factiva

F
The enemy within

Edward Wilding is chief technical officer of Data Genetics International, a company specialising in all aspects of computer crime investigation, incident response and forensic evidence.
1,098 words
1 October 2007
Banking Technology
English
(c) 2007 Informa UK Ltd

A disgruntled employee's $3.1 million sabotage at UBS provides an object lesson in systems security, says Edward Wilding.

When UBS PaineWebber hired Roger Duronio as a full-time IT systems administrator in 1999, it failed to do a background check on him. It was an oversight that was to prove calamitous.

Duronio had worked at UBS PaineWebber for two years and was paid a salary of $125,000. He expected a bonus of $50,000, but when in early 2002 he realised this was not forthcoming, he resigned on the spot. Duronio was escorted out the door, hell-bent on revenge.

Unbeknown to UBS, Duronio had by this time devised a logic bomb – a malicious computer program – designed to unleash maximum havoc against the UBS computer network on a date subsequent to his departure from the bank. The sleeping time bomb, which he installed from home onto the bank's central servers in Weehawkin, New Jersey – and on hundreds of servers across the United States – was set to delete all of the files on the host server in the bank's central data centre and in every distributed server in every US branch office.

Expecting that his logic bomb would ultimately crash the share price of UBS, Duronio gambled $21,000 on the stock market in anticipation of this effect.

At 0930 on 4 March 2002 the logic bomb "detonated" just as morning trading was getting into full swing. The bomb caused mayhem, crashing 2,000 servers in 370 branch offices, leaving some 17,000 brokers unable to trade. Duronio programmed the bomb to inflict maximum disruption – it re-initialised itself each time an afflicted server was rebooted and backup routines were also disabled.

A nightmare scenario ensued for the UBS IT team. The bank's computer experts, supported by 200 technicians from IBM, were forced to troubleshoot over several sleepless nights. Trading was down for days and in some branches for weeks. "It was the magnitude of it," testified UBS IT manager Elvira Maria Rodriguez. "If I had a scale of 1 to 10, this would be a 10-plus." UBS PaineWebber reportedly spent $3.1 million to assess the damage and restore its computer systems, a direct cost that did not even account for disrupted and lost business.

At trial, Special Agent Gregory O'Neil of the US Secret Service told how a team of 14 agents conducted a four-hour search at Duronio's home. They found a folded piece of paper on the dresser in Duronio's master bedroom with the source code for the logic bomb printed on it. The source code found on the dresser matched the source code found on the damaged servers.

Defence counsel pointed out that in 2001 and 2002 the bank's networks allowed more than one person to log onto the system simultaneously with the same user ID and password, and that system administrators, numbering some 40 employees at the time, all had the same root password. The network was also said to be riddled with holes that could be exploited by a hacker or another system administrator to plant the malicious code. They also implied that that the damage had been caused by Cisco Systems during a routine security penetration test of the UBS network, and that computer forensic experts relied upon by the prosecution could not be trusted because among their number was a reformed computer hacker.

None of these alternative explanations gained any credence with the jury, which found Duronio guilty of computer sabotage and securities fraud in July 2006. He was sentenced to 97 months without parole –the maximum term under US sentencing guidelines – and ordered to make $3.1 million in restitution to UBS PaineWebber.

Ironically, had UBS PaineWebber commissioned a $500 background check on Roger Duronio at the time of

2008 Factiva, Inc. All rights reserved.

his application for employment, the bank might have thought twice about hiring him. He had a criminal record that included charges of burglary, aggravated assault, drug-related offences, a tax violation, and a pre-sentencing report that listed charges against him from the 1960s, 1970s, 1980s, and 1990s.

“This is one of the most egregious examples that I’ve seen of behaviour that probably could’ve been predicted had PaineWebber known about the background of this individual,” said **Michael Hershman** who investigated Duronio’s background following the attack. “If I was a potential employer, based on our searches that took place in less than 24 hours, I would’ve had enough information to have said I’m not sure this is a good hire for us.”

Lessons to learn

The Duronio case shows just how devastating the malicious acts of one insider can be. At a practical level, though, the threats of systems sabotage may best be mitigated by the judicious mixture of procedural and technical controls.

These are too numerous to outline in full here, but readers should be advised that:

The segregation of duties is essential in a controlled IT environment. Never become reliant on any individual. Key processes should be clearly documented so an uninitiated operator can perform them. Assign supervisory or administrative rights to at least two people, but not to a wider group than is strictly necessary.

The aftermath of a disaster is not the time to test the integrity of your back-ups! Disaster recovery programmes should be tested an revised regularly.

Backups are the single most important defence against a range of potential computer disasters and their maintenance should never be entrusted solely to an individual.

At least one current backup tape set should be stored off-site; in the aftermath of the IRA bombing of Bishopsgate in central London in 1993, firms that maintained back-up tapes on site in fireproof safes were denied access to their premises, and hence their tapes, by the fire brigade because the targeted buildings had suffered such severe structural damage.

Beware of the risk that a logic bomb need not necessarily destroy data. The damage wrought may be more insidious and difficult to detect, such as the introduction of random data errors within financial and accounting systems and spreadsheets, or critical control data.

Exit procedures must be devised and carefully coordinated in the event of suspension or dismissal.

Despite the considerable effort involved, now is the right time to shakedown emergency procedures, and to sharpen up and test the IT control environment and business continuity plans.

Document BNKTC00020071001e3a10000w

2008 Factiva, Inc. All rights reserved.