# VĀKŠANAS TIEŠSAISTES SISTĒMAS SERTIFIKĀCIJAS PĀRBAUDES LAPA

| INFORMĀCIJAS DROŠĪBAS GARANTIJAS STANDARTI | | STATUSS | | |
|---|---|---|---|---|
| **Prasības** | **Avots** | **Ieviests** | **Nav ieviests** | **Tiks pilnveidots** |
| Organizatori iesniedz dokumentus, kas pierāda, ka tie atbilst standartā ISO/IEC 27001 noteiktajām prasībām, bez pienākuma to formāli pārņemt. Šim nolūkam tie ir:<br>a) veikuši pilnīgu riska novērtējumu, kurā noteikta sistēmas darbības joma, parādīta ietekme uz darbību, gadījumā ja ir notikuši dažādi informācijas drošības pārkāpumi, uzskaitīti draudi informācijas sistēmai un tās ievainojamība, izveidots riska izvērtējuma dokuments, kurā ir uzskaitīti arī pretpasākumi, lai novērstu šādus draudus, un aizsardzības līdzekļi, kas tiks izmantoti, ja draudi rodas, un, visbeidzot, sagatavots saraksts, kurā prioritārā kārtībā uzskaitīti nepieciešamie uzlabojumi;<br>b) izstrādājuši un īstenojuši pasākumus, kā apieties ar risku, ņemot vērā personas datu aizsardzību un privātās dzīves un ģimenes dzīves aizsardzību, un pasākumus, kuri tiks veikti, gadījumā ja rodas risks;<br>c) rakstveidā noteikuši nenovērstos riskus;<br>d) nodrošinājuši organizatoriskus līdzekļus, lai saņemtu informāciju par jauniem draudiem un drošības uzlabojumiem. | *TS – 2.1. punkts* | | | |

| | | | | |
|---|---|---|---|---|
| Organizatori izvēlas drošības kontroles, kas balstās uz 2.1.punkta a) apakšpunktā noteikto riska analīzi, no šādiem standartiem:<br>1) ISO/IEC 27002; vai<br>2) Informācijas drošības foruma "Labas prakses standarta" (*Information Security Forum's "Standard of Good Practice"),*<br>lai risinātu šādus jautājumus:<br>a) riska novērtējumi (ieteicama ISO/IEC 27005 vai cita īpaša un piemērota riska novērtēšanas metodoloģija);<br>b) fiziskā un vides drošība;<br>c) cilvēkresursu drošība;<br>d) saziņas un operāciju pārvaldība;<br>e) standarta piekļuves kontroles mehānismi papildus tiem, kas noteikti šajā īstenošanas regulā;<br>f) informācijas sistēmu iegāde, izveidošana un uzturēšana;<br>g) informācijas drošības starpgadījumu pārvaldība;<br>h) pasākumi, lai labotu un mazinātu robus informācijas sistēmās, kuru rezultātā varētu notikt apstrādāto datu iznīcināšana, nejauša nozaudēšana, izmainīšana, neatļauta izpaušana vai piekļuve tiem;<br>i) atbilstība;<br>j) datortīklu drošība (ieteicams ISO/IEC 27033 vai "Labas prakses standarts"). EN 18.11.2011 *Official Journal of the European Union* L 301/5<br><br>Šo standartu piemērošanu var ierobežot un attiecināt tikai uz tām organizācijas daļām, kuras ir būtiskas vākšanas tiešsaistes sistēmai. Piemēram, cilvēkresursu drošību var attiecināt tikai uz personālu, kam ir fiziska vai tīkla piekļuve vākšanas tiešsaistes sistēmai, un fizisko/vides drošību var attiecināt tikai uz ēku (ēkām), kur tiek mitināta sistēma. | *TS – 2.2. punkts* | | | |

| FUNKCIONĀLĀS PRASĪBAS | | STATUSS | | |
|---|---|---|---|---|
| **Prasības** | **Avots** | **Ieviests** | **Nav ieviests** | **Tiks pilnveidots** |
| Vākšanas tiešsaistes sistēma sastāv no tīmekļa lietotnes, kas izveidota, lai vāktu paziņojumus par atbalstu vienai pilsoņu iniciatīvai. | *TS– 2.3. punkts* | | | |
