ВОЈНОТЕХНИЧКИ ИНСТИТУТ
Београд, Ратка Ресановића 1, тел (011) 2508-308, факс (011) 2508-474
www.vti.mod.gov.rs/infolab infolab@vti.vs.rs

Упутство за проверу безбедности информација у ИКС за приређивање посебних игара на срећу на аутоматима

Q3-120-047

Обавезна примена од:
25.05.2021.

О Д О Б Р А В А :
ДИРЕКТОР
п у к о в н и к
др Бојан Павковић, дипл. инж.

С А Д Р Ж А Ј

Издање број: **1**	Број измена					Ознака копије:
Укупно страна: **9**						
Прво издање:25.05.2021.						

1. ПРЕДМЕТ УПУТСТВА

Овим упутством се дефинише поступак провере техничких и функционалних карактеристика сегмента безбедности информација ИКС за приређивање посебних игара на срећу на аутоматима.

2. ПОДРУЧЈЕ ПРИМЕНЕ

Упутство се примењује у процесу провере испуњености техничких и функционалних карактеристика опреме за приређивање игара на срећу на аутоматима, а у домену безбедности информација. Примена упутства је обавезна за сва физичка и правна лица која су на било који начин укључена у процес провере.

3. ТЕРМИНИ, ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

3.1. Дефиниције

Приређивач: је организатор игара на срећу на аутоматима.

Лабораторија: је лабораторија за проверу испуњености информатичких карактеристика опреме за приређивање игара на срећу на аутоматима.

Апликативни софтвер: је програм који је дизајниран за помоћ корисницима при извршавању неког задатка (прикупљање података са аутомата).

Инсталација: је поставка софтерског производа на рачунар

Софтвер: је скуп инструкција, програма и процедура које се упућују процесору рачунара, а на основу којих он извршава специфичне операције.

Хардвер: је скуп физичких елемената уграђених у рачунарски систем.

Играч: је физичко лице, које учествује у играма на срећу на аутомату.

Аутомат: је самостални уређај/систем који омогућава играчу да учествује у процесу игара на срећу.
У документу су коришћени и изрази страног порекла, писани етимолошки или фонетски.

3.2. Скраћенице

ИКС: Информационо комуникациони систем за приређивање посебних игара на срећу на аутоматима,

DNS: Domain name system - Систем имена домена - хијерархијски и децентрализовани систем именовања рачунара повезаних на Интернет или приватну мрежу,

КИУ: Контролор испуњености услова (руководилац лабораторије),

КПБП: Контролор за проверу безбедности података,

КИУИКС: контролор испуњености техничких и функционалних услова ИКС.

4. ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

- ПРАВИЛНИК (П1) о информационо-комуникационом систему за приређивање посебних игара на срећу на аутоматима – Сл. гласник РС 152/2020.,
- ПРАВИЛНИК (П2) о техничким и функционалним карактеристикама столова и аутомата за игре на срећу, начину и поступку испитивања испуњености потребних услова – Сл. гласник РС 152/2020.,

