MENLO SECURITY

웹 및 이메일 기반 사이버 공격으로부터 괴스겐 원자력 발전소 보안 보호

Menlo Security 클라우드 플랫폼을 사용하면 직원들은 조직을 위험에 빠뜨리지 않고 필요에 따라 웹을 브라우징하고 이메일에 액세스할 수 있습니다.

사례 연구

개요

괴스겐 원자력 발전소

1979년 설립된 스위스의 괴스겐 원자력 발전소 (Gösgen Nuclear Power Plant)는 오늘날 스위스 전 지역에 1,020메가와트의 전력을 공급하고 있습니다.

과제

조직을 위험에 빠뜨리지 않고 직원의 인터넷 액세스를 지원해야 합니다.

스위스의 기존 인터넷 격리 솔루션은 복잡할 뿐만 아니라 업데이트에도 시간이 많이 소요되었습니다.

유지 관리에 따른 부담 없는 직원들을 보호할 수 있는 솔루션이 필요했습니다.

해결책

Menlo Security 클라우드 플랫폼을 채택했습니다.

가져오기 및 실행 명령을 단말 장치에서 폐쇄형 가상 브라우저 환경으로 이동합니다.

활성 컨텐츠를 제거하고 직원들의 브라우저에 안전한 컨텐츠를 렌더링합니다.

유지 관리 부담을 가중시키는 클라이언트 기반 격리

원자력 발전소에 있어 사이버 보안의 중요성은 누구나 아는 사실입니다. 한 번의 실수로 컴퓨터 한 대만 감염되더라도 지역 전체의 전력 공급이 차단되어 사람들이 위험에 빠질 수 있습니다. 또한 오늘날 사이버 보안 침해의 위험이 그 어느 때보다도 커지고 있습니다. 공격자가 피싱 이메일을 스핀업(spin up)하거나 위조 웹 양식을 만들거나 유명 웹사이트를 위험한 멀웨어로 감염시키기가 더욱 쉬워졌습니다. 실제로 2019 Verizon Data Breach 보고서에 따르면 2018년에 발생한 사이버 공격의 99%가 웹과 이메일에서 시작되었습니다.

스위스 아강(Aa River)에 위치한 괴스겐 원자력 발전소의 사이버 보안 팀은 이러한 위험을 그 어느 누구보다도 잘 알고 있습니다. 이 팀은 직원 생산성과 위험의 균형을 맞출 수 있는 사이버 보안 솔루션이 필요하다는 판단하에 VMware ThinApp 기반의 자체 격리 솔루션을 개발함으로써 사용자를 위한 안정적이면서도 안전한 인터넷 액세스를 유지하는 데 우선 주력했습니다. 자체 솔루션은 가상 브라우저의 모든 인터넷 트래픽을 사용자 장치에서 근본적으로 격리시켰으며 이를 통해 멀웨어의 단말 액세스를 효과적으로 차단했습니다.

"이전에는 모든 잠재적인 멀웨어 문제를 수동으로 점검해야 했습니다. 이제 업무가 훨씬 간편해졌습니다. Menlo Security 클라우드 플랫폼으로 만족할만한 보안 수준을 달성할 수 있게 되었습니다."

괴스겐 원자력 발전소
IT 보안 책임자,
François Gasser

격리 방식은 사용자가 조직을 위험에 빠뜨리지 않고 필요에 따라 웹을 브라우징하고 이메일에 액세스할 수 있는 안전하고 안정적인 고도의 기술로 인정받았습니다. 그러나 VMware를 통한 ThinApp 업데이트가 거의 진행되지 않아 인터넷 격리 솔루션과 관련된 정기적인 유지 관리 작업의 상당 부분을 괴스겐 IT 팀에서 담당해야 하는 문제가 발생했습니다. 또한 사이버 보안 팀이 모든 직원들 장치의 모든 클라이언트가 최신 상태로 유지된다고 확실하게 보장하지 못했습니다.

괴스겐의 보안 및 네트워크 엔지니어인 Manuela Schweizer는 "우리는 점점 더 낙후되고 있었습니다. [특히] 가상 배포를 위한 Firefox를 준비하는 워크로드가 상당했습니다. 결국 브라우저 개발은 계속 진행하면서 [IT] 부서의 워크로드를 줄여줄 수 있는 새로운 솔루션을 찾게 되었습니다."라고 당시 상황을 설명했습니다.

Menlo Security 클라우드 플랫폼에서 해결책을 제시했습니다.

괴스겐의 IT 보안 책임자인 Schweizer와 François Gasser는 발전소의 IT 컨설팅 및 구현 파트너인 BOLL Engineering 및 BNC Business Network Communications AG와 함께 직원들을 위한 기본 인터넷 브라우징 환경을 지원하면서 모든 이메일 기반 및 웹 기반 사이버 보안 위협으로부터 발전소를 보호할 수 있는 안정적인 인터넷 격리 솔루션을 모색했습니다. 또한 솔루션은 IT 담당자들의 유지 관리 부담도 줄여줄 수 있어야 했습니다.

최종적으로 두 가지 솔루션을 평가했지만 Menlo Security 클라우드 플랫폼의 우수성을 확인하는 데 그리 오랜 시간이 걸리지 않았습니다. 특히 로그 파일에서 직접 현저한 차이가 나타났습니다. Gasser는 빠르게 변화하는 사이버 위협의 특성을 고려할 때 빠른 해결책을 제시할 수 있다는 점에서 이를 중요한 역량으로 평가했습니다.

