RSA White Paper

Why Passwords Aren't Strong Enough: Making the Case for Strong Two-factor Authentication

The risks associated with the use of password-only authentication are not new. In 1995, the US Computer Emergency Response Team (CERT) reported that approximately 80 percent of the security incidents they received were related to poorly chosen passwords. Fifteen years later, 44 percent of organizations are still using just a password to secure remote access to their intranet[1].

With today's threat landscape and the increased value placed on the information created and stored, systems that rely on static passwords for security are left vulnerable and at risk of being breached. In this paper, we will examine the need for two-factor authentication and explore the return on investment that can be realized in order to help organizations make an informed decision when contemplating their strategic move toward stronger security.

[1] Forrester Research, "Best Practices: Implementing Strong Authentication in Your Enterprise," July 2009

RSA®

The Security Division of EMC

Contents

Among business professionals surveyed on password management , 66 percent of respondents saw employees keep paper password records at work. Moreover, 40 percent saw employees track passwords on Post-It® notes or scraps that were affixed to their computer.

The Need for Strong Authentication

Organizations face a more advanced threat landscape and a complex regulatory environment that can directly impede on their business objectives. Therefore, protecting access to information and assuring the identities of users requesting that access is a core element of any security initiative.

There are a number of reasons to justify the need for stronger security and to help build the case for investing in two-factor authentication:

- **Movement of new business applications online**. Organizations continue to recognize the opportunities and cost efficiencies associated with providing access to information online. As a result, more web-based applications are being launched to help facilitate the demand for instant access to information.
- **Increased demand for remote access**. The global nature of business and employee mobility has forced many organizations to provide anytime, anywhere access to enable employee productivity.
- **Access privileges to new user populations**. Contractors, partners and suppliers now require on-demand access to proprietary information such as sales forecasts, competitive intelligence, pricing charts, inventory, and customer data.
- **Increase in customer-facing portals**. There is an increased demand by customers to provide real-time access to information and the self-service options that enable them to manage their accounts online.
- **Regulatory compliance**. Numerous regulations have been issued in the last few years requiring organizations to enact security measures that prevent unauthorized access to information.
- **Advanced threats**. Threats to information continue to evolve and are becoming more challenging to contain. From the inside, employees engage in poor password management practices and work around established security policies to make their jobs easier. From the outside, phishing and malware are become an increasingly nefarious threat and fraudsters are beginning to recognize the value of enterprise credentials.

Inside the Threat Landscape

There are a number of internal and external threats that organizations must contend with in order to protect their information. These threats are often the single biggest factor in prompting organizations to apply two-factor authentication to protect access to their network and their valuable business data.

Internal Threats

Employees use countless systems and applications that require separate and disparate log-ins and passwords. This often leads to unsafe password practices such as using the same password on multiple systems, sharing passwords, and keeping record of passwords in handwritten or electronic documents. Among business professionals surveyed on password management[2], 66 percent of respondents saw employees keep paper password records at work. Moreover, 40 percent saw employees track passwords on Post-It notes or scraps that were affixed to their computer. Poor password management practices are putting organizations at risk every day.

The growth of the mobile workforce and anytime, anywhere access is another example of the threat posed by insiders. While many mobile employees access the corporate network through a trusted source such as their company laptop or mobile device, the use of public computers and wireless hot spots is a very common practice for accessing corporate systems, creating an opportunity for a key logger and other malicious programs to steal employees' passwords. In the 2008 Insider Threat Survey conducted by RSA, 58 percent of respondents stated they frequently or sometimes accessed their work email via a public computer while 65 percent frequently or sometimes accessed their work email via a public wireless hot spot.

The growth of the mobile workforce and anytime, anywhere access is another example of the threat posed by insiders.

[2] RSA Password Management Survey

Businesses are Increasingly Vulnerable to Cyber Threats

The distribution of malware has extended beyond the financial industry and is increasingly affecting businesses in the healthcare, insurance, telecommunications, and education market, as well as government agencies. The intended goal for most cybercriminals has been to infect online users with a Trojan to collect their bank account information or credit card numbers. However, the Trojans are collecting much more than just that information.

Consumers are also employees, and employees conduct personal business and check personal email accounts from corporate workstations. Similarly, as organizations make access available to a wider array of resources over the Web via technologies such as SSL VPN, the variety of computers touching the network expands to include personal machines such as the family computer. As a result, organizations are put at higher risk for Trojan infections and data loss.

