한국남부발전, MAXPATROL로 주요 정보인프라에 대한 보안 강화

과 제

+ **보안취약점 및 컴플라이언스 관리 솔루션 도입**
+ **자체 또는 외부 컨설팅 업체를 통한 보안취약성 점검을 정보시스템 인프라 전반을 다루는 자동화된 보안평가 솔루션으로 대체**
+ **정부의 보안평가 기준에 따라 모든 정보시스템의 컴플라이언스를 통제**

주요 인프라를 관리하는 모든 공기업과 마찬가지로 한국남부발전은 정부에서 규정하고 있는 정보 보안 기준을 준수해야 합니다. 이전에는 전문 보안컨설팅 업체를 통하여 발전소와 사무실의 IT 시스템을 점검하고 , 정부의 보안규정 준수여부를 관리했습니다.

외부 컨설팅업체를 통한 수동평가 방식은 시간, 비용 그리고 평가의 완성도 측면에서 최선의 관리 방식은 아니었습니다. 한국남부발전 보안정보전략처는 "연 1회 정도로 수행되는 보안 평가는 급속도로 변화하는 IT 인프라와 지능화 되고 있는 보안위협에 대응하기에는 부족한 점이 많았습니다. 정부의 보안평가와는 별도로 자체적인 보안 점검을 통해 상시적 으로 보안 문제점들을 개선하고 싶었고, 또한 외부 컨설팅 비용 절감의 필요성도 느끼고 있었습니다" 라고 이야기 합니다.

그리고 다양한 보안위협 요소에 대하여 즉각적인 조치 프로세스의 개선도 필요하였습니다. "우리회사는 다양한 IT시스템에 대하여 독립적으로 운용되는 여러 개의 솔루션을 통해 취약점을 점검해 왔습니다. 이런 비효율적 방법과 더불어 공급사의 보안 업데이트가 원활하지 않을 경우, 신종 보안위협에 노출될 수 밖에 없습니다. 주요 인프라를 관리함에 있어 이러한 위험요소는 최우선적으로 해결해야 할 문제입니다. 따라서 최신 보안업데이트의 보장과 동시에 IT 시스템 전반에 걸쳐 취약점과 컴플라이언스 모두를 평가할 수 있는 단일 솔루션이 필요했습니다. 그리고 보안평가 작업시 생성되는 데이터들의 보안 유지도 중요한 문제이므로 보안평가 과정이나 평가결과의 기밀성 유지 기능도 주요 검토사항이었습니다" 라고 설명합니다.

해결책

MaxPatrol 취약점 및 컴플라이언스 관리 솔루션

현재 한국남부발전에 MaxPatrol 취약점 및 컴플라이언스 관리 솔루션이 구축되어 있습니다. 전사 정보통신 인프라를 대상으로 정기적인 보안점검이 이루어 지고 있으며, 필요한 시점에 여러 기종의 네트워크 장비는 물론이고 윈도우, 리눅스, 유닉스 운영 체제의 서버들을 즉시 자동 스캔할 수 있습니다.

정부의 보안취약점 점검 항목은MaxPatrol 컴플라이언스 모드에 기본으로 탑재되어 있습니다. 이를 통해 국내 취약점관리규정에 대한 정기 점검은 물론 ISO 27001과 같은 국제 기준에 대한 컴플라이언스 평가도 빠르게 수행할 수 있습니다.

MaxPatrol의 감사 모드는 IP별 설치된 소프트웨어, 버전 정보, 업데이트 및 패치 등 한국남부발전의 IT 인프라에 대한 전반적인 자산현황 정보를 제공하며, 펜테스트 모드는 Positive Technologies 의 분석기술을 통해 취약점과 잘못된 환경설정들을 파악합니다. 또한 MaxPatrol 서버는Positive Technologies 에서 제공하는 신규위협 패치버전을 정기적으로 자동 업데이트합니다.

MaxPatrol의 에이전트리스 기술은 각 지역 사이트에서 운영되고 있는 여러 발전소와 사무실에 신속하게 구축할 수 있는 장점을 가지고 있습니다. 한국남부발전은 프로젝트 시작 후 한 달도 채 되지 않은 2014년 12월부터자동화된 취약점 및 컴플라이언스 점검을 수행할 수 있게 되었습니다.

