Mazcenas risinājums drošai informācijas apstrādei

Sagatavoja: CERT.LV IT drošības speciālists Kārlis Podiņš
Publicēts: 2019.gada 10. janvārī

Eksistē jomas, kurās ar mazu budžetu un bez specifiskām zināšanām ir jānodrošina augsta drošības informācijas apstrāde – piemēram, pētnieciskie žurnālisti, NVO, u.c. Drošības risinājuma izvēle vislielākajā mērā ir atkarīga no apdraudējuma raksturojuma. Šajā rakstā tiek apskatīts potenciālais apdraudējums pret Latvijas pētniecisko žurnālistu, kura rīcībā esošā informācija atsevišķus indivīdus interesē tādā mērā, ka tie būtu gatavi nolīgt kibernoziedzniekus. Šajā rakstā piedāvāsim, pēc CERT.LV drošības ekspertu viedokļa, vienu no labākajiem risinājumiem, kurā sabalansēta drošība, funkcionalitāte un lietošanas ērtums - izmantojot Google pakalpojumus.

Īsumā apkopojums par „+" un „-":

+ Iekārtas un programmatūru izveidojuši, uztur un 24x7 režīmā monitorē Google inženieri.
Biežāk izmantotie uzbrukumi ir vērsti pret plaša pielietojuma operētājsistēmām – Windows, macOS un nespēs inficēt Google pakalpojumu serverus vai Chromebook iekārtu.

- Visa jūsu informācija un aktivitātes būs pieejamas Google korporācijai un noteiktos gadījumos tiesībsargājošām un drošības iestādēm[1]. Ja šis risks ir pieņemams, tad pakalpojuma izmantošana ir pieļaujama.

Risinājuma arhitektūra

Ja visu informācijas apstrādi pārvirza uz Google mākoņpakalpojumiem, kuriem piekļūst ar Google kontu no vienas Chromebook iekārtas, tad sensitīvā informācija paliek vienā noslēgtā, vertikāli integrētā ekosistēmā, ko izstrādājuši un 24x7 režīmā aizsargā vieni no pasaulē labākajiem inženieriem. Jūsu Chromebook būs vienīgā iekārta, no kuras būs iespējams piekļūt jūsu Google kontam – drošības vārdā gan nāksies aizmirst par e-pastu telefonā, paziņojumiem viedpulkstenī u.tml. funkcionalitāti.

No vienas puses jūs zaudējat kontroli pār informāciju, uzticot to Google pakalpojumiem. No otras puses jūs iegūstat ļoti drošu un kontrolējamu piekļuvi no ārpuses. Chrome operētājsistēmai ir ierobežota funkcionalitāte, un ļaundariem iegūt attālinātu kontroli pār iekārtu ir sarežģīti. Tipiskās dokumentu apstrādes vajadzības nodrošina Google standarta funkcionalitāte, vispār neizmantojot trešo pušu aplikācijas.

Ņemot vērā, ka risinājums balstās uz Google kontu, nepieciešams pievērst īpašu uzmanību konta paroles veidošanai un aizsardzībai.

