Akamai

보안

현대 로펌의 보안

중요 애플리케이션 및 클라이언트 데이터 보호

서론

법률 전문가는 매일 민감한 데이터를 처리합니다. 그래서 많은 회사가 보다 최신 보안 제어에 투자하고, 제로 트러스트 개념을 중심으로 IT 시스템과 프로세스를 설계함으로써 중요한 애플리케이션을 보호하고 최종 사용자 접속을 제어하는 데 주력하고 있습니다.

제로 트러스트 접근 방식은 최소 권한 모델을 구축해 권한이 부여된 사용자, 시스템 및 애플리케이션이 권한을 갖고 있는 기능에만 접속하게 함으로써 측면 이동, 랜섬웨어 및 무단 접속을 차단합니다. 제로 트러스트 접근 방식을 구축하는 가장 유연하고 안전한 방법 중 하나는 마이크로세그멘테이션을 활용하는 것입니다.

이제 몇 가지 과거 사례를 통해 이것이 왜 중요한지 살펴보겠습니다.

주요 보안 유출: 법률 업계에 울린 경종

지난 수년간 미국 연방 당국은 대형 로펌이 많은 기업 데이터를 보관하는 주요 장소이기 때문에 사이버 범죄자의 공격 대상이 되기 쉽다고 경고해 왔습니다. FBI는 2009년부터 유명 로펌들이 조직화된 사이버 범죄자의 표적이 되고 있다고 경고하기 시작했습니다. 2011년에는 200곳의 대형 로펌을 초청해 해당 분야를 대상으로 하는 정교한 사이버 공격의 증가 추세에 대해 논의했습니다.

> **제로 트러스트 접근 방식을 구축하는 가장 유연하고 안전한 방법 중 하나는 마이크로세그멘테이션을 활용하는 것입니다.**

Law.com에 따르면 2014년 이후 14개 주에서 100곳 이상의 로펌이 데이터 유출을 신고했습니다. American Bar Association의 2022년 Legal Technology Survey Report는 법률 업계의 기술 사용에 관한 연례 설문 조사로, 이에 따르면 모든 규모의 로펌 중 4분의 1 이상이 보안 유출 사례를 경험한 것으로 나타났습니다. 유출의 영향은 랜섬웨어로 인한 가동 중단부터 클라이언트 데이터가 인터넷으로 이전된 이후 법적 분쟁에 이르기까지 다양합니다.

2015년에는 해커가 표적으로 삼은 업계 순위에 관한 Cisco 연간 보고서에 법률 분야가 처음으로 등장했습니다. 그 결과, 많은 금융 기관이 로펌과 함께 비즈니스를 운영하는 경우 사이버 보안 관행에 대한 정기 감사를 받도록 로펌에 요구하기 시작했습니다.

특히 국제 로펌인 Mossack Fonseca & Co와 DLA Piper에서 발생한 두 건의 대규모 유출은 법률 및 금융 업계 전체에 경각심을 불러 일으켰습니다. 'Panama Papers'라고 불리는 이 유출 사건에서 해외 로펌인 Mossack Fonseca & Co.는 40년 동안 누적된 1천 백만 건이 넘는 문서가 유출되었습니다. 이 유출 사건으로 글로벌 기업과 영향력 있는 세계 리더들의 조세 피난처 및 해외 계좌가 노출되어 심각한 결과를 초래했습니다. 2018년 이 회사는 유출로 인한 피해로 운영을 중단한다고 발표했습니다. 로펌은 보유하고 있는 정보를 보호하기 위해 가능한 모든 노력을 기울여야 할 수탁자로서의 윤리적 의무가 있습니다. 'Panama Papers' 데이터 유출 사건은 로펌과 클라이언트 간 기밀 정보가 유출된 가장 큰 규모의 사례였고, 이 사건으로 법률 업계의 사이버 보안 접근 방식이 크게 변화했습니다. 그러나 보안 체계 개선에 대한 경각심이 높아졌음에도 공격자들은 속도를 늦출 기미를 보이지 않습니다.

> **로펌 4곳 중 1곳 이상이 유출을 경험했습니다.**
>
> - American Bar Association의 2022년 Legal Technology Survey Report

Mossack Fonseca & Co의 유출과 동시에 40여 개국에 진출한 세계 최고의 로펌 중 하나인 DLA Piper는 NotPetya 멀웨어 공격의 피해자가 되었습니다. 이로 인해 몇 주간 업무가 중단되고 수백만 달러의 영업 손실과 복구 비용이 발생했으며 평판이 크게 훼손되었습니다.

