CPNI
Centre for the Protection of National Infrastructure

Insider misuse of IT systems

May 2013

This paper is a brief summary of the types of insider cases that CPNI has examined as part of its Cyber Insiders Programme. The mostly anonymous examples given here are representative of real cases that CPNI has collected.

The 2013 Price Waterhouse Coopers (PWC) information security breaches survey[2] shows the following results in relation to insider crimes. Furthermore, the survey found that 10% of companies' most serious breaches were caused deliberately by staff. It is likely that not all of these cases were malicious and that some were caused by poor organisational factors and weak security culture. However, we interpret the sabotage figures solely as malicious acts.

Type of Incident	Total Responses	% of Large Orgs that Experienced (>250 staff)	% of Small Orgs that Experienced (<50 staff)
Security Breaches	632	84%	57%
Unauthorised Access	528	66%	35%
DPA Breaches	528	44%	17%
Misuse of Confidential Information	528	31%	12%
Loss or leakage of confidential information	528	49%	17%
Sabotage of systems/data (at least 1 case)	662	6%	

Table 1: Insider-related figures from the PWC Data Breaches Survey

CPNI's insider case study collection and analysis of other sources, such as the PWC breaches survey, has found that most insider cases involving misuse of IT can be categorised as:

- Insider-facilitated Computer Network Exploitation (CNE)
- Exfiltration of sensitive information
- Illegal lookups and process corruption
- System sabotage
- Fraud

[2] www.gov.uk/government/uploads/system/uploads/attachment_data/file/191670/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

Insider-facilitated CNE

CPNI is aware of cases from multiple infrastructure sectors where employees have initiated cyber intrusions from the internet by physically installing malware onto their employer's systems, using USB sticks. Once on the system, the malware communicates with an (external) attacker over the internet, who can direct it remotely. In most of these cases, this method was used where spear-phishing was too difficult, or the attackers were able to cultivate employees with access in the target organisation.

CNE incidents are more usually initiated by spear-phishing emails, where an employee opens attachments that contain malware. In most cases, the employee acts inadvertently, but some cases may be deliberate, where the employee is acting for an external party.

Exfiltration of sensitive information

State and corporate espionage are perhaps the most common threats that spring to mind when we think of insider activities. Many companies' net value is in their Intellectual Property (IP) and the loss or theft of IP can prove very damaging. Companies struggle to monitor staff sufficiently to prevent them stealing IP and many cases of these crimes appear in media reporting every year. Many insider IP theft cases happen when employees are about to move to rival organisations and want to take material there, possibly to present as their own or to make the next job easier. Many thefts involve downloading files onto portable devices (e.g. USB sticks, lap-tops, tablets or portable hard drives), or emailing them to private webmail accounts.

State espionage cases can involve similar methods, but are not usually associated with imminent moves to rival organisations. Canadian naval intelligence officer Jeffrey Delisle was convicted of espionage last year, having exfiltrated documents from sensitive Canadian databases onto portable media and uploading the data at home to mail servers owned by his Russian handlers. Delisle conducted these activities for years before being caught[3].

Other individuals might steal IP or sensitive data for the direct financial gain. An example of this is that of Daniel Houghton who worked for the Secret Intelligence Service (SIS, or MI6) between 2007 and 2009. Houghton had downloaded over 7,000 top secret files on to a memory stick and an external hard drive, which he intended to sell to the Dutch security services[4]. The Dutch tipped off MI6 and Houghton was arrested after a sting operation and charged under the Official Secrets Act.

Many of these cases are difficult to detect; Houghton and Delisle both held legitimate access privileges that allowed extraction of files from sensitive databases, which are locked down for most staff. Many organisations also fail to enforce the storage of sensitive information in designated areas, making it difficult to identify theft of sensitive files amongst the 'noise' of normal downloads.

[3] www.bbc.co.uk/news/uk-20112616
[4] www.bbc.co.uk/news/uk-england-london-11176434

Illegal lookups and process corruption

Insiders can exploit the access they have to systems to commit fraud. A recent high profile example is that of Jessica Harper who stole £2.4m whilst working for Lloyds Bank's fraud department[5]. She fraudulently submitted invoices to herself over a period of 5 years, feeling it was money she deserved for working such long hours.

Personal data are also at risk from insider fraud. There have been cases of employees searching corporate databases for specific information or people stealing vast quantities of data (e.g. credit card details) to commit fraud and fund organised crime in the UK. Many insider acts such as these are opportunistic in nature, but some are linked to wider organised crime networks that cultivate employees in key positions. CPNI is aware of cases where employees have inappropriately or illegally granted loans, licenses or permits to individuals, often in exchange for payment or to help friends or family. Criminal and terrorist groups are also known to have coerced employees with key accesses to look up details of individuals or facilities they are interested in.

System sabotage

Employee disgruntlement can sometimes lead to an insider attack. An individual who feels he/she hasn't been treated fairly may choose to commit an insider attack in an attempt to cause harm to his/her company. This could be very costly to an organisation, as in the case of Vitek Boden[6]. Boden was a disgruntled employee working for Hunter Watertech, an Australian firm that installed SCADA (Supervisory Control and Data Acquisition) radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia. After quitting his job with Hunter Watertech and being refused another job by Maroochy Shire Council, Boden decided to get his revenge by tampering with the council's sewage regulation systems and causing 800,000 litres of raw sewage to spill into local parks and rivers.

A less physical example is that of a software programmer who didn't feel he was getting the merit he deserved for his work. As a result he chose to alter a couple of lines in the source code of a software programme that controlled his company's finances. This resulted in the software crashing and causing the company substantial financial losses. The problem with the above example is that the programmer had write access to alter the code as part of his job so his actions went unnoticed.

General points

Insider threat is a major problem facing business today. As discussed in this report, an attack could vary from exfiltrating large volumes of data via e-mail or removable media, attempting to sabotage IT systems to disrupt key services, manipulating data for personal/disruptive gain or abusing access to commit fraud. In many cases, protective monitoring systems are sufficient to attribute the insider crime after it has been committed, but not to detect any precursor activities which might have raised suspicion that something was going to happen.

[5] www.bbc.co.uk/news/uk-england-london-19675834
[6] csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf