Spillemyndigheden

Spillemyndighedens certificeringsprogram

Krav til sårbarhedsscanning – SCP.05.00.DK.2.1

Indholdsfortegnelse

Formålet med krav til sårbarhedsscanning

1

Krav for sårbarhedsscanning er med til at sikre, at tilladelsesindehavers spilsystem og forretningssystemer scannes med henblik på at afdække eventuelle svagheder, der potentielt kan udnyttes til at opnå adgang til fx følsomme oplysninger.

1.1 Overblik over dette dokument

Der er fastsat krav til frekvensen for sårbarhedsscanninger samt hvilke testvirksomheder, der er godkendt til at foretage sårbarhedsscanning af tilladelsesindehavers spilsystem og forretningssystemer. Disse krav beskrives i afsnit 2 "Frekvens og testvirksomheder".

Sårbarhedsscanning skal gennemføres ved at scanne spilsystemet og forretningssystemerne på en måde, der afdækker svagheder i komponenter. Tilladelsesindehaver skal desuden beskytte systemerne bedst muligt. Krav til dette beskrives i afsnit 3 "Rammen for sårbarhedsscanning".

Spillemyndigheden har desuden fastlagt hvilken type sårbarhedsscanning, der skal foretages. Dette samt processen beskrives i afsnit 4 "Processen for gennemførsel af sårbarhedsscanning".

1.2 Version

Spillemyndigheden reviderer løbende certificeringsprogrammet. Seneste version samt versionshistorik er tilgængelig på Spillemyndighedens hjemmeside.

Version 1.0 af 2014.07.04
- Ny struktur i forhold til den tidligere version 1.3, samt en række opdateringer på en række områder. Derfor udstedes ny version 1.0. Det er hensigten fremover er at følge normal versioneringsnummerering.

Version 1.1 af 2015.12.21
- Udvidelse af anvendelsesområdet til også at omfatte udbud af lotterier og væddemål på heste- og hundevæddeløb.

Version 1.2 af 2020.01.01
- Spillemyndigheden har fjernet kravet om at testvirksomhedens akkreditering skal henvise til en specifik version jf. afsnit 2.2.

Version 2.0 af 2023.01.01
- Opdatering af krav til akkrediterede testvirksomheder og personale. Præciseret, at sårbarhedsscanning skal være PCI-godkendt. Præcisering af krav hvis sårbarhedsscanning ej bestået. Afsnit om anvendelse af intern funktion er fjernet. Derudover er der foretaget generelle tilpasninger og specificeringer.

Version 2.1 af 2023.10.01
- Opdateret visuelt layout af dokumentet. Få sproglige rettelser. Ingen ændringer til krav.

Ved udgivelse af en ny version af certificeringsprogrammet offentliggør Spillemyndigheden, hvis nødvendigt, retningslinjer for en overgangsordning og gyldigheden af allerede gennemførte sårbarhedsscanninger.

Det skal fremhæves, at det er den danske version, der er bindende. Den engelske version er udelukkende af vejledende karakter.

1.3 Anvendelsesområde

Retningslinjer for sårbarhedsscanning finder anvendelse på udbud af online væddemål (§ 11 i lov om spil), landbaseret væddemål (§ 11 i lov om spil), onlinekasino (§ 18 i lov om spil) og lotterier (§ 6 i lov om spil).

Frekvens og testvirksomheder

2

2.1 Frekvens for sårbarhedsscanninger

Tilladelsesindehaver er ansvarlig for at sikre, at der med et interval på maksimalt tre kalendermåneder bliver gennemført en sårbarhedsscanning i overensstemmelse med kravene i dette dokument.

2.1.1 Første sårbarhedsscanning

Tilladelsesindehaver skal have foretaget en sårbarhedsscanning første gang inden, der kan udstedes tilladelse til spil, medmindre Spillemyndigheden har oplyst andet. Se afsnit 2.1.3 i de generelle krav for yderligere oplysninger.

