SmartHealth Data Breach

TEAM 2 - RAGAPRABHA, SUMIAH, BIJAL

The Incident

Smart Healthcare Systems faced a data breach on 16th March 2016.

Confidential data regarding pricing was stolen from product database.

Investigation

Hackers accessed the database by compromising existing employee’s password

Concerned employee saved a copy of his old password on his home computer

Hackers compromised his home computer

Hackers then tried combination of passwords similar to the old password and gained access in 100+ attempts

Root Cause Analysis

Hackers were able to get into the system using something as simple as a dictionary style attack

They were able to succeed because of SmartHealth’s weak spot

Existing password policy needs immediate revision

Issues with existing policy

Current password policy allows users to set weak passwords

- Repeated patterns
- Common dictionary words

Additionally,

Employee feedback revealed that remembering different password for systems within the organization is difficult and hence they store local copies of password

Goals/Expectations

- Password creation should be strengthened
- Password should be able to withstand brute-force, dictionary and keylogger attacks
  - Discourage the use of the smaller passwords, similar patterns.
- Password policy should not be such that users are forced to write down their passwords.
  - Discourage use of system generated passwords/ educate users on not storing their passwords
- Single password for all systems
- Repeated failed attempts should not be ignored.
- Educate employees on strong password creation.

Questions?