기업보안 강화를 위한 취약점 진단 통합관리 체계 구축

문호건, 박성철
KT-ICT Convergence연구소

요 약

기업활동에서 IT에 대한 의존도가 증가함에 따라 기업들은 다양한 소프트웨어 및 하드웨어 플랫폼에서 제공되는 서비스들을 운영하고 있다. 서비스들이 보급, 확대되는 과정에서 새로운 보안 취약점들이 나타나고, 이들 취약점을 악용한 기업정보의 유출 및 해킹 등 보안사고의 발생도 비례하여 증가하고 있다[1].

특히 다양한 유형의 사업을 운영하는 지주회사 또는 대기업 그룹사의 경우, 사업영역 별로 운영 중인 IT 인프라의 보안 취약점이 네트워크로 연결된 타 사업용 IT 인프라에 대한 사이버 침해의 통로로 악용될 가능성이 있다.

이 같은 문제의 해결을 위해 기업들은 사업영역 별로 보유한 IT 인프라의 보안 취약점 진단과 대응을 위한 솔루션들을 도입, 운영해 오고 있다.

하지만 기업의 보안 거버넌스 관점에서 보안 취약점 관리도 전사적인 보안 정책과의 연계 강화, 투자 중복의 방지, 효과적인 관리와 통제에 대한 필요성이 대두되기 시작했다. 보안 거버넌스 체계 강화에 대한 기업의 요구변화에 맞춰 보안 취약점의 통합관리를 지원하는 상용 솔루션들이 일부 출시되고 있으나 기업들이 기 운영하고 있는 개별 취약점 진단 솔루션과의 연동, 로그관리 및 기업이 요구하는 특화된 기능 구현 등의 어려움이 도입에 장애가 되고 있다.

따라서, 대기업을 중심으로 개별 보안 취약점 진단 솔루션들을 연동하여 기업보안 거버넌스를 효과적으로 지원할 수 있도록 취약점 관리업무 프로세스의 재설계와 함께 취약점 진단 통합관리 체계를 구축하고 있다[2][3][4].

본 고는 보안 취약점 관리업무의 문제점을 소개하고, 최근 대기업을 중심으로 활발히 구축이 추진되고 있는 웹 기반의 취약점 진단 통합관리 체계의 개념, 기능 및 운영 프로세스를 소개한다. 아울러, 기업 IT 인프라에 대한 보안 취약점 진단 데이터를 축적하여 기업 내부의 보안위험 요소를 사전예측하고, 정보보호의 투자 대비 효과(ROSI: Security Return on Investment)를 효과적으로 산정하는 인프라로서 활용 가치를 소개한다.

Ⅰ. 서 론

네트워크로 연결된 다양한 IT 서비스 인프라를 운영하고 있는 기업의 전체 보안 수준은 보안 대응이 가장 취약한 시스템의 수준과 일치한다. 이는 보안대응 수준이 기업의 모든IT 인프라에 동일하게 적용되어야 전체적인 보안 수준의 향상을 기대할 수 있다는 의미와 같다. 따라서, 기업보안 담당자는 IT 인프라의 소프트웨어적인 보안 취약점을 이용한 내, 외부의 불법적인 사이버 공격 위험을 최소화하기 위해 주기적으로 보안 취약점을 진단해야 한다.

하지만, 기업에서 IT 인프라의 취약점을 관리할 때 다음과 같은 운영상의 어려움에 공통적으로 직면하고 있다.

첫째, 보안 취약점의 진단과 대응에 필요한 일정 수준의 전문지식을 갖춘 운영자를 확보하기 어렵다. 보안 취약점은 관리대상에 따라 개별적인 전문성이 요구되므로 한 명의 운영자가 대응할 수 있는 관리범위가 제한적이다.

둘째, 보안 취약점 진단 및 대응과 관련한 이력 관리가 어렵다. 규제법이 정한 관리적, 기술적 보호조치 항목에 대해 자체적인 대응 조치를 하고, 감독기관의 정기적인 심사를 받은 결과에 대한 이력을 지속적으로 관리하는 것은 운영자에게 추가적인 업무부담으로 작용한다.

