

Nuair nach mbíonn aon duine idir eatarthu

Cosnaíonn criptiú an ábhair a théann trí fhreastalaí an t-eolas. Má bhíonn an freastalaí as an áireamh, ní gá an cheist a chur fiú. Ní hionann an dá rud.

Beirt duine, comhrá amháin

Nuair a bhíonn beirt ag caint duine le duine i seomra, ní gá d'aon duine geallúint a thabhairt nár chuala siad aon rud. Níor chuala siad é mar ní raibh siad ansin. Nuair a thugann beirt píosa páipéir dá chéile, ní gá d'aon duine eatarthu mionnú nár léigh siad é. Níl aon duine idir eatarthu.

Sin mar a oibríonn an chuid is mó de rudaí sa saol laethúil. Ní shínimid comhaontuithe rúndachta leis an aer a iompraíonn ár nglórtha, ná leis an bpáipéar atá inár lámha. Ní bhraitheann rún an chomhrá ar gheallúint ó idirghabhálaí, mar níl aon idirghabhálaí ann. Sin ceann de na bealaí is láidre le bheith príobháideach: ní mar gheall go n-iompraíonn duine nó rud éigin go maith iad féin, ach mar nach bhfuil aon duine nó rud ann.

Nuair a bhogtar an comhrá go cainéal digiteach, athraíonn sé seo de réir réamhshocraithe. Is é seo an gnáthmhúnla: nascann beirt le freastalaí, faigheann an freastalaí an teachtaireacht, criptíonn sé é nó stóráilann sé criptithe é, agus tugann sé don fhaighteoir é. Tá an freastalaí sa lár. Is féidir leis an bhfreastalaí a bheith macánta. Is féidir iniúchadh a dhéanamh air. Is féidir leis feidhmiú i ndlínse fhabhrach agus faoi pholasaí príobháideachais docht. Is féidir go bhfuil sé sin ar fad fíor. Ach tá an freastalaí sa lár.

An difríocht idir criptiú agus gan bailiú (an dara cuid)

In alt níos luaithe sa tsraith seo, d'argóineamar nach hionann criptiú an ábhair agus gan meiteashonraí a bhailiú. Tá céim eile ann ar chóir a rá go soiléir: ní hionann ach oiread rud a chriptiú a théann trí fhreastalaí agus gan freastalaí a bheith ann ar chor ar bith.

Cosnaíonn an chéad mhúnla — freastalaí sa lár, ábhar criptithe — an t-eolas ó oibreoir an fhreastalaí, ón bhfoireann cothabhála, nó ó ionsaitheoir seachtrach a dhéanann dochar don chóras. Agus tá sé sin tábhachtach. Ach ní chuireann sé deireadh leis an bhfreastalaí. Tá an freastalaí fós ansin. Tá sé fós ag próiseáil meiteashonraí. Is pointe é fós a bhféadfadh ordú cúirte, idirghabháil dhlíthiúil, brú polaitiúil, nó sárú slándála tarlú dó. Is pointe é fós ar gá muinín a chur i dduine éigin.

Ní chosnaíonn an dara múnla — gan freastalaí a bheith idir an dá cheann — an t-ábhar criptithe níos fearr: má tá an chriptagrafaíocht láidir, tá an t-eolas cosanta sa dá chás. Ní hé an t-ábhar a athraíonn. Is é an rud a athraíonn ná nach mbaineann an cheist «*céard faoin bhfreastalaí?*» le hábhar a thuilleadh, mar níl aon fhreastalaí ann le ceist a chur faoi.

Iontaobhas, easpa, agus an difríocht eatarthu

Is féidir an t-iontaobhas a bheith tuillte. Tá cuideachtaí macánta ann. Tá iniúcháirí dian ann. Tá dlíthe atá fabhrach don úsáideoir ann. Tá seirbhísí tromchúiseacha ann a chloíonn go hiomlán leis an méid thuas. Ní droch-

shocrú é an t-iontaobhas, nuair a thugtar d'oibreoir é atá ina thuilleamaí.

Ach is iontaobhas é an t-iontaobhas i gcónaí, is cuma cé chomh láidir is atá sé. Is réiteach sóisialta é, ní réiteach teicniúil. Is féidir le cuideachta úinéirí a athrú. Is féidir le dlínse rialtas a athrú. Is féidir le hordú cúirte teacht amárach. Is féidir leochaileacht nua a aimsiú an mhí seo chugainn. Ní tharlaíonn aon chuid de seo de bharr droch-rúin. Tarlaíonn sé mar go bhfuil an t-oibreoir ann, agus tá gach rud atá ann faoi réir thaismeacha an tsoil.

Níl easpa oibreora faoi réir na dtaismeacha céanna sin. Ní féidir le hordú cúirte sonraí a iarraidh ó fhreastalaí nach bhfuil ann. Ní féidir le hionsaitheoir dochar a dhéanamh d'fhreastalaí nach bhfuil ann. Ní féidir le hathrú i bpolasaí cuideachta dul i bhfeidhm ar shonraí nach raibh ag an gcuideachta sin riamh. Tá an frása tábhachtach simplí: ní féidir sonraí nach bhfuil ann a chailleadh.

Maidir leis an argóint dhlísteanach ar thaobh an fhreastalaí

Is gnách go mbíonn trí argóint bhailí ag an té a thairgeann seirbhís teachtaireachtaí gairmiúil le freastalaí sa lár. Ar an gcéad dul síos, go bhfuil an freastalaí riachtanach chun seachadadh a chinntiú nuair a bhíonn an faighteoir as líne. Ar an dara dul síos, go bhfuil criptiú an ábhair láidir agus nach féidir leis an oibreoir é a léamh dá bhrí sin. Ar an tríú dul síos, go gcloíonn an tseirbhís le dlí na hEorpa agus go bhfuil na sonraí cosanta ag an dlí.

