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 игара на срећу преко средстава електронске комуникације

Q3-120-036

Обавезна примена од: **28.05.2021.**

О Д О Б Р А В А :
ДИРЕКТОР
пуковник
др Бојан Павковић, дипл. инж.

С А Д Р Ж А Ј

Издање број: **2**	Број измена					Ознака копије:
Укупно страна: **10**	1					
Прво издање: 02.06.2014.						

1. ПРЕДМЕТ УПУТСТВА

Овим упутством се дефинише поступак за сертификацију софтвера којима се проверава безбедност података. Настало је ревизијом документа Q3-120-036 Упутство за проверу безбедности информација, од 02.06.2014.год.

2. ПОДРУЧЈЕ ПРИМЕНЕ

Упутство се примењује у процесу провере испуњености информатичких услова опреме за прирећивање игара на срећу путем средстава електронске комуникације, а у домену безбедности информација. Примена упутства је обавезна за сва правна и физичка лица која су на било који начин укључена у процес провере.

3. ТЕРМИНИ, ДЕФИНИЦИЈЕ И СКРАЋЕНИЦЕ

3.1. Дефиниције

Прирећивач: је организатор игара на срећу путем средстава електронске комуникације.

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

Апликативни софтвер: је програм који је дизајниран за помоћ корисницима при извршавању неког задатка.

Инсталација: је поставка софтерског производа на рачунар.

Синтакса: скуп правила.

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

Трансакционо програмирање: је извршавање скупа наредби по принципу „све или ништа“. Уколико се из било ког разлога прекине извршавање програма у току извршавања трансакционог блока, биће поништен резултат већ извршених наредби.

Хардвер: је скуп физичких елемената уграђених у компјутерски систем (нпр. монитор, тастатура, миш, процесор и др.).

3.2. Скраћенице

ИКС: Информационо комуникациони систем за прирећивање игара на срећу преко средстава електронске комуникације,

УИС: Управа за игре на срећу,

КИУ: Контролор испуњености услова (руководилац лабораторије),

КТИРМ: Контролор техничке исправности рачунарске мреже ИКС за игре на срећу преко средстава електронске комуникације,

КПБП: Контролор за проверу безбедности података ИКС за игре на срећу преко средстава електронске комуникације,

КИУИКС: контролор испуњености техничких и функционалних услова ИКС,

VPN: Virtual private network (Виртуелна приватна мрежа) - приватна комуникациона мрежа која омогућава корисницима да преко јавне мреже одржавају заштићену комуникацију,

ДСМК: Документи система менаџмента квалитетом.

4. ВЕЗА СА ДРУГИМ ДОКУМЕНТИМА

- Закон о играма на срећу - Сл. гласник РС бр.18/2020,
- Закон о информационој безбедности – Сл. гласник РС бр.6/2016, 94/2017 и 77/2019,
- ПРАВИЛНИК (П1) о информационо-комуникационом систему за приређивање игара на срећу преко средстава електронске комуникације – Сл. гласник РС 152/2020,
- ПРАВИЛНИК (П2) о начину вођења базе података о лицима која су остварила добитак код приређивача игара на срећу – Сл. гласник РС 152/2020,
- ПРАВИЛНИК (П3) 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,
- Q3-120-011 Упутство за проверу испуњености техничких и функционалних карактеристика информационо комуникационог система за приређивање игара на срећу преко средстава електронске комуникације,
- Q3-120-016 Упутство за проверу рачунарске мреже ИКС за приређивање игара на срећу преко средстава електронске комуникације,
- Q3-120-021 Упутство за проверу квалитета системског софтвера и хардвера ИКС за приређивање посебних игара на срећу преко средстава електронске комуникације,
- Q3-120-026 Упутство за проверу квалитета апликативног софтвера ИКС за игре на срећу преко средстава електронске комуникације,
- Q3-120-031 Упутство за проверу поступка регистрације и управљања налогом играча ИКС за игре на срећу преко средстава електронске комуникације,
- Q1-001-001 Пословник о квалитету Војнотехничког института,
- Q2-080-001 Процедура за преиспитивање захтева, дефинисање понуде и уговарање услуга,
- 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 25051 Software engineering-Software product Quality Requirements and Evaluation (SQuaRE)-Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing,
- ISO/IEC/IEEE 26512:2018 - Системски и софтверски инжењеринг – Захтеви за наручиоце и добављаче информација за кориснике,
- SRPS ISO/IEC 27001:2014 - Информационе технологије-Технике безбедности - Правила праксе за контроле безбедности информација

