Spillemyndighedens certificeringsprogram

Retningslinjer for sårbarhedsscanning

SCP.05.00.DK.1.2

Indhold

1 Formålet med retningslinjer for sårbarhedsscanning

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

1.1 Overblik over dette dokument

Der er fastsat en række krav til, hvordan testvirksomheder bliver akkrediteret til at foretage certificering af tilladelsesindehaveres spilsystem, forretningsgange og forretningssystemer, samt hvordan selve certificeringen skal foretages. Disse krav til akkreditering af testvirksomheder og certificering af tilladelsesindehavere beskrives i afsnit 2 "Certificering".

Sårbarhedsscanning skal gennemføres ved at scanne spilsystemet og forretningssystemerne på en måde, der afdækker svagheder i komponenter. Dette kan være særligt relevant, når der sker opdateringer af systemet. Disse krav beskrives i afsnit 3 "Rammen for sårbarhedsscanning".

Spillemyndigheden foreslår en metodik til sårbarhedsscanningen. Denne metodik beskrives i afsnit 4 "Processen for gennemførsel af sårbarhedsscanning".

1.2 Version

Spillemyndigheden vil løbende revidere certificeringsprogrammet og seneste version samt versionshistorik er tilgængelig på spillemyndighedens hjemmeside: https://spillemyndigheden.dk/certificeringsprogrammet

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.

Spillemyndigheden offentliggør retningslinjer for gyldigheden af eksisterende certificeringer, samt tidligere inspektioner og prøvninger, ved udgivelsen af nye versioner af certificeringsprogrammet.

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

1.3 Anvendelsesområde

Retningslinjer for sårbarhedsscanning finder anvendelse på udbud af:

- Online væddemål
- Landbaseret væddemål
- Onlinekasino
- Lotterier

2 Certificering

2.1 Certificeringsfrekvens

Tilladelsesindehaver er ansvarlig for at sikre, at der med et interval på maksimalt 3 kalendermåneder sker certificering i overensstemmelse med kravene i dette dokument.

2.1.1 Første certificering

Tilladelsesindehaver skal som udgangspunkt være certificeret første gang inden der kan udstedes tilladelse til spil, medmindre Spillemyndigheden har oplyst andet.

2.1.2 Fornyet certificering

Tilladelsesindehaver skal som udgangspunkt have foretaget en ny certificering inden 3 måneder fra seneste certificering. Det skal fremgå af standardrapporten, hvornår der er sket fornyet certificering.

2.2 Akkrediterede testvirksomheder

Testvirksomheder skal opnå ISO/IEC 17020-akkreditering og/eller ISO/IEC 17025-akkreditering med udgangspunkt i de kriterier, der er beskrevet i de følgende afsnit. 'Spillemyndighedens certificeringsprogram – SCP.05.00.DK' skal fremgå eksplicit af akkrediteringsscopet.

Selve akkrediteringen foretages af *Den Danske Akkrediterings- og Metrologifond (DANAK)* eller et tilsvarende akkrediteringsorgan, som er omfattet af *European co-operation for Accreditations* multilaterale aftale om gensidig anerkendelse eller medlem af *International Laboratory Accreditation Cooperation*.

For at sikre, at de nødvendige kvalifikationer er til stede, når en certificering udføres, skal testvirksomheden og dennes ansatte leve op til følgende minimumskrav. Dokumentation for, at kravene er opfyldt, skal vedlægges certificeringen.

2.2.1 Krav til testvirksomheden

Testvirksomheden skal:

a) have mindst 2 års erfaring med sårbarhedsscanning af systemer eller et lignende nært beslægtet fagområde,
b) være akkrediteret som Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
c) arbejde med udgangspunkt i ISO/IEC 17020-akkrediteringen og/eller ISO/IEC 17025-akkrediteringen, der henviser til kravene i SCP.05.00.DK, og
d) sikre, at tilstrækkeligt kvalificeret personale udfører certificeringen.