- ПРАВИЛНИК (П3) о облику и садржини налепнице за означавање и регистрацију столова, аутомата за игре на срећу и уплатно-исплатних места у кладионици – Сл. гласник РС 152/2020.,
- ПРАВИЛНИК (П4) о условима за обављање поправке столова и аутомата за игре на срећу – Сл. гласник РС 152/2020.,
- ПРАВЛНИК (П5) о изменама и допунама правилника о техничким и функционалним карактеристикама столова и аутомата за игре на срећу, начину и поступку испитивања испуњености потребних услова – Сл. гласник РС 152/2020.,
- ПРАВИЛНИК (П6) о изменама и допунама правилника о условима за обављање поправке столова и аутомата за игре на срећу – Сл. гласник РС 152/2020.,
- ПРАВИЛНИК (П7) о ближим условима за спровођење аудио и видео надзора, начину чувања документације и телесне заштите у играчници, спровођење видео надзора и чување документације у аутомат клубу, односно кладионици – Сл. гласник РС 152/2020.,
- Q2-080-001 Процедура за преиспитивање захтева, дефинисање понуде и уговарање услуга,
- Q3-120-043 Упутство за проверу испуњености техничких и функционалних карактеристика информационо комуникационог система за приређивање посебних игара на срећу на аутоматима,
- Q3-120-044 Упутство за проверу рачунарке мреже ИКС за приређивање посебних игара на срећу на аутоматима,
- Q3-120-045 Упутство за проверу системског и апликативног софтвера и хардвера ИКС-а за приређивање посебних игара на срећу на аутоматима,
- Q3-120-046 Упутство за проверу испуњености техничких и функционалних карактеристика аутомата за приређивање посебних игара на срећу,
- Q3-120-048 Упутство за проверу подсистема џекпот ИКС за приређивање посебних игара на срећу на аутоматима,
- Q3-120-049 Упутство за проверу испуњености техничких и функционалних карактеристика столова за приређивање посебних игара на срећу
- SRPS ISO/IEC 25023:2017 - Системски и софтверски инжењеринг – Захтеви за квалитет и вредновање система и софтвера (SQuaRE) – Мерење квалитета системских и софтверских производа,
- SRPS ISO/IEC 25040 (ен) - Системски и софтверски инжењеринг – Захтеви за квалитет и вредновање система и софтвера (SQuaRE) – Процес вредновања,
- SRPS ISO/IEC 27001:2014 Информационе технологије-Технике безбедности-Системи менаџмента безбедношћу информација-Захтеви

НАПОМЕНА: Код примене референтног документа важи последње издање (укључујући и његове измене)

5. БЕЗБЕДНОСТИ ИНФОРМАЦИЈА У ОКВИРУ ИКС

За проверу безбедности информација, потребно је доставити документе:
- општу изјаву о безбедности,
- политика безбедности података,
- административне контроле,
- надгледање и праћење ИКС,
- контрола природе и животне средине.

5.1. Општа изјава о безбедности

Овом изјавом приређивач дефинише безбедност следећих елемената ИКС:

- Компоненте ИКС које генеришу, преносе, обрађују или процесирају случајне бројеве да би се одредио исход игре.
- Компоненте ИКС које смештају и обрађују податке о тренутном стању улога играча.
- Тачкама улаза и излаза из ИКС и његових подсистема.
- Комуникационе мреже које преносе конвертоване податке са аутомата на сервер.

5.2. Политика безбедности података

Документ који дефинише политику безбедности података треба да опише активности лица (оператора) које управља подацима о безбедности и које управља спровођењем политике безбедности. Политика безбедности података треба да:

- дефинише улогу оператора у измени и/или допуни ИКС.
- буде одобрена од стране руководства,
- буде саопштена свим запосленим и релевантним спољашњим учесницима,
- буде преиспитана у планираним временским интервалима.

5.3. Административне контроле

Административне контроле подразумевају групу докумената коју креира приређивач и чијом применом се остварују циљеви безбедности информација у ИКС.

5.3.1. Безбедност људских ресурса

Ови документи треба да дефинишу безбедносне улоге и одговорности запослених, а у складу са подацима о безбедносној политици:

- Сви запослени у организацији добијају одговарајућу обуку о значају безбедности и редовно се ажурира организациона политика и процедуре које су потребне за функционисање њиховог посла.
- Политика контроле приступа мора бити установљена, документована и базирана на безбедносним захтевима за физички и логички приступ ИКС и/или његовим компонентама.
- Запосленима треба обезбедити олакшице при приступу сервисима за чије коришћење је потребно овлашћење.
- Права приступа свих запослених ИКС и/или његовим компонентама треба да буду уклоњена након престанка њиховог радног односа , уговора или споразума , и биће прилагођена насталим променама.

5.3.2. Услуге трећих лица

Безбедносне улоге и одговорности трећих лица која пружају услуге за правилно функционисање ИКС, треба да буду дефинисане и документоване у складу са подацима о безбедносној политици:

- Споразуми са трећим лицима која пружају услуге, укључују приступ, обраду или управљање ИКС и/или његовим компонентама морају обухватити све релевантне безбедносне захтеве.
- Услуге, извештаји и евиденције које пружа треће лице морају се пратити и контролисати од стране руководства најмање једном годишње.

