Enterprise Password Assessment Solution

Detack GmbH

- Founded in 2001
- Specialist for Premium IT-Security Audits
- Customer Focus on Financial Sector
- ATM Audits / Telematics Solution Audits / IBM Mainframe Audits / SAP
- Self-Developed Software (EPAS / Sign IA)
- What Our Customers Value:
  - Professional Services of Highest Quality
  - Trustful Collaboration / Reliability
  - Thought Leadership

http://www.npr.org/sections/alltechconsidered/2016/02/09/466175264/password-security-is-so-bad-president-obama-weighs-in

You've heard it before. Change your password. Change. Your. Password.

But now, Americans are getting that message from the top. Password security is in such a sorry state, our commander in chief is weighing in with a call to action.

Published February 9, 20163:55 PM ET

epas

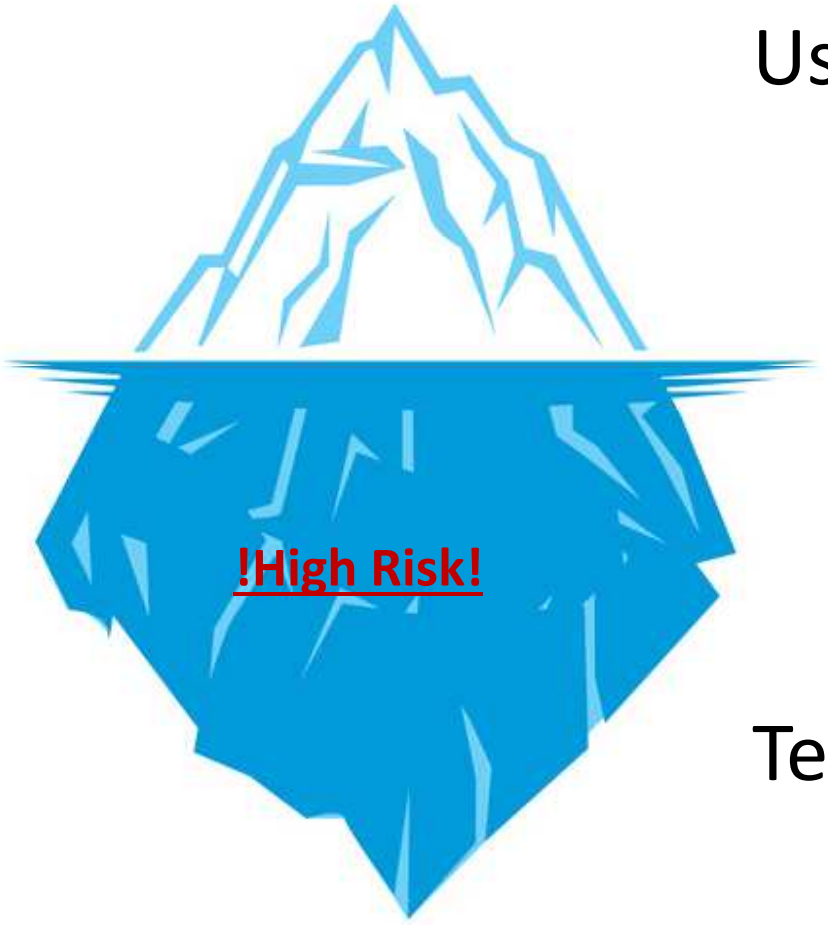
The Password is Dead –

Long Live the Password!

epas

Nothing Works Without Authentication…

epas



Picture source: Fotolia

User-Accounts

Technical / Service Accounts

epas

Password Policies Still Produce Weak Passwords

Pa$$w0rd!

Porsche911

Porsche9!!

RSA@2016

epas

- Passwords & Password Hashes
- Password Attack Methods
- What Makes a Secure Password?
- Password Strength Measurements
  - Password Policies
  - Entropy
  - Structural Entropy

epas

Passwords

- To **authenticate or provide access** for a certain person or service to systems, services or objects.

- Passwords are **stored on the server** which provides authentication. Anyone with **administrative access** to this server would also have **access to** the storage facilities and **the password data**.

  → The technology used to solve this problem is **one-way encryption or hashing**.

epas

Password Hashes

- Hash functions take **any size of input and output a known, constant size output**. They are one way functions.

- A user wanting to authenticate, enters the password in the login box. The server will be able to **compute the hash of the input and compare it with the hash stored** on the disk.

