RIIGI INFOSÜSTEEMI AMET

XXXXXXX
Piksel OÜ
piksel@piksel.ee

12.11.2021 nr 8-1/21-0179/211668

VÄLJAVÕTE

ETTEKIRJUTUS

Ettekirjutuse tegija	Riigi Infosüsteemi Ameti standardi ja järelevalve osakonna juhtivekspert Erika Adams
Ettekirjutuse tegemise aeg ja koht	12.11.2021, Tallinn
Ettekirjutuse adressaat	Piksel OÜ (10126529) Asukoht: Tartu maakond, Tartu linn, Lai tn 30 Telefon: +372 7409120 e-posti aadress: piksel@piksel.ee
Adressaadi vastutav isik	XXXXXXXX

Resolutsioon:

võtnud aluseks korrakaitseseaduse (edaspidi KoRS) § 28 lg 1 ning hinnanud riikliku järelevalvemenetluse käigus välja selgitatud asjaolusid teen **kohustusliku ettekirjutuse**

vaadata üle ning kõrvaldada käesoleva ettekirjutuse lisades 1 kuni 4 esitatud raportites välja toodud kõrge ja keskmise tasemega turvanõrkused Piksel OÜ poolt hallatavates infosüsteemides ja võtta kasutusele meetmed, mis väldivad sarnaste haavatavuste tekkimise või haavatavuste tekkimisel nende viivitamatu kõrvaldamise tulevikus.

Määran ettekirjutuse täitmise tähtajaks **07.01.2022**.

Ettekirjutuse täitmisest palume hiljemalt selleks tähtajaks Riigi Infosüsteemi Ametit teavitada, esitades ettekirjutuse täitmist kinnitavad tõendid ja asjakohase teabe.

Vaidlustamisviide:
Isikul, kes leiab, et ettekirjutusega rikutakse tema õigusi, on 30 kalendripäeva jooksul arvates sellise asjaolu teadasaamisest õigus esitada vaie Riigi Infosüsteemi Ameti peadirektorile (Pärnu mnt 139 a, 15169 Tallinn, e-post info@ria.ee) haldusmenetluse seaduses sätestatud korras või Tallinna Halduskohtusse (Tallinna Kohtumaja, Pärnu mnt 7, 15082 Tallinn, e-post tlnhktallinn.menetlus@kohus.ee) halduskohtumenetluse seadustikus sätestatud korras.

Ettekirjutuse vaidlustamine ei peata ettekirjutuse täitmist ega sunnivahendi rakendamist, kui Riigi Infosüsteemi Amet või kohus ei otsusta teisiti.

Sunniraha hoiatus:

Kui ettekirjutus jäetakse määratud tähtajaks täitmata või täidetakse osaliselt, määrab Riigi Infosüsteemi Amet Piksel OÜ-le KoRS § 23 lg 4 alusel sunniraha **4000** eurot.

Juhul, kui Piksel OÜ ei täida ettekirjutust määratud tähtajaks või ei tasu vabatahtlikult sunniraha, edastatakse ettekirjutus kohtutäiturile täitemenetluse alustamiseks. Sellisel juhul lisanduvad sunnirahale kohtutäituri tasu ja muud täitekulud. Asendustäitmise ja sunniraha seaduse (ATSS) § 2 lõike 2 kohaselt võib sunniraha rakendada korduvalt kuni ettekirjutusega taotletava eesmärgi saavutamiseni.

Sunniraha vabatahtlikul tasumisel märkida selgituseks „Riigi Infosüsteemi Ameti riiklikjärelevalve asjas nr 8-1/21-0179 sunniraha“ ja viitenumbriks 2800045496.
Sunniraha tuleb tasuda Rahandusministeeriumi pangakontole alljärgnevalt:
SEB Pank EE891010220034796011 (BIC/SWIFT: EEUHEE2X)
Swedbank EE932200221023778606 (BIC/SWIFT: HABAEE2X)
LHV Pank EE777700771003813400 (BIC/SWIFT: LHVBEE22)
Luminor Bank EE701700017001577198 (BIC/SWIFT: NDEAEE2X)

Piksel OÜ-l tuleb Riigi Infosüsteemi Ametit teavitada ettekirjutuse täitmisest või sunniraha tasumisest hiljemalt täitmise tähtajaks e-posti aadressil jvo@ria.ee.