| Ja sistēmas administrēšanai ir nepieciešamas vairākas lomas, tad tiek izveidoti dažādi piekļuves kontroles līmeņi, ievērojot mazākās konfidencialitātes pielaides principu. | *TS– 2.4. punkts* | | | |
| Publiski pieejamās funkcijas ir skaidri nodalītas no funkcijām, kas ir paredzētas administrēšanas mērķiem. Nekāda piekļuves kontrole neliedz lasīt informāciju, kas ir pieejama sistēmas publiskajā daļā, ieskaitot informāciju par iniciatīvu un paziņojuma par atbalstu elektronisko veidlapu. Parakstīšanās par iniciatīvu ir iespējama, tikai izmantojot šo publisko daļu. | *TS– 2.5. punkts* | | | |
| Sistēma atklāj un novērš paziņojumu par atbalstu dubultu iesniegšanu. | *TS–2.6. punkts* | | | |

| PRETPASĀKUMU STATUSA NOVĒRTĒJUMS | | | STATUSS | | | | |
|---|---|---|---|---|---|---|---|
| | | | Ieviests | Nav ieviests | Pieņemts risks | Plānots | Nav piemērojams |
| **Draudi** | **Pretpasākumi** | **Avots** | | | | | |
| Injekcija | Sistēma ir aizsargāta pret injekcijas kļūdām, piemēram, strukturētās vaicājumu valodas (SQL) vaicājumiem, direktoriju vieglpiekļuves protokola (LDAP) vaicājumiem, XML valodas XPath vaicājumiem (XML Path Language (XPath) queries), operētājsistēmas (OS) komandām vai programmas argumentiem (program arguments). | *TS – 2.7.1 punkts* | | | | | |
| Injekcija | Visi lietotāju ievadītie dati tiek validēti. | *TS– 2.7.1. a) punkts* | | | | | |
| Injekcija | Validēšanu veic vismaz servera puses loģika (*server-side logic*). | *TS – 2.7.1. b) punkts* | | | | | |
| Injekcija | Izmantojot jebkādus interpretatorus, neuzticami dati ir skaidri nodalīti no komandas vai vaicājuma. Attiecībā uz SQL vaicājumiem tas nozīmē saistošo mainīgo (*bind variables*) izmantošanu visos sagatavotajos priekšrakstos un saglabātajos procesos un izvairīšanos no dinamiskiem vaicājumiem. | TS – *2.7.1. c) punkts* | | | | | |
| Starpvietņu skriptošana (XSS) | Visi lietotāju ievadītie dati, kas tiek nosūtīti atpakaļ uz pārlūkprogrammu, tiek validēti (izmantojot ievadīto datu validāciju). | *TS – 2.7.2. a) punkts* | | | | | |
| Starpvietņu skriptošana (XSS) | Visi lietotāju ievadītie dati ir pienācīgi kodēti, pirms tie tiek iekļauti izvades lapā. | *TS – 2.7.2. b) punkts* | | | | | |
| Starpvietņu skriptošana | pienācīga izvaddatu kodēšana nodrošina, ka šādi ievadītie dati | *TS – 2.7.2. c) punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (XSS) | vienmēr tiek apstrādāti kā teksts pārlūkprogrammā. Netiek izmantots aktīvs saturs. | | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Sistēmai ir stipra autentificēšanas un sesiju pārvaldība. | *TS – 2.7.3. punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Akreditācijas dati (*credentials*), kad tos saglabā, vienmēr tiek aizsargāti, izmantojot jaukšanu vai šifrēšanu. | *TS – 2.7.3. a) punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Akreditācijas datus nevar uzminēt vai pārrakstīt vāju konta pārvaldības funkciju dēļ (piemēram, konta izveidošana, paroles maiņa, paroles atgūšana, vāji