WIDE ANGLE

INFORMATION SECURITY AND RISK MANAGEMENT

Powered by **NTT Com Security**

Four steps to successful penetration testing

In cyberspace, the more connected your business is, the more attackers will be looking for ways to access your data. It's essential that you test your network regularly to discover potential weaknesses before anyone else does. A penetration test – a hands-on test that includes exploitation of vulnerabilities within a system or company – is one of the most effective ways to do this.

Security consultants are often called in when a system is about to go live, or in the event of a breach, but if you find critical security issues that late in the day there's little time to action the results of the test. You either have to start again, or cross your fingers and hope for the best. Organizations that use penetration testing as a proactive exercise to highlight risks can not only secure budget, but also change development cultures by demonstrating the value of building security into systems and applications early on.

Whether you are thinking about implementing a security testing program for the first time or are looking to make the most of your existing penetration testing, there are four steps you should take to get the most from your investment.

1 Plan

- Security needs to be integrated into everything you do. The sooner security considerations are factored into a project plan, the less costly it will be, for example, developers should include security at the design phase
- Engage external experts regularly – it's difficult to be objective if you are responsible for both configuring and maintaining the security infrastructure in your workplace, as well as validating and reporting on its effectiveness
- Establish the information you need before you start and how you want it packaged – results must be actionable so that remediation can be continuously managed by the technical teams

2 Maintain

- Penetration testing should be done regularly – after each upgrade or significant change to the network and infrastructure – and follow a structured plan
- Feed the results into your continuous testing program, reducing both the impact and likelihood of a breach by prioritizing the defensive steps necessary to protect your organization

3 Follow through

- The test report should include an executive summary showing the risks the organization faces, as well as an evaluation of the consequences and recommended improvements
- The results of the penetration test should feed back into and help to reevaluate the state of your risk assessment process. This will help you determine if your potential risk is acceptable or unacceptable based on your own expected losses
- Risk should be related to your business – just because something is high risk in one industry does not mean it has the same implications for your organization
- Consider all suggestions on how to improve your security and prioritize the most urgent changes
- Investigate the background to the specific risks you face – the how, where and why – through a root cause analysis

4 Other considerations

- Penetration testing is not just about the network and applications. Don't forget staff awareness and physical security; people and processes should be evaluated too. An organization can have everything on the perimeter perfectly configured and every tool working, but if an employee clicks on a link in a phishing email, that investment is wasted

A penetration test requires skilled individuals with knowledge of networking, development, and in some cases psychology. Our penetration testing experts will provide you with an evidence-based picture of relevant vulnerabilities and associated risks. Armed with this valuable insight, you can prioritize the defensive steps required to protect your business.

Questions?

Don't let attackers exploit the risks in your organization's online presence, customer transactions, employee productivity or partner communications.

Contact us to find out more about our WideAngle Penetration Testing Services, or visit our penetration testing page.

NTT Communications | NTT Com Security

www.nttcomsecurity.com