1 Google publicē t.s. pārredzamības atskaiti par piekļuvi lietotāju datiem: https://transparencyreport.google.com/

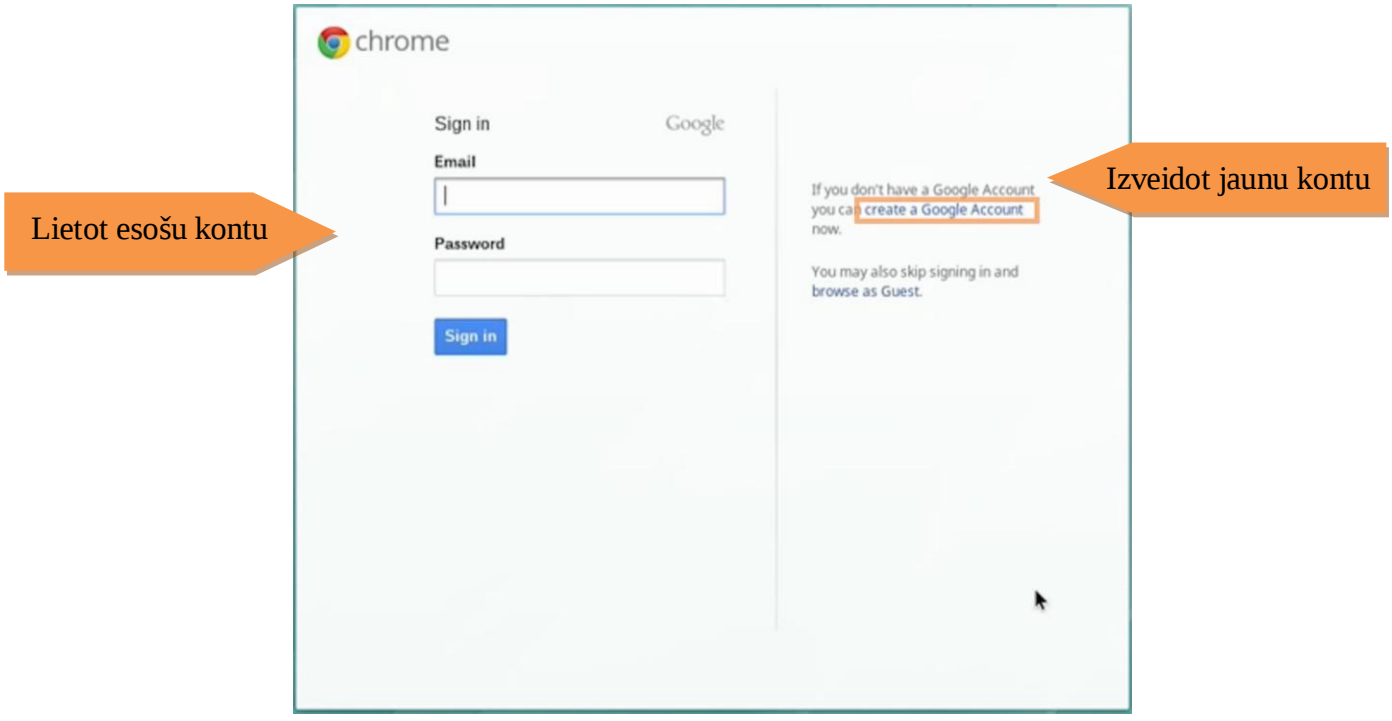
Izmaksas

Šī risinājuma izmaksas ir salīdzinoši zemas. Svarīgākā izmaksu pozīcija ir Chromebook klēpjdators (sākot no 200 EUR, vai arī var izmantot jau esošu Chromebook, pirms tam atjaunojot rūpnīcas iestatījumus – *power wash*) un vēlama arī fiziskā autentifikācijas iekārta (sākot no 40 EUR, atkarībā no funkcionalitātes). Abonēšanas maksas nav, tāpat nav nepieciešams personāls iekārtu uzturēšanai – iekārtas automātiski instalē operētājsistēmas atjauninājumus. Chromebook iekārtas būs funkcionālas ilgāku laiku, ja tās salīdzina ar klasiskiem datoriem, jo lielu daļu skaitļošanas veic serveri Google datu centros, turklāt Google sola, ka nopērkot jaunākā modeļa Chromebook iekārtām atbalsts un atjauninājumi tiks nodrošināti 6,5 gadus.

Google konta konfigurācija

Chromebook iekārta tiek piesaistīta īpašnieka Google kontam, t.i. nav atsevišķa iekārtas parole kā parasta datora gadījumā.

Ir iespējams izveidot gan jaunu Google kontu, gan izmantot esošo. Pareizi veicot konfigurāciju, abas iespējas ir vienlīdz drošas.

