최근 사이버공격 대비 기업 보안강화 권고 2026-10-03

□ 개요

- 최근 국내 금융권 및 민간기업 대상으로 다수의 침해사고가 발생함에 따라 추가 공격에 대비하여 기업·기관의 보안강화 필요
- 특히 기업은 최근 초기 침입에 자주 악용되는 웹·API 취약점과 인증정보 노출 여부를 우선 점검하고, 침입 이후 내부 시스템 접근 및 중요정보 유출을 차단할 수 있도록 단계별 보호조치 이행 권고

□ 주요 보안점검 및 모니터링 사항

구분	우선 점검사항	주요 모니터링 대상
① 외부 노출 시스템	미사용 서비스 차단, 취약점 보완, 관리 기능 접근 제한	여러 경로·서비스에 대한 반복 접근, 설정·백업 파일 조회 시도
② 웹·API	데이터·기능별 권한 검증, 입력값 처리 점검, 조회 범위 제한	식별자를 변경한 연속 조회, 접근 거부 이후 다른 경로를 통한 조회
③ 계정·인증정보	관리자 다중인증 적용, 노출 키 폐기·교체, 최소권한 설정	새로운 접속 환경에서의 인증정보 사용, 계정 생성·권한 확대
④ 서버·내부망	서비스 계정 권한 축소, 시스템 간 통신 제한, 보안 프로그램 작동 확인	웹서버의 비정상 명령 실행, 내부 시스템 탐색, 신규 외부 통신
⑤ 중요정보·대응체계	다운로드 권한 제한, 로그 통합 관리, 초동대응 절차 점검	다수 자료의 순차 조회, 비정상 반출, 로그 삭제·수집 중단

□ **주요 보안강화 방안**

① 외부 노출 자산 확인 및 취약점 조치

- 인터넷에서 접근 가능한 도메인·하위 도메인, IP주소, 웹서비스 및 원격접속 서비스의 운영 현황을 확인하고 담당자가 지정되지 않은 자산과 시험용·미사용 서비스 정리
- 관리자 페이지, 데이터베이스 및 관리용 접속 기능은 업무상 필요한 대상과 지정된 접속 경로에서만 접근하도록 제한
- 운영체제, 웹 프레임워크, 라이브러리 등의 보안 업데이트를 적용하고, 즉시 조치가 어려운 경우 접근 제한 등 임시 보호조치와 후속 조치 일정 관리
- 웹 공개 경로에 환경설정 파일, 소스코드 저장소 정보, 백업 파일 및 상세 오류정보가 노출되는지 점검

② 웹·API 취약점 및 접근권한 검증 강화

- 로그인 여부와 별도로 각 요청에 대해 해당 데이터·기능의 이용 권한을 서버에서 검증하고, 일반 사용자의 관리자 기능 접근 차단
- 별도 시험 계정을 이용하여 문서번호·사용자번호 등 요청값 변경 시 다른 사용자의 정보가 조회·수정되는지 확인하고, 권한 없는 요청이 거부되도록 조치
- 데이터베이스 질의는 매개변수화된 쿼리 등 안전한 방식을 사용하고, 사용자 입력이 질의문이나 시스템 명령으로 해석되지 않도록 구현 점검
- 외부 URL의 내용을 가져오는 기능은 허용된 목적지·프로토콜로 통신을 제한하고, 내부 관리 서비스 및 클라우드 인증정보 제공 경로에 접근하지 못하도록 통제
- 계정·인증토큰별 호출 횟수, 조회 기간, 반환 건수 및 다운로드 용량에 업무 특성에 맞는 제한 적용

③ 계정 및 인증정보 보호

- 관리자·원격접속 계정에 다중인증(MFA, Multi-Factor Authentication)을 적용하고, 일반 업무 계정과 관리 계정을 구분하며 미사용 계정·불필요한 권한 회수
- 소스코드, 코드저장소 변경 이력, 설정 파일 및 협업도구에서 비밀번호·접근키·인증토큰 노출 여부 점검
- 노출된 인증정보는 게시물·파일 삭제에 그치지 않고 사용 차단 및 폐기·교체를 수행하며, 해당 정보의 사용 이력을 확인하여 추가 접근 여부 조사
- 시스템 간 연동 계정과 접근키는 필요한 자원·기능에만 권한을 부여하고, 가능한 경우 유효기간이 짧은 임시 인증정보 사용. 보호나라 인증정보 보호 권고
- 유지보수를 위한 외부 계정은 필요 시 최소한의 권한만 부여하여 생성하고 다중인증(MFA) 적용과 사용 이후 반드시 제거(네트워크 접속 연결도 동일하게 운영)

④ 서버 침해 및 내부 시스템으로의 확산 방지

- 웹·애플리케이션 실행 계정의 관리자 권한을 제거하고, 데이터베이스·파일 저장소 접근권한을 업무에 필요한 범위로 제한

- 웹서버에서 내부 시스템으로 연결되는 통신은 서비스 운영에 필요한 대상·포트만 허용하고, 불필요한 인터넷 송신 제한
- 파일 업로드 경로에서는 서버 측 스크립트가 실행되지 않도록 설정하고, 웹 경로의 비인가 파일 생성·변경 여부 점검
- 백신 및 단말 탐지·대응 도구(EDR)의 작동 상태를 확인하고, 웹서버 프로세스의 비정상 명령 실행과 내부 시스템 접속 시도에 대한 경보 설정

⑤ 정보 유출 탐지 및 연계 모니터링 강화

- 중요정보 조회·다운로드·내보내기 기능은 사용자별 업무 범위로 제한하고, 응답에 포함되는 개인정보·내부정보를 필요한 항목으로 최소화
- 웹·API, 인증, 서버, 데이터베이스 및 클라우드 로그의 시간을 동기화하고, 계정·요청 식별정보 등을 활용하여 시스템 간 행위를 연계 확인
- 로그에는 발생 시각, 요청 경로, 처리 결과, 접근 대상 및 전송량 등 분석에 필요한 정보를 기록하되 비밀번호·인증토큰 원문 등 비밀정보가 저장되지 않도록 설정
- 대량 요청뿐 아니라 소량의 조회가 반복되어 누적되는 정보 접근도 확인할 수 있도록 단시간 탐지와 장시간 누적 분석을 함께 수행

□ 침해 의심 시 대응 방안

- 침해사고 발생 또는 의심 정황 확인 시 한국인터넷진흥원에 신고

※ KISA 인터넷 보호나라(https://boho.or.kr) → 해킹 사고 신고 또는 상담(국번없이 118)

- 침해가 의심되는 시스템은 추가 피해 확산 방지를 위해 네트워크에서 신속히 격리

※ 사고 분석에 필요한 시스템 로그 및 관련 증적을 훼손·변조되지 않도록 보존

□ 작성 : 위협분석단 AI종합분석팀

이전 글 Cisco 제품 보안 업데이트 권고

다음 글 금융권 등 개인정보 유출 사고 피해보상금 지급 등 사칭 피싱 주의 권고

목록으로

개인정보처리방침 | FAQ | RFC 2350

KISA 대국민서비스 바로가기