Spillemyndigheden's Certification Programme

Requirements for penetration testing

SCP.04.00.EN.2.0

Table of contents

Table of contents 2
1 Objectives of the requirements for penetration testing 3
1.1 Scope of this document 3
1.2 Version 3
1.3 Applicability 4
2 Frequency and testing organisations 4
2.1 Penetration testing frequency 4
2.1.1 Initial penetration test 4
2.1.2 Renewed penetration test 4
2.1.2.1 Postponement of penetration test 4
2.2 Testing organisations 4
2.2.1 Requirements for testing organisations 5
2.2.2 Requirements for personnel who performs the penetration test 5
2.2.3 Requirements for personnel who assess and attest the result of the penetration test 5
3 Penetration testing framework 6
3.1 Objective of the penetration testing 6
3.2 Protected components 6
3.2.1 Updating software and hardware 6
4 Penetration Testing process 6
4.1 Standard report and plan for "not passed" penetration test 7

1 Objectives of the requirements for penetration testing

The requirements for penetration testing shall ensure, that the gambling system and business systems of the licence holder are tested for vulnerabilities, which possibly could be exploited to gain unauthorised access to e.g. sensitive information.

1.1 Scope of this document

There are requirements for how often a penetration test must be completed, and which testing organisations can perform penetration testing of the licence holders gambling system and business systems. These requirements are described in section 2 "Frequency and testing organisations".

The penetration test of the gambling system and business systems shall be conducted in a way that exposes vulnerabilities in components and whether these vulnerabilities can be exploited by unauthorised persons. Besides this the licence holder shall protect their systems in the possible way. These requirements are described section 3 "Penetration testing framework".

The Danish Gambling Authority specifies several scenarios, which shall be tested as part of the penetration test, and a process for when a test is not passed. These requirements are described in section 4 "Penetration testing process".

1.2 Version

The Danish Gambling Authority continuously revises the certification programme. The latest version and the version history are accessible at The Danish Gambling Authority's website.

Date	Version	Description
2014.07.04	1.0	A new document structure than the previous version 1.3 alongside with a range of updates in different areas. A new version 1.0 is therefore published. It is the intention to follow normal versioning for future changes.
2015.12.21	1.1	Extension of applicability to cover offering of lotteries and betting on horse- and dog races.
2020.01.01	1.2	Spillemyndigheden has removed the requirement saying the ATO's accreditation must refer to a specific version cf. section 2.2.
2023.01.01	2.0	Update of requirements for accredited testing organisations and staff. Clarification of requirements if penetration test is not passed. The section on use of an internal function to perform vulnerability scans and penetration tests has been removed. Furthermore, general adjustments and specifications have been made.

When a new version of the certification programme is released, The Danish Gambling Authority will, if necessary, publish guidelines for a transition period and validity of already completed penetration tests.

It must be emphasised that only the Danish version is legally binding. The English version holds the status of guidance only.

1.3 Applicability

Requirements for penetration testing is applicable for offering of:

- Online betting
- Land-based betting
- Online Casino
- Lotteries

2 Frequency and testing organisations

2.1 Penetration testing frequency

The licence holder is responsible for having a penetration test completed in accordance with the requirements in this document with an interval of maximum of 12 months.

2.1.1 Initial penetration test

The licence holder shall have a penetration test completed before a licence to offer games can be issued unless The Danish Gambling Authority has informed otherwise.

2.1.2 Renewed penetration test

The licence holder shall, as a rule, have completed a new penetration test within 12 months of the latest penetration test. The standard report shall reflect when the new penetration test was completed.

The standard report, which documents the renewed penetration test, shall be in the Danish Gambling Authority's possession no later than 2 months after the penetration test was completed.

2.1.2.1 Postponement of penetration test

The licence holder can choose to postpone the penetration test up to two months from the time where a new penetration test should have been completed. The new penetration test must be finalised no later than 14 months after the latest penetration test and the standard report must be submitted to The Danish Gambling Authority within the same deadline.

The Danish Gambling Authority must be notified before the penetration test is postponed.

The deadline for renewal of penetration test is shortened with the equally amount of time the former 12-month deadline was postponed. Meaning that if you for instance make use of the maximum two months postponement, then the next penetration test is due 10 months later. The expected time for the next penetration test shall reflect this and be noted in the standard report.

The option to postpone the penetration test only applies to the licence holder. This means that the option does not apply to any suppliers the licence holder may have.

2.2 Testing organisations

To ensure that the necessary qualifications are in place during the penetration test the testing organisation and their staff shall fulfil the requirements in this section.

2.2.1 Requirements for testing organisations

Testing organisations shall attain minimum one of the following accreditations/approvals:

- ISO/IEC 17025-accreditation with reference to Spillemyndighedens certification programme SCP.04.00.DK, or
- ISO/IEC 17065-accreditation with reference to Spillemyndighedens certification programme SCP.04.00.DK, or
- Approved Scanning Vendor (ASV) approval.

