Mindtree

Welcome to possible

Vulnerability assessment and penetration testing service.

Business challenges

- Did you know that the number of vulnerabilities in your operating systems and applications are extremely high?
- Did you know that unattended vulnerabilities will expose your company to data leakage / theft and can result in costly down time due to malicious attacks?
- Is it possible to identify these vulnerabilities periodically and patch them to avoid being attacked by hackers?
- Is there a way to attempt penetration into my network and applications in a controlled manner to identify weaknesses in my security architecture and Information Security Management System (ISMS)?

All applications and operating systems have in-built vulnerabilities due to improper development of their software code. These vulnerabilities can be used by hackers to launch attacks on the network, websites and servers of enterprises. Such attacks can result in costly downtime, theft of proprietary information and loss of customer data. This can result in loss of image among customers as well as costly lawsuits filed by customers or regulatory agencies. It is important for enterprises to periodically assess these vulnerabilities and patch them to avoid such attacks.

Our offering

Hackers are getting bolder and more creative in the way they attempt to penetrate the networks and websites of enterprises. Survey data has consistently proved that around 70% of such attacks are from disgruntled or malicious employees. Therefore it is very important for enterprises to test the robustness of their security infrastructure (the firewall policies, type of IDS etc.) and their Information Security Management System (the password policy, privileges given to employees to access various systems etc.). This is done through periodic 'penetration testing' exercises and action taken on any gaps and weaknesses unearthed.

Key benefits

- Proactive early warning security intelligence with respect to vulnerabilities thereby preventing unnecessary and expensive downtime and data theft
- Helps meet regulatory and compliance requirements
- Trusted advisory services provided with our service helps your organization be future-ready in preventing attacks
- Customized reports provide comprehensive information to help you take both strategic and tactical decisions

Mindtree's 'Vulnerability Assessment and Penetration Testing' service uses a combination of state-of-art tools like Accunetix WVS, Metasploit Pro, Nessus Professional, Backtrack etc, and experienced ethical hackers with appropriate certifications like CEH. It helps enterprises conduct intelligent 'Vulnerability Assessments' and 'Penetration Tests'. Our ethical hackers have many years of experience in this field and have exposure to a wide range of industry verticals and operating systems, applications, networks and security devices. They are selected after stringent background checks and their expertise is used to help our customers identify and take action on vulnerabilities and weaknesses in their IT assets and Information Security Management System (ISMS). They can conduct black box, gray box and white hat penetration tests to help customers improve their security infrastructure and information security policies. Mindtree delivers this service through our ISO 27001 certified cyber lab as well as by deputing our consultants to customer offices. Mindtree also helps customers patch the vulnerabilities unearthed by our consultants.

With the aid of tools used, we provide insightful reports to the top management as well as the IT operations staff of the enterprise. This will help them take both strategic and tactical decisions to make their Information Security Management System (ISMS) future-ready.

About Mindtree

Mindtree is a global information technology solutions company with revenues of over USD 400 million. Our team of 11,000 experts engineer meaningful technology solutions to help businesses and societies flourish. We enable our customers achieve competitive advantage through flexible and global delivery models, agile methodologies and expert frameworks.