5.3.3. Управљање имовином

Сва имовина, укључујући и радно окружење ИКС и/или његових компоненти , мора имати номинованог власника у складу са безбедносном политиком:

- Попис треба да буде сачињен за сву имовину.
- Средства се класификују у зависности од њихове критичности, осетљивости и вредности.
- Свако средство мора да има одређеног "власника" који мора да обезбеди да се подаци и средства класификују на одговарајући начин. Такође је одговоран за периодични преглед средстава.
- Мора се дефинисати поступак за уклањање средства из употребе, као и за додавање нових средстава.
- Расходована опрема мора да се уклони и одложи безбедно користећи документоване процедуре.

5.3.4. Управљање кључевима за шифровање

Управљање кључевима за шифровање морају бити такође у складу са безбедносном политиком:

- Процес добијања или генерисања кључева за шифровање мора бити документован.
- Ако је кључ истекао, такође мора бити документован процес за управљање.
- Мора да постоји документован процес за укидање кључева .
- Мора да постоји документован процес за безбедно мењање тренутног шифровања сета кључева.
- Мора да постоји документован процес којим се одређује место за складиштење свих кључева за шифровање .
- Мора да постоји начин да се опорави шифрован податак са истеклом енкрипцијом кључа за одређени временски период након што је кључ за шифровање постао неважећи.

5.3.5. Управљање инцидентима

Поступак извештавања о инциденту везаном за безбедност података мора бити документован у складу са политиком безбедности података.

- Процес управљања инцидентима мора да садржи дефиницију шта представља инцидент када је у питању безбедност података.
- Процес управљања инцидентима мора документовати на који начин се извештава о инциденту преко одговарајућих канала управљања.
- Процес управљања инцидентима се врши према процедурама које обезбеђују брз и ефикасан одговор у вези са инцидентом , укључујући:
    - Процедуре за руковање различитим врстама инцидената везаних за безбедност података,
    - Процедуре за анализу и идентификацију узрока инцидента,
    - Комуникација са онима који су погођени овом инцидентом,
    - Извештавање о инциденту одговарајућем органу,
    - Контролисан опоравак од инцидената везаних за безбедност података.

5.3.6. Пословање и опоравак од „испада“ система

У случају да ИКС постане неоперабилан, неопходно је обезбедити његов опоравак кроз:

- План за опоравак који мора да садржи метод за чување података о игри. Ако се користи копија података, метод за опоравак података треба да буде описан,

- План за опоравак који мора да разграничи околности под којима ће бити примењен.
- План за опоравак који мора да обезбеди да се подаци значајни за опоравак (recovery site) физички одвоје од података који се користе у процесу имплементације (production site).
- План за опоравак који мора да садржи упутства за опоравак са детаљно описаним корацима за поновно успостављање функционалности игре на recovery site-у.
- План пословања мора да садржи процесе потребне за обнову и наставак играчких активности након активирања опоравка система, коришћењем различитих сценарија за одговарајући ИКС.

5.4. Надгледање и праћење ИКС

ИКС мора имати уграђено праћење критичних компоненти (нпр. аутомата, централних хостова, мрежних уређаја, firewall, праћење спољашњих линкова, итд.).

Приређивач је дужан да на видном месту, на улазу у играчницу, као и у унутрашњости просторија, истакне обавештење да је простор под аудио и видео надзором.

Истицањем обавештења сматра се да је лице обавештено о обради личних података.

Приређивач је приликом обраде података дужан да поступа у складу са прописима којима се уређује заштита података о личности.

Надгледање догађаја на аутоматима се обезбеђује видео надзором у свакој играчници. Праћење преко видео стрима мора бити у реалном времену. Видео стрим мора имати и временски запис.

Непрекидан видео надзор обухвата снимање:

- уласка - изласка из аутомат клуба, односно кладионице,
- аутомата за игре на срећу,
- уплатно-исплатног места,
- играча и посетилаца.

