How Not to Secure a CA

Michael Barwise

Fox-IT have published a preliminary report on the DigiNotar breach. It appears that the number of spoofed certificates is much greater than previously suspected, and the Iran was a prime target, so once again we may have an example of the increasing importance of malicious hacking in the political arena. But what appalled me most when I read the report was the sheer lack of basic security Fox-IT found. Remember, DigiNotar is a root certification authority - a critical component of the network of trust upon which secure web commerce relies.

I quote from the Fox-IT report:

- "The most critical servers contain malicious software that can normally be detected by anti-virus software."
- "The separation of critical components was not functioning or was not in place."
- "...the CA-servers, although physically very securely placed in a tempest proof environment, were accessible over the network from the management LAN."
- "All CA servers were members of one Windows domain [accessible using a single] user/password combination."
- "The password was not very strong and could easily be brute-forced."
- "The software installed on the public web servers was outdated and not patched."
- "No antivirus protection was present on the investigated servers."
- "An intrusion prevention system is operational. It is not clear ... why it didn't block some of the outside web server attacks."
- "No secure central network logging is in place."

I'm wondering what else could have been done to make the attackers' job easier. I'm also wondering how many of our other critical services - banks, government departments, health services, are as secure as this. Actually, I'm not wondering - I know.

But I do indeed wonder how long we, as a supposed profession, are going to allow this state of affairs to continue. In the avionics industry they don't keep building planes that fall apart in the air, so why do we do it in e-commerce?

Originally appeared on the Infosecurity Network, September 2011