Strong Passwords Are Essential — But Not Enough

Devolutions

STRONG PASSWORDS ARE ESSENTIAL AND LONG, UNIQUE PASSPHRASES ARE EVEN BETTER

An estimated 81% of hacking-related data breaches are due to weak passwords, which have one or more of these characteristics:

- Composed only of numbers
- Composed only of letters
- Too short
- Uses a pattern
- Easy to guess (the #1 worst password is "123456" followed by "password")
- Uses personal information
- Are generic (e.g. "admin")

On the other end of the spectrum are strong passwords, which have all of these characteristics:

- At least 14 characters long
- No personal or generic information (e.g. popular song, etc.).
- Composed of upper-case and lower-case letters
- Includes symbols and numbers

Ideally, using strong passwords would be enough to lock down accounts and network access. However, that isn't always the case. Some end users undermine security and put the organization at risk by:

- Using the same password for multiple accounts
- Insecurely sharing passwords with colleagues
- Improperly storing passwords in spreadsheets and text files, etc.

This means that while strong passwords are essential — and long, unique passphrases are even better — they are not enough to protect endpoints, networks and organizations. Here are 5 things that should also be part of the security puzzle:

1. End User Training

70% of employees don't understand basic cybersecurity. As such, organizations need to create a culture of security awareness by providing adequate, ongoing end-user training through various methods (e.g. presentations, videos, articles, one-on-one coaching, etc.) that highlight risks like phishing. Some organizations are also enrolling end users in online cybersecurity courses so they can grasp the fundamentals.

2. Two-Factor Authentication (2FA)

2FA combines something end users know (e.g. username + password) with something they have (e.g. a device) or something they are (e.g. biometric). While 2FA is not bulletproof, it adds an important layer of authentication — and when combined with Single Sign-On (SSO), it makes life much easier for administrators. Note: if you are exploring various 2FA solutions for your organization, we invite you to read our reviews of some of the most popular options.

3. Centralized Password Management Platform

A robust centralized password management platform like Devolutions Password Server or Devolutions Hub enables your organization to:

- Enforce strong password standards.
- Prevent users from choosing passwords they have selected in the past.
- Screen proposed passwords against lists of known compromised passwords.
- Enforce a minimum password age (this prevents users from circumventing the password system by creating a new password, and then changing it back to an old one).
- Allow end users to store and share confidential information (including but not limited to passwords) in secure vaults.
- Track and audit all password changes.
- Notify end users when it's time to change their passwords before they expire (more on this below).

Due to security fatigue, lack of awareness, and sometimes just plain laziness, research has found that when end users reset their passwords, they often choose weaker ones rather than stronger ones. As such, a growing number of organizations are either eliminating the practice, or they are dialing back the frequency of password resets. For example, instead of forcing end users to reset their password(s) once every three months, they are mandating it once a year.

4. Privileged Access Management (PAM)

88% of companies with more than 1 million folders lack appropriate access limitations, and 58% of companies have more than 100,000 folders accessible to all employees. Having a PAM tool, as well as the right technologies and policies in place, can significantly reduce the size of the threat surface. Here is a list of best practices to follow:

- Analyze all privileged accounts to confirm alignment with acceptable and standardized risk levels.
- Implement the principle of least privilege (POLP).
- Enforce an effective Segregation of Duties (SoD) in order to avoid giving certain users "too many hats" to wear at work. Also keep in mind, however, that when multiple end users have overlapping tasks, if one of them gets compromised, it will most likely expose privileged access to systems.

- Monitor all privileged account usage and enforce strict controls for sharing credentials.
- Use high-trust authentication methods for privileged access using suitable PAM tools and technologies.
- Augment and extend privileged identity management with access governance controls to meet ongoing compliance needs (e.g. mandate that account owners certify they still require privileged access after a period of time).

5. Patch and Vulnerability Management

Unpatched and outdated software is responsible for 22% of data hacks. Here is a list of best practices for addressing this gap:

- Use a good discover tool that relies on a mix of active and passive discovery features to identify physical, virtual, and on/off-premises devices that access the network — including MAC devices, which are more vulnerable to cyber threats than many people believe.
- Don't just focus on operating systems — as many as 80% of software vulnerabilities derive from non-Microsoft apps running on Windows.
- Create a process to patch weekly. Different vendors have various patching release cycles, and trying to keep up with all of them is tedious and can lead to gaps.
- Deploy a flexible architecture that allows agentless and agent support for servers.
- Mitigate exceptions by locking down user permissions, applying whitelisting, and so on.
- Bridge the gap between IT Operations teams and IT Security teams (more on this below).

A survey of 600 IT decision-makers has revealed that 67% do not believe their IT Operations teams and IT Security teams work in a cohesive manner. As a result, there is a lack of basic security hygiene in the organization.

Advice from Our CSO Martin Lemay

"Consider avoiding exposing systems directly to the Internet. Although you might have strong passwords and a good patch management lifecycle -- and 0-day exploits – undiscovered threats might still be able to penetrate them and expose the environment to unnecessary risks. IP restriction strategies and VPN technologies can also help avoid such situations. If there are systems that must be exposed directly to the Internet, implement detailed auditing technologies to detect malicious activities."