2.1.2 Fornyet sårbarhedsscanning

Efter den første sårbarhedsscanning skal tilladelsesindehaver have foretaget en ny sårbarhedsscanning inden tre måneder fra seneste sårbarhedsscanning. Det skal fremgå af standardrapporten, hvornår der er foretaget en fornyet scanning.

Standardrapporten som dokumenterer den fornyede sårbarhedsscanning skal være Spillemyndigheden i hænde senest én måned efter, at penetrationstesten er foretaget.

2.1.3 Sårbarhedsscanning i forbindelse med penetrationstest

Sårbarhedsscanningen der skal foretages forud for udstedelse af tilladelse og den ene af de minimum fire sårbarhedsscanninger, der skal foretages årligt, kan være foretaget i forbindelse med en penetrationstest gennemført i henhold til "SCP.04.00 Spillemyndighedens certificeringsprogram - krav for penetrations-test".

For at en sårbarhedsscanning foretaget i forbindelse med en penetrationstest skal kunne betragtes som en gyldig sårbarhedsscanning i henhold til certificeringsprogrammet, skal den være gennemført i overensstemmelse med kravene i dette dokument.

2.2 Testvirksomheder

For at sikre, at de nødvendige kvalifikationer er til stede, når en sårbarhedsscanning udføres, skal test-virksomheden og dennes ansatte leve op til kravene i dette afsnit.

2.2.1 Krav til testvirksomhed

Testvirksomheder skal være godkendt som Approved Scanning Vendor (ASV).
Godkendelsen foretages af Payment Card Industry (PCI) Security Standards Council (SSC).
Dokumentation for testvirksomhedens godkendelse vedlægges standardrapporten. Alternativt kan der linkes til godkendelsen i standardrapporten.

2.2.2 Krav til personale som vurderer og attesterer resultat af sårbarhedsscanning

Resultatet af sårbarhedsscanningen og eventuelt afledte udbedringer af sårbarheder skal vurderes og attesteres af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

a. Have mindst 5 års praktisk erfaring med at foretage PCI ASV Vulnerability Scanning og

b. være certificeret ASV Employee.

Vejledning: Vurderingen og attesteringen kan foretages af fx to personer, der i fællesskab opfylder kravene.

Rammen for sårbar-hedsscanning

3

Spillemyndighedens krav til sårbarhedsscanning er baseret på Payment Card Industry – Data Security Standard (PCI-DSS).

3.1 Formål med sårbarhedsscanning

Ved sårbarhedsscanning skal testvirksomheden afdække svagheder i tilladelsesindehavers tekniske infrastruktur, som potentielt kunne blive udnyttet til uautoriseret indtrængen via eksterne interfaces.

3.2 Beskyttede komponenter

Spilsystemet og forretningssystemerne i tilladelsesindehavers produktionsmiljø skal være beskyttet mod eventuelle angreb fra uvedkommende. I særdeleshed skal komponenter, som indeholder følsomme oplysninger om kunder, beskyttes. Definitionen af komponenter og disses væsentlighed skal ses i sammenhæng med Spillemyndighedens program for styring af systemændringer SCP.06.00.DK, afsnit 3.3.3.

Tilladelsesindehaver kan ved segmentering af deres interne netværk, herunder hvilke dele af systemet, som kommunikerer via offentlige netværk med følsomme oplysninger, mindske risikoen for uautoriseret adgang.

3.2.1 Opdatering af software og hardware

Det er tilladelsesindehavers ansvar, at systemernes komponenter er opdateret til et niveau, der frembyder den højest mulige sikkerhed og ikke kompromitterer systemernes integritet, så risikoen for uautoriseret adgang til fx følsomme oplysninger mindskes.

