IT 365

BEST PRACTICE GUIDE

Penetration Testing

...a vital component in your IT security toolkit

Your organisation wants assurance that its digital data is protected against cybercriminals. Penetration testing helps provide this assurance by actively demonstrating the quality of your digital security perimeter.

MAKE PENETRATION TESTING PART OF YOUR DIGITAL SECURITY STRATEGY

Cybercriminals don't play by the rules. They'll exploit every system weakness and play every trick they need to in order to get to what they want – which is usually valuable business data.

Conducting a penetration test (also known as a 'pen test') means playing a similar game. For this reason, penetration testing is most effective when carried out by someone outside your organisation. They don't think in line with your internal rules and culture, making them more creative in their attempts to break through your perimeter and endpoint security.

The primary purpose of penetration testing is to demonstrate the strength of your IT security measures. However, the test process may throw light on areas of weakness in your digital security setup. It's essential these weaknesses are documented and quantified, and the appropriate remedial action taken.

It's important that any penetration testing is part of a wider digital security strategy. While these tests may reveal weaknesses in endpoint or perimeter security, they cannot be relied upon to identify every possible flaw.

To be effective, penetration testing should be carried out on your live IT systems. It should also be carefully controlled and lead to a comprehensive report of issues tested and the outcomes.

ANSWERS TO COMMON QUESTIONS ABOUT PENETRATION TESTING

What size of business should consider using penetration testing?

No business is too small to attract the attention of cybercriminals, and smaller businesses are often targeted because it's assumed their security measures will be weaker.

In what areas is penetration testing particularly effective?

Because penetration testing targets your entire security system, rather than specific apps, it can test for weaknesses that occur at the point where two or more systems interact. These weaknesses may not be picked up by functional tests of each individual app.

What risks are associated with penetration testing?

The nature of the testing, which means emulating tactics adopted by hackers, could result in issues with your internal systems such as data corruption, exposure of secure data or server crashes. For these reasons, penetration testing should be carried out with great care.

Should employees be aware penetration testing is taking place?

For tests to be effective, they should be carried out under realistic conditions. Employees should be given no more than their usual warning about the risks from cybercriminals.

HOW WE CAN HELP YOU WITH PENETRATION TESTING AND DIGITAL SECURITY

We have helped many firms implement and test robust perimeter and endpoint security strategies and systems. We have also worked with organisations whose security has been breached, usually as a result of human error. This adds up to considerable experience in helping firms protect their data and IT systems from cybercriminals.

To find out more about how we can help your business better protect itself against cybercriminals, give us a call on 0345 051 0600 or email enquiries@itsupport365.co.uk. We would be pleased to have a no-obligation conversation with you. Alternatively, follow us as we share news updates and information on Twitter, Facebook and LinkedIn.

A comprehensive digital security strategy isn't an optional extra in today's connected world. Every day thousands of UK companies suffer digital attacks and while many don't succeed, it only takes one hacker to break through to create a serious problem for your business.