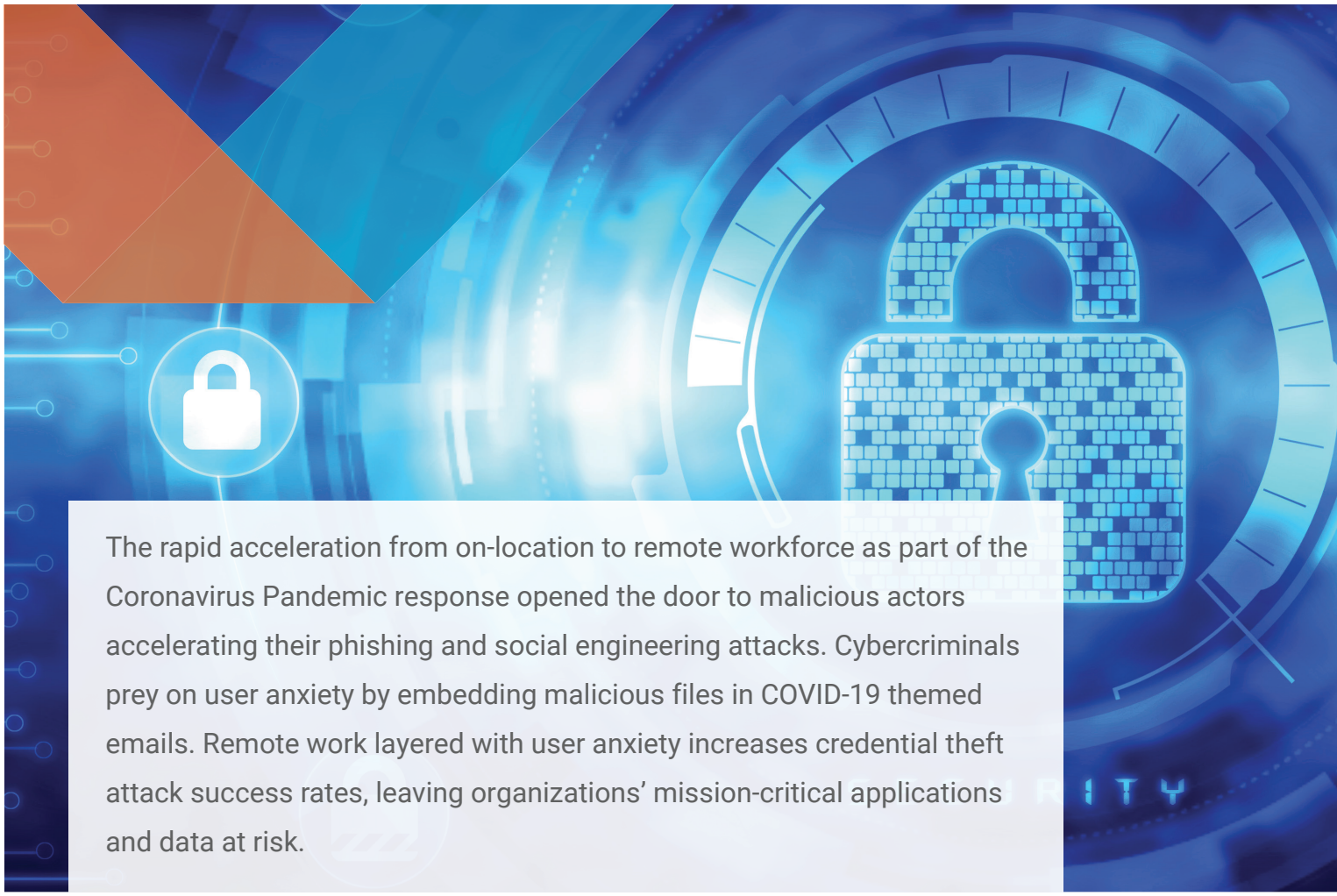
APPSIAN

EXECUTIVE BRIEF

Protecting Remote Users From the Latest Barrage of Social Engineering Attacks

Piyush Pandey • CEO



The rapid acceleration from on-location to remote workforce as part of the Coronavirus Pandemic response opened the door to malicious actors accelerating their phishing and social engineering attacks. Cybercriminals prey on user anxiety by embedding malicious files in COVID-19 themed emails. Remote work layered with user anxiety increases credential theft attack success rates, leaving organizations' mission-critical applications and data at risk.

