AKAMAI 고객 사례

동해대학교(Tunghai University)

동해대학교의 보안을 강화하고 인시던트 관리 시간을 단축하는
Akamai Secure Internet Access Enterprise

동해대학교 보안팀의 리소스를 절감하고 외부 보안 알림을 줄일 수 있도록 지원한 Akamai

공격자들이 보안 방어 체계를 우회하기 위해 더 정교한 방법을 사용함에 따라 오늘날의 기업은 복잡한 사이버 위협에 직면하게 되었습니다. 이러한 공격에 대한 선제적 방어의 필요성과 글로벌하고 다양한 대학 구성원들이 요구하는 유연성 및 자율성 사이에서 어떻게 균형을 맞출 것인가?

이것이 동해대학교의 컴퓨터센터팀이 고민하고 있던 문제였습니다. 동해대학교는 디지털 학습을 도입하고 스마트 캠퍼스를 구축해 캠퍼스 안팎의 학생과 교직원에게 무료로 초고속 무선 인터넷 접속을 지원합니다. 매 학년 초에 학생들은 학교에 와서 개인 노트북을 대학의 네트워크에 연결합니다.

그러나 학생들의 디바이스에 바이러스 백신 설치를 의무화하지 않는 IT 정책 때문에 많은 노트북이 멀웨어에 감염되었습니다. 이렇게 감염된 디바이스로 인해 캠퍼스 안팎에서 네트워크 장애가 발생하고 대역폭이 과도하게 소모되며 악성 봇넷 트래픽이 유발됩니다. 또한 이 멀웨어는 측면 이동(lateral movement)을 통해 대학이 관리하는 컴퓨터로 침입하며, 동해대학교는 타이중 네트워크 지역 센터(Taichung Network Regional Center)로부터 '대학의 네트워크가 공격당했으며 비정상적인 접속이 발생하고 있다'는 알림을 받습니다.

네트워크 기술 디렉터인 오우치엔휘(Chien-Hui Ou)는 "컴퓨터센터에서는 학생과 교직원을 대상으로 정보 보안 교육을 실시했고, 이메일이나 웹 페이지에서 수상한 링크를 클릭하지 않도록 강력하게 권장합니다. 그러나 공격자들은 어떤 것이 정상인지 사용자들이 바로 알아볼 수 없는 교묘한 방법을 계속 고안하고, 결국 사용자를 공격의 희생자로 만듭니다."라고 말합니다.

"악성 코드의 분석과 식별에 의존하는 기존의 안티바이러스 소프트웨어와 정보 보안 솔루션만으로는 충분하지 않습니다. 새로운 변종 멀웨어가 등장했는데 안티바이러스 벤더사가 코드를 규명하지 못하고 시그니처를 업데이트하지 못한다면 멀웨어는 탐지되지 않을 것입니다. 그리고 웹 트래픽을 암호화하는 트렌드 때문에 공격자들은 현재 이런 암호화된 채널을 사용해 공격을 일으키고 있으며, 따라서 제로데이 공격에 대처하기가 점점 더 어려워지고 있습니다."라고 동해대학교 네트워크 그룹의 창광진은 설명합니다.

동해대학교 (Tunghai University)
대만 타이중
eng.thu.edu.tw

업계
공공 부문

솔루션
Secure Internet Access Enterprise

주요 장점

- 보안 체계 강화 및 보안 관리와 인시던트 해결 시간 단축
- 감염된 디바이스에서 C2(Command and Control) 서버 트래픽을 선제적으로 차단 및 측면 이동 감소
- 외부 보안 알림 감소
- CapEx에서 OpEx로 투자를 전환해 보안 예산 최적화

의심스러운 연결을 효과적으로 차단하는 Akamai

동해대학교 컴퓨터센터팀은 기존의 보안 체계를 개선할 필요가 있다는 것을 깨닫고 DNS를 보안 컨트롤 포인트로 활용하는 제품을 살펴보기 시작했습니다. 컴퓨터센터팀은 이러한 접근 방식을 통해 학문의 자유에는 영향을 미치지 않으면서 대학의 전반적인 보안 포스처를 개선할 수 있다고 생각했습니다.

대학은 경쟁 평가 프로세스를 통해 Akamai Secure Internet Access Enterprise를 최종 솔루션으로 선택했습니다. Secure Internet Access Enterprise는 모든 DNS 요청을 분석해 네트워크와 사용자를 선제적으로 보호하는 클라우드 기반 서비스입니다. 인터넷 트래픽에 대한 Akamai의 탁월한 가시성을 바탕으로 요청된 웹 콘텐츠를 차단하거나 전송하기 전에 모든 쿼리를 실시간 위협 인텔리전스와 비교합니다.

창광진 담당자는 "Secure Internet Access Enterprise는 랜섬웨어나 코인 채굴 멀웨어 등 악성 콘텐츠를 전송하거나 사용자 정보를 빼낼 수 있는 도메인에 대한 DNS 요청을 탐지해 차단합니다. 학생의 컴퓨터가 캠퍼스 밖에서 사용하는 동안 멀웨어로 손상된 경우, 컴퓨터가 캠퍼스 네트워크로 돌아가도 멀웨어는 여전히 C2 서버에 외부적으로 연결할 수 없을 것입니다."라고 말합니다.

