Spillemyndigheden

Spillemyndighedens certificeringsprogram for væddemål og onlinekasino

Krav til penetrationstest – SCP.04.00.DK.3.0

Indholdsfortegnelse

Formålet med krav til penetrationstest

1

Krav til penetrationstest skal sikre, at base platform, spilplatform og forretningssystemer testes med henblik på at afdække mulig udnyttelse af eventuelle svagheder i systemerne. Svagheder, 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. Præcisering af krav hvis penetrationstest 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. Tilføjet CREST-akkreditering for penetrationstest, som anerkendt akkreditering for testvirksomhed.

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 penetrationstest.

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

1.2 Anvendelsesområde

Krav til penetrationstest 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 penetrationstest

Tilladelsesindehaver og spilleverandør er ansvarlig for at sikre, at der med et interval på maksimalt 12 kalendermåneder bliver gennemført en penetrationstest i overensstemmelse med kravene i dette dokument.

2.1.1 Første penetrationstest

Tilladelsesindehaver og spilleverandør skal have gennemført en penetrationstest 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 penetrationstest

Tilladelsesindehaver og spilleverandør skal som udgangspunkt have gennemført en ny penetrationstest inden 12 måneder fra seneste penetrationstest. Det skal fremgå af standardrapporten, hvornår der er gennemført en fornyet penetrationstest.

Standardrapporten, som dokumenterer den fornyede penetrationstest, skal være Spillemyndigheden i hænde senest to måneder efter, at penetrationstesten er foretaget.

2.1.2.1 Udsættelse af penetrationstest
Tilladelsesindehaver og spilleverandør kan vælge at udsætte penetrationstesten op til to måneder fra tidspunktet, hvor der skulle være gennemført en ny penetrationstest. Den nye penetrationstest skal således være afsluttet senest 14 måneder fra seneste penetrationstest og standardrapporten skal være Spillemyndigheden i hænde inden samme frist.

Spillemyndigheden skal underrettes, inden penetrationstesten udsættes.

Fristen for fornyelse af penetrationstest forkortes med den tid den tidligere 12 måneders frist har været udsat. Hvis man fx udnytter de maksimale to måneders udsættelse, skal næste penetrationstest senest gennemføres efter 10 måneder. Det forventede tidspunkt for næste penetrationstest skal afspejle dette og anføres i standardrapporten.

2.2 Testvirksomheder

For at sikre, at de nødvendige kvalifikationer er til stede til at udføre en penetrationstest, 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 Penetration Testing
- ISO/IEC 17025-akkreditering i henhold til Spillemyndighedens certificeringsprogram for væddemål og onlinekasino SCP.04.00.DK, eller
- ISO/IEC 17065-akkreditering i henhold til Spillemyndighedens certificeringsprogram for væddemål og onlinekasino SCP.04.00.DK, eller
- Approved Scanning Vendor (ASV) godkendelse.

CREST-akkreditering foretages af CREST membership body.

ISO-akkreditering skal foretages af DANAK (Den Danske Akkrediteringsfond) eller et tilsvarende akkrediteringsorgan, som er medunderskriver af EA´s (European co-operation for Accreditation) multilaterale aftale om gensidig anerkendelse mht. prøvning eller for certificeringsorganer udenfor EA's område af et akkrediteringsorgan, der er medunderskriver af ILAC's (the International Laboratory Accreditation Cooperation) multilaterale aftale om gensidig anerkendelse mht. prøvning.

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

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

2.2.2 Krav til personale som udfører penetrationstesten

Penetrationstesten skal udføres af personale, der er tilstrækkelig kvalificeret. Testvirksomheden skal derfor ansætte og oplære tilstrækkelig kvalificeret, kompetent og erfarent personale. Det forventes at personalet som udfører penetrationstest, har mindst 5 års praktisk erfaring med penetrationstest og har en personlig certificering, som demonstrerer kompetence for penetrationstest. Det kan fx være en af følgende:

- Offensive Security Certified Professional (OSCP)
- EC-Council: Certified Ethical Hacker (CEH), Licensed Penetration Tester Master (LPT Master),
- Global Information Assurance Certification (GIAC): GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN),
- CREST Penetration Testing Certifications,
- Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification,
- Tiger Scheme: Senior Security Tester, Qualified Security Tester.

2.2.3 Supervisering, vurdering og signering af standardrapporten

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

Vejledning: En person som superviserer, vurderer og signerer, kan samtidig være med til at udføre penetrationstesten jf. kravene om supervisering i afsnit 2.3 i SCP.00.00 Generelle krav.

Rammen for penetrationstest

3

Spillemyndighedens krav til penetrationstest er baseret på opnåede erfaringer med tilsyn på området, anbefalinger fra og dialog med branchen.

3.1 Formål med penetrationstest

Formålet med penetrationstest er at identificere og forsøge at udnytte eventuelle svagheder i base platform, spilplatform og forretningssystemer.

3.2 Beskyttede komponenter

Platformene og forretningssystemerne i tilladelsesindehavers og spilleverandørs 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 mindskes.

Processen for gennemførsel af penetrationstest

4

Med højst 12 måneders interval skal tilladelsesindehaver have foretaget en penetrationstest af deres base platform og forretningssystemer.

Med højst 12 måneders interval skal spilleverandør have foretaget en penetrationstest af deres spilplatform og forretningssystemer.

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

Penetrationstesten skal omfatte, men ikke begrænses til, de eventuelle svagheder, der er blevet afdækket ved sårbarhedsscanningen, jf. Spillemyndighedens krav til sårbarhedsscanning SCP.05.00.DK.

Testvirksomheden skal derudover forsøge at opnå uautoriseret adgang til base platform, spilplatform og forretningssystem. Den uautoriserede adgang skal forsøges eskaleret til det højeste adgangsniveau, og udføres både med og uden adgangsoplysninger (white box/black box). Derigennem efterprøves som minimum følgende scenarier:

- Manipulering af resultatgenerering
- Påvirkning af spillets afvikling
- Svindel med spillernes midler
- Tyveri af spillernes midler
- Manipulering af revisionsegnede logge
- Adgang til følsomme oplysninger
- Manipulering af følsomme oplysninger
- Manipulering af dataoverførsel til SAFE

4.1 Standardrapport og plan for "ikke-bestået" penetrationstest

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

'Bestået' skal benyttes, når penetrationstesten er gennemført uden, at der er fundet sårbarheder.

'Bestået efter rettelser' skal benyttes, når penetrationstesten har vist sårbarheder, der er blevet udbedret og en efterfølgende test har vist at sårbarhederne ikke længere er til stede.

'Ikke bestået' skal benyttes, hvis der er sårbarheder, som 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. Tilladelsesindehaveren eller spilleverandøren skal derefter hurtigst muligt udbedre sårbarhederne og senest tre måneder efter have gennemført en ny penetrationstest, som dækker de identificerede sårbarheder.

Efter fornyet penetrationstest, skal der indleveres dokumentation til Spillemyndigheden for, at sårbarhederne er udbedret.

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 er gennemført en fuldstændig penetrationstest af tilladelsesindehavers base platform og forretningssystemer eller spilleverandørs spilplatform og forretningssystemer efter udbedring af sårbarheder, vil datoen for gennemførsel af denne penetrationstest være udgangspunktet for fastsættelse af tidsfristen for den næste penetrationstest.