celestix

WHITEPAPER

How to reduce the cost and complexity of two factor authentication

Published September 2012

48% of small and medium sized businesses consistently cite technical complexity and cost of ownership as the two biggest obstacles to deploying two-factor authentication technology.

Introduction

A recent authentication survey commissioned by Celestix found almost half of all organizations cited complexity as a major impediment when deploying two-factor authentication. Cost was the second largest response with both the cost of deployment and on-going management identified as issues with many traditional authentication solutions.

How can organizations benefit from two-factor authentication while at the same time keeping costs and complexity at a minimum? This white paper explores what makes two-factor authentication complex and costly while making recommendations on what a business should look for in an authentication solution.

The issue of security

Identity theft is a widely understood issue and most people are aware that the theft of personal credentials can result in network breach in which a loss of data is the end result. The loss of corporate confidential data is the primary impact but the remediation of such a breach can be costly also. Affected organisations typically have to deal with;

- Loss of business
- Loss of customer/stakeholder confidence
- Loss of competitive advantage
- The risk of financial penalties levied by regulatory bodies.

Static passwords, just how effective are they?

- In July 2012, hackers stole 500,000 unencrypted users' passwords from a Yahoo! Website.
- In June 2012, hackers stole 6.5 million users' passwords from Linkedin. Again, the passwords were not encrypted.

Most organizations rely on the use of a username and password to authenticate users before access is granted to secure critical information assets. This method is particularly prevalent in small and medium businesses where cost and complexity prevent the use of more secure options for login.

Static passwords represent the single biggest security risk to all organizations because they offer little or no protection against a determined fraudster. Social engineering, phishing, keystroke logging, network sniffing, shoulder surfing, are all included in the list of exploits that can be used to obtain a static password.

Phishing attacks often hog the limelight when it comes to identity theft in the news. Certainly such attacks claim their fair share of victims and protection against phishing is essential.

However, one of the reasons that identity theft is such a great threat to organizations is the sheer diversity of ways in which an identity can be compromised. Many such cases are a result of user negligence as opposed to malicious intent. Every laptop that is lost or left at an airport, every PC with a Post-it note listing passwords on it, and every time a password is used for multiple systems, there is a risk of exposure that must be considered.

Impact of third-party breaches on an organization

Many organizations express little concern about the high profile identity theft from consumer style companies such as Sony, eHarmony and LinkedIn. The reason for such a lackadaisical attitude stems from the incorrect belief that those breaches don't affect the organization. But what if a trusted employee happens to use the same password for system

log in as they do for some of these commercial sites?

Even if an organization's information systems are impervious to hacking, the replication of a static password on other sites leaves an organization vulnerable.

Estimating the cost of a security breach is hard to quantify although a recent survey by Symantec stated the cost to companies of $500,000 to address in terms of compensation, business disruption, revenue loss and other expenses. [1]

What makes two-factor authentication costly and complicated?

Two-factor authentication is a fundamental weapon in the fight against the cybercriminal. However, there is a widespread perception that such solutions can be complex and expensive to procure, provision and manage. There are many factors that affect the cost of two factor authentication solutions and organizations should consider all factors, not just the upfront cost of product.

Existing IT Environment

Most organizations will have heterogeneous IT environments that have evolved over time and to meet certain business requirements. The rise in cloud computing and outsourced IT has further complicated the IT landscape. An authentication solution not only needs to integrate with a variety of remote access and network-based access technologies but also be flexible enough to meet the increasing demands for securely publishing applications in cloud, hosted and on premise scenarios.

Another, often overlooked, consideration is how an authentication solution will integrate with an organization's existing directory service. Many traditional solutions require manual synchronization of users with corporate Active Directory and this manual task can take a great deal of time to complete. Solutions that include automated Active Directory synchronisation will save time and cost when deploying and amending the user numbers.

Token Management

Traditional two-factor authentication solutions rely on the use of physical hardware tokens as the form factor for generating a dynamic One Time Password (OTP). The management overhead associated with administering and supporting such tokens can be very high because tokens not only have an inherent cost to procure, they also need to be issued securely to workers who, by definition, are working remotely. This introduces a cost of provisioning that must be factored into any budget for deployment of such a solution. The provisioning process can lead to frustrating, time consuming and costly works being required.

Provisioning a hardware token to a remote worker first involves setting the user up in a repository. Next, the token must be assigned to the user and finally it must be despatched. The despatch process will likely involve the use of a secured transit such as courier or registered mail service. This process could take an average of two hours and the transit service alone could cost up to $50 per user, doubling the cost of the hardware token itself.

Hardware tokens contain a battery so every time a battery dies the token must be replaced, which results in the provisioning process taking place and incremental costs being incurred. In the event of a token being damaged or lost this will also require the provisioning of a new token to the user.

The issue of lost tokens is considerable. Surveys indicate that an organization with 600 users would typically expect up to 10 tokens lost per month, equating to 1.67% of the install base. If the hardware token costs $50 and it costs an additional $50 to despatch the token then the cost of handling lost tokens alone can add a cost of $1000 per month which should also be factored in to any solution costs.

Helpdesk Costs

Surveys indicate that on average a traditional two-factor authentication system can generate two helpdesk calls per day. Typically these would be from remote users who have questions relating to the use of their hardware token. User education is a serious consideration. Many users call in to question why they have received a token, what do they do with it, and why should they use it.

Then there are the more serious issues of users being unable to authenticate because they have lost their token, or de-synchronised their tokens.

Two-factor authentication is an enabling solution so ease of use should be considered very carefully. Adding technology that complicates a process or is at odds with the way in which users interface with their corporate resources may result in increases in helpdesk costs and cost.