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

5. ЗАХТЕВИ БЕЗБЕДНОСТИ ИКС

Подносилац захтева-приређивач треба да достави Лабораторији број и назив документа, према Прилогу 1 или Прилогу 2, документа Q3-120-026: Упутство за проверу квалитета апликативног софтвера ИКС за игре на срећу преко средстава електронске комуникације,

5.1. Општа изјава

Овим захтевима би се осигурало да играчи нису изложени непотребним ризицима уколико одлуче да учествују у интерактивној игри. Ови безбедносни захтеви ће се примењивати на следеће критичне компоненте интерактивног играчког система.

- Компоненте ИКС које записују, смештају, процесирају, деле, преносе или преузимају осетљиве податке о играчу, на пример : детаљи о кредитној/дебитној картици, подаци о аутентификацији, подаци о рачунима играча.
- 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 наведених система.
- Комуникационе мреже које преносе осетљиве податке о играчима.

5.2. Политика безбедности података

Документ који дефинише политику безбедности података има за циљ да опише приступ оператора који управља подацима о безбедности и који управља спровођењем политике безбедности. Политика безбедности података треба да:

- учествује у процени којом се захтева преиспитивање када долази до измена у ИКС или процеса оператора који мењају профил ризика ИКС.
- буде одобрена од стране руководства;
- буде саопштена свим запосленим и релевантним спољашњим учесницима;
- буде преиспитана у планираним временским интервалима,

5.3. Административне контроле

Безбедност људских ресурса

Безбедносне улоге и одговорности запослених требају бити дефинисане и документоване 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-у и / или његовим компонентама.
- Запосленима треба обезбедити олакшице при приступу сервисима за чије коришћење је потребно овлашћење.
- Права приступа свих запослених у ИКС -у и / или његовим компонентама морају бити уклоњена након престанка њиховог радног односа , уговора или споразума , или ће бити прилагођена насталим променама.

Услуге трећих лица

Безбедносне улоге и одговорности трећих лица која пружају услуге 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-ом и / или његовим компонентама морају обухватити све релевантне безбедносне захтеве.
- Услуге, извештаји и евиденције које пружа треће лице ће се пратити и контролисати од стране руководства најмање једном годишње.
- Права приступа трећим лицима која пружају услуге ИКС-у и / или његовим компонентама морају бити уклоњена након престанка уговора или споразума, односно, потребно је обезбедити могућност промене тих права.

Управљање имовином

Сва имовина, укључујући и радно окружење ИКС-а 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.
- Политика треба да укључи прихватљиво коришћење средстава у складу са ИКС - ом и његовим оперативним окружењем.
- 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.

Управљање кључевима за шифровање

Управљање кључевима за шифровање ће пратити дефинисани процеси 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 .

Ток развоја софтвера

Набавка и развој новог софтвера ће бити дефинисани у складу са политиком безбедности података.

- Инсталационо окружење мора бити логички и физички одвојено од развојног и тест окружења.
- Запослени који раде на развоју софтвера морају бити спречени да мењају код у инсталационом окружењу.
- Мора да постоји документован начин за проверу да се тест софтвер не извршава на инсталационом окружењу.
- Да бисте заштитили личне податке, мора да постоји документован начин да се обезбеди да се изворни подаци не користе у тестирању.

- Сва документација која се тиче развоја софтвера и апликација треба бити доступна и сачувана у току трајања животног циклуса софтверског производа.

Контрола измена

Обављање измена хардвера и софтвера у оквиру ИКС се врши коришћењем формалних процедура, у складу са политиком безбедности података.

Процедуре за контролу измена апликација морају да осигурају да се само одобрене и тестиране верзије апликација имплементирају на инсталационој играчкој платформи.

