CONVERGE 360 SUMMARY REPORT

Redmond MAGAZINE

THE STATE OF PASSWORD SECURITY IN THE ENTERPRISE

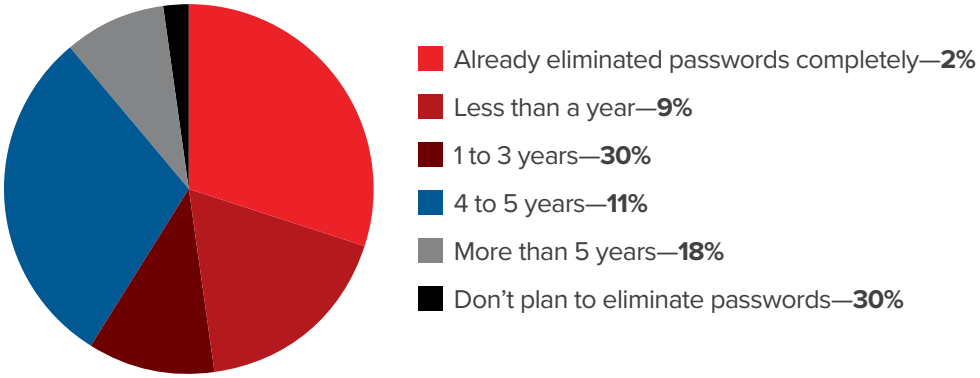
By Brien M. Posey

A recent Authentication Security Strategy survey by Enzoic and Redmond magazine revealed insights into the way that passwords are currently being used in various organizations, and what the future looks like regarding this ubiquitous authentication method.

PASSWORDS WILL BE AROUND FOR A LONG TIME

One of the study's key findings was that passwords aren't going away any time soon. The survey asked respondents how long they expect passwords to remain as one of the authentication methods used in their environments. Less than 2% of those surveyed indicated that they have already done away with password-based authentication, with an additional 9% saying that they would be phasing out password use within the next year. This means that nearly 90% of organizations plan to continue using passwords for at least a year or more and 60% for the at least the next 4 years. In fact, the study found 30% of those surveyed have no plans for moving away from passwords.

HOW LONG DO YOU EXPECT PASSWORDS TO REMAIN AS ONE OF THE AUTHENTICATION METHODS IN YOUR ENVIRONMENT?



OPINIONS ON PASSWORD EXPIRATION ARE STILL DEEPLY DIVIDED

In recent years, NIST, SANS, Microsoft, and others have begun recommending against the use of password-expiration policies. This recommendation is based on the idea that users are more likely to use weak passwords if they are required to change their passwords frequently. In spite of these recommendations, many organizations are reluctant to abandon their long-standing password-expiration policies.

In the study, only 53% of organizations indicated that they would either eliminate their password-expiration policy or substantially extend the expiration period so that passwords do not expire as frequently. In contrast, 47% of those surveyed indicated that they do not plan to make any changes to the policies.

HAVE YOU OR DO YOU EXPECT TO ELIMINATE OR SUBSTANTIALLY EXTEND PASSWORD EXPIRATION POLICY?

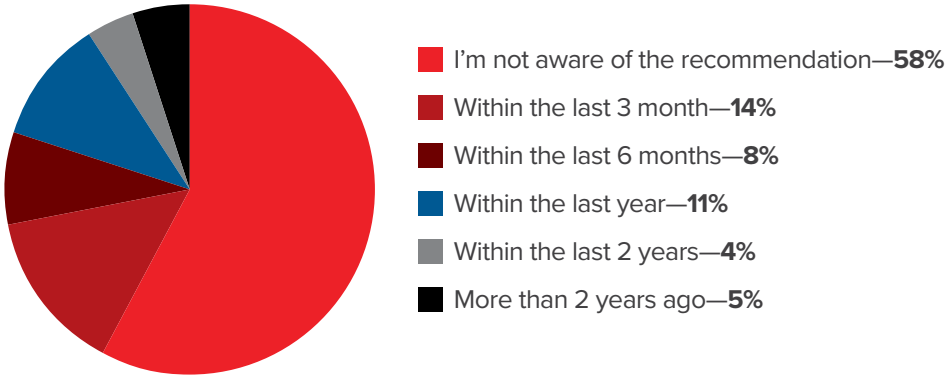
ORGANIZATIONS MAY BE UNAWARE OF EVOLVING PASSWORD BEST PRACTICES

For many years, password best practices mandated the use of password-complexity rules governing password-composition requirements. Such rules for example, might require users to create passwords consisting of a mixture of upper case letters, lower case letters, numbers, and special characters. More recently however, NIST has reversed course and begun recommending against the use of character-composition requirements for passwords. The main reason for this recommendation is that users will often attempt to circumvent the requirement by replacing letters with similar looking characters (a practice known as leetspeak). For example, a user might use "@" in place of the letter "a". The end result is weak passwords that are relatively easy to crack.

Rather than requiring the use of overly complex passwords, NIST recommends screening users' passwords against a list of passwords that are known to have been compromised. That way, organizations can prevent users from choosing a password that is already known to the hacker community.