Organizations reviewing two-factor authentication may want to consider the benefits of self-provisioning as part of the solutions they evaluate. Enabling the user to carry out basic account profile management such as PIN reset should lower the number of inbound helpdesk calls.

On-going Management and Reporting

The time involved in the management of any technology should always be considered when making an initial investment. Proprietary systems often require a process of education before an administrator can effectively manage the system. Many solutions focus so greatly on the core functionality of the product that they neglect the usability of the system.

Proprietary systems are not always intuitive and it can often take time for the administrator to orientate themselves with the system. Complexity results in incremental cost if professional services are required to aid installation and orientation.

Features such as contextual help and comprehensive documentation will help both administrator and user when trying to get to grips with an authentication solution.

With the continued need to comply with data handling regulations, reporting has become a significant concern for all organizations. Solutions that do not include simple and effective reporting may cause the administrator to customise reports which will take time and effort to manage.

Comprehensive reporting on the key performance of the authentication system is essential to make effective decisions on the authentication polices and also to justify the authentication solution to the organization's management. Graphical representation of data in charts and graphs that can be generated in minutes and exported for further analysis allows a business to meet compliance and regularly requirements.

Two-factor authentication solutions that provide an intuitive interface, pre-canned and customizable reports, self-provisioning portals and incorporated contextual help should lower the overheads of deployment and on-going management.

User Adoption

User adoption is an important consideration that has become increasingly relevant as IT continues on the path to consumerization. The emphasis now is more about how to provide simple, easy to use systems for users. Any solution that introduces complexity is likely to be rejected from mainstream IT users.

Two factor authentication solutions address this challenge with the option to provide soft tokens, on-screen keyboards, and in some case the delivery of One Time Passwords via SMS delivery. Such solutions remove the need to carry an additional hardware token form factor but more importantly they allow the user to use tools they are already familiar with such as apps and SMS. As a result the user adoption rate is far higher.

The Combatting cost and complexity

Many organizations believe they are too small or not of sufficient worth to be a target but opportunity makes a thief and lost laptops, static passwords and indiscriminate phishing attacks are aimed at anyone.

The continued increase in regulatory compliance should also not be understated. Compliance can apply to businesses of any size and the results of non-compliance can be as significant as the cost of a data breach.

One method of deploying two-factor authentication while lowering the cost and complexity is to consider the latest trends in this marketplace. After many years of providing a limited range of form factors, suppliers in this market have begun to deliver new and innovative solutions to meet the needs of a much broader range of organizations.

Tokenless Form factor

One such trend that promises to both lower the financial barriers and simplify the provisioning and management process is the use of "tokenless two factor authentication". Tokenless methods typically provide a soft token that can be run on a smart device, or they can deliver a One Time Password via SMS to a mobile device.

Easier User Provisioning

User provisioning is often much faster and easier when no hardware token is involved and this should reduce the initial costs of deployment and roll out. On-going costs can also decrease due to the fact that with no hardware token there is no need to renew and replace lost, damaged or expired tokens.

User adoption and satisfaction is typically higher when soft token solutions are deployed because the user no longer needs to carry an additional token for use when logging on. Users are typically more familiar with smart devices and they are comfortable with downloading apps and using them on a daily basis.

Contact

USA +1 (510) 668-0700
UK +44 (0) 1189 596198
Singapore +65 6781 0700
Japan +81 (0) 3-5210-2991

www.celestix.com
info@celestix.com

OTPs on smartphones

This familiarity with form factor of smartphones (for generating OTPs) has other benefits. Users are very sensitive to the whereabouts of their cell phone or smart device and so any loss or damage is often noticed and rectified promptly. Devices are easy to back up and restore if found or replaced, allowing the user to get back to work quickly. Compare this to the process required to provision new hardware tokens to users and the cost differential is significant.

Helpdesk costs should also decrease due to the simplified nature of soft tokens and SMS in particular.

Summary

Traditional approaches to authentication involve considerable investment both in upfront cost and also on-going costs of management. They also require regular involvement from an experienced IT administrator.

Token less authentication solutions can provide compelling cost savings and lower the complexity and on-going costs because of the easier to use token form factor and the ease with which the solution can be provisioned and used.

Celestix HOTPin addresses these issues head on and delivers a solution that does not compromise the core purpose of the solution, to secure the user's identity from theft.

Meeting the Requirements - HOTPin Technology Highlights

Reduced complexity: HOTPin authentication server includes an instance of RADIUS server on board, providing organizations with simple deployment and easy connectivity with any standard perimeter access gateway device. With a simple management console and a multitude of reporting options as standard, the solution is easy to manage and provides excellent visibility on your investment.

Simplified provisioning and higher adoption: HOTPin is tokenless, providing OTP generation via soft token or SMS. User provisioning can be offered in multiple methods, from app store download or through a simple to navigate self-service portal. User adoption is high because the technology is simple to use and requires no additional hardware.

Low TCO: HOTPin lowers the cost of authentication when compared with traditional hardware solutions. Initial investment is low because there are no hardware tokens to procure and issue. The renewal process is also low cost because there are no hardware tokens to renew and replace. HOTPin licensing model is simple, with a single HOTPin license allowing for the use of both soft token and SMS OTP generation.

Flexible deployment options: HOTPin authentication service is available as software or appliance form factor for on premise deployment or as a managed service with pay as you go price model.

Customization: HOTPin can be customised out of the box to allow for re-branding of the soft token. This presents organizations with an opportunity to enforce company branding or to offer HOTPin as a rebranded service to their customers.

[1] Symantec Authentication survey 2011 Two-factor authentication