Akamai

백서

DDoS 공격의 11가지 오해

분산 서비스 거부(DDoS) 공격은 최근 몇 년 동안 그 규모, 범위, 분포, 정교함이 급격히 증가했으며, 일부 기록적인 공격으로 인해 그 심각성이 더욱 부각되고 있습니다. 안타깝게도 여전히 많은 기업들이 충분히 방어할 수 있다고 생각하거나 표적이 될 가능성이 낮다고 생각하는 구시대적인 사고방식에 머물러 있습니다. 현실은 다음과 같습니다. 이러한 공격의 피해자들은 금융 서비스에서부터 이커머스, 게임에 이르기까지 모든 주요 업계에 걸쳐 있습니다. 실제로 헬스케어, 에너지 및 유틸리티, 교육 및 운송 등 중요한 공공 인프라에 대한 공격은 특히 우려되고 있습니다. Akamai는 2023년에 아시아 태평양 지역의 한 고객을 초당 900기가비트(Gbps)의 대규모 공격으로부터 보호했습니다. 같은 해 말에는 미국 금융 서비스 고객을 대상으로 한 역대 최대 규모의 공격 중 하나인 복잡한 공격 기법이 혼합된 634Gbps, 초당 5500만 패킷(Mpps) 공격을 방어했습니다. 이는 Akamai가 지금까지 방어한 공격 중 가장 큰 규모인 1.44Tbps, 385Mpps의 전 세계 분산 공격에 이어 두 시간 가까이 지속된 공격입니다. 이러한 이벤트를 통해 사이버 범죄자들이 계속해서 경제의 주요 핵심 영역을 공략하고 있다는 것을 알 수 있습니다.

이러한 공격의 규모 때문에 일부 소규모 기업은 DDoS 공격의 표적이 될 리스크가 낮다고 생각할 수 있지만, 현실은 모든 업계의 비즈니스 크리티컬 서비스 및 애플리케이션이 쉽게 표적이 될 수 있다는 것입니다. 정치적, 이념적 동기를 가진 핵티비스트의 증가와 Killnet 및 Anonymous Sudan과 같은 사이버 범죄 집단이 제공하는 서비스형 DDoS의 상대적으로 저렴한 비용으로 인해 거의 모두가 표적이 될 수 있습니다. 기업들은 초기 공격뿐만 아니라 지속적인 공격도 우려해야 합니다. 공격자들이 동시 랜섬웨어 DDoS(RDDoS)나 삼중 갈취 캠페인과 같은 기타 악성 공격을 시도하는 동안 네트워크 및 보안 리소스를 분산시키기 위한 연막으로 DDoS 공격이 점점 더 많이 이용되고 있습니다. 마지막으로, 고도로 정교하고 분산된 DDoS 공격을 조율하기 위한 인공 지능 툴의 도입이 증가하고 있으며 이는 일관된 가용성과 성능을 보장해야 하는 기업 및 공공기관에 중대한 방어 과제를 안겨주고 있습니다.

위협이 점점 더 복잡해지고 하루가 다르게 진화함에 따라 안타깝게도 DDoS 방어에 대한 많은 오해가 여전히 존재하며, 그 중 일부는 보안 벤더사에 의해 조장되기도 합니다. DDoS 방어는 보안 전략의 기본 원칙이기 때문에 이러한 잘못된 통념이 DDoS 방어에 미치는 위험을 정확하게 이해하는 것이 중요합니다.

오해 1

총 용량은 사용 가능한 방어 리소스의 전체 범위를 나타낸다.

총 용량이 중요하지만 단순한 네트워크 용량 수치는 중요한 세부 정보를 생략하여 오해를 일으킬 수 있습니다. DDoS 방어 기술 솔루션을 평가하는 기업은 다음과 같은 질문을 해야 합니다.

- 공격 트래픽을 처리하는 데 쓰이는 네트워크 용량은 얼마나 됩니까?
- 방어 시스템의 리소스 중 공격 차단에 **명시적으로 할당된** 리소스는 얼마나 됩니까?
- 해당 플랫폼의 모든 고객 오리진과 각 고유 테넌트에 정상 트래픽을 전송하는 데 사용할 수 있는 네트워크 및 시스템 리소스는 얼마나 됩니까?

이러한 질문은 중요합니다. 왜냐하면 네트워크 총 용량에 콘텐츠 전송 등 다른 요구 사항도 포함되어 있다면 실제 DDoS 방어 용량은 사업자가 주장하는 것보다 훨씬 작을 수 있기 때문입니다.