Volumes of business data are landing in the hands of online criminals, usually unknown to most organizations. To demonstrate, when RSA released its findings in October 2008, after nearly three years of work tracking the Sinowal Trojan, the data discovered in the hands of online criminals extended beyond bank accounts and credit and debit cards; they had also collected information such as email addresses and passwords and FTP and VPN login credentials. This discovery was one of the first in many to follow that demonstrated just how vulnerable the sensitive data of organizations and government agencies are to the threat of Trojans.

External Threats

Using methods such as advanced social engineering, phishing scams, Trojans, and other forms of malware, hackers are seeking to steal company-sensitive information such as intellectual property and trade secrets by targeting VPN credentials and corporate networks. Botnets, in particular, present a serious threat to organizations as most infections come with malware program designed specifically to infiltrate corporate networks and perform specific tasks that siphon out sensitive information or steal passwords. Today, botnet activity can be accounted for in nearly 90 percent of the Fortune 500[3]. This puts small and mid-sized businesses, capable of spending only a fraction of what their counterparts do on security technology, especially at risk.

Another form of external threat targeting organizations is spear phishing, a form of phishing attack that is mainly targeted at employees or high-profile targets in a business. Spear phishing emails attempt to get a user to divulge personal or sensitive information or click on a link or attachment that contains malicious software. Once the user clicks on the link or attachment, malware is installed, usually in the form of a key logger. With this method, the hacker is able to steal anything the user types including corporate credentials, bank account information, or other sensitive passwords.

The True Costs of Password Authentication

The use of a single password as a means of securing access continues to dominate. With limited IT budgets, organizations often use cost as the biggest hurdle to overcome in making the case for two-factor authentication. However, the authentication method once viewed as “free” has actually become expensive in terms of ongoing management and support costs. According to the Gartner Group, between 20 to 50 percent of all help desk calls are for password resets – and cost up to $38 per call on average. This can be taxing on IT resources and does not account for the lost productivity time for the end user.

Compliance is another consideration when determining the actual costs of passwords. Multiple government and industry regulations exist that require the use of two-factor authentication in order to meet compliance. By failing to provide additional protection beyond a static password for users accessing sensitive data, organizations may be subject to hundreds of thousands of dollars in regulatory fines and penalties.

[3] Source: RSA Anti-Fraud Command Center

Finally, passwords are too easily compromised and put organizations at risk for a data breach. The average cost to a business for a data breach in 2009 was $6.75 million[4] which factors in numerous costs such as customer notification, forensics and investigation, legal fees, and potential fines. Then there are the intangible costs such as the impact of a breach on customer loyalty and loss of reputation.

An Overview of Two-factor Authentication

The key difference between password-based authentication and two-factor authentication is that the user must provide more than one factor, or proof, in order for a successful authentication to be made.

The elements of two-factor authentication include something you know and something you have. The first element, or something you know, refers to a factor that is known by the user such as a password or PIN number. The second element, or something you have, refers to a physical token or something embedded on a device or computer such as a software token, digital certificate or flash shared object, or a biometric identifier such as a fingerprint scan.

To assure positive proof of an identity, a user must successfully present both factors to the system in order to gain access. For instance, token-based two-factor authentication requires a user to enter a username and password (something you know) and the code that appears on their token at that time (something you have). If both the password and token code are recognized by the system, the user is authenticated and granted access to the resource.

In deciding on what two-factor authentication to deploy, organizations can choose from a range of solutions and form factors available on the market today. Each solution and form factor offer different value propositions in terms of security, portability, scalability, ease of use, reliability and, of course, cost of ownership (see sidebar for more information on how to choose the right two-factor authentication solution to meet your business needs).

Organizations often focus solely on cost and in the process overlook the long-term benefits that can be derived.

RSA Authentication Decision Tree

What is the right authentication solution for your business?

The RSA Authentication Decision Tree is an interactive tool designed to help you learn about, evaluate and select the most appropriate two-factor authentication solution based on your business needs. The tool takes into account several factors including the types of information being protected, the end user population and the technical environment where the solution will be deployed. The Authentication Decision Tree guides you through a series of questions and provides you with a personalized analysis that lays out your authentication options in an easy-to-understand report. To access the Authentication Decision Tree and receive your customized report, visit www.rsa.com.

