랜섬웨어 감염에 대비한 기업의 보안점검 권고

문서 번호	A3AEGIS-20200911-01
작성 일자	2020 년 9 월 11 일
제공 부서	㈜에이쓰리시큐리티 관제센터 aegisteam

랜섬웨어 감염에 대비한 기업의 보안점검 권고

□ 개요

o 최근 기업 대상 랜섬웨어 감염 및 정보유출 사고가 지속적으로 발생하고 있어 각 기업의 철저한 보안 점검 및 대비 필요

□ 주요 사고 사례

o (서버) 보안 설정이 미흡하여 랜섬웨어 감염 및 주요 자료 유출

- [사례1] 쉬운 패스워드를 사용하거나 접근제어 정책 없이 외부에서 원격포트(3389, 22)로 접속
- [사례2] 내부망에 접근하기 위해 구축한 VPN 장비의 취약한 계정관리 및 보안 업데이트 미적용
- [사례3] 보안지원이 종료되거나 보안 업데이트가 적용되지 않은 운영체제 및 소프트웨어 사용

o (PC) 보안 수칙을 준용하지 않아 랜섬웨어 감염 및 주요 자료 유출

- [사례1] 공문, 이력서, 견적서 등으로 위장한 악성메일의 첨부파일(랜섬웨어) 실행
- [사례2] P2P 프로그램을 통해 다운로드 받은 최신 영화 등으로 위장된 파일(랜섬웨어) 실행
- [사례3] 취약한 버전의 브라우저를 이용해 악성코드(랜섬웨어)가 은닉된 웹사이트 방문

o (NAS) 보안 설정이 미흡하여 랜섬웨어 감염 및 주요 자료 유출

- [사례] 접근제어 없이 공장 출하 시 설정된 기본 관리자 패스워드를 사용하거나, 보안 업데이트 미적용

□ 보안 권고 사항

o 서버 보안 강화 방안

- 보안 지원이 종료된 운영체제 및 소프트웨어는 신속하게 업그레이드를 수행하고, 매월 운영체제 및 주요 프로그램(메일, 웹, JAVA 등)의 보안 업데이트 확인적용
- 기본 원격포트(22. 3389) 사용을 자제하고, OTP 등을 통한 추가 인증 강화
- VPN 장비를 운영하는 경우, 허가된 사용자와 단말기만 업무망에 접근할 수 있도록 설정하고 OTP 등을 통한 추가 인증 강화
- 다수의 서버를 운영하는 경우 내부 서버 간 원격접속이 불가능 하도록 접근제어설정
- 주요 관리자 PC에 대한 주기적인 보안 점검 및 인터넷망 분리 운영
- 랜섬웨어 감염에 대비한 기업의 보안점검 권고

☞ 특히 아래의 취약점을 이용하여 감염되는 사례가 있으니 반드시 보안 업데이트 등 조치 필요

(1) 윈도우 Exchange 서버 취약점 보안 업데이트 권고 (CVE-2020-0688)

(2) 윈도우 RDP 원격코드실행 취약점 보안 업데이트 권고 (CVE-2019-0708)

(3) 유닉스/리눅스 계열 운영체제 Sudo 명령어 취약점 보안 업데이트 권고 (CVE-2019-14287)

(4) 펄스시큐어社 VPN 제품 취약점으로 원격에서 세션 탈취가 가능한 취약점 (CVE-2019-11540)

o PC 보안 강화 방안

- 피싱 메일에 주의하고 본문 링크 클릭, 첨부파일 다운로드, 실행에 주의
- P2P 프로그램 사용 시, 다운로드 받은 파일에 대한 확장자 확인* 후 실행 * 확장자명이 실행 파일(.exe 등)인 경우, 악성코드일 가능성이 높으므로 백신점검 및 삭제
- 매월 운영체제 및 주요 프로그램(웹브라우저, Flash, Java 등)의 보안 업데이트 확인적용
- 상용 메일을 통한 주요 업무 자료 송수신 금지 ※ 불가피한 경우, OTP 설정 및 허가된 사용자 단말기 추가

CONFIDENTIAL AND PROPRIETARY

A3SECURITY

등을 통해 인증 강화

o NAS 보안 강화 방안

- 최초 설치 시 기본 관리자 패스워드는 반드시 변경 후 사용
- 자동 업데이트를 활성화하여 최신 펌웨어 유지
- 인터넷을 통한 직접 접속은 차단하고, 사내망에서 운영 권고 ※ 불가피한 경우, 장비의 비밀번호 관리 및 백업, 보안 업데이트 등 철저한 관리 필요

☞ 특히 아래의 취약점을 이용하여 감염되는 사례가 있으니 반드시 보안 업데이트 등 조치 필요

o QNAP社 PhotoStation 제품 등 관리자 권한탈취 취약점 (CVE-2019-7192 ~ CVE-2019-7195)

o 공통 보안 강화 방안

- 중요 파일 및 문서 등은 네트워크와 분리된 오프라인 백업 권고
- 자료유출에 대비해서 DRM 등 문서암호화 보안솔루션 도입 권고
- 유추하기 어려운 패스워드(숫자, 대소문자, 특수문자 조합 8자리 이상)사용으로 관리 강화
- 사용하지 않는 네트워크 서비스는 비활성화하고, 인가된 관리자만 접속할 수 있도록 방화벽 등에서 접근제어설정
- 신뢰할 수 있는 백신을 설치(최신 버전 유지, 실시간 감지 적용 등)하고 정기적으로 검사 진행

o 이상 징후 포착 및 침해사고 발생시, 한국인터넷진흥원으로 즉시 신고 ※ 'KISA 인터넷보호나라&KrCERT' 홈페이지(www.krcert.or.kr 또는www.boho.or.kr) - 상담및신고- 해킹사고 ※ 한국인터넷진흥원 인터넷침해대응센터 종합상황실(02-405-4911~5, certgen@krcert.or.kr)

o 참고 : 랜섬웨어 대응을 위한 안내 가이드 및 백업 가이드(www.boho.or.kr, 자료실)

□ 작성 : 침해사고분석단 사고분석팀