Information Leakage

Generally speaking the majority of information leakages are deliberate security breaches from within an organisation primarily perpetrated by an employee, however there have been occasions where trusted third parties have been the culprits.

Rits' experience has shown that leakages regularly occur within organisations. These incidents include the emailing of confidential documents or the removal of information using portable media such as laptops, memory stick, Blackberrys, PDAs to name but a few.

But what about the accidental information leakages or those that occur through lack of awareness by an employee? For example the posting of technical information on bulletin boards, generally for legitimate reasons to assist solving a particular configuration problem, can provide the necessary information to launch a network attack. For example, stating the firewall brand, platform on which it is installed and the problem encountered on a bulletin board reduces the work that a hacker has to go to in identifying which potential vulnerabilities and organisation is susceptible to. It can in fact be likened to taking the needle out of the haystack and placing it on the table in full view.

Countermeasures

Countermeasures to prevent information leakage range from employee awareness to technical enforcement. However, solely relying on the integrity of an individual not to divulge such a valuable company asset may not be the most appropriate approach. While an employee may be content in their job today this may not be the case tomorrow. Consequently, technical countermeasures should also be considered.

Technical countermeasures work independently of an individual in that they provide a consistent and automated approach to preventing and detecting information leakage. They can be applied at various levels within the organisation for example at the desktop, server, application and Internet and email gateways layers.

Five actions to reduce the risk of information leakage:

1. Use encryption to prevent information being read by unauthorised individuals, especially if the information is being sent externally.
2. Block or quarantine emails and/or attachments that contain key words for example 'confidential'.
3. Restrict network access to sensitive information to only those individuals who require access.
4. Serialisation of documents, this can be extended for highly sensitive documents to include small textual modifications for each recipient of the document, which, if leaked, would identify the individual responsible.
5. Do not underestimate the value of user awareness. If individuals know the repercussions of posting seemingly innocuous information on a bulletin board then they probably will not do it.