The ROI Benefits of Strong Authentication

Organizations often focus solely on cost and in the process overlook the long-term benefits that can be derived. Two-factor authentication offers significant benefits including:

Reduce risk

As more valuable data is made available and a higher volume of transactions are conducted online, the risks to information continue to grow. The costs associated with a data breach continue to rise and the bad publicity associated with them can have an adverse impact on brand value and customer loyalty. In addition, the division between consumers and the enterprise continues to disappear and cyber threats are increasingly targeting business credentials. Two-factor authentication can help organizations mitigate their risk by proving the identities of users before granting access to sensitive information and applications.

[4] Ponemon Institute, Fifth Annual U.S. Cost of Data Breach Study, January 2010

Government regulations such as Sarbanes-Oxley, PCI Data Security Standard, U.S. Data Breach Notification laws and the Health Insurance Portability and Accountability Act are just a few of the regulations that call for the use of two-factor authentication to protect access to the corporate network.

Enable employee mobility

The mobile workforce is growing and organizations are expanding their operations and opening remote offices around the globe. To enable employee mobility and increase productivity, remote access is now being offered by organizations of all sizes. Two-factor authentication offers an additional layer of protection to facilitate secure remote access to critical business systems and information.

Create new business opportunities

Extending applications to the Internet has allowed organizations to provide new and convenient online services for their customers and easier access to information for their partners and suppliers. But, perhaps the single most inhibiting factor preventing many organizations from fully utilizing and realizing the potential of the online channel is security. In any online environment, it is important to establish trust with the user. Two-factor authentication provides organizations with the assurance that their users are who they say they are.

Lower costs

Some business applications provide the ability for companies to address expensive, labor-intensive internal processes. Order processing, human resource systems, forms processing applications and numerous other personnel intensive business procedures are being automated to introduce efficiencies and reduce costs. As critical components of the business infrastructure, it is important to authenticate users before granting access to these applications. In addition, with the high volume and cost of password resets, two-factor authentication can reduce the cost of help desk support.

Compliance

Government regulations such as Sarbanes-Oxley, PCI Data Security Standard, US Data Breach Notification laws and the Health Insurance Portability and Accountability Act are just a few of the regulations that call for the use of two-factor authentication to protect access to the corporate network in order to meet compliance requirements. Failure to meet these requirements could result in regulatory fines and penalties.

Conclusion

Unlike password management systems, two-factor authentication delivers the security necessary to protect access to sensitive data and allows users to safely conduct business. Additionally, the hidden costs associated password security actually outweighs the perceived high price tag of implementing strong authentication. Moving away from thinking about costs to the benefits that can be realized with enhanced security creates a compelling case to show the return on investment from two-factor authentication.

Myth	Reality
I use passwords because they don't cost me anything.	Passwords are actually expensive to manage when you consider that 20 to 50 percent of calls placed to the help desk are for password resets. When the average cost of a help desk call is factored in, passwords actually come with many hidden costs.
My business uses strong passwords and our employees are required to change them on a regular basis so this lowers my risk.	Strong passwords that include numbers, capital letters or characters are harder for a hacker to guess, but also harder for employees to remember. This creates a spike in help desk calls and is what leads employees to write down passwords on paper which actually increases risk.
My business can't afford the cost of two-factor authentication.	Two-factor authentication is very cost-effective – and not just for large organizations. Many vendors offer packages built for small and mid-sized businesses with a limited IT budget.
The cost of two-factor authentication outweighs the benefits.	The cost of two-factor authentication is much lower than what it would cost if your organization experiences a data breach or the fines and penalties you will have to pay for being non-compliant. In addition, two-factor authentication can help create business opportunities that generate new revenue which far outweighs the cost of paying for stronger security.
Cyber threats only target large organizations and the government.	Quite the opposite. Cybercriminals are targeting small and mid-sized businesses on a frequent basis because they usually have limited security controls in place, making them more vulnerable to an attack.

Perhaps the single most inhibiting factor preventing many organizations from fully utilizing and realizing the potential of the online channel is security.

About RSA

RSA, the Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control; encryption & key management; governance & risk management; compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

RSA®
The Security Division of EMC

www.rsa.com

SIDROI WP 0310