- An attacker who gets hold of the password hashes stored on disk, is **not able to recover the plain-text password** of the user - hashing being a one-way function.

epas

Password Attack Methods

There are two types of attacks by which passwords can be recovered from password hashes:

- **Mathematical:** finding and exploiting weaknesses in the hash algorithm – this rarely works, and any flawed algorithm is quickly discontinued anyway

- **Probing:** trying different passwords in the attempt to obtain the same hash value as the stored one – this is the most used and effective attack method

A Secure Password

- ✓ **Length –** the longer a password, the more secure
- ✓ **High entropy –** use as many different characters as possible
- ✓ Cannot be found in **dictionaries**
- ✓ Does not consist of or include **account or known information**
- ✓ Is not derived from a known word in a **predictable** manner

A **secure password** is defined as a character string which is **difficult to predict** and which **requires unrealistic resources in order to recover it** from its cryptographic hash.

epas

Strength Measurements

- **Password Policy (subjective)**
  - enforce length requirements or other simple restrictions
- **Entropy (objective)**
  - pure mathematical entropy, the strength of a password depends on “randomness”
- **Structural Entropy (objective)**
  - combines mathematical entropy with language specific character grouping

epas

Password Policy

Pa$$w0rd!

- Does not take into account a password's **randomness** or **inclusion in a dictionary** (mostly)
- Does not prevent **password sharing or reuse**, on the same system or across different systems
- **Service accounts / technical accounts are usually exempt** from a password policy, especially when regarding the validity time

epas

Structural Entropy

Mathematical Entropy with a few Improvements:

- Detects dictionary usage
- Detects spatial patterns: *qwerty, azerty, asdf, etc*.
- Detects repeatable sequences: *aaaaa, bbbbb, etc.*
- Detects sequences: *abcdefg, 987654321, etc.*
- Detects other common patterns: l33t speak, first letter capitalization, years, dates

→ **Realistic Password Strength Estimation**

Why EPAS?

→ Passwords are still **THE authentication instrument**

→ Passwords are **here to stay**

→ More than **60% of passwords** we have audited do not satisfy minimum security standards and are **weak**