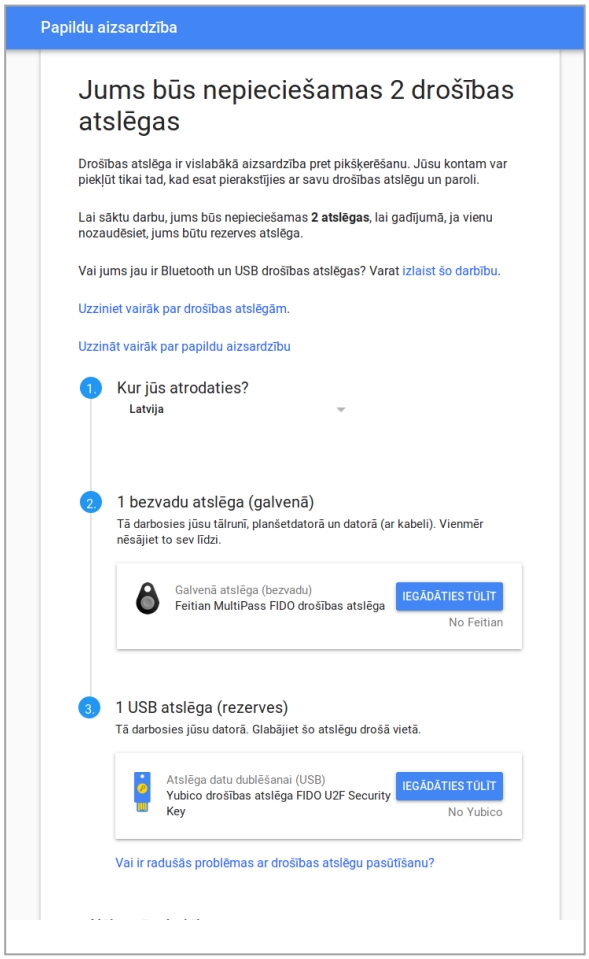


Visas darbības ar Chromebook piesaistīto Google kontu jāveic tikai no Chromebook iekārtas – šo Google kontu nedrīkstētu izmantot nekur citur. Jauna Google konta gadījumā jāizveido parole. Esoša Google konta izmantošanas gadījumā parole jānomaina.

Izveidojiet drošu paroli, sekojot kādai modernai, atzītai paroļu veidošanas metodoloģijai. Šo paroli jāizmanto vienīgi Google kontam, tādejādi samazinot konta uzlaušanas risku.

Papildu drošībai vēlams izmantot fizisku divfaktoru autentifikācijas iekārtu (*security key*). Piekļuvei jūsu kontam būs nepieciešama parole, un fiziskās autentifikācijas iekārtas pievienošana pie Chromebook (USB spraudnī vai izmantojot bezvadu savienojumus). Tas vienkāršākajā izpildījumā izmaksā dažus desmitus EUR, bet ļauj piedalīties Google papildu aizsardzības programmā (*Advanced Protection Program*), kuras ietvaros ir atslēgta daļa Google ekosistēmas funkcionalitāte, kas rada lielākos kiberdrošības riskus. Tāpat šo autentifikācijas iekārtu iespējams pievienot Twitter, Facebook u.c. kontiem.

Pieslēgt papildu aizsardzību iespējams lapā: https://myaccount.google.com/advanced-protection/enroll/details

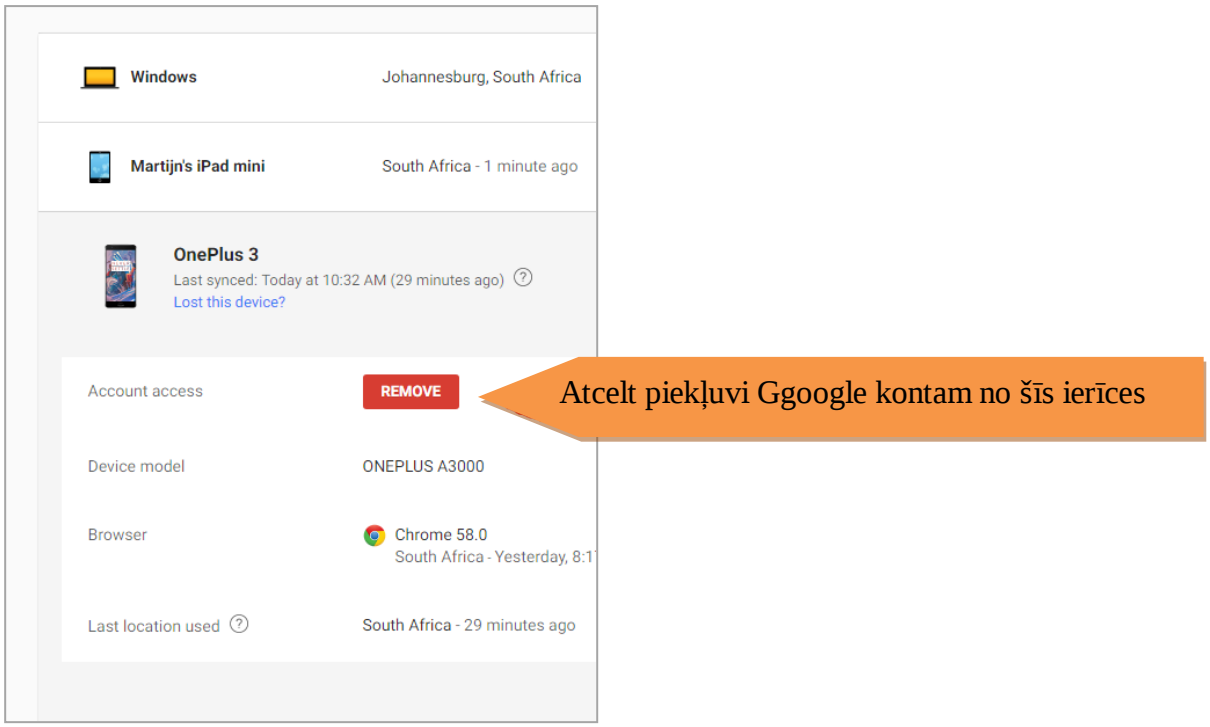


Tiek izveidotas divas autentifikācijas iekārtas – lietošanā esošā, kā arī rezerves – lai tehnisku problēmu gadījumā spētu piekļūt savam Google kontam.

