Article

Sep 2022

What should I look for in a Pentesting company?

Not sure what to look for when engaging a pentesting company? Keep reading to find out what you should expect from the experts.

You may be wondering how to find the right pentesting company. You want someone with experience in attacking networks, but not just any old hacker will do! This article provides helpful tips on hiring professionals who know their stuff, so your information stays safe from harm while also keeping business operations running smoothly.

Are they selling you a scan OR dedicated pentesters to do the right job?

Consider a house with an open front door, while that door can be locked, just how much could a robber access if they walked inside the house? A filing cabinet? A safe? What could they do with the contents? Are codes and keys easy to find lying around? Perhaps they could find keys to the car or back shed.

A scan will simply let you know about the open door, a penetration test will help you understand what damage that open door could cause and how that can be prevented. While scans are a popular and readily available option for all organisations, they are only capable of searching for low hanging fruit.

A penetration test makes use of the results, effectively understanding what can happen if these scan results were to be used by someone malicious.

While scan results are holes that need to be patched, a penetration test will identify what can happen after, how can these be taken advantage of.

Do you feel that they truly understand your needs?

Not all penetration tests are built equal and no one tester is comfortable touching all technologies. A good firm knows when to walk away and when something is right up their alley and as such, they will make a strong effort to talk through your processes, technologies and really understand the organizational risk if they were to be successfully exploited.

Whether you need a penetration test performed for the sake of compliance or it is a part of a product release, any firm engaging you should want to understand not only your end goal, but the technologies and applications you need reviewed.

Ideally, they will have performed the work previously or have team members that are comfortable with the technology being tested.

After all, even if a mechanic has spent decades repairing cars, they aren't likely to be willing or equipped to repair your steam train.

Do they have processes in place to ensure your organization's availability and safety?

Mistakes happen, however when it comes to your critical systems, those mistakes can lead to lost revenue at best and a safety hazard at worst. Take for example a pentest occurring on industrial control systems or machines responsible for medical procedures. While a pentester may not be standing in the same warehouse or office, due diligence to understand the device being attacked should be taken.

Furthermore, the firm should have processes, procedures and escalation chains in place for if something were to go wrong or if they had identified a potentially risky device and wanted to proceed with exploitation.

On the other end of the pentester's screen is a device in a physical space performing a job or providing a service that real people rely on and ideally any firm finding and/or exploiting problems with that device would understand that better than anyone.

Are they open when talking about their people, technology and processes?

When it comes to determining whether or not a company is truly open, there are a few key factors to consider. Is the company open, willing and passionate when they discuss their people, technology and processes?

Are they willing and able to go into detail about their people, technology and processes so that you trust they have the knowledge to understand yours?

By taking these factors into account, you can get a better sense of how open a company really is.

Here's a helpful summary of the above points:

- Know what you're buying into - Is it just a automated scan or a thorough pentest?
- Have they heard your business needs and are creating a bespoke plan to your business?
- Do they have processes in place to ensure your organisations availability and safety?
- Are they open and willing to discuss all aspects of their business with transparency?

Get in touch with Waterstons Australia today for a complimentary vulnerability scan and consultation.

info@waterstons.com.au

+61 2 9160 8430