Riigikogu juhatusele

26.11.2026

Pöördumine seoses Riigikogu liikmete arvutitesse paigaldatud tarkvara jälgimisvõimalustega

Pöördun Riigikogu juhatuse poole seoses tõsiste küsimustega, mis on mul tekkinud Riigikogu liikmete kasutusse antud arvutitesse paigaldatud tarkvara funktsioonide ning sellest tulenevalt Riigikogu liikmete töö ja suhtluse konfidentsiaalsuse tagamise suhtes.

Hiljuti – hinnanguliselt mõned nädalad tagasi – täheldasin, et minu kasutuses olev Apple'i sülearvuti hakkas tarbima ebatavaliselt palju energiat. Täislaetud aku tühjenes 1–2 tunniga, olgugi et varem sai arvutit akutoitel kasutada hinnanguliselt vähemalt 4–5 tundi. Asja lähemalt uurides ilmnes, et väga suure energiatarbimisega paistis silma taustal töötav protsess TMLoginMgr. See ajendas mind lähemalt uurima, milline tarkvara on minu arvutisse paigaldatud, milliseid funktsioone see täidab ja millised juurdepääsuõigused on sellele antud.

Pärast 26. novembril 2026 tehtud operatsioonisüsteemi värskendust kuvati mulle arvukalt süsteemiteateid pealkirjaga „Device Control and Data Access Added“. Nendes teadetes informeeriti mind sellest, et minu arvutit haldav organisatsioon on andnud mitmele programmile õigused, mis võimaldavad muu hulgas pääseda ligi minu andmetele, jälgida klaviatuuril sisestatavat ja külastatavaid veebilehti ning salvestada ekraanil toimuvat.

Arvuti seadistusi kontrollides ilmnes, et vastavad ulatuslikud juurdepääsuõigused olid antud muu hulgas programmidele Apex One (Mac) Security Agent, Trend Micro XDR Endpoint Sensor, iCore Security, iCore Service ja Terminal. Kõik vastavad juurdepääsuõigused olid sisse lülitatud. Olles nende ulatusest teadlikuks saanud, lülitasin need ise välja.

Apple'i operatsioonisüsteemis kuvatud selgituse kohaselt võimaldavad kõnealused õigused programmidele muu hulgas lugeda ja saata e-kirju, jälgida klaviatuuril sisestatavat, jälgida veebilehtede külastamist, salvestada ekraanil toimuvat ning juhtida teisi arvutis olevaid programme.

Samuti nähtub Trend Micro avalikust tehnilisest dokumentatsioonist, et ettevõtte XDR-turvalahendused võimaldavad administraatoritel teostada ka macOS-i operatsioonisüsteemiga arvutites mitmesuguseid kaugtoiminguid, sealhulgas lugeda ja kopeerida faile, täita käske, käivitada skripte ning jäädvustada programmide töömälu sisu.[1]

Mõistan vajadust tagada Riigikogu infosüsteemide turvalisus. Samas ei saa küberturvalisuse tagamise vajadusest automaatselt tuletada õigust luua tehnilisi võimalusi Riigikogu liikmete tegevuse ja suhtluse jälgimiseks. Küsimus ei ole üksnes selles, kas selliseid võimalusi on

---

[1] Vt https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-response-actions-mdr ja https://docs.trendmicro.com/en-us/documentation/article/trend-micro-cloud-one-workload-security-remote-shell

tegelikult kasutatud, vaid ka selles, kelle käsutuses need võimalused on, millised tagatised välistavad nende kuritarvitamise ning kas Riigikogu liikmeid, kelle kasutuses olevates seadmetes toimuvat on kõnealusel moel võimalik jälgida, on sellest ka nõuetekohaselt teavitatud.

Riigikogu liikmete puhul on see küsimus erilise kaaluga, pidades silmas nii põhiseaduse §-st 62 tulenevat vaba mandaadi põhimõtet kui ka põhiseaduse §-des 26 ja 43 sätestatud õigust eraelu puutumatusele ja sõnumisaladusele. Riigikogu liikmetel peab olema võimalik pidada konfidentsiaalset kirjavahetust muu hulgas kodanike, ajakirjanike, advokaatide ja võimalike rikkumistest teavitajatega, kartmata, et nende suhtluse sisu võib saada kõrvalistele isikutele teatavaks.

Eeltoodust lähtudes palun Riigikogu juhatusel tagada asjaolude väljaselgitamine ning anda vastused järgmistele küsimustele.

