암호 구성 지침

1- 개요

암호는 정보 보안의 핵심 요소이다. 암호는 사용자 계정을 보호하기 위해 사용한다. 그러나 잘못 구성된 암호는 개별 시스템, 데이터, 또는 [단체 이름]의 네트워크에 손상을 가져올 수 있다. 이 지침은 안전한 암호를 생성하기 위한 최상의 방법을 제공한다.

2- 목적

이 지침의 목적은 강력한 암호생성을 위한 최상의 방법을 제공하는 데에 있다.

3- 범위

이 지침은 제3자와 관련된 모든 직원을 포함하여 [단체 이름]에서 일하는 직원, 계약자, 인턴, 공급업체 및 대리인에게 적용된다. 이 지침은 사용자 레벨 계정, 시스템 레벨 계정, 웹 계정, 이메일 계정, 화면보호기 보호, 클라우드 서비스, 로컬 라우터 로그인을 포함하되 이에 국한되지 않는 모든 종류의 암호에 적용된다.

4- 지침서

모든 암호는 다음 지침을 충족하거나 그 이상이어야 한다.

강력한 암호는 다음과 같은 특징이 있다:

- *최소한 12개의 영문과 숫자가 포함되어 있다.*
- *대문자와 소문자를 모두 포함한다.*
- *적어도 하나의 숫자를 포함한다 (예: 0-9).*
- *최소한 하나 이상의 특수 문자를 포함한다 (예: !$%^&*()_+|~-=\`{}[]:";'<>?,/).*

잘못되거나 약한 암호는 다음과 같은 특성이 있다:

- *여덟 자 미만이다.*
- *외국어를 포함한 사전에서 찾을 수 있거나 비속어, 방언, 전문용어이다.*
- *생년월일, 주소, 전화번호와 같은 개인정보나 가족 구성원, 애완동물, 친구, 판타지 캐릭터의 이름을 포함한다.*
- *건물 이름, 시스템 명령어, 웹사이트, 회사, 하드웨어 또는 소프트웨어 등 업무와 관련된 정보를 포함한다.*
- *aaabbb, qwerty, zyxwvuts, 123321 등 특정 알파벳 및 숫자 패턴을 포함한다.*
- *일반 단어를 거꾸로 쓰거나 앞뒤에 숫자를 포함하고 있다 (예: terces, secret1, 1secret).*
- *"Welcome123" "Password123" "Changeme123" 와 유사한 형태이다.*

절대로 암호를 적어두어선 안 된다. 대신 쉽게 기억할 수 있는 암호로 만들어야 한다. 노래 제목, 확약, 또는 다른 어구들에 기반을 둔 암호를 만드는 것도 한 방법이다. 예를 들어, "This May Be One Way To Remember" 같은 어구는 TmB1w2R! 또는 여기서 변형된 암호가 될 수 있다.

(주의: 이 예제 중 하나를 암호로 사용하면 안 됨!)

패스프레이즈

패스프레이즈는 일반적으로 공개/개인 키 인증에 사용된다. 공개/개인 키 시스템은 모두가 알고 있는 공개적인 키와 사용자 개인에게만 공개된 개인 키 사이의 수학적 관계를 정의한다. 개인 키를 잠금해제 하기 위한 패스프레이즈 없이는 사용자는 액세스를 얻을 수 없다.

패스프레이즈는 사용 중인 암호와 유사하다. 그러나 패스프레이즈는 비교적 길고 여러 단어로 구성되어 있어 사전을 사용한 공격에 대해 더욱 강한 보안을 제공한다. 강력한 패스프레이즈는 일반 암호 생성 지침을 따라 대문자와 소문자, 숫자, 그리고 특수문자를 포함해야 한다 (예: TheTrafficOnThe101Was&!$ThisMorning!).*

나는 [단체 이름]의 암호 생성 지침을 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