기업 정보

+ **업종:** 전력 생산
+ **사업 영역:** 화력 등 총7 개 발전소 운영 및 해외 발전사업
+ **시장 점유율:** 대한민국 전체 전력 생산량의 약10%
+ **지주사:** 대한민국 최대 규모 공기업 한국전력의 자회사

주요 성과

+ **자율적인 컴플라이언스 관리**
  ISO 27001등의 국제 기준과 미래창조과학부 등 정부의 보안규정 준수를 위한 정기적인 자체 점검 수행
+ **보안 비용 절감**
  외부 보안 컨설팅 업체 의존도 감소
+ **보안위협의 가시성 증대**
  정기적으로 업데이트 되는 단일 솔루션을 통한 취약점 통합 관리로 신종 보안위협에 대한 선제적 대응수준 향상
+ **기밀 정보 보호**
  모든 평가정보의 관리 용이성 및 기밀성 향상

결 과

정부의 보안규정 및 평가에 대한 컴플라이언스 자체 관리와 위험요소 가시성 향상, 컨설팅 등 보안평가에 소요되는 비용 절감

한국남부발전 보안담당자들은

"MaxPatrol 덕분에 정보인프라에 대한 취약점 및 컴플라이언스 관리를 효율적으로 통제 할 수 있게 되었습니다. 연간 1회 외부 컨설팅 업체를 통한 보안 평가 대신 필요한 시점에 자체적으로 평가를 수행합니다. 이를 통해 컨설팅 비용 절감 뿐만 아니라 평가기준의 일관성과 평가결과의 신뢰성도 높아졌습니다. 그리고 MaxPatrol의 정기 업데이트는 새로운 보안취약점이 발견되는 즉시 위험성 여부를 검사할 수 있게 해줍니다."

"모든 취약점 및 컴플라이언스 관리 업무를 하나의 솔루션으로 통합함으로써 업무의 효율성을 높였습니다. 빠른 시간내 정부의 보안평가를 준비할 수 있게 되었고 새로 도입되는 서버, 네트웍 등 ICT 장비에 대하여 업무적용 전 사전 보안적합성 검사와 환경설정 작업들을 신속하게 처리할 수 있습니다."

"모든 보안관리 정보가 우리 ICT 센터 내에 저장됨으로써 중요자료와 개인 정보 등이 안전하게 보호되고 있으며, MaxPatrol의 유연한 보고서 기능은 각종 실무자료를 다양하게 제공하고 있습니다. 또한 사용자 보안레벨에 따라 정보 제공을 제한하는 권한관리 기능도 유용합니다."

라고 평가하고 있습니다

IT 시스템에서MaxPatrol의 효과를 체험한 한국남부발전은 이제 SAP와 발전제어시스템 그리고 가상화 플랫폼의 취약점 및 컴플라이언스 관리를 위해 솔루션의 확대 도입을 검토 중입니다.

Positive Technologies 소개

Positive Technologies는 취약점 진단, 컴플라이언스 관리, 위협 분석 솔루션 분야의 글로벌 리더로서, 전세계 1천 여 고객들에게 솔루션을 제공하고 있습니다. 개발 단계의 애플리케이션 보호, 네트워크 및 애플리케이션 취약점 진단, 규제 요구사항과의 컴플라이언스, 실시간 공격 차단 등 비즈니스와 관련된 모든 보안 문제에 완벽히 대처합니다. 고객 및 연구에 대한 헌신과 노력의 결과, SCADA, 금융, 통신, 웹 애플리케이션, ERP 보안 분야에서 최고의 권위를 가지고 있다는 평가를 얻고 있으며 2012년 IDC 보고서*에서는 가장 빠르게 성장하는 보안 및 취약점 관리 기업으로 선정되기도 했습니다.
Positive Technologies에 대한 보다 자세한 사항은 www.ptsecurity.com에서 확인할 수 있습니다.

*출처: Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. 매출 2천만 달러 이상 관련 분야 사업자의 2012년 전년대비 매출 성장률을 바탕으로 함.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com www.ptsecurity.com