1. Milline kaugjuhtimist, andmete kogumist ja kasutaja tegevuse jälgimist võimaldav tarkvara on Riigikogu liikmete kasutusse antud arvutitesse paigaldatud ning millised funktsioonid on selles tarkvaras aktiveeritud?
2. Kas Riigikogu liikmete arvutitesse paigaldatud tarkvara võimaldab mingitelgi tingimustel kasutaja teadmata:
    - jälgida reaalajas ekraanil toimuvat või jäädvustada ekraanipilte;
    - jälgida ja salvestada klahvivajutusi;
    - tutvuda e-kirjade ja muude elektrooniliste sõnumite sisuga;
    - tutvuda arvutis olevate dokumentide sisuga ning kopeerida dokumente ja muid faile;
    - jälgida veebilehtede külastamist;
    - käivitada kaugelt programme, käske ja skripte;
    - aktiveerida arvuti mikrofoni või kaamerat?
3. Millistel isikutel, asutustel ja teenusepakkujatel on otsene või kaudne juurdepääs nimetatud funktsioonidele ja nende vahendusel kogutavatele andmetele?
4. Millisel õiguslikul alusel, kelle otsusega ja millal on Riigikogu liikmete arvutites kõnealused juurdepääsuõigused aktiveeritud? Kas Riigikogu juhatus on nende õiguste andmise heaks kiitnud ning kas ja kuidas on sellest Riigikogu liikmeid informeeritud? Kas operatsioonisüsteemi värskenduse järel kuvatud süsteemiteated kajastasid uute juurdepääsuõiguste andmist või juba varem antud õiguste olemasolu?
5. Milliseid andmeid Riigikogu liikmete arvutites toimuva kohta automaatselt kogutakse, kuhu need edastatakse, kus neid säilitatakse, kui kaua neid säilitatakse ja kellel on neile juurdepääs?
6. Kas administraatoritel on võimalik kasutaja poolt välja lülitatud juurdepääsuõigusi kaugelt ja kasutaja teadmata uuesti aktiveerida?
7. Kas kõik administraatorite tehtavad kaugtoimingud Riigikogu liikmete arvutites logitakse viisil, mis välistab logide tagantjärele muutmise või kustutamise nende samade administraatorite poolt? Kes teostab nende toimingute üle sõltumatut järelevalvet?
8. Kas ja millal on minu kasutuses oleva arvuti puhul tehtud kaugtoiminguid, mille käigus on jäädvustatud ekraanil toimuvat, jälgitud klaviatuuril sisestatavat, tutvutud kirjavahetuse või dokumentide sisuga või kogutud muid minu tegevust puudutavaid

andmeid? Palun võimaldada mul tutvuda minu arvutit puudutavate asjakohaste tegevuslogidega.

9. Millest oli tingitud protsessi TMLoginMgr hiljutine ebatavaliselt suur energiatarbimine minu arvutis, milliseid ülesandeid see protsess sel ajal täitis ning kas selle tegevus hõlmas andmete kogumist, töötlemist või edastamist?
10. Millised õiguslikud, organisatsioonilised ja tehnilised tagatised on kehtestatud selleks, et välistada Riigikogu liikmete tegevuse ja konfidentsiaalse suhtluse põhjendamatu jälgimine nii Riigikogu Kantselei töötajate kui ka teiste asutuste (sh julgeolekuasutuste) ja väliste teenusepakkujate poolt?
11. Kas Riigikogu liikmetel on võimalik kasutada Riigikogu Kantselei antud arvuteid selliselt, et oleks tehniliselt välistatud kolmandate isikute juurdepääs nende konfidentsiaalse suhtluse ja dokumentide sisule, sealhulgas ekraanil kuvatavale ja klaviatuuril sisestatavale? Kui ei, siis kas ja kuidas kavatsetakse selline võimalus Riigikogu liikmetele tagada?

Ühtlasi palun tagada, et minu kasutuses oleva arvuti haldamise, selles tehtud kaugtoimingute ning sellest andmete kogumise ja edastamisega seotud olemasolevad logid ja muud asjakohased andmed, sealhulgas kesksetes haldussüsteemides ja väliste teenusepakkujate valduses olevad logid ja andmed, säilitataks vähemalt käesolevas pöördumises tõstatatud küsimuste lõpliku selgitamiseni.

Pean oluliseks, et Riigikogu juhatus käsitleks seda küsimust mitte pelgalt ühe Riigikogu liikme arvutit puudutava tehnilise probleemina, vaid Riigikogu kui põhiseadusliku institutsiooni sõltumatuse ning kõigi Riigikogu liikmete töö konfidentsiaalsuse tagamise küsimusena.

Palun vastata esitatud küsimustele kirjalikult ja sisuliselt, eristades seejuures tarkvara tehnilisi võimalusi, tegelikult aktiveeritud funktsioone ning nende funktsioonide senist kasutamist.

Lugupidamisega

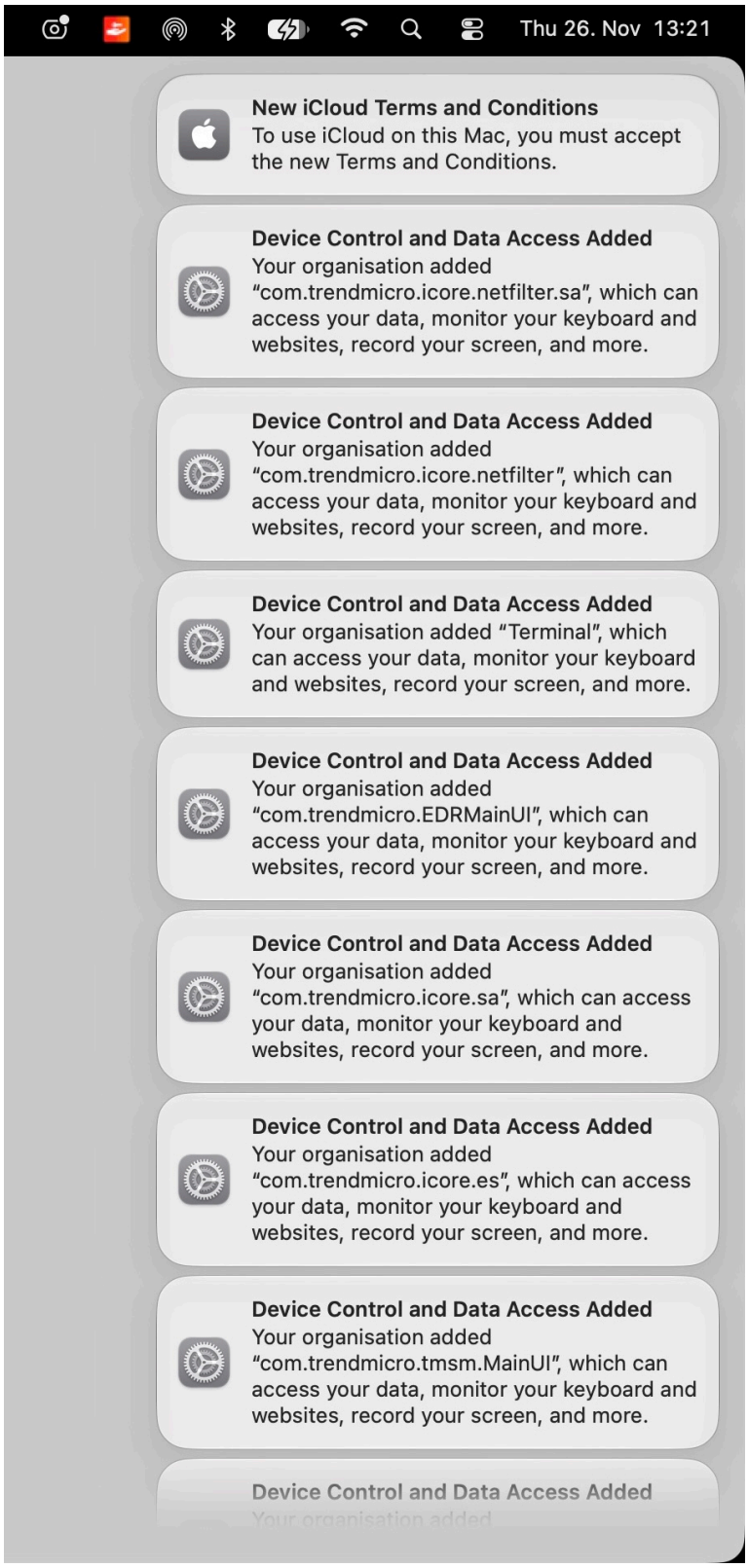
