In hindsight, we need foresight

Michael Barwise

According to the BBC, on 28th March 2011 a 75-year-old Georgian grandmother disconnected Armenia from the Internet. Apparently, while scavenging for copper cables in a duct close to the Georgian/Armenian border she severed the fibre optics feeding all three Armenian wholesale ISPs. The entire country was offline for several hours.

That reminds me of an incident a few years back in Manchester. A commercial ISP with redundant upstream connectivity went dead when vandals dumped a wheelie bin full of petrol down a street manhole and set fire to it. The ISP's connections to all its redundant providers ran through the same duct.

In the week of 14th March 2011, RSA suffered a security breach. There's been a huge fuss about whether the company's SecurID product has been compromised., but the really interesting thing is how the breach happened. RSA's own analysis of the attack states that an incoming email carried a malicious attachment - an Excel spreadsheet containing a crafted Flash movie. One low-privileged employee retrieved this email from their personal spam folder and opened the attachment. The malware compromised the user's PC, elevated its privilege level, then penetrated the network, gaining access to servers the compromised user was not normally privileged to access.

This in turn reminds me of USS Yorktown. In 1997 the Ticonderoga-class cruiser - managed via an NT4 network - went dead in the water after someone entered a zero in a spreadsheet, causing a "divide by zero" error which crashed the remote database manager. The crash took out the propulsion systems and Yorktown had to be towed home.

By now you may be scratching your head and asking: "What's the old goat banging on about?" Well, quite simply, all these incidents have a common factor, and that is lack of foresight. In the first two cases - particularly the second, where the specific aim was redundancy - using the same duct doesn't seem terribly sensible. In the case of RSA - the provider of a globally deployed strong authentication system - it's odd that an email identified by a user's email client as spam ever got that far - particularly with a highly anomalous attachment in tow. So much for email filtering. Furthermore, a host used by a low-privileged functionary should not have unfettered access to high-privilege servers even if its privilege level is locally elevated. Ideally, they should be on entirely segregated networks. And in the Yorktown case, a single database engine should not have been the kingpin of all onboard operational systems.

Underlying every one of these incidents there was at least one obvious accident waiting to happen. But it had not been covered for due to lack of attention to detail at critical points in systems. You can't exercise foresight if you can't see what you're looking at. I consider this to be the greatest weakness in our ever-increasing reliance on technologies in everyday life, and I believe it will bring us to our knees very soon unless we fix it now. But how? No technological fix can protect against sloppy conceptualisation, design or implementation - particularly a technological fix that's the outcome of sloppy conceptualisation, design or implementation.

But maybe I overstate the case. After all, some 10,000 shipping containers fall overboard in transit every year due to top-heavy loads - because they don't get weighed and sorted before loading - and nobody seems to mind much. But just maybe, to quote Buddhist master Henepola Gunaratana, *"we are simply not paying enough attention to notice that we are not paying attention"*.

Originally appeared on the Infosecurity Network, April 2011