셋째, 보안 취약점들을 신속하게 탐지하고 상시 대응하기 어렵다. 대부분의 기업은 소수의 보안 관리자가 전체 IT 인프라에 대한 보안관리를 담당하는 경우가 많다. 다수의 장비, 운영체제, 응용 프로그램 및 네트워크 서비스 등 일상적인 보안 취약점 관리가 필요한 대상이 증가함에 따라 상시 보안대응을 위한 충분한 시간적 여유가 없다.

넷째, 취약점 진단 시스템에 등록된 IT 자산과 자산관리 시스템의 정보가 일치되지 않은 경우가 있다. 기업에서 일반적으로 자산관리와 보안관리 업무가 분리되어 있어 취약점을 진단하는 시점에 자산관리시스템에 등록된 정보가 현행화 되지 않아 등록되지 않은 자산이 취약점 스캐너에 탐지되는 상황도 자주 발생한다.

다섯째, 보안 취약점 진단 결과에 따른 다양한 분석 보고서 작성이 어렵다. 대부분의 기업들이 운영하고 있는 취약점 진단 솔루션들은 시스템 운영 방식,취약점 진단 영역및 진단 로그의 형태가 제각기 상이하다. 이 같은 문제로 인해 개별적인 보안 취약점 진단 결과를 바탕으로 기업보안의 수준을 일관되게 파악할 수 있는 보고서를 작성하는 것이 어렵다.

여섯째, 보안 취약점 진단과 결과 조회를 위한 접근제어용 인증 및 권한관리가 어렵다. 대부분의 시스템은 계정(ID)과 비밀번호(Password)만으로 시스템 접근제어를 하고 있다. 보안 최고책임자가 하위 조직의 보안관리 책임자 및 시스템 운영자의 접속 인증 및 권한관리 설정을 할 수는 있다. 하지만 기업의 인사시스템과 연동하지 않을 경우 시스템 접근제어를 효과적으로 하기 어려워진다.

그림 1. 운영자 업무수행 요구사항

이상과 같이 기업 IT인프라의 보안 취약점을 관리하는 운영자들이 직면한 어려움을 해결하기 위해 개별 보안 취약점 진단 솔루션들을 연동하여 기업 IT 인프라의 보안 취약점 진단 정보를 통합 관리하여 웹 포털 서비스 형태로 제공할 수 있는 시스템의 필요성이 증가하고 있다.

이 같은 서비스는 보안 거버넌스 담당부서가 웹 포탈을 통해 지시한 보안정책의 이행 현황과 결과를 지속적으로 파악하는데 효과적인 수단을 제공한다. 또한 개별 보안 취약점 진단 솔루션의 운영에 대한 일정관리를 정책적으로 설정할 수 있게 함으로써 특정 시점에 기업의 보안 취약점 수준을 일률적으로 파악하고 대응할 수 있게 한다.

사업영역 별로 보안 취약점과 조치내역에 대한 이력정보가 데이터베이스로 축적되면 보안이 취약한 영역에 대해 사전대응을 하는 의사결정에 근거를 제공할 수 있다. 이는 정보보호와 관련한 투자 대비 효과의 산정에 정량적인 근거를 제공하는 효과도 있다.

기업이 보유한 다양한 종류의 서비스 인프라와 이들로부터 탐지된 보안 취약점 진단 정보들이 지속적으로 축적하면 향후 빅데이터(Big data) 분석과 같은 기법을 적용하여 인프라의 보안 위험을 사전에 예측하고, 대응하는 것도 가능할 것이다.

본 고는 기존의 보안 취약점 관리체계가 갖는 운영상의 문제를 해결하고, 기업보안의 거버넌스 강화를 지원할 수 있는 취약점 통합관리 체계를 설계 및 구현하는 방안을 제시한다.

2장에서는 기존 보안 취약점 관리의 문제해결을 위한 운영자의 요구사항을 정리하고, 기존의 개별 시스템들을 연동하여 보안 관리자가 표준화된 관리 프로세스를 통해 진단업무를 수행할 수 있게 하는 취약점 진단 포털 구성형태는 3장에서 설명한다. 4장은 기업에서 요구하는 취약점 진단 보고서 관련 양식과 통계처리를 소개한다. 결론에서는 기업 내 IT인프라 구성 자산의 보안 취약점 관리정보의 축적을 통해 기업에 내재한 일상적인 보안위험 요인을 사전 예측하고 보안대응의 정량적 효과를 산정하기 위한 방안을 제시한다.