2.2.2 Krav til personale, der superviserer og attesterer certificeringen

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.2.1 ovenfor. Udførslen skal superviseres, og certificeringserklæringen skal attesteres af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

a) 5 års erhvervsmæssig erfaring med sårbarhedsefterprøvning af systemer, eller et lignende nært beslægtet fagområde, og
b) være certificeret som
    - International Council of E-Commerce (EC-Council) Certified Ethical Hacker (CEH),

- International Council of E-Commerce (EC-Council) Licensed Penetration Tester (LPT),
- Information Assurance Certification Review Board (IACRB) Certified Penetration Tester (CPT),
- Global Information Assurance Certification (GIAC) Certified Penetration Tester (GPEN),
- CESG CHECK Team Leader,
- CESG CHECK Team Member,
- CREST Infrastructure Certification,
- CREST Registered Tester,
- Tiger Scheme Senior Security Tester,
- Tiger Scheme Qualified Security Tester, eller
- Offensive Security Certified Professional (OSCP).

Vejledning: Prøvning, supervisering og attesteringen kan foretages af flere personer, der i fællesskab opfylder kravene.

3 Rammen for sårbarhedsscanning

Spillemyndighedens program for sårbarhedsscanning er til dels inspireret af Payment Card Industry – Data Security Standard (PCI-DSS).

3.1 Formål med sårbarhedsscanning

Ved sårbarhedsscanning skal den akkrediterede testvirksomhed 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 udefrakommende. 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.

3.3 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. Herved mindskes risikoen for uautoriseret adgang til følsomme oplysninger.

3.3.1 Opdatering af komponenter

Hvis der sker opdatering af komponenter hos tilladelsesindehaver eller en underleverandør, skal der scannes for sårbarheder for at sikre, at systemets integritet er intakt.

Sårbarhedsscanning er således nødvendig ved væsentlige opdateringer eller ændringer i infrastrukturen eller brugen heraf (f.eks. installation af nye systemkomponenter, tilføjelse af et underetværk eller tilføjelse af en webserver). Hvad der bedømmes som "væsentligt", afhænger i høj grad af opsætningen af et givent miljø, og det kan som sådan ikke forud defineres af Spillemyndigheden. Det betragtes altid som væsentligt, hvis opdateringen eller ændringen kan påvirke eller give adgang til følsomme oplysninger og/eller komponenter, jf. Spillemyndighedens program for styring af systemændringer SCP.06.00.DK, afsnit 3.3.3.

3.3.2 Intern funktion hos tilladelsesindehaver

Den akkrediterede testvirksomhed kan tillade, at sårbarhedsscanning som beskrevet i afsnit 3.3.1, kan foretages af en intern funktion hos tilladelsesindehaver, hvis primære formål er at foretage løbende sårbarhedsscanning af systemerne. Funktionen skal være bemandet med kvalificeret personale samt være organisatorisk adskilt fra funktionen, der implementerer systemændringer.

Såfremt sårbarhedsscanningen foretages af en intern funktion hos tilladelsesindehaver vurderer, godkender og certificerer den akkrediterede testvirksomhed scanningerne hver tredje måned. Det skal fremgå af standardrapporten, hvorvidt denne fremgangsmåde er anvendt.

Denne mulighed kan kun benyttes af tilladelsesindehavere. Den kan ikke benyttes af underleverandører uden selvstændig tilladelse til udbud af spil i Danmark.

4 Processen for gennemførsel af sårbarhedsscanning

Den akkrediterede testvirksomhed kan anvende National Vulnerability Database – Common Vulnerability Scoring System-skalaen (NVD CVSS) eller et lignende scoringssystem med tilsvarende niveau, til at vurdere om tilladelsesindehavers 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.

Hvis der er sårbarheder i tilladelsesindehavers systemer, som ikke kan rettes op inden udløbet af den foregående scanning, skal der sammen med standardrapporten indleveres et bilag indeholdende en plan for udbedring samt kompenserende kontroller. Disse sårbarheder skal være rettet op til næste scanning.