Spillemyndigheden's Certification Programme

Requirements for vulnerability scanning

SCP.05.00.EN.2.0

Table of contents

1 Objectives of the requirements for vulnerability scanning

The requirements for vulnerability scanning seeks to ensure that the gambling system and business systems of the licence holder are scanned for vulnerabilities, that potentially could be exploited to gain access to e.g. sensitive information.

1.1 Scope of this document

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

The vulnerability scan of the gambling system and business systems shall be conducted in such a way that exposes vulnerabilities in components. The licence holder shall furthermore protect the systems in the best possible way. These requirements are set out in section 3 "Vulnerability Scanning Framework".

The Danish Gambling Authority has prescribed, what kind of vulnerability scan must be used. This along with the process is described in section 4 "Vulnerability Scanning 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	

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 vulnerability scans.

It must be emphasised that only the Danish version is legally binding. 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 Frequency and testing organisations

2.1 Vulnerability scan frequency

The licence holder is responsible to for having a vulnerability scan completed in accordance with the requirements in this document with an interval of maximum of 3 months.

2.1.1 Initial vulnerability scan

The licence holder shall have a vulnerability scan completed before a licence to offer games can be issued, unless the Danish Gambling Authority has informed otherwise.

2.1.2 Renewed vulnerability scan

After the initial vulnerability scan the licence holder shall have a new vulnerability scan completed within 3 months from the latest vulnerability scan. The standard report must reflect, when the new vulnerability scan has been completed.

The standard report, which documents the renewed vulnerability scan, shall be in the Danish Gambling Authority's possession no later than 1 months after the vulnerability scan is completed.

2.1.3 Vulnerability scan in connection with penetration test

The vulnerability scan completed prior to issue of a licence and 1 of the minimum 4 vulnerability each year may be done in connection with a penetration test completed in accordance with "SCP.04.00 Spillemyndighedens certification program – Requirements for penetration testing".

In order to consider a vulnerability scan completed in connection with a penetration as a valid vulnerability scan in accordance with the certification programme, it must be completed in compliance with the requirements in this document.

2.2 Testing organisations

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

2.2.1 Requirements for testing organisations

Testing organisations shall be approved as Approved Scanning Vendor (ASV).

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

Documentation for the approval shall be enclosed with the standard report. Alternatively, a link to the approval can be provided in the standard report.

2.2.2 Requirements for personnel who assess and attest the result of the vulnerability scan

The result of the vulnerability scan 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 5 years of practical experience with performing PCI approved vulnerability scans and
b) be an approved ASV Employee.

Guidance: Assessment and attesting can be carried out by e.g. two persons who in conjunction fulfil the requirements.

3 Vulnerability Scanning Framework

The Danish Gambling Authority's requirements for vulnerability scanning is based on Payment Card Industry – Data Security Standard (PCI-DSS).

3.1 Objective of the vulnerability scanning

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

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 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.

If an update is made to a significant component, which is part of the external interfaces at the licence holder or a supplier, it may be necessary to scan for vulnerabilities to ensure the integrity of the system. What is considered a "significant component" depends of the configuration of a given environment and cannot be predefined by the Danish Gambling Authority. What components are considered significant can be seen in connection with section 3.3.3 in the change management programme.

Guidance: The Danish Gambling Authority does not stipulate the requirements for, which type of vulnerability scan is completed in this situation. If a vulnerability scan, in this situation, is completed in compliance with the requirements in this document, it can be considered as a valid vulnerability scan and reported to the Danish Gambling Authority. The Danish Gambling Authority points out that vulnerability scans, which are reported to us, shall cover the ENTIRE gambling system and business system.

4 Vulnerability Scanning process

The scanning, the reporting to the licence holder and the quality control etc. shall be in compliance with the requirements prescribed by PCI DSS.

4.1 Type of vulnerability scan

With a maximum of 3 months interval the licence holder shall have completed a "PCI ASV vulnerability scan" scan of their gambling system and business systems. The vulnerability scan shall be performed by an Approved Scanning Vendor (ASV) cf. section 2.2.

Depending on the testing organisations delivery model the scan can be started by the licence holder.

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.

4.2 Assessment of vulnerabilities

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.

4.3 Standard report and plan for "not passed" vulnerability scans

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

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

'Passed after remediation' shall be used, when the vulnerability scan has uncovered vulnerabilities cf. section 4.2, which have been remediated and a following re-scan has shown, that the vulnerabilities ar no longer present; this includes suppliers.

'Not passed' shall be used, if there are vulnerabilities cf. section 4.2 in the licenceholder's systems, which cannot be remediated before the deadline for submitting the 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 vulnerabilities shal be remediated before the next scan.

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 vulnerability scan of the gambling system and business system is performed after remediation of vulnerabilities (re-scan), the date of the re-scan can be the point of reference for determining the deadline for the next vulnerability scan.