DDoS 방어 용량은 기술에만 국한되지 않습니다. 어느 시점에 기술이 효과적으로 작동하지 않는다면 에스컬레이션, 인시던트 대응, 미세 방어 조정을 위한 전담 인력이 있습니까? 가장 강력한 방어는 자동화 및 머신 인텔리전스와 사람의 전문 지식을 결합해 심층적인 방어 기능을 제공하는 것입니다.

팁

공급업체의 총 네트워크 용량과 플랫폼 안정성 간의 차이점, 공격 방어, 정상 트래픽 전송을 위한 용량을 얼마나 보유하고 있는지 자세히 살펴보세요. 이러한 세그먼트는 고유한 세그먼트로 간주되어야 합니다. 예를 들어 공격 트래픽의 네트워크 라우팅, 공격 트래픽 차단 또는 방어, 정상 트래픽을 데이터 센터로 다시 전송하는 등 목적별로 용량을 할당해야 합니다.

오해 2

인터넷 서비스 사업자 또는 클라우드 서비스 사업자의 DDoS 방어는 충분하다.

안타깝게도 많은 기업들은 여전히 인터넷 서비스 사업자(ISP)가 제공하는 보안 기능이 충분하다고 생각합니다. 현실은 다음과 같습니다. ISP는 일반적으로 대역폭이 제한적인 상용 DDoS 방어 서비스만 제공합니다. ISP의 하드웨어는 자체 인프라와 사용자 간에 공유되기 때문에 용량 및 CPU 사이클이 제한됩니다. 이제 DDoS 공격은 두 인프라를 모두 압도할 정도로 방대해졌으며, ISP는 다른 프로덕션 리소스에 대한 부수적인 피해를 방지하기 위해 트래픽을 널 라우팅(블랙홀링)합니다. 모든 트래픽을 블랙홀링함으로써 기업은 최종 사용자의 정상적인 트래픽과 서비스를 잃게 되며, 이로 인해 공격이 성공하게 되어 실질적으로 비즈니스가 오프라인 상태가 됩니다.

또한, 클라우드 서비스 사업자(CSP)가 고객이 직접 제어를 설정하고 CSP의 클라우드 환경 내에서 보안 체계에 대한 주권을 유지할 수 있도록 허용하는 경우도 있지만, 대부분의 CSP는 일반적으로 책임을 지지 않고 고객에게 불법 DDoS 트래픽에 대한 요금을 청구하는 경우가 많습니다. 이러한 경우, 최신 DDoS 공격의 규모와 크기에 따라 피해자에게 상당한 초과 비용으로 이어질 수 있습니다.

팁

ISP 또는 CSP와 DDoS 방어 조항을 면밀히 검토하고 협상하세요. 또한 ISP가 클라우드 백업과 함께 강력한 온프레미스 DDoS 방어 하드웨어를 사용하는지 확인하여 작지만 빠른 DDoS 공격은 온프레미스에서 방어하고 대규모 증폭 공격은 클라우드 DDoS 방어 서비스를 통해 적절히 방어할 수 있도록 해야 합니다.

오해 3

모든 방어 시간 SLA는 동일하게 만들어진다.

때로는 숫자가 오해를 불러일으킬 수 있습니다. 방어 시간(TTM)은 보안 벤더사들이 자주 마케팅하는 수치입니다. TTM은 정상적인 트래픽과 사용자에게 영향을 주지 않으면서 악성 DDoS 트래픽을 얼마나 빨리 차단하거나 정지시키는지를 의미합니다. 하지만 여기에는 많은 해석의 여지가 있습니다. 예를 들어, 어떤 벤더사는 트래픽이 급증해도 최소 5분 이상 지속되지 않으면 이를 DDoS 공격으로 간주하지 않을 수 있습니다. 따라서 이미 공격을 받고 있어도 SLA 타이머가 작동하지 않을 수 있습니다. 평균 공격 지속 시간이 5분 이하라는 점을 고려할 때 이 문제의 심각성을 알 수 있습니다. 즉, 벤더사가 광고한 10초의 방어 시간이 실제로는 5분이 넘을 수 있다는 의미입니다.

또 다른 벤더사는 방어 규칙을 얼마나 빨리 배포할 수 있는지를 두고 공격 방어 시간을 정의합니다. 이는 공격 차단이나 이 제어가 활성화되는 품질 또는 일관성을 반영하지 않습니다. 결국 중요한 것은 **정상적인 사용자나 서비스에 미치는 영향을 최소화하면서** 인터넷 기반 자산을 보호하고 백업 및 실행하는 데 걸리는 시간입니다. 벤더사의 SLA의 세부 사항을 주의 깊게 읽으시기 바랍니다.