→ Before EPAS, there was **no legal way to audit passwords**

→ Password **policies are not enough** to get strong passwords

epas

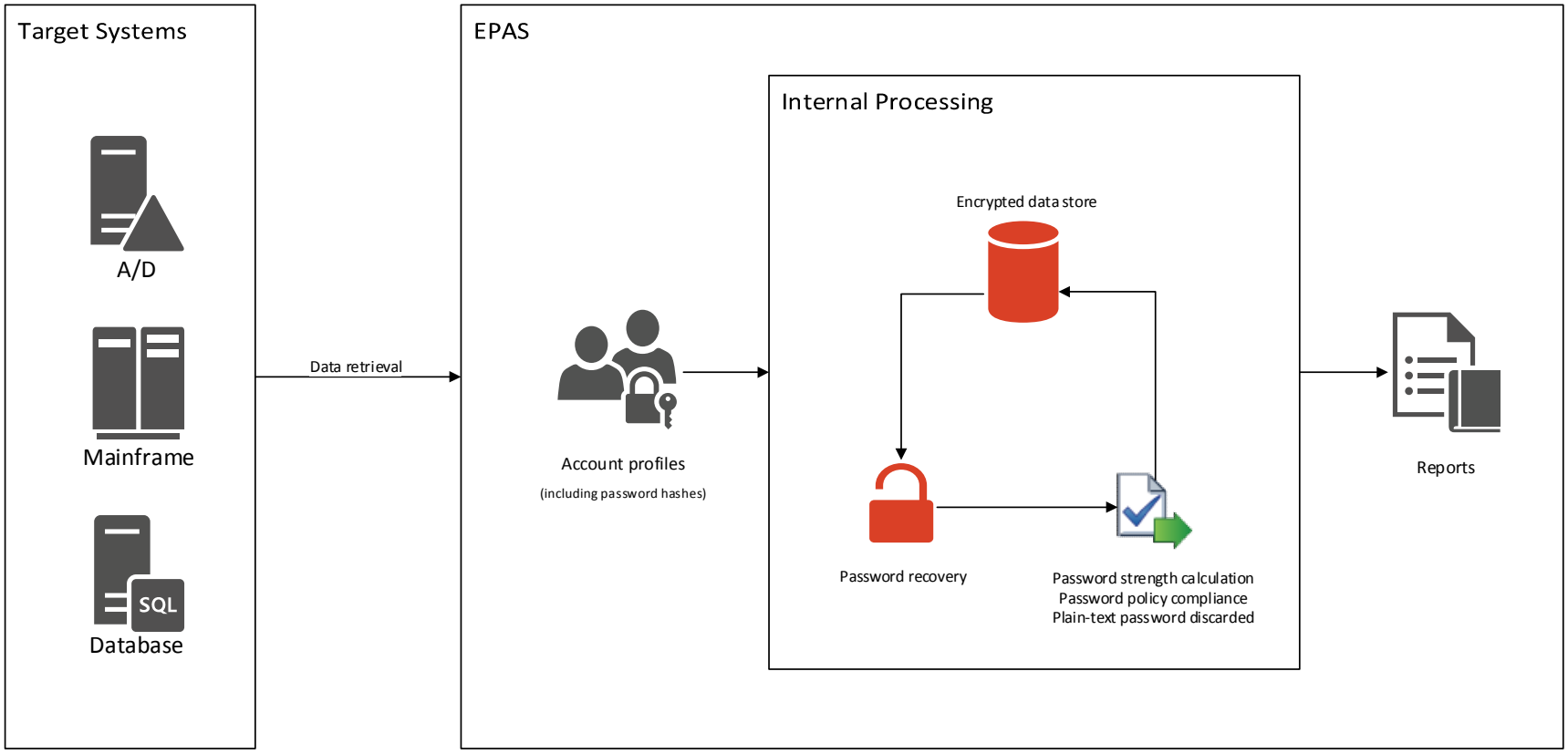
epas

Helps you to:

- **Implement strong passwords**
- **Builds resilience against password attacks**
- **Secures user- AND technical / service accounts**
- **See what you could not see before**
- **Comply with all data protection laws**