Faktilised asjaolud ja menetluskäik:

KorS § 6 lg 1, KüTS § 12 lõigete 2 ja 3 ja 14 lõike 1 järgi on RIA küberturvalisuse tagamise ning küberintsidendi ennetamise ja lahendamise kontekstis korrakaitseorgan. RIA-s tegutseb intsidentide käsitlemise osakond CERT-EE, kelle ülesanne on tuvastada, jälgida ja lahendada Eesti arvutivõrkudes toimuvaid küberintsidente ning teavitada tuvastatud ohtudest.

31.05.2021 tuvastas CERT-EE küberintsidentidega seotud olnud veebilehtedele haavatavuse seire käigus ülikriitilised turvanõrkused ja haavatavused Piksel OÜ-le kuuluva veebilehtede XXXXXXXXX ja XXXXXXXXXXXXX osas. XXXXXXXXXX XXXXXXXX XXXX XXXXXXX XXXXX XXXXXXX

13.07.2021 juhtunu täpsemate asjaolude väljaselgitamiseks ja võimaliku ohu ennetamiseks või tõrjumiseks algatas RIA saadetud järelepärimisega nr 8-1/21-0179/211093 Piksel OÜ suhtes riikliku järelevalvemenetluse.

14.07.2021 andis Piksel OÜ RIA-le teada, et on parandanud ära kõrgema ohtlikkusega haavatavused. XXXXXXXXXXX XXXXXXXXXX XXXXXXXXXXX XXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXX

19.08-20.08.2021 tuvastas CERT-EE seire käigus Piksel OÜ-le kuuluva veebilehtedelt XXXXXXXXXXX ja XXXXXXXXXX sarnaseid turvanõrkuseid, mis asuvad XXXXXXXXX IP aadressi XXXXXXXX.70 peal. XXXXXXXXXX XXXXXXXXXXXX XXXXXXXX

XXXXXXXXXX XXXXXXXXXXXXXX XXXXXXXXXXXXX XXXXXXXX XXXXXXXXX XXXXXXXXX

Seire tulemused koos haavatavuste kirjeldustega on raporteeritud (registreeritud CERT-EE pileti nr CERT-122326) ning 26.08.2021 kirjaga Piksel OÜ-le haavatavuste parandamiseks edastatud.

21.08.2021 viidi läbi 31.05.2021 tuvastatud haavatavuste osas veebilehtede XXXXXXXXXX ja XXXXXXXXXX kordusseire, tulemustest nähtus, et esineb endiselt haavatavusi (s.h kriitilise tasemega haavatavusi, mille CVSS skoor oli >X). Arvestades asjaoluga, et endiselt esines kõrge ohtlikkuse tasemega haavatavusi, määras RIA oma 26.08.2021 kirjaga nr 8-1/21-0179/211093 Piksel OÜ-le tähtaja kõrgete tasemetega haavatavuste kõrvaldamiseks hiljemalt 03.09.2021. Sama kirjaga teavitati Piksel OÜ-d õigusest esitada RIA-le asja kohta oma arvamusi ja vastuväiteid.

03.09.2021 andis Piksel OÜ RIA-le teada, et on parandanud täiendavalt väljatoodud kõrgema ohtlikkusega haavatavused ning on tegelenud teiste piksel.ee serveris asuvate veebisüsteemide ülekäimisega. Sama teavitusega esitas Piksel OÜ RIA-le veebilehe XXXXXXX XXXXXX XXXXX XXXXXXXXXX XXXXXXXX

20.-23.10.2021 viis CERT-EE läbi 21.08.2021 tuvastatud haavatavuste osas veebilehtede XXXXXXXXXXX, XXXXXXXXXX, XXXXXXXXXXX ja XXXXXXXXXX kordusseire. Tulemustest nähtus, et esineb endiselt kõrge ohtlikkuse tasemega haavatavusi, mida ei ole kõrvaldatud. XXXXXXXX XXXXXXXXXX XXXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

Riigi Infosüsteemi Ameti selgitused ja põhjendused:

KorS §-i 4 järgi on avalik kord ühiskonna seisund, milles on tagatud õigusnormide järgimine ning õigushüvede ja isikute subjektiivsete õiguste kaitstus.