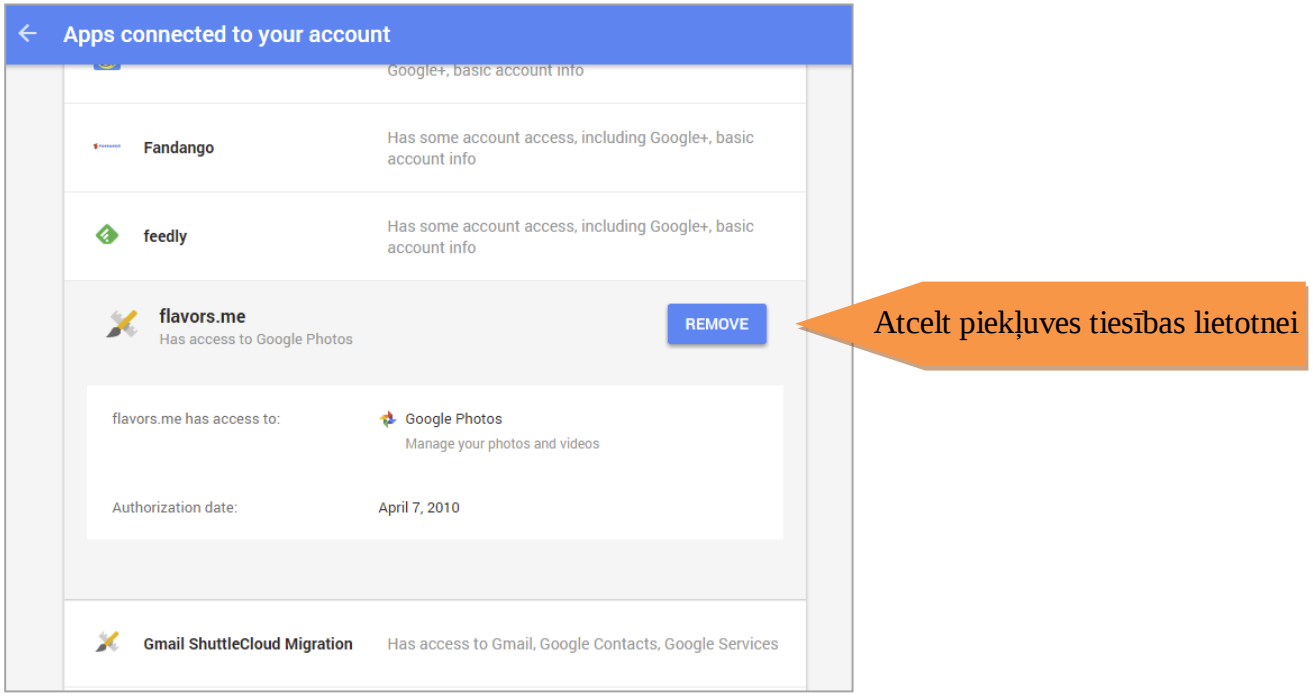
Šajā risinājumā iespējas atgūt pieeju Google kontam, ja nozaudēta autentifikācijas iekārta vai aizmirsta parole, ir stipri ierobežotas, un aizņem vairākas dienas. Tāpēc rezerves divfaktoru autentifikācijas iekārtu un uz papīra pierakstītas paroles (ja tādu izveidojat, neuzticoties savai atmiņai) glabāšana ir vēl viens risks, kura risinājums atkarībā no apdraudējuma līmeņa varētu būt seifs, bankas glabātuve vai „burka, kas bezmēness naktī norakta kādā mazapmeklētā dabas liegumā".

Ja izlemjat lietot jau esošu Google kontu, konta konfigurācijas lapā jāatceļ **visu** iepriekš lietoto ierīču autentifikācija, kā arī **visu** lietotņu tiesības darboties ar Google kontu. Jaunam kontam, kas izveidots no Chromebook iekārtas, nav jābūt citām autentificētām iekārtām un lietotnēm.

