Top five IT security threats and how to combat them

Best practices from Quest Software help companies improve business outcomes through smart identity and access management strategies

June 12, 2012 Faced with external security threats from hackers and others, along with a growing array of even more dangerous internal security threats, companies worldwide are feeling the heat. Industry experts agree that strong identity and access management (IAM) technology and practices should be the cornerstone of every security strategy, but, legacy IAM offerings often are considered overly complex and difficult to maintain a problem compounded by the advent of cloud and mobile trends affecting enterprise access. Quest Software provides a modular approach to IAM ideally suited to address a full range of security concerns. This advisory provides the top threats companies should prepare for, and specific IAM best practices they should follow to combat threats early on.

Organisations traditionally have had only two options to address identity and access management:
1. solving specific pains in an ad-hoc manner with system and task-specific tools and practices from a variety of vendors
2. implementing a monolithic framework that seeks to address issues enterprise-wide through an almost entirely customised approach.

These options either are too customised and cumbersome to be sustainable, or too controlling and rigid to address todays new market realities. Neither adequately addresses the business-driven needs that are forcing organisations into action.

There is a better way. Quest Software, with its Quest One Identity Solutions, makes security and compliance simple and effective. Unlike identity and access management solutions from legacy vendors, which require extensive and costly customisation, Quest Softwares modular, yet integrated, approach addresses immediate concerns, but is nimble enough to tackle future business needs with an eye firmly on simplifying some of the most complex challenges organisations face today.

Quest Software identifies five top security threats and offers a set of solutions, proven in the real-world, that make achieving security and compliance not only simpler, but less expensive and more effective.

1. Internal excessive privilege System Administrators with complete access to servers and data can pose a tremendous internal threat if they turn against the company. Similarly, everyone from admins up to executives poses a threat to security and data if they maintain excessive access rights after changing positions or taking on different roles.

2. Third party access giving partners and other third parties appropriate access to data is no longer cut and dried. Data stored in the cloud may be located across the country or overseas, or sit on physical servers owned by one vendor, but housed in facilities owned by any number of data centres. Employees of these third parties often have direct access to unencrypted data, or they may retain copies of both encrypted or unencrypted data.

3. Hactivism politically motivated hacking is on the rise, by operations such as Anonymous Operation and Lulz-Sec. Members of these groups assert that much of their success comes not from their technical expertise, but from having found easy targets. While an organisation may not have control over whether or not it is attacked, effective identity and access management strategies and technologies, and basic employee security training, will reduce the chances that attacks will succeed.

4. Social engineering social engineering is the age-old technique of using lies, deception and manipulation to gain sufficient knowledge to dupe an unwary employee or company. Using public social channels to detail every aspect of your upcoming unplugged vacation trip may be just what a scammer needs to put an attack in motion.

5. Internal negligence negligence typically is an offence committed by management when they should have known better. Most successful data security breaches have some element of managerial negligence associated with them, such as simply forgetting to check log reports for clearly suspicious patterns.

The lessons how to combat security threats
* Adopt a least privilege security posture that gives each employee the least privilege necessary to accomplish required tasks, and ensures that

unnecessary access rights are revoked whenever an employee changes roles. Some of the most common implementation options to help get to a least privilege state include:
o assigning appropriate access directly to users based on well-defined roles
o limiting access to administrator and/or root accounts making sure that the passwords to these accounts are not shared, are changed frequently and that controls are in place to limit and track their use.

* Embrace an access review policy and regular, automated access alerts that notify two or more administrators of access changes, employee changes or other critical issues. To prevent access creep, access privileges must be dynamically linked to human resources and staffing databases. Notifying more than one administrator helps overcome negligence.

* Lock the front door by fostering education, encouraging diligence and developing processes such as regularly changed passwords, or by adopting harder security access technologies with tools such as Microsoft Active Directory or multifactor authentication. Employee education can cover the logistics and basics of security, but also can address topics such as the psychology and known techniques of social engineering hacks.

* Achieve compliance by implementing access control and separation of duties practices and technologies, and developing, implementing and enforcing secure policy on all system access. Provide a complete audit trail of policy and activities, and eliminate non-compliant login practices.

John Milburn, vice president and general manager, Identity and Access Management, Quest Software, said, Todays security challenges are drastically different than they were just a few years ago. The advent of cloud computing, mobile access and new compliance concerns has essentially taken everything organisations thought they knew about security best practices and flipped it on its head.

As the nature of doing business changes, companies need to get smart fast about building strong and sustainable identity and access management strategies. As a trusted advisor and steadfast technology provider for nearly 90 per cent of the Fortune 500, Quest Software has amassed the knowledge, experience, and technology necessary to successfully guide organisations through the new security landscape.

###

About Quest Software
Established in 1987, Quest Software (Nasdaq: QSFT) provides simple and innovative IT management solutions that enable more than 100,000 global customers to save time and money across physical and virtual environments. Quest products solve complex IT challenges ranging from database management, data protection, identity and access management, monitoring, user workspace management to Windows management

Quest, Quest Software and the Quest logo are trademarks or registered trademarks of Quest Software in the United States and certain other countries. All other names mentioned herein may be trademarks of their respective owners.