최근에는 Grubman Shire Meiselas & Sacks가 랜섬웨어 공격을 받아 레이디 가가(Lady Gaga), 르브론 제임스(LeBron James), 마돈나(Madonna) 등 유명 클라이언트에 관한 756GB의 데이터 손실이 발생했습니다. 로펌이 랜섬 지불을 주저하자 공격자들은 레이디 가가에 대한 정보를 유출하고 다른 클라이언트의 정보가 포함된 데이터를 경매에 부쳤습니다.

현대 로펌:
최신 사이버 보안 솔루션의 필요성

위에서 언급한 유출 사건은 대부분 민감한 클라이언트 데이터, 합병 정보, 지적 재산, 금융 정보를 훔치려는 목적으로 피싱, 멀웨어, 랜섬웨어를 포함한 APT(Advanced Persistent Threat) 공격과 연루된 것입니다. 막대한 금액에 현혹된 공격자들은 공격 툴과 전문 팀에 상당한 투자를 하는 조직적인 범죄 그룹의 지원을 받고 있습니다.

> **IT 환경에서 적절한 세그멘테이션이 이루어지지 않은 기업은 데이터 유출 시 피해 보험 청구가 거부될 수도 있습니다.**

이제 더 많은 클라이언트가 비즈니스 협력을 함께할 로펌 회사를 정할 때 사이버 보안을 중요한 요소로 고려하고 있습니다. 최신 보안 제어 기능이 없다면, 보안 체계를 개선하고 클라이언트의 데이터 보안을 중시하는 기업에 비즈니스 기회를 빼앗길 수 있습니다. 사이버 보험사도 민감한 데이터와 애플리케이션을 위한 일종의 세그멘테이션을 요구하는 경우가 많습니다. IT 환경에서 적절한 세그멘테이션이 이루어지지 않은 기업은 데이터 유출 시 피해 보험 청구가 거부될 수도 있습니다.

보완이 필요한 부분:
회사의 중요한 애플리케이션 보호

이와 같이 로펌은 더 이상 과거에 그랬던 것처럼 특권 정보의 안전한 저장소가 아닙니다. 오늘날 사이버 범죄자들은 로펌을 민감한 독점 기업 데이터의 저장소이자 사이버 보안 공격의 최적의 표적으로 인식하고 있습니다.

사실 로펌은 대부분의 클라이언트보다 더 쉬운 공격 대상으로 인식되곤 합니다. 그렇기 때문에 기업의 특정 데이터를 원하는 공격자는 먼저 로펌을 통해 데이터를 얻으려고 합니다. 저장된 데이터의 민감한 특성과 다양성, 그리고 일반적으로 취약한 보안 제어로 인해 로펌은 공격자들에게 유리한 표적이 됩니다.

공격자들은 로펌의 업무상 중요한 애플리케이션, 특히 문서 관리 시스템(DMS)과 이메일에 저장된 정보에 관심이 많습니다. IT 보안 측면에서 로펌의 가장 중요한 비즈니스 애플리케이션은 DMS와 이메일 애플리케이션입니다. 이러한 애플리케이션은 매우 기밀하고 민감한 특별한 클라이언트 정보를 공유하며, 대부분의 경우 더 이상 온프레미스 데이터 센터에만 상주하지 않습니다.

DMS 애플리케이션은 파일 및 폴더의 중앙 집중식 구성, 버전 관리, 이메일 관리, 문서 편집, 인덱싱, 검색, 권한 관리 등 광범위한 기능을 제공합니다. 이 애플리케이션은 가상화 서버와 베어 메탈 서버가 혼합된 이기종 IT 환경에 배포되는 경우가 많으며, 다양한 수준의 내부 보안을 이용하는 여러 다른 시스템과의 통합이 필요합니다. 이러한 통합을 통해 로펌은 DMS의 효율성을 높일 수 있지만, 이로 인해 보안이 약화되고 공격표면이 크게 증가할 수 있습니다.