Hvis der sker opdatering af væsentlige komponenter, som er del af de eksterne interfaces hos tilladelses-indehaver eller en underleverandør, kan der være behov for at scanne for sårbarheder for at sikre systemets integritet. Hvad der betragtes som "væsentlige komponenter", afhænger af opsætningen af et givent miljø, og kan derfor ikke foruddefineres af Spillemyndigheden. Hvilke komponenter der betragtes som væsentlige kan ses i sammenhæng med afsnit 3.3.3 i program for styring af systemændringer.

Vejledning: Spillemyndigheden stiller ikke krav til, hvilken type sårbarhedsscanninger tilladelsesindehaver foretager i denne situation. Hvis der i denne situation foretages en sårbarhedsscanning i overensstemmelse med kravene i dette dokument, kan den betragtes som en gyldig sårbarhedsscanning og rapporteres til Spillemyndigheden. Spillemyndigheden gør opmærksom på at sårbarhedsscanninger, der rapporteres til os, skal omfatte HELE spilsystemet og forretningssystemet.

Processen for gennemførsel af sårbarhedsscanning

4

Scanningen, rapporteringen til tilladelsesindehaver og kvalitetskontrollen mv. skal være i overensstemmelse med kravene i henhold til PCI DSS.

4.1 Type af sårbarhedsscanning

Med højst tre måneders interval skal tilladelsesindehaver have foretaget en "PCI ASV Vulnerability Scanning" af deres spilsystem og forretningssystemer. Sårbarhedsscanningen skal foretages af en Approved Scanning Vendor (ASV) jf. afsnit 2.2.

Afhængig af testvirksomhedens leverancemodel kan scanningen igangsættes af tilladelsesindehaver.

Vejledning: 'Spilsystem' og 'forretningssystem' er defineret i de generelle krav og omfatter både frontend, backend, datawarehouse og spil uanset om det drives af tilladelsesindehaver eller en leverandør.

4.2 Vurdering af sårbarheder

Testvirksomheden kan anvende National Vulnerability Database – Common Vulnerability Scoring System-skalaen (NVD CVSS) eller et lignende scoringssystem med tilsvarende niveau, til at vurdere om tilladelses-indehavers systemer har et tilfredsstillende niveau af sikkerhed.

Hvis enkelte delelementer for tilladelsesindehavers sårbarhedsscanning scorer 4 eller højere på NVD CVSS-skalaen skal tilladelsesindehaver udbedre de afdækkede sårbarheder i systemerne og scannes på ny.

4.3 Standardrapport og plan for "ikke-bestået" sårbarhedsscanning

I standardrapporten skal det anføres om sårbarhedsscanningen er bestået, bestået med rettelser eller ikke bestået.

'Bestået' skal benyttes, når sårbarhedsscanningen er gennemført uden, at der er fundet sårbarheder; dette inkluderer underleverandører.

'Bestået efter rettelser' skal benyttes, når sårbarhedsscanningen har vist sårbarheder jf. afsnit 4.2, der er blevet udbedret og en efterfølgende re-scan har vist at sårbarhederne ikke længere er til stede; dette inkluderer underleverandører.

'Ikke bestået' skal benyttes, hvis der er sårbarheder jf. afsnit 4.2, der ikke kan udbedres inden fristen for indsendelse af rapporten til Spillemyndigheden udløber; dette inkluderer underleverandører. I denne situation, skal der sammen med standardrapporten indleveres et bilag indeholdende en plan for udbedring af sårbarheder samt en beskrivelse af kompenserende kontroller. Disse sårbarheder skal være rettet op inden næste scanning.

I praksis kan en 'ikke bestået' rapport ikke accepteres af Spillemyndigheden, uden at bilaget indeholder en plan for udbedring og beskrivelse af kompenserende kontroller.

Hvis der efter udbedring af sårbarheder er gennemført en fuldstændig sårbarhedsscanning (re-scan) af spilsystemet og forretningssystemerne, kan datoen for re-scanningen være udgangspunktet for fastsættelse af tidsfristen for den næste sårbarhedsscanning.