Jisc penetration testing service
Legitimate interests assessment
Conducted 30/04/18

Jisc’s penetration testing service allows customer organisations to have the security of key systems tested using techniques – both technical and human – likely to be used by hostile attackers. By fixing the vulnerabilities found by testers, organisations can reduce the likelihood of them being used by attackers to gain access to those systems and the personal data they hold and have access to.

The service is designed for systems – such as human resources, virtual learning environments, finance, email and remote access – that process large amounts of personal data about all, or many, of the organisation’s staff and students. Improving the security of those systems is therefore a significant benefit to all those individuals as well as to the organisation itself.

Personal data processed

A penetration test may involve processing personal data in two ways. If the customer has requested a social engineering component, then a small number of individuals will be contacted to attempt to persuade them to disclose passwords or other information that would help an attacker. If a social or technical test succeeds, this may result in the tester gaining access to personal data held by the vulnerable system. Both activities are essential to the purpose of the test, but both are conducted in ways, and within processes and policies, that minimise the risk of harm.

Targets of social engineering tests clearly cannot be informed in advance, as this would defeat the purpose of the processing. Data about them will only be taken from public sources, or information generally available within their organisation. No special category data is used. Where individuals were victims of the social engineering activity, their names, the technique and the information they disclosed will be provided to the customer organisation in confidence. The organisation is expected to contact these individuals promptly to provide both information and training to reduce the security risk that the test discovered.

Safeguards

If access to personal data is achieved by the tester, the customer organisation is immediately informed to enable it to secure the data against unauthorised access by others. The organisation is offered the choice whether to stop the test, or to continue according to the agreed plan. The data are saved to a password-protected, encrypted device in case the customer needs them either as evidence or for further internal investigation. Once the customer has accepted the final report – which contains only a summary of the types of data found – the data are securely deleted.
To minimise risks, an initial scoping discussion agrees details of the systems to be targeted, ensuring that the site is aware of – and has plans to address – any security vulnerability or breach that may be found. To reduce the risk to confidentiality, both Jisc staff and those at the customer organisation to whom they report are bound by contracts including confidentiality clauses. To minimise risks to availability and integrity, Jisc recommends running the test against cloned copies of the target systems, rather than against live services.

Jisc requires the customer organisation to authorise the test in writing to ensure there is no breach of the Computer Misuse Act 1990 or, if the customer organisation authorises the use of interception during the test, the Investigatory Powers Act 2016. As part of the scoping discussion the customer must disclose any areas (e.g. IP address ranges for BYOD or eduroam) where personal devices may be present: these will be excluded from the test, as the organisation cannot lawfully authorise access or interception. If software is run on any customer-managed device this will be solely to test whether passwords can be obtained: all other information will be deleted immediately.

At the conclusion of the test, Jisc will provide the customer organisation with a list of all non-public data that was accessed, all accounts whose credentials were accessible, and any alterations made to software, files or configurations. The organisation is expected to take appropriate measures (e.g. changing passwords on compromised accounts) to ensure that activities conducted as part of the test do not create a continuing security risk.

**Future actions**

The service may be subject to the future EU ePrivacy Regulation, currently being developed. The legal and technical arrangements should be reviewed when a final text is available: expected to be in late-2018 or 2019.

**Conclusion**

The purpose of a penetration test is to determine whether and how confidentiality can be breached. Having this done by authorised, external, individuals – within an agreement that provides contractual, process and technical safeguards – represents a lower risk than the same activity conducted by the organisation’s own staff, and a far lower risk than it being done by hostile attackers. There is a possible impact on the targets of the social engineering component of the test, since these may be upset either at having been chosen as targets or having fallen victim to the attack.

However, the process includes safeguards to minimise this impact and to help individuals and their organisations to benefit from it. The penetration test does therefore involve a limited risk to a small number of individuals, but organisations that improve their security using the test results, provide a much greater benefit to all their staff and students. We conclude that the processing of personal data involved is both necessary and proportionate and that the balancing test required of any processing serving a legitimate interest is satisfied.