팁

SLA에 나열된 공격 방어 시간에 대한 세부 정보를 확인해야 합니다. 이 세부 정보는 실제 중요한 시간 = 공격 탐지 시간 + 방어 조치 적용 시간 + 공격 차단 및 중지 시간 + 방어 조치의 품질 및 일관성을 알려줍니다. 정상적인 사용자에게 영향을 미치지 않으면서 DDoS 공격을 방어할 수 있는 **진정한 0초 SLA**를 제공하는 벤더사를 선택하세요.

오해 4

널 라우팅(블랙홀링) 및 전송률 제한은 허용 가능한 방어 수단이다.

널 라우팅(블랙홀링)은 일부 DDoS 방어 서비스 공급업체의 일반적인 기본 방어 조치입니다. 자산이 공격을 받고 있고 해당 공격 용량으로 인해 다른 고객이나 서비스에 리스크가 있는 경우, 공급업체는 해당 리소스의 트래픽을 가상 블랙홀로 보내 부수적인 피해를 방지하려고 시도할 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 공급업체의 인프라에 따라 다른 고객이 오프라인 상태가 되거나 성능 저하를 겪을 수도 있습니다.

여러 보안 공급업체가 제공하는 또 다른 기본 DDoS 방어 조치에는 공유 환경 내의 대응책으로 고객 트래픽에 대한 속도 제한을 추가하는 것이 포함됩니다. 하지만 자산이나 서비스가 계속 가동되는 것처럼 보이기 위해 정상 트래픽의 20%~40%를 줄이는 행위는 공격을 받는 고객이 원하는 결과가 아닙니다. 속도 제한은 레이어 3, 4, 5에서 DDoS 공격을 처리할 때 2차 또는 3차 대응 수단으로 효과적입니다. 레이어 7 DDoS 공격에 직면했을 때는 속도 제한이 초기 제어 수단으로 더 효과적일 수 있지만 항상 시그니처 방어를 먼저 적용해야 합니다. 개방형 시스템 상호 연결 모델의 어떤 레이어에 영향을 미치든, 60% 이하가 아니라 100%의 디지털 인프라를 DDoS 공격으로부터 효과적으로 보호할 수 있어야 합니다.

팁

평상시와 공격을 받을 때 얼마나 자주 블랙홀링이나 트래픽 전송률 제한 조치를 취하는지 서비스 공급업체에 문의하시기 바랍니다. 서비스 공급업체가 언제 어떤 상황에서 트래픽을 블랙홀링할 것인지, 서비스를 복원하기 위해 충족해야 할 기준은 무엇인지 알아보는 것이 좋습니다.

오해 5

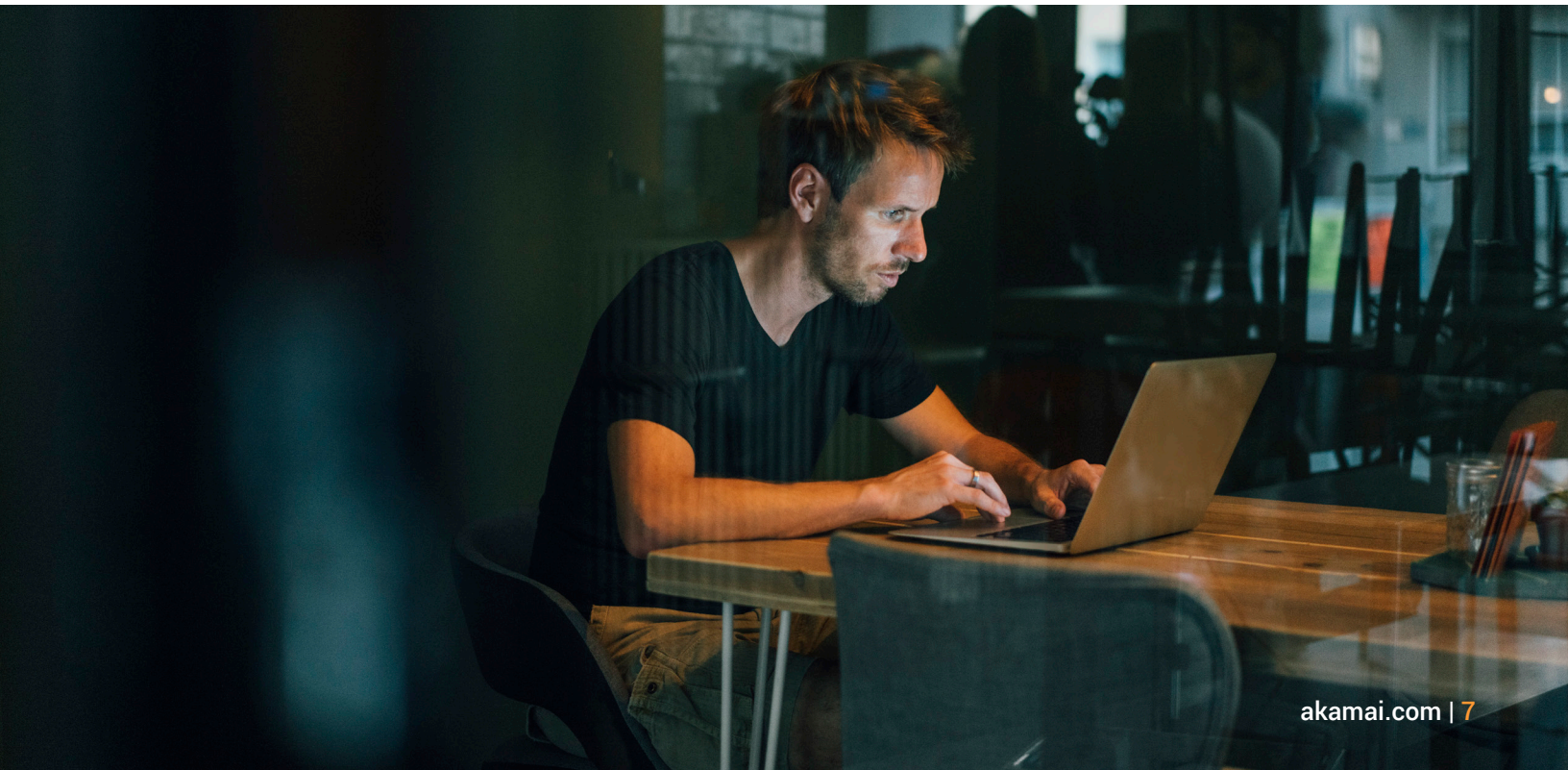
클라우드 플랫폼을 누구와 공유하는지는 중요하지 않다.