Ⅱ. 요구사항 분석

취약점 진단 통합관리 체계는 규제법에서 요구하는 준수 항목을 관리하여 기업이 보유하고 있는 정보자산의 보안취약점을 자가 진단, 조치할 수 있게 함으로써 사이버 침해사고를 예방하는 것을 목적으로 한다.

기업의 규모가 커지고 사업영역이 다양할수록 보안취약점 진단업무는 사업영역의 특성에 따라 진단대상, 점검항목과 진단주기 등에 대한 요구가 달라진다.

따라서, 기업이 보유한 취약점 진단 솔루션들을 사업영역에 따라 독립적으로 운영할 경우, 특정 시점에 기업 정보자산의 보안 취약점을 일정한 수준에서 관리하기가 어려워진다. 또한 기업보안 거버넌스 측면에서 진단대상 IT인프라의 현황, 취약점 정보의 수집, 분석 및 대응 과정을 보안 최고책임자가 효과적으로 통합관리하기 어렵다.

더욱이 기업이 운영하고 있는 개별 보안 취약점 진단 시스템은 용도와 벤더에 따라 사용방법 및 진단 결과 보고서의 양식이 다양하다. 이로 인해 시스템을 효과적으로 운영하고 진단 결과에 따라 대응할 수 있는 운영자를 육성하는데 많은 시간이 소요된다.

기업이 공통적으로 직면한 보안취약점 관리의 어려움을 극복하기 위한 방안으로 기존의 개별 취약점 진단 솔루션들을 연동하여 웹 기반의 통합관리 서비스 형태로 구축할 수 있다.

웹 기반의 보안 취약점 진단 통합관리 서비스 제공을 위한 시스템 요구사항은 〈표 1〉과 같이 시스템 운영 공통영역, 취약점

진단 대상인 자산관리 영역, 취약점 진단기능 영역, 진단결과 분석을 기반으로 한 의사결정 지원 영역으로 나눌 수 있다.

표 1. 취약점 진단 통합관리 영역별 요구사항

항목	요구 사항
공통사항	■ 편리한 사용자 인터페이스 – 웹 기반 사용자 인터페이스 – 온라인 도움말 제공 – 진단 신청, 조치 이행, 통계 및 점검 이력조회 기능 제공 ■ 업무 프로세스 지원 기능 제공 – 진단 일정계획 수립 및 설정 – 진단 이행여부 확인 – 업무절차 및 자료공유 ■ 인증 및 권한 관리 기능 제공 – 사용자 별 진단 및 결과조회 인증 및 권한 설정 – 사용자 등록, 변경 및 해지 설정
자산관리 영역	■ 자산 정보 현행화 – 자산관리 시스템 연동 – 자산관리자 현행화를 위한 인사 시스템 연동 ■ 진단대상 범위 확대 – 네트워크 장비 취약점 – 애플리케이션 소스 취약점
진단기능 영역	■ 진단 관리업무의 중앙 집중화 – 진단 프로세스 지원 – CISO 또는 조직 별 보안관리자가 취약점 진단 및 대응 수준 현황을 실시간으로 파악할 수 있게 지원 ■ 자산관리 시스템 연동 – 자산관리 시스템 DB에서 취약점 진단대상 자산 범위 확인 – 자산 및 인사관리 시스템을 통해 취약점 진단 및 결과 리포트 조회 권한 설정 ■ 진단결과 리포트 가독성 개선 – 진단 영역 별 결과보고서를 진단 체크리스트 기준으로 자동 요약 – 중요한 정보는 폰트 차별화, 그래픽 및 도표 병행
의사결정 지원영역	■ 진단 현황 및 취약수준 이력 관리 – 자산, 관리자 및 조직 별 – 주간, 월간, 분기, 반기 및 연간 이력관리 – 관리적 취약점 통계 산출 – 다양한 조건 별 통계산출 ■ 보고서 작성 지원 – 진단 이력 별 요약 및 상세보고서 – Crystal Report를 이용해 작성된 다양한 그래프 및 표 형태의 보고서 – HTML, Word, Excel 및 PDF 파일 등 다양한 파일 형식의 보고서 ■ 정보관리 지원 – 보안 취약점의 Knowledge DB화 – 보안공지, S/W 업데이트 정보 – 관련 부서 취약점 점검 결과 공지 – 공통 기술문의 대응을 위한 게시판

상기 요구사항을 기반으로 기업보안 관리자와 시스템 운영자가 취약점 현황 및 대응 추이를 쉽게 관리할 수 있게 함으로써 보안 사고를 예방하는데 중점을 둔 웹 기반의 통합관리 서비스 형태로 구축할 수 있다.

