Spillemyndigheden's Certification Programme

Instructions on Penetration Testing

SCP.04.00.EN.1.2

Table of contents

Table of contents 2
1 Objectives of the Instructions on Penetration Testing 3
1.1 Scope of this document 3
1.2 Version 3
1.3 Applicability 3
2 Certification 4
2.1 Certification frequency 4
2.1.1 Initial certification 4
2.1.2 Renewed certification 4
2.2 Accredited testing organisations 4
2.2.1 Requirements for accredited testing organisations 5
2.2.2 Requirements for personnel at the accredited testing organisations 5
3 Penetration Testing Framework 5
3.1 Objective of the penetration testing 5
3.2 Protected components 6
3.3 Updating software and hardware 6
3.3.1 Component updates 6
3.3.2 Internal function with the licence holder 6
4 Penetration Testing Process 7

1 Objectives of the Instructions on Penetration Testing

The Instructions on Penetration Testing seeks to ensure that the gambling system and business systems of the licence holder are tested for vulnerabilities that could be exploited to gain access to sensitive information.

1.1 Scope of this document

This document contains the requirements specifying how testing organisations obtain accreditation for conducting certification of the gambling system, business processes and business systems of the licence holder as well as instructions on how to conduct the certification. The requirements concerning accreditation of the testing organisation and certification of the licence holder can be found in section 2 "certification".

The Penetration Test shall be conducted in such a way that exposes vulnerabilities in components. This is particularly relevant during system upgrades and updates. These requirements are set out in section 3 "Penetration Testing Framework".

Spillemyndigheden specify a number of mandatory penetration scenarios. These scenarios are set out in section 4 "Penetration Testing Process".

1.2 Version

Spillemyndigheden will continuously revise the certification programme, making the latest version and the version history accessible at Spillemyndigheden's website: https://spillemyndigheden.dk/en/certification-programme

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.

Spillemyndigheden will publish guidelines regarding the validation of existing certifications together with previously performed inspections and tests, when new versions of the certification programme is released.

It is important to emphasise that only the Danish version is legally binding and that the English version holds the status of guidance only.

1.3 Applicability

Instructions on penetration testing is applicable for offering of:

- Online betting

- Land-based betting
- Online Casino
- Lotteries

2 Certification

2.1 Certification frequency

The licence holder is responsible to ensure to be certified in accordance with the requirements in this document with an interval of maximum of 12 months.

2.1.1 Initial certification

The licence holder must, as a rule, be certified before a licence to offer games can be issued, unless Spillemyndigheden has informed otherwise.

2.1.2 Renewed certification

The licence holder must, as a rule, have completed a new certification within 12 months of the latest certification. The standard report must reflect, when the certification has been renewed.

The licence holder can choose to postpone the certification up to two months from the time where a new certification should have been completed. The new certification must be finalised no later than 14 months after the latest certification and the standard report must be submitted to Spillemyndigheden within the same deadline. Use of this postponement requires that the testing is commenced within 12 months of the latest certification.

Spillemyndigheden must be notified before the certication is postponed.

The deadline for renewal of certification is shortened with the equally amount of time the former 12 month deadline has been postponed. Meaning that if you for instance make use of the maximum two months postponement, then the next certification is due 10 months later. The time for the next certification shall be reflected in the standard report.

2.2 Accredited testing organisations

Testing organisations shall attain ISO/IEC 17020 accreditation and/or ISO/IEC 17025 accreditation based on the criteria described in the following sections. 'Spillemyndigheden's certification programme – SCP.04.00.DK' must appear from the accreditation scope.

The accreditation will be undertaken by DANAK, the Danish Accreditation and Metrology Fund, or a similar accreditation body being covered by the multilateral agreement on reciprocal recognition of the European Co-operation for Accreditation or a member of the International Laboratory Accreditation Cooperation.

To ensure that the necessary qualifications are in place during the certification the testing organisation and their staff shall fulfil the following requirements. Documentation that the requirements are fulfilled shall be enclosed with the certification.

