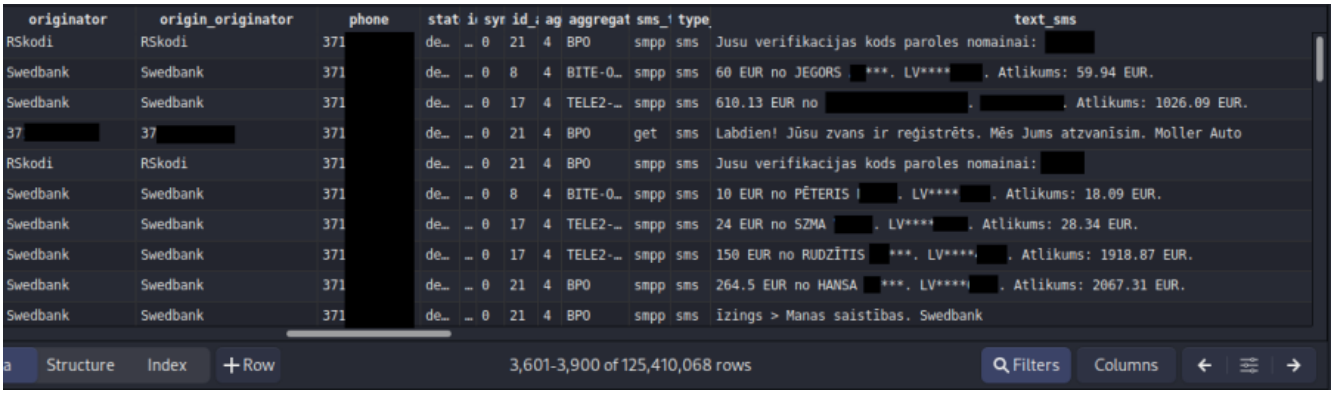
Viimase nelja aasta sõnumid rippusid lahtisel veebiriiulil: andmeleke paljastas ka eestlaste teavitused

19 min tagasi - 12.11.2026 Autor: AM

Mis saab telefoniekraanile saabuvast lühisõnumist pärast seda, kui oled paki kättesaamise koodi pakiautomaati toksinud või lennule registreerunud? Enamasti kustutame me need südamerahuga või laseme lihtsalt vanade teavituste kultuurkihti vajuda. Paraku selgus nüüd, et miljonid sellised sõnumid elasid edasi kohas, kuhu pääses ligi igaüks, kel vähegi huvi.

Küberturbeportaali Cybernews uurijad avastasid hiljuti internetist täiesti kaitseta ja avalikult ligipääsetava andmebaasi, mis peitis endas enam kui 125 miljonit SMS-sõnumit. Lekke allikaks osutus telekommunikatsioonieттevõtte CSC Telecom Läti haru. Kuigi server asus lõunanaabrite juures, ulatub selle hooletuse vari otsapidi Eestisse: andmebaasis rullub lahti nelja aasta jagu tekstisõnumeid, mida teiste seas saatsid Eesti klientidele lennufirma AirBaltic ja ehituskaupluste kett DEPO.

Kõige kõhedusttekitavam on asjaolu, et leke ei olnud pelgalt vana ja tolmune arhiiv. Andmebaas sisaldas kirjeid alates 2022. aasta oktoobrist kuni 2026. aasta septembrini ning see uuenes reaalajas.



Ehituspoe tellimustest pangaandmete ja meditsiiniteadeteni

Eesti kasutajate puhul torkavad lekkinud andmestikus esimesena silma AirBalticu ja DEPO Eesti filiaalide saadetud teavitused. Neist sõnumitest vaatasid vastu reisijate perekonnanimed, detailsed lennuplaanid, klientide telefoninumbrid,

tellimuste numbrid ja teated kauba kohaletoimetamise kohta. Üksikuna võttes võib tunduda, et teadmine kellegi ostetud kruvikarbist või Riia-lennust pole maailma lõpp, kuid tervikpilt on märksa süngem.

Lisaks ees- ja perekonnanimedele ning telefoninumbritele olid täies mahus nähtavad sõnumite tekstid, mis sisaldasid ühekordseid turvakoode, pankade hoiatusi, arstivisiitide broneeringuid, meditsiiniliste analüüside tulemusi ning täpsete koduste aadressidega tarneteateid.

Andmebaasi olid koondunud sõnumid suurematelt pankadelt, meditsiiniasutustelt, populaarsetelt e-poodidelt, riigiasutustelt ja isegi Läti riiklikult hädaabinumbrilt 112. Tavaline SMS ei ole turvaline suhtluskanal, kuid olukord, kus teenusepakkuja jätab kogu sõnumiliikluse Internetti vedelema, muudab kasutaja täiesti kaitsetuks.

Nelja aasta sõnumitest saab kokku panna elulood

Kui pahalane saab enda käsutusse nelja aasta pikkuse sõnumiajaloo, ei ole tal vaja palju abi, et ohvrist terviklik pilt maalida. Selline andmehulk on nagu miljonist pisikesest killust koosnev digitaalne mosaiik: iga eraldiseisev teavitus on tühine, aga kui need kõik kõrvuti lauale laduda ja tehisarul analüüsida lasta, joonistub välja inimese täpne elumuster. Ründaja näeb täpselt, millises pangas sa arveldad, kus poodides käid, millal reisid ja kodu tühjaks jätad, milliseid terviseuuringuid sulle on tehtud ning kui palju raha kulutad.

„Tundliku teabe mitmekesisust võidakse kasutada iga telefoninumbri kasutaja kohta detailse profiili loomiseks ja nende anonüümsuse kaotamiseks," selgitasid Cybernewsi eksperdid.

See tähendab, et isegi kui telefoninumber oli varem seotud vaid mõne üksiku teenusega, võimaldab nelja aasta sõnumite ristviitamine viia numbri kokku konkreetse inimese, tema koduse aadressi ja terviseandmetega.

See on omakorda ideaalne vundament ülitäpsete õngitsusrünnakute ja petukõnede korraldamiseks – pettur teab sulle helistades täpselt, mis pangas sa oled ja millist pakki parasjagu ootad.

Miks hoiti lühisõnumeid alles ligi neli aastat?

Lisaks otsesele turvaohule tõstatab juhtum terava küsimuse Euroopa Liidu isikuandmete kaitse üldmääruse (GDPR) täitmise kohta. Andmekaitsereeglid ütlevad selgelt, et ettevõtted tohivad isikuandmeid säilitada vaid nii kaua, kui see on vajalik nende algselt seatud töötlemise eesmärgi täitmiseks.

Lühisõnumite vahendaja ülesanne on toimetada tekst punktist A punkti B. Kui sõnum on adressaadini jõudnud ja arveldus tehtud, kaob igasugune praktiline vajadus selle sisu säilitamiseks. Miks pidi telekomiettevõte hoidma sõnumite täistekste, telefoninumbreid ja metaandmeid alles peaaegu neli aastat? Sellele küsimusele peavad nüüd vastuse leidma andmekaitseasutused.

Seniks aga tasub oma digitaalne hügieen kriitilise pilguga üle vaadata. Kus vähegi võimalik, vaheta SMS-põhine kaheastmeline tuvastamine turvalisema autentimisäpi, Mobiil-ID või Smart-ID vastu ning suhtu äärmise ettevaatusega igasse ootamatusse sõnumisse, mis palub sul mõnele lingile klõpsata – isegi siis, kui saatja paistab teadvat sinu viimast ehituspoe tellimust.

- Uudised
- Turvalisus

Pilt