Мрежа за видео надзор мора бити логички одвојена од других рачунарских мрежа.

Лабораторији је потребно доставити следећу документацију видео надзора:

- Пројекат изведеног видео надзора у свакој играчници,
- Процедуре које описује поступак архивирања видео података,
- Карактеристике сториџ опреме,
- Техничке карактеристике камера и монитора за праћење,
- За софтвер видео надзора,
- Процедуре за управљање видео надзором.
- Акти којима се именују лица за управљање видео надзором.

Критична компонента видео надзора која не испуњава захтеве тестова надгледања и праћења мора се одмах искључити из система. Компонента не сме бити враћена у рад док не постоји документован доказ да је грешка исправљена.

5.4.1. Праћење

- Сатови свих компоненти ИКС морају бити синхронизовани са договореним извором времена у циљу обезбеђивања конзистентог креирања Log датотеке.

- Log датотека мора садржати податке о активностима корисника , о изузецима и податке који се тичу безбедности и који ће бити креирани и чувани у одговарајућем периоду ради помоћи будућим истрагама и надзора контроле приступа.
- Активности систем администратора и оператора система морају бити записане у Log датотеци.
- Log подаци морају бити заштићени од неовлашћеног приступа.
- Свака измена, покушај измене, приступ подацима или друга промена или приступ Log датотеци мора бити детектован од стране ИКС. Систем мора имати могућност да се види ко је прегледао или мењао дневник и када су вршене измене.
- Log датотека праћења активности мора да се периодично разматра користећи одговарајућу документацију. Запис сваког прегледа мора мора бити документован.
- Било која грешка у раду ИКС мора бити пријављена и анализирана, и предузете одговарајуће мере.
- Мрежни уређаји са ограниченим капацитетом складиштења морају онемогућити сву комуникацију уколико се попуни Log датотека.

5.4.2. Контрола криптографије

Политика о коришћењу и контроли криптографије мора бити примењена за заштиту података:

- Сваки поверљив или лични податак мора бити криптован.
- Квалитет криптовања мора бити у складу са степеном поверљивости података.
- Употреба алгоритама за шифровање мора бити периодично преиспитана од стране квалификованих запослених лица са циљем обезбеђивања безбедног шифровања.
- Промене алгоритама за шифровање у циљу исправљања недостатака морају бити реализоване на што бржи начин. Ако то није могуће, алгоритам мора бити замењен.
- Крипто кључеви не смеју се чувати без одговарајуће крипто заштите.

5.4.3. Контрола приступа

Расподела привилегија приступа мора бити ограничена и контролисана на основу пословних захтева и принципа најмањих привилегија.

- Процедура за регистрацију и одјављивање мора бити на месту за давање и укидње приступа свим сегментима ИКС.
- Сви корисници имају јединствени идентификатор корисника.
- Лозинка мора бити контролисана путем формалног процеса управљања.
- Лозинке морају да испуњавају пословне захтеве за дужину (број знакова), сложеност и трајање (временско).
- Приступ апликацији и оперативном систему мора бити контролисан безбедним Log поступком.
- Поред лозинке, за контролу приступа удаљених корисника користити одговарајуће методе аутентичности.
- Сваки физички приступ деловима ИКС, као и сваки логички приступ апликацији или оперативном систему, мора бити забележен .
- Употреба опреме за аутоматизовану идентификацију и аутентификацију везе са појединих локација, као и сама опрема морају бити формално документоване и бити укључени у редован преглед права приступа од стране менаџмента .

- За апликације које садрже висок ниво ризика време предвиђено за конекцију мора бити ограничено.
- Употреба апликација које би могле да промене функционалности системских апликација, као и контролних апликација мора бити ограничено и строго контролисано.

