HYPR Info Brief

Six Best Practices to Secure Authentication for Energy and Utilities

The clear and present cyberthreat to energy and utility companies has taken center stage with the recent CISA (Alert AA22-083A) and FBI warnings about Russia-based cyberattacks on the energy sector. Even before the warnings, however, the 2021 Colonial Pipeline hack underscored the dangers from cyber vulnerabilities in this critical industry. Tens of millions of dollars in losses and thousands of East Coast gas stations running dry, all because of one hacked password.

For those following security trends in the sector, the Colonial Pipeline attack came as no surprise. In 2019, a cyberattack on an unnamed U.S. utility company disrupted power grids in Utah, Wyoming and California. In a recent survey of global utilities by Siemens and the Ponemon Institute, 56% of respondents reported that, in the past 12 months, their organization experienced at least one attack that resulted in the loss of private data or an outage.

It's essential for energy and utilities to ensure their security controls are robust enough to withstand unauthorized attempts to access systems and networks. As part of our commitment to improving cybersecurity across all sectors, we'll look at the best practices for implementing secure authentication for energy and utility companies.

Best Practices to Secure Authentication for the Energy Sector

1. Embrace Zero Trust

In response to the major SolarWinds and Colonial Pipeline attacks, the administration issued the Executive Order on Improving the Nation's Cybersecurity. One of its primary focuses is that organizations critical to national infrastructure should abandon a "secure perimeter" defense in favor of a Zero Trust framework. The traditional concept of a well-defined perimeter no longer holds; today an enterprise is a fluid entity with cloud applications, mobile access, IoT devices and an increasingly distributed workforce creating multiple, shifting points of entry. Zero Trust presupposes that any user or device can be a threat, even if it was previously authenticated; therefore, access can never be automatically granted, and a principle of "never trust, always verify" should be adopted.

Zero Trust and Multi-Factor Authentication

Strong authentication forms the foundation of a Zero Trust architecture. Multi-factor authentication (MFA) requires someone to provide two or more independent verification methods — "something they know" (security question, PIN or a one-time password), "something they have" (i.e., a phone or other device) or "something they are" (i.e., a fingerprint or their face) — to prove their identity and gain access to a system. MFA makes it much more difficult (although not impossible) for hackers to impersonate someone else and should be considered a minimum baseline to secure authentication for energy and utilities. This is reiterated in the guidance contained in the March 24th CISA Alert A22-083A, titled "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector," which calls to "Enforce MFA to authenticate to a system."

|

2. Eliminate Shared Secrets from the Authentication Process

Multi-factor authentication itself cannot ensure secure authentication for energy companies. As previously noted with the Colonial Pipeline attack, a single compromised password, which an employee likely used elsewhere, led to the breach of the entire system. According to a recent survey, 82% of people reuse passwords over multiple accounts. Credential stuffing attacks have become inexpensive and trivial to execute. With breached passwords available en masse on the dark web, if one of the factors in MFA is a password, then your multi-factor is really single-factor authentication.

Moreover, any type of shared credential can be breached and exploited. OTP codes, security questions and centralized biometrics all can be compromised or intercepted during transmission. That's why it's critical to remove shared secrets entirely from the login flow. The 2021 Verizon Data Breach Investigations Report found that credentials are the target of 94% of breaches for energy and utility companies — higher than any other industry. If credentials are never shared or centrally stored then the biggest attack target is eliminated and phishing, push notification attacks and man-in-the-middle attacks fail.

3. Leverage Public Key Infrastructure

Authentication technologies based on public key infrastructure (PKI), also called asymmetric cryptography, use a private-public cryptographic key pair to authenticate a user's identity instead of the traditional system where a password or other identifiers are shared and verified. PKI ensures that even if a hacker breaches the servers of the service provider, they will be unable to hijack user accounts or access the sensitive information they store. With PKI, the private key is stored on the user device — a mobile phone, smart card or security key — while the public key is registered with the authenticating server. Such systems generally also incorporate additional verification factors, such as biometric recognition, local to the device. These are the technologies known as True Passwordless MFA. Secure authentication for energy and utilities can be greatly improved by deploying PKI-based passwordless MFA.

4. Make Your MFA Interoperable

Large, diverse workforces and complex, distributed and interconnected energy generator and provider systems pose unique challenges to secure authentication for energy and utility companies. A single utility may have thousands of employees, contractors and field maintenance teams requiring access from various devices to both legacy and modern cloud-based applications.

In such an environment, it's essential that any MFA solution implemented work interoperably across multiple operating systems and identity providers. Vendor lock-in to an identity provider causes delays and introduces future risk in terms of flexibility, scalability and compliance. It also deters innovation, which is just one reason why enterprises are choosing to decouple identity from authentication.

5. Follow Security Directives

Many energy providers and utilities are governed by the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) regulations. Among its requirements, CIP mandates strong user authentication controls at the entry points to electronic security perimeters. Moreover, the TSA recently issued a second security directive for Critical Pipeline Owners and Operators. The directive includes multiple specific cybersecurity measures including the use of MFA. Other government cybersecurity regulations, such as the OMB's guidance on the May 2021 Executive

Order and guidelines from the National Institute of Standards and Technology (NIST) provide more granular detail about acceptable methods of multi-factor authentication, specifically regarding resistance to phishing.

These directives also form the baseline for legal precedent and open the door for potential litigation if violations of secure authentication measures lead to security breaches. Insurance coverage and costs also come into play as many insurance companies now mandate that companies implement MFA and other best practices or risk voiding their policy.

6. Provide the Best User Experience

Make sure your authentication processes don't keep out the people you do want in. Methods that create too many obstacles will cut into your organization's productivity as well as make it less secure. People will avoid or resist adoption of authentication methods they find difficult or inconvenient. When possible, employ frictionless solutions that use processes and technologies familiar to your workforce. Ideally, a single action by the user initiates the multi-factor authentication flow.

In all cases, secure offline authentication must be an option so that workers don't need to turn to your helpdesk to gain access. Organizations can implement offline authentication via secure decentralized PINs, which ensure offline access doesn't entail any extra risk.

Ensure Secure Passwordless MFA with HYPR

The urgency to improve authentication security for energy and utility companies cannot be overstated. IBM's 2020 Cost of a Data Breach report put the estimated cost of a single data breach for energy and utility providers at $6.4 million, second only to healthcare. HYPR makes it easy to implement True Passwordless™MFA for organizations across all verticals. It turns an ordinary smartphone into a PKI-backed security key for frictionless authentication that means less hassle for your team, increases productivity, saves you money and — most importantly — a more secure authentication system for your workforce and applications.

To find out how HYPR can make your systems more secure, talk to our team or arrange a demo.