sesiju identifikatori (ID)). | *TS – 2.7.3. b) punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Sesiju ID un sesiju dati netiek atklāti vienotajā resursu vietrādī (URL). | *TS – 2.7.3. c) punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Sesiju ID nav neaizsargāti pret sesiju fiksācijas uzbrukumiem. | *TS – 2.7.3. d) punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | sesiju ID noilgst, kas nodrošina, ka lietotāji pārtrauc savienojumu. | *TS – 2.7.3. e) punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | sesiju ID netiek rotēti pēc veiksmīgas pieteikšanās. | *TS – 2.7.3. f) punkts* | | | | | |
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | personas dati elektroniskā formātā tiek šifrēti, kad tie tiek saglabāti vai nosūtīti kompetentajām iestādēm dalībvalstīs saskaņā ar Regulas (ES) Nr. 211/2011 8. panta 1. punktu, kodu pārvaldīšanai un dublikātu sagatavošanai notiekot atsevišķi. | *TS – 2.7.7. a) punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | Tiek lietoti stipri standarta algoritmi un stipras atslēgas saskaņā ar starptautiskajiem standartiem. Pastāv kodu pārvaldības sistēma. | *TS – 2.7.7. b) punkts* | | | | | |
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | Paroles tiek jauktas (*hashed*) ar stipru standarta algoritmu, un tiek izmantots pienācīgs "sāls" (*salt*). | *TS – 2.7.7. c) punkts* | | | | | |
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | Visas atslēgas un paroles tiek aizsargātas no nesankcionētas piekļuves. | *TS – 2.7.7. d) punkts* | | | | | |
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | Administratīvie akreditācijas dati, personas dati, kas ir savākti no parakstītājiem, un to dublikāti tiek aizsargāti, izmantojot stiprus šifrēšanas algoritmus. | *TS – 2.11. punkts* | | | | | |
| Nedrošas kriptogrāfiskās glabāšanas ievainojamību izmantošana | Parakstītāja personas dati ir pieejami tikai sistēmā, ieskaitot dublikātu šifrētā formātā. Datu apskates vai sertificēšanas nolūkā, ko veic valsts iestādes saskaņā ar Regulas (ES) Nr. 211/2011 8. pantu, organizatori var eksportēt šifrētos datus. | *TS – 2.13. punkts* | | | | | |
| URL piekļuves ierobežošanas kļūda | Ja tiek lietoti ārējie drošības mehānismi, lai nodrošinātu autentifikācijas un sankcionēšanas pārbaudes lapas piekļuvei, tiem ir jābūt pienācīgi konfigurētiem attiecībā uz katru lapu. | *TS – 2.7.8. a) punkts* | | | | | |
| URL piekļuves ierobežošanas kļūda | Ja tiek lietota kodu līmeņa aizsardzība, kodu līmeņa aizsardzībai ir jābūt katrai nepieciešamajai lapai. | *TS – 2.7.8. b) punkts* | | | | | |
| *Brute Force* uzbrukums | Sistēmas administrācijas daļa ir aizsargāta. Ja tā ir aizsargāta ar vienfaktora autentificēšanu, tad parole sastāv vismaz no desmit zīmēm, kuru skaitā ir vismaz viens burts, viens cipars un viena īpašā zīme. Var arī izmantot divfaktoru autentificēšanu. | *TS – 2.7.3. h) punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Neautorizēta piekļuve | Parakstītājiem ir piekļuve tikai datiem, kas ir ievadīti sesijā, kurā tie pabeidz aizpildīt paziņojuma par atbalstu veidlapu. Līdzko paziņojums par atbalstu ir iesniegts, iepriekšējā sesija tiek slēgta un ievadītajiem datiem vairs nevar piekļūt. | *TS – 2.12. punkts* | | | | | |
