

Ní hionann criptiú agus a bheith príobháideach: cad a deir meiteashonraí fút

Dhá rud dhifriúla is ea ábhar criptithe agus meiteashonraí infheicthe. Nuair a labhraíonn seirbhís faoi "chriptiú deireadh-go-deireadh", ní insíonn sí ach leath an scéil.

An glas nach gcosnaíonn gach rud

Fógraíonn cuid mhór de sheirbhísí teachtaireachtaí an lae inniu criptiú deireadh-go-deireadh. Agus is fíor é: taistealaíonn ábhar na dteachtaireachtaí criptithe, sa chaoi nach féidir le duine ar bith ar an mbealach – ná fiú an soláthraí seirbhíse – an téacs a léamh agus é á tharchur. Go dtí sin, tá an ráiteas cruinn.

Is é an fhadhb ná nach bhfuil san ábhar ach cuid den scéal. Cé nach féidir le duine ar bith an méid a deir tú a léamh, tá rudaí eile ar eolas ag an tseirbhís le cruinneas an-ard: cé leis a labhraíonn tú, cén t-am, cé chomh minic, ó cén suíomh garbh, ar cén gléas, cé mhéad teachtaireacht a sheolann tú agus cé mhéad a fhaigheann tú, cé mhéad comhad a roinneann tú. Meiteashonraí (metadata) a thugtar air seo ar fad. Agus deir meiteashonraí, i go leor cásanna, beagnach an oiread céanna leis an teachtaireacht féin.

Cad a nochtann meiteashonraí

Ní gá teachtaireacht a léamh chun go leor rudaí a fháil amach. Má ghlaonn duine ar oinceolaí nó má scríobhann sé chuige gach maidin Máirt ag a naoi a chlog ar feadh sé mhí, ní gá an comhrá a chlosteáil chun tuairim a fháil faoi cad atá ag tarlú. Má mhalartaíonn beirt céad teachtaireacht sa lá agus má stopann siad go tobann de é a dhéanamh, ní gá ceann amháin a léamh chun an méid a tharla a thuiscint. Má fhaigheann comhairleoir cánach fiche teachtaireacht i ndiaidh a chéile ón gcliant céanna an oíche roimh dhúnadh ráithiúil, labhraíonn an patrún as féin.

Nochtann meiteashonraí patrúin iompair: cé atá i gcuidreamh le cé, cad iad na sceidil atá ag gach duine, cathain a bhíonn siad ina ndúiseacht, cathain a bhíonn siad ina gcodladh, cathain a thaistealaíonn siad, cé na cliaint is gníomhaí, cé na caidrimh ghairmiúla is déine. Is féidir le freastalaí a bhailíonn meiteashonraí próifíl mhionsonraithe a thógáil de shaol pearsanta agus gairmiúil aon úsáideora gan focal amháin den mhéid a scríobhann sé a léamh riamh.

Tá sampla stairiúil ann a léiríonn é seo go crua. Chuir iar-stiúrthóir an NSA, Michael Hayden, in iúl é go neamhbhalbh in 2014: *"We kill people based on metadata"*. Thagair an ráiteas d'oibríochtaí míleata na SA i gcoinne spriocanna a aithníodh go heisiach bunaithe ar a bpatrúin chumarsáide. Níor léadh teachtaireacht amháin. An graf teagmhála agus na sceidil amháin.

An bhfíric go mbailíonn seirbhís meiteashonraí, ní chiallaíonn sé go riachtanach go n-úsáidfidh sí iad i gcoinne a húsáideoirí. Ciallaíonn sé go bhfuil an cumas aici é sin a dhéanamh, agus go bhfuil an cumas sin freisin ag tríú páirtí a bhfuil rochtain aige ar na sonraí sin – trí ordú cúirte, trí shárú slándála nó trí dhíol le tríú páirtithe má cheadaíonn téarmaí na seirbhíse é.

Rochtain ar an leabhar teagmhála

Veicteoir eile a théann beagnach gan tabhairt faoi deara: an liosta teagmhála. Iarrann cuid mhór de sheirbhísí teachtaireachtaí rochtain ar leabhar teagmhála an fhóin agus iad ag clárú. Uaslódálann siad gach uimhir chuig a bhfreastalaí chun a thaispeáint cé eile atá ag úsáid na seirbhíse. Ón nóiméad sin, tá léarscáil iomlán ag an gcuideachta de chaidrimh an úsáideora, fiú mura bhfuil teachtaireacht amháin scríofa aige do dhuine ar bith riamh.

I gcás gairmí faoi rún gairmiúil – dlíodóir, dochtúir, síceolaí, comhairleoir – tá cliant sa leabhar teagmhála sin. Má uaslódáladh an leabhar teagmhála chuig freastalaí tríú páirtí, tá ainmneacha na gcliant i mbonneagar nach bhfuil smacht ag an ngairmí ar a dhlínse agus ar a bheartais. Ní bhriseann an rún gairmiúil an lá a sceitheann duine éigin comhrá: briseadh é i bhfad níos luaithe, ag tráth an toilithe don uaslódáil.

