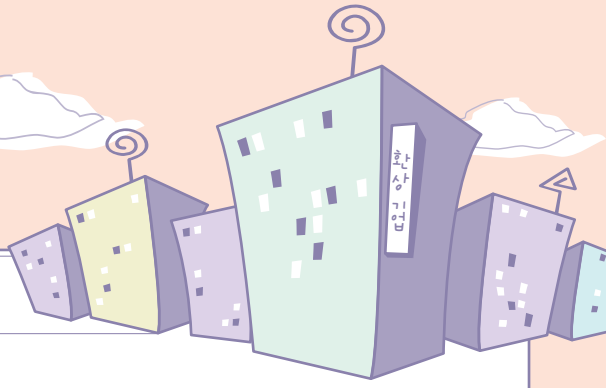
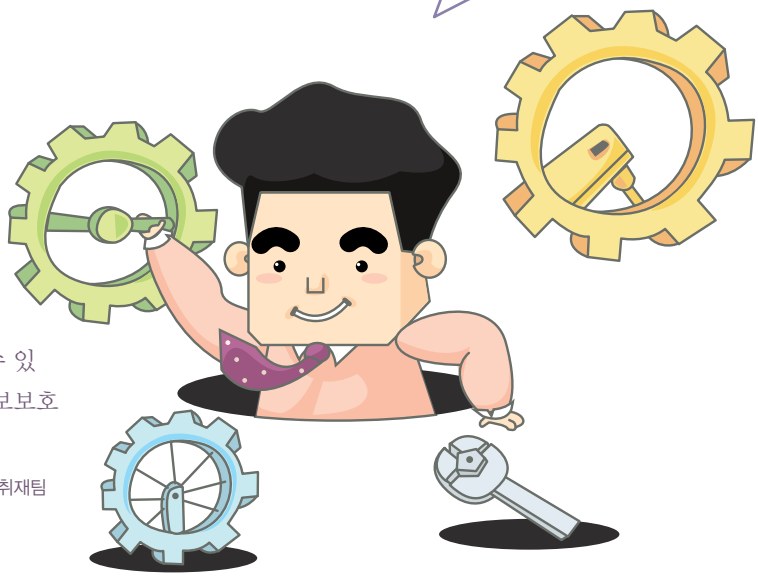


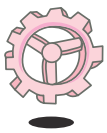
보안 솔루션 도입기



매일 아침 정보보호와 IT 관련 뉴스를 꼼꼼히 챙겨보는 김 대리는 최근 부쩍 정보보호 관련 사건사고 기사가 늘어났다는 사실을 알게 됐다. 증가된 사건사고만큼 김 대리가 몸담고 있는 환상기업에게도 보안사고가 더 이상 남의 집 불구경이 아닐 수 있다는 사실이 걱정된 김 대리. 이를 위해 정보보호 솔루션 도입을 검토하기 시작했다.

정보보호뉴스 취재팀

정보보호 솔루션 도입이 기업 정보보호의 종착점이나 대응의 만능열쇠가 될 수 없지만 그럼에도 불구하고, 정보보호 인력 부족과 보다 효율적인 보안정책 운영을 위해 정보보호 솔루션의 도입은 필요하다고 생각한 김 대리. 특히 취약한 웹 구조를 갖고 있는 환상기업의 단점을 보완시켜 줄 수 있는 솔루션에는 무엇이 있으며, 또 어떤 과정을 통해 도입할 것인지를 살펴보는 것에서부터 김 대리의 보안 솔루션 도입기는 시작됐다.



다양한 보안 솔루션, 오히려 머리 아파

보안 솔루션의 최근 동향을 조사하던 김 대리는 순간 머리가 아팠다. 정보보호 솔루션이라면 방화벽이나 바이러스 백신 정도가 전부일 것이라고 생각했기 때문이다. 조사결과 최근에는 침입방지 시스템이라고 불리는 IPS를 비롯해 UTM(Unified Threat Management), ESM(Enterprise Security Management) 등 수십가지의 보안 솔루션이 등장해 있었다. 일주일에 걸쳐 보안 솔루션의 이름과 기능을 조사하던 김 대리는 이번 기회를 통해 기업 규모와 정보보호의 중요성을 기준으로 필수적인 정보보호 솔루션의 종류를 다음과 같이 정리해 볼 수 있었다.