ISO-accreditation shall be done by DANAK (the Danish Accreditation Fund) or a similar accreditation body, who is co-signer of EA's (European co-operation for Accreditation) multilateral agreement on reciprocal recognition regarding testing, or for labs outside EA's jurisdiction, by an accreditation body, who is co-signer of ILAC's (the International Laboratory Accreditation Cooperation) multilateral agreement on reciprocal recognition regarding testing.

The ASV-approval is done by Payment Card Industry (PCI) Security Standards Council (SSC).

Documentation for the testing organisation's ISO-accreditation or ASV-approval shall be enclosed with the standard report. Alternatively, a link to the accreditation or approval can be provided in the standard report.

2.2.2 Requirements for personnel who performs the penetration test

The penetration test shall be performed by staff with sufficient qualifications, which means the testing organisation shall hire sufficiently qualified, competent, and experienced personnel.

2.2.3 Requirements for personnel who assess and attest the result of the penetration test

The result of the penetration test and any possible remediation of vulnerabilities shall be assessed and attested by one or more persons, who warrant(s) that the work has been carried out to adequate professional standards. These persons shall meet the following requirements:

a) Have at least five years of practical experience with penetration testing of systems, and
b) Have a personal certification, which demonstrates competence regarding penetration testing. It could for instance be one of the following:
    - Offensive Security Certified Professional (OSCP),
    - EC-Council: Certified Ethical Hacker (CEH), Licensed Penetration Tester Master (LPT Master),
    - Global Information Assurance Certification (GIAC): GIAC Certified Penetration Tester (GPEN), GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),
    - CREST Penetration Testing Certifications,
    - Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification,
    - Tiger Scheme: Senior Security Tester, Qualified Security Tester.

Guidance: Assessment and attesting can be carried out by e.g. two persons who in conjunction fulfil the requirements. Persons, who assess and attest, can participate in the penetration work cf. section 2.2 on supervision in SCP.00.00 General requirements.

3 Penetration testing framework

The Danish Gambling Authority's requirements for penetration testing is based experience in the area, recommendations from and dialogue with the industry.

3.1 Objective of the penetration testing

The purpose of penetration testing is to identify and seek to exploit any vulnerabilities in the licence holders gambling system and business systems.

3.2 Protected components

The gambling system and business systems in the licence holder's production environment shall be protected against any attacks from unauthorised persons. Particularly components containing sensitive information concerning customers shall be protected. The definition of components and their relevance shall be seen in context with The Danish Gambling Authority's Change Management Programme SCP.06.00.EN, section 3.3.3.

The licence holder can minimise the risk of unauthorised access by segmenting the internal networks including which sub-systems communicates sensitive information by public networks.

3.2.1 Updating software and hardware

It is the licence holder's responsibility, that system components are updated to a degree that ensures the highest level of security possible and does not compromise the integrity of the systems, so the risk of unauthorised access is minimised.

4 Penetration Testing process

With no more than 12 months interval the licence holder shall have a penetration test completed of their gambling system and business systems.

Guidance: 'Gambling system' and 'business system' are defined in the general requirements and cover both frontend, backend, datawarehouse and games regardless of these are operated by the licence holder or a supplier.

The penetration test shall cover, but not be limited to, any weaknesses uncovered during the vulnerability scanning, cf. The Danish Gambling Authority's requirements for vulnerability scanning SCP.05.00.DK.

The testing organisation shall furthermore seek to gain unauthorised access to the licence holder's gambling system and business systems. The unauthorised access shall be attempted escalated to the highest access level possible and completed with and without access credentials available (whitebox/blackbox). Through this access the following list of scenarios shall as a minimum be tested:

- Manipulation of result generation
- Affecting the execution of games
- Fraud with customer funds
- Theft of customer funds
- Manipulation of audit logs
- Access to sensitive information
- Manipulation of sensitive information
- Manipulation of data transfer to SAFE

4.1 Standard report and plan for "not passed" penetration test

In the standard report is must be stated whether the penetration test is passed, passed with remediation, or not passed.

'Passed' shall be used, when the penetration test is completed without finding any vulnerabilities; this includes suppliers.

'Passed after remediation' shall be used, when the penetration test has uncovered vulnerabilities, which have been remediated and a following test has shown, that the vulnerabilities are no longer present; this includes suppliers.

'Not passed' shall be used, if there are vulnerabilities in the licence holder's systems, which cannot be remediated before the deadline for submitting the report to the Danish Gambling Authority; this includes suppliers. In this situation an annex containing a plan for remediating the identified vulnerabilities and a description of compensating control measures, shall be submitted along with the standard report. The licence holder shall afterwards as soon as possible remediate the vulnerabilities and within 3 months have completed a new penetration test.

After the new penetration test, the licence holder shall submit documentation showing that vulnerabilities have been remediated.

In practise a 'not passed' report cannot be accepted by the Danish Gambling Authority, without the annex containing a plan for remediation and a description of compensating controls.

If a complete penetration test is performed of the gambling system and business systems after remediation of any vulnerabilities, the date of completion of this penetration will be the point of reference for determining the deadline for the next penetration test.