Forging Effective Security with Password Enforcement

Passwords Are the Weakest Link in Enterprise Security

Users Employ Poor Password Practices

- 90% of businesses support users who utilize the same password for multiple accounts.
- 21% of business users are in violation of their organization’s password reuse policies.

Businesses Fail to Enforce Strong Password Requirements

- 35% of organizations do not place any restrictions on password combinations.
- 41% of organizations do not have a minimum password length.
- 57% of organizations allow users to share their passwords with others.
- 40% of organizations allow users to reuse previously set passwords.
- 52% of organizations do not regularly review passwords to ensure they are compliant.

Compromised passwords are sold on the dark web, granting criminals access to businesses’ most sensitive applications and data.

Violations of Password Policies Result in Significant Consequences to Businesses

- 35% of business users are in violation of their organization’s password reset policies.
- 35% of surveyed organizations are able to directly correlate password breaches to business-impacting consequences.

- Average amount businesses spend repairing damage caused by each violation of password policies:
  - Security breach — malware infection: $5,580
  - Security breach — data compromise: $5,580
  - Unexpected server failure/problems: $5,580
  - Failure to meet regulatory compliance: $5,580
  - Production environment downtime: $5,580
  - Unexpected endpoint device failures: $5,580
  - Production environment performance issues: $5,580
  - Damage to company reputation: $5,580
  - Unexpected database failures/problems: $5,580

Key Elements Needed for Strengthening Password Controls

- Monitor the dark web to identify compromised passwords.
- Immediately close the gaps on vulnerabilities.
- Enforce the use of strong passwords at the time they are created.
- Block the use of any compromised password strings on existing accounts.
- Unify and centralize password policies.
- Enabling adaption to changing conditions in real-time.
- Continuous password enforcement reinforces the weak point in enterprise security to forge an unbeatable chain of access controls.

For more information about Enzoic for Active Directory, go to: www.enzoic.com/active-directory/

Real-world consequences that were attributed to a password policy infraction:

- Security breach — malware infection: 37%
- Security breach — data compromise: 37%
- Unexpected server failure/problems: 30%
- Failure to meet regulatory compliance: 28%
- Production environment downtime: 25%
- Unexpected endpoint device failures: 20%
- Production environment performance issues: 20%
- Damage to company reputation: 15%
- Unexpected database failures/problems: 10%
- Security breach — data compromise: 5%

0% 5% 10% 15% 20% 25% 30% 35% 40%