SPECOPS

NIST & Compliance: Future-proofing your password policy

Fourteen years after authoring the National Institute of Standards and Technology (NIST)'s official guidance on password security (Special Publication 800-63, appendix A), Bill Burr says he was wrong. It turns out, 8 character passwords with complexity (special characters, capitalization, and numbers), and periodic password changes, aren't all they're cracked up to be. In a recent interview with The Wall Street Journal, Bill apologized for the guidance that has unintentionally encouraged poor password behavior. While he wanted to provide guidelines based on real life data, there wasn't much empirical evidence at the time of the publication. A lot has changed since then – we now have a multitude of mega breaches to shape future best practices.

SPECOPS

What was once best practice, is now an anti-pattern...

Users are accumulating more and more passwords, and many of the recent breaches are the direct result of their compromise. The Verizon 2017 Data Breach Investigations Report found that 81% of hacking-related breaches leveraged stolen and/or weak passwords. As hackers find new ways to exploit password-protected systems, widely accepted password policies, such as character complexity and periodic password expirations, must be changed.

In this paper, we will scrutinize conventional best practices, using knowledge attained from the new Digital Identity Guidelines from NIST. We will also examine the extent to which the NIST recommendations have impacted compliance requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes–Oxley Act (SOX). In the end, we will formulate a strategy that aligns best practice with compliance needs.

Shifting burden from users to authenticators

At the heart of the new guidance from NIST lies a theme: Simplify passwords for users, and place the burden on the authentication system. It pretty much asks organizations to change how they view password security. Perhaps, it has become blatantly obvious that when it comes to password security, users can't seem to avoid predictable pitfalls.

In the document, security is addressed in the chapter titled *Memorized Secret Verifiers*. A memorized secret verifier is any system that needs to check the validity of a password or PIN. In most organizations, that means Active Directory and supporting business systems.

ABOUT SPECOPS

Specops Software develops unique password management and desktop management products based on Microsoft technology. We build on top of Active Directory and Group Policy with innovative, simple, and cost-efficient solutions for organizations around the world.

specopssoft.com/blog

SPECOPS

The NIST Don'ts

Character compositions

Studies show that user annoyance with password policies results in weak passwords. When users are focused on getting into the system, a strong password takes a backseat to a memorable (easy) password. NIST discourages composition requirements, such as a mixture of character types, when setting passwords. While this is not prohibited, the recommendation is to avoid complexity rules, and instead check passwords against known dictionary lists.

Forced password expiration

When forced to set a new password, users conform to predictable patterns – character substitutions, leetspeak, incrementing numbers, and other common habits that do not stand a chance against hackers. Users also have a tendency to forget new passwords. Some resort to writing them down, others forget them altogether, putting a strain on the helpdesk with reset requests. NIST discourages regular password expiration (memorized secrets changing arbitrarily) but requires a password change if there is evidence of compromise.

Knowledge-based authentication

Commonly used for authentication prior to a password reset, knowledge-based authentication (KBA) is an authentication system in which users are required to answer a "secret" question to confirm their identity – *Where did you attend high school?* It goes without saying that answers to such questions are susceptible to social engineering. Social engineering is a form of hacking – a hacker tricks the system into thinking they are an authorized user by using information that is readily available. As such, NIST warns against "specific types of information when choosing memorized secrets."

The NIST Do's

Encourage length

When it comes to password length, NIST requires at least 8 characters, and recommends as long as 64 characters. Size matters, and longer is stronger. Shorter passwords are prone to brute-force attacks. Passphrases, a combination of words that are meaningless together, are easier to remember and harder to crack.

Block dictionary lists

As credentials exposed in one breach can open the door to other systems, NIST requires comparing prospective passwords against a list of common/compromised passwords. These passwords are compiled in a password dictionary, and blocked for future use. It is a bit of a catch-22. To proactively check against a password dictionary, and prevent the creation of vulnerable passwords, you do so when the password is changed. Therefore, if using a password dictionary to strengthen security, you need to make sure the password change is frequent enough to take into account the latest lists. Whether that means periodic password expirations, or manually forcing changes as new dictionaries are added, it is a decision you will have to consider.

Multi-factor authentication

When personal information is available online, passwords are not enough. NIST requires multi-factor authentication to ensure users are properly protected. Tech giants like Google, Microsoft, and Apple all have multi-factor authentication options available to users. Multi-factor authentication requires more than one method of authentication from independent categories of credentials: something you know (password), something you have (mobile device), and something you are (fingerprint).

