Information Security Now - 16

John Mitchell

The predecessor of the Internet (Arpanet) was designed to survive an atomic war. As such, the prime directive of any Internet connected computer is to respond with a “yes” to any enquiry from another computer asking the question “are you still operational”. This very response mechanism has since been exploited by hackers “pinging” internet addresses with the hope of getting a response from another computer. Knowing that a computer is on-line presents them with the opportunity of either subverting it, or launching a denial of service attack against it. As the internet is a *network of networks* which consists of millions of private, public, academic, business, and government networks that are linked by a broad array of electronic and optical networking technologies, it stands to reason that international co-operation is required to protect the service. But what if a sovereign government decides to remove another country from the internet? Well, this is exactly what happened in 2007, when it is alleged that Russia conducted denial of service attacks against Estonian government web sites. Whether Russia was responsible is a moot point, but the fact remains that for two weeks Estonia had severe Internet availability problems.

Responsibility for protecting the UK infrastructure rest with the Centre for the Protection of National Infrastructure (CPNI). This is a government agency that provides protective security advice to businesses and organizations across the national infrastructure. Note the use of the word advice”. It is up to the recipient of the advice to take the relevant action. In many cases the decision is likely to be taken on commercial considerations (even not-for-profit organizations have budgets), along the lines of “will implementing this advice cost me more than I am likely to lose as a result of any disruption”? So what is in the interests of UK plc may not make commercial sense to a single company. Now most organizations are selfish, rather than altruistic, so the message has to be that we are all in the same boat so let’s share the cost in order to reduce the pain. However, the issue is now clouded by the growth of outsourcing, off-shoring and cloud computing. Whose infrastructure is your critical application running on? It is possible that the critical infrastructure you are relying on is hosted in another country over which the UK has no control. Do they have the equivalent of a CPNI? Where is your data? Who manages your email? Where is the attack coming from? Do we have jurisdiction in that area? Anyone who receives unsolicited communications (SPAM) know just how difficult it is to stop it.

The US Government has had some success in prosecuting spammers, but the majority carry out their business without interruption as they operate from countries without extradition agreements. Spam is a limited form of denial of service which can easily be ramped-up to overwhelm a target as Steve Gibson of Zone Alarm firewall fame found when he inadvertently questioned the technical ability of a thirteen-year old hacker. Gibson knew how to protect himself, but was helpless against the storm of continuous and various attacks against his web site. In the end, only a public apology stopped the maelstrom

of “pings” against his IP address. And therein lies the problem. In much the same way as the launching of the Dreadnaught battleship by the British in 1906 made all other battleships obsolete and hence set a level playing field for all nautical nations, we now have a situation where countries without an investment in expensive, up-market, weapon systems, now have a level playing field when it comes to cyber warfare.

It has often been said that the next war will be won by the side with the fastest computers. This makes sense as the faster the computer, the quicker it can both attack other devices and defend itself against counter-measures. Military aircraft still have old fashioned, mechanically based, inertia guidance systems in case the state-of-the-art GPS satellite navigation system is disrupted. True business continuity planning. What fall-back do we have if we lose the Internet? Precious little is the answer. But going back to where I started from, the Internet it is designed to survive an atomic war; which is more than we humans are. Do I see the founding of a machine civilization which will outlive us?

John is Managing Director of LHS Business Control, a corporate governance consultancy which he founded in 1988. 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