# Internal & External Penetration Testing & Data Stream Protection

*Corporations that take a proactive approach, will be better off then their competitors who take reactive measures.*

OTTAWA, ONTARIO, CANADA, July 22, 2021 /EINPresswire.com/ -- Why Your Company Needs Penetration Testing

When it comes to a business' cyber security, there is only so much that can be done from an internal perspective. Strategy, planning, and assessing are important parts of corporate networking, but when it comes to the security, an outside-in approach needs to be taken. A lot of effort and time goes into setting up security measures, they need to be thoroughly tested to make sure that they work. This is why [pen testing companies](#) are an important part of corporate cyber security. This even goes for smaller businesses – if your company has any online portal or network, it can be subject to a network breach or hack. Pen testing companies approach a business' internal network from the perspective of a hacker and look for exploitable weaknesses.

A properly conducted pen test can provide companies with valuable insight to their networks and let them know ahead of time what vulnerabilities are in their network, and how they can be patched up. As technology and hacking techniques improve, pen tests need to be done regularly to make sure that the network is continually protected against outside attacks. The biggest risk are the companies' registered users because every network is vulnerable and common paths are already protected. The main weakness is the interactive legal interfaces that are available to the authorized users. Pen tests actively seek out these weak points and test to see if they are susceptible to exploitation. Penetration & network security tests can allow businesses to take a more proactive approach to protecting not only their own data, but also their clients' sensitive information as well.

What is a Penetration Test?

Penetration Testing, also sometime referred to as "ethical hacking", is when a company employs another agency to conduct an authorized cyber attack on their network. The pen testing company then employs hacking techniques to find any gaps in the corporation's network and software, including trying to access private information, payment files, user accounts, and more. While doing the "ethical hacking", the pen testing company will use simulated attacks like

phishing, looking for open ports, creating backdoors, if they can change or affect data, or installing spyware / malware. Of course, prior to doing this simulation, the pen testing company signs a thorough legal waiver to ensure that any and all sensitive data that is found is not shared or used in any way.

What Happens After the Pen Testing?

Once the pen test has been completed, the "hacking" company provides a full security audit to the corporation. This audit outlines the various testing that was done, and what areas of the corporation's network and data that they were able to breach. Along with that information, the pen testing company also provides their recommendations for fixing the security issues within the network, and often can take care of the fixes for the corporation if needed as well.

For any corporation that stores sensitive data, whether it is internal records, client information, or anything else like that, it is important to take cybersecurity seriously. Data breaches are becoming more and more common, and if a company has not taken the proper steps to ensure their data is secure, it can be seen as negligence. Corporations that get ahead of their would-be cyber attackers, and take a proactive approach, will be better off then their competitors who take reactive measures.

Anna Anthony
Ideabytes Inc.
+1 613-355-0411
email us here

---

This press release can be viewed online at: https://www.einpresswire.com/article/546929099