Ministerstvo financí
Státní dozor nad sázkovými hrami a loteriemi
Mgr. Karel Blaha
ředitel odboru 34

Letenská 15, Praha 1 - Malá Strana, 118 10
Pracoviště:
Legerova, 69, Praha 1, 110 00
Sekretariát tel.: 25704 3322

č. j.: MF-30513/2016/3402-12
PID: MFCR6XYEDD

V Praze dne 21. prosince 2016

Standard Ministerstva financí k provozování hazardních her dle zákona č. 186/2016 Sb., o hazardních hrách

Ministerstvo financí – Státní dozor nad sázkovými hrami a loteriemi v zájmu zaručení řádného provozování hazardních her a zajištění řádného technického vybavení ve smyslu § 87 odst. 1 písm. e) zákona č. 186/2016 Sb., o hazardních hrách (dále jen „zákon o hazardních hrách“), vydává Standard minimálních technických parametrů pro zařízení, jejichž prostřednictvím jsou provozovány hazardní hry, a požadavků na ochranu a uchovávání herních a finančních dat a jejich technické parametry.

POŽADAVKY NA ZAŘÍZENÍ, JEJICHŽ PROSTŘEDNICTVÍM JSOU PROVOZOVÁNY HAZARDNÍ HRY, A NA OCHRANU A UCHOVÁVÁNÍ HERNÍCH A FINANČNÍCH DAT A JEJICH TECHNICKÉ PARAMETRY

I.
Zařízení, jehož prostřednictvím je provozována hazardní hra

1) Zařízení, jehož prostřednictvím je provozována hazardní hra podléhající povolení, (dále jen „zařízení“) je tvořeno uceleným souborem hardwaru a softwaru provozovatele hazardní hry, který slouží k vykonávání činností podle § 5 zákona o hazardních hrách.
2) Zařízení musí obsahovat server, který slouží k řízení činností podle § 5 zákona o hazardních hrách a k ukládání finančních a herních dat (dále jen „server“). Pro identifikaci serveru se použijí obdobně podmínky stanovené v bodu VIII.
3) Zařízení, jejichž prostřednictvím jsou provozovány loterie, bingo, technická hra nebo živá hra anebo internetová hra, v níž o výhře nebo prohře rozhoduje zcela nebo zčásti náhoda, musí obsahovat generátor náhodných čísel.

II.
Ochrana a uchovávání herních a finančních dat

Nestanoví-li zákon o hazardních hrách nebo tento standard jinak, zařízení a způsob nakládání provozovatele hazardní hry s herními a finančními daty v něm uchovávanými musí splňovat technické požadavky na systém řízení bezpečnosti informací, které jsou stanoveny technickou normou ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.

III.
Umístění serveru

1) Server musí být umístěn v prostoru, který je určen pro umístění informační a komunikační techniky v nepřetržitém provozu a zajišťuje serveru stabilní provoz bez okolních vlivů (dále jen „datové centrum“).
2) V datovém centru přijme provozovatel hazardní hry k zajištění fyzické bezpečnosti serveru opatření
   - zabezpečující ochranu na úrovni objektu, v němž je umístěno datové centrum,
   - zamezující neoprávněnému vstupu do datového centra,
   - zamezující poškození a zásahu do datového centra a
   - předcházející poškození, odcizení nebo zneužití serveru nebo přerušení jeho provozu.
3) K zajištění fyzické bezpečnosti datového centra použije provozovatel hazardní hry u opatření podle předchozího odstavce prostředky fyzické bezpečnosti, a to alespoň
   - mechanické zábranné prostředky,
   - zařízení elektrické zabezpečovací signalizace,

- prostředky omezující působení požárů,
- prostředky omezující působení projevů živelních událostí,
- systémy pro kontrolu vstupu,
- kamerové systémy,
- zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a
- zařízení pro zajištění optimálních provozních podmínek.