Ⅲ. 취약점 진단 통합관리 포털 구조

본 고의 기업보안 강화를 위한 취약점 진단 통합관리 체계를 구현한 시스템은 〈그림 2〉와 같이 4개의 기능 계층으로 구성된다[5].

시스템의 운영자 계층은 진단 시스템 별 운영자와 보안 최고 책임자로 구성된다.

시스템 별 운영자는 자신이 관리해야 하는 진단대상 자산에 대해 시스템, 네트워크 및 응용 프로그램 영역 별로 보안 취약점 진단을 실행하고 결과를 취합하여 등록한다.

보안 최고 책임자는 취약점 진단을 위한 대상, 일정, 항목 등에 대한 정책을 관리하고 시스템 사용자 인증 및 권한제어를 위한 그룹관리를 한다. 또한 취약점 진단 및 대응 이력관리와 연계하여 조직 별 보안수준을 모니터링 함으로써 보안 수준을 관리한다.

시스템 인터페이스 계층은 운영자의 웹 이용과 관련한 시스템 인터페이스와 인증 및 권한관리 기능을 제공한다.

취약점 진단 통합관리 시스템과 연동하는 개별 진단 시스템들은 다양한 하드웨어와 소프트웨어 상에서 운영되고 있다. 따라서, 운영 시스템의 플랫폼과 무관하게 공통적인 운영 인터페이스를 제공하기 위해 웹 포털 서비스 형태를 제공한다.

운영자 인증 및 권한관리는 인사관리 시스템의 데이터베이스를 연동하여 적용한다. 보안 최고 책임자는 운영자의 소속, 직급 및 직무에 따라 시스템의 운영 및 진단결과 데이터베이스에 대한 접근 권한을 설정한다.

진단관리 기능 계층은 취약점 진단 통합 관리 시스템의 핵심 계층으로 진단 시스템과 연동하여 보안 진단 및 취약 수준 관리를 수행한다.

세부 기능으로는 〈표 2〉와 같이 5가지가 있다.

진단 시스템 계층은 시스템, 네트워크 및 응용 프로그램 영역의 보안 취약점을 진단하는 기존의 진단 시스템 그룹을 나타낸다. 진단 시스템 그룹은 기업이 운영하는 서비스와 IT 인프라에 따라 다양하게 구성될 수 있다.

진단 시스템들은 운영자가 지정한 자산영역에 대해 정기 또는 부정기적인 일정계획에 따라 진단업무를 수행하고 결과 보고서를 다양한 형식의 파일로 생성한다.

