**Why Businesses Needs Penetration Testing Services**

Security breaches of high-profile businesses has continued to dominate headlines in the media in recent times. This increasing trend indicates increased security risk for businesses, whether small or big. As they grow in complexity and operations, malicious hackers also develop sophisticated ways of attacks. It’s no more a time where you install anti-virus software and firewalls and assume your business to be safe. a Businesses now need to test how resistant or vulnerable they are to cyber threats and likewise build effective mechanism and remediation strategy.

In order to find out how vulnerable your system is and how any malicious cybercriminal can get unauthorized access, you need to hire the services of a professional penetration testing consultancy.

If you are still not convinced, let’s looks at some of the reasons why penetration testing is vital for your organization’s security health.

**Penetration Testing Exposes Hidden Vulnerabilities Before the Hackers Do**

Perhaps the best way to check your security level is to study how your system can be hacked. Penetration testing offers ability to test how resistant your system is to hacking attempts. It simulates the actions of potential hacker by exploiting vulnerabilities that result from software bugs, code mistakes, service configuration error or insecure settings. The only difference between penetration testing and real hacking is that it is performed in a safe and controlled environment.

**Saves Remedial Cost and Reduces Downtime**

If your business actually goes through a security breach, it will cost you severe financial and reputational damage. According to a [recent report](https://safeatlast.co/blog/data-breach-statistics/), an average data breach in 2018 costed $3.86 million globally, which was 6.4% more than its previous year. Businesses require substantial amount of investment to get things back on track along with weeks or months to recover from its loss. Penetration testing amounts to lesser financial investment to identify your security loopholes as compared to larger losses and recovery costs incurred after a breach.

**Enables Security Regulations Compliance**

Regular penetration testing also helps businesses achieve compliance with security standards such as PCI DSS, ISO 27001 and HIPAA. Compliance not only ensures that a business is following best security practices but also rules out the chances of incurring heavy fines due to non-compliance.

**Ensures Customer Loyalty and Good Reputation**

Security attacks can compromise your customer’s sensitive data and result in disgruntled customers who may not trust doing business with you again. Penetration testing helps avoid costly data breaches that can put your customer’s loyalty and organization’s reputation at stake.

For these reasons, it’s important that businesses get regular penetration testing services to showcase how vulnerable their IT infrastructure is. Moreover, penetration testing can help prioritize security, comply with regulations and develop defensive mechanisms.