/allkirjastatud digitaalselt/

Varro Vooglaid
Riigikogu liige

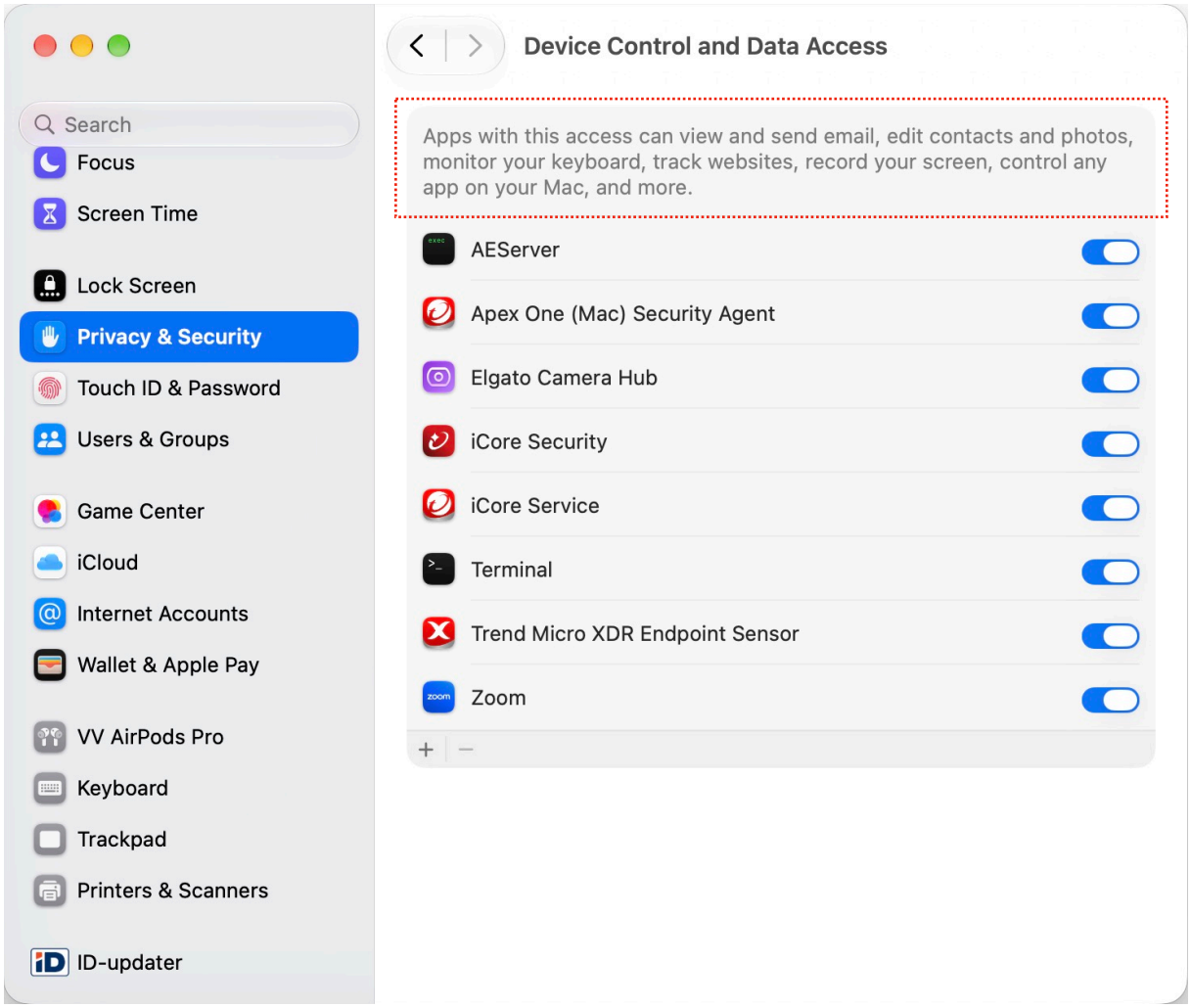
26. november 2026

Lisad: ekraanipildid operatsioonisüsteemi teadetest, arvuti juurdepääsuõiguste seadistustest ja protsessi TMLoginMgr ebatavaliselt suurest energiatarbimisest.

LISA 1. Ekraanipilt operatsioonisüsteemi tarkvarauuenduse järgsetest teadetest.



LISA 2. Ekraanipildid operatsioonisüsteemi juurdepääsuõiguste vaikeseadistustest.



LISA 3. Ekraanipilt protsessi TMLoginMgr ebatavaliselt suurest energiatarbimisest.