An difríocht idir criptiú agus gan bailiú

Is éard is criptiú ann ná an t-ábhar a chosaint. Is éard is príobháideacht ann ná gan an rud nach dteastaíonn a bhailiú. Rudaí difriúla iad seo, agus tá an difríocht ríthábhachtach ó thaobh oibríochta de. Is féidir le seirbhís gach teachtaireacht a chriptiú go foirfe agus ag an am céanna fios a bheith aici ar beagnach gach rud faoina húsáideoirí trí mheiteashonraí. Tá an dá rud ag luí go hiomlán le chéile. Go deimhin, is é an tsamhail ghnó is mó sa tionscal é.

Ní hé an cheist cheart chun fíorphríobháideacht seirbhíse a mheas ná "*an gcriptíonn sí an t-ábhar?*". Tá an cheist sin freagartha le blianta anuas. Is é an cheist cheart ná: "*cad iad na meiteashonraí a ghineann sí agus cá stóráiltear iad?*". Agus, thar aon rud eile: "*cad iad na meiteashonraí nach gá di a ghiniúint?*".

Tá bonneagar a íoslaghdaíonn meiteashonraí trí dhearadh (privacy by design) – ní trí ghealltanais, ní trí bheartas inmheánach – níos príobháidí ó thaobh struchtúir de ná bonneagar a bhailíonn agus a chriptíonn iad. Toisc nach féidir sonraí nach bhfuil ann a sceitheadh, ná a dhíol, ná a thabhairt do ordú cúirte nó a chailliúint i sárú slándála.

Don léitheoir gairmiúil

Má chuimsíonn do ghníomhaíocht ghairmiúil rún, rúndacht nó go simplí meas ar fhaisnéis tríú páirtithe, is fiú na ceisteanna a chur san ord seo:

1. An gcriptíonn an aip a úsáidim le haghaidh cumarsáide an t-ábhar? (Is dócha go gcriptíonn.)
2. An gcriptíonn sí na meiteashonraí? (Is dócha nach gcriptíonn.)
3. An gineann sí meiteashonraí *nach dteastaíonn* uaithi chun feidhmiú? (Beagnach cinnte go ngineann.)
4. Cá bhfuil na meiteashonraí sin stóráilte agus faoi cén dlínse? (Is dócha lasmuigh den Limistéar Eacnamaíoch Eorpach.)
5. An bhfuil a fhios ag mo chliant nó ag mo phaitinn go bhfuil a chuid sonraí ansin?

Is í an cheist dheireanach an ceann míchompordach. Toisc gurb é an freagra macánta i bhformhór na gcásanna ná: níl.

Is é an t-alt seo an chéad cheann i sraith faoi fhíor-oibriú uirlisí cumarsáide gairmiúla. Pléifidh eagráin amach anseo comhlíonadh GDPR i dteachtaireachtaí agus coincheap an rúin ghairmiúil san aois dhigiteach.

Foinsí agus léitheoireacht bhreise

- Hayden, M. – Dearbhú ag Ollscoil Johns Hopkins, 2014 ("We kill people based on metadata"). Athscríbhinní poiblí ar fáil.

- GDPR (Rialachán an AE 2016/679), Airt. 4 agus 5 – sainmhíniú ar shonraí pearsanta agus prionsabail na próiseála (is sonraí pearsanta iad meiteashonraí).
- EDPS agus EDPB – tuairimí ar phróiseáil sonraí tráchta agus meiteashonraí i gcumarsáid leictreonach (treoir ePrivacy).

[← Roimhe seo](#)[Stair ghearr ar an tseala céir](#)[Ar aghaidh → An rún gairmiúil san aois dhigiteach](#)

Léitheoireacht le déanaí

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Beir an t-alt seo leat áit ar bith a dteastaíonn sé uait.

[↓ Markdown](#) [↓ Téacs simplí](#) [↓ PDF](#)

Íoslódálfar an comhad chuig do ghléas. Ón áit sin is féidir leat é a shábháil, é a iompórtáil go Solo2 nó é a roinnt cibé áit is mian leat. Ní chinneann Cuadernos an ceann scríbe duitse.

Séala céir · SHA-256 b886ca926a801e7c03b2e4cbc134eefc334519feb7496feda5172b0207d46f44

Cuadernos Lacre · Foilseachán de chuid [Menzuri Gestión S.L.](#) · scríofa ag R.Eugenio · curtha in eagar ag foireann [Solo2](#).

Ní úsáideann an suíomh Gréasáin seo fianáin agus ní lódálann sé acmhainní ó thríú páirtithe. Úsáideann sé cuntar cuairteanna anaithnid féin-óstáilte (Umami, ar ár bhfreastalaí Eorpach) agus an t-íosmhéid JavaScript is gá le haghaidh do rogha téama éadrom/dorcha. Gan lorgaire, gan próifiliú, gan roinnt sonraí. Más mian leat sinn a leanúint: [RSS](#).