Start with Identity and Zero Trust

For years, security professionals have said that the perimeter is shifting away from traditional controls like firewalls and focusing on enforcing user access. As many organizations shift to fully remote. The Coronavirus shift toward a fully remote workforce for many organizations heightens the urgency over maintaining access governance controls that protect information.

Many organizations moved from partial remote workforce to fully remote workforce in the span of a week, or in some cases nearly overnight. This means more devices accessing an organization's systems and software, but many without the required firewall protections or forced security patch updates done on-premises. Any one of those devices, if compromised by malware, can lead to a system-wide attack.

To rapidly accelerate security, organizations need to find a way to move towards a Zero Trust model, one that verifies and never trusts. This means knowing all the devices, users, applications, and data across the organization. Then, working towards creating the appropriate controls for each of those categories.

For organizations that have a matured cybersecurity posture, identifying people, hardware, and data may be faster since that information is already contained within risk assessments. To accelerate a Zero Trust strategy, organizations can leverage current identity and access controls and add context such as location, time of day, and application to limit user activity. By doing this, organizations can limit the impact of malware installed as part of a social engineering attack.

Embrace Adaptive Multi-Factor Authentication (MFA)

After setting contextual controls, organizations using adaptive MFA can apply those controls to modules within applications. MFA acts as the key that unlocks access to applications, but even within that access, organizations need to provide additional layers of access protection.

Organizations can use context, such as time of day or location, to trigger inter-application MFA. For example, if a user is trying to access a payroll module within an application from an anomalous location, adaptive MFA uses that context and requires the user to provide additional authentication information to prove their identity. By forcing this additional authentication, the adaptive MFA ensures that the user is who they say they are, rather than implicitly trusting the user.

This additional level of access security prevents malicious actors from leveraging stolen credentials throughout the organization's Software-as-a-Service (SaaS) application. Cybercriminals may be able to gain entrance to the application itself, but the additional layer of security around sensitive data and applications that comes from using adaptive MFA means that the organization is adding another "gate" that needs to be unlocked, thus protecting the information by restricting abnormal access.

Incorporate Data Masking

Organizations often assume that encryption acts as an unfailing security technology. An incorrect implementation or attacker who can crack the algorithm puts the data at risk.

Incorporating data masking by applying contextual controls to what information is visible to a user acts as another layer of defense against stolen credential use. For example, assume a remote worker lives on the west coast of the United States. Incorporating geolocation as part of the user's access and data visibility would give the user access and visibility into sensitive information as long as the person is in that geographic location. Applying data masking based on geographic location protects sensitive data even if a cyber attacker gains entrance to an application by making the sensitive data "invisible" to them. If a cybercriminal on the east coast of the United States gains entrance to the application with stolen credentials, then the cybercriminal would have access but not visibility to the information.

Many organizations may consider data masking a way to "protect from over-the-shoulder" risk when users are in public locations. However, even with the workforce nearly fully remote as a social distancing strategy, data masking can provide a much-needed additional level of defense.

Appsian Provides Defense in Depth at the Identity Perimeter

As organizations look to protect data from social engineering attacks, they need solutions that help protect the Identity perimeter. Adding additional layers of security at the network level may no longer work as more companies turn to remote work either as a preventative Coronavirus measure or in the longer term, to cut costs.

Appsian's suite of solutions enables organizations to accelerate their identity and access defense in depth strategies and secure their mission-critical ERP applications. Appsian delivers the control and visibility that traditional ERP applications like PeopleSoft and SAP (ECC or S4) inherently lack. With our Security Platform, organizations can create contextual access policies and fine-grained data security controls then monitor user access as a way to detect potential credential theft.

For more information about how Appsian can increase security at your identity perimeter, contact us today or schedule a demo.

This article was originally published at TechSpective.

Written by

Piyush Pandey, CEO at Appsian is a technology executive with 18 years of global experience in strategy, sales, mergers & acquisitions, and operations within software companies. Over the last 10 years, he has worked with enterprise software companies including Oracle, Epicor, Concur, Citrix and Microsoft on various transactions. He has held various leadership positions at Procera, Deutsche Bank, Stifel, Wipro Technologies and a wireless startup.

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com

www.appsian.com