

Straight Talking – Why you must rein in your power users

Dec 2009

By Bob Tarzey, Analyst and Director, Quocirca Ltd

Within any organisation, a small group of employees have the ability to wreak havoc on its IT infrastructure: the privileged users that manage it. Granting privileges to such users is necessary for them to be able to do their job but when things go wrong the consequences can be serious.

In the majority of cases, harm may be unintentional - but that's cold comfort if an essential disk is wiped or a server goes down at peak time.

Worse still, some privileged users deliberately abuse their status. An example here includes the UBS systems administrator Roger Duronio, who was convicted in 2006 for sabotaging his employer's IT systems in retaliation over a compensation dispute.

In addition to IT systems, privileged users may also have access to intellectual property; such information can never be considered secure until privileged users are under control.

It's not just the privileged users themselves that are the problem, privileged accounts are often targeted by hackers. This is because such accounts are often left with default settings, making them easier to get access to than standard user accounts. Furthermore, if a hacker can impersonate a privilege user, he will have far wider access to the target systems.

It is not just in an organisation's own interest to get the privileged user issue under control, regulators and standards bodies have something to say about the matter too.

The ISO-27001 IT security standard states "the allocation and use of privileges shall be restricted and controlled". The Payment Card Industries Data Security Standard (PCI-DSS), which any business taking credit or debit card payments should adhere to, recommends "auditing all

privileged user activity" as well as avoiding the use of vendor-supplied defaults for system passwords.

Despite all this, recent Quocirca research, which involved interviews with 270 IT managers from across Europe, shows that despite claiming to adhere to certain standards, many organisations still allow bad practice when it comes to the management of privileged users. These included leaving default privileged accounts in place, allowing privileged users to share accounts (meaning no one individual can be held accountable when a problem arises) and the granting of far more privileges than are necessary for a given individual.

Quocirca's research shows that the take-up of certain IT security standards is high: for example 60 per cent of IT managers claim to have implemented or be implementing ISO-27001. Even so, bad practices are rife: around half of respondents admit to the sharing of privileged user accounts, including some that have implemented ISO-27001. In fairness, the standard is often implemented gradually and selectively but those that are reassured by a given organisation's claims to comply might be shocked to find that such underlying weaknesses in IT management can remain in place. Other standards and regulations such as PCI-DSS and Basel II are less forgiving.

What can be done?

First, organisations need to understand why the issue is important and what the risks are of not controlling privileged access. It is hard to persuade IT managers to start policing themselves, especially those with a security hat on - they are deluged with problems caused by malware, mishandling of data and others misbehaviours of standard users.

They often believe that having a high level of privileged access means they will be best positioned to deal with any issue, as nothing will be unavailable or hidden to them. However, it is in their own interests to take another look at their activities.

Most IT managers, as with the majority of other employees, are basically trustworthy, but sometimes it is necessary to be able to prove this. Besides which, with many standards and regulations demanding that privileged access is limited, businesses need relevant controls and processes in place. IT managers in turn need to have the confidence they can deliver on this.

Some attempt this with manual processes but these can be cumbersome and ineffective, especially when it comes to monitoring and auditing privileged users' activities. But there are tools available on the market that can automate many of the tasks.

Privileged user management tools operate at two levels: first, they allow the monitoring of software, including operating systems, databases and applications, to ensure privileged user accounts are not left with default passwords and that privileged access is granted only to specific named users. Secondly, such tools enable continuous monitoring of users while acting under privilege, providing an audit trail that protects the innocent privileged users as well as the business.

If it proves hard to persuade IT managers to monitor themselves, educating the business managers they serve should help - they are likely to be shocked at how exposed their organisation is from the cavalier management of privileged access.

Read more in Quocirca's report, Privileged user management - It's time to take control It's free to silicon.com readers on Quocirca's website

http://www.quocirca.com/pages/analysis/reports/view/store250/item22042/?link_683=22042

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>