AxiCom

Source: Financial Times {Main}
Edition:
Country: UK
Date: Monday 19, March 2007
Page: 11
Area: 512 sq. cm
Circulation: ABC 439104 Daily
BRAD info: page rate £46,700.00, scc rate £91.00
Phone: 020 7873 3000
Keyword: Imprivata

imprivata

NETWORK SECURITY

Gatekeepers mislay the keys

All-powerful 'administrator' passwords have been poorly managed, writes Guy Clapperton

By now every worker who uses a desktop computer understands the basic rules of passwords. Don't use your cat's name because everyone will know it. Change your password regularly. And don't tell anyone what it is.

But what is less well known is the difficulty of managing and safeguarding the passwords governing the IT systems that lie behind a company's network of computers. These administrator passwords, or "privileged passwords", are often in disarray and expensive to maintain.

According to a recent report by IDC, the market research firm, and the security specialist CyberArk, the need to manage privileged passwords manually rather than automatically can cost $500,000 a year for a typical Fortune 500 company.

Every IT system comes with a few "super-accounts" or "administrator accounts" that allow an administrator to set up a system, explains Calum Macleod, European director for CyberArk. "By definition these systems have to be set up in such a way that in the event of a disaster and the need for a change [such as installing a new application], those accounts still need to be there," he says.

Yet administrator accounts – and in particular their passwords – remain largely unmanaged, according to the report.

"In some cases systems come with a predefined password from the manufacturer; in many cases we've found companies haven't changed these passwords since buying the system," says Mr Macleod. "And the fact is that every box made by that manufacturer went out of the door with that same password."

The discrepancy between the careful management of individual users' passwords and those of the underlying system has its roots in the early days of computerisation, when IT was run from a mainframe centre and personal computing had yet to became a reality.

> There's conflict between the desire for a strong password policy and a human inability to comply

Many of the processes established then have changed little, while there have been drastic changes in the way individual workers use their desktop computers.

"The whole era of distributed computing took off and people had applications on small servers rather than one mainframe, but the policies in place stayed the same," says Mr Macleod. "One of the problems was who had access to these systems."

In the past, easy access to administrator accounts was seen as a necessity for those running an IT department and IT managers were far more focused on external threats such as hackers and viruses than internal ones.

Since administrator accounts are usually shared among a group rather than attached to a particular individual, it is hard to track and audit what an authorised employee has been up to, including tampering with sensitive data.

"We're discovering that a lot of banks have sensitive data that is not being secured properly because administrators have access to their accounts anonymously," says Mr Macleod.

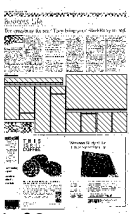
Alex Raistrick, director of the network security specialist Consentry, believes one difficulty is that organisations apply strong password policies but fail to follow them through. "I was speaking at the end of last year to a large bank with a couple of hundred thousand users worldwide, which has very strong policies on allowing people to install applications," he says. "They examine the need over a period of time so they end up with a lot of people with administrative rights [and] a lot of uncontrolled applications on their machine, and they don't have an audit trail."

Part of the problem is that administrative privileges are often assigned to a machine rather than an individual. Control comes down to who is on the network and who is allowed to do what, which is untraceable when employees have a shared log-in.

The situation is made worse by the requirement to maintain a complex password and change it periodically, believes David Ting, chief technology officer of the security specialist Imprivata. IT managers are as much at fault as the average office worker. "A [conflict] exists between the desire to implement a strong password policy and a human being's ability to comply with it. This is due to the average person's inability to remember a large number of complex, ever-changing strings." says Mr Ting. "Many IT administrators have revealed that they have used the same network credentials for years."

This matters because of the damage that can be done by someone controlling access to so much corporate data. The IDC report also points to costly outages, missed legal obligations when it becomes impossible to find out who has installed what, and labour-intensive work including a cost of $30 to change every individual administrator password on an ad hoc basis. The cost is high because manual changes to administrator accounts must be carried out by at least two people to ensure that the process is done correctly, and often requires physical access to a system.

