IT firm's global infrastructure

Task Title	Penetration testing of an IT firm's global infrastructure
Industry Vertical	Information Technology (Software development)
Industry Details	• IT firm developing business process management software products • Global customer base • Multiple office locations • Geographically dispersed servers
Location	Pune (India)
Time to solution	1.5 month

Business Situation

The IT Company in the case, provides .Net and Java based application products to multiple customers globally. Deployments of the sold products happen over internet. Besides this, the IT firm has multiple locations where the servers are deployed for quick and easy deployment of software to their clients. For example, the USA customers connect to servers in Boston, while those in India connect to Pune servers.

IT firm wanted to perform detailed network penetration test on their USA and India infrastructure. The concern was to ensure no data leak protection happened, while USA and India offices connected to each other for daily work purposes.

Another purpose was to ensure that the product deployment infrastructurecould withstand a denial of service attack. SecMyIT was approached to perform tests andprovide technology design consultancy to achieve better cyber security practices

SecMyIT's Solution

- SecMyIT had a kickoff meeting with firm's CEO and IT manager to define testing scope.
- An internal testing of network infrastructure, proxy servers, internet connectivity, and server access was suggested. An external testing in a black hat mode was suggested for deployment infrastructure.
- After performing reconnaissance, a series of internal network test to capture L2-L3 attacks were
- performed. This was followed by a series of tests such as, trying to decipher windows passwords on the fly, download spyware, download files from internet which were supposed to be blocked by network policies, disable anti-virus etc.
- A non-intrusive internal test was performed to ensure that firewalls at USA and India ends were
- configured properly.
- A separate destructive denial of service test was performed on the deployment infrastructure. An
- elaborate ethical hacking attempt was performed too, to ensure perimeter defense is adequate, and only the online services required for deployment functionality purpose and available and secure.
- A lite-pen-test on the deployment network infrastructure was performed too, to ensure external and internal security on that infrastructure

- A report with all severity 1, 2, 3 vulnerabilities and the corresponding suggestions to fix, was created.
- IT firm's tech management was informed about maintaining the confidentiality of the report
- Based on the vulnerabilities found, a cyber security design change was suggested.
- After concluding the test and signing the reports, SecMyIT acted as security consultants to the IT firm for upcoming months. The tasks performed were patch management system re-design,antivirus product deployment, deployment infrastructure security revamp etc.

Benefits

- IT firm's management could roll out more product securely, using revamped deployment
- infrastructure, which helped them gain confidence for future such plans.
- IT firm could secure business contracts with firms in Europe due to the fact that the infrastructure was certified for cyber security and met international standards
- As an outcome of penetration test, vulnerabilities resulting into data leak were found, and fixed by
- deploying appropriate IT policies and software checks. This helped IT firm achieve a better internal security.

Learn More About us at :
www.secmyit.com

For Further Information, Please Contact
contact@secmyit.com