분 류	Step 1	Step 2	Step 3	Step 4
네트워크 보안	방화벽(Firewall)	침입탐지시스템(IDS) 프로토콜 분석도구	침입방지시스템(IPS)	네트워크 접근통제 (NAC)
시스템 보안	바이러스 백신 시스템 방화벽	스팸차단 소프트웨어 패치관리시스템(PMS)	보안운영체제 시스템취약점 분석툴	
애플리케이션 보안		웹방화벽(WAF) 스팸메일차단솔루션	문서저작권관리(DRM) DB 보안 솔루션 웹스캐너(취약점분석)	소스코드 분석도구 취약점스캔 Appliance
통합 보안관리	로그관리 및 분석도구	보안구성관리(SCM)	통합보안시스템(UTM) 전사적보안관리(ESM)	위협관리시스템(TMS) 위험관리시스템(RMS) 포괄적위협관리(CTM)
인증 및 접근통제	싱글사인온(SSO)	스마트 카드 통합접근관리(EAM)	하드웨어 토큰 일회용 비밀번호(OTP) 통합계정관리(EIM)	바이오인식시스템 (지문, 정맥, 얼굴, 홍채, 다중인식 등)
PC 보안	바이러스 백신 안티 스파이웨어	개인용 PC 방화벽	개인용 안티스팸	통합 PC 보안
기타보안	가상사설망(VPN)	공개키기반구조(PKI) 무선랜 보안(Wireless)	모바일 보안(Mobile) RFID 보안	기업정보 유출방지
보안 서비스	인증(공인/사설)	솔루션 유지보수	보안관제 보안교육훈련	보안 컨설팅

단 계	적용범위	설 명
Step 1	소규모 조직(15명 이하), 비영리 기관	조직을 안전하게 운영하기 위한 최소한의 보안 솔루션
Step 2	중소기업	중소 규모의 조직에서 효과적인 보안 체계를 갖추기 위한 보안 솔루션
Step 3	대기업	대규모 조직에서 관리 및 통제를 효율적으로 하기 위한 보안 솔루션
Step 4	기밀정보를 다루는 주요 조직	군사, 주요 정부기관, 핵심 사업부 등 고도의 보안 수준을 요구하는 조직을 위한 보안 솔루션

▲ 기업 규모별 정보보호 보안 솔루션 맵(출처 : 2007 CERT 구축 및 운영 가이드(CONCERT, KISA 공동발행))

중소기업에 속하는 기업규모와 보안수준 등을 고려해 볼 때 환상기업의 경우 현재 Step 2에 속해 있었으며, 김 대리는 여러 보안 솔루션 가운데 웹 취약점을 악용하는 공격에 대비해 웹 보안 솔루션 도입을 우선적으로 검토하기로 결심했다. 그렇다면 기업에서 사용되는 웹 방화벽을 어떻게 어떤 기준으로 도입해야 할까.

내 몸에 맞는 보안 솔루션

보안 솔루션을 도입하기 위해 김 대리가 가장 우선적으로 고려한 것은 환상기업의 네트워크 규모 및 아키텍처, 기존 장비의 운영 현황이었다. 기업의 현재 상황을 정확히 파악하지 않고서는 아무리 좋은 장비일지라고 환상기업에는 적합하지 않을 수 있기 때문이었다. 그리고 곧 기업 환경과 각 보안 솔루션에 요구되는 기능과 성능을 종합적으로 검토할 수 있는 단계인 BMT(BenchMarking Test)를 위해 바쁘게 움직이기 시작했다.