보고서는 개별 시스템이 생성한 문서를 그대로 제공하거나 취

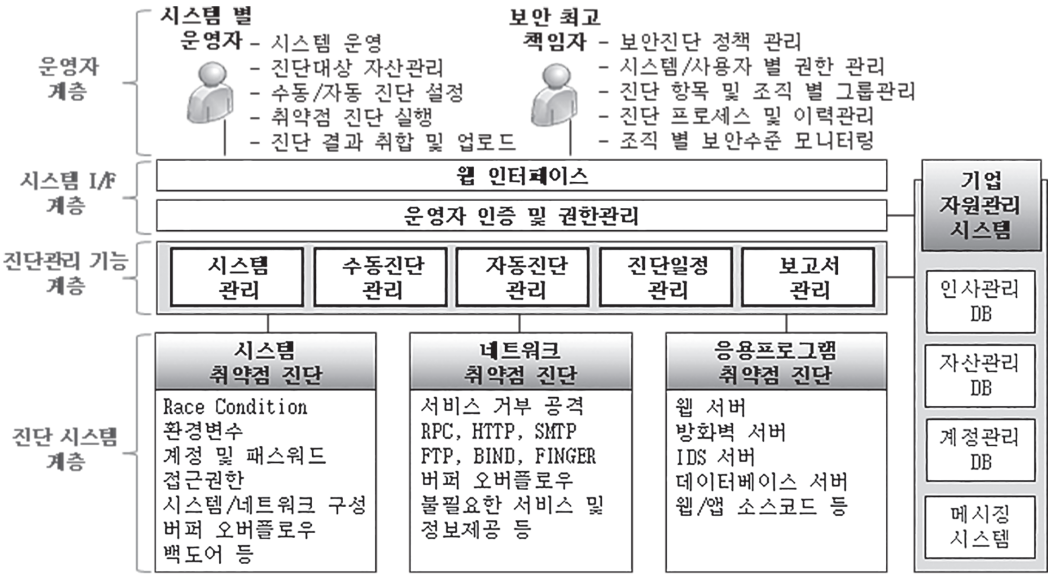

그림 2. 취약점 진단 통합관리 시스템 개념도

약점 진단 통합관리 시스템의 보고서 관리 모듈에서 별도로 정의한 양식으로 내용을 재 구성하여 웹을 통해 조회할 수도 있다.

취약점 진단 통합관리 시스템의 운영과정에서 시스템의 이상 상황이 발생하면 기업 자원관리 시스템의 메시징 시스템을 통해 메일(e-Mail) 또는 SMS(Short Message Service)를 통해 보안 관리자에게 대응 요청을 한다.

진단관리 기능 계층은 개별 진단 시스템들이 제공하는 인터페이스 규격에 따라 연동한다.

표 2. 시스템 공통 관리기능

관리기능	기능 개요
시스템 관리	■ 진단 대상 시스템 정보조회 및 관리 ■ 시스템 담당 조직 및 담당자 설정 ■ 취약점 진단 이행 현황에 관련된 통계 관리
수동진단 관리	■ 취약점 진단 통합관리 시스템과 연동할 수 없는 개별 취약점 진단 시스템의 경우 개별 진단 수행 결과를 통합관리 시스템에 업로드
자동진단 관리	■ 자동진단 주기 설정 ■ 취약점 진단대상 자산과 분야를 선택해서 진단을 할 경우 진단 현황 모니터링 기능을 제공 ■ 시스템 장애 발생시 담당자에게 SMS/e-mail 발송
진단일정 관리	■ 진단업무 별로 목표 일정 지시 및 진단 완료 현황정보 제공 ■ 진단대상 별 진단업무 진행 현황 및 이력 관리
보고서 관리	■ 진단 시스템 별 결과 리포트 저장 ■ 위험수준 별로 취약점 발견 내역 및 대응 가이드라인 제공 ■ 조직 및 자산 별로 취약 수준 변화 추이에 대한 정보 제공

〈그림 3〉은 취약점 진단 통합관리 시스템의 운영 프로세스를 나타낸 것이다.

운영 업무는 보안 취약점 진단 업무 수행과 관련한 프로젝트 생성, 진단 대상 및 진단 시스템 선정, 진단 실행, 진단결과 조회로 진행된다.

운영업무를 지원할 수 있는 보조적인 기능으로 보안 현황 파악, 조직 별 보안 관리자 정보 관리, 진단 대상 시스템의 정보 현행화 관리 그리고 진단업무 진행과 관련한 각종 공지 양식 관리가 있다.

이 중에서 핵심 업무인 보안 취약점 진단 수행 프로세스의 주요 내용은 다음과 같다.

1) 진단 프로젝트 생성

기업 내부의 특정 조직 또는 IT 인프라에 대한 취약 수준 확인 및 관리를 위해서는 우선 하나의 프로젝트를 생성해야 한다. 취약 수준의 관리 목적에 따라 진단 대상 IT인프라와 조직의 범위가 달라지기 때문에 보안 관리자는 프로젝트 단위로 관리를 한다.

2) 진단 도구, 조직 설정

진단 프로젝트에서 진단 분야에 따라 진단 도구와 수행조직을 선택한다. 이때 보안 최고 책임자가 수행조직을 지정할 수도 있고, 사업 영역에 따라 관련 수행조직을 직접 선택할 수 있다. 〈그림 4〉는 진단 분야를 선택할 수 있는 화면을 나타낸다.