Autentificētās iekārtas var pārvaldīt Google konta sadaļā "pierakstīšanās un drošība": https://myaccount.google.com/security#activity



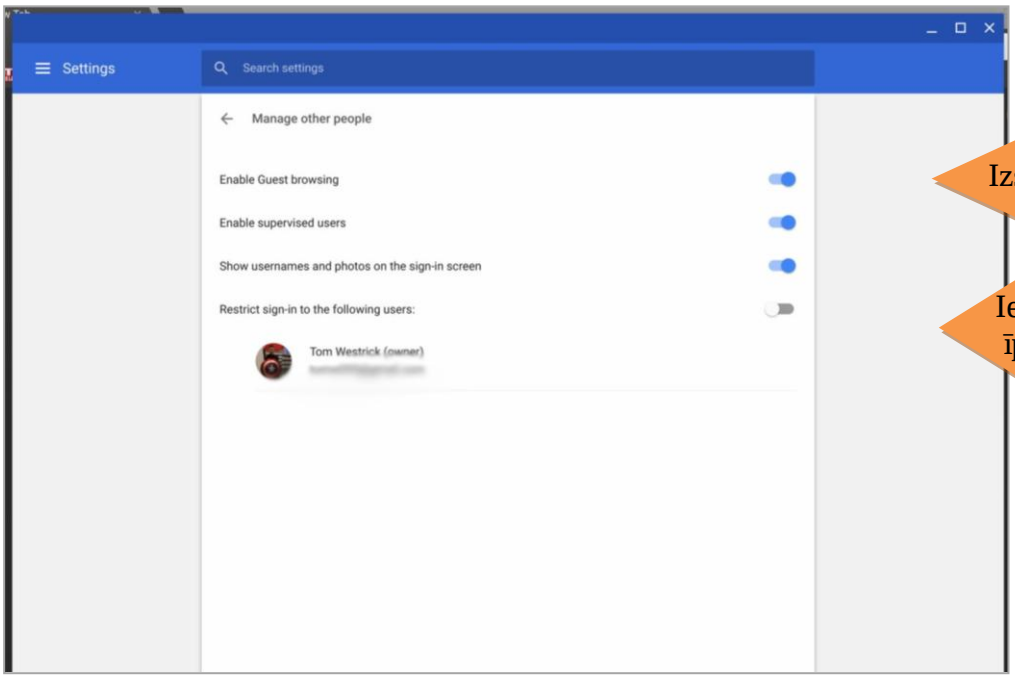
Autorizētās lietotnes var pārvaldīt sadaļā "lietotnes, kas var piekļūt jūsu kontam": https://myaccount.google.com/security#connectedapps.



Chromebook iekārta un tās konfigurācija

Ieteicams izvēlēties vieglu un izturīgu iekārtu, jo adekvāta drošības līmeņa nodrošināšanai tai vienmēr jābūt jums līdzās. Fiziska piekļuve iekārtai ļaundariem paver iespējas piekļūt jūsu sensitīvajai informācijai.

Chromebook iekārta jau ar rūpnīcas iestatījumiem ir ļoti droša. Iekārtas konfigurācijā jāatslēdz iespēja izmantot viesu profilu (*guest account*), un jāatļauj pieslēgšanos iekārtai tikai ar jūsu Google kontu (*restrict sign-in to the following users*) – tādējādi iekārtu varēs izmantot tikai ar jūsu Google kontu un paroli. Tāpat uz iekārtas vajadzētu instalēt pēc iespējas mazāk aplikāciju no Google PlayStore, kā arī piesardzīgi izvēlēties apmeklējamās mājaslapas. Vēl augstākam drošības līmenim var izvērtēt risinājumus, kā ierobežot sekošanu, izmantojot sīkdatnes.



Noslēgums

Jūs esat izveidojis samērā noslēgtu un grūti uzlaužamu risinājumu tipiskiem biroja uzdevumiem – teksta dokumentiem, izklājlapām, prezentācijām, audio un video atskaņošanai, e-pastam u.tml. Uz Chromebook iekārtas nebūs iespējams instalēt patvaļīgu programmatūru, bet arī ļaundaru iespējas pievienot savu programmatūru būs stipri apgrūtinātas. Visu sensitīvo informāciju turpmāk būtu jāapstrādā tikai uz Chromebook iekārtas un ar to saistītajā Google kontā, kontam nepieslēdzoties no citām ierīcēm. Tāpat regulāri pārskatiet drošības notikumu žurnālēšanas ierakstus par ierīcēm, kas pieslēgušās Google kontam. Aizdomu gadījumos vērsieties CERT.LV vai pie Google palīdzības dienesta.