보안 솔루션의 BMT

BMT는 IT 장비나 소프트웨어 제품을 구매하기 전 객관성을 확보하고 기업이나 기관에 최적화된 솔루션을 찾기 위해 실시하는 테스트다. BMT를 수행하기 위해서는 테스트 장비와 이에 대한 전문 인력 보유, 소프트웨어와 하드웨어 등이 종합적으로 고려되어야 한다. 하지만 BMT 수행과정에서 적지 않은 비용이 발생하기 때문에 중소규모의 기업에서는 BMT를 수행하기에는 많은 어려움이 따르게 된다. 이로 인해 중소기업에서는 기본적인 테스트와 동종업계의 정보보호 부서로부터 자문을 얻어 보안 솔루션을 도입하고 있다.

국내 기업의 현실에서 실제 BMT를 진행하지 못하더라도 기업이 필요로 하는 보안 솔루션의 기능과 성능에 대해서는 별도의 시나리오를 작성해 보안 솔루션을 비교해 보는 과정은 반드시 필요하다. 다음은 웹 방화벽을 도입하기 위한 실제 BMT 시나리오의 한 예제다.

1. 일 정 : ◎◎◎◎ 년 ◎◎월 ◎◎일 ◎시
2. 장 소 : ◎◎◎◎ 센터
3. 참가인원 (총 O명) : [A사] ◎◎◎ 과장 외 ◎명,
   [B사] ◎◎◎ 대리 외 ◎명
4. 환 경 : Windows 2000 Server/IIS 5.0/MS SQL Server 2000/ASP
5. 시나리오 상세정보
   - 5.1 기능면 : 항목별 가중치 부여
     - Injection Flaw(SQL Injection 등)
     - XSS(Cross Site Scripting)
     - 데이터 절취
     - 서비스 거부공격(DoS)
     - 불필요한 파일 노출
     - 시스템 정보노출차단(에러페이지 노출차단)
     - 웹서버 구성 취약점 방어
     - 인증 취약점(Session 변조)
     - 파일 다운로드
     - 파일 업로드
   - 5.2 관리면
     - 편의성, 유연성, 확장성
     - 통보 및 리포팅
     - 운영관리
     - 로그관리, 백업 및 복구관리
   - 5.3 성능 및 안정성
     - Response Time
     - 장애 발생시 서비스 영향도
   - 5.4 기술지원 및 유지보수
6. 진행정보
   - 6.1 기능 : 취약한 웹사이트에서 취약성 확인 후 방어할 수 있는지 확인
     로그를 확인하고, 어떤 형식으로 동작하는지 확인
   - 6.2 관리 : 실제 웹사이트에 도입하여 운영시 고려해야 할 사항 검토
   - 6.3 성능 : 웹방화벽(WAF) 설치 전후의 Throughtput 비교
   - 6.4 BMT 진행 당일 기능 평가를 위한 구성 가이드에 따라 적절한 설정 후 테스팅
   - 6.5 각 평가항목별 가중치 부여, 최종점수 산출 후 적합한 제품 선정

▲웹 방화벽 BMT 시나리오 〈출처 : 2007 CERT 구축 및 운영 가이드(CONCERT, KISA 공동발행)〉

웹 방화벽 도입에 필요한 기능별 테스트 항목은 OWASP(Open Web Application Security Project)와 Web-appsec(Web Application Security Consortium)을 참고할 경우, 보다 다양한 테스트 항목을 선정할 수 있다.

보안 솔루션 실제로 보고 사기

보안 시장에 판매되는 모든 보안 솔루션을 테스트하기보다, 비용 및 시장조사 등을 통해 3개의 제품을 1차 선별한 뒤 사전에 마련된 시나리오를 기준으로 각 제품의 데모를 꼼꼼히 비교해 제품을 선정하기로 한 김 대리. 특히, 보안 솔루션은 제품 벤더의 설명보다는 장비의 동작과정을 보안 관리자의 눈으로 직접 확인해야 한다는 사실을 다시 한번 절실하게 깨닫게 됐다. 그런 의미에서 이번 웹 방화벽의 도입 과정은 향후 더 많은 보안 솔루션 도입을 검토해야 할 김 대리에게 더할 나위 없는 소중한 경험이었다. S