3) 진단 항목 설정

스크립트 진단인 경우 체크 리스트에서 보안 점검을 할 세부 분야와 질문 항목을 선택할 수 있도록 메뉴를 제공한다. 필요한

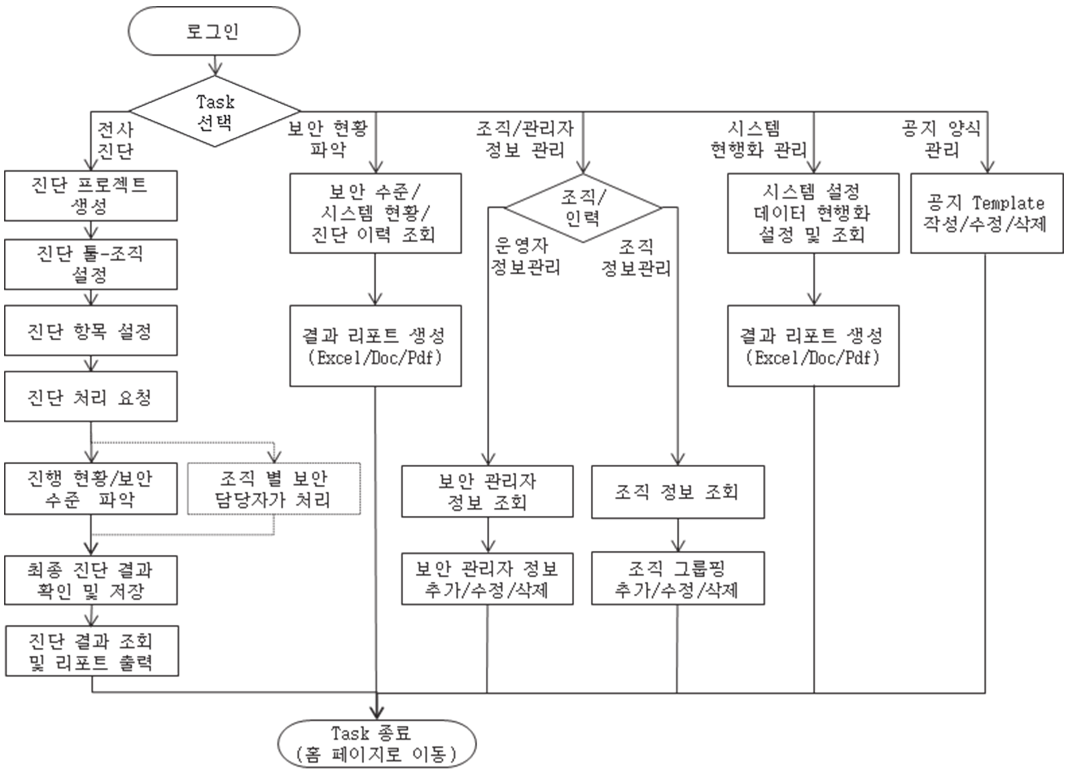

그림 3. 취약점 진단 통합관리 업무 프로세스

그림 4. 진단분야 선택화면

경우 진단 도구 별로 세부 진단 항목을 지정한다. 예를 들어 소스 취약점 진단인 경우 여러 개발 언어 중 java, c#을 선택하고 app 종류 중에서는 iOS app으로 선택하는 등의 처리를 할 수 있다.

4) 진단 처리 요청

보안 최고 책임자가 하위 조직의 보안 또는 시스템 운영자에게 신규 진단 프로젝트 생성을 알리고 진단 수행과 취약점 보완, 그리고 취약 수준 관리를 할 수 있도록 한다. e-mail 또는 SMS로도 공지를 할 수 있다.

5) 진행 현황/보안 수준 파악

보안 관리자가 담당 조직과 시스템들에 대해서 보안 취약점 진단 상황과 진단 결과를 확인할 수 있다. 진단 결과 드러난 취약점의 대응을 시스템 운영자에게 메일로 독려 할 수 있다.

6) 조직 별 보안 담당자가 처리

조직 별 보안 관리자가 담당 하위 조직의 보안 취약점 진단 현황을 확인하고 진단 및 조치를 독려한다.

