AKAMAI 고객 사례

랜섬웨어 대응 및 복구에 Akamai 솔루션을 활용하는 유출 복구 서비스 기업

포괄적인 네트워크 가시성

IT 인프라 간 세그멘테이션

랜섬웨어 위협에 대한 대응

고객사

한 글로벌 장비 제조업체가 주요 보안 인시던트 발생 이후 미국의 유출 복구 서비스 제공업체와 계약을 체결했습니다.

도전 과제

빠르게 확산되는 랜섬웨어

한 글로벌 제조업체는 멀웨어 공격으로 인해 비즈니스 운영에 악영향을 받은 후 보안 침해 복구 서비스 기업과 협력해 IT 환경의 보안을 복원하고 개선하고자 했습니다. 직원의 노트북에서 시작된 공격은 기업의 백업 서버에 침투했을 뿐 아니라 빠르게 확산하면서 대부분의 운영 위치에 영향을 미쳤습니다.

솔루션 선택

방화벽 전체에 인터넷 접속 제한 룰을 적용하는 등의 초기 방어 방법은 빠르게 악화되는 보안 침해를 막기엔 너무 느렸습니다. 환경의 복잡성과 분산된 엔터프라이즈 네트워킹으로 인해 제한 룰 구현 및 적용이 느리고 효과가 없었습니다.

또한 레거시 컴퓨터에 대한 가시성은 보안 침해를 조사하고 방어하는 업무를 담당하는 인시던트 대응 담당자에게 중요한 문제였습니다. 유출 복구 서비스 기업은 멀웨어가 더 많은 자산에 측면 확산하기 전에 세그멘테이션을 신속하게 가속해야 할 필요성을 느끼고 Akamai Guardicore Segmentation을 추천했습니다.

Breach Remediation Company

업종
IT

솔루션
Akamai Guardicore Segmentation

주요 장점
- 측면 이동을 통한 랜섬웨어 확산 방어
- 네트워크 흐름에 대한 정밀한 가시성 제공
- 최신 및 레거시 머신 보안
- 신속한 인시던트 대응 지원

Akamai

Akamai Guardicore Segmentation의 장점

즉각적인 가시성

이 유출 복구 서비스 기업은 3시간 만에 3000대가 넘는 회사 서버에 Akamai 에이전트를 신속하게 프로비저닝했습니다. 또한 배포 후 불과 몇 분 만에 네트워킹 및 통신 흐름에 대한 정밀한 가시성을 확보했고, 인시던트 대응 팀이 유출 조사 및 격리 확인에 필요한 컨텍스트과 정확한 데이터를 확보할 수 있었습니다.

정책 적용 기간 단축

팀은 필요한 가시성을 확보한 직후 더욱 광범위한 환경에서 중요한 자산을 세그먼트화하는 조치를 취했습니다. 유일하게 작동하는 제조 라인을 담당하는 2개의 중요한 프로덕션 애플리케이션을 빠르게 식별하고 보호할 수 있었습니다. Akamai Guardicore Segmentation을 이용해 감염된 서브넷과 데이터 센터의 일부에서 애플리케이션으로의 연결을 제한하는 정책을 즉시 도입했습니다. 레거시 방화벽을 사용했다면 몇 주가 소요되었을 작업입니다.

또한 간단한 쿼리를 통해 인터넷에 연결된 레거시 머신이 레거시 방화벽을 우회하면서 격리 제한을 시도한 것을 밝혀냈습니다. 팀은 이러한 규정을 준수하지 않은 통신을 발견한 후 레거시 머신을 비롯한 모든 서버에 대한 인터넷 접속을 몇 분 만에 효과적으로 제한하는 정책을 생성했습니다.

복구 중 측면 이동 방지

팀은 복구 프로세스의 다음 단계로 해당 제조업체의 애플리케이션 클러스터를 다시 생성해 Akamai 에이전트에 반영했습니다. 팀은 모든 수신 연결을 차단하는 초기 정책을 설정했으며 Akamai Guardicore Segmentation을 이용해 의존성을 파악했습니다. 그런 다음 요구사항을 검증하고 컨텍스트을 파악한 후에만 필요에 따라 통신을 허용 목록에 포함했습니다. 팀은 이 접근 방식으로 재감염 리스크 없이 랜섬웨어 공격에 영향을 받은 애플리케이션을 복구하고 온라인 상태로 되돌릴 수 있었습니다.

미래 보호

유출 복구 서비스 기업은 Akamai Guardicore Segmentation을 활용해 고객인 제조업체가 랜섬웨어 공격에서 회복할 수 있도록 지원하며 상당한 부가 가치도 성공적으로 제공할 수 있었습니다. 이를 통해 기업은 매출 증대, 풋프린트 확장, 고객의 IT 및 보안 목표 실현에 대한 지원 강화 등의 기회를 얻게 되었습니다.

단계별 복구 과정에서 도입한 내부 데이터 센터 세그멘테이션 덕분에 공격표면이 크게 축소되었습니다. 현재 이 기업의 보안 체계가 개선되었고 향후 유출로 인한 영향도 크게 줄었습니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

> “[Akamai] 솔루션을 사용해 4시간 만에 공격의 확산을 막고, 기본 네트워킹을 수정하지 않고 '청정한' 네트워크 세그먼트에서 가동 중단된 프로덕션 라인을 복구할 수 있었습니다. 동시에 IR 조사와 방지가 이루어지고 있었습니다.
>
> CISO, 보안 침해 복구 서비스 기업

 | 지원 | 2023년 06월 발행