APPSIAN

EXECUTIVE BRIEF

Access Governance is Critical for Preventing Phishing Attacks

Piyush Pandey • CEO

The news is flooded with stories about cybercriminals successfully engaging in phishing and social engineering aimed at exploiting people's COVID-19 fears, all in order to steal user credentials to business applications and VPNs. From fake delivery notifications to World Health Organization (WHO) impersonations, malicious actors are preying on people's emotions during this pandemic.

The credentials used for authentication are ultimately an organization's network perimeter. This puts organizations in a difficult position — they can limit employee's access to these systems and risk negative impacts on productivity and business continuity, or they could bury their head in the sand and hope nothing bad happens. Many are choosing the latter, and the implications are being felt worldwide.

Why There is a Correlation Between a Stressful Environment and Cyber Attack Volume

Social engineering fundamentally relies on taking advantage of strong emotions to trick people into taking actions that can cause them harm. This crisis has emotions running high, and many employees are stuck in a state of fight or flight.

Research shows that stress impairs the brain's ability to make decisions. That's why, when people are under stress, they often take more risks and engage in activities that could cause them harm. In other words, employees are not forgetting their phishing trainings, their brains are functionally incapable of making good decisions.

Cybercriminals rely on emotional responses — whether it's clicking on links, downloading documents, or opening attachments — emotionally charged content (e.g., fake layoff announcement email with a malware attachment) is more likely to result in a successful attack

The problem isn't the people, it's the cybercriminals and the tactics they use.

The Principle of Least Privilege

Often, companies view data protection solely from the compliance and financial risk perspective. Unfortunately, this doesn't go nearly far enough. It is recommended that companies consider limiting user access to resources based on the principle of least privilege, or the absolute minimum access necessary to complete a job function. Least privilege is a governance strategy that has never been more relevant than today — especially as organizations rely on remote workforces. Fundamentally, when users have more access than necessary, they may accidentally (or intentionally) violate compliance requirements designed to protect the organization.

Today, access governance is largely dictated by predetermined roles and permissions usually classified into groups (administrator, power user, etc.) This classification of permissions is tied to authentication processes like username / password security models that are heavily targeted by cybercriminals through phishing and social engineering. Further, if a phishing attack compromises a user's credentials, then the cybercriminal may access or acquire as much sensitive data as their victim's role will allow. This is precisely were least privilege should kick in.

The rise of phishing attacks that target coronavirus fears not only places organizational data at risk, but it also places employees at risk — especially those with high privileges. Many employees use the same credentials for multiple applications, such as social media networks and shared cloud drives. If one set of credentials is compromised, multiple systems are now at risk.

Limiting access to data according to the principle of least privilege provides organizations with the tools necessary to prevent catastrophic data breaches. A good question to ask yourself is, what data should my administrators and power users have access to? Do they need easy access to executive payroll data? Do they need easy access to other employee social security numbers? What do they really need easy access to in order to do their job?

The truth is, they will likely need access to some sensitive data, so how do you protect data that still falls under the principal of least privilege?

Zero Trust

"Zero trust" often sounds harsh — trust no one, assume a threat at all access points, and never grant access by default (e.g., a predetermined role and privilege.) At first glance, this mentality appears to go against corporate values like collaboration and integrity, but, in reality, it fosters them.

Moving toward an IT culture based on zero trust means that an organization can identify all devices, users, applications, and data across its ecosystem. Then, the organization can establish the appropriate controls that limit access where appropriate.

Fundamentally, a zero trust model encourages collaboration and integrity while also supporting employees who mean well but could be making risky decisions while under stress — coronavirus related or otherwise. By setting zero trust identity and access controls, organizations ensure constant alignment between who an employee is and what they have access to, thus, mitigating risk.

Protecting Workforce Health While Maintaining Data Health

As organizations face the distinct possibility of the Coronavirus requiring nearly all workforce members to do their jobs remotely, balancing data health and employee health becomes a concern. Fortunately, today's advanced technologies provide a variety of solutions.

The Coronavirus may be acting as a catalyst for organizations to change their approach to managing user access to sensitive information. Unfortunately, many companies that once required employees to work on-premise when they manage sensitive data are having to reconsider policies and scramble to maintain business continuity.

Multi-Factor Authentication

Part of establishing an effective zero trust model involves finding solutions that allow organizations to apply contextual attributes when granting access. Attribute-based controls adapt to different contexts and ultimately drive how and when users can access information. For example, an attribute might be geolocation or time of day. Adaptive multi-factor authentication (MFA) takes these attributes and requires additional authentication as users move across systems or within applications. For example, to log into an ERP system, passing a standard authentication challenge is required. Then, to update direct deposit or access payroll information, an adaptive MFA challenge should be deployed. Zero trust means that just because they passed through the front door of the application, they can't execute the most sensitive transactions.

As employees work remotely, organizations may want to incorporate adaptive MFA so employees in finance or human resources can securely authenticate to their ERP systems. Adaptive MFA will detect anomalous locations or times for activity, trigger an additional authentication process, and prevent malicious actor access.

Ultimately, zero trust and adaptive MFA protect the organization, the person whose information was almost leaked, and the employee whose credentials were stolen. The organization can be alerted to the cyber criminal's attempt to gain entry to its networks, the person whose data was almost leaked retains privacy, and the employee whose credentials were phished is protected from the negative impact of their privilege being hijacked.

Remote Access Means Phishing and Phishing Requires Additional Strategies

Organizations have tried to protect themselves from phishing attacks for years. What they have not done is protect themselves during a time of social, emotional, and physical upheaval. But, the current upward trend in phishing attacks should come as no surprise to organizations. Cybercriminals never rest — they take advantage of any weaknesses in an IT ecosystem, both digital and human.

Maintaining strong identity and access governance strategies ensures that both data and end-users can be protected during these strange and unusual times.

This article was originally published by Mission Critical Magazine.

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