SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

Why Passwords Don't Work

Bill Burr, the author of the NIST Password standards in 2003 (NIST SP 800-63), conceded in an interview with the Wall Street Journal in 2017, that the password paradigm he designed was a failure.

The requirements of; 8-20 characters; one uppercase letter; one lowercase letter; one special character; cannot match the username; cannot repeat passwords every x times; change the password every 30/60/90 days, etc., has not only failed to secure user environments, but led to practices that help assure that bad actors have access to the very systems and data that need to be secured.

Companies spend millions of dollars each year on identification and access management (ID&AM) programs, yet the return on these investments is, for all intents, zero. With sixty-one percent (61%) of all cyberattacks occurring as the result of employee action, or employee inaction, it is time to reexamine the entire approach to ID verification, validation and security.

Consider:

1) Almost 20% of corporate work areas in the business world have passwords written down in clear text somewhere in the work area.
2) One of the most frequent vectors of attack is the theft of credentials; usually via phishing ***(there is a great video circulating the web of a "news reporter" interview millennials about their password security, and the interviewer successfully gets the passwords for about ten people just by asking social questions)***
3) Passwords are hard to remember and everyone who uses passwords tends to use the same passwords or password methods over and over
4) Bad actors now have enough data on people's behavior to often accurately predict how people will structure their passwords and use that knowledge to breach multiple accounts tied to that user

During a recent CheckPoint Webinar on *2019 Cyber Security Threat Predictions*, the speaker told the story of how Apple employees in Ireland were being offered € 20,000, to sell their credentials to others. All the while, Forrester estimates the average cost of a password reset to be $70 and that across all industries, companies average 1.4 password resets (when NIST SP 800-63 is followed) per user per year. That accounts, per Gartner, for between 30% and 40% of helpdesk volume annually.

The situation is not that much better in organizations that fully implement a multi-factor authentication ("MFA") solution. MFA is fine, but when the weakest link in the password itself, even those environments are prone to be vulnerable.

Are there solutions?

Fortunately, there are. CAC, PIV, PIV-I are among the ID standards that support biometric verification and eliminate the need for passwords. These standards support:

- Logon authentication – including single sign on
- Physical access authentication
- Application authentication via APIs, SDKs and single sign on support

How does biometric work?

These biometric-based standards work on a two-factor authentication model. First, an employee is issued a card, the size of a credit card, with a gold chip embedded. The chip contains encoded information that matches the identity of the person whose photograph and name appear on the card. This encoded information is based upon a pre-defined set of standards including; fingerprints, background checks, retina scans, etc. Additionally, the chip holds critical certificates. Typically, the chip will have a digital signature certificate (used by email systems to certify that the sender is actually who they claim to be), and SHA-256 based encryption keys, used to encrypt and decrypt secured data.

These cards must be placed into a HID-Compliant reader that is either attached or built into the desktop/laptop/mobile device. The card is read by the system (whether a standalone system or a Windows Server based enterprise) and the use must enter a challenge key. The challenge key is either the card's PIN or a one-time use token sent to the user's registered device (such as a cell phone).

What happens if someone tries to hack the biometric?

The biometric standards have a "failed attempt" safety net. Typically, after five failed tries, the middleware that handles the biometric card will physically disable the card. At that point, even if the bad actor were to get access to the correct PIN or challenge key, the card will no longer work anywhere and access will be denied.

What are the costs to do biometric?

To do a soup to nuts implementation for biometric from both a logical access and physical access perspective will cost on the order of $300 per person upon purchase and $30 per person per year

thereafter for six years. At the same time, there are areas of large cost savings that emerge from moving away from passwords. On average, an organization will see a 42-month payback period and go cashflow positive before the end of the fourth year after purchase. And in those organizations with more complex ID&AM systems, the payback period will be shorter than that.

Are the any downsides?

The biggest downside is complacency. Going biometric is not a panacea and does not guarantee that you cannot be hacked. However, it does significantly reduce the chance of compromise from the business as usual ("BAU") scenario. Additionally, you will end up making changes to your organization. If you have a password audit team, they will need to be redeployed. Your helpdesk staffing levels will be able to drop by 30-40%. If you have a comprehensive password manager system and/or a self-service password reset system, they will have to be de-installed. And, if your employees lose or forget their biometric card, then they will be unable to work until they either get or replace their card. Guest access will be a thing of the past.

Conclusions

Passwords do not work, and the continued use of passwords in the corporate world is costing business billions and billions of dollars. It is time to try something that actually protects our critical infrastructure.

Knowledge and awareness are your best defense!
Please follow me on twitter: @stevewertheim