

Cybercrime Gets Organised

Historically, IT security and information risk management has been largely focused around building a solid defence against external threats, protecting the company and its data from attacks by 'unknowns' from outside the business.

However, we are now seeing a sharp rise in attacks from inside the organisation, which is forcing boardrooms to demand a complete view of their entire threat environment. A 2006 survey from Goldman Sachs agrees, finding insider threat to be the number two driver for security spending in Fortune 1000 firms. As a consequence, businesses are increasingly looking to Enterprise Security Management (ESM) tools to provide in-depth consolidation, management and reporting of data, from every security device on the corporate network - not simply along the perimeter.

And being able to generate a transparent view of enterprise security is vital as the frequency and sophistication of insider attacks grow. Examples are all too easy to find: in late 2005, the Financial Services Authority (FSA) took the significant step of issuing a warning to the City that 'mafia' gangs are infiltrating British banks, sidestepping anti-fraud systems and stealing confidential data. They are doing so,

not by attacking the firewalls of these major institutions, but by stealing the identities and passwords of employees.

Organised Armies

Such attacks have catastrophic consequences for the enterprise, including the loss of customer confidence, regulatory penalties and massive financial cost. Conversely, the realisation that money can be made, with less risk and greater success than brute force attacks, has led to an explosion of interest from the criminal underworld.

With maverick cyber criminals, botnets for rent, exploit writers for hire, and the appearance of organised criminal gangs, attacks now go after applications rather than just operating systems and network perimeters. Using exploits written to attack, and botnets for distribution, thieves are now installing hidden key-loggers into company systems to capture passwords by logging local and remote access user keystrokes.

Organising Insiders

But malicious technical wizardry aside, one of the greatest threats to the integrity of the organisation comes from the most innocuous source: the single rogue employee, on the lookout for some quick cash. Simply walking into work and downloading huge swaths of confidential data to an iPod, USB drive or similar storage device will circumvent hundreds of thousands of pounds of perimeter security infrastructure in an instant.

Insider threat in this context is already a significant issue in the US, where illegitimate websites now auction stolen passwords, payroll and other forms of company confidential data, to the highest bidder. Last year, eight Bank of America employees stole over 700,000 customer records with the express purpose of profiting from the action.

As evidenced in the US and with the warning from the FSA, insider threat is evolving, but the most effective access point remains the employee. Such cases generated significant media attention in the UK when two people were jailed for stealing nearly £200,000 from actor and comedian Ricky Gervais, with the help of an insider. The insider was never caught. Similarly, Sumitomo Bank hit the headlines when fraudsters tried to steal £220m from its London offices by compromising the financial service institution's IT systems from the inside.

Automating Insider Detection

Insider threat is just one of a host of internal security challenges facing businesses today. However, the common strand connecting all of these incidents is the ineffective management of security data, and the corresponding need to automate threat detection, just as has been done at the perimeter level.

Most companies are so inundated with security information from each point security device that they simply do not have the resources to manually correlate the information, make sense of it, and identify deviant activity. In the financial sector, for instance, approximately 75 per cent of checks are manual. But with the



A 2006 survey from Goldman Sachs agrees, finding insider threat to be the number two driver for security spending in Fortune 1000 firms.

average FTSE 500 company receiving over 5 million security events each day, one or two innocuous looking internal attacks could easily go undetected until after the thief is long gone.

To put this in a real world perspective, a business traveller could remotely log into his company's network from Sweden. At the same time, a rogue employee is using the traveller's password and PC back at head office to download and steal company confidential data. One of these attempts is clearly a criminal act since the employee cannot be in two places at once, but in an environment without automation this is likely to pass unnoticed.

Informative Protection

Faced with exactly this challenge of detecting a small number of 'real' attacks from the sheer weight of security information generated by its myriad of perimeter and internal security devices, Iberdrola, one of the world's largest private utility companies, invested in a comprehensive Enterprise Security Management strategy.

Instead of manually identifying and quarantining attacks, the ESM tool has automated the process, managing the entire

security portfolio, including event logging, monitoring, and alerting analysts to potential attacks. However, it is real-time correlation of security data that holds the key to reducing and managing insider threat. Individual security events may pose no obvious threat, yet by correlating them together, as in the business traveller analogy, potentially innocent occurrences become highly malicious attacks or suspicious downloads of confidential information.

So while there is no silver bullet to insider threat, enterprises must take decisive action to limit security risk, not simply by taking a wider view of the threat posture of their businesses, but by automating the process of incident detection combined with prompt response. ESM is one of the most effective ways of managing this process, and with the Sarbanes-Oxley, Basel II and Combined Code imposing strict rules on data security - and even stricter financial and criminal penalties - few boardrooms can afford to ignore this corporate lifeline. To find out more about combating cyber crime and insider threat, visit www.arcsight.com or e-mail info@arcsight.com and request our white paper on Insider Threat.



Brian T. Contos, CISSP Chief Security Officer, ArcSight Inc