모든 기업은 보안이 필요합니다. 도박, 성인용 콘텐츠 웹사이트 등의 그레이 마켓(Gray Market)과 같이 논란이 많은 기업들은 자주 공격의 대상이 되며, 이러한 기업들 역시 DDoS 보안 방어를 필요로 합니다. 심지어 범죄 활동과 테러 공격을 조장하는 기업도 정상적인 클라우드 벤더사로부터 사이버 보안 서비스를 구매했습니다.

이러한 사이트는 자신과 상관없다고 생각하기 쉽습니다. 불법 기업 또는 자주 공격을 받는 기업과 클라우드 플랫폼을 공유하는 경우 부수적인 피해를 볼 가능성이 높습니다. 벤더사의 리소스가 고갈되거나 사용할 수 없는 상태가 되어 기업이 위험에 노출될 수 있습니다.

팁

클라우드 보안 벤더사의 제한적 사용 정책을 주의 깊게 읽고 보안 플랫폼 리소스를 고위험 대상과 공유하지 않는지 확인하시기 바랍니다. 또한 용량 및 기능에 관한 오해 1과 오해 2의 팁을 다시 한번 살펴보세요.



오해 6

웹 애플리케이션 방화벽은 DDoS 방어에 충분하다.

웹 애플리케이션 방화벽(WAF)은 대규모 웹 애플리케이션 및 API 보안(WAAP) 솔루션의 일부이며 애플리케이션 레이어(레이어 7) 공격에 효과적인 DDoS 방어 기능을 제공합니다. 기본 네트워크 레이어(레이어 3) 또는 전송 계층(계층 4) 방어 기능을 제공할 수 있지만 모든 IP, 포트 및 프로토콜을 포괄적으로 다루는 것만으로는 충분하지 않습니다.

DDoS 공격은 다양한 방식과 형태로 나타나고 있으며, 인프라 레이어(레이어 3 및 레이어 4), HTTP 애플리케이션 레이어(레이어 7) 및 DNS 인프라를 표적으로 삼을 수 있습니다. 또한 공격자들은 동적으로 공격을 전환하는 경우가 많으며, 예를 들어 DNS에서 시작한 후 다른 레이어나 프로토콜로 공격을 확장할 수 있습니다. 진정한 DDoS 방어는 레이어 3, 레이어 4, 레이어 7 및 DNS를 보호할 수 있는 특정 강점과 기능을 갖춘 강력한 솔루션 플랫폼을 도입하는 심층 방어 전략에서 비롯됩니다. 하나의 솔루션만으로는 항상 모든 기반을 커버하기에 충분하지 않으며, 정상적인 트래픽이나 서비스를 과도하게 방어하여 기업을 공격에 취약하게 만들고 더 높은 수준의 리스크에 노출시킬 수 있습니다.

