Whitepaper

sms|passcode

THE NEXT GENERATION OF CLOUD SECURITY: BEST PRACTICES FOR FENDING OFF HACKERS IN REMOTE ACCESS

EXECUTIVE SUMMARY:

With the rise in popularity of cloud services has come a wave of new malware threats aimed at compromising the identities of users attempting to access information remotely. Organizations are advised to carefully consider the level of security provided by the cloud service provider before proceeding with a contract. With the number of security breaches today, it is not enough to employ simple user names and passwords to protect vital information in the cloud. Cloud providers should look to offer security solutions for the end-user or organization utilizing the cloud, including services that ensure that end-users can use the solution in an effective and secure way.

By offering adaptive, flexible and strong multi-factor authentication for cloud access, SMS PASSCODE is the trusted partner for organizations interested in securing remote access to cloud services.

PROTECT AGAINST THE STORM

Cloud services have become massively popular, as a growing number of organizations enable remote access to resources like applications and data that are stored offsite. With this significant increase in remote access comes a new challenge in ensuring security and compliance by authenticating the identities of users accessing these resources. The timing could not be more critical. In a 2013 study, a research firm discovered that the number of identity fraud victims increased by 1 million over the previous year, with the cost of these breaches jumping to $21 billion.

$21 BILLION

COST OF IDENTITY FRAUD IN 2013

While malware and hacking attacks have evolved to take advantage of the new ways that users are accessing data, old traditional methods like usernames and passwords still enjoy broad usage, even as they fail to provide the comprehensive security needed to protect against the current threats – the Zeus virus, also known as Trojan.Zbot – is a perfect example of one of these current threats. In a typical Zeus attack, the malware hijacks the users' credentials entered – including the token code – and sends these credentials to the hacker via instant message so the hacker can log in with the credentials instead. Meanwhile, the user is none the wiser that the "secure" access he thought he was using wasn't that secure after all.

To protect against modern threats like these, SMS PASSCODE is exploring a new way of thinking about securing access to remote services and cloud-based applications.

THE VIEW FROM THE CLOUD

Storing data offsite in huge, third-party data centers, known colloquially as the 'cloud,' has introduced new economies of scale for organizations that lack the resources to store this level of data in-house. Yet many businesses continue to struggle with securing remote access to data as security risks evolve.

Today, more and more end-users are granted access to cloud-based solutions like Microsoft Office 365, Salesforce, Google Apps and other business applications. Some cloud solutions offer generic security measures for authenticating users accessing these systems in the cloud, giving the end-user the responsibility of choosing which type of security to use, and relying on personal judgment to determine the security is strong enough to protect access effectively. To mitigate these concerns, SMS PASSCODE delivers adaptive multifactor authentication that is custom-designed for securing access to remote services.

TAKE RESPONSIBILITY FOR CLOUD SECURITY

Data protected by usernames and passwords is at the mercy of threats like brute-force attacks, phishing or simply outright identity theft. It has become increasingly obvious that usernames and passwords are ineffective ways of authenticating access, yet their use is still widespread as users balk at more cumbersome forms of authentication like tokens and certificates.

While the effectiveness of simple user names and passwords has collapsed, the amount of data stored in the cloud and systems offered continues to escalate. Cloud providers must accommodate access to millions of users from all over the world. A centralized breach in a cloud-based solution would pose a serious risk to the data of thousands – if not more – organizations. Therefore, it is the responsibility of the cloud provider to ensure strong, flexible security that is extremely hard to compromise, yet is easy for the end-user to use.

AIM FOR TOTAL SECURITY

As higher security for cloud access becomes more of a necessity, organizations are beginning to implement standards for authenticating users. One of the major problems organizations face is how to handle user identities in the cloud. Often it means that IT departments must maintain an additional set of user credentials for each and every cloud solution used by their employees. This approach requires cumbersome procedures and extra work for IT. To bypass this problem, IT should use a centralized method that gives each user a single identity that provides access to a variety of different cloud solutions.

Using an approach that provides strong authentication while simultaneously freeing end-users from being dependent on specific software, hardware or features ensures that users accessing company assets are qualified ahead of time.

BEST PRACTICE: USE SAML

One such option is Security Assertion Markup Language, or SAML. A SAML setup requires three roles: the end-user, the service provider and the identity provider. The service provider role is held by cloud solutions, such as Microsoft Office 365, Salesforce or Google Apps. The identity provider role handles user authentication and identity management for the service provider. The identity provider in this scenario can be used as a centralized system to handle authentication and identity management for multiple service providers at once. By utilizing a SAML identity provider, organizations can gain all the recognized benefits that are traditionally associated with on-premise authentication solutions.

From the organization's point of view, using SAML is a time saver, since it frees the organization from having to maintain multiple instances of user credentials; one in the local area network (LAN) and multiple in the cloud. This way, the organization can keep its authentication and security mechanisms the same for all users, regardless of whether they are accessing data from the cloud or from the LAN, thus saving time and money while boosting security.

By offering adaptive, flexible and strong multi-factor authentication for cloud access, SMS PASSCODE is the trusted partner for organizations interested in securing remote access to cloud services.

ABOUT SMS PASSCODE

SMS PASSCODE is a technology leader in adaptive multi-factor authentication, improving enterprise security and productivity by delivering an easy to use and intelligent solution that helps ensure the safety of corporate networks and applications.

SMS PASSCODE authenticates users through their mobile devices, helping IT managers address evolving business needs with cloud applications and mobile security by dynamically authenticating users based on geo-location and login behavior patterns.

The solution secures remote access systems including Microsoft, Citrix, Cisco and Checkpoint.

Governments, telcos, enterprises and financial institutions in more than 40 countries appreciate its cost-effective, secure and easy-to-maintain offering, making SMS PASSCODE their trusted partner to securely authenticate access to services while preventing identity theft.

For more information, visit www.smspasscode.com

www.smspasscode.com

sms | passcode
adaptive user authentication