Testing for security consultants.

A five step simple to understand approach to computer security.

By : Khawar Nehal

Date : 1 October 2017

There are many confusing terms explained by trainings related to security. There are many hair raising articles related to computer security causing unnecessary worry and depression among those who want to use computers for their efficiency and benefit.

There are too many so called experts and real experts running around claiming they know something about security.

What I have done is explained in simple layman and easy to implement business terms how to separate the experts from those who act like some expert in security.

If you want to test a security consultant who claims they have certificates or degrees in cracking which they want to call somehow hacking.

Before giving them the job do the following :

1. Request the admin of an ISP with more than 10,000 paying customers to place a file named “prize.txt” in some directory on their billing computer. Pay them for the service if you have to. The file shall contain a sentence which only you and the admin of the ISP knows the contents of.

2. Ask the “experienced” crackers or so called hackers with certificates in “ethical” or whatever hacking they want to call it. The real capable people might have NO certificates.

3. Tell them to cut the jargon and ask the security expert to crack or since they want to call it “hack” into the machine and get the data in the file.

4. Watch the lame actors give a billion excuses as to why they cannot do it. That just means all their techniques are not capable of providing them any access to the ISP's computers. When you encounter this case, hire the admin of the ISP as a security consultant for your organization. Fire all IT department people who disagree with the methods used by the ISP admin on securing computers. The lack of skills related to security and the adamant holding on to old techniques is the main reason for lack of security in organizations. The management is responsible on depending on less qualified people and accepting breaches as a part of reality. This is not the case in ISPs and that is the reason such an example organization was selected.

5. If they cracker/security consultant can get access to the file, then ask them to explain how it was done to make sure it displays the existence of security loophole in the network and computer security systems. Make the ISP pay for the research done and/or pay for it yourself. Then hire the cracker/consultant for your company security. Make sure you make them sign a contract which makes the organization secure from internal and external threats and they are to report all info to the owners of the company. The owners need other people to decipher what the report says instead of bugging the capable expert to explain what is in their report. Again fire all IT Department people who complain that the security policies to secure the system are not implementable. Hire new people who can implement them and ask the consultant to teach the new IT people on how to implement the policy.

If you have a better idea or you can make suggestion to improve this idea, please email to khawar@atrc.net.pk