Team: Team 15

Inject Number: 12

Inject Duration: 70 Minutes

Inject Start Date/Time: Sat, 02 Feb 2019 16:51:47 +0000

From: CISO

To: Security Team

Subject: (3.1.1|3.1.2|3.1.8) Password Policy Creation and Implementation

Weak passwords have been a problem for us in the past.

Create Policy:
Create a policy on passwords for use within the organization and send that policy in a business memo to the Chief Information Security Officer in Word document or pdf. Ensure the policy is customized to include team name and the specific requirements defined below as well as industry best practice.

While NIST 800-63B states 8 characters and single factor are acceptable for AAL-1, many of the caveats are difficult to vet (for example, the 8-character password has not been part of a previous breach, checking for context-specific passwords, etc.) and as such, the CISO has decided to standardize on the following:

The policy must feature:
1. Complexity: minimum of 1 special character, 1 upper case character, 1 lower case character, 1 numerical character
2. 10 character minimum
3. Lockout the user after 5 failed password attempts with a minimum of a 5 minute timeout before additional attempts can be tried
4. Users/administrators passwords must be changed every 90 days
5. No password hints

Implement the Policy on all systems/services:
Implement the policy on all devices/accounts and document the implementation in a business memo utilizing a table with the system/service name on one axis and then the 5 requirements described above on the other axis. Check the box verifying the compliance once it is implemented for each requirement or describe why you couldn't for that

device/service and briefly describe if there are any mitigating controls for non-compliant items.

Thank you.

CISO