**Attālinātā monitoringa kiberdrošības prasības.**

|  |  |
| --- | --- |
| **Prasība** | **Apraksts** |
| 1. Vienota pieslēgšanās un piekļuves pārvaldība | Jānodrošina lomās balstīta piekļuves kontrole (RBAC) ar integrāciju Active Directory / Entra ID. Lietotājiem un lomām jāspēj piešķirt tiesības līdz lauku/objektu līmenim. Jānodrošina iespēja auditēt piešķirtās piekļuves un to izmaiņas. |
| 1. Piekļuves pārvaldība datortīklā | Piegādātājam jānodrošina atbalsts un visa nepieciešamā informācija, lai ierobežotu informācijas sistēmas piekļuvi Pasūtītāja datortīklā, izmantojot tikai nepieciešamos portus un protokolus. Ja atsevišķām sistēmas funkcionalitātēm nepieciešama piekļuve no ārējiem tīkliem, jāparedz droši piekļuves mehānismi (piemēram, Azure Application Proxy vai līdzvērtīgs risinājums), lai novērstu tiešu piekļuvi no publiskā tīkla. |
| 1. Audita žurnālu pieejamība | Sistēmā jāveido audita ieraksti vismaz par šādām darbībām: lietotāju autentifikāciju un autorizāciju; pieejas tiesību piešķiršanu, maiņu un atcelšanu; datu piekļuvi, izmaiņām un dzēšanu; sistēmas konfigurācijas un drošības iestatījumu izmaiņām. Audita žurnāliem jābūt iespējai automātiski nosūtīties uz organizācijas SIEM (Microsoft Sentinel). Piegādātājam jānodrošina visa nepieciešamā informācija un tehniskais atbalsts, lai nodrošinātu veiksmīgu integrāciju ar SIEM Sentinel. |
| 1. Datu šifrēšana pārraides laikā | Jānodrošina pilnvērtīga datu šifrēšana visām sistēmas komponentēm pārraides laikā (TLS 1.2 vai jaunāka versija), tostarp rezerves kopijām un integrācijas datu plūsmām. |
| 1. Datu šifrēšana glabāšanā | IS jānodrošina, ka visa informācija (ieskaitot datu bāzes saturu, failu pielikumus, konfigurācijas un rezerves kopijas) tiek šifrēta glabāšanas laikā (diskā vai datu bāzē), izmantojot spēcīgus šifrēšanas algoritmus (piemēram, AES-256). Sensitīvie dati (paroles, kriptogrāfiskās atslēgas) operatīvajā atmiņā jāglabā šifrētā formā un jāizdzēš pēc izmantošanas. |
| 1. Atbilstība kiberdrošības un datu aizsardzības regulām | Ārpakalpojuma sniedzējam un piegādātajai informācijas sistēmai jāatbilst MK  noteikumiem Nr. 397 “Minimālās kiberdrošības prasības” un Nacionālās kiberdrošības likumam. Piegādātājam jāspēj iesniegt pierādījumus par atbilstību un jārīkojas saskaņā ar šīm prasībām. |
| 1. Rezerves kopēšanas un atjaunošanas stratēģija | Piegādātājam jāizstrādā un jāuztur dokumentēta rezerves kopiju un atjaunošanas procedūra, ievērojot provizoriskās RTO ≤ 72h un RPO ≤ 24h  prasības. Piegādātājam jānodrošina visa nepieciešamā informācija un atbalsts, lai Pasūtītājs varētu veikt regulāru rezerves kopiju un atjaunošanas procedūru testēšanu. |
| 1. Droša integrāciju pārvaldība | Integrācijām jāizmanto drošības mehānismi (IP adrešu filtri, PKI klienta sertifikāti). Vajadzības gadījumā jāatbalsta OAuth2.0 vai SAML autentifikācija. Piegādātājam jāspēj iesniegt pierādījumus par konfigurācijām (API Gateway, PKI, šifrēšana). |
| 1. Ielaušanās testēšanas atbalsts, drošības auditi | Pirms nodošanas ekspluatācijā piegādātājam jānodrošina atbalsts Pasūtītāja pārstāvjiem drošības testu veikšanā, lai identificētu iespējamos ievainojamību riskus. Piegādātājam jānovērš visi kritiskie un vidējā riska kategorijas drošības audita ieteikumi, kas identificēti testu rezultātā, pirms sistēmas pieņemšanas, tostarp aktuālās OWASP Top 10 ievainojamības. |
| 1. Fizisko personas datu apstrāde | Ārpakalpojuma sniedzējam un viņa sadarbības partneriem jāievēro Fizisko personu datu apstrādes likuma un VDAR (GDPR) prasības, kā arī jāapstrādā personas dati atbilstoši šīm prasībām. |
| 1. IS Komponentu aktualitāte, uzturēšana | Nodrošināt, ka visas IS izmantotās komponentes, tostarp atvērtā pirmkoda risinājumi, ir aktuālās, uzturētas un ar pieejamiem drošības atjauninājumiem. Komerciālajām komponentēm jābūt ražotāja atbalstītām, atvērtā pirmkoda – kopienas vai uzturētāja atbalstītām. Ja komponenti atjaunināt nav iespējams, nepieciešams saskaņot ar Pasūtītāju un ieviest kompensējošus kontroles mehānismus. |
| 1. Datu nodošana pēc līguma beigām | Pēc līguma izbeigšanas Pretendentam jānodod visas Pasūtītāja informācijas sistēmās glabātās datu kopijas (tostarp konfigurācijas un žurnālfaili) Pasūtītājam ar pieņemšanas–nodošanas aktu. Pēc akta parakstīšanas Pretendentam ir pienākums pilnībā un droši dzēst visus atlikušos Pasūtītāja datus, to kopijas un atvasinājumus no savas infrastruktūras (tostarp rezerves kopijām), kā arī iesniegt rakstisku apliecinājumu par dzēšanas veikšanu. |