Sama seaduse § 15 lõike 1 sätestab üldnormina avaliku korra eest vastutava isikuna isiku, kes on põhjustanud ohukahtluse või ohu, rikub avalikku korda või on põhjustanud sellise olukorra tekkimise võimaluse, mille realiseerumisel tekib oht või ohukahtlus. Lõike 4 kohaselt on seisundivastutuse korral, ehk kui oht lähtub asjast endast, avaliku korra eest vastutavaks isikuks asja omanik.

KorS § 5 lõiked 2 ja 6 annavad ohukahtluse, ohu ja korrarikkumise definitsioonid, millede kohaselt ohu kahtlus ja oht on olukorrad, kus ilmnenud asjaoludele antava objektiivse hinnangu põhjal ei saa välistada korrarikkumist (ohu kahtlus) või saab pidada korrarikkumise tõenäosust piisavaks (oht). Korrarikkumine on defineeritud sama sätte lõikes 1, mis ütleb, et korrarikkumine on avaliku korra kaitsealas oleva õigusnormi või isiku subjektiivse õiguse rikkumine või õigushüve kahjustamine.

Kohaliku omavalitsuse korralduse seaduse (KOKS) § 6 lõigete 1 ja 2 järgi on omavalitsusüksuse ülesanne korraldada vallas või linnas:

1) sotsiaalteenuste osutamist, sotsiaaltoetuste ja muu sotsiaalabi andmist, eakate hoolekannet, kultuuri-, spordi- ja noorsootööd, elamu- ja kommunaalmajandust, veevarustust ja kanalisatsiooni, heakorda, jäätmehooldust, ruumilist planeerimist, valla- või linnasisest ühistransporti ning valla või linna teede ehitamist ja korrashoidu, kui need ülesanded ei ole seadusega antud kellegi teise täita ja
2) koolieelsete lasteasutuste, põhikoolide, gümnaasiumide ja huvikoolide, raamatukogude, rahvamajade, muuseumide, spordibaaside, turva- ja hooldekodude, tervishoiuasutuste ning teiste kohalike asutuste ülalpidamist, juhul kui need on omavalitsusüksuse omanduses. Seega on kohalik omavalitsus oma ülesannete täitmise korraldamisega haldusüksuse territooriumi piires avaliku korra eest vastutav isik.

KüTS § 2 punktis 1 sätestatud definitsiooni järgi loetakse võrgu- ja infosüsteemiks (edaspidi süsteem) elektroonilise side võrku elektroonilise side seaduse § 2 punkti 8 tähenduses, seadet või omavahel ühendatud või seotud seadmete rühma, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringuga või edastatakse eelnimetatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks.

Piksel OÜ pakub oma serveris IP aadressiga XXXXXXXXXX teiste teenuste hulgas ka veebilehtede XXXXXXXXXX ja XXXXXXXXXX vahendusel XXXXXXXXXX haldamise infosüsteemi XXXXXXXXXX ja XXXXXXXXXX XXXXXXXXXX infosüsteemi XXXXXXXXXX, standardlahenduste platvormi (edaspidi süsteemid), mille kasutajate sihtrühmaks on kohalikud omavalitsused. Infosüsteemid on mõeldud kohalike omavalitsuste, haridusasutuste, huvikoolide ja lasteaedade töökorralduslike protsesside hõlbustamiseks kohalike omavalitsuste elanikele. XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX Mõlema infosüsteemi platvormi omanikuks on Piksel OÜ, kes arendab, haldab ning otsustab infosüsteemi tehnilise arhitektuuri eest, sh tark- ja riistvaraliste seadmete valimise ja kasutamise üle. Mõlema infosüsteemi puhul on tegemist andmebaasiga, kus toimub programmi põhine digitaalsete andmete kogumine, automaatne töötlemine, digitaalsete andmete salvestamine, mis saadakse päringuga või edastatakse infosüsteemi asjakohaste komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks Piksel OÜ haldusalas olevasse serverisse. **Seega on meil tegemist KüTS mõistes võrgu- ja infosüsteemidega, millede vahendusel osutatakse KOKS alusel kohalike omavalitsustele pandud avalike ülesandeid.**