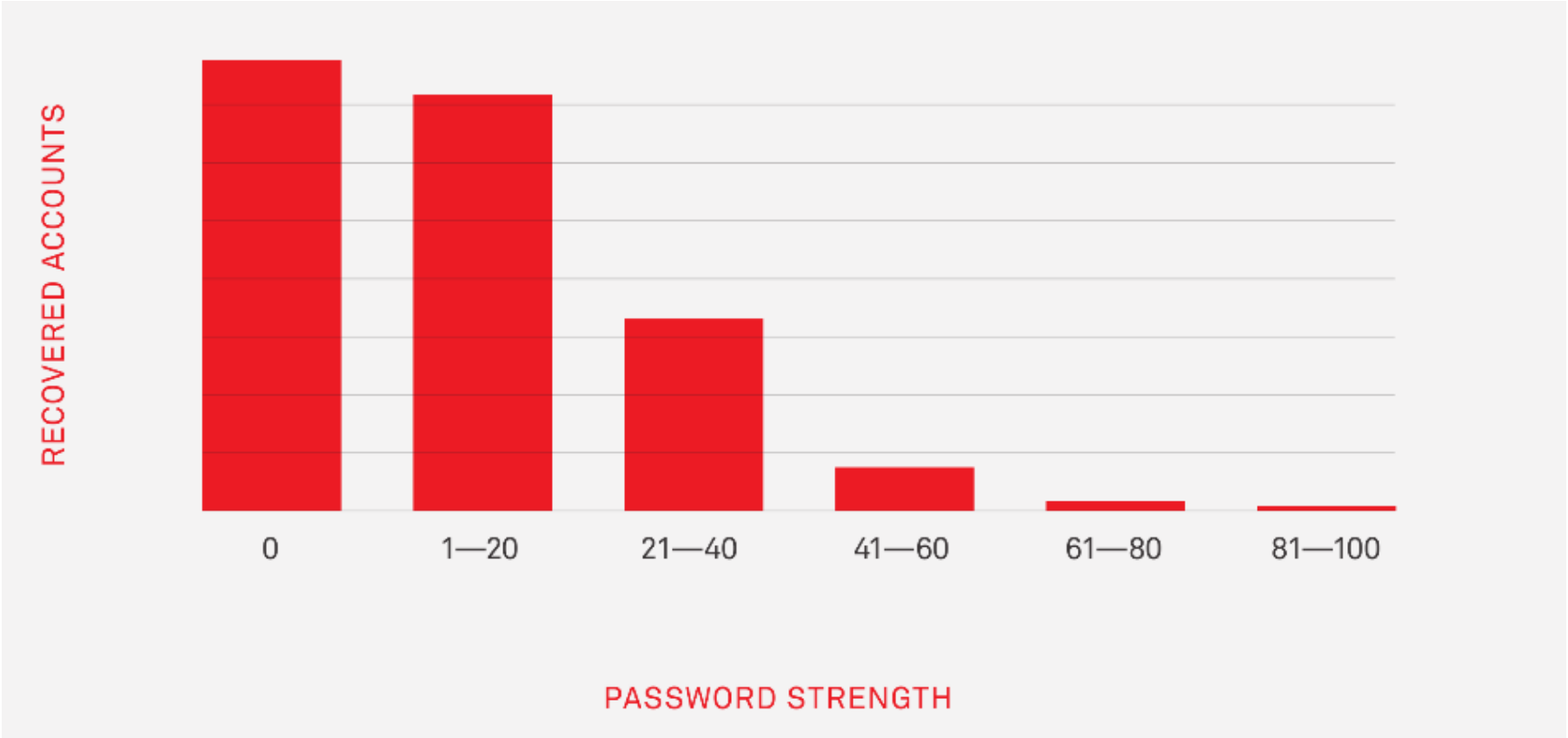
epas

Password Assessment Process (EPAS)