Secure Internet Access Enterprise를 도입하기 전에는 정보 보안 인시던트를 방어하기 어려웠습니다. 일단 비정상적 접속 신고가 접수되면 네트워크 관리 직원은 IP 주소로 손상된 컴퓨터를 추적하고, 로그 파일에서 접속 기록을 찾아 피해 당사자에게 인시던트가 발생했다고 알린 다음, 해당 당사자에게 바이러스 제거 절차에 협조해 줄 것을 요청해야 했습니다.

"이 때문에 인시던트 해결에 1주일 정도 걸렸으며, 저희 학교 보안 리소스 역시 지나치게 많이 소모되었습니다."라고 창은 설명합니다. 하지만 Secure Internet Access Enterprise를 배포한 뒤 보안 인시던트 보고 횟수가 급감했고 리소스가 경감되어 다른 보안 프로젝트에 집중할 수 있었습니다.

특히 Secure Internet Access Enterprise는 배포와 설정이 빠르고 간편합니다. 따라서 시스템을 운영하기 전에 먼저 네트워크와 분리한 후 테스트해야 하는 기존의 물리적 장비와는 차별화됩니다. Secure Internet Access Enterprise를 통해 DNS 트래픽이 직접 Akamai 플랫폼으로 전송되도록 설정만 하면 몇 분 안에 프로세스가 완료됩니다."라고 덧붙였습니다.

오우 디렉터는 "클라이언트 컴퓨터가 어떤 멀웨어에 감염됐는지, 컴퓨터가 코인 채굴 멀웨어에 감염되기 전에 어떤 웹 링크를 클릭했는지 보안팀이 신속하게 파악할 수 있도록 Secure Internet Access Enterprise가 상세한 인시던트 보고서를 자동으로 제공합니다. 데이터가 SIEM과 통합되기 때문에 이 보고서는 최근의 비정상적인 네트워크 활동을 파악해 선제적으로 대응할 수 있도록 도와줍니다."라고 말합니다.

> Secure Internet Access Enterprise를 배포한 뒤 보안 인시던트 보고 건수가 급감했고, 리소스를 절감해 다른 보안 프로젝트에 집중할 수 있었습니다.

창광진(Kuang-Chin Chang)
동해대학교 네트워크 그룹

상당한 인력 및 비용 절감

동해대학교 전자컴퓨터센터 양차오퉁(Chao-Tung Yang) 디렉터는 전략적 이점을 강조합니다. "정보 보안은 현재도 중요하지만 앞으로도 디지털 애플리케이션의 발전에 따라 점점 더 중요해질 것입니다. 동해대학교는 언제나 IT 애플리케이션 보호와 정보 보안에 우선순위를 두었고, 총장은 정보 보안에 대한 투자를 지원합니다.

한걸음 물러서서 IT의 현재 성장 방향을 살펴보면, 클라우드 기반 서비스가 중심을 차지하게 될 것이 분명합니다. 이전 방어 시스템은 소프트웨어와 하드웨어의 조합으로 구축됐는데, 이를 유지 관리하고 패치를 업데이트하는 등의 작업에는 노동력과 시간이 소모됩니다."라고 양 디렉터는 말합니다.

Akamai의 클라우드 기반 서비스는 이를 변화시켜 유지 관리 인력에 드는 비용을 전반적으로 절감합니다. 양 디렉터는 클라우드 기반 정보 보안 서비스의 미래에 대해 낙관적인 전망을 내놓으며 "클라우드 기반 서비스 덕분에 필요한 노동력이 절감될 뿐만 아니라 컴퓨터실의 물리적 공간도 줄어들며 에어컨 사용과 전기 사용량도 감소합니다. 이는 장비실의 에너지 사용량을 줄이려는 컴퓨터센터의 노력과도 일치합니다."라고 말합니다.

"또한 클라우드 기반 서비스를 이용하는 것은 물리적 장비를 구입하는 것과는 달리 대규모 일회성 지출을 할 필요가 없습니다. Secure Internet Access Enterprise는 연 단위로 임대하기 때문에 대학 입장에서 재정적 부담이 줄어듭니다."라고 말합니다.

양 디렉터는 "정보 보안 작업은 지속적으로 진행되어야 합니다. 그러나 Secure Internet Access Enterprise를 사용하면 인시던트 관리 작업의 양이 크게 줄어들어 봇넷 공격에 대한 방어를 강화하고 보다 포괄적으로 활동을 분석할 수 있는 역량을 가질 수 있게 됩니다."라고 언급합니다.

> 특히 Secure Internet Access Enterprise는 배포와 설정이 빠르고 간편합니다. 따라서 시스템을 운영하기 전에 먼저 네트워크와 분리한 후 테스트해야 하는 기존의 물리적 장비와는 차별화됩니다.
>
> **창광진(Kuang-Chin Chang)**
> 동해대학교 네트워크 그룹

동해대학교(Tunghai University)는 1955년에 설립된 대만의 첫 사립대학교로, 유일하게 유치원부터 박사 과정까지 모든 교육 프로그램을 갖춘 최초의 교육 기관입니다. 동해대학교에는 예술대학, 과학대학, 공학대학, 경영대학, 사회과학대학, 농업대학, 순수 미술 및 크리에이티브 디자인 대학, 법학대학, 국제대학 등 현재 9개의 단과 대학이 있습니다. 약 1만 7천여 명의 학생이 재학 중이며 500여 명의 교수가 재직 중입니다. http://eng.thu.edu.tw/