팁

DDoS 방어 솔루션이 특정 종류의 DDoS 공격 또는 구축 설계에 편향되지 않도록 해야 합니다. 상호 운용성을 유지하고 통합된 신속 대응 보안 서비스 팀의 지원을 받아 프로덕션 리소스를 보호하는 여러 전용 DDoS 방어 기능을 제공할 수 있는 단일 벤더사가 최상의 보안을 유지할 수 있습니다. 이러한 자산이 하이브리드 네트워크 및 클라우드 호스팅 환경에 배포되면 상황은 복잡해집니다. 방어 서비스는 네트워크 또는 배포 모델과 무관해야 합니다.

오해 7

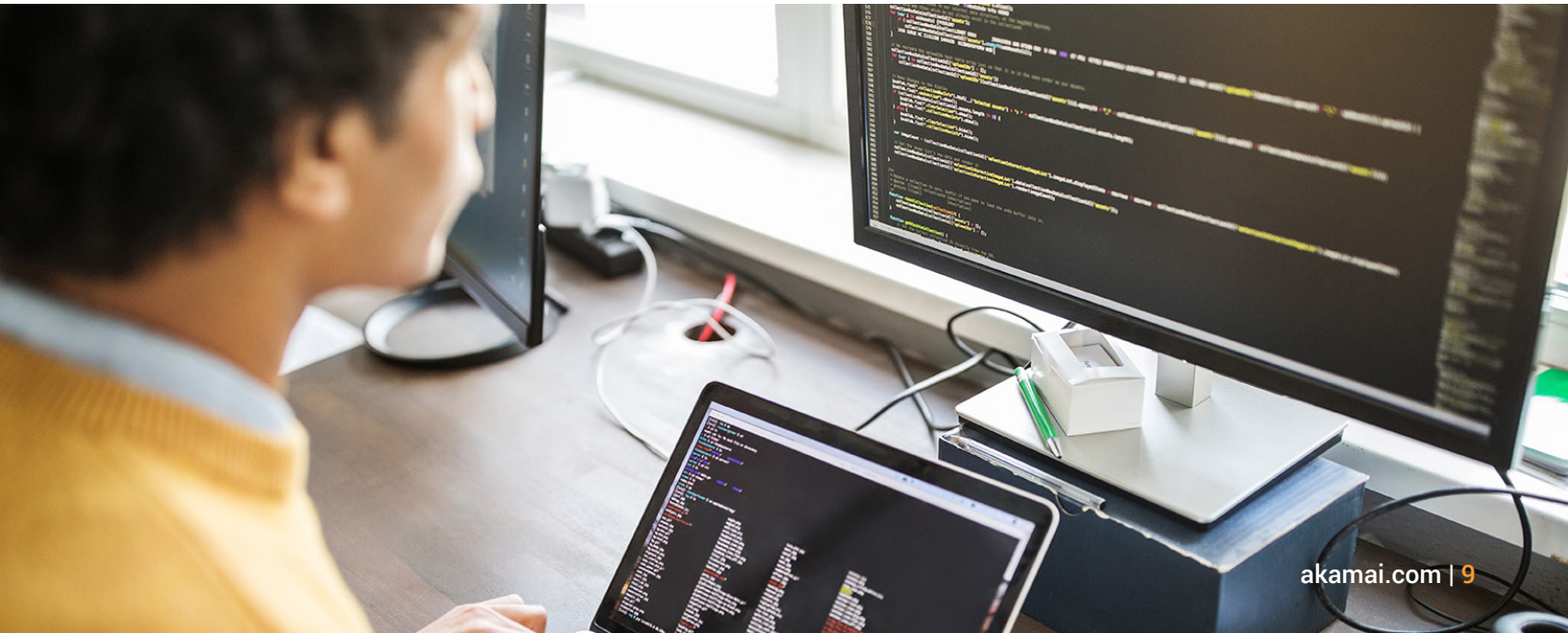
올인원 보안 플랫폼 = 더 나은 보안 경험

일부 공급업체는 단일 클라우드 플랫폼 위에 다양한 서비스를 제공합니다. 이로 인해 단기간 내에 보안 컨트롤을 배포하고 통합하는 데 따르는 기술적 복잡성이 줄어들 수 있지만 동일한 백엔드 인프라와 네트워크를 공유하는 여러 서비스는 환경의 다른 부분이 중단되는 경우 플랫폼 중단, 부수적인 손상 및 복구 문제에 취약합니다. 이러한 원스톱숍 벤더사는 단일 플랫폼 접근 방식의 한계로 인해 기능을 희생하는 경우가 많습니다.