Tá an trí argóint sin fíor. Ní athraíonn ceann ar bith acu nádúr an scéil. Is fíor go gceadaíonn freastalaí teachtaireachtaí a stóráil le haghaidh seachadadh níos déanaí; is fíor freisin gur féidir seachadadh moillithe a réiteach ar bhealach eile, trí phrótacail chumarsáide dhíreacha idir gléasanna atá á bhfeabhsú le blianta fada agus atá i bhfeidhm inniu. Is fíor go bhfuil criptiú an ábhair faoi bhealach láidir i seirbhísí tromchúiseacha. Agus is fíor go gcosnaíonn dlí na hEorpa úsáideoirí níos mó ná dlíthe go leor áiteanna eile.

Ní hé an cheist an bhfuil seirbhísí le freastalaí sa lár dlíthiúil, ná an bhfuil siad sábháilte, ná an gcosnaíonn siad an t-eolas. Is féidir leo a bheith, tá siad dlíthiúil, agus de ghnáth bíonn siad sábháilte. Is é an scéal ná gur rogha ailtireachta é freastalaí a bheith sa lár, ní éigeantas teicniúil é. Agus bíonn iarmhairtí ag gach rogha. Gintear gníomhaí i gcónaí in ailtireacht le freastalaí sa lár ar gá muinín a bheith agat as. Ní tharlaíonn sé sin le hailtireacht gan freastalaí sa lár.

An rud a deir an dlí, agus an rud a dhéanann an ailtireacht

Ní éilíonn an GDPR múnla sonrach ailtireachta. Éilíonn sé torthaí: íoslaghdú sonraí, cuspóir teoranta, cosaint trí dhearadh agus de réir réamhshocraithe, agus an cumas an comhlíonadh a léiriú. Is féidir le seirbhís le freastalaí sa lár na riachtanais seo go léir a chomhlíonadh. Cloíonn seirbhís gan freastalaí sa lár le go leor acu trí thógáil, ní trí dhearbhu. Tá íoslaghdú iomlán — gan aon rud a bhailiú nach bhfuil fíor-riachtanach chun an teachtaireacht a sheachadadh — simplí nuair nach bhfuil freastalaí ann a d'fhéadfadh aon rud a bhailiú.

Maidir le gnáthúsáid nach bhfuil íogair, tá ailtireacht le freastalaí go hiomlán réasúnta, agus is socrú bailí é muinín a chur in oibreoir tromchúiseach. Maidir le húsáidí eile — iad siúd a bhaineann le rún gairmiúil rialaithe, iad siúd a bhfuil freagracht dhiantalach ag baint leo, nó iad siúd a bhaineann le faisnéis an-íogair — ní só é easpa pointe muiníne, is buntáiste struchtúrach é.

Don léitheoir gairmiúil

Comhlánaítear na ceisteanna ba chóir a chur maidir le seirbhís cumarsáide gairmiúil, atá eolach cheana féin ó ailt roimhe seo sa tsraith seo, le ceist ailtireachta amháin eile:

1. An gcriptíonn sé an t-ábhar faoi bhealach? (Is dócha go ndéanann.)
2. An ngineann agus an stóráil sé meiteashonraí faoin té a mbím ag caint leis agus cathain? (Is dócha go ndéanann.)
3. An bhfuil freastalaí ar an mbóthar idir mo ghléas féin agus gléas an fhaighteora?

4. Má tá: cé a oibríonn é, cén dlínse ina bhfuil sé, agus céard ba ghá tarlú sula dtabharfadh sé sonraí fúm?
5. Mura bhfuil: ní bhaineann na ceisteanna thuas le hábhar.

Níl an difríocht idir an dá chatagóir ina méid, ach ina gcineál. Agus é á mhíniú do chliant, d'othar, nó do chomhghleacaí, is é an fhoirmle is macánta an ceann is simplí freisin: i gcás amháin tá duine éigin sa lár; sa chás eile, níl.

Dúnann an t-alt seo an chéad sraith de Cuadernos Lacre. Tar éis dúinn labhairt faoi chriptiú, meiteashonraí agus rún gairmiúil, críochnaímid an pictiúr ailtireachta: is rudaí difriúla iad criptiú an ábhair agus gan freastalaí a bheith sa lár. Is féidir leis an dá rud a bheith dlíthiúil; ní chuireann ach ceann amháin deireadh leis an bpointe muiníne.

Foinsí agus léitheoireacht bhreise

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Bunús an phrionsabail gur chóir ráthaíochtaí córais a chur i bhfeidhm ag na foircinn, ní sa chainéal idirmheánach.
- Rialachán (AE) 2016/679, Airt. 25 — cosaint sonraí trí dheardh agus de réir réamhshocraithe.
- Rialachán (AE) 2016/679, Airt. 5.1.c — prionsabal íoslaghdaíthe sonraí.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Caibidlí ar ailtireachtaí a íoslaghdaíonn bailiú sonraí trí thógáil.

[← Roimhe seo](#)[GDPR agus teachtaireachtaí gairmiúla: cén fáth go sáraíonn an chuid is mó na rialacha gan fios a bheith acu](#)[Ar aghaidh](#) → [CUADERNOS LIST SCHREMS TITLE](#)

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 d3d6c18c2592bface57957e97b3cd832606b0e005ab3851e645689ef7c6aa849

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](#).