| Neautorizēta piekļuve | Gadījumos, kad vākšanas tiešsaistes sistēmām, kas tiek izmantotas pilsoņu iniciatīvām, ir kopīga aparatūra un operētājsistēmu resursi, tās neapmainās ar datiem, tai skaitā piekļuves/šifrēšanas akreditācijas datiem. Turklāt tas ir atspoguļots riska novērtējumā un īstenotajos pretpasākumos. | *TS – 2.8. punkts* | | | | | |
| Neautorizēta piekļuve | Dati, ko sniedz parakstītāji, ir pieejami tikai datubāzes administratoram/organizatoram. | *TS – 2.10. punkts* | | | | | |
| Neautorizēta piekļuve | Lietotnes darbojas, izmantojot viszemāko privilēģiju komplektu, kas tām ir nepieciešams, lai darbotos. | *TS – 2.19.2 punkts* | | | | | |
| Aplikāciju kļūda | Paziņojumā par atbalstu ievadīto datu inertība ir atomiska. Tas nozīmē, ka, līdzko lietotājs paziņojuma par atbalstu veidlapā ir ievadījis visu nepieciešamo informāciju un validējis savu lēmumu atbalstīt iniciatīvu, sistēma vai nu nodod visus veidlapas datus datubāzei, vai – kļūdas gadījumā – nesaglabā nekādus datus. Sistēma informē lietotāju par viņa pieprasījuma veiksmīgu vai neveiksmīgu apstrādāšanu. | *TS – 2.14. punkts* | | | | | |
| Bojāta autentifikācija un sesiju pārvaldība | Paroles, sesiju ID un citi akreditācijas dati tiek nosūtīti, tikai izmantojot transporta slāņa drošību (Transport Layer Security (TLS)) | *TS – 2.7.3. g) punkts* | | | | | |
| Nedrošu tiešo objektu atsauču ievainojamību izmantošana | Sistēmai nav nedrošas tiešās objektu atsauces. | *TS – 2.7.4. punkts* | | | | | |
| Nedrošu tiešo objektu atsauču ievainojamību izmantošana | Attiecībā uz tiešajām atsaucēm uz ierobežotiem resursiem lietotne pārbauda, ka lietotājs ir sankcionēts piekļūt attiecīgajam pieprasītajam resursam. | *TS – 2.7.4. a) punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Nedrošu tiešo objektu atsauču ievainojamību izmantošana | Ja atsauce ir netiešā atsauce, tiešās atsauces kartēšana ir aprobežota ar vērtībām, kas ir sankcionētas tikai attiecībā uz pašreizējo lietotāju. | *TS – 2.7.4. b) punkts* | | | | | |
| Nepietiekoša Transporta slāņa ievainojamību izmantošana | Sistēmai ir nepieciešama visaktuālākā hiperteksta drošas pārsūtīšanas protokola versija (HTTPS), lai piekļūtu jebkādiem sensitīviem resursiem, izmantojot spēkā esošus sertifikātus, kuru termiņš nav beidzies, kas nav atsaukti un atbilst visiem vietnē lietotajiem domēniem. | *TS – 2.7.9. a) punkts* | | | | | |
| Nepietiekoša Transporta slāņa ievainojamību izmantošana | Sistēma piešķir karodziņu "drošs" visām jūtīgajām sīkdatnēm. | *TS – 2.7.9. b) punkts* | | | | | |
| Nepietiekoša Transporta slāņa ievainojamību izmantošana | Serveris konfigurē TLS sniedzēju, lai tas atbalstītu tikai šifrēšanas algoritmus, kas atbilst labākajai praksei.<br>Lietotāji tiek informēti, ka tiem ir jāatļauj TLS atbalsts savā pārlūkprogrammā. | *TS – 2.7.9. c) punkts* | | | | | |
