RISK REDUCTION THROUGH PENETRATION TESTING

Real World Attacks Let You Plan for the Unexpected

Reduce the chances of a successful attack

COMMON REASONS TO GET A PENETRATION TEST

ANNUAL COMPLIANCE REQUIREMENTS

An annual penetration test and report is a sign of a mature Information Security Program. PCI, FERPA, HITECH, FISMA, SOX, GLBA, FACTA, and GDPR are just some of the regulatory requirements that require a penetration test.

RISK REDUCTION

A comprehensive vulnerability review and ethical hacking report helps identify weaknesses that could lead to a data breach. The team at Cyber Security Services will help prioritize remediation efforts. The reduction of risk to the organization is often the driving force behind a penetration test.

PRIORITIZATION OF VULNERABILIITES

Our team of experts will create a report and assist with the remediation of the holes identified. We will meet as many times as it is needed to make sure the vulnerabilities have been fixed.

PREVENTION OF A DATA BREACH

The goal is to identify high risk concerns that could lead to a costly data breach. This gives your organization time to fix the concern before it becomes a serious problem.

Internal Network Penetration Testing

Application Penetration Testing

Wireless Penetration Testing

External Network Penetration Testing

More Information: **1-800-390-1053**
www.CyberSecurityServices.com/Penetration-Testing

Penetration Testing Options for the Enterprise

Internal Network Penetration Test

Our ethical hackers and security experts review from the perspective of an inside attacker. This is a weakness that attackers are increasingly exploiting at organizations across the globe. The chances of an internal employee with malicious intentions or an unwanted guest gaining access to the corporate network is higher than many would think. The internal network penetration test may also provide insights into the risk of ransomware or other malicious programs from bringing down your systems. There have been instances of healthcare organizations and banks being down for days due to a vulnerable system. The internal network penetration test will assist in identifying those holes and put your organization on track to fixing them.

External Network Penetration Test

The easiest way for an attacker to gain access to a network is through servers or network equipment that are exposed to the internet. The systems that are exposed to the internet will be hit daily with attack attempts simply for being on your network. The external penetration testing team will help identify the most likely entry points so that they can be fixed before there is a successful attack.

Application Penetration Test

Applications are a high valued target for hackers and identity thieves. The penetration test will focus on applications that are critical to your business operations. A successful hack of an application can often lead to personally identifiable information or other sensitive data stored in a database. An application penetration test takes the skills of a developer and a hacker to identify weaknesses. Our experts will identify the problem areas and help resolve them using a cost-effective approach.

Wireless Penetration Test

A wireless network is very convenient to organizations. It is also very convenient to those seeking to do harm. The wireless penetration test will look at ways that your wireless network can be exploited. We will also guide the team on how to fix those vulnerabilities. Cyber Security Services has experts in a variety of wireless technologies so that we can create a project plan for any concerns identified during the assessment.

Social Engineering Tests

Social Engineering remains the easiest way for hackers and identity thieves to gain access to sensitive information. The social engineering expert will take advantage of the human elements of the organization. The goal is to determine how well employees are trained on information security best practices.