IV.
Generátor náhodných čísel

1) V zařízení, které podle bodu I. musí obsahovat generátor náhodných čísel, musí být generátor náhodných čísel zdrojem náhody.
2) Generátor náhodných čísel je buď samostatně stojící součást zařízení nebo integrovaná součást serveru nebo koncového zařízení. Pro identifikaci samostatně stojícího generátoru náhodných čísel se použijí obdobně podmínky stanovené v bodě VIII.
3) Generátor náhodných čísel musí být takové povahy, aby
   - náhodný proces tvorby výsledku hry nebylo možné ovlivnit a
   - výsledek náhodného procesu
     - byl nezávislý na předchozích výsledcích,
     - odpovídal v pravděpodobnosti dosažení jednotlivých možných výsledků hazardní hry teoretickým pravděpodobnostem a
     - byl nepředvídatelný bez úplné znalosti postupu tvorby výsledku hry včetně všech nastavení nebo počátečních hodnot.
4) Generátor náhodných čísel, který využívá ke stanovení herního výsledku deterministický algoritmus, musí
   - pracovat s délkou periody alespoň 2^{64} zabezpečující generování náhodného procesu tak, aby v případě konkrétní hazardní hry nedocházelo k rozpoznatelnému opakování výsledků,
   - vytvářet posloupnost výsledků hry na základě počátečních hodnot, které jsou náhodné nebo nepředvídatelné, a
   - být integrovanou součástí serveru nebo koncového zařízení.
5) Generátor náhodných čísel, který využívá ke stanovení herního výsledku fyzikální jevy, musí v případě, že využívá
   - makroskopické jevy, zejména kostky, ruletové kolo nebo losovací osudí, využívat k náhodnému procesu tvorby výsledku hry předměty vyrobené z nezměnitelného materiálu, u kterého nedochází běžným užíváním k jeho opotřebení,
   - mikroskopické jevy, zejména šum nebo kvantové jevy, být integrovanou součástí serveru nebo koncového zařízení.
6) Dochází-li při tvorbě výsledku hry na základě rozsahu hodnot generované posloupnosti náhodných čísel k dalšímu zpracování výsledků náhodného procesu, musí být software

k tomu určený součástí serveru nebo koncového zařízení a musí být zajištěno, že toto zpracování splňuje požadavky na výsledek náhodného procesu podle odstavce 3 tohoto bodu.

V.
Kryptografické prostředky

Pro přenos a ukládání herních a finančních dat a přístup k softwaru zařízení musí být v zařízení používány kryptografické algoritmy a kryptografické klíče splňující minimální požadavky na kryptografické algoritmy uvedené v příloze tohoto standardu tak, aby byla zajištěna nezměnitelnost a důvěrnost herních a finančních dat a softwaru zařízení.

VI.
Ukládání herních a finančních dat

1) Zařízení musí využívat takového mechanismu ukládání herních a finančních dat, aby nemohlo dojít k jejich ztrátě.

2) Provozovatel hazardní hry je za účelem splnění povinnosti podle odstavce 1 tohoto bodu povinen zálohovat herní a finanční data uložená na serveru tak, aby byla zajištěna kompletní obnova herních a finančních dat, zejména zajistit zálohování herních a finančních dat v dostatečné vzdálenosti od datového centra nebo jiným způsobem tak, aby nemohlo dojít ke ztrátě záložní sady finančních a herních dat ze stejného důvodu, z jakého může dojít ke ztrátě herních a finančních dat uložených na serveru.

POŽADAVKY NA KONCOVÉ ZAŘÍZENÍ PROVOZOVANÉ V HERNÍM PROSTORU

VII.
Uvedení koncového zařízení do provozu

Koncové zařízení může být provozovatelem v herním prostoru instalováno, reinstalováno nebo odpojeno pouze osobou, která pro něj zajišťuje odborný servis koncových zařízení.

VIII.
Identifikace koncového zařízení

1) Koncové zařízení musí být označeno jedinečným identifikačním štítkem ve formě registrační známky vydávané pověřenou osobou.

2) Registrační známka musí být pevně připevněna na přední nebo boční straně vnějšího pláště koncového zařízení, a to tak, aby byla viditelná.

IX.
Vnější zabezpečení koncového zařízení

1) Koncové zařízení musí být takové konstrukce, aby bylo zamezeno násilnému či jinému nedovolenému vniknutí do koncového zařízení za užití síly takové intenzity, kterou je možné očekávat.

2) Koncové zařízení musí být vybaveno čidlem nebo jiným bezpečnostním zařízením, které zaznamená pokus o násilné či jiné nedovolené vniknutí do koncového zařízení, odpojení

nebo ovlivnění napájecích nebo datových kabelů nebo jiné ovlivnění jeho provozu. Čidlo nebo jiné bezpečnostní zařízení musí rovněž zaznamenat veškeré autorizované vstupy do vnějších uzamykatelných částí koncového zařízení.

3) Při pokusu o násilné či jiné nedovolené vniknutí do koncového zařízení, o odpojení nebo ovlivnění napájecích nebo datových kabelů nebo o jiné ovlivnění jeho provozu musí být koncové zařízení automaticky přepnuto do chybového stavu, kterým se rozumí stav, při kterém není umožněna hra technické hry ani jiné transakce v uživatelském kontu.

4) Nenaznačuje-li již čidlo nebo bezpečnostní zařízení nutnost dalšího trvání chybového stavu, může být automaticky obnoven provoz koncového zařízení.