| Tīkla trafika noklausīšanās | Administratora piekļuvei vākšanas tiešsaistes sistēmas pārvaldības saskarnei ir īsa sesijas noildze (maksimāli 15 minūtes). | *TS – 2.19.3 punkts* | | | | | |
| Neautorizēta piekļuve | Visi sistēmas aktivitātes žurnāli ir vietā. Sistēma nodrošina, ka visus audita žurnālus, kas reģistrē izņēmumus un citus ar drošību saistītus notikumus, kuri uzskaitīti turpmāk, var ģenerēt un saglabāt, līdz dati ir iznīcināti saskaņā ar Regulas (ES) Nr. 211/2011 12. panta 3. vai 5. punktu. Žurnāli tiek pienācīgi aizsargāti, piemēram, saglabājot tos šifrētos datu nesējos. Organizatori/administratori regulāri pārbauda žurnālus attiecībā uz aizdomīgu darbību.<br><br>Žurnālu saturs ietver vismaz:<br>a) datumus un laikus, kad organizatori/administratori veic pieteikšanos un veic atteikšanos;<br>b) veiktos dublējumus; | *TS – 2.16. punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | c) visas datubāzes administratoru izmaiņas un atjauninājumus. | | | | | | |
| | Pastāv pienācīga drošības konfigurācija, kura nodrošina vismaz to, ka:<br>a) visas programmatūras komponentes ir aktuālas, tai skaitā operētājsistēma, tīmekļa/lietotnes serveris, datubāzes pārvaldības sistēma (DBMS), lietotnes un visas kodu bibliotēkas;<br>b) ir atspējoti, izņemti vai nav instalēti nevajadzīgi OS un tīmekļa/lietotnes servera pakalpojumi;<br>c) sākotnējās konta paroles tiek grozītas vai tiek atspējotas;<br>d) ir izveidota kļūdu apstrāde, lai novērstu steka izsekošanu (*stack trace*) vai citu pārlieku daudz informācijas saturošu ziņojumu noplūdi;<br>e) drošības iestatījumi izstrādes struktūrās (*development frameworks*) un bibliotēkās tiek konfigurēti saskaņā ar labāko praksi, piemēram, OWASP vadlīnijām. | *TS – 2.7.6. punkts* | | | | | | |
| | DBMS, kas tiek lietota, ir aktualizēta un tiek nepārtraukti uzlabota attiecībā uz jaunatklātiem ļaunprātīgas izmantošanas gadījumiem. | *TS – 2.15. punkts* | | | | | | |
| | Fiziskā drošība<br>Neatkarīgi no tā, kāda veida mitināšana tiek lietota, iekārta, kas mitina lietotni, ir pienācīgi aizsargāta, kas nozīmē:<br>a) mitināšanas telpas piekļuves kontroli un audita žurnālu;<br>b) dublējumu datu fizisko aizsardzību pret zādzību vai nejaušu novietošanu nevietā;<br>c) serveris, kas mitina lietotni, ir instalēts drošā statīvā. | *TS – 2.17. punkts* | | | | | | |
| | Sistēma tiek mitināta uz servera, kas savienots ar internetu un kas ir instalēts “demilitarizētā zonā“ (DMZ), un ko aizsargā ugunsmūris. | *TS – 2.18.1 punkts* | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Kad ugunsmūra produkta attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, tie tiek nekavējoties instalēti. | *TS – 2.18.2 punkts* | | | | | |
| | Visu ienākošo un no servera izejošo datu plūsmu (kas paredzēta vākšanas tiešsaistes sistēmai) pārbauda uguns-<br>mūra noteikumi, un tā tiek reģistrēta. Ugunsmūra noteikumi neatļauj jebkādas plūsmas, kas nav vajadzīgas<br>sistēmas drošai lietošanai un administrēšanai. | *TS – 2.18.3 punkts* | | | | | |
| | Vākšanas tiešsaistes sistēma ir jāmitina uz pienācīgi aizsargāta produkcijas tīkla segmenta, kas ir nodalīts no<br>segmentiem, kurus izmanto neproduktīvas sistēmas, piemēram, izstrādes vai testēšanas vidēm. | *TS – 2.18.4 punkts* | | | | | |