7) 최종 진단 결과 확인 및 저장

시스템 담당자는 보안 취약점 보완이 모두 끝나면 최종적으로

취약점 진단을 하고 결과를 확인한다. 잘못 탐지한 건이나 예외 건이 있는 경우 상위 보안 관리자에게 취약 수준 평가결과의 조정을 요청한다.

8) 진단 결과 조회 및 리포트 출력

취약점 진단을 한 이력, 각 진단 상세 결과를 기업이 정의한 양식에 따라 재구성 후 화면 또는 파일로 조회할 수 있게 한다. 보고서는 상시 확인 및 출력 가능하다.

V. 진단 결과 분석

취약점 진단 결과 리포트는 보안관리자와 기업 경영자에게 기업의 위험수준에 대한 인식과 대응 방안 결정에 매우 중요한 데이터를 제공한다.

보안 취약점 진단 통합관리 시스템은 등록된 모든 자산에 대해 관리 조직 별, 진단 도구 별, 기간 별로 취약점 통계를 확인하고 조회할 수 있는 페이지를 제공한다. 통계 정보는 자산 및 조직 별로 진단 및 대응 이력에 대한 정보를 다양한 그래픽 형태로 표현할 수 있다.

취약점 진단 리포트는 기업 IT 인프라에 내재한 보안 취약점 진단 정보에 대해 다양한 통계분석 능력을 결합해 전체 인프라의 보안 상황에 대해 높은 가시성을 제공할 필요가 있다.

이를 통해 기업보안 최고 책임자가 각종 보안 이슈를 정확히 이해하고 우선순위를 파악하여 대응을 하게 함으로써 기업 IT 인프라의 정상화에 걸리는 시간을 줄일 수 있게 한다.

기업 경영자는 개별 사업부문의 취약점 탐지 및 대응현황 정보를 기반으로 운영인력의 인사관리를 위한 기초자료로 활용할 수 있다.

취약점 진단 및 대응 이력 데이터가 축적되면 기업의 잠재적

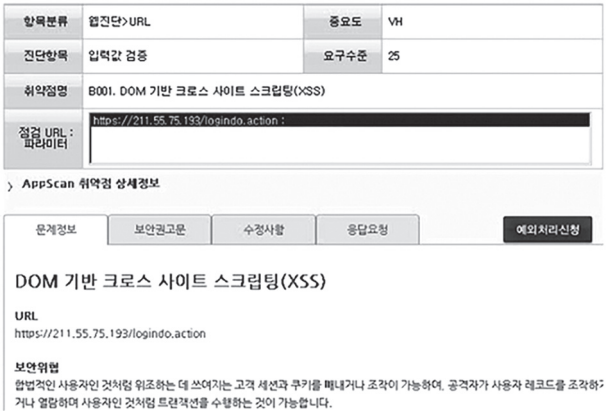

그림 5. 웹 취약점 진단 결과 리포트 예

인 보안위험 요소를 식별하고, 위험에 대한 사전예측이 가능해진다. 이를 통해 기업보안을 위한 정보보호의 투자 대비 효과를 극대화할 수 있다.

〈그림 5〉는 웹 취약점 진단 결과 리포트의 예를 나타낸다. 진단 솔루션의 결과 리포트는 시스템 운영자에게 전달되어 대응 조치를 할 수 있게 한다.

개별 취약점 진단 솔루션의 탐지 결과는 자산, 조직 및 탐지일별로 집계되어 〈그림 6〉과 같이 기업 전체의 보안 취약점 탐지 현황 정보를 나타낼 수 있다.

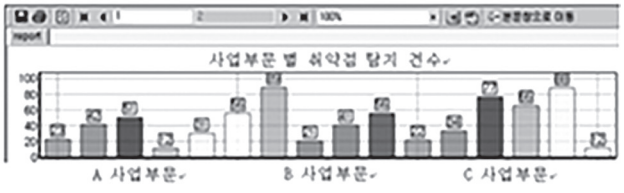

그림 6. 취약점 탐지 건수 통계표

〈그림 7〉은 사업부문 별 보안 취약점 현황을 기반으로 보안 대응에 따른 이전 대비 취약점 개선율을 나타낸다. 이 정보를 기반으로 기업 내 IT 인프라 보안관리 실태를 쉽게 파악할 수 있다.