Compliance requirements

Access management and authentication are at the core of compliance – after all critical personal data is at risk. As long as passwords hold the access key to corporate systems, it is imperative to view compliance requirements in the backdrop of current wisdom about secure passwords.

HIPAA

HIPAA is designed to protect against unauthorized access. While the HIPAA Privacy Rules do not have explicit requirements on user passwords, there is a strong emphasis on the storage of, and access control to, electronic protected health information (ePHI). Sections 164.308(a)(5)(i) and 164.308(a)(5)(ii)(D) require that the following plan is in place when appropriate:

- A security awareness and training program for all members of its workforce
- Procedures for creating, changing, and safeguarding passwords

HIPAA may be ambiguous, but healthcare organizations are subject to the full extent of its rules. The burden falls on healthcare IT to figure out how to put these into practice.

PCI DSS

In contrast, PCI DSS requirements are more specific, and subject to less interpretation. The PCI-DSS standard has this to say about passwords:

- 8.2.3: A minimum length of at least seven characters
- 8.2.3: Both numeric and alphabetic characters
- 8.2.4: Change user passwords/passphrases at least once every 90 days

The full list of password requirements is easy to follow and can be easily achieved with password policy settings.

SOX

The main intention of SOX is to establish verifiable security controls to protect against disclosure of confidential data, and tracking of personnel to detect data tampering that may be fraud related. While there is no specific mention of passwords in SOX, section 404 deals with access management and the demand for greater internal controls:

- State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting

The aforementioned is the silent aspect of password compliance within SOX. It is not uncommon to find experts, and auditors making recommendations around character length and composition, as well as periodic password changes.

What about GDPR?

With the EU General Data Protection Regulation (GDPR) coming into full effect May 2018, all organizations collecting or processing data for individuals within the EU are in the midst of developing their compliance strategy. The new regulation carries an impact well beyond the European Union. A recent PwC pulse survey found that over half of US multi-nationals have GDPR readiness as their top data-protection priority.

Much to the disappointment of security teams and IT departments, the 88 page regulation leaves room for interpretation. It calls for reasonable levels of data protection, but doesn't define what that really means. The following are some common themes that appear throughout the document:

- Data protection by design and by default (Article 25): Security procedures from day one, both within and beyond technical solutions, consistently baked through your organization and its processes.
- Secure IT networks (Recital 49): Secure enough to resist accidental or unlawful events that may compromise confidentiality of data. At the very least, this means good security practices, especially for business systems housing sensitive data, such as Active Directory.
- Privacy Impact Assessment (Recital 76, and 84): Mitigate threats of a personal data breach via an objective assessment. The intention is to identify risks within projects, networks, and systems, and address vulnerabilities via the appropriate measures.

While there is no mention of passwords, the GDPR will require organizations to have the appropriate access policies in place. The execution is closely tied to password policies as it enables user administration within a system and organization. Complying with best practice standards, some of which are highlighted below, are a natural start.

