Organisations that need information systems infrastructures for managing data, business procedures, activities and client relationships must have robust IT security programs in place. Since they have data stored and processed through their systems, regardless of the industry and size, no business is safe from malicious criminals. They need comprehensive approach for protecting their network from cyber incidents before they take place.

Regardless of who you entrust with your IT infrastructure’s security, one of the most important component of your security program must be penetration testing. It’s now considered a best practice to identify and make corrective actions for improving organizational security.

**Why Do You Need a Business Security Plan?**

One cannot stress enough on the importance of having a proactive approach towards cyberthreats. An organization that strives to achieve better security culture needs to create a plan emphasizing speed, quick response and preventive controls.

A good security program must include a number of activities to address possible inefficiencies and vulnerabilities in the system. Intrusion prevention and vulnerability scanning tools are good, but they are not enough. You also need consistent audits and testing along with a set of enforced policies to protect your data, users and system. This is where penetration testing is of utmost importance.

**Why Penetration Testing?**

In order to protect the confidentiality, integrity and availability of your assets, you need to hire certified penetration testing professionals for assessing potential vulnerabilities and risks associated with your organization. Simply put, the process of scanning, testing, hacking and securing a system can combat inside or outside threats to an organization. It simulates real-life scenarios and detects malicious or suspicious behaviour patterns. A professional pentester is able to evaluate these risk factors and review the effectiveness of your current security controls.

Penetration testing provides internal and external testing. Internal testing involves assessing from inside a corporate network by mimicking an insider attack from a user who is authorised and has privilege to access. In external testing, the attacker will break through intrusion detection and firewalls to learn how an outsider could be able to enter and exploit the system after gaining access.

A penetration test can test all parts of your security program, including policy compliance and your ability to identify and respond to incidents. It goes beyond vulnerability scanning and provides more information to organizations on their security readiness. A pentester not only finds potential problems but also documents security training needs.

To find out more about how you can make penetration testing a part of your organizational security program, contact Aardwolf Security and talk to our security experts.