2.2.1 Requirements for accredited testing organisations

The accrediting testing organisation:

a) Shall have at least two years' experience in penetration testing of systems or a similar closely related subject area,

b) Shall be accredited as Payment Card Industry (PCI) Approved Scanning Vendor (ASV),
c) Shall work on the basis of the ISO/IEC 17020 accreditation and/or ISO/IEC 17025 accreditation, which refers to the requirements of SCP.04.00.DK, and
d) Shall ensure that staff with sufficient qualifications will carry through the certification.

2.2.2 Requirements for personnel at the accredited testing organisations

The certification shall be carried through by staff with sufficient qualifications cf. sections 2.6.1 above. Work done in relation to the certification shall be supervised and the declaration of certification shall be 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) Five years of professional experience in penetration testing of systems or a similar closely related subject area, and
b) Shall be certified as:
    - International Council of E-Commerce (EC-Council) Certified Ethical Hacker (CEH),
    - International Council of E-Commerce (EC-Council) Licensed Penetration Tester (LPT),
    - Information Assurance Certification Review Board (IACRB) Certified Penetration Tester (CPT),
    - Global Information Assurance Certification (GIAC) Certified Penetration Tester (GPEN),
    - CESG CHECK Team Leader,
    - CESG CHECK Team Member,
    - CREST Infrastructure Certification,
    - CREST Registered Tester,
    - Tiger Scheme Senior Security Tester,
    - Tiger Scheme Qualified Security Tester, or
    - Offensive Security Certified Professional (OSCP).

Guidance: Testing, supervision and attestation can be carried out by staff who in conjunction fulfil the requirements.

3 Penetration Testing Framework

Spillemyndigheden's Instructions on Penetration Testing is in part inspired by Payment Card Industry – Data Security Standard (PCI-DSS).

3.1 Objective of the penetration testing

When performing penetration testing the accredited testing organisation shall seek to exploit any vulnerabilities in the licence holders gambling system. The penetration test should cover but not be limited to the weaknesses uncovered during the vulnerability scanning, cf. Spillemyndighedens Instructions on Vulnerability Scanning SCP.05.00.EN.

3.2 Protected components

The gambling system and business systems in the licence holder's production environment shall be protected against any attack from outsiders. The components containing sensitive information concerning customers in particular shall be protected. The definition of components and their relevance follows from Spillemyndigheden'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.

3.3 Updating software and hardware

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

3.3.1 Component updates

In the event of an update of components of the licence holder or a supplier, a new vulnerability test must be conducted to ensure that the systems integrity remains intact.

Penetration testing is necessary after significant up-dates or changes to infrastructure or the use of it (for example any installation of new system components, addition of a sub-network or addition of a web server), in the case where the vulnerability scan has elements that score 4 or higher on the NVD CVSS scale. What will be considered to be "significant" changes will depend to a high degree on the set-up of a given environment and therefore it cannot be defined as such by Spillemyndigheden. It is, however, always considered significant if an upgrade or a change is capable of affecting or providing access to sensitive information and/or components cf. Spillemyndigheden's Change Management Programme SCP.06.00.EN, section 3.3.3.

3.3.2 Internal function with the licence holder

The accredited testing organisation can allow that penetration testing as described in section 3.3.1 is conducted by a dedicated internal function at the licence holder undertaking penetration testing of the systems. This function shall be manned with appropriately skilled staff as well as being organisationally separated from the function implementing system changes.

If the penetration testing is conducted by an internal function at the licence holder, the accredited testing organisation shall assess, approve and certify these tests every three months. The standard report shall clearly state whether this method has been used.

This option is only available to licence holders. The option cannot be used by suppliers without an individual licence to offer gambling in Denmark.

4 Penetration Testing Process

When performing penetration testing the accredited testing organisation shall seek unauthorised access to the systems of the licence holder. 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 minimum list of scenarios shall 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