암호화 정책

1- 개요

“목적” 참고.

2- 목적

이 정책의 목적은 상당한 공개 검토를 받아서 효과적으로 작동함이 입증된 알고리즘에 대해서는 암호화 사용을 제한하는 지침을 제공함에 있다. 추가적으로, 이 정책은 미국 이외의 지역에서 암호화 기술 보급 및 사용에 대한 연방 규정을 지키고 법적 권한을 부여받기 위한 방향을 제공한다.

3- 범위

이 정책은 [단체 이름] 또는 개인 소유의 컴퓨터 또는 워크스테이션을 사용하여 [단체 이름]의 네트워크에 접속하는 [단체 이름]의 모든 직원, 계약자, 인턴, 공급 업체 및 대리인에게 적용된다.

4- 정책

a) 워크스테이션의 암호화

1. 모든 [단체 이름]의 개인 컴퓨터, 워크 스테이션 및 데이터 저장소는 Mac 사용자의 경우 VeraCrypt ,FileVault과 윈도우 사용자의 경우 bitlocker 등 신뢰할 수 있는 오픈 소스 암호화 소프트웨어를 사용하여 전체 디스크 암호화를 사용해야 한다.
2. 강력한 암호를 가진 화면잠금은 필수이다. 지키고 있는 사람이 없는, 사용중이지 않은 기기는 2분 이내로 자동 화면잠금이 활성화 되어야 한다.
3. 암호화된 기기는 사무실을 떠나기 전 전원을 꺼야한다.
4. 전체 디스크 암호화는 다음 알고리즘 중 하나를 사용해야 한다.
    a. AES-Twofish-Serpent
    b. SHA-512
    c. AES
    d. Triple DES

b) 스마트폰 암호화

1. [단체 이름]의 네트워크에 연결된 모든 스마트폰 뚠 태블릿은 반드시 각 스마트폰의 보안설정에서 전체 디스크 암호화 지원을 사용하여 암호화 되어야한다.
2. 직원들은 강력한 암호를 사용해야 한다.
3. 강력한 암호를 가진 화면잠금은 필수이며, 2분 이내로 자동 화면잠금이 활성화 되어야 한다.

c) [단체 이름]의 저장 장치 (하드디스크, USB 플래시 드라이브와 백업)

4. 모든 저장 장치는 [단체 이름]에 속하며 [단체 이름]의 정보가 있을시 전체 디스크 암호화를 통해 암호화 되어야 한다.
5. 직원들은 강력한 암호를 사용해야 한다.

d) 주요 계약 및 인증

1. [단체 이름]은 사용자들이 [단체 이름]의 직원들이 주고받는 이메일에 대하여 (해싱, 데이터 압축, 대칭 키 암호화 (symmetric-key cryptography) 및 공개 키 암호화 (public-key cryptography)를 제공하기 위하여) PGP 암호화를 사용하도록 장려한다.

2. 엔드 포인트(end points)는 세션 키를 교환하거나 파생되기 전에 반드시 인증되어야 한다.

3. 신뢰를 쌓기 위해 사용하는 공개 키는 사전에 인증되어야 한다. 인증의 예시로는 암호화되어 서명된 메세지를 통한 전파, 공개 키 해시의 수동적 인증이 있다.

4. 인증을 사용하는 모든 서버는 (예: RADIUS 또는 TACACS) 신뢰할 수 있는 공급자가 서명한 유효한 인증서가 설치되어야 한다.

5. SSL 또는 TLS를 사용하는 모든 서버 및 응용 프로그램에는 잘 알려지고 신뢰할 수 있는 공급자가 서명한 인증서를 가져야 한다.

e) 키 생성

1. 암호화 키는 분실, 도난, 또는 손상을 방지할 수 있는 안전한 방식으로 생성되고 저장되어야 한다.

2. 키 생성은 산업 표준의 난수 생성기(RNG)를 통해 시드되어야 한다. ***NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2*** 를 예시로 참고한다.

나는 [단체 이름]의 "암호화 정책"을 읽었으며 [단체 이름]에 계속하여 고용되기 위한 조건 중 하나로 이에 따를 것을 동의한다. 나는 위 정책을 위반할 경우 해고될 수도 있단 걸 이해한다.

_____

사용자 서명

_____

날짜