Sir/Madam,

The leaked hashes use MD5 hashing algorithm, which according to my observation is providing very little protection in case of database leaking.

The hashing algorithms like MD5 and SHA-family of algorithms are the standard one's but not that strong.

After trying to crack the passwords I came across certain drawbacks of company's policy.

1. The passwords were using very common combinations and there was no specific rules on their creation.

2. The length was short which in case of cracking could be an advantage for the hackers.

3. Salting was not implemented as it creates a strong hash value.

4. Strong hashing algorithms were not used.

The changes I would suggest in the password policy are:

1. Creating combination of letters, numbers and symbols is the best approach to begin with.

2. Don't let users use common words, their username, personal information or combination of that as a password.

3. The length should be increased.

4. Hashing algorithms like bcrypt, scrypt or PBKDF2 can be used. It is ought to increase the time in cracking.

OBSERVATIONS:

e10adc3949ba59abbe56e057f20f883e:123456

e99a18c428cb38d5f260853678922e03:abc123

d8578edf8458ce06fbc5bb76a58c5ca4:qwerty

96e79218965eb72c92a549dd5a330112:111111

3f230640b78d7e71ac5514e57935eb69:qazxsw

fcea920f7412b5da7be0cf42b8c93759:1234567

f6a0cb102c62879d397b12b62c092c06:bluered

25d55ad283aa400af464c76d713c07ad:12345678

5f4dcc3b5aa765d61d8327deb882cf99:password

8d763385e0476ae208f21bc63956f748:moodie00

Thank you