I hope this message finds you well. Following the recent security assessment and analysis of the leaked password hashes, I have identified several vulnerabilities in our current password protection mechanisms and password policy. This email outlines these findings and provides recommendations to significantly enhance our security posture.

Findings

Hash Algorithm Used: The passwords in the database were protected using the MD5 hashing algorithm. MD5 is a cryptographic hash function that is now considered weak due to its susceptibility to collision attacks. This weakness makes MD5 less effective in protecting passwords against modern cracking techniques.

Level of Protection: MD5 provides minimal protection for hashed passwords. Given its vulnerabilities, cracking passwords hashed with MD5 is relatively straightforward using tools such as Hashcat in conjunction with common wordlists like 'rockyou.txt'.

Password Policy Analysis: Upon analyzing the cracked passwords, the following observations were made regarding our current password policy:

- *Minimum Password Length:* The policy requires a minimum password length of 6 characters
- *Password Creation Requirements:* There are no specific constraints on password composition, allowing users to create passwords with any combination of letters and words.

Recommendations

1. ***Adopt Stronger Hashing Algorithm*:** We should move away from MD5 and adopt a more robust hashing algorithm like bcrypt, scrypt, crypt-SHA or PBKDF2. These algorithms are designed to be computationally intensive and are resistant to brute-force attacks. They will provide much stronger protection for our passwords.
2. ***Implement Salting:*** Incorporate unique salts for each password before hashing. Salting involves adding a unique, random value to each password before hashing. It ensures that even if two users have the same password, their hashed values will be different, making it far more challenging to use precomputed hash tables for attacks.
3. ***Enforce a Stronger Minimum Password Length**:* Raising the minimum length to at least 10 characters will enhance security. Longer passwords are much more resistant to brute-force attacks.
4. ***Strengthen Password Policy**:* Introduce policies that mandate the use of a mix of uppercase letters, lowercase letters, numbers, and special characters. This will enhance password strength and reduce the likelihood of successful attacks.
5. ***Educate Users on Password Practices:*** Guide users to avoid common words, phrases, or easily guessable patterns in their password. They must be encouraged to use passphrases-combinations of random words or phrases-along with special characters and numbers to create stronger passwords.

6. ***Advocate for Password Managers:*** Recommend the use of password managers to generate and store complex passwords securely. This reduces the risk of password reuse and improves overall password management.

I believe these changes will significantly improve our defense against potential breaches and align our practices with current security standards. If you have any questions or need further details, I'm happy to discuss them.

Best regards,
Rishika Hazarika
Governance Analyst
Goldman Sachs.