기존의 보안 솔루션으로는 동적이고 모바일에 기반한 엔드포인트를 보호할 수 없습니다. 많은 기업과 마찬가지로 로펌도 주로 보안 툴에 대한 투자를 경계에 집중하고 있기 때문입니다. 경계 보안 솔루션은 더 이상 중요한 애플리케이션을 보호하는 데 필요한 수준의 보호 기능을 제공하지 못합니다. 또한 현재 많은 로펌에는 공격자가 감염된 엔드포인트를 통해 네트워크에 접속한 후 측면으로 이동해 민감한 데이터 시스템에 접속하는 것을 탐지하거나 방지하는 데 필요한 제어 기능이 여전히 부족한 실정입니다.

이 모든 과제에 직면한 수많은 최신 로펌들은 업계 고유의 변화하는 요구사항을 해결할 수 있는 차세대 사이버 보안 솔루션에 투자하기 시작했습니다. 소프트웨어 기반의 세그멘테이션, 특히 마이크로세그멘테이션은 권한 있는 사용자 및 시스템만 중요한 애플리케이션과 통신할 수 있도록 네트워크 내에서 통신을 제어하는 보다 정밀한 접근 방식을 제공함으로써 민감한 애플리케이션 및 데이터를 보호하며 제로 트러스트 접근 방식을 지원합니다. 이는 공격자가 네트워크 내에서 측면으로 이동하기 훨씬 어렵게 만들어 유출 가능한 범위를 제한합니다.

코로나19로 인해 더욱 어려워진 상황에서

- 원격 근무로 전환하는 로펌들
- 근무 방식의 전환으로 직원은 더 이상 회사 사무실이 아닌, 보안되지 않는 홈 네트워크를 통해 네트워크에 접속합니다.
- VPN 및 VDI 솔루션의 사용이 증가함에 따라, 보안 정책을 구축하고 네트워크 트래픽을 권한 있는 사용자로 제한하는 작업은 더욱 어려워졌습니다.

Akamai가 로펌의 클라이언트 데이터 보호를 지원하는 네 가지 방법

완벽한 가시성

포괄적인 워크로드 가시성을 확보해 민감한 데이터가 포함된 애플리케이션에 대한 모든 열린 연결을 파악할 수 있습니다.

사용자 접속 제어

온프레미스 또는 클라우드 어디에 있든 애플리케이션 및 데이터에 대한 접속을 제어하는 정책을 구축합니다.

소프트웨어 기반의 세그멘테이션

DMS 및 이메일과 같은 중요한 애플리케이션을 빠르고 유연하게 마이크로세그멘테이션해 유출 시 노출을 제한합니다.

위협 탐지 및 방어

동적 세그멘테이션과 디셉션 기능을 결합해 능동적인 유출을 탐지 및 격리하고 클라이언트 데이터를 보호합니다.

Akamai Guardicore Segmentation으로 보안 통합

Akamai Guardicore Segmentation은 비즈니스에 중요한 애플리케이션을 보호할 수 있도록 업계에서 가장 포괄적인 마이크로세그멘테이션 솔루션을 제공합니다. 이 솔루션으로 세그멘테이션 정책을 보다 빠르게 구축하고 지속적인 유지 관리를 간소화하며 궁극적으로 측면 이동에 의존하는 위협을 효과적으로 방어할 수 있습니다.

> **많은 로펌이 클라이언트 데이터를 보다 효과적으로 보호하기 위해, 권한 있는 사용자와 시스템만 중요한 애플리케이션과 통신할 수 있도록 네트워크 내 통신을 제어하는 보다 정밀한 접근 방식을 구축하기 위해 마이크로세그멘테이션과 같은 솔루션을 도입하고 있습니다.**

Akamai 솔루션은 데이터 센터의 모든 애플리케이션과 기타 자산 및 해당 의존성에 대한 시각적 맵을 제공합니다. 보안 운영자는 네트워크 및 프로세스 수준의 보안 정책을 빠르고 직관적으로 생성하고 적용해 중요한 애플리케이션과 자산을 격리하고 세그멘테이션할 수 있습니다. 이러한 소프트웨어 정의 세그멘테이션 접근 방식은 기본 인프라로부터 독립적이므로 IT가 온프레미스 시스템(기존 및 최신), VM, 컨테이너, 클라우드 및 디바이스의 전체 워크로드를 지속적으로 보호할 수 있습니다.

