mitie

SECURITY

Make Better Security Decisions

The Impact of Penetration Testing & Live Exercises

Penetration testing

What is it? And why you need it

Penetration testing, also known as Unauthorised Access Testing, is simply the process of testing your security protocols to identify any weaknesses in your physical security. To conduct the test, an individual must analyse your security, plan their 'attack' and attempt to exploit any weaknesses that are identified.

There are many reasons for carrying out penetration tests at your locations. Primarily, they allow you to identify flaws in your physical security. By deliberately exploiting these weaknesses, the test highlights ways in which the security could be improved in future to prevent malicious attacks that would look to exploit the same area.

The testing can also be used to identify the level of real-world risk to your organisation, showing how susceptible the location is to an intrusion.

The tests can do more than just show weakness however. Tests can prove just as useful if the intruder fails in their attempt, as this can provide assurances to staff and management that the existing controls are as effective as possible at stopping unauthorised access occurring. Testing is also a great way of motivating the teams on the ground at the location, by motivating them and keeping them on-point by testing their skills. Alternatively, it can also identify any issues in staff attitude or appearance should they be cause for concern.

Penetration tests don't just identify weaknesses, they motivate teams and hone staff skills

Implementing other live exercises

Live exercising is the process of testing a security teams' procedures and performance in the response to a risk or threat. Live exercises can provide invaluable intelligence that can help you identify gaps in your security, or processes that can be made more effective or efficient.

There are a wide variety of potential live exercises you can conduct at your locations, for example suspicious packages, protest action, or terror related incidents. Any that are undertaken should be based on your unique risk profile and the most appropriate potential risks and threats you face. If you are based in a city, for example, conducting live exercises based on dealing with protest action may be appropriate as there is an increased likelihood these events would impact your business.

Live exercising delivers actionable intelligence to analyse and enhance your security

Conducting live exercises keeps your team well trained in the latest processes and breeds confidence throughout the team that in the event of an incident they are well placed to manage it effectively and minimise the risks to your business. They also provide a fantastic platform to assess your security staff and identify high performing individuals.

Identifying The Risks

To successfully conduct penetration tests and live exercises, we must have a clear understanding of what is at the location, and why someone might attempt to gain access or cause harm.

One of the main assets being protected at a location, is your people. All staff, contractors and site visitors are under the protection of your security team, so they must be able to prevent unauthorised access and incidents to prevent harm coming to any individual on site. It must also come into consideration that the target may well be someone on site, and not necessarily assets with a monetary value. As well as people, intruders may be targeting property, anything from supplies to equipment used at the facility.

We must also remember that knowledge is power, which makes information a popular target. Documents, intellectual property, customer details and more, are all assets which can prove to be lucrative should they fall into the wrong hands. Anywhere on site that holds sensitive business data must be strongly analysed in the security process to ensure sufficient measures are taken to protect it. Finally, you must consider the reputational risk should an intruder manage to get into your location. Even if they do not harm anyone or take anything of value,

their mere presence is cause enough for concern as it may identify to others that the location has flaws and could cause immeasurable brand damage.

Once we have identified the key areas that may require specific security solutions, we must identify the likely source of the threat, so that a test can be conducted as true to life as possible, for example, an office environment is less likely to be the target of terrorists but may be a target for petty thieves.

The threat can come from numerous places, but commonly we can group these as; petty criminals, kids, protesters, urban explorers, 'insiders', organised criminals, industrial spies and terrorists. To conduct the most useful test, we must conduct some analysis of the location and identify what group poses the biggest threat.

Be proportional to your risk when planning a test. Make sure the intrusion type is **relevant to your location**

