Spillemyndigheden's Certification Programme

Instructions on Vulnerability Scanning

SCP.05.00.EN.1.1

Table of contents

1 Objectives of the Instructions on Vulnerability Scanning

The Instructions on Penetration Testing seeks to ensure that the gambling system and business systems of the licence holder are scanned 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 vulnerability scan of the gambling system and business systems 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 "Vulnerability Scanning Framework".

Spillemyndigheden propose a methodology for vulnerability scanning. This methodology is set out in section 4 "vulnerability Scanning 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.

If the certification programme is modified, as a rule, certifications already issued will remain in force.

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 vulnerability scanning 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 3 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 3 months of the latest certification. The standard report must reflect, when the certification has been renewed.

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. The scope of the accreditation shall be extended to include 'Spillemyndigheden's certification programme – SCP.05.00.EN.1.'.

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 vulnerability scanning 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.05.00.EN.1., 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 vulnerability scanning 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, eller
- Tiger Scheme Qualified Security Tester.

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

3 Vulnerability Scanning Framework

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

3.1 Objective of the vulnerability scanning

When performing vulnerability scanning the accredited testing organisation shall uncover vulnerabilities in the technical infrastructure of the licence holder, which could potentially be exploited to obtain unauthorised access through public interfaces.

3.2 Protected components

The gambling system and business systems in the licence holders 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 performed to ensure the systems integrity is intact/uncompromised.

Vulnerability scanning is necessary after significant updates 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). 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 vulnerability scans as described in section 3.3.1, is conducted by a dedicated internal function at the licence holder, that undertakes vulnerability scanning 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 the vulnerability scan is conducted by a dedicated internal function the accredited testing organisation shall assess, approve and certify these tests every three months. The certification 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 Vulnerability Scanning Process

The accredited testing organisation can use the National Vulnerability Database – Common Vulnerability Scoring System scale (NVD CVSS) or a similar scoring system of equal quality when evaluating whether the systems of the licence holder has an adequate level of security.

If any elements in the licence holders vulnerability scan scores 4 or higher on the NVD CVSS scale, the licence holder must remedy the uncovered vulnerabilities and get scanned again.

If the scan uncovers vulnerabilities in the licence holders system that cannot be remedied within the expiration of the previous scan, the certification must be accompanied with a remedial plan and compensating controls must be in place. These vulnerabilities must be fixed for the next quarterly scan.