데이터 센터의 위치에 관계없이 개별 애플리케이션 또는 논리적으로 그룹화된 애플리케이션을 중심으로 정책을 생성할 수 있습니다. 이러한 정책으로 서로 통신할 수 있는 애플리케이션과 통신할 수 없는 애플리케이션을 지정함으로써 제로 트러스트 접근 방식을 지원할 수 있습니다. Akamai Guardicore Segmentation만의 또 다른 중요한 기능은 통합 유출 탐지 및 대응으로, 여러 전용 툴을 관리해야 하는 복잡성을 줄여줍니다. 유출 탐지 및 대응 기능은 뉴욕주 금융감독청(DFS)의 규정, PCI DSS와 같은 기타 업계의 요구사항을 준수하는 데 필요하며, 로펌에 대한 감사를 수행해야 하는 주요 고객에 의해 그 필요성이 계속 증가하고 있습니다.

Akamai Guardicore Segmentation: 중요한 애플리케이션을 위한 포괄적인 보호

클라이언트 데이터 보호: 제로 트러스트 프레임워크의 기반을 구축하며 더 복잡해지고 상호 연결이 강화되는 환경에서 네트워크 보안 위생 및 모범 사례를 적용합니다.

보다 광범위한 IT 인프라에서 중요한 애플리케이션 분리: DMS 또는 이메일 애플리케이션과 같은 고부가가치 자산을 링펜싱 정책으로 세그멘테이션해 법률 회사 안팎에서 위협에 노출될 가능성을 줄입니다.

안전하고 신속한 클라우드 도입: 전환 전에 워크로드를 매핑하고 모든 중요한 애플리케이션 및 해당 의존성에 대한 인벤토리를 확보합니다. 링펜싱 정책은 전환 프로세스 전반에서 워크로드에 따르는 일관된 보안의 기반으로 이러한 맵을 사용합니다. 이러한 접근 방식을 통해 워크로드를 클라우드로 보다 빠르고 안전하게 전환하고, 동일한 보안 제어 기능을 갖출 수 있습니다.

효율적인 유출 방어를 통해 비즈니스 연속성 보장: 동서 트래픽에 대한 정밀한 가시성을 확보하고 비정상적인 움직임을 알리도록 설정된 유출 지표를 사용해, 랜섬웨어나 다른 위협으로 인해 비즈니스가 중단되기 전에 공격자를 저지할 수 있습니다.

측면 이동 제한을 통한 리스크 감소: 내부 경계를 설정하고 비즈니스에 중요한 애플리케이션 및 시스템을 방어함으로써 공격표면을 줄입니다. 그러면 공격의 측면 확산을 효과적으로 방어해 유출 시 피해를 제한할 수 있습니다.

결론

Akamai Guardicore Segmentation은 로펌 공격에 사용될 수 있는 열린 연결을 시각화하고 이해할 수 있는 솔루션을 제공합니다. 이 솔루션을 통해 기업은 마이크로세그멘테이션으로 이러한 연결을 보호할 수도 있습니다.

Akamai 솔루션은 가상화 머신 및 베어 메탈 머신, 온프레미스, IaaS 또는 PaaS에 상주하는 하이브리드 IT 환경 전반에서 로펌의 중요한 애플리케이션에 대한 포괄적인 보안 범위를 제공합니다. 그리고 애플리케이션 의존성 및 흐름에 대한 가시성, 정밀한 세그멘테이션 정책 적용, 통합 유출 탐지 및 대응 기능을 제공합니다. 이러한 기능은 로펌의 비즈니스를 중단시킬 수 있는 데이터 손실 및 비즈니스 가동 중단 시나리오를 방지하는 데 있어 매우 중요합니다.

로펌은 Akamai Guardicore Segmentation을 사용해 환경을 더 잘 파악하고, 중요한 애플리케이션을 보호하며, 유출 시 미치는 영향과 응답 시간을 크게 줄일 수 있습니다. 솔루션과 함께 제공되는 소프트웨어 기반 세그멘테이션 기능은 기존의 방화벽을 포함한 다른 여러 세그멘테이션 솔루션에 비해 훨씬 더 비용 효율적이고, 시간을 절약해 주며, 더 유연하고, 더 효과적입니다. 결과적으로 Akamai Guardicore Segmentation은 업계 최고의 보안 솔루션으로서 오늘날 로펌의 보안 문제를 해결할 수 있는 완벽한 기능을 갖추었습니다.

클라이언트의 소중한 데이터를 보호하는 방법을 알아보세요.
akamai.com/guardicore에서 자세한 내용을 확인하시기 바랍니다.