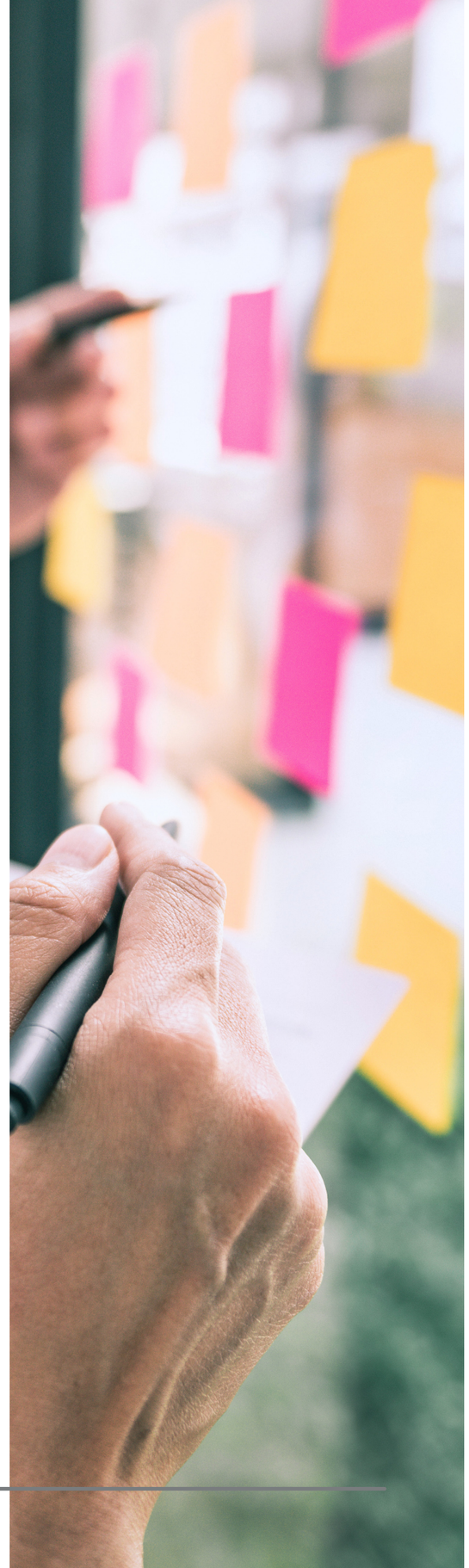
Preparing for the test

There are numerous stages in conducting a penetration test or other live exercise, but all must start with detailed preparation for both the business and those conducting the test or exercise. Firstly, all parties must be clear on what site is to be targeted with the test, it is a simple step, but confusion over the correct location can mean wasted time and resource.

Once the location is set, the scope of the test must be agreed. With a penetration test, how far should the tester go? Is it simply enough to gain access to the premises or should an item be taken? For a live exercise, what constitutes the end of the exercise?

When deciding on the scope of the test, it is important to ensure that whatever activity is agreed it will not bring harm to any individual or asset.

Finally, the penetration tester must have an agreed point of contact on the targeted premises. This person should be known to the front-line security team. In addition to a point of contact, it is important the tester has a form of written confirmation regarding the test and explaining who they are, as well as photo identification in case the security team succeed in preventing the intrusion and the tester needs to prove their credentials to the security team. If conducting a different form of live exercise, it is vital that all necessary teams are fully briefed on the scenario and that whatever the exercise is, no individuals come to harm.



Utilising the outcome of the test

After every test or exercise it's important to have a debrief and provide value to the security team on the ground. The intelligence gathered from these tests can prove to be invaluable in improving security protocols.

It's important not to be overly negative in the report, and uncontrollable factors that aided in the success of the test must be taken into consideration. The aim of the report is to provide intelligence that highlights areas for improvement in the security, including any previously unidentified flaws in the current procedures.

Intelligence from testing is invaluable when evaluating your security

Once the report and debrief have been concluded, it is important to use the intelligence to improve the service your security team provides. If the test has identified weaknesses or flaws in the current procedures, it is important to devise a solution to ensure that potential intruders with malicious intent cannot exploit the location in the same way as the tester, or that incidents similar to the exercise can be effectively managed.

However, if the entry attempt was unsuccessful and the security team prevented the intrusion, or the exercise was dealt with in an appropriate manner, the team should receive the appropriate praise for their work. It is important to highlight any areas in which they excelled to ensure that best practice is maintained in future.

Once any remedial changes to processes have been implemented, it is worth considering conducting a new penetration test or live exercise to ensure that the new measures adequately meet your needs and to check that new processes and procedures put in place to rectify previous issues have not negatively impacted another area of the security service.

Always implement the outcomes of testing to improve your security

Stay ahead with penetration testing and live exercising

Penetration testing and live exercising are vital tools in a security teams' armoury, as they identify areas to improve but can also provide peace of mind that current measures in place are adequate for the location. However, it is important to remember that penetration testing and live exercising are not static. Tests and exercises should be conducted on a regular basis as processes can change, which can allow for new weaknesses to be exploited. It keeps the skills of the security team honed, and with constant change in technology and available information, new risks and threats could be posed to your business.

With a professional stance on penetration testing and live exercising, you can minimise the risks to your people, assets and environments and continually improve your security service.

Tests and exercises should be conducted on a regular basis as processes can change, which can allow for new weaknesses to be exploited

mitie

SECURITY

Want to learn more about penetration testing and live exercising?

Phone: 0330 678 0710
Email: alwaysprepared@mitie.com
Website: www.mitie.com/security
Twitter: @MitieSecurity