Donnell Sample

CST 221

11/15/2020

User Interface and security

1. One-Factor logging into root

* A user will be required to enter their password to access super user
  + Authentication scheme
* The password must be a mix of alpha-numeric characters 1 uppercase, 1 special character and 12-20 characters in length
  + Data input requirements
* The user password will be encrypted
* The password will never display as it being typed in clear text
* If five attempted are exhausted and authentication error message will appear and the account will be locked
  + Secure and hack proof
* The user gets 5 attempted to access as root user
* The user will have to use sudo command with passwd to reset root password
  + Outlined security policies

1. Two-factor Authentication – logging into the system

* A user will require to enter a username, password and a six digit verification code that automatically displayed on a trusted device.
  + Outline authentication scheme and factors required
* A user name will be a mix of alpha-numeric character and be 8-20 characters in length
* A password must be a mix of alpha-numeric characters, 1 uppercase, 1 special character and 12-20 characters in length
* The user will have to enter a trust device code from a phone number or email
  + Clear outline of data input requirement
* Username and password will be encrypted
* Password will never be displayed as it is being typed
* Code user gets in email or phone will always change if after 5 minutes or resent
  + Outline of security and hack proof
* The user must change their password every 90 days
* The user may not reuse last 8 passwords
* The user will not be able to log in if the trusted device code is wrong
* Trusted device must have a valid email or phone number
* User will be locked out after 5 unsuccessful attempts to log in
* The user will be informed to possibly change passwords if they cannot log it
* The user will not be informed which authentication factor for user name and password is incorrect
  + Outlined security policies

1. Multi-factor authentication updating applications

* A user will require to enter a username and password
* A user will be required to answer a security question
* A user will be required to enter a pin
  + Authentication scheme
* A user name will be a mix of alpha-numeric character and be 8-20 characters in length
* A password must be a mix of alpha-numeric characters, 1 uppercase, 1 special character and 12-20 characters in length
* Security question answer must be alpha characters
* Pin must be numeric only 4 digits
  + Clear outline of data input requirement
* Username and password will be encrypted
* Password will never be displayed as it is being typed
* A right or wrong answer will never be shown when security question is answered
* Pin will never be displayed when typed
  + Secure and hack proof
* The user must change their password every 90 days
* The user may not reuse last 8 passwords
* User must answer the security questions provided
* Pin and security question answers will not change unless reset by the user
  + Outlined security policies