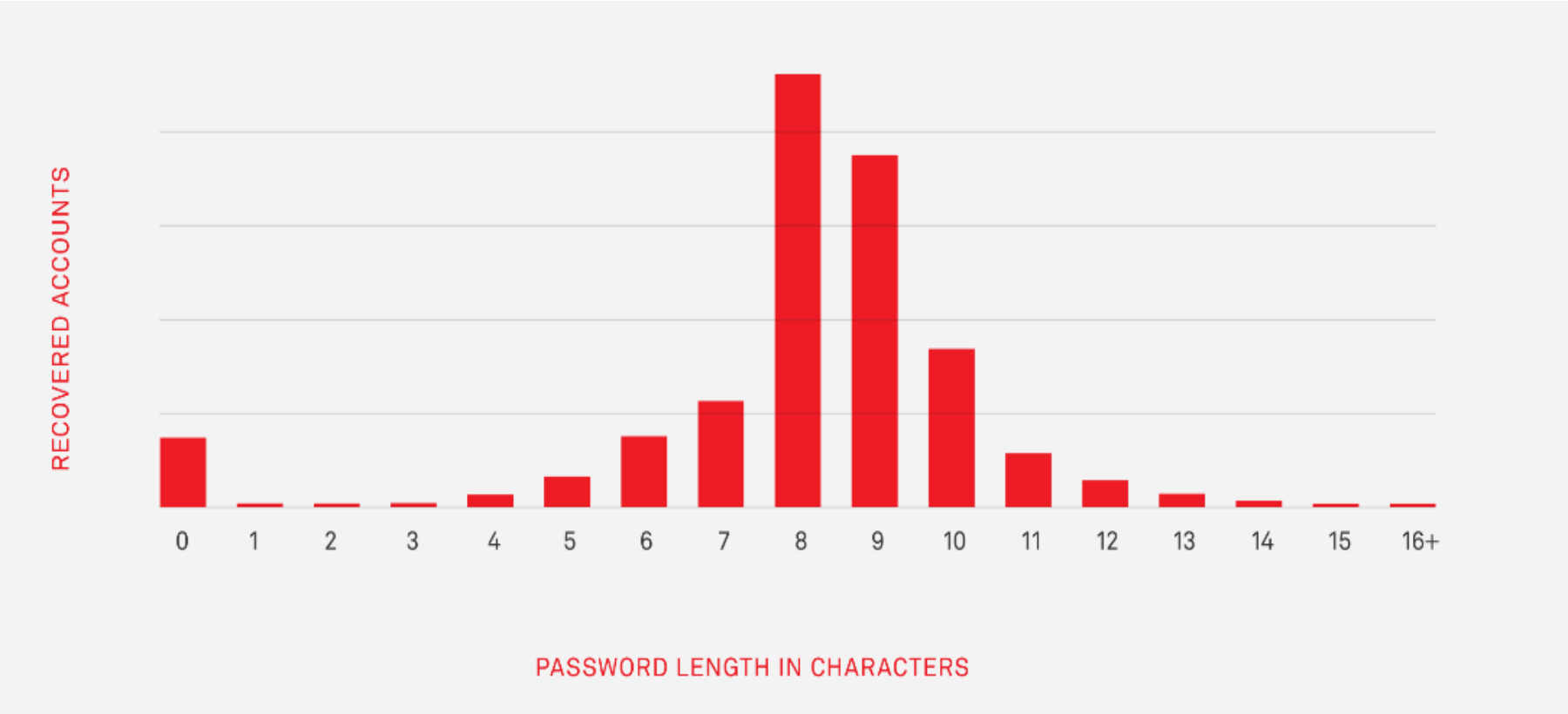
epas

EPAS Password Audit Results



epas

EPAS Password Audit Results



epas

EPAS Password Audit Results

Alphabetical lower case	245822
Alphabetical upper case	15394
Numeric	138226
Special	38
Alphanumeric lower case	389396
Alphanumeric upper case	25881
Alphabetical upper and lower case	10567
Alphabetical lower case incl. special	15190
Alphabetical upper case incl. special	995
Special and numeric	1835
Alphanumeric upper and lower case	20568
Alphanumeric lower case incl. special	12937
Alphanumeric upper case incl. special	693
Alphabetical incl. special	1616
Alphanumeric incl. special	1302

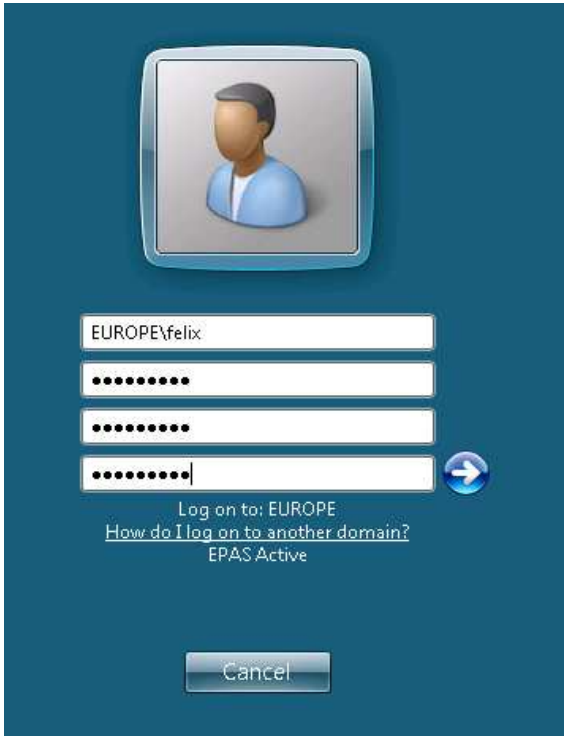
epas

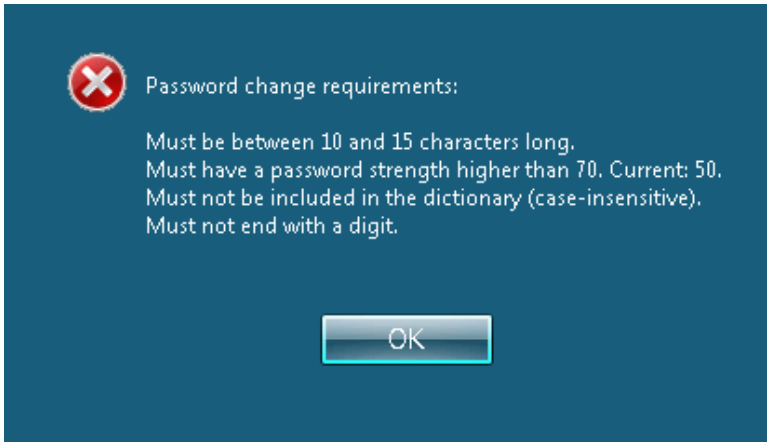
EPAS Password Audit Results

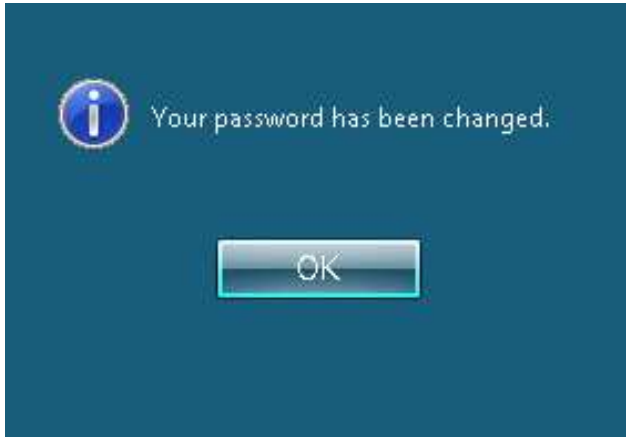
The password is empty	18
Found in the initial or default passwords list	7
Found in the known account information	6941
Found by applying derivation rules to the known account information	572871
Found by applying hybrid rules to the known account information	9619
Found in the chosen dictionary or dictionary list	27855
Found by applying derivation rules to the dictionary or dictionary list	224124
Found by applying hybrid rules to the dictionary or dictionary list	27059
Found by fast brute forcing short password candidates	6990
Found by trying all possible combinations up to a given length	4994