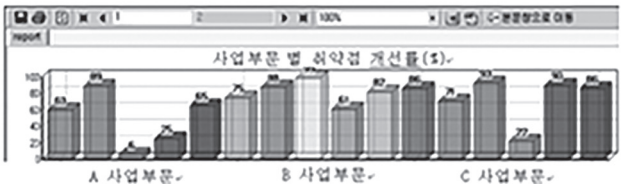

그림 7. 취약점 개선율 통계표

기업보안 취약점과 대응 이력 데이터를 데이터 베이스화 하여 관리함으로써 보안업무의 효율성과 생산성을 극대화하기 위해 빅 데이터 분석을 지원하는 기반을 제공한다. 이를 위해 개별 진단 시스템의 결과 리포트를 보안 관리자와 경영자 용으로 재구성한 형태로 제공함으로써 반복적인 수작업을 최소화한다. 또한 기업 IT 인프라의 비즈니스 연관 정보를 반영하여 가장 중요한 문제를 용이하게 식별할 수 있게 하고, 관련성이 높은 데이터를 함께 표시하도록 하고 있다.

IV. 향후 과제

기업의 IT 인프라에 대한 의존도가 증가함에 따라 보안 취약점들을 악용한 정보 유출 및 해킹 등 보안사고를 예방하기 위해 취약점 진단 정보의 활용이 점차 중요하게 인식되고 있다.

현재 기업보안 취약점 진단 솔루션 시장은 단일 진단 솔루션, SaaS(Security as a Service) 및 취약점 진단 통합관리 솔루션 시장으로 나눌 수 있다. 이미 대부분의 기업에서는 취약점 진단과 대응을 위해 필요에 따라 개별 취약점 진단 솔루션들을 도입, 운영해 오고 있다.

진단해야 할 IT 인프라가 증가함에 따라 기업의 보안관리를 성공적으로 구현하려면 자산, 취약점 및 위협정보를 효과적으로 통합하고, 분석할 수 있어야 한다.

본 고에서 소개한 취약점 진단 통합관리 시스템은 보안 거버넌스를 효과적으로 지원할 수 있도록 취약점 관리업무 프로세스의 재설계와 함께 개별 취약점 진단 솔루션들을 시스템 및 데이터 단위에서 연동하고, 웹 서비스 형태로 운영자 인터페이스를 제공한다.

하지만 취약점 진단 시스템의 운영을 위해서는 진단 조건의 설정, 진단 리포트에 기반한 대응에 전문성이 필요하고, 운영 성과에 대한 경영층의 이해를 이끌어 내기 위해서는 보고용 리포트의 가공에 적지 않은 노력이 필요한 단점이 있다.

따라서, 보안 취약점 진단 통합관리 시스템의 활용도를 높이기 위해서는 진단 기능의 자동화, 연관분석 기능의 고도화와 함께 결과 리포트를 운영자와 경영자 측면에서 가독성과 가시화를 향상시키는 것이 여전히 중요한 과제로 남아있다.

이상의 과제를 어떻게 해결하느냐에 따라 향후 기업보안 취약점 진단 솔루션 시장의 판도가 바뀔 것으로 예상된다.

참 고 문 헌

[1] KISA, “2013년 주요 침해사고 사례와 대응”, 2013.12

[2] 나일 소프트, http://www.nilesoft.co.kr/

[3] 안랩, http://www.ahnlab.com/

[4] 장승주, “컴퓨터 시스템 보안 및 보안취약점 점검 도구 동향”, IITA, 2008.11.5

[5] KT-ICT, “취약점 진단 통합관리 시스템 설계서”, 2013.8

약 력

문 호 건

1985년 숭실대학교 공학사
1987년 중앙대학교 공학석사
2005년 부산대학교 공학박사
1987년~현재 KT-ICT Convergence연구소 R&D Infra 보안부장
관심분야: 보안 거버넌스, 보안 Big data 분석, 사이버공격 조기경보

박 성 철

2004년 POSTEC 컴퓨터공학과 석사
2004년~현재 KT-ICT Convergence연구소 융합보안팀 선임연구원
관심분야: 보안인증 관리, 보안 빅데이터 분석