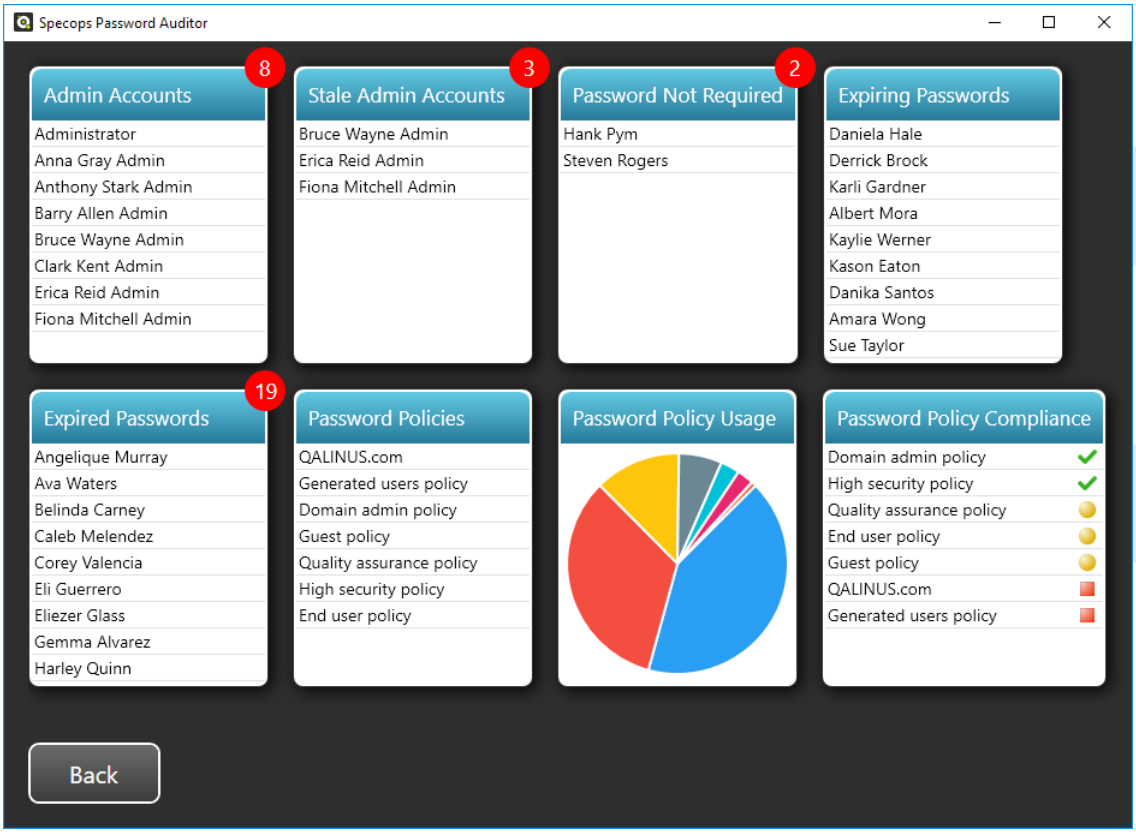
Future-proofing existing policies

With authorities such as NIST challenging the status quo, it may be time to re-evaluate existing password policies. If you are in an industry that abides by compliance policies, you are not required to act until the requirements catch up to new recommendations. That is not to say that you cannot take steps to strengthen passwords, while still meeting current standards. The following best practices can help you, regardless of the compliance requirements you are facing.

Password Audit

Start with a password audit. You can do this internally (with approval of course), or through an ethical hacking company. If you decide to go the DIY route, there are tons of free online tools at your disposal. These tools typically allow you to check the NTLM hash of passwords, stored in the Active Directory database, against the same lists available to hackers. If you want to take a more proactive approach, consider a password policy solution that enables banning dictionaries out-of-the-box.

Another free resource is Specops Password Auditor. The tool scans your Active Directory for weak password policies and displays interactive reports containing password-related information, such as policy usage, expirations, and relative strength. For each password policy, you can drill down and see how the settings compare to various industry standards, including NIST, PCI, and SANS. The tool also identifies other security vulnerabilities that may have slipped through the cracks, such as stale administrative accounts, or accounts that do not require passwords, as shown in the screenshot below. An added benefit is that the tool does not send any information outside of your environment.



Ban common passwords

As long as users continue using common/predictable passwords, dictionary attacks will continue to work. Attackers can use multiple dictionaries including foreign words, phonetic patterns, and lists from recent data breaches. With the right tools in place, such as Specops Password Policy, organizations can ban any dictionary list from being used in their organization. Specops Password Policy supports custom, online, and hash dictionaries in password creation for Active Directory. Additional settings allow you to block partial words, words in reverse, and their predictable compositions – this means not only blocking company name, but also its variations (i.e. Specops2017, Specops123!, IloveSpecops).

Turn on MFA

Use multi-factor authentication everywhere you can, especially for privileged users or when accessing critical systems such as a self-service password reset. Specops uReset enables users to authenticate with various identity services – ranging from identities they established themselves to ones that turn a smart phone into a high-trust identification device.

Expiration based on role

If you are considering what to do about password expirations, make sure you have the right tools in place. Multi-factor authentication mitigates the risk of a password that never expires. If you are not currently using multi-factor authentication, keep in mind the different roles in your organization. Periodic password changes may not be necessary for low-privileged users, but you may want it for your administrator accounts. The expiration frequency should vary across different user groups, and the password policies in place.

Final thoughts

With password security best practices in constant flux, our effectiveness in safeguarding our organization requires scrutiny. Unfortunately, the regulatory bodies we must abide by do not always pave a clear direction. This is where our own judgement must fill in the gaps. Putting demands on the authentication system shifts the burden away from users making poor choices. For example, using a dictionary list in your policy, specifically one that can be configured to include leaked lists, will help prevent the predictable pitfalls that users can't seem to avoid.

There is no "set it and forget it" when it comes to password policies. It is a continuous process that must respond to user behavioral patterns, and the emergence of new threats.