

Wednesday, February 11, 2009

Malicious insider attacks to rise

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

The world's biggest software maker has warned companies to expect an increase in "insider" security attacks by disgruntled, laid-off workers.

Microsoft said so-called "malicious insider" breaches are on the rise and will worsen in the present downturn.



A company's well-being could go out the door with an ex-employee

"With 1.5 million predicted job losses in the US alone, there's an increased risk and exposure to these attacks," said Microsoft's Doug Leland.

"This is one of the most significant threats companies face," he said. As the general manager of the newly formed Identity and Security unit at the company, Mr Leland told BBC News the effects of such attacks can be far reaching.

"The malicious insider is classed as the greatest security concern because they have access, and relatively easy access, to corporate assets," said Mr Leland.

Trillion dollar losses

A groundbreaking study last year by Verizon in the US found that insider breaches accounted for 18% of attacks with the remainder coming outside the company - for example by hackers, government agencies or business partners.

The report covered 230 million records over four years across the financial, technology, retail and food sectors.

Meanwhile a study by McAfee pegged total global economic losses due to data theft and security breaches thanks to organised crime, hackers and inside jobs at \$1 trillion last year.

The problem is not just a serious one for business.

Just this week, on the heels of some high-profile government breaches, President Obama announced an immediate 60-day review

of how the federal government uses technology to protect secrets and data.

"The national security and economic health of the United States depend on the security, stability and integrity of our nation's cyberspace, both in the public and private sectors," said John Brennan, the President's top adviser for counterterrorism and homeland security.



Customers lose faith in organisations that can't keep data safe

'Well-meaning insiders'

Symantec, the world's top security software maker, agreed that the financial downturn will lead to an increase in malicious insider breaches. Kevin Rowney, founder of the firm's Data Loss Prevention Unit, said in most cases people are motivated by "revenge, fear or greed."

But Mr Rowney also noted that "one of the biggest problems that is often ignored is the problem of well-meaning insiders.

"Their actions act as a prequel event to a lot of the attacks by more malicious parties. These people help proliferate the spread of confidential data, which makes it easier for malicious insiders to get a hold of it."

A report last week by the Ponemon Institute, a privacy and data-protection research group, found that 88% of data breaches were caused by simple negligence on the part of staff.

Mr Rowney said common scenarios involve employees stealing information to sell to a third party, to get back at a company for being laid off or demoted or to try and get a job at another company.

"We have even seen it as bad as people who got [lay-off notice]pink slips, that day going to a customer data base and forwarding huge blocks of this data out the door so they can then set up shop and sell to the same customers the next day," explained Mr Rowney.

'Crown jewels'

While insider attacks are lower in number, Mr Rowney said they can be more devastating because the employee knows where "the crown jewels" are kept - unlike a hacker who has to go on something of a "fishing expedition" to find a company's valuable assets.

This points to a simple lack of emphasis on who the bad guy really is when it comes to security breaches he claimed.

"The outstanding, unsolved, unaddressed risk management problem that has existed for years is that everyone is focusing on the hacker.

"It feels more sexy and interesting to fend against the assailant from the outside rather than face the possibility that the guy in the next



cubicle is ripping off corporate data," said Mr Rowney.

Microsoft's Mr Leland said the issue also highlights the complex problems that security officers face.

"On the one hand it's all about keeping the bad guys out, the malware, the viruses out of our systems. And on the other you want to let the good guys in - the people who need to have access to your system and information so that they can be productive. Getting the balance right is key."

Microsoft's solutions include encrypting data as well as the need for companies to react more quickly in rescinding an employee's access to data if they have been laid off or moved to another department. Mr Rowney admitted many companies have been slow off the mark to protect their assets from the inside and that the problem is largely preventable.

"Data loss prevention systems specialise in the detection of precisely these events. The report by Verizon indicates these protections are a critical form of risk management that no enterprise can no longer afford to ignore.

"We can slow down or even roll back the wave of data breach events that now dominate the headlines," said Mr Rowney.

Experts say many insider attacks are preventable.