Spillemyndigheden

The Danish Gambling Authority's Certification Programme for betting and online casino

Requirements for vulnerability scanning – SCP.05.00.EN.3.0

Contents

Objectives of the requirements for vulnerability scanning

1

The requirements for vulnerability scanning shall ensure, that the base platform, game platform and business systems are scanned to uncover possible vulnerabilities in the systems. Vulnerabilities that possibly could be exploited to gain unauthorised access to e.g., sensitive information or affecting execution of games.

1.1 Version

Version 1.0 of 2014.07.04
- 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.

Version 1.1 of 2015.12.21
- Extension of applicability to cover offering of lotteries and betting on horse- and dog races.

Version 1.2 of 2020.01.01
- Spillemyndigheden has removed the requirement saying the ATO's accreditation must refer to a specific version cf. section 2.2.

Version 2.0 of 2023.01.01
- Update of requirements for accredited testing organisations and staff. Clarified, that vulnerability scans shall be PCI approved. Clarification of requirements if vulnerability scan 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.

Version 2.1 of 2023.10.01
- Updated visual layout of the document. Minor linguistic corrections. No changes to requirements.

Version 3.0 of 2025.01.01
- Changes have been because of the introduction of supplier licences. CREST Accreditation Vulnerability Scanning is added as a recognized accreditation for testing organisations. CREST-certification is added as a recognized personal certification for personnel who prepares/performs vulnerability scans.

The Danish Gambling Authority continuously revises the certification programme for betting and online casino. The latest version is accessible at The Danish Gambling Authority's website.

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.

1.2 Applicability

Instructions on vulnerability scanning is applicable for provision of online- and land-based betting (§ 11 in the Danish Gambling act), , online casino (§ 18 in the Danish Gambling act) and supply of games (§ 24a in the Danish Gambling act).

Frequency and testing organisations

2

2.1 Vulnerability scan frequency

The licence holder and game supplier are 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 and game supplier shall have a vulnerability scan completed before a licence to offer or supply games can be issued unless the Danish Gambling Authority has informed otherwise. See section 2.1.2 and 2.1.3 in the general requirements for further information.

2.1.2 Renewed vulnerability scan

After the initial vulnerability scan the licence holder and game supplier 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 month 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 – 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 attain minimum one of the following accreditations/approvals:
- CREST Accredited Vulnerability Assessment.
- Approved Scanning Vendor (ASV).

CREST-accreditation is done by the CREST membership body.

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

Documentation for the testing organisations CREST-accreeditation 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 prepares the vulnerability scan

The vulnerability scan shall be prepared by staff, who are sufficiently qualified. The testing organisation shall therefore hire and educate sufficiently qualified, competent, and experienced personnel. It is expected that personnel who prepares the vulnerability scan, has at least 5 years of practical experience with vulnerability scanning and has a personal certification, which demonstrates competence with vulnerability scanning. This can be one of the following:

- Certified ASV employee
- CREST CPSA or CRT certification

2.2.3 Supervision, assessment and attest of the standard report

Preparation/performing the vulnerability scan shall be supervised cf. the requirements for supervision in section 2.3 in the general requirements. Furthermore, the result of the penetration test and the need for possible remediation of vulnerabilities shall be assessed. It is the superviser's responsibility to sign the standard report, and thereby warrant that the vulnerability scan has been completed in an appropriate professional manner.

Guidance: A person who supervise, assess and signs, can also prepare the vulnerability scan cf. the requirements for supervision in section 2.3 in SCP.00.00 General requirements.

Vulnerability scanning framework

3

3.1 Objective of the vulnerability scanning

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

3.2 Protected components

The base platform, game platform and business systems in the 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 and game supplier 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 and game supplier'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, 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, 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 licence holder's entire base platform and business systems or the game supplier's entire game platform and business systems.

Vulnerability scanning process

4

The scanning, the reporting to the licence holder and game supplier and the quality control etc. shall comply with the requirements prescribed by PCI DSS or the requirements prescribed by CREST.

4.1 Type of vulnerability scan

With a maximum of 3 months interval the licence holder shall have completed a "PCI ASV vulnerability scan" or a "vulnerability scan complying with the requirements of CREST" of their base platform and business systems.

With a maximum of 3 months interval the game supplier shall have completed a "PCI ASV vulnerability scan" or a "vulnerability scan complying with the requirements of CREST" of their game platform and business systems.

The vulnerability scan shall be prepared and completed by a testing organisation compliant with the requirements in section 2.2.

Depending on the testing organisations delivery model the scan can be started by personnel with the licence holder or game supplier.

Guidance: 'base platform', 'game platform' and 'business system' are defined in the general requirements and cover both frontend, backend, datawarehouse and games.

4.2 Assessment of vulnerabilities

The testing organisation can use the National Vulnerability Database – Common Vulnerability Scoring System scale (NVD CVSS) or a similar scoring system when evaluating whether the licence holder's or game supplier's systems have an adequate level of security.

If any elements in the licence holder's or game supplier's vulnerability scan scores 4 or higher on the NVD CVSS scale, the licence holder or game supplier 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.

'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 are no longer present.

'Not passed' shall be used, if there are vulnerabilities cf. section 4.2 in the licence holder's systems, which cannot be remediated before the deadline for submitting the report to the Danish Gambling Authority. 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 shall 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 licence holder's base platform and business systems or game supplier's game platform and business systems 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 required vulnerability scan.