Somewhat surprisingly, over half of the organizations surveyed (58%) were unaware of the NIST recommendation to replace password character composition policies with a blacklist-based approach. Another 14% of those surveyed had only become aware of the new recommendations within the last three months.

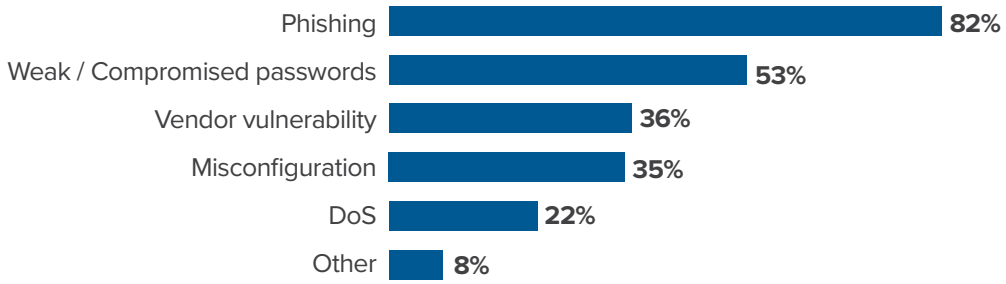
WHEN DID YOU BECOME AWARE OF THE RECOMMENDATION FROM NIST TO REPLACE PASSWORD CHARACTER COMPOSITION POLICY WITH A BLACKLIST-BASED APPROACH?



CYBERATTACKS REMAIN A TOP CONCERN

The survey asked respondents which types of cyberattack vectors they were most concerned about. The top concern, which was shared by 82% of respondents was phishing attacks. This was followed by over half indicating that they were concerned about the risks posed by weak or compromised passwords which are a frequent entry point for hackers.

WHICH OF THESE TYPES OF CYBERATTACK VECTORS ARE YOU MOST CONCERNED ABOUT?



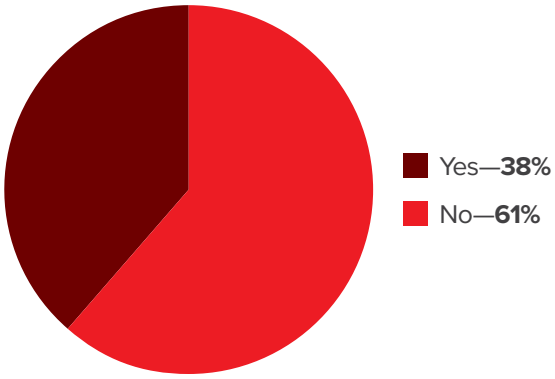
When taken together, these two results indicate that the top security concerns shared by survey respondents revolve around human error (users falling for phishing attacks or using a weak or compromised password).

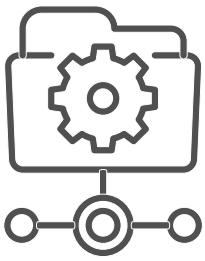
Other security concerns ranked lower among the results with roughly a third of respondents indicating that they were concerned about misconfigurations (35%) and vendor vulnerabilities (36%). Additionally, 22% of those surveyed were concerned about denial-of-service attacks.

ORGANIZATIONS LACK THE MEANS TO ADDRESS THEIR SECURITY CONCERNS

Those who responded to the survey are clearly concerned about the risks posed by weak or compromised passwords. The NIST recommendation to compare users' passwords against a blacklist of passwords that are known to have been compromised is an indication that NIST shares this concern. Even so, the survey found that only 38% of organizations actually have a way of determining whether their users' passwords have been compromised.

DO YOU HAVE A METHOD TO DETERMINE WHEN EXISTING PASSWORDS HAVE BEEN COMPROMISED?





Ideally, the solution that you adopt should integrate directly into your Active Directory environment, since the Active Directory is the mechanism that handles authentication for the entire organization.

This finding is completely understandable. Cross referencing user passwords against an always up-to-date blacklist is difficult. Such functionality is not integrated into the Windows operating system, meaning that those who want to use blacklist-based checking will need to adopt a third-party solution. It's no wonder that over 60% of organizations surveyed do not have a means of determining whether their users' passwords have been compromised.

ADDRESSING THE PROBLEM

Studies have shown that over 70% of users reuse their passwords. The reason why this is such a problem is because when data breaches occur, hackers compile lists of the passwords that have been obtained. The hackers know that any username and password combinations in the list are likely to have been used on other sites.

From an enterprise IT perspective, this means that users are likely using their work passwords on other websites. If one of those sites is breached, then your users' passwords may be exposed, making it far easier for a hacker to gain access to your organization.

The best way to avoid this problem is to adopt an authentication strategy that is not based on passwords, but this is not yet a realistic option for most organizations. Since passwords will remain a fixture in the enterprise for the foreseeable future, the best option is to adopt a third-party solution that compares your users' passwords against those that have been leaked to the dark web.

There are a number of tools available that can do this, but such tools vary in terms of their scope and capabilities. Ideally, the solution that you adopt should integrate directly into your Active Directory environment, since the Active Directory is the mechanism that handles authentication for the entire organization. Additionally, such a solution should be completely transparent so that there is no additional burden placed on end users.