Information Security Now - 19

John Mitchell

I always advise my clients to have regular penetration tests conducted against their systems. My standard mantra is every 90 days, or whenever there is a change to their firewall, whichever is the sooner. Things move very fast in this area and an annual check is simply not sufficient. Most organisations force password changes much more frequently, on the basis of minimising exposure to a compromised account and yet they are willing to leave their entire network exposed for up to a year. Very perverse behaviour. Regarding the actual testing we once conducted an experiment where we had one group who looked at the potential exposures from a theoretical viewpoint and another group which conducted the actual ethical hacking. The theory group spent some three weeks examining the infrastructure, the firewall configuration and the tools available to hackers. They suggested a few tweaks which were then applied. We then let the hackers loose and they were into the network within 20 minutes, thus showing the immense gulf between theory and practice and bringing me nicely to the gulf between auditing controls and actually examining the results of control failures.

For my non-audit colleagues a quick briefing on the “systems based audit approach”. The underlying process comprises four stages: gain an understanding of the system; identify where the controls should be to minimise risk; ascertain whether there is a control actually in place; test the control for its effectiveness in managing the risk. It takes a bit of time, but is pretty surgical in its approach. I tend to short circuit this process by going straight to the last bit which is testing control effectiveness. I do this by hacking the data. All systems rely on good quality data. Indeed the only rationale for any system is to process the data to produce reliable information for decision making. Therefore, for all systems we should know the data quality rules. I use this information to peer into the databases using a variety of analytical tools to ascertain whether the data complies with the rules. If it does things are likely to be okay from a control viewpoint. If they don’t, then I know that there is a control failure somewhere along the line. The full system based approach is akin to my earlier description of the theoretical approach to perimeter security, whereas my looking at the data is akin to the actual penetration test. The challenge with any theoretical approach is that you are limited by your own imagination, whereas a practical attack by someone else will not have the same constrains. The system based audit approach tend to review a process in isolation and may miss key risks from outside the immediate area. My approach may well detect data irregularities as a result of unauthorised manipulation by (say) IT staff or hackers. I have found some really weird control deficiencies simply by examining the data: the £80 billion asset as a result of poor input validation (should have been £8,000); the insurance fraud because the perpetrator knew that claims under $1,000 were paid without investigation (never rely on secrecy as a control mechanism); the corrupted links in the pensions database which meant that contributions were not going to the correct fund; the incorrect depreciation which overstated the balance sheet; the incorrect debt ageing which had an adverse impact on the uncollectable debt provision. However, the best one was the Unix compiler that thought that one divided by one was 0.99999666663333. Not to much of a concern for a financial calculation, but it could have had a really adverse affect on a missile guidance system. Target Bagdad, hello Tel Aviv.

It's also quicker and cheaper, which is something my clients like. Which brings me back to the cost of regular penetration testing. This is the main push back I receive when I make my recommendation for more frequent testing; although things have got easier since SOX[1] came on the scene. Gordon and Loeb[2] show that a small incremental investment in security results in superior breach protection, so the client can make an economic assessment of the return on the additional security investment. With the cost of security breaches to companies rising, every security officer should consider the total cost of a breach against the protection cost. The use of "ethical" hackers will almost certainly be less than the cost of a penetration by a "black hat". Not least is the embarrassment caused when an "amateur" hacker breaks into your systems, as the US Government found out when trying to extradite Gary McKinnon for allegedly breaking into 97 military computers whilst seeking information on aliens. Perhaps they should have hushed the whole thing up and presented him with the Congressional Medal for services to the state, rather than owning up to the complete waste of their last 10 years in trying to harden their sites from cyber attack? Which brings me back to my point that you should never rely on secrecy of the process as a control mechanism. Much better to assume that the enemy knows your processes at least as well as you do. The trick is to make it so difficult that the cost of the attack is greater than what could be gained. Prevention has to be the name of this game as detection may be too little and too late.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a former chair of the Information Risk Management and Audit (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454

[1] Sarbanes Oxley - USA
[2] The Economics of Information Security Investment