You've got your IDS...

Michael Barwise

You've got your IDS, you've got your firewall, your policies, your security management committee and all the rest. Maybe you've even got your pristine new ISO 27001 certificate. So you're secure, right? Not according to the Western Australian Auditor General. His report on the security of government agencies published on 15th June 2011 makes interesting reading.

Fourteen of the fifteen government agencies audited exhibited well-known vulnerabilities detectable from the public internet using common tools and exploitable to penetrate the agency's systems. The auditors were able to access internal systems and modify files at three randomly chosen agencies without being detected, despite the presence of IDS. That's quite impressive, considering that *"nearly all the agencies we examined had recently paid contractors between $9 000 to $75 000 to conduct penetration tests on their infrastructure. Some agencies were doing these tests up to four times a year."*

Next, the auditors left USB sticks that would phone home if used lying around in the offices of the agencies. In eight of the offices, staff plugged these completely unknown USB sticks into their work computers. Although not noted in the report, this tells me that they were almost certainly using an unpatched Microsoft OS and AutoPlay had not been disabled - strongly suggestive of an elderly unhardened raw "off the CD" rollout. Incidentally, only three of the USB sticks were reported as lost property, and *"several USBs found their way into home computers or the networks of private organisations..."*

From the policy perspective, twelve of the 15 agencies had failed to address both internet threats and social engineering, nine had performed no risk assessments, and seven had no incident response plans or procedures. So one wonders what was in their policies and procedures. No one doesn't - almost certainly they consisted of no more than the standard set of vague threats against users. But of course they did *exist*, which is what matters.

Now I don't believe that the Western Australian Government is *particularly* bad at infosec. Indeed, Australia is in general considered above average. So this is a common - most likely a universal - problem, and it's clearly not only an elephant in the room but also a crocodile on the sofa. A hungry one - which we should note well, as any one of us may be sitting down there quite soon. That twelve agencies out of the 15 had not addressed external threats comes as a surprise to me - from the penetration test results I'd have thought it would be more like all 15. But nine agencies not conducting risk assessments and seven having no incident response plans, although it suggests a very low level of both expertise in and commitment to security, is quite typical in my experience.

The current emphasis of infosec, like that of most corporate externality-driven disciplines, is still "compliance" - fulfilling requirements mandated by some authoritative regulator or standards body with the smallest possible effort and expenditure - "what's the least I can get away with doing to fulfil the letter of the law?" It's an attitude that leads to quarterly pen tests missing what a single focused exercise can uncover first time round using commonplace tools available on the web. But that's inexcusable. Or alternatively, the results of the pen test not being acted on, which is completely Kafka-esque. It's an attitude that leads to the kind of disaster this audit successfully simulated. But it's just not good enough. On average in the UK alone there are around three personal data breaches per day. That's not good enough either.

Meanwhile the prime thrust of infosec consultancy is ISO 27001 certification - typically, the preparation and maintenance of twenty-odd document sets demonstrating that security is managed using the procedures specified by the standard. Not checking whether that's the best way for the organisation. Not discovering whether it gets results. Nor whether the organisation is actually secure.

But of course I'm being naive - that lovely certificate is the goal, not security. The certificate that opens commercial doors to lucrative contracts. The certificate that can already exonerate you in court if you get breached, despite only around 0.4 per cent of UK businesses having one. Nevertheless I can't help feeling that if the ISO 27001 audit were half as penetrating (in all senses) as the one just conducted by the Western Australian Auditor General, business might stand a chance of surviving in the face of rapidly escalating risk. It's time to start actually addressing security instead of just playing games with paper.

Originally appeared as "Penetrating insights from Down Under..." on the Infosecurity Network, June 2011