Spillemyndighedens certificeringsprogram

Krav til penetrationstest

SCP.04.00.DK.2.0

Indhold

1 Formålet med krav til penetrationstest

Krav til penetrationstest skal sikre, at tilladelsesindehavers spilsystem og forretningssystemer testes med henblik på at afdække mulig udnyttelse af eventuelle svagheder i systemerne. Svagheder, der potentielt kan udnyttes til fx at opnå uautoriseret adgang til følsomme oplysninger.

1.1 Overblik over dette dokument

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

Penetrationstesten skal teste spilsystemet og forretningssystemerne på en måde, der afdækker svagheder i komponenter og hvorvidt disse svagheder kan udnyttes af uvedkommende. Tilladelsesindehaver skal desuden beskytte systemerne bedst muligt. Krav til dette beskrives i afsnit 3 ”Rammen for penetrationstest”.

Spillemyndigheden specificerer en række scenarier, som der skal testes for i forbindelse med penetrationstesten, samt en proces for tests, der ikke er bestået. Disse scenarier beskrives i afsnit 4 ”Processen for gennemførsel af penetrationstest”.

1.2 Version

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

Dato	Version	Beskrivelse
2014.07.04	1.0	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.
2015.12.21	1.1	Udvidelse af anvendelsesområdet til også at omfatte udbud af lotterier og væddemål på heste- og hundevæddeløb.
2020.01.01	1.2	Spillemyndigheden har fjernet kravet om at testvirksomhedens akkreditering skal henvise til en specifik version jf. afsnit 2.2.
2023.01.01	2.0	

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.

1.3 Anvendelsesområde

Krav til penetrationstest finder anvendelse på udbud af:

- Online væddemål
- Landbaseret væddemål
- Onlinekasino
- Lotterier

2 Frekvens og testvirksomheder

2.1 Frekvens for penetrationstest

Tilladelsesindehaver 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 skal have gennemført en penetrationstest 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 penetrationstest

Tilladelsesindehaver 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 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.

Muligheden for udsættelse af penetrationstesten gælder kun for tilladelsesindehaveren. Muligheden gælder således ikke for tilladelsesindehaverens eventuelle leverandører.

2.2 Testvirksomheder

For at sikre, at de nødvendige kvalifikationer er til stede, når en penetrationstest 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 de følgende akkrediteringer/godkendelse:

- ISO/IEC 17025-akkreditering i henhold til Spillemyndighedens certificeringsprogram SCP.04.00.DK, eller
- ISO/IEC 17065-akkreditering i henhold til Spillemyndighedens certificeringsprogram SCP.04.00.DK, eller
- Approved Scanning Vendor (ASV) godkendelse.

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 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 tilstrækkeligt kvalificeret. Testvirksomheden skal derfor ansætte tilstrækkeligt kvalificeret, kompetent og erfarent personale.

2.2.3 Krav til personale som vurderer og attesterer resultatet af penetrationstesten

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

a) Have mindst 5 års praktisk erfaring med penetrationstest af systemer og
b) Have en personlig certificering, som demonstrerer kompetence indenfor 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 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.

Vejledning: Vurderingen og attesteringen kan foretages af fx to personer, der i fællesskab opfylder kravene. Personer som vurderer og attesterer, kan være med til at udføre penetrationstesten jf. afsnit 2.2 om supervisering i SCP.00.00 Generelle krav.

3 Rammen for penetrationstest

Spillemyndighedens krav til penetrationstest er baseret på opnåede erfaringer 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 tilladelsesindehavers spilsystem og forretningssystemer.

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 mindskes.

4 Processen for gennemførsel af penetrationstest

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

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.

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 tilladelsesindehavers spilsystem 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; dette inkluderer underleverandører.

'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; dette inkluderer underleverandører.

'Ikke bestået' skal benyttes, hvis der er sårbarheder i tilladelsesindehavers systemer, som 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. Tilladelsesindehaveren 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 tilladelsesindehaveren indlevere dokumentation 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 spilsystemet og forretningssystemerne efter udbedring af sårbarheder, vil datoen for gennemførsel af denne penetrationstest være udgangspunktet for fastsættelse af tidsfristen for den næste penetrationstest.