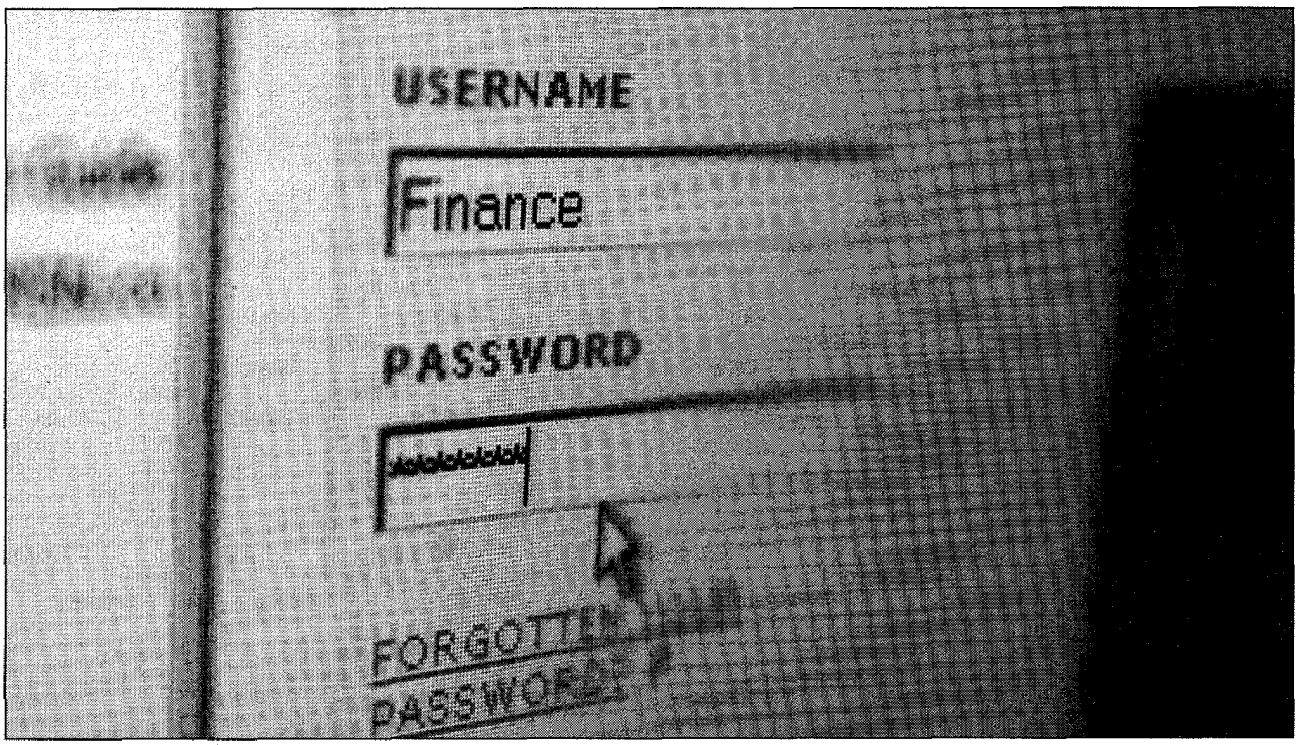
According to a separate survey by Cyber-Ark, 30 per cent of administrative account passwords are never changed. So while the average employee follows the rules – albeit reluctantly – it is easy for those who can do the real damage to ignore them with impunity.



AxiCom

Source: Financial Times {Main}
Edition:
Country: UK
Date: Monday 19, March 2007
Page: 11
Area: 512 sq. cm
Circulation: ABC 439104 Daily
BRAD info: page rate £46,700.00, scc rate £91.00
Phone: 020 7873 3000
Keyword: Imprivata

imprivata®



Costly: the need to manage privileged passwords manually can cost $500,000 a year for a typical Fortune 500 company Jamie Han