AhnLab

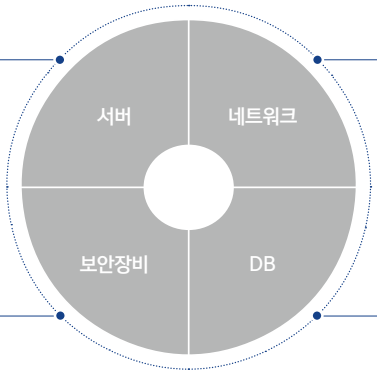
인프라 취약점 점검

주요 정보시스템의 안전성 및 신뢰성 확보

서버, 네트워크, 보안장비, DB 등 주요 정보시스템의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협요인을 파악하고 이에 대한 분석 및 대응 방안을 제시합니다.

서비스 개요

운영 중인 주요 정보시스템의 모든 위협요소를 도출하여 발생 원인을 분석하고 대응 방안을 제시하는 서비스입니다.



기밀성·무결성·가용성 확보

서비스 보안 등 다각적인 취약점 진단
- 자체 개발 점검툴 사용
- 취약점 및 설정 오류 점검
- OS별 특화된 점검
- 계정관리
- 시스템 영향 최소화

네트워크를 통한 보안위협 최소화

네트워크 환경 및 장비 보안성 검토
- 자체 개발 체크리스트 사용
- 네트워크 장비 영향 최소화
- 네트워크 장비별 특화된 점검

시스템 운영 적절성 확보

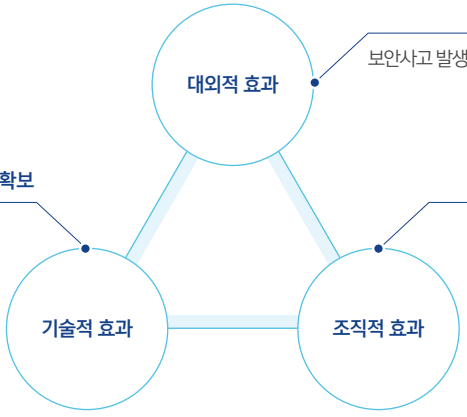
보안장비에 대한 보호조치 검토
- 자체 개발 체크리스트 사용
- 취약점 및 설정 오류 점검
- 기능별, 장비별 특화된 점검
- 방화벽, IDS, VPN 등의 장비별·기능별 특화된 점검
- 보안정책 점검

시스템 운영 안전성 확보

DB 고유 취약점 제거
- 자체 개발 체크리스트 사용
- 시스템 영향 최소화
- 벤더별 특화된 점검

서비스 필요성

내·외부 위협요소 파악 및 피해 최소화를 위한 대응 방안 제시로 정보시스템의 안전성 및 신뢰성을 확보하여 기업 경쟁력 상승에 도움이 됩니다.



대외 이미지 향상

보안사고 발생 가능성 최소화로 기업 신뢰도 향상

주요 정보시스템에 대한 안전성 확보

기밀성·무결성·가용성 보장

정보보호 개선활동

정보시스템 취약점 개선
각종 보안위협 제거

점검항목

인프라 취약점 진단 점검항목은 서버, 네트워크, 보안장비, DB 등의 주요 정보시스템에서 발생할 수 있는 각종 보안위협에 대비할 수 있는 항목으로 구성되어 있습니다.

서버	네트워크	보안장비	DB
· 보안정책 및 접근통제 관리 현황 점검 · TCP/IP 구성, OS 취약점 · 계정관리, 파일시스템, 불필요서비스 점검 · 원격접속, 감사정책, 레지스트리 설정 점검 · 응용서비스, 보안설정, 패스워드 관리 현황 점검	· 네트워크 구성 분석 및 점검 · 운영 및 모니터링 관리 현황 점검 · 네트워크 구성, 접근 제어, 가용성 점검 · 패스워드, 로그, 원격 관리, 보안설정 점검	· 설정 구조 점검 · 기능 및 운영 관리 환경 점검	· 계정관리 점검 · 접근통제 점검 · 로그관리 점검 · 패치관리 점검 · 주요 업데이트 점검

수행절차

운영 중인 정보시스템 환경을 고려하여 현황 점검 및 취약점을 진단하고 도출된 결과에 대한 문제점 및 원인 분석과 평가를 통해 안전한 정보시스템 운영 환경을 제공합니다.

정보시스템 현황 파악	점검 대상 선정	정보시스템 취약점 진단	진단 결과 분석	보고서 및 보안대책 제시
• 시스템 구성 현황 및 운영 파악 • 네트워크 구성 현황 파악 • 응용시스템 현황 파악	• 정보시스템 중요도에 따른 우선순위 부여 • 유사 플랫폼별 분류 및 대표 시스템 선정	• 자체 개발 점검툴 및 체크리스트를 활용한 진단	• 진단도구를 통해 도출된 보고서 분석 • 수동 점검 결과 분석	• 결과보고서 작성 • 발견된 취약점 대응 방안 제시

AhnLab
경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901
© 2021 AhnLab, Inc. All rights reserved.