5) Koncové zařízení musí být vybaveno systémem, který v případě, že nelze obnovit provoz koncového zařízení automaticky podle odstavce 4 tohoto bodu, informuje obsluhu herního prostoru (dále jen „obsluha“) o trvajícím chybovém stavu. K obnovení provozu koncového zařízení z trvajícího chybového stavu může dojít pouze na základě autorizovaného zásahu obsluhy. Pokud nelze chybový stav odstranit bezodkladně, na základě autorizovaného zásahu proplatí obsluha sázejícímu výhru po ověření její výše na příslušném elektronickém ukazateli a sázejícího odhlásí z jeho uživatelského konta, odstavec 3 tohoto bodu tímto není dotčen.

X.
Vnitřní zabezpečení koncového zařízení

1) Veškeré části koncového zařízení, jejichž manipulací by mohl být ovlivněn náhodný proces výsledku hry nebo dálkový přenos výsledku hry nebo uchovávání herních a finančních dat a jejich dálkový přenos na server, musí být umístěny ve vnitřní samostatně uzamykatelné části koncového zařízení.

2) Ve vnitřní samostatně uzamykatelné části musí být umístěny alespoň

   - software sloužící k řízení činnosti koncového zařízení,
   - generátor náhodných čísel, je-li jím koncové zařízení vybaveno,
   - software zabezpečující telekomunikační datové spojení se serverem,
   - software k řízení systému zobrazovacího zařízení,
   - software k řízení systému úložiště bankovek a mincí a
   - úložiště bankovek a mincí.

3) Je-li koncové zařízení vybaveno generátorem náhodných čísel, musí být ve vnitřní samostatně uzamykatelné části rovněž umístěny systémy počítadel.

4) Požadavek na umístění ve vnitřní samostatně uzamykatelné části koncového zařízení podle odstavců 1 až 3 tohoto bodu neplatí pro generátor náhodných čísel, který zároveň slouží k zobrazení výherní kombinace nebo jiného výsledku hry, a systém počítadel, je-li s generátorem náhodných čísel funkčně nedělitelný. Taková část koncového zařízení musí splnit podmínky vnějšího zabezpečení podle bodu IX.

5) Úložiště bankovek a mincí musí být umístěno ve vnitřní samostatně uzamykatelné části určené výhradně pro tento účel.

6) Vnitřní samostatně uzamykatelné části musí být vybaveny samostatným zabezpečením, které splňuje podmínky bodu IX.

XI.
Zobrazovací zařízení

1) Každá herní pozice musí být vybavena obrazovkou nebo jiným zobrazovacím zařízením.

2) Je-li herní pozice vybavena dotykovou obrazovkou, musí být obrazovka přesná a nesmí obsahovat žádné skryté nebo neoznačené tlačítko nebo dotykový bod, který může ovlivnit hru, s výjimkou případů uvedených v herním plánu.

3) Koncové zařízení, které je vybaveno generátorem náhodných čísel, který zároveň slouží k zobrazení výherní kombinace nebo jiného výsledku hry, nebo je vybaveno mechanickou nebo elektromechanickou částí, která slouží výhradně k zobrazení výherní kombinace nebo jiného výsledku hry, musí být konstruováno takovým způsobem, aby se zobrazované výsledky shodovaly s ukazateli na obrazovce herní pozice; pokud se neshodují, přepne se koncové zařízení automaticky do chybového stavu.

XII.
Telekomunikační datové spojení

1) Každé koncové zařízení musí být vybaveno telekomunikačním datovým spojením se serverem, které slouží k přenosu herních a finančních dat, a to za jednotlivé herní pozice po každé odehrané hře technické hry.

2) Koncové zařízení, které neobsahuje generátor náhodných čísel, musí být vybaveno takovým telekomunikačním datovým spojením, které pracuje při přenosu výsledku hry s dobou odezvy nižší než 0,3 vteřiny.

XIII.
Tiskárna

1) Každé koncové zařízení musí být vybaveno tiskárnou nebo být připojeno k tiskárně takovým způsobem, aby po stisku tlačítka umístěného na dotykové obrazovce nebo vnějším plášti koncového zařízení bylo možné v herním prostoru vytištění dokladu o zůstatku na uživatelském kontu.

2) Doklad o zůstatku na uživatelském kontu musí obsahovat alespoň

   - identifikační údaje provozovatele hazardních her,
   - označení provozovny,
   - výrobní číslo herní pozice,
   - identifikační údaje hráče,
   - datum a čas vytištění a
   - jedinečný identifikátor dokladu o zůstatku na uživatelském kontu.

3) Koncové zařízení musí na obrazovce herní pozice zobrazit informaci o tom, že nastala skutečnost nebo se vyskytla závada, která znemožňuje tisk.