| | Pastāv lokālā tīkla (LAN) aizsardzības mehānismi, piemēram:<br><br>a) Layer 2 (L2) piekļuves saraksts/pārmijportu drošība;<br>b) neizmantoti pārmijporti tiek atspējoti;<br>c) DMZ ir uz īpaša virtuālā lokālā tīkla (VLAN)/LAN;<br>d) nevajadzīgos pārmijportos nav iespējots L2 trunking. | *TS – 2.18.5 punkts* | | | | | |
| | Kad attiecīgi OS jauninājumi un ielāpi, lietotņu izpildlaiki, lietotnes, kas darbojas uz servera, vai pretvīrusu<br>programmas tiek publiskotas, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti. | *TS – 2.19.4 punkts* | | | | | |
| | Organizatoru klientu drošība<br>Abpusējas drošības labad organizatori veic nepieciešamos pasākumus, lai aizsargātu savu klientu lietotni/ierīci, ko<br>tie izmanto, lai pārvaldītu un piekļūtu vākšanas tiešsaistes sistēmai. | *TS – 2.20. punkts* | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Lietotāji veic ar uzturēšanu nesaistītus uzdevumus (*non-maintenance tasks*) (piemēram, biroju automatizāciju) ar mazāko privilēģiju skaitu, kas ir nepieciešams to darbībai. | *TS – 2.20.1 punkts* | | | | | |
| | Kad OS, jebkādas instalētas lietotnes vai pretvīrusu programmas attiecīgi jauninājumi un ielāpi kļūst publiski pieejami, šādi jauninājumi vai ielāpi tiek nekavējoties instalēti. | *TS – 2.20.2 punkts* | | | | | |
| | Sistēma aizsargā pret starpvietņu pieprasījumu (*cross-site*) viltošanas kļūdu. | *TS – 2.7.5 punkts* | | | | | |
| | Sistēma aizsargā pret neatļautu novirzīšanu un pārvirzīšanu. | *TS – 2.7.10 punkts* | | | | | |
| | Risks, ka kāda persona autentificējas datubāzē, izmantojot "jaukšanas apiešanu" (*pass-the-hash*), ir samazināts. | *TS – 2.9. punkts* | | | | | |
| | Pastāv pienācīga drošības konfigurācija, ieskaitot elementus, kas ir uzskaitīti TS 2.7.6. punktā. | *TS – 2.19.1 punkts* | | | | | |
| | Risks, ka kāda persona autentificējas sistēmā, izmantojot "jaukšanas apiešanu", ir samazināts. | *TS – 2.19.5 punkts* | | | | | |

| REGULAS (ES) Nr. 211/2011 PUNKTA 6(4)(c) PRASĪBU IEVIEŠANA | | STATUSS | | |
|---|---|---|---|---|
| **Prasības** | **Avots** | **Ieviests** | **Nav ieviests** | **Tiks pilnveidots** |
| Sistēma sniedz iespēju attiecībā uz katru dalībvalsti iegūt ziņojumu, kurā iekļauta iniciatīva un parakstītāju personas dati, pēc šīs dalībvalsts kompetentās iestādes veiktās verifikācijas. | *TS – 3.1. punkts* | | | |
| Eksportēt parakstītāju paziņojumus par atbalstu ir iespējams Regulas (ES) Nr. 211/2011 III pielikumā noteiktajā formātā. Sistēma var nodrošināt iespēju eksportēt paziņojumu par atbalstu sadarbspējīgā formātā, piemēram, paplašināmās iezīmēšanas valodā (XML). | *TS – 3.2. punkts* | | | |
| Eksportētie paziņojumi par atbalstu tiek iezīmēti kā "ierobežotai izplatīšanai" attiecīgajai dalībvalstij un marķēti ar atzīmi "personas dati". | *TS – 3.3. punkts* | | | |
| Eksportēto datu elektroniska nosūtīšana dalībvalstīm tiek aizsargāta pret pārtveršanu, izmantojot piemērotu pilnīgu šifrēšanu. | *TS – 3.4. punkts* | | | |