Focusing on the Future of Authentication

Weak and stolen passwords result in data breaches that cost businesses millions of dollars each year. Biometrics and multi-factor authentication (MFA) offer a stronger solution. And yet, hackers can still spoof fingerprints and voices. Take a look at the future of authentication and determine what options make the most sense for your organization.

Most experts agree that MFA provides a more secure environment for valuable data assets. With MFA, organizations require at least two verification methods to establish identity, instead of relying on passwords alone. For instance, authentication could include a password in conjunction with a fingerprint or verification text.

However, the extra steps can impede productivity and cause frustration. For instance, dirt can render fingerprints unreadable and that means rejection of authorized users. And it takes time to drag out the cell phone to locate and enter one-time passcodes. Users tend to resist adopting complicated authentication measures, leaving organizations vulnerable.

Consequently, the future of authentication must combine more effective security with improved user experience. No single technology will provide the silver bullet. More likely, the answer lies in strengthening existing verification methods in combination with emerging technology to reduce risk while creating a seamless environment for the user.

Risk-based Authentication

One option already in use involves adjusting the authentication requirements based on risk. For instance, an employee who accesses a given network regularly from the same device represents a low risk. In that case, the system might require just single-factor authentication, allowing the user access with minimal disruption.

On the other hand, if the system detects an access attempt from an unusual location or a new user, it will consider the action a high risk. It might deny access or ask for additional authentication. Most internet users have experienced a form of risk-based authentication when logging into a banking application on a new device, for instance.

Strengthen Biometrics with Anti-Spoofing

Biometrics have significantly improved security. However, the technology needs to evolve even further. For instance, with a high-quality voice recording or fingerprint mold, hackers can fool some voice and fingerprint recognition systems. Fortunately, researchers continue to improve biometric technology.

For example, security providers work to increase the security of fingerprint systems with increasingly sophisticated anti-spoofing measures. These tools determine with greater precision the "liveness" of the finger presented. Additional measures need to address other biometric modalities, such as palm scans and facial recognition.

Behavior-based Authentication

In the ideal future of authentication, verification will occur behind the scenes, almost without conscious user involvement. The benefits of this "frictionless authentication" include a seamless user experience. Additionally, reduced user involvement in the authentication process means reduced risk due to human vulnerability.

For example, with behavior-based authentication, the system weighs multiple factors to determine the level of access. Unusual access attempts or significant changes in bandwidth use would trigger an alarm, for instance. The system may also factor in keystroke dynamics, mouse movements and other biometric patterns.

Behavioral-based authentication involves machine learning, determining behavior patterns over time for individual users or devices. It also provides continuous authentication. That is, even if a user gains initial access, the system analyzes behavior throughout the session and makes adjustments, particularly in a high-risk environment.

Embrace the Future of Authentication

Organizations need to ensure the security of vital intellectual assets and customer information. At the same time, they seek to improve user experience and support productivity. With so many authentication options available to you, choosing the right approach can prove challenging.

The cyber security experts at eMazzanti understand your need to balance security with usability and budgetary constraints. We can help your organization choose and implement the authentication methods that best meet your business needs.