

A wolf in sheep's clothing

Firewalls, spam filters and segregated networks. These IT-based elements are all well and good but how do you legislate for the weakest link in the humans within your organisation? Why go to the trouble and cost of securing the network, only for all your good work to be circumvented by a manipulative sociopath prepared to pick up the phone and blag a password from the helpdesk, or audacious enough to walk through the office reception and into the server room?

Human hacking or Social Engineering is the term used to describe the manipulation of staff to gather sensitive information. It can include such things as entering the building under false pretences or persuading staff to share passwords. And it's a threat you cannot afford to overlook: analysts at The Gartner Group have referred to it as the single greatest security risk in the decade ahead.

Social engineering is of particular threat to public sector organisations which, by their very nature, have an open access policy. Members of the public, contractors, tradesmen and part-time workers make it difficult to keep track of all the individuals coming and going. And even if you have a water-tight entry system, the social engineer

can often con their way in by duping the doorman. For instance, it is relatively simple to use the Google search engine to find out the job roles of senior employees and make an appointment.

You can also use Google to tap into IT user forums. Here, IT personnel will often post queries regarding problems they may be having with the firewall or router. The hacker can then use this information to identify the organisation knowing that it currently has little IT protection.

Security policies alone are not enough to protect you from the Social Engineer. What is needed is a penetration test which seeks out potential weakspots in the organisation. To catch a thief you really do have to act like a thief. Typically, the testing team will meet with a select few from the IT and security departments to establish the criteria for a successful hit. The tester will then try to carry out these objectives in a given timeframe, dressed as an employee or printer maintenance contractor, for instance, in an effort to pass unnoticed.

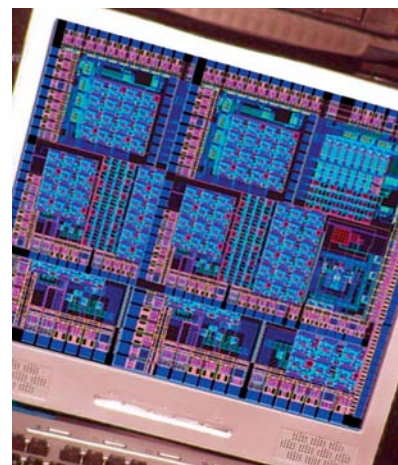
Specific examples of scams used in Social Engineering tests include planting a USB key with a sanitised Trojan. When docked with an in-house PC by an unsuspecting employee, this

then sends an activation alert to the penetration tester's HQ. Another example could be extracting a document labelled 'Secret' off-site. Or, more simply, by gaining access to passwords: in a recent test, the domain administrator password was obtained in just 15 minutes on a supposedly secure site. Gaps in physical security usually crop up as a result of gaps in understanding between Facilities

Management and IT departments. Think about it: you manage the equipment in the server room, but who's responsible for the fire protection systems in there? You arrange for the server rooms to be secured, but who keeps the keys / access cards? It may be a loyal member of staff, difficult to dupe, but we've still succeeded in the past.

Clients are continually astonished by the level of access we achieve during social engineering tests. While most expect us to gain access to the building, all are surprised when, at the debrief later in the day, we show them a collection of photographs and a detailed itinerary of the infiltration.

We find clients' views fall into two camps: those who believe physical security is impossible to achieve and can't see the point in testing it; and



those who are scared of the political problems the results could bring.

Yet effective testing can address the concerns of both. Solutions to the vulnerabilities exposed are sometimes technical, requiring a few simple changes to be made to physical security controls. This will deter all but the most determined social engineer or force them to take risks, leaving a trail of information behind them and increasing the chance that they are apprehended. It is advisable that the organisation then routinely carry out further tests on a regular basis to protect against new threats and maintain staff vigilance, perhaps on a weekly, monthly, bi-annual or annual basis. Then you should be in a better position to spot the wolf in sheep's clothing.

Ken Munro, Managing Director, SecureTest

Kids appoints new Chief Executive

Kids, the national charity and leading service provider for all disabled children, young people and their families is delighted to announce the appointment of a new Chief Executive.

Kevin Williams, who is currently National Secretary for YMCA England will join Kids in early May 2006. "We are delighted that Kevin is joining Kids, and we look forward to his leading Kids into the future with his breadth of management experience and knowledge in delivering services to children and young people," says Frances Prens, Chairman of the Kids Board of Trustees.

Note: Following six years as Chief Executive, Dr Sam Brier left Kids in October 2005 to take up freelance consultancy opportunities providing management, training and research. The Kids Board of Trustees appointed CR Search and Selection to find a new permanent Chief Executive, during which time

Caroline Emerton, Kids' Director of Finance and IT has served as Interim Chief Executive.

- Kids is a national registered charity (number: 275936) dedicated to working with disabled children, young people and their families to help them make the most of their abilities from an early age. It's support and services offer a range of approaches to the inclusion of disabled children and young people in everyday life. Founded 35 years ago, Kids is unique in the range and scope of the services it provides to children with a range of disabilities - supporting their educational, social and emotional development, as well as to parents and young carers.

- There are 700,000 disabled children in Britain under the age of 18 years. (Source: Department for Work and Pensions Family Resources Survey GB: 2002/2003).

- Since 2003, Kids has incorporated Kidsactive, previously an independent charity renowned as the leading national voice for the policy and practice of inclusive play. It's work of direct services on adventure playgrounds and supporting mainstream play services towards inclusion, is now carried out through Kids London and Kids National Development Division respectively. The name is retained in the branding of national inclusive play training courses and publications as 'Kids active'.

- The Kids National Development Division runs the Playwork Inclusion Project (PIP), funded under a strategic partnership with the Sure Start Unit at the Department for Education and Skills (DfES). It aims to increase the inclusion of disabled children in play and childcare settings through a programme of training, publications and national policy and development work.

- It runs the National Inclusive Play Network, providing information and support to play providers through bi-monthly e-mail bulletins, regional network meetings and an e discussion group on inclusive play.

- "Kids is a beacon of excellence and good practice". The Rt Hon Margaret Hodge, MBE MP, Minister for Children, speaking at the Kids annual conference, 6 October 2004 (The Royal Hospital Chelsea, central London).

For more information, please contact: Debbie Hyde at Oasis
Media Tel: 020 7450 9057
debbie.hyde@oasismedia.co.uk
Tel: 07956 320 486

To join the network go to:
www.kids.org.uk/ndd/nipnetwork