20.-23.10.2021 viis CERT-EE läbi 21.08.2021 tuvastatud haavatavuste osas veebilehtede XXXXXXXXXX, XXXXXXXXXX, XXXXXXXXXX ja XXXXXXXXXX kordusseire Piksel OÜ poolt teada antud turvanõrkuste kõrvaldatuse kontrollimiseks. Seire tulemused koos turvanõrkustega on esitatud raportites, mis on registreeritud CERT-EE pileti nr CERT-122325 ja on käesoleva ettekirjutuse lahutamatuks osaks. Raportid on lisatud käesoleva ettekirjutuse lisadena 1 kuni 4. Seirati Piksel OÜ XXXXXXXXXX XXXXXXXXXX servereid. Seire viidi läbi XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX. Seire tulemused näitavad, et esineb endiselt hulganisti turvanõrkuseid, mis võimaldavad ligipääsu serveris asuvate infosüsteemide andmetele selleks õigust mitteomavate isikute poolt. Samuti esinevad turvanõrkused, mida ära kasutades on võimalik andmeid muuta või XXXXXXXXXX

XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

Turvanõrkuste seireanalüüsist nähtub, et Piksel OÜ XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX ja sisaldab seetõttu hulganisti turvanõrkusi, mis on seadnud ohtu kõik Piksel OÜ teenustega seotud kasutajad ja nendega seotud andmed, kuna võimaldab XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX infosüsteemides oleva teabe osas.

XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX
XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX.

Eeltoodust tuleneb, et Piksel OÜ pakutav platvormteenus ja sellega seotud riist- ja tarkvara on ohuks kolmandate isikute subjektiivsetele õigustele, kuna Piksel OÜ pakutavate serveritega seotud teenuste puhul ei ole tagatud sinna sisestatud andmete terviklus ja konfidentsiaalsus. Seega on meil tegemist asjast (serverist) lähtuva ohuga ehk arvestades tuvastatud turvanõrkuste olemust ja kriitilisust, võib pidada piisavalt tõenäoliseks, et lähitulevikuks leiab aset korrarikkumine isikute subjektiivsete õiguste rikkumise või õigushüve kahjustamise näol. Järelikult on KorS § 15 lõike 4 kohaselt avaliku korra eest vastutavaks isikuks asja omanik Piksel OÜ.

Lähtudes KorS § 8 proportsionaalsuse ja § 9 otstarbekuse põhimõttest, on Riigi Infosüsteemi Amet menetluse kestel korduvalt juhtinud tähelepanu ohtu põhjustavatele kriitilistele turvanõrkustele, palunud nende osas Piksel OÜ-lt sekkumist ja selgitusi ning andnud puuduste kõrvaldamiseks erinevaid tähtaegu.

Vaatamata sellele, et Riigi Infosüsteemi Amet on korduvalt edastanud turvatesti raporteid haavatavuste ja turvanõrkuste kohta ei ole Piksel OÜ 23.10.2021 seisuga kriitilisi ohte kõrvaldanud, pannes sellega ohtu ühiskonna seisundi, õigusnormide järgimise ning õigushüvede ja isikute subjektiivsete õiguste kaitstuse tagamise. Sellest tulenevalt leiab Riigi Infosüsteemi Amet, et pidades silmas eesmärki hoida ära võimalikud korrarikkumised, on kohustusliku ettekirjutuse tegemine antud asjas vajalik tagamaks Piksel OÜ poolt infosüsteeme käitava ohtliku riist- ja tarkvara kõrvaldamiseks.

Ettekirjutuse saatmine ja üle andmine:

Ettekirjutus saadetakse RIA dokumendihalduse süsteemi Delta kaudu krüpteeritult Piksel OÜ seadusliku esindaja ID-kaardi sertifikaatidega ettevõtte üldisele e-posti aadressile: piksel@piksel.ee

(allkirjastatud digitaalselt)

Erika Adams
juhtivekspert
peadirektori volitusel

Lisa 1 XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

Lisa 2 XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

Lisa 3 XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX

Lisa 4 XXXXXXXXXX XXXXXXXXXX XXXXXXXXXX