ICE/PSWD - Your z/OS Image Sentry

An Integrity Controls Environment (ICE) Application

The 2017 Data Breach Investigations Report* (DBIR) notes that 81% of hacking-related system breaches leveraged either stolen logon credentials and/or weak, sometimes even guessable, user passwords.

ICE/PSWD Answers the Challenge

With this shocking statistic in mind, we designed and developed ICE/PSWD to answer the password integrity challenge. Our goal is to provide a way forward for implementing the DBIR Best Practice recommendations, within the z/OS Mainframe Community.

The First DBIR Challenge – "Make people your first line of defense".

Using simple Parmlib constructs, ICE/PSWD makes it easy to adopt practices commonly experienced on the WWW when transacting with digital commerce sites/online services such as your bank and your entertainment sites. Namely, letting the user know (Email or TEXT) that their credentials (UserId and Password) are being used (or someone is attempting to use them) to access their online account(s).

Users defined to ICE/PSWD are notified of z/OS Logon attempts and, equally importantly, attempts to reset their password. This simple but absolutely critical enrichment of z/OS Security brings the user on board, including them in the z/OS Security Paradigm. No matter what your current perimeter defenses are, adding the user into the mix is a common sense best practice. We should remember that the user is the only person who will know for certain, at any point in time, if and how they are using their credentials.

The Second DBIR Challenge – "Encourage stronger passwords".

This is easy to say, but harder to do. The z/OS Security systems do support stronger password constructs in the form of syntax format rules but often don't get an opportunity to enforce them. It's possible to define more than one rule, some simple, some complex and some really complex. But, during a password reset, users only need to meet the requirements of the simplest rule and, therefore, the complex ones go unused.

Users defined to ICE/PSWD can be bound to one or more specific syntax rule(s) ensuring that users with privileged system access are bound to complex syntax rules and less privileged users enjoy, perhaps, something less complex. To ensure that users are not rushed into selecting a new password, notice of upcoming expirations can be sent days or even weeks in advance. This is intended to promote frequent password resets that meet the security requirements for a particular user group.

The Third DBIR Challenge – "Use multi-factor authentication".

There is no doubt, multi-factor authentication will add integrity to the strength of credentials used to access any system, including z/OS. But once you're in, you're in. If you've hacked in with a stolen credential, one of your first or last actions might be to reset the stolen password, thus preventing the rightful owner from gaining access. Now we know that ICE/PSWD has already notified you that your credential has been used to logon. So, what's next? Simply a complete defense of the password reset process as described on the reverse. Read on.

* Verizon's 2017 Data Breach Investigations Report

NewEra Software, Inc.

18625 Sutter Blvd., Suite 950 • Morgan Hill, CA 95037 • 800-421-5035 • 408-520-7100

www.newera.com • www.newera-info.com/Docs.html

Multi-Factor Authentication (MFA) is generally used to ensure that those individuals who are attempting to log on are in possession of additional materials - a secret code or a physical object that will, in addition to their otherwise valid logon credential, be used to authenticate their right to system access.

While ICE/PSWD has many of the attributes of MFA, it differs as follows: ICE/PSWD exploits the use of One-Time Passwords (OTP) and becomes operational only at the intercept point of an attempted password reset. MFA, on the other hand, is active for all logons BUT not at all active at the password reset intercept point during a logon. In addition, the MFA secret or object must be known to the user and thus possibly stolen or misappropriated. The OTP Value used by ICE/PSWD is unknown, is generated by the system, and is transmitted, via email or TEXT only, at the time of an attempted password reset. During this initial reset attempt, the desired new password is *not* actually reset. This action takes place only when the user returns to the originating system and enters the necessary OTP values.