특정 기술 및 보안 문제를 해결하도록 설계된 특수 목적의 CDN, DNS, DDoS 방어 플랫폼 또는 솔루션의 투명한 메시는 더 높은 품질의 완화 및 성능을 제공하여 방어 태세를 최적화합니다.

팁

통합된 보안 경험을 구현하기 위해 동일한 인프라를 공유하지 않아도 된다는 점을 염두에 두어야 합니다. 다양성을 기반으로 하는 방어 접근 방식에서는 원활한 사용자 경험과 고성능 보안 방어를 동시에 제공할 수 있는 기본 아키텍처를 사용합니다.



오해 8

IPv6에는 DDoS 방어가 필요하지 않다.

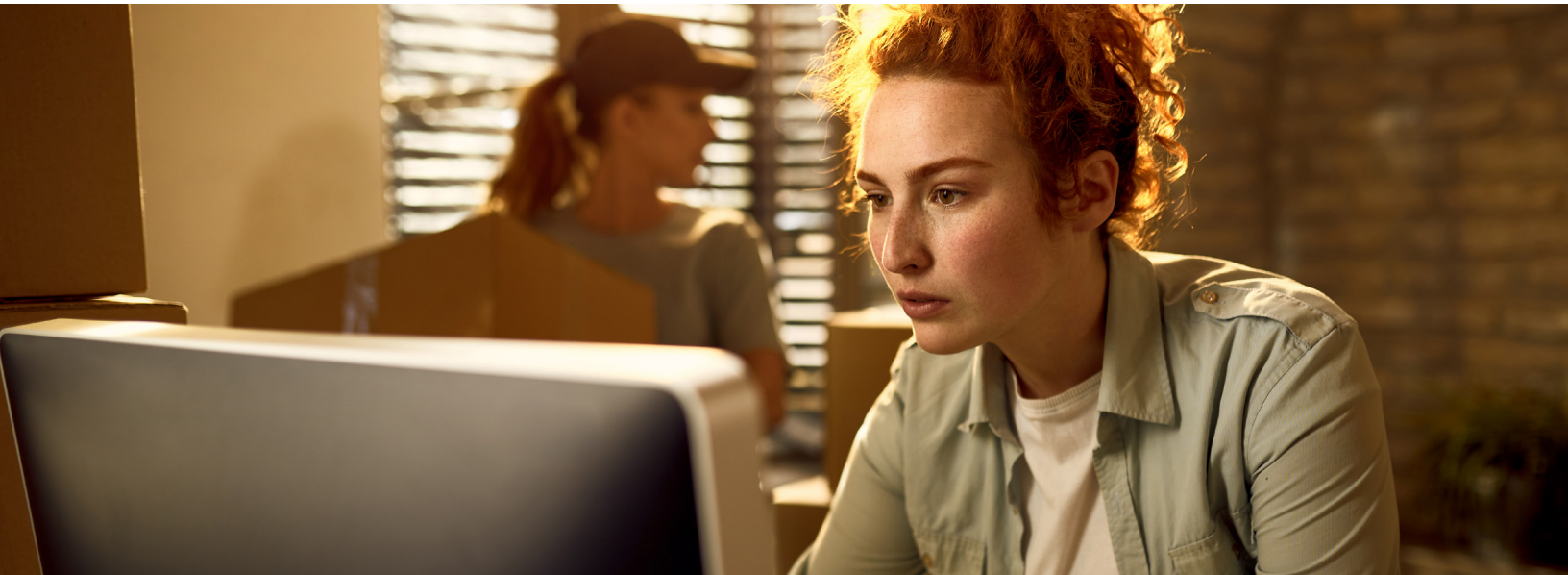
Google에 따르면 인터넷 트래픽의 약 45%가 IPv6 호환 디바이스에서 발생한다고 합니다. DDoS 공격 측면에서 IPv6는 IPv4보다 큰 주소 공간 및 IPsec과 같은 기본 제공 보안 기능과 같은 몇 가지 향상된 기능을 제공하지만, 이러한 종류의 공격에 대한 본질적인 방어 기능은 제공하지 않습니다.

DDoS 공격은 대량의 트래픽으로 네트워크를 압도하거나 취약점을 악용하거나 IP 버전과 무관한 다양한 공격 기법을 사용해 IPv4 및 IPv6 네트워크를 모두 표적으로 삼을 수 있습니다. 사이버 범죄자들은 이미 IPv6의 크게 확장된 IP 공간을 이용하여 훨씬 더 큰 규모의 DDoS 공격을 발생시키고 있습니다. 공격자들은 네트워크의 임의 주소로 트래픽을 전송하여 물리적 네트워크 레이어에 브로드캐스트 과부하를 일으키고 라우터 또는 네트워크 리소스를 묶어 소진시키는 경우도 있습니다.

