PARM CYBER SOLUTIONS | PENETRATION TESTS

Proactively identify and mitigate potential litigated situations. Expertly manage claims towards a positive outcome.

MODERN CYBER THREAT LANDSCAPE

With the evolving landscape of cybersecurity and the ever-increasing sophistication of cyber threats, traditional defensive measures and post-event mitigation strategies are no longer sufficient. In order to avoid the high financial, reputational, and legal costs of cyber attacks, organizations must now adopt a proactive approach to cyber risk management. By using PARM's advanced penetration test services, organizations can now successfully identify the weaknesses of their systems, both technological and human, and efficiently address those vulnerabilities.

TECHNOLOGICAL PENETRATION TESTS

The penetration test or pen test allows business owners to determine if their organization is able to withstand cyber attacks and evaluate the resilience of their key business processes. Conducting a pen test significantly reduces the risk of incurring real damages from the actions of cybercriminals. The pen test can be thought of as being a professional, controlled ethical hacker attack. After the test is conducted, customers can be provided with a detailed report of all the weaknesses of their information systems and recommendations for their elimination, with tips on improving the overall security of business-critical systems.

SOCIAL ENGINEERING PENETRATION TESTS

In recent years, attacks that leverage social engineering have become increasingly popular, with the majority of cyber espionage attacks starting with a phishing e-mail. As a result of a successful attack, attackers can gain control of the organization's workstations. This in turn allows them to access confidential documents, use the infected machines to launch attacks on the systems of other companies, transfer funds, and so on. In an effort to counter this threat, our penetration tests also include advanced social engineering testing.

This allows business owners to evaluate the level of awareness and knowledge of their personnel on cyber threats and information security. The results can help identify the main weaknesses and areas of concern, with recommendations on how to fix them. This can then provide the basis for the development of security awareness programs focused on the areas of concern identified during testing.

Our penetration test services follow a simple 4-step methodology:

1 - Risk Study & Audit Plan Preparation

Our specialists work in collaboration with the customer to make a list of the critical parts of the information system and determine the test plan.

2 - Testing

All of the selected nodes of the system are scanned for vulnerabilities. Social engineering vulnerability testing is conducted. Every stage of the work is documented in detail and entered into the record.

3 - Reports & Recommendations

The customer receives a report with the list of found weaknesses grouped by severity, with a list of recommendations to address the vulnerabilities that were found.

4 - Systems Recheck

Once the vulnerabilities have been addressed, another test is conducted to verify the quality of the work performed.

BENEFITS

- Identify security gaps
- Ensure business continuity and resilience
- Assess your employees' level of cyber risk awareness
- Protect your company's brand and reputation

PROACTIVE RISK MANAGEMENT

PARM

ProActive Risk Management (PARM) is a leading global provider of enterprise risk management and security services. By taking an integrated approach to risk management and by recruiting the security industry's top talent, PARM has positioned itself as its clients' trusted vulnerability partner, providing an unmatched level of service based on its patented Five Dimensions of Risk Management.