Контрола измена инсталационе верзије софтвера мора да садржи:

- контролу верзија софтвера или софтверских компоненти ;
- детаље о разлогу за измене ;
- детаље о особи која врши измене;
- копије претходних верзија софтвера ;
- политику која се примењује у случају хитних измена ;
- процедуре за тестирање измена ;
- раздвајање дужности између програмера, тима који обезбеђује квалитет, миграционог тима и корисника;
- процедуре које обезбеђују да се приликом измена изврши ажурирање техничке и корисничке документације.
- све измене треба тестирати кад год је то могуће на платформи која је конфигурисана идентично као циљна платформа. Ако тестирање не може да се темељно спроведе, онда треба изоловати или уклонити неиспитане играчке платформе са мреже или применити налог за корекцију и извршити накнадно тестирање.

Управљање инцидентима

Поступак извештавања о инциденту везаном за безбедност података ће 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 мора обратити одговорном менаџеру и 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.

Пословање и опоравак од „испада“ система

Неопходно је оправити (повратити) већ постојеће стање система у случају да ИКС постане неоперабилан.

- План за опоравак мора садржати метод за чување података о играчевом налогу и подацима о игри. Ако се користи копија података, метод за опоравак података треба да буде описан, или документовати потенцијални губитак података.

- План за опоравак мора разграничити околности под којима ће бити примењен.
- План за опоравак мора обезбедити да су подаци значајни за опоравак (recovery site) физички одвојени од података који се користе у процесу имплементације (production site).
- План за опоравак 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 система

ИКС мора имати уграђено праћење критичних компоненти (нпр. централних хостова, мрежних уређаја, firewalls, праћење спољашњих линкова, итд.). Критична компонента која не испуњава захтеве тестова надгледања и праћења морају се одмах искључити из система. Компонента не сме бити враћена у рад док не постоји документован доказ да је грешка исправљена.

Захтеви за DNS

- Примарни сервер који се користи за решавање DNS упита мора бити физички смештен у центру за безбедан смештај података.
- Логички и физички приступ примарном DNS серверу се мора ограничити на овлашћено особље.
- Мора да постоји бар један секундарни сервер који је у стању да реши DNS упите. Секундарни сервери морају да се налазе у посебном канцеларијском простору у односу на примарни сервер.

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 ће бити записане у Log датотеци.
- Log подаци морају бити заштићени од неовлашћеног приступа.
- Свака измена, покушај измене, приступ подацима или друга промена или приступ било систему или 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 информационог система мора бити пријављена и анализирана, а одговарајуће мере предузете.
- Мрежни уређаји са ограниченим капацитетом складиштења ће онемогућити сву комуникацију уколико се попуни Log датотека.

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.

Контрола приступа

Расподела привилегија приступа ће 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 информационим системима.
- 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 ИКС 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 морају 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.

Firewall

- Firewall (заштита од неауторизованог приступа) се налази на граници било која два различита домена безбедности .
- Сви прикључци на ИКС домаћина морају да прођу кроз најмање једну апликацију, тј. 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-a.
- 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.

Даљински приступ

Даљински приступ се дефинише као било који приступ изван система или система мрежа , укључујући било који приступ из других мрежа у оквиру исте установе . Када је дозвољен, даљински приступ ће прихватити само удаљене конекције дозвољене применом firewall-a и ИКС подешавања. Безбедност удаљеног приступа ће бити проверена 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.

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

Зоне безбедности

ИКС и повезани комуникациони системи 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.

Опрема за безбедност игре

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

Заштита ИКС-а

- 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 ИКС компоненте 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 записи:

- Апликације набављене од акредитованог произвођача (Прилог 1, Упутство Q3-120-026)
- Апликације креиране од стране произвођача (Прилог 2, Упутство Q3-120-026)
- Извештај о извршеној провери испуњености техничких и функционалних карактеристика ИКС за приређивање игара на срећу преко средстава електронске комуникације, (Прилог 4, Упутство Q3-120-011)

7. ОДГОВОРНОСТИ И ОВЛАШЋЕЊА

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