이 실제로는 이러한 통념에 동의하지 않으면서도, 마치 이 통념이 사실인 것처럼 방어 전략을 수립하곤 합니다. 하이브리드 접근 방식을 예로 들겠습니다. 온프레미스 보안 솔루션을 강화하고자 하는 기업이 동일한 벤더의 클라우드 기반 솔루션을 추가하여 업그레이드합니다. 원스톱 솔루션은 간편하지만 반드시 심층적 방어 수단을 제공하는 것은 아닙니다. 동일한 기반 기술로 여러 방어 레이어를 구축할 경우 레이어 간 동일한 갭(Gap)과 취약점을 공유하므로 똑같이 위험에 노출됩니다.

팁: 서로 다른 강점과 약점을 가진 우수한 기술을 여러 레이어에 걸쳐 적용하여 한 레이어의 갭을 다른 레이어로 방어하도록 합니다.

잘못된 통념 8. 모든 SOC는 동일한 수준의 지원을 제공한다.

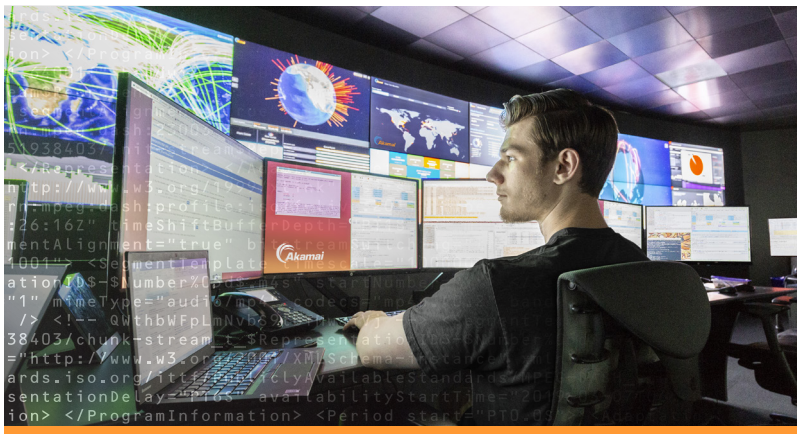
많은 벤더가 데이터 시트에서 보안관제센터(SOC) 지원을 광고하고 있습니다. 하지만 연중무휴 24시간 SOC 지원만으로는 충분하지 않습니다. 중요한 것은 자산이 공격당하고 있을 때 받을 수 있는 서비스와 전문 지식의 수준입니다. DDoS 방어 솔루션 제공업체를 평가할 때 다음과 같은 사항을 고려해야 합니다. '공격 전, 공격 중, 공격 후 어떤 유형의 지원 및 분석을 받을 수 있는가?' 'SOC는 지속적인 방어를 보장하기 위해 어떻게 구성되어 있는가?' 'SOC에 문의했을 때 만나게 되는 담당자가 실제 방어 조치를 수행하는 분석가인가, 아니면 단순한 에스컬레이션 담당자에 불과한가?' '벤더의 보안 전문가는 공격 방어 교육을 받았는가? 기존 방어 장치로 트래픽을 라우팅하는 일종의 교통경찰 역할만 하지는 않는가?' '맞춤형 런북을 제공하는가?' 보안 제공업체의 SOC가 실제 가치를 발휘하려면 사고 대응팀의 일원으로 역할을 수행해야 합니다.

팁: 서비스 제공업체의 SOC로부터 받을 수 있는 예상 지원의 품질을 평가해야 합니다. 공격 탐지 및 방어 조치 외에도 통합 및 테스트, 사고 문제 해결, 사후 분석(교훈), 공격면을 줄이는 데 도움이 되는 설계 지원을 제공하는지 알아보시기 바랍니다.

잘못된 통념 9. DDoS 방어 서비스는 포괄적이다.

저렴한 가격이 매력적으로 보일진 몰라도, 숨은 비용이 여기저기에 존재합니다. 일부 벤더는 저렴한 가격을 제공하지만 방어할 공격 건수나 규모를 제한합니다. 이러한 벤더는 공격의 횟수나 규모가 너무 클 경우, 기업이 온라인 비즈니스를 정상적인 상태로 복구하기 위해 애쓰는 동안에도 공격을 차단하기 전에 더 높고 비싼 서비스 티어로 업그레이드하도록 요구할 것입니다. 벤더와 가격을 비교할 때는 트레이드오프와 리스크 수준에 미치는 영향을 이해해야 합니다.

팁: 서명하기 전에 견적 가격에 포함된 내용을 이해해야 합니다.



일부 벤더는 공격의 횟수나 규모가 너무 클 경우, 기업이 온라인 비즈니스를 정상적인 상태로 복구하기 위해 애쓰는 동안에도 공격을 차단하기 전에 더 높고 비싼 서비스 티어로 업그레이드하도록 요구할 것입니다.

DDoS 보안은 복잡하고 시간이 많이 소요되며, 끊임없이 변화합니다. 클라이언트, 고객, 직원과 연결된 상태를 유지하는 것은 비즈니스의 기반입니다. 그 어떤 오류도 있어서는 안 됩니다. 그러나 혼자서 높은 비용을 부담할 필요는 없습니다. Akamai는 웹 보안을 위한 가장 신뢰할 수 있는 최대 규모의 클라우드 전송 플랫폼을 제공합니다. 자세한 내용은 www.akamai.com/secureapps에서 살펴보시기 바랍니다.

Akamai