epas

EPAS Password Quality Enforcer

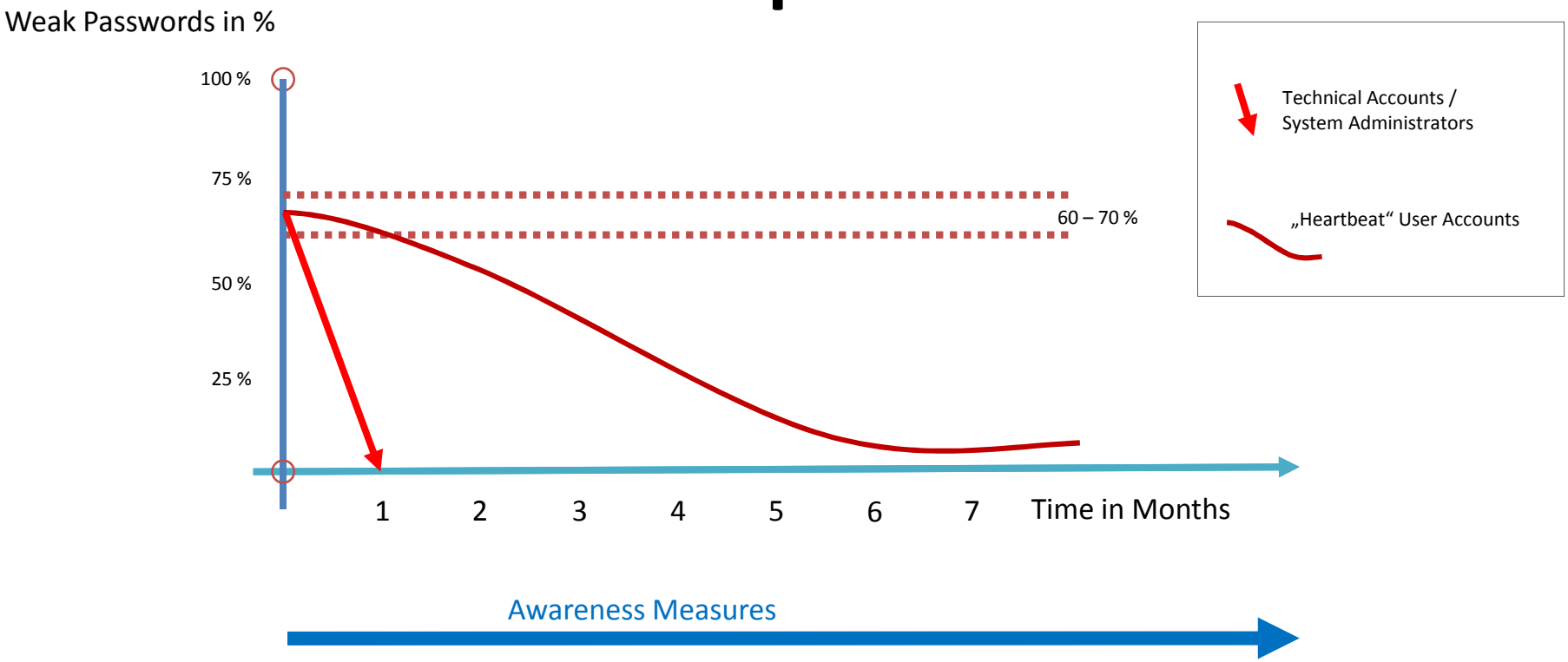






epas

EPAS Password Strength Development



epas

epas

Helps you to protect your:

- **Data**
- **Reputation**
- **Intellectual Property**
- **Data Integrity**
- **Market Share**
- **Revenue and Profit**

epas

Interesting4ME - 0

I4nMtEeresting - 78

I4nMtEeresting? - 100

epas

References

- EPAS Operations Manual / Management Interface Tooltips
- 2600 The Hacker Quarterly, Volume 31, Number Four
- https://tech.dropbox.com/2012/04/zxcvbn-realistic-password-strength-estimation/
- http://arxiv.org/abs/cond-mat/0203436

epas