Menlo Security 클라우드 플랫폼은 Isolation Core™ 기반 Secure Web Gateway를 지원하며 가져오기 및 실행 명령을 단말 장치에서 폐쇄형 가상 브라우저 환경으로 이동함으로써 사용자 브라우저에 안전한 컨텐츠만 렌더링될 수 있게 해줍니다.

JavaScript 및 Flash를 비롯한 모든 활성 코드가 가상 브라우저 환경에서 실행되며 직원 시스템에 액세스할 수 없습니다. 대신 프록시 서비스를 통해 모든 활성 코드가 제거된 후 렌더링된 웹 페이지가 직원들에게 제공됩니다. 즉, 프록시 서비스로 스크립트를 제거하고 자동으로 Flash 동영상을 MP4 파일로 변환합니다. 결과적으로 단말에 클라이언트 소프트웨어를 설치할 필요가 없으므로 직원들의 속도, 성능 또는 기본 환경에 영향을 미치지 않고 웹을 브라우징하고 이메일의 링크와 문서에 액세스할 수 있습니다. 괴스겐 발전소는 Menlo 솔루션을 통해 기존의 웹 필터링 제어 및 액세스 기능은 물론 탁월한 멀웨어 차단 성능이라는 추가적인 이점까지 얻게 되었습니다.

원활한 배포

괴스겐 사이버 보안 팀은 데이터 개인 정보 보호 문제를 고려하여 IT 팀에서 빌드 및 유지하는 프라이빗 클라우드 환경에 Isolation Core™ 기반 Secure Web Gateway를 지원하는 Menlo Security 클라우드 플랫폼을 배포하기로 결정했습니다. 발전소는 현재 정책 및 관리 서버 이외에 격리 노드 4개를 운영하고 있으며 이 노드에서 활성 코드를 실행하고 웹 컨텐츠의 수정 버전을 렌더링하는 복잡한 작업을 처리합니다.

Menlo Security, BOLL 및 BNC의 협력으로 원활하게 롤아웃되었습니다. 직원들은 인트라넷 뉴스를 통해 새로운 플랫폼에 대한 정보를 얻었으며 별도 교육이 필요하지 않았습니다. 사실 직원들은 기초 기술에 대해 전혀 알지 못합니다. 단말 장치에 에이전트 또는 특수 브라우저를 설치하지 않아도 되며 추가 노력으로는 이전 가상화 브라우저에서 클라이언트에 로컬로 설치된 Firefox 브라우저로 변환한 것 밖에 없었습니다.

Schweizer는 웹 인터페이스를 통해 작동되어 시간을 절약할 수 있는 업데이트 메커니즘에 만족해하고 있습니다. 다른 모든 관리 작업 또한 이 웹 인터페이스를 통해 직관적으로 수행될 수 있습니다. 그는 "새 펌웨어에 문제가 생기더라도 롤백이 쉽게 수행됩니다."라고 말했습니다.

단말에 대한 악성 코드 차단

괴스겐 원자력 발전소의 550명 전 직원은 물론 몇몇 외부 파트너까지 2019년 2월 말부터 Menlo Security 클라우드 플랫폼을 통해 생산성이 크게 향상되었습니다. Gasser에 따르면 팀원들은 단말에 어떠한 악성 코드도 도달할 수 없다는 강한 확신을 갖게 되었으며 그 결과 직원들이 이전에 차단될 수 밖에 없었던 웹사이트에 안전하게 액세스할 수 있게 되었습니다.

웹 기반 사이버 공격을 제거하고 공격 벡터를 현저하게 줄일 수 있는 방법을 알아보려면 menlosecurity.com에 방문하거나 korea@menlosecurity.com으로 문의하십시오.

BOLL
IT Security Distribution

BOLL Engineering AG(BOLL)는 스위스 보안 채널 산업을 선도하는 우수 유통업체로 1988년에 설립되었습니다. BOLL은 IT 보안 및 개방형 네트워크 제품을 주력 분야로 일반적인 판매 지원 수준을 넘어서는 포괄적인 서비스를 고객에게 제공합니다.

Menlo Security와 BOLL의 파트너십은 KKG의 의사 결정 과정에서 Menlo의 격리 플랫폼을 채택하고 제로 트러스트 인터넷 방식을 지원하는 데 중요한 역할을 담당했습니다. KKG 비즈니스 프로세스에 대한 BOLL의 이해와 지원은 Menlo 솔루션의 원활한 배포에 큰 도움이 되었습니다.

MENLO SECURITY

자세한 내용은 다음 연락처로 당사에 문의하십시오.

menlosecurity.com

(650) 695-0695

korea@menlosecurity.com

Menlo Security 회사 소개

Menlo Security는 조직에서 위협을 제거하고 생산성을 완전히 확보할 수 있는 격리 기반의 우수한 클라우드 보안 플랫폼을 제공합니다. 이 플랫폼은 클라우드 보안의 본질을 이행하는 유일한 솔루션으로, 악의적인 공격을 방어하기 위해 가장 안전한 제로 트러스트 방식을 제공하며 최종 사용자가 온라인 작업 과정에서 보안 기능이 실행되는 것을 인식하지 못하고 보안 팀의 업무 부담도 없애줍니다. 이제 조직은 조직 내 사용자에게 보안에 대한 걱정 없이 비즈니스 계속 수행할 수 있는 안전한 온라인 환경을 제공할 수 있습니다.