5.4.4. Firewall

- Firewall (заштита од неауторизованог приступа) мора да се налази на граници било која два различита домена безбедности .
- Сви сегменти ИКС морају да имају најмање један ниво заштите.
- Firewall је део оперативног система са следећим карактеристикама:
    - само апликације у релацији са Firewall-ом се могу налазити на Firewall-у , и
    - само ограничен број налога може бити представљен Firewall-у (нпр. само налог администратора система)
- Firewall мора одбацити све конекције осим оних које су посебно одобрене .
- Firewall мора да одбаци све конекције са дестинација које нису на мрежи из које потиче порука (нпр. РФЦ1918 адресе на јавној страни интернет Firewall-а.)
- Firewall мора да одржава дневник ревизија за све промене параметара који контролишу конекције које су дозвољене од стране Firewall-а.
- Firewall мора да одржава дневник ревизија за све успешне и неуспешне покушаје конектовања. Евиденција о покушајима мора да се чува 90 дана и да се прегледа месечно због неочекиваног саобраћаја.
- Firewall мора да онемогући сву комуникацију уколико је дневник ревизија попуњен.

5.4.5. Даљински приступ

Даљински приступ треба дефинисати као било који приступ ван система ИКС, укључујући било који приступ из других мрежа у оквиру мрежа приређивача. Када је дозвољен, даљински приступ ће прихватити само удаљене конекције дозвољене применом firewall-а и ИКС подешавања. Безбедност удаљеног приступа треба да се проверава за сваки појединачни случај. Такође:

- Неовлашћен удаљени корисник нема право да ради послове администратора (додавање корисника, мењање дозволе , итд),
- Неовлашћен удаљени корисник нема право да приступа бази података, осим да проналази податке коришћењем постојећих функција,
- Неовлашћен удаљени корисник нема право да приступа оперативном систему,
- ИКС мора да води евиденцију које описују деловање преко удаљеног приступа.

5.4.6. Копије

Бекап односно копије података и софтвера се праве редовно, и морају бити редовно тестиране у складу са политиком прављења копија.

5.5. Контрола природе и животне средине

5.5.1. Зоне безбедности

ИКС приређивача морају бити смештени у објектима који пружају физичку заштиту од пожара , поплава, земљотреса и других облика природних или изазваних катастрофа.

- Безбедност (препреке као што су зидови, картица која контролише улазак или излазак) се мора користити ради заштите области у којима су смештене ИКС компоненте,

- Безбедносна подручја морају бити заштићена одговарајућим контролама уласка, како би се осигурало да је приступ ограничен само на овлашћено особље,
- Сваки приступ мора бити забележен у безбедној евиденцији,
- Покушај неовлашћеног приступа мора бити регистрован.

5.5.2. Опрема за безбедност игре

- Сервери ИКС морају бити лоцирани у сервер собама које ограничавају неовлашћен приступ.
- Сервери ИКС морају бити смештени у полицама које се налазе у безбедном окружењу.

5.5.3. Заштита ИКС

- Све компоненте ИКС морају бити обезбеђене адекватним основним напајањем.
- Све компоненте ИКС морају имати уређај за непрекидно напајање (УПС), који је подршка у случају нестанка струје.
- Потребно је имати адекватан систем хлађења за опрему која је смештена у серверској соби.
- Напајање и телекомуникациони каблови за пренос података или подршку информационим сервисима морају бити заштићени од пресретања или оштећења.
- Потребно је обезбедити адекватну заштиту од пожара за компоненте ИКС које су смештене у серверској соби.

НАПОМЕНА:
Елементи наведени под тачком 5. проверавају се увидом у документацију, као и „online“ приступом ресурсима подносиоца захтева-приређивача.

6. ПРЕГЛЕД ЗАПИСА

Као резултат спроведених активности настају следећи индиректни записи:

- Извештај о извршеној провери техничких и функционалних карактеристика ИКС за приређивање посебних игара на срећу на аутоматима; према прилогу 4, Упутства Q3-120-043.
- Извештај о извршеној допунској провери техничких и функционалних карактеристика ИКС за приређивање посебних игара на срећу на аутоматима; према прилогу 5, упутства Q3-120-043.

7. ОДГОВОРНОСТИ И ОВЛАШЋЕЊА

За реализацију појединих активности одговорна су лица која су одређена да учествују у спровођењу упутства. За контролу и примену овог упутства одговоран је КПБП.