Spillemyndigheden

Spillemyndighedens certificeringsprogram for væddemål og onlinekasino

Krav til sårbarhedsscanning – SCP.05.00.DK.3.0

Indholdsfortegnelse

Formålet med krav til sårbarhedsscanning

1

Krav til sårbarhedsscanning skal sikre, at base platform, spilplatform og forretningssystemer scannes med henblik på at afdække eventuelle svagheder i systemerne. Sårbarheder, der potentielt kan udnyttes til at opnå uautoriseret adgang til fx følsomme oplysninger eller påvirkning af spillets afvikling.

1.1 Version

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.

Version 3.0 af 2025.01.01
- Der er foretaget konsekvensrettelser på baggrund af introduktion af leverandørtilladelser. CREST Accredited Vulnerability Scanning er tilføjet, som anerkendt akkreditering for testvirksomhed. Tilføjet CREST-certificeringer, som anerkendte personlige certificeringer for personale som tilrettelægger/udfører sårbarhedsscanning.

Spillemyndigheden reviderer løbende certificeringsprogrammet for væddemål og onlinekasino. Den seneste version er tilgængelig på Spillemyndighedens hjemmeside.

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.

1.2 Anvendelsesområde

Retningslinjer for sårbarhedsscanning finder anvendelse på udbud af online- og landbaseret væddemål (§ 11 i lov om spil), onlinekasino (§ 18 i lov om spil) og levering af spil (§ 24a i lov om spil).

Frekvens og testvirksomheder

2

2.1 Frekvens for sårbarhedsscanninger

Tilladelsesindehaver og spilleverandører er ansvarlige 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 og spilleverandør skal have foretaget en sårbarhedsscanning første gang inden, der kan udstedes tilladelse til at udbyde eller levere spil, medmindre Spillemyndigheden har oplyst andet. Se afsnit 2.1.2 og 2.1.3 i de generelle krav for yderligere oplysninger.

2.1.2 Fornyet sårbarhedsscanning

Efter den første sårbarhedsscanning skal tilladelsesindehaver og spilleverandør 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 sårbarhedsscanningen 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 - krav til penetrationstest".

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 testvirksomheden og dennes ansatte leve op til kravene i dette afsnit.

2.2.1 Krav til testvirksomhed

Testvirksomheder skal opnå minimum én af følgende akkreditering/godkendelse:
- CREST Accredited Vulnerability Scanning.
- Approved Scanning Vendor (ASV).

CREST-akkreditering foretages af CREST membership body.

ASV-godkendelse foretages af Payment Card Industry (PCI) Security Standards Council (SSC).

Dokumentation for testvirksomhedens CREST-akkreditering eller ASV-godkendelse vedlægges standardrapporten. Alternativt kan der linkes til akkrediteringen eller godkendelsen i standardrapporten.

2.2.2 Krav til personale som tilrettelægger sårbarhedsscanningen

Sårbarhedsscanningen skal tilrettelægges af personer, der er tilstrækkelig kvalificeret. Testvirksomheden skal derfor ansætte og oplære tilstrækkelig kvalificeret, kompetent og erfarent personale. Det forventes at personalet som tilrettelægger sårbarhedsscanningen, har mindst 5 års praktisk erfaring med sårbarhedsscanning af systemer og har en personlig certificering, som demonstrerer kompetence for sårbarhedsscanning. Det kan være en af følgende:

- Certificeret ASV employee.
- CREST CPSA eller CRT certificering.

2.2.3 Supervisering, vurdering og signering af standardrapporten

Tilrettelæggelsen/udførslen af sårbarhedsscanningen skal superviseres jf. kravene til supervisering i afsnit 2.3 i de generelle krav. Derudover skal resultatet af sårbarhedsscanningen og behovet for eventuelt afledte udbedringer af sårbarheder vurderes. Det er superviserens ansvar at vurdere resultatet af sårbarhedsscanningen og underskrive standardrapporten og derved indestå for, at sårbarhedsscanningen er udført fagligt forsvarligt.

Vejledning: En person som superviserer, vurderer og signerer, kan samtidig tilrettelægge sårbarhedsscanningen jf. kravene i afsnit 2.3 om supervisering i SCP.00.00 Generelle krav.

Rammen for sårbar-hedsscanning

3

3.1 Formål med sårbarhedsscanning

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

3.2 Beskyttede komponenter

Base platform, spilplatform og forretningssystemerne i 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 og spilleverandør 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 tilladelsesindehaver og spilleverandørs 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, 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 forud defineres 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 specificerer ikke, 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 tilladelsesindehavers base platform og forretningssystemer eller hele spilleverandørs spilplatform og forretningssystemer.

Processen for gennemførsel af sårbarhedsscanning

4

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

4.1 Type af sårbarhedsscanning

Med højst tre måneders interval skal tilladelsesindehaver have foretaget en "PCI ASV Vulnerability Scanning" eller en "sårbarhedsscanning i overensstemmelse med kravene i CREST" af deres base platform og forretningssystemer.

Med højst tre måneders interval skal spilleverandør have foretaget en "PCI ASV Vulnerability Scanning" eller en "sårbarhedsscanning i overensstemmelse med kravene i CREST" af deres spilplatform og forretningssystemer.

Sårbarhedsscanningen skal tilrettelægges og udføres af en testvirksomhed, som lever op til kravene i afsnit 2.2.Afhængig af testvirksomhedens leverancemodel kan scanningen igangsættes af personale hos tilladelsesindehaver eller spilleverandør.

Vejledning: 'Base platform', 'spilplatform' og 'forretningssystem' er defineret i de generelle krav og omfatter både frontend, backend, datawarehouse og spil.

4.2 Vurdering af sårbarheder

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

Hvis enkelte delelementer for tilladelsesindehavers eller spilleverandørs sårbarhedsscanning scorer 4 eller højere på NVD CVSS-skalaen skal tilladelsesindehaver eller spilleverandør 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.

'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.

'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. 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 tilladelsesindehavers base platform og forretningssystemer eller spilleverandørs

spilplatform og forretningssystemer, kan datoen for re-scanningen være udgangspunktet for fastsættelse af tidsfristen for den næste påkrævede sårbarhedsscanning.