XIV.
Systémy počítadel

1) Koncové zařízení, které obsahuje generátor náhodných čísel, musí být vybaveno alespoň dvěma na sobě nezávislými systémy počítadel, které zaznamenávají součty jednotlivých skupin herních a finančních dat určených k uchovávání na místě, a to
    - elektronickými a
    - elektromechanickými nebo pulsními.
2) Počítadla musí být alespoň osmimístná; v případě, že zaznamenávají rovněž části peněžních jednotek musí být počítadla alespoň desetimístná.
3) Koncové zařízení musí ukládat data podle odstavce 1 tohoto bodu takovým způsobem, aby bylo možno kdykoli provést statistické testy ověřující hodnoty parametrů koncového zařízení nebo hazardní hry, které jsou stanoveny v zákoně o hazardních hrách.

XV.
Přijímání bankovek a mincí

1) Přijímá-li koncové zařízení bankovky a mince, musí být konstruováno takovým způsobem, aby bylo chráněno proti vandalismu, zneužití nebo podvodné činnosti.
2) Koncové zařízení musí být schopno určit směr a rychlost bankovky nebo mince při vložení do zařízení. Není-li bankovka nebo mince vkládána běžným způsobem, musí být koncové zařízení automaticky přepnuto do chybového stavu.
3) Všechny přijímané bankovky a mince musí být uloženy do úložiště bankovek a mincí v koncovém zařízení.
4) Hodnota každé přijaté bankovky a mince musí být neprodleně zobrazena na ukazateli zůstatku na uživatelském kontu. V případě, že provozovatel technické hry za použití bezpečných a spolehlivých metod umožňuje pro vkládání peněžních prostředků na uživatelské konto bezhotovostní platby, použije se věta první i na takto přijaté peněžní prostředky.
5) Zařízení nesmí umožnit vložení bankovek nebo mincí nebo musí odmítnout a vrátit vložené bankovky a mince, je-li nefunkční nebo je-li v chybovém stavu.

Minimální požadavky na kryptografické algoritmy

I. Symetrické algoritmy

a) Blokové a proudové šifry pro ochranu důvěrnosti a integrity

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů Triple Data Encryption Standard (3DES) s využitím délky klíčů 168 bitů, omezené použití jen se zatížením klíče menším než 10 GB, postupně přecházet na AES,

2. Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu,

3. Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB,

4. Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB,

5. Twofish s využitím délky klíčů 128 až 256 bitů,

6. Serpent s využitím délky klíčů 128, 192, 256 bitů,

7. Camellia s využitím délky klíčů 128, 192 a 256 bitů,

8. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů.

b) Módy šifrování s ochranou integrity

1. CCM,

2. EAX,

3. OCB,

4. Složená schémata typu „Encrypt-then-MAC“.

Poznámka:

Schémata typu „Encrypt-then-MAC“, musí používat k šifrování pouze uvedené šifrovací módy a k výpočtu MAC pouze uvedené módy pro ochranu integrity.

c) Módy šifrování

1. CTR,

2. OFB,

3. CBC,

4. CFB.

Poznámka:

Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným inicializačním vektorem, při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru, při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače, v případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

d) Módy pro ochranu integrity

1. HMAC,

2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 109 MAC,

3. CBC-MAC-EMAC,

4. CMAC.

II. Asymetrické algoritmy

a) Pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více,

2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů a více,

3. Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů a více.

b) Pro procesy dohod na klíči a šifrování klíčů

1. Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů a více, délky parametru cyklické podgrupy 224 bitů a více,

2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů a více,

3. Elliptic Curve Integrated Encryption System - Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více,

4. Provably Secure Elliptic Curve - Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů a více,

5. Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více,

6. Rivest Shamir Adleman - Optimal Asymetric Encryption Pedding (RSA-OAEP) s využitím délky klíčů 2048 a více,

7. Rivest Shamir Adleman - Key Encapculation Mechanism (RSA-KEM) s využitím délky klíčů 2048 a více.

III. Algoritmy hash funkcí

a) SHA-2

1. SHA-224,

2. SHA-256,

3. SHA-384,

4. SHA-512,

5. SHA-512/224,

6. SHA-512/256.

b) SHA-3

1. SHA3-224,

2. SHA3-256,

3. SHA3-384,

4. SHA3-512,

5. SHAKE-128,

6. SHAKE-256.

c) Ostatní hashovací funkce

1. Whirpool,

2. RIPEMD-160,

3. SHA 1 s omezeným použitím.

Poznámka:

SHA-1 se nesmí používat pro generování nových digitálních podpisů, časových razítek, jakékoliv jiné aplikace vyžadující nekolizní SHA-1.

SHA-1 lze používat pouze pro ověřování již existujících digitálních podpisů a časových razítek, generování a ověřování HMAC-SHA1, funkce pro odvozování klíčů a pseudonáhodné generátory náhodných čísel.