일반적으로, 깨끗한 IPv6 환경을 보장할 수 없기 때문에 현재 IPv4와 IPv6 간의 세분화는 복잡성을 더욱 가중시킵니다.

팁

IPv6에 대한 DDoS 방어는 네트워크 모니터링, 트래픽 필터링, 속도 제한, 특수한 DDoS 방어 서비스 이용 등 IPv4와 유사한 전략과 기술을 필요로 합니다.



오해 9

멀티레이어의 방어는 필요하지 않다.

대부분의 기업은 이러한 오해를 실제로는 믿지 않지만, 간혹 사실인 것처럼 방어 전략을 수립하기도 합니다. 집을 보호할 때 현관문을 잠근다고 해서 뒷문과 창문을 열어두면 안 되는 것과 마찬가지입니다. 진정한 DDoS 방어는 공격자가 단 한 번의 공격으로 목표를 달성하지 못하도록 원활하게 작동하는 여러 겹의 보안 레이어를 구축함으로써 달성할 수 있습니다.

세계적 수준의 DDoS 방어는 네트워크 엣지에서 방화벽의 부하를 줄여주는 네트워크 클라우드 방화벽에서 시작됩니다. 그런 다음 하이브리드 DDoS 방어 모델에는 온프레미스 하드웨어 어플라이언스 기반 보호를 통해 짧지만 예리한 DDoS 공격을 방어하고, 대규모의 복잡하고 볼륨이 큰 DDoS 공격에 대해서는 전용 클라우드 기반 보호로 전환하는 것이 포함됩니다. 또한 네트워크 엣지에서 보안 정책을 동적으로 구축할 수 있는 프록시 서비스를 사용하고 기본 또는 보조 모드에서 권한 DNS 솔루션으로 추가 계층화하는 등 이와 유사한 계층화 전략으로 DNS 인프라를 보호해야 합니다. 마지막으로, WAF 기능이 포함된 강력한 WAAP 솔루션으로 모든 애플리케이션과 API를 보호해야 합니다.

팁

서로 다른 독특한 강점을 가진 동급 최고의 기술과 솔루션을 레이어화해 사이버 범죄자가 공격에 성공하기 어렵게 만드는 포괄적인 심층 방어 전략을 구축해야 합니다.

오해 10

모든 보안관제센터(SOC)는 동일한 수준의 지원을 제공한다.

많은 벤더사가 보안관제센터(SOC) 지원을 광고합니다. 하지만 연중무휴 24시간 SOC 지원만으로는 충분하지 않습니다. 중요한 것은 자산이 공격당하고 있을 때 받을 수 있는 서비스와 전문 지식의 수준입니다. DDoS 방어 솔루션 사업자를 평가할 때 다음과 같은 사항을 고려해야 합니다.

- 공격 전, 공격 중, 공격 후 어떤 종류의 지원 및 분석을 받을 수 있습니까?
- SOC는 방어의 연속성을 보장하기 위해 어떻게 인력을 배치합니까?
- SOC에 문의했을 때 만나게 되는 담당자가 실제 방어 조치를 수행하는 분석가입니까, 아니면 에스컬레이션 담당자입니까?
- 공급업체에 방어 교육을 받은 보안 전문가가 있습니까, 아니면 단순히 기성 방어 장비로 트래픽을 라우팅하는 일종의 '교통 경찰' 역할만 합니까?
- 맞춤형 런북을 제공합니까?

보안 공급업체의 SOC가 실질적인 가치를 제공하려면 인시던트 대응팀의 일원으로 역할을 해야 합니다.

