Enhanced authentication

Enhancing user authentication in this new environment.

April 2020

The rapid spread of COVID-19 has had a significant impact on organizations around the world, but they have found ways to minimize disruption by moving to a remote workforce model. Enabling a remote or cloud based work environment requires organizations to enhance how they authenticate users.

Enhancing user authentication

Cybercriminals are exploiting COVID-19 to launch cyberattacks, with a signficiant increase in phishing and account compromise attacks. While companies have moved to a remote workforce, along with leveraging cloud solutions, to enable their people to continue working, there is a risk they are opening up access to their most valuable assets. If it's easier for an employee to access, it could make life easier for an attacker.

Potential risks and challenges of weak authentication

Enabling remote access to critical assets and moving services to the cloud increases the threat landscape and opens opportunities for an attacker to gain access.

- The existing password policy and authentication approach may be a fit for on-premise use, may not be appropriate in a remote, cloud-based environment.
- Cloud services are being leveraged like never before and may not have been integrated with the organization's existing authentication approaches.
- Allowing the use of personal devices, whether through a formal "Bring Your Own Device" approach, or informally to encourage user productivity, increases the attack surface and authentication challenge with potentially insecure devices.

Upgrade your password policy

As a tactical goal, companies should focus on strengthening their current authentication controls, particularly around their password policy. For example, companies that are heavily dependent on password-based authentication should re-assess their password policy, including those recommended by the NIST *Special Publication 800-63B Digital Identity Guidelines.* Increasing password complexity to enforce excessively long or complex memorized secrets is less likely to be memorable, and it is more likely that they will be written down or stored electronically in an unsafe manner. Also, keystroke logging, phishing, and social engineering attacks are equally effective on lengthy, complex passwords as simple ones. Organizations should consider updating the policy to include:

- Passwords must be at least 8 characters long if chosen by the user, or 6 if chosen randomly by credential service provider;
- Use password dictionaries to check against "black list" of unacceptable passwords;
- Limit the number of failed authentication attempts; and
- Force password changes if there is evidence of compromise of authenticator.

Black lists, hashed storage and rate-limiting access attempts are more effective at preventing modern brute-force attacks. Perhaps the greatest danger to enterprise security is the continued belief that passwords are an effective method of determining user identities. Passwords are susceptible to multiple forms of attack, hence we recommend expediting the journey to enhanced user authentication methods.

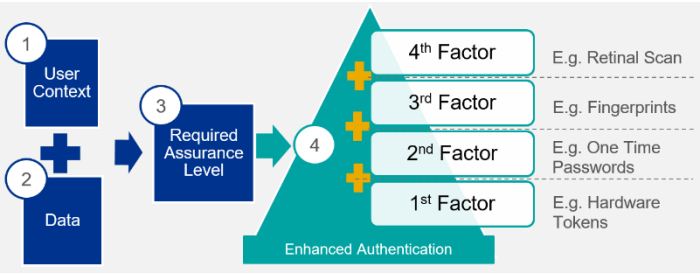
Enhanced authentication

Although organizations have defined policies requiring strong passwords and password controls, industry research has found that users continue to re-use passwords across multiple accounts. This increases the risk that a password compromise will affect all the user's accounts.

Organizations should align the user authentication method, whether through the use of one-time passwords sent to their mobile device, tokens on registered devices or leveraging password-less solutions, against the context and sensitivity of the data being accessed. This approach aligns the level of protection with the data and aims to ensure only the most relevant people can access and leverage the data.

User context in which information or access request is submitted can be determined based on various factors such as geographic location, IP address, device used, and function. Sensitivity of data can be determined based on a company's information classification scheme aligned with crown jewels.

It takes authentication to the next level by including multiple factors of authentication, as noted in the figure below.



Key advantages of enhanced authentication

- Improves productivity by asking for additional authentication information based on the sensitivity of the data being protected;
- Lowers customer friction, improving the ease of use and simplifying the authentication experience;
- Allows for better protection against phishing and account takeover attacks; and
- Focuses the controls on those systems with the most sensitive data, reducing the 'one-size fits all' approach to implementing security.

We can help to define an appropriate journey for enhanced authentication to better respond to current and future workplace needs while improving security effectiveness and optimizing efforts and related costs.

To determine a future proof journey, we help organizations re-assess their existing access management and authentication controls, develop a risk-based roadmap and help to implement and enforce these controls.

Our approach involves working to immediately enhance existing access management and authentication policies, standards and controls, and to minimize the end user impact and business disruption. This is done through the following:

- Update and immediately implement stronger password policies;
- Define and implement dictionarybased black lists and rate limiting controls;
- Integrate current on-premise and cloud-based solutions into a single authentication approach;
- Prioritize those applications and systems with the most sensitive data for enhanced authentication techniques; and
- Identify additional user context, such as function, location or device, which should be used to drive enhanced authentication controls.

Working shoulder-to-shoulder with you, KPMG can help you to identify and quickly navigate the path forward. KPMG can help you work through strategy and governance, organization transformation and implement solutions to strengthen your current authentication posture.

Contact us

Hartaj Nijjar
Partner & National Leader,
Cyber Security
416 228 7007
hnijjar@kpmg.ca

John Heaton
Partner,
Cyber Security
416 476 2758
johnheaton@kpmg.ca