Use a safe password

Václav Šamša
KeyShield & SecureAnyBox

Agenda

- Introduction about passwords and attacks
- What is the difference
- How can a user recognize the difference?
- What the organization usually does (and should not do)
- What is the fitting solution
- DEMO
- Q&A

What is a password?

- Proves that you know some pre-shared secret
- Password – ancient technology invented by armies:
  - You know the word
  - They let you pass
- OTP – One Time Password
- ODP - One Day Password
- Long term password
- Before – one word for a whole unit
- Now – every account has own word

Is it a must to use a safe password?

- Safe? Safe against what?
- Why 4 digits PIN is still OK?
- Why it is not recommended to use the same PIN for all your cards?
- It is all about the maximum number of attempts the attacker can deliver
- 3 attempts per card – OK for 1 card, bit worst for 30 cards (with 30 cards – 30 x 3 = 90 attempts for 9.999 combinations)

What is the difference?

- Is it possible to use a so-called brute force attack?
- Is it possible to use a dictionary attack?
- It is possible if the attacker can steal the database
- It is much worst if the attacker can steal it unseen (located outside the protected perimeter)
- It seems that all the user needs to know is what type of system he or she is going to use (and set the password)
- Is the offline attack risk or not in some particular case?

How can a user recognize the difference?

- User has usually no chance to learn what is the risk
- A regular user can recognize:
  - Workstation/notebook
  - Information System owned by own organization
  - Information System owned by different organization
  - E-shop, portal – job related use
  - E-shop, portal, hobby/game site – private use
- Some users can understand what is
  - Authentication
  - SSO

What the organization usually does (and should not do)

- Organizations generate policies or rules or instructions like:
  - The minimum length of a password is 15 chars
  - Each password must contain Capital & lower letters, numbers and ..
  - Password expires in … (90) days max
  - Do not use password repeatedly. We keep track of you …
- Keep your passwords in secret storage!
- Most important is good encryption!

What the organization usually does (and should not do)

- Ask yourself and fairly answer **NO**
- IT staff are different human beings than other employees
- Privileged accounts are used by the IT staff only
- Rules are not applied to the IT staff because they „know“
- IT staff member can install and use own personal favourite tool
- Users are idiots because they do not understand IT

What is the fitting solution

- Do not instruct the users to use „safe password“ – provide them with a tool which generates a good password for different cases
- Do not want the users to backup passwords – provide them with a reliable and seamless backup solution
- Keep in mind the shared accounts – almost everything outside enforces you to use “organization account“ instead of “personal account“ – easy to use sharing is a must
- Password etc are very valuable, sometimes critical – do not go without audit (SIEM for larger orgs)

What is the fitting solution

- Hide all your policies and rules in the tool configuration
- Do not stress users (and yourself) by enforcing them to decide whenever they are going to use a new account
- Password etc are very valuable, sometimes critical – do not go without audit (SIEM for larger orgs)
- Sharing protects you against access loss. Offer smart back door for personal but still accounts owned by the organization

What is the fitting solution

- Let the IT staff live a standard user‘s life: files, docs, email, messaging, meals, attendance, entrance, remote access, etc
- Privileged account is always much better than privileged access
- Help anybody who is using privileged accounts to use them in a secure and easy to handle way
- Easy to handle doesn‘t mean convenient. You must unlock 2 locks if your private property door is equipped with 2 locks – insurance companies want to see 2 damaged lock before they pay …

What is the fitting solution

- Does it make sense to buy some solution for the IT staff only? No. Not at all. Every computer user needs such a solution nowadays.
- The demand is growing every day
- Does it make a difference if your organization is private or public owned? No. Not at all.
- The difference is if your password protects access to personal, strategical, or so data or if it is needed to order a meal

What is the fitting solution

- Have you ever seen an IT staff member using 4 different passwords? For everything?
- Have you ever seen personal accounts with 19 chars long password and admin/root/administrator with 6?
- Have you ever heard somebody saying: You should not see how I handle my passwords because it is a tragedy. But no worries, I do sales, logistic, HR only …
- If so, you do not have the fitting solution yet

DEMO time!

- Code:
- If enough time
  - run the demo
- Else
  - Goto Q&A

Questions & Answers

Václav Šamša
KeyShield & SecureAnyBox
vsamsa@tdp.cz