팁

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

오해 11

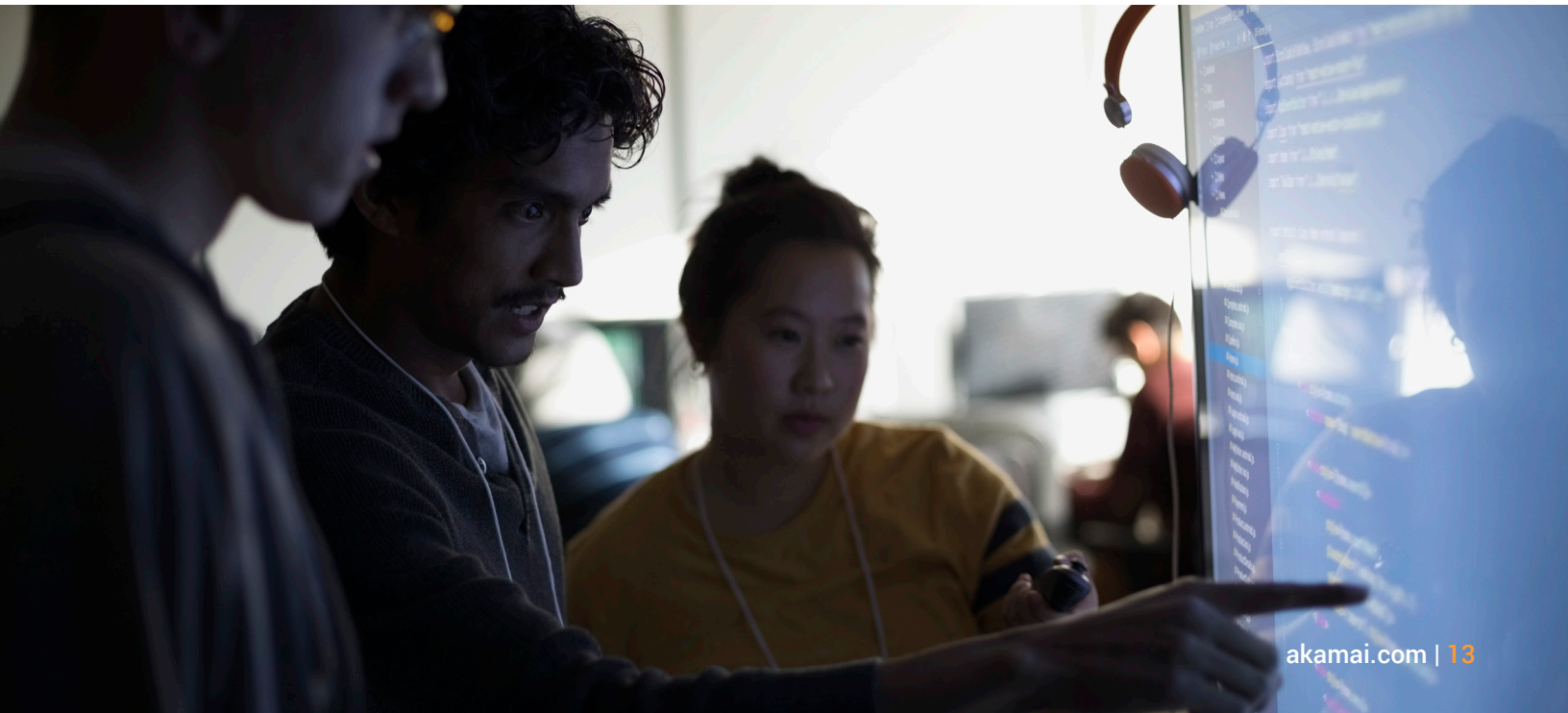
DDoS는 이제는 일반적인 공격 방식이므로, 기본적인 보안 조치만으로 충분하다.

"공짜 점심은 없다"라는 격언은 DDoS 방어에 있어 가장 적절한 표현일 것입니다. 저렴한 가격이 매력적으로 보일 수 있지만 숨겨진 비용이 있는 경우가 많습니다.

일부 벤더사는 저렴한 가격을 제공하지만 방어할 수 있는 공격의 수나 규모를 제한합니다. 이러한 벤더사는 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. 성숙한 DDoS 보안 벤더사는 고객이 '상시가동형' 및 '온디맨드' DDoS 방어 중에서 선택할 수 있는 유연성을 제공하고, 이들 사이를 원활하게 전환해 운영 비용을 낮게 유지하면서 동급 최고의 보호 기능을 제공합니다. 벤더사와 가격을 비교할 때 장단점과 DDoS 보안 체계에 미치는 영향을 이해해야 합니다.

팁

서명하기 전에 견적 가격에 포함된 내용을 이해해야 합니다.



DDoS 보안은 복잡하며 오늘날의 급변하는 환경에서 상당한 시간과 리소스가 필요합니다. 어제 효과적이었던 방법이 오늘 또는 내일은 작동하지 않을 수 있습니다. 최종 사용자, 고객, 직원과의 연결 상태를 유지하는 것은 비즈니스 성공의 토대입니다. 그 어떤 오류도 있어서는 안 됩니다. 그러나 혼자서 높은 비용을 부담할 필요는 없습니다. 가장 포괄적이고 유연하며 신뢰할 수 있는 DDoS 방어 플랫폼인 Akamai가 도와드릴 수 있습니다.

Akamai의 DDoS 보안 솔루션에 대해 자세히 알아보세요.

Akamai Security 소개

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com 및 akamai.com/blog를 확인하거나 X(기존의 Twitter), LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 10월 발행.